REQUERIMIENTO

I. ESPECIFICACIONES TÉCNICAS

1. DENOMINACIÓN DE LA CONTRATACIÓN

Provisión de solución de seguridad perimetral de Red y Equipos Balanceadores de la marca F5 Networks o equivalente para la plataforma de internet de SUNAT.

2. FINALIDAD PÚBLICA

Garantizar operatividad e incrementar el nivel de disponibilidad de los servicios que brinda la SUNAT, para la prestación de un servicio de calidad, que permita las coordinaciones entre los miembros de la institución y éstos con terceros, garantizando al personal las herramientas suficientes mientras presten sus servicios para la SUNAT, a fin de lograr un óptimo resultado en los objetivos propuestos por la institución, fortaleciendo la capacidad de gestión interna.

La SUNAT dentro de su PEI (2018-2020) ha establecido sus objetivos estratégicos institucionales, entre los cuales se encuentra en el Objetivo Estratégico N° 01: "Mejorar el cumplimiento tributario y aduanero", indicando que la SUNAT, como parte del Estado, desarrollará los mecanismos y estrategias necesarios para, en el marco de sus competencias, mejorar significativamente el cumplimiento de las obligaciones tributarias y aduaneras por parte de los contribuyentes y usuarios de comercio exterior.

3. ANTECEDENTES

La SUNAT tiene la misión de servir al país proporcionando los recursos necesarios para la sostenibilidad fiscal y la estabilidad macroeconómica. En ese contexto, la administración tiene como prioridad maximizar el cumplimiento tributario, o minimizar las brechas de incumplimiento, manteniendo la confianza en el sistema tributario y su administración.

La SUNAT cuenta con dos centros de cómputo capaces de atender los servicios internet. Un data center es contingencia del otro y cada uno se encuentra en capacidad de atender la carga de los usuarios a través de la internet.

En cada centro de cómputo se tiene un grupo de servidores web, los cuales poseen un contenido idéntico.

Los servicios web que la SUNAT brinda se basan actualmente bajo los protocolos HTTP y HTTPS (SSL).

Se dispone de cuatro (04) enlaces (desde y hacia) internet por cada centro de cómputo, los cuales tienen una operación independiente y manejan un rango de IPs públicas por cada enlace. Los servicios web que la SUNAT brinda se basan actualmente bajo los protocolos HTTP y HTTPS (SSL).

Los servidores web de cada centro de cómputo accedan a los servidores de aplicaciones de su propia sede.

A nivel de bases de datos, se mantienen en ambos centros de cómputo las cuales se encuentran replicadas en el modo de operación activo / activo.

4. OBJETIVOS DE LA CONTRATACIÓN

4.1. Objetivo general

Garantizar la continuidad de la operatividad e incrementar el nivel de disponibilidad de los servicios que brinda la SUNAT a los contribuyentes.

4.2. Objetivo específico

Renovación tecnológica de la plataforma de seguridad perimétrica y equipos Balanceadores que gestionan los servicios web que se brinda a través de internet vía la adquisición del equipamiento correspondiente por un periodo de 1826 días calendarios.

5. DEFINICIONES

Cuando se mencione en la presente los siguientes términos y expresiones tendrán el significado que se indica a continuación:

(a) **Sistema, Solución, Plataforma,** Equipos es el conjunto de bienes, servicios, hardware, software y accesorios a ser provistos por el Proveedor de acuerdo con el Contrato.
(b) **SUNAT,** Superintendencia Nacional de Aduanas y de Administración Tributaria.
(c) **Contratista,** El proveedor que celebra un contrato con una Entidad de conformidad con las disposiciones de la Ley y el Reglamento
(d) **Postor,** participante que presenta su oferta en el procedimiento de selección.
(e) **DGIT,** División de Gestión de Infraestructura Tecnológica.
(f) **DAT**, División de Arquitectura Tecnológica.
(g) **DEC,** División de Ejecución Contractual de la SUNAT.
(h) **Defecto, falla,** es cualquier algoritmo, rutina, subrutina u otra instrucción codificada, contenida en el software o firmware, capaz de causar al procesador que opere de manera incorrecta, o cualquier desperfecto en el hardware que impide que la solución opere correctamente.
(i) **SCTR,** Seguro Complementario de Trabajo de Riesgo.
(j) **EPP,** Equipo de Protección Personal.
(k) **Solución,** conjunto de sistemas
(l) **Sistema, Plataforma** es el conjunto de bienes, servicios, hardware, software y accesorios a ser provistos por el Contratista de acuerdo al Contrato.
(m) **Licencia,** Las licencias tienen carácter de perpetuidad, es decir no existe fecha de caducidad.
(n) **SO,** se refiere al sistema operativo.
(o) **Recurso**, Se refiere a los equipos o aplicaciones de SUNAT a los cuales se permitirá el acceso desde Internet.
(p) **Defecto, falla,** es cualquier algoritmo, rutina, subrutina u otra instrucción codificada, contenida en el software, capaz de causar al procesador que opere de manera incorrecta. Es cualquier desperfecto en el hardware que impide que la solución opere correctamente.
(q) **Documentación**, es el conjunto de manuales funcionales y de usuario, y otras especificaciones técnicas que serán suministradas por el contratista conjuntamente con la solución.
(r) **Sitio de instalación**, es el sitio y ubicaciones designados por la SUNAT para la instalación de los bienes y servicios adquiridos
(s) **Proyecto**, es el conjunto de actividades a llevar a cabo por el Contratista conforme al contrato para suministrar la solución, y brindar los servicios contratados.
(t) **Técnico certificado**, es el personal del postor que cuenta con una certificación del fabricante en la solución o equipos a ofertar. La certificación debe ser emitida a través del centro de instrucción autorizado por el fabricante. Puede ser profesional, bachiller, egresado, técnico o especialista.
(u) **Instructor certificado**, es la persona que cuenta con una certificación del fabricante para capacitar en la solución o equipos a ofertar. La certificación debe ser emitida a través del centro de instrucción autorizado por el fabricante. Puede ser profesional, bachiller, egresado, técnico o especialista.

