Servicio de
Patrimonio, Compras
y Contratación
Universidad Zaragoza

CONTRATO DE SUMINISTRO

PROCEDIMIENTO ABIERTO

OFERTA: VARIOS CRITERIOS DE ADJUDICACIÓN

CONTRATO SUJETO A REGULACIÓN ARMONIZADA SI ☐ NO ☒

☒ Tramitación ordinaria ☐ Tramitación urgente ☐ Tramitación anticipada

Expte. nº 00112-2016

PLIEGO DE PRESCRIPCIONES TÉCNICAS

ÍNDICE DEL CLAUSULADO

OBJETO DEL CONTRATO
PRESCRIPCIONES TÉCNICAS
1. ALCANCE DEL PROCEDIMIENTO
2. REQUISITOS TÉCNICOS DE LOS EQUIPOS SOLICITADOS
3. FORMACIÓN

Nº Expediente: 00112-2016

PLIEGO DE PRESCRIPCIONES TÉCNICAS

Objeto del contrato:

Suministro, instalación, puesta en funcionamiento y formación de equipos de seguridad para la red de datos de la Universidad de Zaragoza.

Prescripciones técnicas:

1. ALCANCE DEL PROCEDIMIENTO

La Universidad de Zaragoza (UZ) está conectada a la Red de Investigación de Aragón RIA la cual le conecta a RedIRIS-NOVA y a Internet. El enlace de la UZ con la RIA es actualmente de 10 Gb/s.
En dicho enlace existen dos firewall diferentes que protegen la red:

- El primero es un Cisco Firewall Services Module (FWSM en adelante) en alta disponibilidad integrado en un router Cisco 6500. Este equipo tiene una antigüedad de más de 10 años, una limitación de ancho de banda de 5Gb/s haft dúplex.
- El otro firewall es un Palo-Alto 5050 que se adquirió en el año 2013.

El objetivo de este procedimiento es adquirir el equipamiento necesario para sustituir el FWSM por unos equipos nuevos en alta disponibilidad que nos permitan aprovechar todo el ancho de banda disponible y los incrementos que en un futuro puedan producirse.

2. REQUISITOS TECNICOS DE LOS EQUIPOS SOLICITADOS.

En este apartado se detallan las características técnicas mínimas requeridas a los equipos que se desea adquirir. Al presentar la oferta, el licitador debe ajustarse a la terminología utilizada en este apartado.
Se requiere que todos los componentes, hardware y software, necesarios para el correcto funcionamiento del equipamiento objeto del suministro tengan una permanencia mínima de 5 años y, consecuentemente, no se encuentren incluidos en procesos de discontinuidad, descatalogación o fin de vida del fabricante. Los licitadores deberán incluir en sus propuestas un documento del fabricante certificando dicha situación
El detalle y las características técnicas que deberán tener las ofertas presentadas por los licitadores son los que se detallan en los apartados siguientes del presente Pliego.

2.1. EQUIPOS SOLICITADOS.

El material objeto de suministro vendrá determinado por los equipos reflejados en la tabla presentada a continuación. Todo el material suministrado deberá ser entregado debidamente ensamblado.

Equipamiento	Cantidad requerida
Equipo cortafuegos (firewalls)	2

Los equipos deberán contar con licencia de IPS (intrusion prevention system) y de control de aplicaciones.

Nº Expediente: 00112-2016

PLIEGO DE PRESCRIPCIONES TÉCNICAS

2.2. CARACTERÍSTICAS GENERALES DE LOS EQUIPOS.

Se tratará de un sistema redundante de dos equipos en configuración activo/pasivo o activo/activo con las siguientes características:
1. Los equipos deberán trabajar en alta disponibilidad, teniendo en cuenta que tendrán como mínimo una conexión de nivel 2 a 1 Gbps entre ellos.
2. Los dos equipos deberán ser exactamente iguales, tanto en el software como en el hardware.
A continuación se detallan los requisitos que deberán cumplir cada uno de los dos equipos objeto de la licitación.

2.3. CARACTERÍSTICAS ESPECÍFICAS DE LOS EQUIPOS.

Las características que debe cumplir cada uno de los dos equipos objeto de la licitación son:

Generales:
Cada equipo cortafuegos debe de cumplir las siguientes características:

1. El cortafuegos debe tener las certificaciones de Internet Computer Security Association (ICSA): Cortafuego, IPS, Antivirus; NSS Labs y Common Criteria.
2. El cortafuegos dispondrá de hasta 80 Gbps de rendimiento de Firewall con paquetes UDP de 1500.
3. El cortafuegos debe ser capaz de manejar hasta 12.000.000 sesiones concurrentes.
4. El cortafuegos debe ser capaz de manejar hasta 300.000 nuevas sesiones por segundo.
5. El cortafuegos debe tener una latencia de 3 µs (para paquetes 64 byte UDP).
6. El cortafuegos dispondrá de hasta 15 Gbps de rendimiento de IPS.
7. Visualización de número de usos y cantidad de tráfico de cada regla.
8. El equipo propuesto debe tener una funcionalidad integrada de Traffic Shaping tanto de tráfico saliente con al menos las siguientes características:
   a. Capaz de establecer el ancho de banda garantizado.
   b. Capaz de establecer el ancho de banda máximo.
   c. Capaz de establecer el ancho de banda máximo asignado por IP.
   d. Capaz de establecer mínimamente 3 niveles de priorización.
9. El equipo debe tener las funcionalidades integradas de IPS, antivirus, Antispam y filtrado de contenidos o categorías web.
10. El licenciamiento de las funcionalidades ha de basarse por equipo, no por usuarios.
11. El control URLs debe tener la funcionalidad de aplicar cuotas de tiempo para aquellas categorías deseadas.

PLIEGO DE PRESCRIPCIONES TÉCNICAS

12. El equipo propuesto deberá disponer de un mínimo de:

    a. 18 interfaces Ethernet 10/100/1000 (cobre).
    b. 16 interfaces Ethernet SFP acelerados.
    c. 8 interfaces SFP+ 10Gbps.
    d. 480Gb de almacenamiento local Solid State Disk incluido.
    e. 1 puerto de consola.
    f. Doble Fuente de alimentación.

Avanzadas:
Adicionalmente, la solución debe tener las siguientes características avanzadas:

13. CONTROL DE APLICACIONES

    a. Capacidad para identificar un mínimo de 2400 aplicaciones activas actuales (incluyendo aplicaciones Web 2.0).
    b. El cortafuegos 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).
    c. Aplicar técnicas de identificación de aplicaciones a todos los puertos TCP / UDP y no sólo en los más comunes.
    d. Utilizar la identificación de la aplicación como base para las decisiones a la hora de establecer políticas de uso, permitiendo un control granular sobre el tráfico de la red.
    e. Capacidad para identificar las aplicaciones bajo túneles HTTPS.

14. IDENTIFICACIÓN DE USUARIOS

    a. Identificar usuarios, integrándose con Microsoft Active Directory y Novel eDirectory
    b. Control de usuarios Citrix.
    c. Control de usuarios de Microsoft Terminal Server.
    d. Soporte de mensajes Radius Accounting para SSO.
    e. Autenticación en servidores remotos mediante LDAP, RADIUS y TACACS+

15. VISIBILIDAD

    a. Funcionalidad de consolidación de logs y diferentes niveles de agrupación (origen, destino, aplicación, amenaza, websites y aplicaciones cloud), para su visualización.
    b. 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.
    c. Se tiene que poder seleccionar un tiempo de logs de hasta 24 horas, así como del tráfico que se está procesando en el firewall y que todavía no ha generado evento de

PLIEGO DE PRESCRIPCIONES TÉCNICAS

log (o "Now"), conocer a qué política de seguridad está aplicando y poder cerrar una conexión desde la misma visualización.

16. SEGURIDAD

a. Arquitectura basada en interfaces, para la aplicación de políticas de seguridad.
b. Capacidad para definir múltiples reglas de seguridad en las interfaces origen / destino, incluyendo "año".
c. Debe soportar varios modos de funcionamiento:
   - Modo transparente.
   - Modo routed y / o modo sniffer.
d. Funcionamiento como IPS basado tanto en patrones (basado en firmas) como en "Rated based". Posibilidad de crear firmas de IPS customizadas.
e. DLP: capacidad de búsqueda de patrones como DNI, tarjetas de crédito, etc., así como a asociaciones concretas. Más funcionalidades:
f. Posibilidad de definición de los tipos de dato en función de palabras clave, palabras clave ponderadas, expresiones regulares, atributos de archivo, diccionario, plantillas corporativas
g. Detección e identificación de documentos mediante "Fingerprint"
h. Posibilidad de añadir marcas de agua en los documentos de office.
i. Descarga y aplicación automática de actualizaciones de las firmas antivirus, antispyware, base de datos de URLs, firmas IPS y de las nuevas aplicaciones identificadas.
j. Funcionalidad integrada de doble factor de autenticación vía token hardware o software, asi como por SMS, integrado en la misma plataforma de seguridad.
k. Funcionalidad de reconocimiento del tipo de dispositivo del cliente (Iphone, Ipad, Android, etc ...) y poder hacer políticas en función del tipo de dispositivo, sin la instalación de ningún agente en el dispositivo remoto.
l. Inspección de tráfico cifrado SSL

17. VPN

a. El dispositivo dispondrá de hasta 4Gbps de rendimiento de VPN SSL y 50 Gbps de rendimiento IPSec (paquetes de 512 bytes).
b. El dispositivo admite hasta un máximo de diez mil usuarios simultáneos VPN SSL sin licencia adicional.
c. El sistema propuesto deberá cumplir los estándares de la industria, sin el apoyo externo adicional de hardware o módulos:

   i. IPSEC VPN (IPv4 e IPv6).
   ii. PPTP VPN.
   iii. L2TP VPN.
   iv. SSL VPN.

