FUNDACIÓ INSTITUT D'INVESTIGACIÓ EN CIÈNCIES DE LA SALUT GERMANS TRIAS I PUJOL

PLIEGO DE PRESCRIPCIONES TÉCNICAS

CONTRATO RELATIVO AL SUMINISTRO Y MANTENIMIENTO DEL NUEVO FIREWALL Y CONSOLA DE CONTROL DE ENDPOINTS PARA EL INSTITUT D'INVESTIGACIÓ EN CIÈNCIES DE LA SALUT GERMANS TRIAS I PUJOL

CONTRATACIÓN NO ARMONIZADA – PROCEDIMIENTO ABIERTO SIMPLIFICADO

Exp. 12514/2022

1. OBJETO DE CONTRATO

El objeto del contrato es el suministro de dos firewalls físicos redundados y en alta disponibilidad, así como de una consola de gestión centralizada de endpoints para la Fundació Institut d' Investigació en Ciencies de la Salut Germans Trias i Pujol (en lo sucesivo IGTP).

2. CARACTERÍSTICAS TÉCNICAS MÍNIMAS OBLIGATORIAS

El licitador tendrá que presentar una solución de 2 firewalls físicos redundados y en alta disponibilidad, formando un único clúster con las siguientes características mínimas:

Deberá disponer de hardware específico (ASIC) que permita asegurar el esfuerzo requerido, específicamente hecho para descargar el uso de CPU principal del equipo en tráfico de capas 4 i 7.

- Tiene que ser capaz de funcionar en modo de alta disponibilidad (HA) tanto en modo activo-activo, como en modo activo-pasivo sin coste de licenciamiento adicional.
- Se tendrá que poder hacer upgrade de firmware de los equipos en HA sin pérdida de servicio.
- Tiene que tener fuentes de alimentación redundantes intercambiables en caliente.
- Su instalación podrá ser en modo router (capa 3) o en modo transparente (capa 2).
- Tendrá que soportar la segmentación en diferentes equipos virtuales que se comportarán como cortafuegos separados, cada uno con sus interfaces propias. Tendrá que soportar al menos 10 de estos equipos virtuales.
- Tendrá que soportar 3 millones de sesiones concurrentes y 280.000 nuevas sesiones por segundo.
- El tráfico mínimo a soportar y analizar en modo firewall será de 27 Gbps (en paquetes UDP de 1518 bytes).
- Tránsito de protección contra amenazas (Firewall, IPS, control de aplicaciones, protección antimalware i filtrado de IPs) de 3 Gbps.
- Tendrá que proveer servicios de SD-WAN a la misma plataforma sin necesidad de licenciamiento adicional, pudiendo revisar el estado de las líneas que conforman el servicio SD-WAN mediante la medición de parámetros como pérdida de paquetes, retraso y jitter , de forma que se puedan definir diferentes técnicas de distribución de tráfico, basadas en el peso asignado a cada interfaz, el estado del tráfico, bien sea por volumen de paquetes o cantidad de sesiones existentes, ancho de banda de cada enlace o por direcciones IP origen y destino.
- El tráfico agregado de VPNs podrá llegar a 13 Gbps.

- Tendrá que contar con la relación de interfaces siguientes:

    - 2 puertos de administración RJ-45
    - 16 puertos GE RJ-45
    - 8 puertos GE SFP
    - 4 puertos SFP/SFP+ que podrán funcionar a 1/10 Gbps según el módulo instalado.

- El equipo se podrá subscribir a servicios de antimalware con Cloud Sandbox incluido, base de datos de firmas IPS, AntiSpam, protección DoS, control de aplicaciones, filtrado de video y sitios web, incluyendo contenido y filtrado DNS. Cada equipo tendrá que estar suscrito a estos servicios durante 5 años.

- El cortafuegos podrá ser gestionado mediante un entorno gráfico bajo protocolo HTTPS y por línea de comandos usando SSH, siendo opcional el uso de HTTP y Telnet, respectivamente. Esta gestión tiene que ser posible sin utilizar una plataforma externa.

- Posibilidad de tener perfiles de usuario con diferentes privilegios, como por ejemplo super administrador, usuarios de solo lectura, usuarios con escritura restringida a ciertos módulos, etc.