1U1200 SUNAT FOLIO 13

6. CARACTERÍSTICAS Y CONDICIONES DE LOS BIENES A CONTRATAR

DESCRIPCIÓN Y CANTIDAD DE LOS BIENES.

ÍTEM	PRESTACIÓN	DESCRIPCIÓN GENERAL	CANTIDAD	UNIDAD DE MEDIDA
1	PRINCIPAL	Balanceadores externos F5 NETWORKS o equivalente	04	Unidades
		Balanceadores internos F5 NETWORKS o equivalente.	04	Unidades
	ACCESORIA	Soporte técnico, a todos los componentes que forman parte de la prestación	01	Servicio
		Servicio de gestión de la plataforma de balanceadores F5 NETWORKS o equivalente.	01	Servicio
2	PRINCIPAL	Solución de seguridad perimetral de Red de Segundo Nivel.	01	Unidades
		Solución de seguridad perimetral para Extranet.	01	Unidades
	ACCESORIA	Soporte técnico, a todos los componentes que forman parte de la prestación	01	Servicio

6.1 CARACTERÍSTICAS TÉCNICAS:

ITEM1:

6.1.1 BALANCEADORES EXTERNOS F5 NETWORKS O EQUIVALENTE

- Se requiere implementar Balanceadores externos(global) que permita a los usuarios externos acceder a través de internet todos los servicios y aplicaciones web de la SUNAT alojadas en los dos Data Centers con los que cuenta la Institución (San Isidro-Surco), haciendo uso de mecanismos de balance de sitios, balance de aplicaciones y servidores locales en cada sitio, haciendo uso de instancias independientes para el balanceo de sitios.
- Los Balanceadores deben ser capaces de realizar un monitoreo del estado de la operatividad de todos los componentes a balancear. Por Ej. Monitorear disponibilidad de las aplicaciones, de la infraestructura, integrándose con equipos del mismo fabricante o de terceros.
- Los Balanceadores deben ser de propósito específico o appliance configurado en alta disponibilidad local HA (1+1), tolerancia a fallas y balanceo de carga y que se instalará en cada Datacenter de la SUNAT (San Isidro y Surco).
- Los Balanceadores deben incluir el Hardware/software y licenciamiento necesario para la configuración en alta disponibilidad HA.
- Dentro de los criterios de alta disponibilidad HA se debe precisar que este es extensible a todos los componentes solicitado.
- Deben ser certificado (ICSA LABS) como Network-Firewall.
- Cada Balanceador debe tener como máximo 1RU.
- Cada Balanceador debe tener fuente redundante AC.
- Cada Balanceador deberá soportar **como mínimo**:
  - Throughput 4 Gbps (con todas las funcionalidades requeridas)
  - 500K conexiones por segundo en **capa 4.**
  - Hardware offload SSL/TLS.
  - Incluya proteccion DDoS en Hardware SYN cookies per second.

GERENCIA DE ARQUITECTURA - Gerencia de Arquitectura Tecnológica - JEFE (e) - JOHNNY ANTONIO VALDEZ ARBAYLO

GERENCIA NACIONAL DE SISTEMAS DE INFORMACIÓN - Gerencia de Arquitectura - GERENTE - FRANCISCO JAVIER ESPARTA CHAN

- La solución debe contar con almacenamiento interno de 400 GB.
- 4 interfaces de 10 Gigabit en Cobre.
- 2 interfaces de 10 Gigabit en Fibra SR.