PLIEGO DE PRESCRIPCIONES TÉCNICAS

v. GRE sobre IPSEC.

d. El sistema propuesto deberá soportar 3 modos de funcionamiento SSL VPN:

vi. Sin cliente - Acceso web: para clientes remotos que sólo necesitan un navegador y no requiere la instalación de ningún software, a fin de acceder vía web en: HTTP / HTTPS Proxy, FTP, Telnet, SMB / CIFS, SSH, VNC i RDP.

vii. Modo túnel: para equipos remotos que ejecutan una variedad de aplicaciones de cliente y servidor.

viii. Modo Puerto Forwarding: utiliza un applet de Java que escucha en el puerto local en el ordenador del usuario. Cuando se reciben datos desde una aplicación de cliente, el puerto delantero cifra y envía los datos al dispositivo SSL VPN, que reenvía el tráfico en el servidor de aplicaciones.

18. ALTA DISPONIBILIDAD

El cortafuegos debe soportar las siguientes características cuando se disponga de dos equipos iguales para instalar en alta disponibilidad.

a. Failover Activo / Pasivo, Activo / Activo y clustering sin necesidad de licencia adicional.
b. Sincronización de configuración y sesiones.
c. Interfaces reservados para gestión.
d. Posibilidad de configurar interfaces HeartBeat redundantes.

19. NETWORKING

a. Soporte Dual Stack IPv4 e IPv6 simultáneamente.
b. Network address translation NAT IPv4, NAT64 y NAT66.
c. DHCP server / DHCP Relay.
d. DNS Server y DNS Proxy.
e. NTP Server.
f. 802.1Q VLANs.
g. Point-to-Point Protocol over Ethernet (PPPoE).
h. Capacidades de virtualización: El equipo debe disponer de al menos 10 dominios virtuales incluidos en el cortafuegos sin coste adicional.
i. 802.3ad Capacidad de crear enlaces LACP para la agregación de puertos.

Nº Expediente: 00112-2016

PLIEGO DE PRESCRIPCIONES TÉCNICAS

20. GESTIÓN Y ADMINISTRACIÓN

a. Soporte de SNMP y sFlow.
b. Exportación de logs vía SYSLOG, FTP, SCP y TFTP.
c. Administración por GUI y CLI directamente en el equipamiento, sin necesidad de instalar un cliente en máquina externa al firewall para su administración y / o cualquier otra función del firewall.
d. Creación de diferentes cuentas de administración con diferentes niveles de acceso.
e. El archivo de configuración debe ser un fichero de texto editable e interpretable.
f. Aplicación de cambios de forma inmediata, sin ninguna espera en su aplicación.

21. OTRAS FUNCIONALIDADES NECESARIAS

a. Balanceo de servidores HTTP con offloading SSL y persistencia de sesiones.
b. Posibilidad de ampliar la seguridad desplegando puntos de acceso inalámbrico con la capacidad de gestionar de manera centralizada y gestionados desde la misma plataforma de seguridad.
c. Arquitectura hardware basada en ASIC.
d. Rendimiento con paquete de 64 bytes superior a 50 Gbps.
e. Capacidad de balanceo de líneas por ip de origen, por número de sesiones, ponderado por pesos, midiendo la latencia y retardo de forma dinámica.
f. Funcionalidades de WAF incorporadas en el propio equipo.
g. Capacidad de integración con Sandbox en formato de appliance virtual del mismo fabricante.
h. Integración mediante icap y wccp con herramientas de terceros.
i. Capacidad de personalizar el cliente VPN.

3. FORMACIÓN.

El adjudicatario deberá incluir en su oferta la realización de un curso de formación para la gestión de los equipos suministrados que se efectuará una vez estén instalados los mismos. Dicho curso se desarrollará a razón de 6 horas diarias y tendrá una duración mínima de 12 horas distribuidas en 2 días. El curso se impartirá en las instalaciones de la UZ.

Zaragoza, a 25/10/2016
EL RECTOR,
P.D. (Resol. 19-4-2016, BOA nº 75 de 20-4-2016)
EL GERENTE,

Fdo.: Alberto Gil Costa