- Soporte de monitorización por SNMP, ya sea v2 o v3.

- Tendrá que tener módulo de enrutamiento, soportando protocolos abiertos como por ejemplo RIP v1/v2, OSPF, IS-IS y BGP.

- Tendrá que soportar IPv4 y IPv6 simultáneamente, y la conversión entre estos tipos de enrutamiento con técnicas de NAT.

- Procesadores Hardware (SPU) preparados para datacenters hyperescalares con aceleración de hardware.

- Soporte de procesamiento hardware con alto rendimiento y muy baja latencia con aceleración de tráfico IPv4, IPv6, CAPWAP, VXLAN, GRE y IPSEC.

- Capacidad de protección antiDoS (Denegación de Servicio) implementada por hardware contra ataques volumétricos.

- Soporte de QoS para hardware incluyendo traffic shaping y queuing.

- La solución ofertada tendrá que incluir coprocesadores hardware para acelerar el tráfico criptográfico, así como la inspección de seguridad por hardware, incluyendo la investigación de firmas de ataques.

- La solución de seguridad tiene que permitir diferentes modos de funcionamiento, pudiéndose combinar entre los diferentes Firewalls virtuales:

  • Modo transparente.
  • Modo routed.
  • Modo sniffer.

La propia plataforma debe tener conectores automáticos con el objetivo de integrarse con identidades terceros y poder recoger información, dirección IP, inventario de objetos y etiquetas. Esta funcionalidad tendrá que estar soportada por los appliances de seguridad (sin necesidad de consola adicional). En concreto se requiere los siguientes:

- Fuentes de identidad: Active Directory i Radius.

- Fuentes de amenazas: Listado de IP,dominios , URLs y hash de malware customizados.

- Cloud pública: Google Cloud, Azure, AWS, Oracle y AliCloud

- Cloud privada: VMware NSX y ESXi.

- Se tiene que poder integrar con plataformas de Cloud privada como Openstack , Kubernetes, Cisco ACI y Nuage

  La misma solución de seguridad debe permitir la creación de automatismos para que:

- Ante la detección de un host comprometido, los cortafuegos envíen: un email, una notificación tipo push a dispositivos móviles, poder banear la dirección IP, invocar funciones AWS Lambda, Google funcions, Azure funcions y Webhook .

- Capacidad de configuración de Proxy explícito por interfaz, con la funcionalidad de Proxy chaining en caso necesario o funcionalidad equivalente.

- Soporte de protocolos RIP v1/v2, OSPF, ISIS, BGP, WCCP y multicast por IPv4 y IPv6, Routing basado en política o PBR y funcionalidades avanzadas SD-WAN.

- Soporte de VRFs (múltiples tablas de Routing) y multiVRF Routing (por BGP y OSPF).

- Soporte Dual Stack IPv4 y IPv6 simultáneamente.

- Network address translation NAT IPv4, NAT64 y NAT66.

- DHCP server / DHCP Relay / DNS Server / DNS Proxy / NTP Server.

- 802.1Q VLANs y Point -to- Point Protocol over Ethernet (PPPoE).

- 802.3ad Capacidad para crear enlaces LACP por agregación de puertos.

- Capacidad de balanceo de servidores a nivel 4 para todos los servicios, así como posibilidad de hacer SSL off- loading del tráfico HTTPS.

- Hace falta que la solución de seguridad tenga capacidades integradas de SD-WAN, en concreto:

  o Balanceo inteligente de conexiones físicas y lógicas, indiferentemente del tipo de conexión WAN (MPLS, 3G/4G, FTTH, VPN, etc..).

  o El número mínimo de conexiones físicas y lógicas que se pueden añadir a la SD-WAN tiene que ser de 256.

  o Verificación de la disponibilidad de Internet para cada línea, por protocolos http , ping , dns y TWANP. El número de Health- checks tiene que ser de como mínimo 100.

  o Verificación de calidad en tiempo real: jitter , packet loss y latencia por línea.

  o Configuración de políticas de SD-WAN inteligente basado en origen (usuarios AD y dirección IP), al destino (dirección IP, aplicaciones y/o servicios de Internet/aplicaciones) y a la línea con mejor calidad de aquel momento basado en valores de jitter , packet loss , latencia, tráfico de subida/bajada o ancho de banda, así como una combinación por pesos.

  o En el caso de necesidad de licenciamiento o suscripciones para activar estas funcionalidades, hará falta que estas estén incluidas a la propuesta durante la duración completa del contrato de 5 años.