- De requerirse debe incluir el cableado y patch cords correspondientes necesarios a ser instalados en cada Datacenter.
- Cada Balanceador deberá de realizar balanceo de carga en capas L4-L7 para todas las aplicaciones basadas en IP (TCP/UDP) soportando como mínimo los protocolos: TCP, UDP, FTP, HTTP, HTTPS, DNS (TCP y UDP), SIP (sobre UDP), RTPS, RADIUS, SQL, RDP
- Cada Balanceador deberá funcionar como un servidor DNS autoritativo de alto desempeño, permitiendo manejar un dominio completo o delegación de parte de un dominio.
- Cada Balanceador deberá permitir la persistencia a nivel global (GSLB), manteniendo las transacciones de los usuarios en un mismo Datacenter por el transcurso de su sesión.
- Los Balanceadores deben permitir balanceo de cargas entre Datacenter(sitio) de acuerdo con la ubicación geográfica. Ante la eventual caída de uno de los sitios, la solución debe ser capaz de direccionar toda la atención de los servicios hacia el sitio disponible. En caso de recuperación de dicho sitio, la solución debe ser capaz de detectar este evento y balancear la carga entre ambos sitios nuevamente.
    - Para algunos servicios permita realizar el balance activo-activo entre los sitios de forma tal que permita asignar carga a cada sitio, permitiendo definir el porcentaje de carga (ej. 50-50, 80-20.etc.)

- Ante la caída de uno de los enlaces de datos (internet), la solución debe ser capaz de detectar este evento y direccionar el tráfico hacia los enlaces disponibles. En caso de recuperación del enlace de datos, la solución debe ser capaz de detectar automáticamente este evento y balancear la carga considerando este enlace nuevamente.
- La solución debe considerar equipamiento para el balance de los enlaces internet a fin de que permita la publicación de los servicios en un entorno multihomed.
- Respecto al tráfico asignado por cada sitio, debe balancear la carga entre los enlaces internet que permiten la publicación de los servicios:
    - Round robin
    - Round robin por pesos
    - Según cantidad de conexiones
    - Según menor tiempo de respuesta
- Los Balanceadores deben controlar el tráfico basado en la geolocalización de los usuarios.
- Los Balanceadores deben proteger contra ataques de denegación de servicio tanto en una topología en línea (inline deployment) como en una topología fuera de línea (TAP mode)
- Debe bloquear ataques a nivel de red como flood, sweep, teardrop, smurf attacks.
- Debe mitigar ataques basados en protocolos, incluyendo SYN, ICMP, ACK, UDP, TCP, IP, DNS, ICMP, ARP
- Debe permitir la creación de reglas basadas en aplicación, independientes para cada una de ellas.
- Debe permitir la creación de reglas globales

- Debe contar con un sistema de protección basado en comportamiento de ataque personalizables.
- Debe incluir la funcionalidad de trabajar como un **firewall statefull full-proxy.**
- Los Balanceadores deben soportar bloqueo basado en geolocalización.
- Debe permitir la definición de horarios (schedules) que apliquen a las reglas configuradas, permitiendo activar reglas
    a) Entre intervalos de tiempo
    b) Hasta una fecha especifica
    c) Después de una fecha específica.
- Debe permitir la creación de listas blancas (White lists) de direcciones IP
- Debe incluir funcionalidad de application delivery controller o integrarse con dispositivos de Application Delivery
- Debe brindar protección contra Ataques de Denegación de Servicio para el protocolo DNS, poder controlar el tráfico DNS de acuerdo al tipo de Registro solicitado y detectar anomalías a nivel del protocolo.
- Debe permitir personalizar los Logs, y ser exportados a un repositorio Syslog externo que conste de uno o varios servidores.
- Debe soportar Port Miss-use, evitando que servicios que pasen través de puertos conocidos que buscan saltar protecciones de Firewall (por ejemplo, un servicio SSH escuchando en el puerto 80 y busque abusar de reglas orientadas a HTTP).
- Debe soportar RTBH (Remotely Triggered Black-hole Route Injection) para protección en caso de implementaciones fuera de línea.
- El equipo debe soportar direccionamiento IPv6 y gestionar clientes IPv6 o IPv4 de manera indiferente.
- Deberá estar habilitado y soportar bases de datos de reputación de IP que permita bloquear tráfico desde y hacia direcciones IP en categorías como:
    a) Scanners
    b) Exploits Windows
    c) Denial of Service
    d) Proxies de Phishing
    e) Botnets
    f) Proxies anónimos.

6.1.2 BALANCEADORES INTERNOS F5 NETWORKS O EQUIVALENTE.

- Los Balanceadores deben ser de propósito específico configurado en alta disponibilidad local HA (1+1), tolerancia a fallas y balanceo de carga y que se instalará en cada Datacenter de la SUNAT (San Isidro y Surco).
- Los Balanceadores deben incluir el Hardware/software y licenciamiento necesario para la configuración en alta disponibilidad HA.
- Dentro de los criterios de HA se debe precisar que este es extensible a todos los componentes solicitado.
- Deberán soportar instancias de balanceadores virtuales
- Lo Balanceadores deben permitir el escalamiento adicionando BLADES o CUCHILLAS adicionales lo cual incrementará las capacidades de performance de manera lineal del CHASSIS.
- Deberá ser certificado (ICSA LABS) como Network-Firewall.
- De requerirse debe incluir el cableado y patch cords correspondientes necesarios a ser instalados en cada Datacenter.
- Cada Balanceador debe tener fuente redundante AC.
- Cada Balanceador deberá soportar **como mínimo** por BLADE o CUCHILLA:

- 1.2 M Request per second en capa 7
- Hardware offload SSL/TLS
- Incluya proteccion DDoS en Hardware SYN cookies per second.
- Cada Balanceador deberá tener memoria: 64GB DDR4 por BLADE o CUCHILLA
- Cada Balanceador deberá contar con capacidad de almacenamiento interno de 500GB por BLADE o CUCHILLA.
- 2 BLADES o CUCHILLAS por CHASSIS.
- Seis (6) puertos de 10G cobre por BLADE o CUCHILLA.
- Seis (4) puertos de 10G SFP+ por BLADE o CUCHILLA
- Máximo licenciamiento de instancias virtuales permitidas por BLADE o CUCHILLA.

- Cada Balanceador deberá ser capaz de realizar balanceo de carga en capas L4-L7 para a todas las aplicaciones basadas en IP (TCP/UDP) soportando como mínimo los protocolos: TCP, UDP, FTP, HTTP, HTTPS, DNS (TCP y UDP), SIP (sobre UDP), RTPS, RADIUS, SQL, RDP
- Cada Balanceador deberá incluir **funcionalidad de Firewall de Aplicaciones (WAF) y** además contar con las siguientes características.
  - Proteger contra el robo de credenciales y datos mediante cifrado a nivel de la aplicación.
  - Realizar la detección y protección de DDoS en L7 utilizando sistemas de aprendizaje automático y análisis de comportamientos.
  - Brindar protección de protocolo API para REST/JSON, XML y GWT.
  - Identificación y mitigación de amenazas de robots malintencionados que intentan saltarse los métodos estándar de detección.
- Cada Balanceador deberá identificar, aislar y bloquear ataques sofisticados sin impactar en las transacciones de las aplicaciones
- Permitir que sólo aquellas aplicaciones validadas sean aceptadas, las transacciones restantes deberán ser bloqueadas utilizando bloqueo por nivel de aplicación basado en el contexto de la sesión del usuario, con privilegios de autorización diferentes.
- Deberá permitir la creación de firmas personalizadas
- Deberá permitir diferentes políticas para diferentes aplicaciones
- Permitir la utilización de un modelo de seguridad positivo a fin de proteger clases enteras de HTTP y HTTPS, más allá de la protección a los ataques conocidos.
- Debe trabajar con modelos de seguridad positiva y negativa.
- Deberá permitir personalizar las páginas de bloqueo
- Deberá prevenir exponer el "OS fingerprinting".
- Deberá soportar:
  a) Restringir protocolo y version utilizada
  b) multi-byte language encoding
  c) Validar URL-encoded characters
  d) Restringir la longitud del método de Request.
  e) Restringir la longitud del URI solicitado
  f) Restringir el número de Encabezados (headers).
  g) Restringir la longitud del nombre de los encabezados
  h) Restringir la longitud del valor de los encabezados
  i) Restringir la longitud del cuerpo (body) de la solicitud
  j) Restringir la longitud del nombre y el valor de las cookies
  k) Restringir el número de cookies
  l) Restringir la longitud del nombre y valor de los parámetros
  m) Restringir el número de parámetros

- Deberá incluir protección a Web Services XML y restringir el acceso a métodos definidos via Web Services Description Language (WSDL) actuando como Firewall XML.
- Poseer firewall de XML integrado, soportando filtrado y validación de funciones XML específicas de la aplicación.
- Poseer políticas de seguridad de aplicaciones pre-configuradas en el equipo.
- Poseer un motor de creación dinámica de políticas de seguridad, con aprendizaje automático de forma de utilización de la aplicación, realizado sobre el flujo de tráfico bidireccional que atraviesa el equipo.
- Deberá poder aprender el comportamiento de la aplicación automáticamente sin intervención humana.
- Deberá permitir la integración con Herramientas de verificación de vulnerabilidades
- Deberá posibilitar la actualización automática de nuevas firmas de ataque
- Deberá presentar protección positiva contra ataques como:
    a) Manipulación de entradas de formulario invalidas
    b) Control de acceso por fuerza bruta
    c) Buffer Overflow
    d) Cross-Site Script;
    e) SQL/SO injection;
    f) Cookie poisoning;
    g) HTTP Request Smuggling;
    h) Manipulación de campos ocultos
    i) Trojan, backdoor y spyware
    j) Detección de evasión
    k) LDAP injection
- Deberá reconocer firmas selectivas y filtros de ataque que deben proteger contra:
    a) Ataques de negación de servicio automáticos
    b) Worms
    c) Vulnerabilidades conocidas
    d) Requests a objetos restringidos
    e) Cloacking
- Deberá esconder cualquier mensaje de error HTTP a los usuarios.
- Deberá remover los mensajes de error de las páginas a mostrar a los usuarios.
- Deberá incluir protección contra el Top 10 de ataques definidos en OWASP
- Deberá proteger contra ataques CSRF
- Deberá proteger el payload AJAX y JSON
- Deberá proteger contra Web Scrapping
- Deberá detectar y detener ataques de denegación de servicio a nivel de Aplicación Web
- Deberá proteger contra fugas de información sensible en las aplicaciones Web, con la opción de bloqueando y/o enmascarar la información.
- Deberá soportar bloqueo basados en geolocalización.
- Deberá incluir seguridad a nivel de aplicación para protocolo SMTP y FTP, con el fin de ayudar a proteger otros servicios críticos de la entidad
- Deberá detectar y detener ataques de denegación de servicio a nivel de Aplicación Web.
- Deberá brindar detección y protección proactiva contra BOTS.
- Deberá brindar protección contra ataques de fuerza bruta con la finalidad de robar credenciales.

