Zaragoza
AYUNTAMIENTO

SERVICIO DE REDES Y SISTEMAS

PLIEGO DE CONDICIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SUMINISTRO DE CORTAFUEGOS CORPORATIVOS DE NIVEL 7 PARA LA RED MUNICIPAL DE COMUNICACIONES DEL AYUNTAMIENTO DE ZARAGOZA.

1 INTRODUCCIÓN. OBJETO Y ALCANCE.

En los últimos años el Ayuntamiento de Zaragoza ha hecho un importante esfuerzo inversor en el ámbito de las tecnologías de la información, avanzando mucho en temas como la administración electrónica tendiendo a cero-papel, los servicios electrónicos al ciudadano, la interconexión entre los centros de trabajo municipales y la interconexión con otras administraciones y redes de terceros. En todo este proceso, la importancia y la criticidad de la conexión a Internet ha sido crucial, posibilitando generalizar el servicio de navegación a todos los trabajadores, el crecimiento exponencial del uso del correo electrónico y las herramientas on-line, el desarrollo de todos los procesos nuevos (y la migración de los existentes) en la web.

Simultáneamente, se han implantado servicios de alto nivel de seguridad a través de internet como el teletrabajo, la telegestión o el acceso remoto, así como la integración en la red de dispositivos móviles e inalámbricos (smartphones).

Para que estos sistemas cumplan su finalidad es necesario garantizar la seguridad en las conexiones a Internet y de los servidores web municipales, para lo que es imprescindible disponer de equipamiento de última generación, frente al que actualmente se está empleando, de forma que permita realizar tareas de protección de la conexión a internet de los equipos informáticos municipales y de todas las aplicaciones web que se ofrecen 24x7 al ciudadano.

Objeto y alcance del contrato.

El presente pliego establece las condiciones y requisitos técnicos mínimos que regirán la contratación del suministro que el Ayuntamiento de Zaragoza precisa en relación a los cortafuegos corporativos de seguridad para la red municipal y los servidores web municipales, con el fin de obtener la máxima fiabilidad, seguridad y eficacia en su funcionamiento de cara al servicio que se presta al ciudadano.

El objeto y alcance del contrato comprende el suministro de varios equipos cortafuegos de seguridad (todos ellos del mismo fabricante), concretamente:

- **dos appliance físicos de cortafuegos de nivel 7 (en cluster de alta diponibilidad),**
- **dos appliances físicos de cortafuegos de servidores web (en cluster de alta disponibilidad)**
- **un appliance virtual para vmware de almacenamiento de los registros de comunicaciones generados por los cortafuegos del contrato.**

Las especificaciones técnicas de los elementos incluidos en este contrato se encuentran a continuación.

La oferta presentada por la empresa licitadora recogerá, como mínimo, todas las condiciones de este Pliego y en caso de duda o disconformidad prevalecerá lo dispuesto en el presente documento.

Zaragoza
AYUNTAMIENTO

2 DEFINICIÓN DE LA SITUACIÓN ACTUAL.

Infraestructura existente, inventario de las instalaciones actuales.
Se adjunta un listado del equipamiento de cada tipo.

El Ayuntamiento de Zaragoza dispone del siguiente equipamiento de seguridad ubicado en 2 centros de proceso de datos (primario y secundario ó de backup):

CPD PRINCIPAL:

1 Nodo principal cortafuegos perimetral Red Municipal: Juniper SSG-550
1 Nodo principal cortafuegos perimetral Red de invitados: Sophos ASG220
1 Nodo principal cortafuegos de core Red Municipal: Cisco FWSM sobre Catalyst 6500

CPD SECUNDARIO (Backup):

1 Nodo secundario cortafuegos perimetral Red Municipal: Juniper SSG-550
1 Nodo secundario cortafuegos perimetral Red de invitados: Sophos ASG220

La definición general de la arquitectura, así como la topología de conexiones no se aportan como información pública al considerarse información sensible de seguridad, y no considerarse necesarias para la valoración de la solución a aportar.

Zaragoza
AYUNTAMIENTO

3 REQUISITOS TÉCNICOS DEL SUMINISTRO

Se solicita el suministro de 2 unidades gemelas de cortafuegos de nivel 7 (aplicación), en formato físico (hardware appliance), configuradas en formato de cluster de alta disponibilidad (HA) para asumir el tráfico de, al menos, los equipos del inventario listado previamente y que van a sustituir en la red de comunicaciones municipal.

Se solicita también el suministro de 2 unidades gemelas de cortafuegos de aplicación web, en formato físico (hardware appliance), configuradas en formato de cluster de alta disponibilidad (HA), para proteger los servidores web del Ayuntamiento de Zaragoza de ataques electrónicos avanzados.

