AYUNTAMIENTO DE CUENCA

Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa

UNIÓN EUROPEA

Pliego de prescripciones técnicas para:

RENOVACIÓN DE LAS PLATAFORMAS DE CORTAFUEGOS DEL AYUNTAMIENTO DE CUENCA

1.- OBJETO Y ALCANCE

1.1.- Objeto del contrato

Para los intercambios electrónicos de información, tanto interna como con el exterior, el Ayuntamiento de Cuenca, gestiona una red de comunicaciones y seguridad de varios edificios. El Ayuntamiento de Cuenca dispone de equipos de seguridad perimetral con diversos servicios y licencias de seguridad habilitados, entre los que están los servicios de cortafuegos, navegación segura por Internet y servicios diversos de monitorización.

Entre estos sistemas implantados se encuentran los sistemas que se encargan de prestar el servicio de Firewalls de Red, se trata de dos equipos de seguridad y altas prestaciones NSA 4600 del fabricante SONICWALL, estos equipo disponen de licencias de inteligencia de seguridad y de soporte hasta el 31 de diciembre de 2022.

Estos equipos deben ser sustituidos por equipos de nueva generación del mismo fabricante, para permitir la continuidad operativa de la gestión actual sobre una misma base tecnológica y actualizar las funcionalidades y características necesarias convenientemente, o por otros equipos de similares características los cuales han de estar **entre los productos del Catálogo de Productos y Servicios de Seguridad de las TIC CCN-STIC 105 Protección de las comunicaciones Apartado 7.4.3. FAMILIA: CORTAFUEGOS**.

1.2.- Alcance del contrato

Proyecto llave en mano, que comprende el suministro, las licencias y los servicios indicados a continuación.

1.2.1- Suministro

Suministro de dos cortafuegos que han de cumplir como mínimo los siguientes requisitos

- Cortafuegos en “Statefull Packet Inspection” (Firewall tradicional basado en puerto – protocolo.
- Cortafuegos con control del sobre las aplicaciones.
- Cortafuegos con inspección del tráfico SSL
- Cortafuegos de nivel 7 en una cadena de análisis compuesta por URL Filtering, Antivirus, IPS, AntiSpyware, FileBlocking y DLP con el 100 % de las firmas disponibles aplicadas sobre cada uno de los filtros
- Conexiones por segundo mínimas (SPI / DPI / DPI SSL): 4.000.000 / 2.000.000 / 350.000
- Balanceo de carga de forma individualizada y personalizada a nivel 4 y 7.
- Disponibilidad de sistema de alimentación eléctrico redundante
- Interfaces:
    - 24x1GbE en cobre
    - 6x10G/5G/2.5G/1G SFP+,
    - 2 x USB 3.0
    - 1 x Puerto consola
    - 1 x Puerto gestión

1.2.2.- Funcionalidades

Características funcionales de los servicios que deberán integrar los sistemas anteriormente requeridos:

- ✓ Instalación en alta disponibilidad Modo de configuración entre dispositivos: activo-pasivo. Posibilidad de compartir licencias en entornos de HA.

- ✓ Cortafuegos de nivel 4. Los equipos ofrecerán todas las funcionalidades básicas de un cortafuego s típico: filtraje de tráfico por ip y puerto con control de sesión, nato, pat, log del tráfico, etc...

- ✓ Cortafuego de nivel 7: Los equipos tendrán que poder filtrar el tráfico a nivel de aplicación pudiendo distinguir las aplicaciones independientemente del puerto que usen. El fabricante tendrá que ir actualizando y ampliando regularmente el listado de aplicaciones reconocidas.

- ✓ Gestión de usuarios: Los equipos tendrán que poder reconocer el usuario que está generando un determinado tráfico. Por eso los equipos tendrán que comunicarse con el Directorio Activo (MICROSOFT) de la red interna del Ayuntamiento. Los equipos tendrán que guardar el detalle del usuario ena los logs del tráfico.