- Deberá realizar la encriptación dinámica de credenciales en el browser,
- Deberá realizar la protección de credenciales encriptando dinámicamente el contenido de la página web y previniendo ataques tipo man-in-the-browser ocasionados por malware.
- Cada Balanceador deberá soportar bloqueo basados en geolocalización.
- Deberá estar habilitado y soportar bases de datos de reputación de IP que permita bloquear tráfico desde y hacia direcciones IP en categorías como:
    a) Scanners
    b) Exploits Windows
    c) Denial of Service
    d) Proxies de Phishing
    e) Botnets
    f) Proxies anónimos
- Deberá considerar una plataforma de gestión centralizada desde la cual se administrarán todos los balanceadores y sus instancias virtuales. Esta solución de gestión debe ser de propósito específico en modalidad de Virtual Appliance configurado en alta disponibilidad HA (1+1).
- La plataforma de gestión deberá considerar un repositorio de LOGS externo con 1TB de capacidad.

ITEM2:

6.1.3 SOLUCIÓN DE SEGURIDAD PERIMETRAL DE RED DE SEGUNDO NIVEL.

- La solución debe ser desarrollo específico o appliance configurado en alta disponibilidad local HA (1+1), tolerancia a fallas y balanceo de carga y que se instalara en cada Datacenter de la SUNAT (San Isidro y Surco).
- Debe incluir el Hardware/software y licenciamiento necesario para la configuración en alta disponibilidad HA.
- Dentro de los criterios de HA, se debe precisar que este es extensible a todos los componentes solicitado.
- El hardware y software de la solución deben ser del mismo fabricante.
- El software del firewall debe de residir en el sistema operativo propietario y deben ser del tipo Unix hardened.
- De requerirse debe incluir el cableado y patch cords correspondientes necesarios a ser instalados en cada Datacenter.
- Debe incluir seis (6) puertos 10 Gigabit de cobre, estos puertos no deben ser usados para la HA.
- Debe incluir Cuatro (4) puertos 10Gigabit con interfaces tipo SR, estos puertos no deben ser usados como HA
- Debe incluir un Throughput mínimo de 20 Gbps de Firewall en Capa 4 con mediciones de tráfico Enterprise o real.
- Software de firewall con licencia ilimitada.
- Debe contar con capacidad para integrar esquemas de red NAT/PAT (Network Address Translation/Port Addres Translation).
- Manejo de ataques y amenazas, como mínimo las siguientes:
    - Denegación de Servicios
    - SYN Flood

  - ICMP Flood
  - Ping of Death
  - IP Spoofing
  - Land Attack
  - Tear Drop.
  - IP Source Route.
  - ICMP Fragmentation o Restrict ICMP Fragment.

- Manejo de políticas utilizando objetos basados en FQDN.
- Manejo de políticas basado en URL considerando uso wildcards.
- Capacidad de manejar políticas basadas en usuarios de Active directory o Grupo de Active directory
- Generación de políticas por protocolo, por regla, basadas en horario; tanto para tráfico de entrada como de salida.
- Entorno de administración remota encriptada.
- Incluya protocolo NTP y sus servicios de sincronismo de reloj desde nube del fabricante
- Incluir el hardware y software dedicado e independiente de los firewalls, para la administración y configuración de los equipos, gestión de eventos y reportes, y almacenamiento local de logs de al menos de 500 Gigabytes. Esta plataforma debe estar configurada en alta disponibilidad HA (1+1)
- El equipo debe soportar direccionamiento IPv6.
- Reporte discriminado de los eventos del firewall. El reporte debe considerar eventos en tiempo real, así como los eventos ya almacenados. La solución de reportes debe ser de la misma marca del firewall.
- Capacidad de Registrar como mínimo los siguientes parámetros funcionales:
  - 2,500 Políticas o reglas de firewall.
  - 1,500 Servicios TCP/UDP.
  - 3,500 Objetos de red IP/NET.
- Dimensión estándar de 19". Incluir accesorios necesarios para su montaje.
- Alimentación eléctrica interna de 100-220VAC 50-60Hz.
- El Firewall debe incluir funcionalidades de Sistema Preventivo de Intrusos (IPS) y no tener limitación o restricción en cuanto al uso de sus funcionalidades.
- El esquema de detección debe ser bidireccional. El Sistema Preventivo de Intrusos (IPS) debe poder analizar el tráfico en ambas direcciones.
- Para la funcionalidad del Sistema Preventivo de Intrusos: la cantidad de firmas debe superar los 900 y tener un Throughput mínimo de 7 Gbps con mediciones de tráfico Enterprise o real.
- Generación de políticas globales o especificas del Sistema Preventivo de Intrusos, por protocolo, por contexto, por regla, basadas en horario; tanto para tráfico de entrada como de salida.