- Soporte de VXLAN y VXLAN VTEP por extensión de nivel 2 sobre redes de nivel 3.

- El sistema propuesto tiene que tener una funcionalidad integrada de Traffic Shaping tanto de tráfico saliente como entrante siendo capaz de reservar ancho de banda y marcar el tráfico con DSCP. Este traffic shaping tiene que basarse en aplicaciones y URLs a nivel global de perfil o por IP.

Los equipos tendrán que incluir las siguientes características a nivel de alta disponibilidad:

- La funcionalidad de alta disponibilidad tiene que estar disponible sin ninguna licencia adicional.

- Soporte HA tipo Activo – Pasivo, Activo - Activo y modo mixto. El modo mixto implica poder tener Firewalls virtuales activos y pasivos de forma mezclada, es decir, el máster de ciertos Firewalls virtuales sea la primera unidad de cortafuegos, mientras que la segunda unidad de cortafuegos es máster del resto de firewalls virtuales a la vez.

- La transferencia de servicio de un equipo al otro se tiene que poder hacer sin cortes, ni pérdida de las conexiones TCP , ni parada de servicio.

- Las configuraciones se tienen que traspasar automáticamente entre los dos equipos.

- Capacidad de funcionamiento en modo activo/activo sincronizando sesiones entre los dos nodos pero manteniendo direccionamiento IP diferenciado a las interfaces de cada nodo del clúster.

- En el caso de necesidad de licenciamiento o suscripciones para activar la alta disponibilidad, hará falta que estas estén incluidas a la propuesta durante la duración completa del contrato.

- Los equipos tendrán que incluir las siguientes características a nivel de visibilidad:

    - Los equipos cortafuegos tienen que poder generar topologías gráficas físicas y lógicas, con la integración de otros cortafuegos del fabricante, para poder ser capaz de ver en un extremo a extremo que está pasando en toda la red.

    - Funcionalidad de consolidación de logs con diferentes niveles de agrupación, en concreto: por origen, destino, aplicación, amenaza, webs y políticas para su visualización.

    - Esta visualización tiene que ser tipo “Drill-down”, es decir, poder seleccionar unos de los objetos agrupados e ir filtrando el resultado en base a esta selección, hasta saber el detalle completo.

    - Estos requerimientos tendrán que poder lograrse desde la misma GUI de los appliances, en tiempo real, y sin necesidad de una consola central de gestión.

2.1. CARACTERÍSITICAS TÉCNICAS ESPECÍFICAS DE SEGURIDAD

Los equipos tendrán que incluir las siguientes características, y también las indicadas en los subapartados (**CONTROL DE APLICACIONES, IPS, ANTIMALWARE, WEBFILTER, DNS FILTER y FUNCIONALIDADES DE NIVEL 7**) , a nivel de seguridad:

- Capacidad de definir políticas de seguridad IPv4/v6 utilizando los parámetros de coincidencia siguientes:

- Como origen (todas las opciones):

    - Capacidad de definir una y/o más de una interfaz de origen, incluyendo “any”. Así como también “zonas”.

    - Capacidad de utilizar direcciones ip , rangos y/o redes, FQDN, países, servicios de internet y direcciones ip reconocidas como origen de redes TOR, proxies anónimos (estas direcciones tienen que actualizarse automáticamente), así como los objetos exportados de los conectores mencionados en el apartado de características generales del equipo.

    - Capacidad para utilizar usuarios/grupos locales o remotos mediante conectores AD, NAC u otros repositorios de identidad.

    - Capacidad para declarar horarios o schedules tanto por día/hora como fecha máxima de vencimiento.

    - Capacidad de selección del servicio que hay que utilizar.

- Como destino:

    - Capacidad de definir una y/o más de una interfaz de destino, incluyendo “any”. Así como también “zonas”.

    - Capacidad de utilizar direcciones ip , rangos y/o redes, así como objetos FQDN, países y servicios de internet.