- ✓ IPS: Los equipos tendrán que incorporar un motor IPS (Intrusion Prevention System) para poder detectar y parar el mayor número posible de ataques. El fabricante tendrá que ir actualizando y ampliando regularmente el listado de ataques reconocidos.

- ✓ Antivirus: Los equipos tendrán que incorporar un motor antivirus para poder detectar y parar el mayor número posible de virus. El fabricante tendrá que ir actualizando y ampliando regularmente el listado de virus reconocidos. Capacidad para detectar virus en más de 10 protocolos TCP diferentes.

- ✓ Servicios de Seguridad propietarios (no de terceros).

- ✓ Visualización de tráfico (aplicaciones, usuarios, etc.) en tiempo real.

- ✓ El cortafuegos tendrá que tener una solución de Gateway antivirus integrada con capacidad de inspeccionar protocolos HTTP/HTTPS – SMTP- FTP – POP3 – IMAP –CIFS/NETBIOS TCP Stream, sin limitación de tamaño de los ficheros.

- ✓ URL filtering: Los equipos tendrán que categorizar las url's y por categorías para gestionar las que los usuarios puedan navegar. El fabricante tendrá que ir actualizando y ampliando regularmente el listado de url's y categorías categorizadas.

- ✓ Motor AV sin límites en el tamaño de ficheros a analizar.

- ✓ Motor DPI que realiza el análisis de los paquetes "al vuelo" (sin necesidad de reensamblaje).

- ✓ Inspección de tráfico cifrado con SSL (DPI-SSL) en puertos diferentes al 443/TCP.

- ✓ Posibilidad de configurar Inclusiones/Exclusiones basadas en categorías de Content Filtering (CFS) para el servicio DPI-SSL.

- ✓ Posibilidad de configurar Inclusiones/Exclusiones basadas en el campo Common Name (CN) del certificado para el servicio DPI-SSL.

- ✓ Posibilidad de configurar simultáneamente múltiples modos/topologías (p.ej.: NAT, L2 Bridge Mode, Transparent Mode, etc.)

- ✓ Desencriptación SSL: Los equipos tendrán que poder des encriptar e inspeccionar el tráfico cifrado. La solución tiene que permitir definir qué categorías de url's o url's concretas se desencripten y qué no.

- ✓ Aplicación de políticas de calidad de servicio (QoS). Los equipos tendrán que poder gestionar el ancho de banda y la prioridad dedicados a cada política de seguridad.
- ✓ Reputación de ip's y/o url's: Los equipos tendrán que poder reconocer ip's públicas y/o url's que sean reconocidas como origen de malware, y por lo tanto parar las conexiones a/desde estas ip's.

- ✓ Sandboxing: Los equipos tendrán que poder enviarlos ficheros que consideren sospechosos al SIEM del Ayuntamiento de Cuenca.

- ✓ Solución de Sandboxing en la nube con múltiples motores.

- ✓ Al usar el servicio de Sandboxing, posibilidad de bloquear la descarga hasta que haya un veredicto.

- ✓ Sandbox Real-Time Deep Memory Inspection™ (RTDMI) para detección de ficheros maliciosos de día cero.

- ✓ VPN: Los equipos permitirán la creación de vpn's, tanto del tipo ipsec cómo del tipo vpn-*ssl . Para la solución vpn-ssl se necesita clientes que se puedan instalar localmente en máquinas Windows como tanto Mac, Linux y Android.

- ✓ Soporte para NetFlow e IPFix.

- ✓ Funciones automatizadas por la protección de ataques DDoS, así como todas aquellas que permitan la mejor protección posible contra ataques y vulnerabilidades avanzadas, como APT's, ataques día 0 o botnets.

- ✓ Proxy. Los equipos tienen que poder funcionar como un proxy de navegación transparente para los usuarios internos, gracias a las funcionalidades de control de aplicaciones, control de usuarios, url filtering, y reporting entre otros.