- Debe permitir que el Sistema Preventivo de Intrusos al administrador la capacidad de distinguir rápidamente sobre una acción muy crítica, no usual y no permitida. Por ejemplo, un usuario no autorizado utiliza el puerto o servicio no autorizado.
- Entorno de administración remota encriptada para los eventos del Sistema Preventivo de Intrusos.
- Reporte discriminado de los eventos del Sistema Preventivo de Intrusos. El reporte debe considerar eventos en tiempo real, así como eventos ya almacenados, por tipos de eventos o incidentes como intentos fallidos. La solución de reportes debe ser de la misma marca del Sistema Preventivo de Intrusos.
- Poder identificar los ataques como mínimo de fuerza bruta, DoS, DDos alertar como mínimo por correo electrónico y permitir restringir el vector de ataque por una cantidad de tiempo definida.
- Permitir y visualizar los eventos, para identificar falsos positivos en modo aprendizaje del Sistema Preventivo de Intrusos.
- Permitir y configurar en modo bloqueo que debe ser implementado por el contratista reduciendo los falsos positivos de eventos.

6.1.4 SOLUCIÓN DE SEGURIDAD PERIMETRAL PARA EXTRANET

- La solución debe ser de desarrollo especifico o appliance configurado en alta disponibilidad local HA (1+1) tolerancia a fallas y balanceo de carga y se **instalará en cada Datacenter de SUNAT (San Isidro y Surco)**.
- Debe incluir el hardware y software, licenciamiento necesario para la configuración en alta disponibilidad HA.
- Dentro de los criterios de HA, se debe precisar que este es extensible a todos los componentes solicitado.
- El hardware y software de firewall deben ser del mismo fabricante.
- El sistema operativo de la solución debe ser de propósito específico y no uno de uso genérico, es decir un SO desarrollado por el fabricante específicamente para propósitos de firewall.
- De requerirse debe incluir el cableado y patch cords correspondientes necesarios a ser instalados en cada Datacenter.
- Debe incluir seis (6) puertos 10 Gigabit de cobre
- Debe incluir cuatro (4) puertos 10 Gigabit con interfaces tipo SR, estos puertos no deben ser usados como HA
- Debe incluir un Throughput mínimo de 09 Gbps de Firewall en Capa 4 con mediciones de tráfico Enterprise o real.
- El software del firewall debe contar licencia ilimitada.
- Debe tener la capacidad de manejar más de una interfaz externa de conexión hacia internet, permitiendo un balanceo de carga.
- Debe incluir funcionalidad y licenciamiento de web filtering.
- Debe contar con capacidad para integrar esquemas de red NAT/PAT (Network Address Translation /Port Addres Translation)
- Manejo de ataques y amenazas, como mínimo los siguientes eventos:

- Denegación de Servicios
- SYN Flood/SYN ATTACK.
- ICMP Flood.
- Ping of Death.
- IP Spoofing.
- Land Attack.
- Tear Drop.
- IP Source Route.
- ICMP Fragmentación o Restrict ICMP fragment.

- Manejo de políticas utilizando objetos basados en FQDN.
- Manejo de políticas basado en URL considerando uso wildcards.
- Generación de políticas por protocolo, por regla, basadas en horario; tanto para tráfico de entrada como de salida.
- Incluya la capacidad de manejar políticas basadas en la geolocalización y tipo de dispositivo cliente
- Manejo de políticas basadas en usuario, integrándose al directorio activo de la SUNAT
- Entorno de administración remota encriptada.
- Incluya protocolo NTP y sus servicios de sincronismo de reloj desde nube del fabricante.
- Capacidad de registrar como mínimo los siguientes parámetros funcionales:
  - 4,000 políticas o reglas de firewall.
  - 2,500 servicios TCP/UDP.
  - 6,200 objetos de red IP/NET.
- La solución debe incluir el hardware y software necesario para la administración y configuración de los equipos, así como la gestión de eventos y reportes y el almacenamiento local de logs al menos de 500 Gigabytes. Para el tema de los logs este puede estar en el equipo, en un equipo de propósito específico o un servidor para tal fin.
- Reporte discriminado de los eventos del firewall. El reporte debe considerar eventos en tiempo real, así como eventos ya almacenados La solución de reportes debe ser de la misma marca del firewall.
- Cumplimiento de los estándares de la certificación: Common Criteria ICSA (International Computer Security Association), NSS Labs o Check Mark.v o NSS Labs inc
- El equipo debe soportar direccionamiento IPv6.
- Dimensión estándar 19", incluir accesorios para su montaje.
- Alimentación eléctrica interna de 100-220VAC a 50-60Hz.
- El Firewall debe incluir funcionalidades de Sistema Preventivo de Intrusos (IPS) y contar con licencia ilimitada y no tener limitación o restricción en cuanto al uso de sus funcionalidades.