- Capacidad de definir políticas de seguridad IPv4/v6 utilizando la siguiente parametrización:

    - Se tiene que poder seleccionar qué tráfico se analizará a nivel 4 y qué tráfico se analizará a nivel 7, por política, sin excepción.

    - La configuración del NAT saliente se tiene que poder configurar dentro de cada una de las políticas de seguridad, de manera granular.

    - Las diferentes funcionalidades de seguridad avanzadas de nivel 7 se activarán de forma individual a nivel de política, nunca a nivel global. Además, estas se gestionarán con perfiles para ser granulares a los permisos. Estas funcionalidades son: antivirus, webfilter , DNS filter , Web Application Firewall, Control de aplicaciones, IPS, y DLP.

- Decidir a nivel de política qué tráfico SSL será descifrado para su análisis y cual solo a nivel de certificado.

- A nivel de logging , hace falta que la solución permita activar el logging de solo nivel 7, o tanto de nivel 4 más nivel 7. Hace falta también que se pueda hacer captura de paquetes a la propia política.

- Capacidad de creación de reglas de DoS a nivel 3 y 4, pudiendo aplicar umbrales por servicios publicados donde poder filtrar por direcciones ip o países
  por: ip_src_session , ip_dst_session , tcp_syn_flood , tcp_puerto_scan , tcp _src_session , tcp_dst_session , udp_flood , udp_scan , udp_src_session , udp_dst_session , icmp_flood , icmp_sweep , icmp_src_session , icmp_dst_ session , sctp_flood , sctp_scan , sctp_src_session y sctp_dst_session .

- Capacidad de definir políticas a nivel de Interfaz para denegar tráfico y no ser procesado por la política de seguridad global. Se tienen que poder utilizar direcciones IP , países, así como rangos y redes ip como origen.

- Para evitar el acceso de redes botnet , los cortafuegos tienen que tener una base de datos de reputación dinámica que bloquee los accesos a nivel de Interfaz.

- Visualización del número de usos y cantidad de tráfico de cada regla de seguridad, de forma ágil tanto a la propia sección de políticas de seguridad, como también dentro de la configuración de cada política. También se deberá ver la última vez que se ha utilizado.

2.1.1. CONTROL DE APLICACIONES

- Capacidad para identificar un mínimo de 2000 aplicaciones activas actuales (incluyendo aplicaciones web 2.0), como por ejemplo distinguir Facebook , de una subaplicación Facebook -chat o post.

- La solución debe clasificar las aplicaciones en diferentes categorías y subcategorías, para poder aplicar reglas de acuerdo con estas categorías/subcategorías (control granular dentro de la aplicación).

- Aplicar técnicas de identificación de aplicaciones a todos los puertos TCP/UDP y no solo a los más comunes.

- Capacidad para identificar las aplicaciones bajo túneles HTTPS.

- Capacidad para identificar aplicaciones Industriales como Modbus .

- Capacidad de creación de firmas de aplicaciones para un reconocimiento personalizado. Es obligatorio que estas aplicaciones customizadas, también sean analizadas por motores de protección (IPS y antimalware).

2.1.2. IPS

- Capacidad para proteger tanto servidores como clientes con un mínimo de 10000 firmas de IPS, agrupados por categoría, severidad, objetivo y protocolo. Ante la identificación de un ataque por IPS, hace falta que el cortafuegos capture el tráfico en un archivo pcap para evidenciarlo y hacer un estudio posterior.

- Capacidad para identificar patrones de ataques basados en comportamiento o rated -base, para bloquear intentos de ataques una vez superado un umbral de uso en un tiempo determinado.

- Capacidad de creación de firmas de IPS para un reconocimiento personalizado.

2.1.3. ANTIMALWARE

- Capacidad de detección de código malicioso (virus, grayware , worms , etc …) basado en firmas conocidas o métodos avanzados de detección.

- Soporte de sandboxing al cloud , con una medida mínima de fichero de 100 MB indistintamente del tipo de fichero.

- Capacidad de eliminación del contenido dinámico (macros, javascript , URL) explotable dentro de documentos ofimáticos y pdf , que se distribuyen por protocolos SMTP, IMAP y HTTP .