Para cumplir las obligaciones en materia de conservación de datos previstas en la Ley 25/2007 de 18 de octubre (Conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicación) de esta infraestructura se solicita un appliance (en modo virtual con VMWare) que permita la recopilación, almacenamiento y explotación de todos los registros de comunicaciones generados por los cortafuegos del contrato.

Se asume que los cortafuegos de nivel 7 que deben ser tecnológicamente de última generación, con todas las funcionalidades propias de nivel 7, por lo que sólo se listarán como obligatorias aquellas funcionalidades más relevantes que puedan ser medidas comparativamente entre máquinas de distintas marcas. Para poder operar en IPv6, todos los equipos debe ser IPv6 Ready a todos los efectos en todas las funcionalidades requeridas.

Los requisitos técnicos de los cortafuegos se estructuran en funcionalidades obligatorias y funcionalidades opcionales valorables (mejoras valorables).

Zaragoza
AYUNTAMIENTO

Funcionalidades activas mínimas y obligatorias por cortafuegos de nivel 7 (POR CADA UNA DE LAS UNIDADES DE CORTAFUEGOS, AMBAS SERÁN IDÉNTICAS)

- Un mínimo de 22 interfaces (puertos) RJ45 Gigabit Ethernet integrados en la máquina (completos para ser usados, transceptor incluido si fuese necesario)
- Un mínimo de 2 interfaces (puertos) 10Gbps integrados en la máquina (completos para ser usados, transceptor incluido si fuese necesario)
- Doble fuente de alimentación redundante intercambiable en caliente (hot-swap) integrada en el equipo (NO externa)
- Disco interno (local) tipo flash ó SSD de, mínimo, 120 Gb.
- Un mínimo de 7 millones de sesiones concurrentes
- Un mínimo de 190.000 nuevas sesiones por segundo.
- Un mínimo de 10 cortafuegos virtuales
- Modo de operación de filtrado de tráfico en modo transparente, disponible simultáneamente al funcionamiento en modo enrutado (no puede ser exclusiva la operación global sólo en un modo o en otro).
- Modo de operación en cluster de alta disponibilidad (HA), tanto en modo Activo/Pasivo como en modo Activo/Activo sin requerir balanceado externo.
- Rendimiento mínimo de 20 Gbps con paquetes de tamaño pequeño, de 64 bytes.
- Número mínimo de usuarios SSL VPN : 10000
- Rendimiento mínimo IPSec VPN : 8Gbps.
- Licencias ilimitadas para todas las funcionalidades requeridas.
- Funcionalidad de inspección profunda de protocolo ESMTP cifrado para análisis de virus y spam.
- Comportamiento que permita enrutar paquetes de vuelta en función del interfaz origen del trafico.
- Funciones de filtrado de URL por categorías y filtrado de contenidos por el tipo de contenido, categorizando las URL de forma automática (permitiendo excepciones manuales a medida).
- Funciones de análisis profundo del tráfico para la prevención de intrusiones (IPS).
- Funciones de análisis profundo del tráfico para amenazas de seguridad (Antivirus, AntiSpyware, ...).
- Funciones avanzadas de enrutamiento (estático, dinámico, enrutamiento basado en políticas, ...)
- Funciones completas de NAT (estático, dinámico, de origen, de destino, de puerto)
- Funcionalidad básica de QoS (marcado de paquetes para aplicación de políticas de Qos).
- Funcionalidad de aplicar programaciones de tiempo (schedules) a los servicios de seguridad configurados (políticas, QoS, etc)
- Posibilidad de configurar la gestión fuera de banda, en un entorno separado de los firewalls de producción (enrutamiento incluido).
- Posibilidad de configurar envío de logs a un sistema externo, al menos mediante syslog.
- Servicios de análisis de log con funciones básicas de reporting.
- Soporte SNMP, aportando documentación de la MIB específica del fabricante.
- Las soluciones SSL VPN deben poder implementarse usando certificados de la FNMT (al menos Clase2CA y EmpleadoPúblico) y el DNI electrónico.

Zaragoza
AYUNTAMIENTO

Funcionalidades activas mínimas y obligatorias por cortafuegos de aplicación web (POR CADA UNA DE LAS UNIDADES DE CORTAFUEGOS, AMBAS SERÁN IDÉNTICAS):

- Dos puertos gigabit Ethernet RJ45 con transceiver incluidos.
- Cuatro puertos gigabit Ethernet RJ45 bypass
- Dos puertos gigabit Ethernet SFP fibra
- Fuentes de alimentación redundantes (hot swap internas al equipo, no externas).
- 4TB de almacenamiento.
- Capacidad de análisis de 750 Mbps de tráfico http/https.
- Capacidades de autoaprendizaje de comportamientos en los accesos, lo que le permite detectar ataques de "día cero", y con capacidades 'anti- defacement', con las que detectar cambios no autorizados de contenidos y restaurarlos.
- Distintos modos de funcionamiento :
  1. proxy inverso
  2. proxy transparente
  3. en línea transparente
  4. monitorización pasiva fuera de linea