- El esquema de detección debe ser bidireccional. El Sistema Preventivo de Intrusos (IPS) debe poder analizar el tráfico en ambas direcciones.
- Para la funcionalidad del Sistema Preventivo de Intrusos: la cantidad de firmas debe superar los 900 y tener un Throughput mínimo de **3 Gbps** con mediciones de tráfico Enterprise o real.
- Generación de políticas globales o especificas del Sistema Preventivo de Intrusos, por protocolo, por contexto, por regla, basadas en horario; tanto para tráfico de entrada como de salida.
- Debe permitir que el Sistema Preventivo de Intrusos al administrador la capacidad de distinguir rápidamente sobre una acción muy crítica, no usual y no permitida. Por ejemplo, un usuario no autorizado utiliza el puerto o servicio no autorizado.
- Entorno de administración remota encriptada para los eventos del Sistema Preventivo de Intrusos.
- Reporte discriminado de los eventos del Sistema Preventivo de Intrusos. El reporte debe considerar eventos en tiempo real, así como eventos ya almacenados, por tipos de eventos o incidentes como intentos fallidos. La solución de reportes debe ser de la misma marca del Sistema Preventivo de Intrusos.
- Poder identificar los ataques como mínimo de fuerza bruta, DoS, DDos alertar como mínimo por correo electrónico y permitir restringir el vector de ataque por una cantidad de tiempo definida.
- Permitir y visualizar los eventos, para identificar falsos positivos en modo aprendizaje del Sistema Preventivo de Intrusos.
- Permitir y configurar en modo bloqueo que debe ser implementado por el contratista reduciendo los falsos positivos de eventos

6.3 VISITA TÉCNICA

- De ser necesario para la elaboración de la oferta, los participantes en el procedimiento de selección podrán realizar los estudios de campo y visitas pertinentes a los locales de la SUNAT (Datacenters) durante la etapa de formulación de consultas, a fin de que puedan verificar in situ las condiciones de la implementación; para lo cual deberán solicitar las facilidades de acceso e información adicional a la siguiente dirección de correo wmayorga@sunat.gob.pe

6.4 CONDICIONES COMPLEMENTARIAS

6.4.1. ENTRENAMIENTO (Aplica para todos los ítems)

6.4.1.1. El contratista deberá entrenar al personal de la SUNAT que se encargará de la administración de los equipos, y debe realizarse para los profesionales de la DAT (1), OSI (2) y DGIT (4) los temas de: instalación, configuración, administración y operación de la solución.

6.4.1.2. La fecha de inicio y horario de la capacitación será coordinada entre la DGIT y el contratista, durante la etapa de implementación.

6.4.1.3. El tiempo mínimo de capacitación deberá ser:

- Solución de Balanceo: Mínimo 40 horas.
- Solución de Firewall: Mínimo 40 horas.

6.4.1.4. El Plan de Capacitación debe contemplar:

- Plan de Cursos.

- Objetivos de los cursos.
- Contenido de los cursos.
- Duración.
- Lugar.
- Perfil requerido de los participantes.
- Material Didáctico y recursos pedagógicos.
- Hardware, software, Equipos de usuarios, Manuales.

6.4.1.5. La capacitación debe abarcar:

- Entrenamiento en la Instalación del Hardware y Software de los componentes de la solución.
- Entrenamiento en la configuración de los componentes de la solución, incluidas las características de seguridad.
- Entrenamiento en la administración y soporte los componentes de la solución, incluidas las características de seguridad.

6.4.1.6. La Capacitación deberá impartirse durante los **primeros 90 días calendarios**, luego de la firma del contrato.

6.4.1.7. El contenido de los cursos debe ser oficial en idioma español, los equipos, medios didácticos, herramientas, programas y material didáctico debe referirse al mismo tipo y versiones de equipos y software de la solución propuesta.

6.4.1.8. La capacitación se brindará en el horario de oficina de Lunes a viernes entre 09:00 horas y 18:00 horas, previa coordinación con la DGIT.