- Capacidad de comprobación de si se trata de un fichero bueno o malicioso, en función del hashing y comparado con la BBDD del fabricante. Capacidad de bloquear mediante comparación con código malicioso de repositorios externos con threat inteligencia.

2.1.4. WEBFILTER

- Capacidad de categorizar más de 250 millones de páginas web en más de 60 categorías web para aplicar: block , monitor y aplicación de cuotas de tiempos o tráfico por categoría.

- Soporte de protocolos http v1.0, 1.1 y 1.2.

- La base de datos de categorías web habrá de consumirse como un servicio cloud en tiempo real y no se podrá basar únicamente en listados locales para tener la categorización de las url's lo más actualizado posible.

- Soporte para restringir el acceso a YouTube y Google en modo “safe search ”.

- Soporte de rating por imágenes por URL.

- Soporte para la creación de listas blancas/negras externas sin necesidad de licencia.

2.1.5. DNS FILTER

- Capacidad de categorizar dominios DNS en más de 60 categorías para poder realizar intercepción del tráfico DNS con las siguientes acciones: block , monitor y redirect (redirigir las consultas hacia un portal web cloud o personalizado de bloqueo).

- La base de datos de categorías DNS deberá de consumirse como un servicio cloud en tiempo real y no se podrá basar únicamente en listados locales para tener la categorización de las url's lo más actualizada posible.

- Soporte para la creación de listas blancas/negras externas sin necesidad de licencia.

2.1.6. OTRAS FUNCIONALIDADES DE NIVEL 7

Otras funcionalidades de nivel 7 que la propuesta tiene que incluir y tienen que estar licenciadas son:

- DLP (Data Leak Prevention)

- Web Application Firewall

  Se valorará que la propuesta tenga la funcionalidad ICAP (Internet Content Adaptation Protocol).

2.1.7. OTROS REQUERIMIENTOS

- **El fabricante del cortafuegos tendrá que estar en la categoría de Leaders, del cuadrante mágico de gartner para los Firewalls de red del año 2021.**

3. FUNCIONALIDADES VPN

- El dispositivo tiene que admitir un mínimo de usuarios simultáneos VPN SSL, ya sea con agente o sin, pero en cualquier caso sin licencia adicional.

- El sistema propuesto tendrá que cumplir los estándares de la industria, sin el soporte externo adicional de hardware o módulos: IPSEC VPN (IPv4 y IPv6), PPTP VPN, L2TP VPN, SSL VPN y GRE sobre IPSEC.

- El sistema propuesto tendrá que soportar 2 modos de funcionamiento SSL VPN:

    - Sin cliente - Acceso web: para clientes remotos que solo necesitan un navegador y no requiere la instalación de ningún agente, para acceder vía web a: HTTP / HTTPS Servidor intermediario, FTP, Telnet, SMB / CIFS, SSH , VNC y RDP.

    - Los sistemas operativos y navegadores compatibles en este modo tendrán que ser como mínimo los que se describen en la siguiente tabla:

Sistema Operativo	**Navegadores**
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox versión 85 Google Chrome versión 88
Microsoft Windows 10 (64 bits)	Microsoft Edge Mozilla Firefox versión 85 Google Chrome versión 88
Microsoft Windows 11 (64 bits)	Microsoft Edge Mozilla Firefox versión 85 Google Chrome versión 88
macOS Big Sur 11.0	Apple Safari versión 14 Mozilla Firefox versión 85 Google Chrome versión 88
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

4. SOLUCIÓN DE CONSOLA CENTRALIZADA DE CONTROL DE ENDPOINTS

Adicionalmente, la solución tendrá que contar con una herramienta que permita aplicar políticas de control de endpoints así como Zero Trust en la red, para así poder autenticar no solo los usuarios que se conectan, sino los dispositivos desde el cual lo hacen. Esta herramienta, que podrá ser instalada en modo appliance o máquina virtual in situ, tendrá que contar con las características siguientes:

- La solución ofertada tendrá que ser del mismo fabricante del Firewall e integrarse nativament.
- El sistema tiene que ser compatible con Windows , MacOS, Linux y Chromebook. También soportará endpoints móviles tipos iPhone y Android.
- El licenciamiento tiene que incluir la consola central incluida, así como la cantidad de endpoints requeridos, en este caso se requieren 100 endpoints.
- Opcionalmente, debe soportar licencias para proteger los endpoints con software de endpoint protection (EPP) y disponer de un sandbox para ficheros sospechosos, sin necesidad de instalar hardware o software adicional, solo con la adición de licencias.
- Soporte de Multitenancy.
- Posibilidad de tener un inventario de las aplicaciones instaladas en los endpoints desde el servidor, el inventario se puede hacer a la inversa, seleccionando una aplicación, y se tienen que mostrar los endpoints que la tienen instalada.
- Detección de nuevo software instalado.
- Desde el entorno gráfico del servidor, podéis ver el estado de las aplicaciones enviadas al sandbox
- Tiene que tener capacidad para enviar alertas por SMTP
- Dispondrá de dashboards gráficos con la información siguiente:
    - Actividad de los endpoints
    - Alertas del sistema
    - Estado de las conexiones, mostrando diferencias entre los que están desconectados desde hace poco con aquellos que llevan mucho tiempo sin conectarse.

- Tipos y versión de sistema operativo de los endpoints.

- El sistema tiene que ser capaz (con las licencias adecuadas) de recibir actualizaciones de nuevas vulnerabilidades detectadas, y avisar qué endpoints pueden estar expuestos a ser atacados. También tiene que ser capaz de aplicar el parche a un endpoint si este está disponible por el fabricante, para solucionar alguna vulnerabilidad.

- El sistema tiene que mostrar qué usuario está conectado a un endpoint en un momento dado

- Permite aplicar hashtags a endpoints dependiendo de su configuración o usuario conectado, para después permitir o denegar el acceso a la red según estos hashtags, mediante reglas

- Posibilidad de tener una configuración de alta disponibilidad del sistema

- Para verificar la identidad de los usuarios, el sistema tiene que contar con una base de datos local de usuarios, y tiene que ser capaz de integrarse con Active Directory y con proveedores de identidad (IdP) SAML.

- El sistema tiene que poder facilitar el despliegue y la instalación de los agentes desde el servidor
- El servidor debe ser en formato VM, siendo su despliegue en las instalaciones de la Fundación.

- La solución estará licenciada para la totalidad de los endpoints durante 5 años.

5. REQUERIMIENTOS DE LICENCIAMIENTO

No se aceptarán sistemas que requieran de costes extra de licenciamiento de las soluciones requeridas. Concretamente se requiere:

- Que los dos equipos de firewall con las características anteriormente mencionadas y con sus funcionalidades (de antimalware con Cloud Sandbox incluido, base de datos de firmas IPS, AntiSpam, protección DoS, control de aplicaciones, filtrado de video y sitios web, incluyendo contenido y filtrado DNS) tengan las licencias incluidas durante un periodo de 5 años.

- Que la solución de consola centralizada de control de endpoints esté licenciada por la totalidad de los 100 endpoints durante el periodo de 5 años.

6. SUMINISTRO, INSTALACIÓN Y CONFIGURACIÓN DE LOS EQUIPOS

Los equipos se instalarán IN SITU en las dependencias de IGTP. Se requiere que el suministro se haga en un periodo máximo de 5 semanas

Esta instalación estará realizada por el equipo IT del IGTP.

Se pide una bolsa de horas de mínimo 25 horas de soporte, incidencias o cambios de configuración de los equipos y las soluciones requeridas.

7. GARANTIA Y SOPORTE TÉCNICO

El soporte técnico de la garantía lo tiene que ofrecer directamente el fabricante.

El soporte será 24x7 vía web o telefónica, con tiempo de respuesta para incidencias críticas de 1 hora y de siguiente día laborable para incidencias no críticas.

Las actualizaciones de software y firmware estarán incluidas.

El periodo de garantía, certificada por el fabricante, tendrá que ser obligatoriamente mínimo de 5 años, incluyendo el hardware y software incluido en la licitación.

8. PLAZO DE ENTREGA

El adjudicatario tiene que presentar una declaración responsable certificando que entregará los equipos a IGTP en un periodo máximo de 5 semanas a partir de la fecha de formalización del contrato y a partir de este periodo empezará la configuración, puesta en marcha.