- ✓ Creación instancias virtuales,..., para crear zonas de seguridad independientes (red perimetral, red interna...), garantizando que el tráfico de una zona no podrá pasar nunca a las otras independientemente de las reglas de seguridad que existan.

- ✓ Los equipos tienen que implementar IPv6 y facilitar la transición de IPv4 a IPv6 de la red corporativa y su conexión hacia Internet.
- ✓ En el servicio de Filtrado Web (CFS), posibilidad de configurar múltiples páginas de bloqueo personalizadas..

- ✓ Monitorización de la salud del sistema. Visibilidad y reporting:
    - El sistema tiene que permitir visualizar todos los logs recogidos por los equipos (tráfico, events de seguridad, etc...) y hacer buscas en ellos de forma intuitiva, mostrando todo el detalle de información posible.
    - El sistema también tiene que agrupar los logs por aplicación, usuario, ip, url, etc... o por cualquier combinación de estos parámetros, como, por ejemplo, qué aplicaciones ha usado determinado usuario, cuántos bytes ha consumido con cada una de ellas, etc...
    - El sistema permitirá extraer varios tipos de informes automatizados y descargables.
    - Entre ellos tendrán que haber informes de la actividad de un determinado usuario de lo Active Directory corporativo: a qué web's ha navegado, durante cuánto de tiempo, qué aplicaciones ha usado (aplicaciones con tráfico hacia Internet que trabaran los cortafuegos), qué categorías de url ha visitado, qué accesos se le han denegado, etc...
    - Visión global, mediante gráficos y otros recursos, del estado de la red en cada momento: cantidad de tráfico, cantidad de malware parado, aplicaciones detectadas, url's más visitadas, usuarios más activos, etc…

1.2.3.- Servicios y Licencias

Servicios de instalación, migración de reglas, puesta en marcha.

Como complemento al suministro y servicios anteriores, deberán contemplarse los servicios de actualización asociados a los cortafuegos, las licencias de inteligencia de seguridad por un periodo mínimo de 3 años.

Como parte de los servicios solicitados, y asociado al periodo para el que se solicitan las correspondientes licencias de inteligencia de seguridad, deberá contemplarse como incluido el correspondiente servicio de soporte y mantenimiento de todos los equipos suministrados, en las condiciones que se reflejan a continuación.

1.2.4.- Soporte técnico del fabricante.

Se incluyen las suscripciones de firmas y patrones de malware/intrusiones y de filtrado de URL, las actualizaciones de software correspondientes, así como de soporte técnico, para reparación y sustituciones de hardware.
En concreto, el mantenimiento que se solicita debe incluir, al menos, los siguientes servicios:

- Soporte para reparación y reemplazo de hardware
- Actualizaciones de mantenimiento y nuevas funcionalidades.
- Soporte 24 x 7
- Soporte y actualizaciones de firmas, en su caso, para los servicios de antivirus, IPS, control de aplicaciones y categorización de contenidos (Web Filtering).
- Control de Aplicaciones (Application Control), con categorías.
- Prevención de Intrusiones (IPS).
- Gateway Antivirus Antivirus (AV).
- Filtrado Web (Web Filtering), con categorías.
- Entorno de ejecución protegido on cloud (Sandbox Cloud)
- Protección contra ataques de denegación de servicio
- Inspección SSL/SSH.
- Filtrado de conexiones geográfico (al menos por país de origen). Permitiendo bloquear tráfico según la zona geográfica
- Antispam

Para estos nuevos equipos, la instalación, configuración y migración de datos desde los equipos a retirar, será realizada por el adjudicatario en coordinación con los técnicos designados por el Ayuntamiento de Cuenca. El adjudicatario, para todos los equipos nuevos, deberá disponer de todos los accesorios de montaje necesarios para que puedan ser instalados en un rack estándar de 19".

Cuenca, en fecha de firma electrónica