6.4.1.9. La certificación del curso, como mínimo debe ser a nivel de asistencia.

6.4.1.10. La capacitación debe ser impartida presencialmente por un instructor certificado por el fabricante para poder impartir capacitaciones oficiales. Se precisa que el instructor certificado por el fabricante es aquel que independientemente de la certificación de conocimiento técnico, cuenta con una certificación adicional que dan los fabricantes a los instructores, que avala que cuentan con el conocimiento necesario para ser instructores y conocen la metodología autorizada del fabricante para ser instructores. Se aceptará carta de parte del fabricante señalando que la persona que dictará el curso es un instructor certificado y que cuenta con el conocimiento y metodología autorizada de fabrica para ser instructores.

6.4.1.11. La capacitación deberá realizarse de modo presencial en la ciudad de Lima, impartirse en idioma castellano o en su defecto con traducción simultánea.

6.4.1.12. Los participantes de la capacitación deben de manifestar el nivel mínimo de satisfacción de la capacitación en la encuesta final del curso para otorgar la conformidad.

6.4.2. GARANTÍA COMERCIAL y/o FÁBRICA (Aplica para ambos ítems)

6.4.2.1. El periodo de garantía de buen funcionamiento es de 1826 días calendarios contados a partir del día siguiente de emitida el Acta de conformidad de la prestación principal emitida por parte de la DGIT.

6.4.2.2. El contratista garantiza que todos los bienes suministrados en virtud del Contrato son nuevos, sin uso, del modelo más reciente e incorporan todas las últimas mejoras en cuanto a diseño y materiales. El Contratista garantiza que los bienes están libres de defectos que puedan manifestarse durante su uso normal y en las condiciones imperantes, ya sea que dichos defectos sean el

resultado de alguna acción u omisión por parte del Contratista o provengan del diseño, los materiales o la mano de obra.

6.4.2.3. La SUNAT notificará al contratista cualquier defecto, inmediatamente después de haberlo descubierto, e indicará la naturaleza del defecto, junto con toda la evidencia disponible. La SUNAT le dará al Contratista la oportunidad que se requiera para que inspeccione el defecto. Una vez recibida tal notificación, el Contratista reparará o reemplazará dentro del plazo de Ley la totalidad de los bienes o partes defectuosas, sin costo alguno para la SUNAT.

6.4.2.4. Si el contratista, después de haber sido notificado, no subsana los defectos dentro del plazo de Ley, la SUNAT podrá tomar las medidas necesarias para corregir la situación por cuenta y riesgo del contratista, sin perjuicio de otros derechos que la SUNAT pueda ejercer contra el contratista en virtud del Contrato.

6.4.2.5. Todos los componentes de los equipos ofertados no podrán presentar adulteraciones ni correcciones, por ejemplo: tarjeta madre, fuente, etc.

6.5 PRESTACIONES ACCESORIAS A LA PRESTACION PRINCIPAL

Comprende el soporte técnico, a lo que está obligado a realizar el contratista, en caso se requiera el contratista puede incluir mantenimiento y revisión de las configuraciones lógicas de los equipos. La vigencia de la prestación accesoria comprende un periodo de 1826 días calendarios contados a partir del siguiente día de la emisión del acta de conformidad de prestación principal, con lo cual el contratista debe cumplir con lo indicado en los numerales siguientes:

6.5.1. SOPORTE TÉCNICO (aplica para ambos ítems)

6.5.1.1. Incluye el servicio de reparación y solución de problemas o incidentes por el personal requerido de acuerdo con lo señalado en el numeral 7.2.1-b) y reemplazo de las partes que se encuentren defectuosas por repuestos originales de los equipos instalados en los Datacenters de SUNAT San Isidro y Surco.

6.5.1.2. El Tiempo de Reparación Máximo será de cuatro (4) horas. Para el cumplimiento de lo indicado, se entenderá como Tiempo de Reparación, al tiempo transcurrido entre la comunicación al Contratista de la existencia del mal funcionamiento del/(los) equipo/(s) por parte de la SUNAT (llamada de servicio) o entrega del equipo de ser el caso y la reparación y puesta en funcionamiento del(los) mismo(s) a satisfacción de la SUNAT. En caso de que el contratista no pudiera concretar la reparación, debe solucionar el inconveniente mediante el reemplazo de la referida unidad por una unidad nueva de igual o superior característica, sin que esto implique costo alguno para la SUNAT.

6.5.1.3. El contratista debe contar con un centro de atención de llamadas de reparación o asistencia técnica instalado de tal manera que le asegure a la SUNAT que se encuentra en condiciones de cumplir con lo estipulado. La SUNAT podrá efectuar llamadas de servicio en horario 7x24x365.

6.5.1.4. Incluye la actualización del software provisto, incluyendo el suministro de nuevas versiones (releases) y reparaciones (en general denominadas comercialmente como patches, temporary fixes, etc.).

6.5.1.5. El contratista no podrá alegar inconvenientes con el fabricante para la obtención de los servicios indicados, incluido gestion de RMA debiendo garantizar en toda circunstancia la posibilidad de escalamiento de los eventos.