UNIÓN EUROPEA
Fondo Europeo de
Desarrollo Regional

Una manera de hacer Europa

CLÁUSULAS TÉCNICAS QUE REGIRÁN LA PETICIÓN DE OFERTAS PARA EL CONTRATO DE SUMINISTRO DE EQUIPAMIENTO PARA ANÁLISIS DE DDoSP PARA REDIMadrid - FUNDACIÓN IMDEA Software ref: 2019-12-DDoS

Índice

1. Introducción

REDIMadrid es la Red Telemática de Investigación de la Comunidad de Madrid y en su trayectoria ha vivido la explosión de Internet que ha supuesto el desarrollo de las tecnologías de la información y las comunicaciones como elemento fundamental de la sociedad de la información.

El objetivo principal de la Red Telemática de Investigación de la Comunidad de Madrid es la provisión de una infraestructura de alta fiabilidad, flexibilidad y capacidad que permita la experimentación de una amplia gama de servicios telemáticos, así como la puesta en marcha de multitud de aplicaciones y proyectos de investigación.

Se pretende también mejorar y favorecer el desarrollo del trabajo cooperativo entre grupos docentes, investigadores y del colectivo científico en general de las diferentes universidades y centros de investigación de la Comunidad de Madrid y posiblemente de otras instituciones, así como la interacción de diferentes grupos de trabajo indisciplinares dispersos, no necesariamente dentro del entorno académico.

Todos estos objetivos llevan al desarrollo de una serie de servicios que, de forma no exhaustiva, podemos ver listados a continuación:

- Servicios de Telefonía sobre IP / Videoconferencia.
- Servicios de Vídeo Bajo Demanda (VoD).
- Servicios de Teleeducación y Teleformación.
- Servicios de Telemedicina.
- Soporte de Redes Privadas Virtuales.
- Servicio de acceso a bases de datos multimedia (Bibliotecas Digitales).
- Servicios de Laboratorios Cooperativos (Laboratorios Virtuales).
- Sistemas de Tiempo Real de altas prestaciones.
- Experimentación de red piloto basada en IPv6 y QoS.
- Experiencias de Supercomputación en Red.

La combinación de los requisitos anteriores se concreta en la necesidad de gran capacidad de transporte a bajo coste y la posibilidad de su ampliación, así como la utilización de Protocolos de Internet (IP) y servicios de nivel 2.

Las necesidades de los investigadores están cambiando y eso exige una estructura de comunicaciones en la que el énfasis esté en los servicios diferenciados y en la utilización de la red como medio de colaboración para grupos cerrados de usuarios o como parte de grandes experimentos científicos de carácter regional, nacional e internacional.

2. Alcance del pliego

El Instituto IMDEA Software necesita adquirir equipamiento que permita la visualización de la red IP de REDIMadrid y la detección de ataques de denegación de servicio.

El equipamiento deberá cumplir las condiciones de hardware indicadas en el apartado 3 "Requisitos Técnicos".

Se solicita suministro hardware, la instalación y configuración y el soporte técnico de fabricante.

El equipamiento deberá cumplir con las condiciones de garantía y soporte indicadas en el apartado 3.4 "Garantía y Soporte".

3. Requisitos Técnicos

- El sistema de detección y visualización deberá cumplir los siguientes requisitos funcionales descritos a continuación. El licitador deberá proporcionar todos los recursos necesarios para desplegar dicha solución, ya sean hardware o software.
- El sistema de detección y visualización recibirá la información de telemetría de la red y realizará perfiles de tráfico para la detección de anomalías y ataques sobre los elementos de red definidos, debiendo alertar de diversas formas de aquellos problemas que encuentre.
- Esta información generará alertas sobre los ataques que se produzcan contra las instituciones conectadas a REDIMadrid, empleando el histórico de trafico recibido de esta telemetría.

- El sistema de detección y visualización deberá analizar e informar sobre los orígenes del tráfico desde diversas vistas incluyendo, routers e interfaces por los que ha circulado el tráfico, con indicación de los proveedores de transito por los que llega, sistemas autónomos origen del tráfico, países y zonas geográficas origen y de destino del tráfico.
- La herramienta deberá, además, analizar el comportamiento de la telemetría recibida, y compararla con la información proporcionada por los routers para así analizar la exactitud de la información.
- Para la monitorización y visualización de la red, se utilizará la información de telemetría (SNMP, Netflow) que proporciona ahora mismo la red de REDIMadrid, en este sentido la solución debe utilizar como método de detección los protocolos BGP, Netflow (y sus variantes Jflow, cFlow, etc.) y SNMP.
- La plataforma y todos los elementos que la constituyen deberán soportar, con prestaciones equivalentes, los protocolos IPv4 e IPv6 de Internet.
- Con caracter general la solución de detección ofertada debe incluir equipamiento o sistemas especializados acordes con las necesidades de un Proveedor de Servicios de Internet, “carrier class”.