- Servicio de bloqueo por país incluido ('Geoip').
- Antivirus.
- Escaneo de vulnerabilidades Web (Web Vulnerabity Scanner)
- Client Certificate Support
- Compresión
- SSL Offloading
- Balanceo de hasta 2 servidores
- Enrutamiento basado en URL (http content routing)

Protección contra ataques especializado de aplicaciones web, como mínimo los listados a continuación:

- Cross Site Scripting.
- SQL Injection.
- Session Hijacking.
- Cookie tampering/poisoning.
- Cross Site Request Forgery.
- Command injection.
- Remote file inclusión.
- Forms tampering.
- Hidden field manipulation.
- Outbound data leakage.
- HTTP Request Smuggling.
- Remote file inclusion.
- Encoding attacks.
- Broken Access Control.
- Forceful browsing.
- Directory traversal.
- Site reconnaissance.
- Search engine hacking.
- Brute force login.
- Access rate control.
- Schema poisoning.
- XML intrusion prevention.
- Recursive payload.
- External entity attack.
- Buffer overflows.
- Denial of Service.

Zaragoza
AYUNTAMIENTO

Funcionalidades activas mínimas y obligatorias para el appliance de logs:

- Integración nativa con la solución propuesta, de forma que su impacto en el rendimiento de los cortafuegos sea mínimo o despreciable.
- Sin limitación de ratio máximo de logs en modo standalone
- Capacidad mínima de 6Gb de logs por día
- Capacidad mínima de 18 millones de sesiones por día
- Capacidad total mínima de 1TB.

Funcionalidades activas mínimas y obligatorias globales de la solución:

- **Soporte 24x7 NBD directamente con el fabricante de los equipos**
- Garantía de funcionamiento y actualizaciones de seguridad de todos los servicios de protección activos disponibles en las máquinas (AV/AS, IPS, URL Filtering, etc)**durante**, al menos, **3 años.**

Funcionalidades opcionales integradas en los propios equipos, entendidas como mejoras valorables por su interés municipal para los cortafuegos de nivel 7 *(sólo se tendrán en cuenta funcionalidades integradas en los equipos, **ACTIVAS** y disponibles en la solución presentada, y **NO** aquellas que necesiten que el Ayuntamiento adquiera adicionalmente algo más aparte de lo propuesto en este contrato)*

1. Funcionamiento en modo proxy explícito para al menos http/https (simultáneamente con el resto de funcionamientos, no exclusivo).
2. Función de QoS aplicable por política, permitiendo aplicar limites de BW (entrada y salida) por usuario o por IP origen dentro de la propia política (el QoS se aplicaría A CADA IP O A CADA USUARIO por separado de los definidos como orígen -source- de la política). Ejemplo: aplicar un BW (in & out) a cada ip o a cada usuario de un segmento de red con una única política.
3. Capacidad de filtrado de nivel 7, identificando la aplicación y permitiendo su uso como parámetro de matching de las políticas del Firewall, no como perfil de seguridad una vez realizado el match de la política usando sólo parámetros tradicionales de nivel L3/L4.
4. Disponibilidad de Portal Cautivo para navegación http/https, permitiendo configurar servidores de autenticación externa para el portal cautivo mediante LDAP.
5. Función habilitada de usar segundo factor de autenticación para proteger la conexión de gestión a las máquinas de, al menos, 5 administradores, bien mediante SMS a móvil o bien mediante tokens específicos de autenticación.
6. Funcionalidad integrada para operar el equipo también como controladora para la gestión de Aps Wifi del fabricante.
7. Funcionalidad de balanceo de tráfico de entrada a servidores, con, al menos, posibilidad de balanceo por ip origen y por sesión.
8. Funcionalidad de balanceo de tráfico de lineas de salida a internet, con, al menos, posibilidad de balanceo por ip origen, por ip destino o por sesión.

4 Ejecución del contrato de suministro.

La empresa adjudicataria pondrá los medios para realizar el suministro de forma coordinada con el Servicio de Redes y Sistemas.

La empresa adjudicataria enviará al Servicio de Redes y Sistemas la documentación correspondiente a todos los mecanismos que permitan al Ayuntamiento el acceso directo al soporte oficial del fabricante del equipamiento (que está solicitado dentro del contrato y deberá estar directamente a nombre del Ayuntamiento, sin necesidad de intermediarios):

- información de soporte online (vía internet)
- información de soporte telefónico
- procedimientos de apertura y gestión de incidencias así cómo acceso a la información del estado el en que se encuentran.

Zaragoza, 8 de Julio de 2014

Jorge Calvera de la Fuente
Técnico Superior en Informática

Alberto Virto Medina
Jefe de Servicio de Redes y Sistemas