3.1. Características del software

El software de detección y visualización podrá ser instalado en hardware dedicado, o en hardware virtualizado. En caso de que el adjudicatario opte por la segunda opción las características que están disponibles actualmente en REDIMadrid y por tanto las que debe cumplir la plataforma para su uso correcto, son las siguientes:

- 32GB RAM.
- 18 Core vCPU.
- KVM hypervisor.
- HDD 2TB.

3.2. Características del módulo de detección y visualización

El sistema de detección y visualización de red deberá detectar problemas en el tráfico de REDIMadrid y visualizar estas alarmas. Asimismo, deberá proporcionar informes sobre el estado de la red, las características mínimas que debe cumplir se exponen a continuación:

- El equipo de detección tiene que ser capaz de desviar el tráfico por BGP hacia el equipo de mitigación.
- El sistema debe soportar detección de anomalías por mal uso de la red mediante el rastreo y notificación de alertas, ciertos patrones de tráfico exceden lo que se considera uso normal de la red y/o violaciones en el uso del protocolo (Patrones de tráfico incluyen TCP SYN, TCP RST, TCP Null, ICMP, IP Null, Fragmentos IP, tráfico de direcciones IP y tráfico de direcciones multicast, entre otras).
- El sistema debe poder mantener líneas de tráfico base por protocolos y objetos de interés.
- El sistema debe identificar el tiempo de inicio y la duración de una anomalía, su tipo, nivel de severidad, patrón de tráfico, y el objeto administrado bajo amenaza si aplica.
- El sistema debe proveer identificación de direcciones IP mediante búsquedas WHOIS y resolución inversa de DNS.
- El sistema debe ser capaz de recomendar un límite de tasa o un filtro de lista de control de acceso (ACL) basado en información de la anomalía. La sintaxis de filtro debe ser adecuada para ser usada en configuraciones Cisco y Juniper (con soporte de FlowSpec, RFC5575) para mitigar un ataque.
- El sistema debe ofrecer a los usuarios la habilidad de generar huellas de tráfico (basadas en IP y Puertos TCP y UDP) arbitrarias para monitorear tráfico interesante.
- El sistema debe ofrecer huellas generadas según los perfiles de tráfico malicioso detectado y ser capaz de desplegarlo a los equipos de limpieza de trafico de forma automática.

- Detección de amenazas basadas en huellas pre-generadas por un proveedor de huellas de ataques, generadas por el gestor, compartidas desde otras empresas asociadas.
- El sistema debe proveer la habilidad de identificar el origen del tráfico malicioso (dirección IP origen del atacante).
- El sistema debe proveer un monitoreo en tiempo real.
- El sistema debe proveer la habilidad para analizar los protocolos de las capas de la aplicación.
- El sistema debe ser capaz de identificar los sistemas autónomos implicados en un ataque, proporcionando información de los interfaces y routers del troncal de REDIMadrid por los que llega el tráfico.
- El sistema debe tener una capacidad incial para monitorerar y detectar como mínimo 200 objetos/redes IP entre IPv4 como IPv6 y sistemas autónomos, este numero de objetos debe poder escalar al menos a 5.000 mediante la compra de licencias.
- La solución debe incluir un módulo de análisis de tráfico sobre la seguridad de la red, para identificación de patrones, y una total visibilidad para trabajar análisis de tráfico y consideraciones futuras. Este análisis de tráfico debe poder almacenarse y generar firmas para su posterior utilización.
- El sistema deberá proveer monitorización para los nodos de Core, los nodos de la red de Borde y Peering teniendo la capacidad de monitorear la capa de Acceso mediante expansión de la plataforma.
- El equipo de monitoreo debe tener capacidad para recolectar tráfico BGP, SNMP y NETFLOW.
- La monitorización netflow se podrá utilizar para caracterizar el tráfico de red y poder realizar funciones de optimización mejorada de la infraestructura de red, análisis de rutas, planificación de capacidad y seguridad.
- El sistema debe aceptar Cisco Netflow, Cisco Netflow v5, Cisco Netflow v9, Juniper jflow v5, Juniper jflow v9, Sflow.

- El sistema debe ser escalable para poder monitorear interfaces a todas las velocidades soportadas por la topología existente.
- El sistema debe soportar el monitoreo de al menos 80.000 interfaces con la misma GUI, solamente con agregar más elementos de recolección de datos.
- El sistema debe soportar el monitoreo de al menos 100 routers con la misma GUI, solamente con agregar más elementos de recolección de datos.
- El Sistema debe aceptar información de rutas BGP de todos los enrutadores monitoreados en la red.
- El Sistema debe soportar sesiones BGP que pueden o no estar autenticadas por sistemas de encriptación tales como MD5.
- El Sistema debe entender información de rutas y los AS-PATH completos y comunidades BGP de múltiples Sistemas Autónomos (SA) independientes, en un ambiente reflejado (usando route reflectors) y/o de un espacio de SA privado, y debe contar con reportes de análisis de tráfico de peering para cada peer, por prefijo IP y de cada objeto administrado por peer y por interface.
- El sistema ofertado debe soportar MPLS, IOS XR de Cisco, IOS estándar, CATOS, entre otros, además sistemas operativos de Foundry , Juniper , Fortinet, Check-Point y PaloAlto.
- El sistema deberá monitorizar y reportar el trafico originado por cada uno de los enlaces del troncal de REDIMadrid, incluyendo el trafico originado por cada uno de las redes externas a REDIMadrid con las que se hace peering.
- Debe proporcionar información sobre la localización geográfica del trafico destinado que pasa por el troncal de REDIMadrid, tanto a nivel de país y continente.
- El sistema permitirá identificar dentro de cada uno los elementos monitorizados cuales son las direcciones IP que generan un mayor tráfico tanto entrante como saliente.
- Debe ser complemente configurable y gestionable vía API REST y CLI.

- Tener una API abierta de tal manera que en el futuro se pueda adaptar al envió de alarmas a un software para configurar reglas de firewall a través de BGP flowspec, en este sendio la API debe debe proporcionar una API JSON para importar/exportar configuraciones de objetos de red para facilitar la operación y la integración con otros software/sistemas.
- El sistema debe soportar algunos modelos de tráfico de red incorporados para el análisis de tráfico, los modelos incorporados definen objetos de red de algunos tipos (por ejemplo, Home/Internet, Neighbor, Sub-Network and Server Farm).
- El sistema permite definir un modelo de red mediante uno o más bloques CIDR, ASNs, interfaces, BGP community string, BGP AS, hostname, protocolos, puertos, aplicaciones, AS Path.

3.3. Solución a ofertar

Como mínimo el sistema de detección y visualización tendrá capacidad para:

- Monitorizar el troncal de REDIMadrid, que comprende ahora mismo 2 router de CORE/peering con RedIRIS.
- Debe ser capaz de analizar el tráfico de hasta 200 objetos/entidades de visualización (redes IPv4, IPv6, Sistemas autónomos, etc.)
- Debe ser capaz de procesar hasta 20.000 flujos por segundo (de forma sostenida tanto en IPv4 como IPv6 y en los formatos de envió de flujos soportados por el troncal de REDIMadrid (Netflow v5 y v9)
- Permitir el acceso de 15 usuarios simultáneos vía las distintas opciones de acceso (CLI, Web interface, API).

3.4. Garantía o Soporte

El servicio de garantía o soporte deberá ser proporcionado por el fabricante de los equipos, del software y/o de los componentes objeto del suministro, aunque la gestión de las incidencias se realizará por el licitador adjudicatario del contrato.

El servicio de garantía del fabricante deberá estar activo durante, al menos, un año a partir del momento del suministro del equipamiento. Este periodo aplicará a todos los equipos, y el software necesario. La garantía del fabricante debe incluir:

- Un soporte especializado de los fabricantes de los equipos, software y componentes suministrados, que asegure la disponibilidad y operatividad del equipamiento de este fabricante.
- La garantía incluirá, entre otros, el soporte para el análisis de incidencias tanto hardware (si se ha ofertado hardware) como software hasta su completa resolución. Este análisis puede requerir el soporte para estudiar y tratar errores, logs, alarmas, avisos, etc, generados por el equipamiento o el software. Asimismo, entre otras posibles, la incidencia se podría solucionar con la sustitución de hardware o con el suministro de parches software específicos o actualizaciones completas del sistema operativo o con la aplicación de configuraciones optimizadas.
- El Servicio también incluirá el acceso al centro de soporte del fabricante, el suministro de las nuevas versiones de software que el fabricante vaya desarrollando y liberando, con nuevas y/o mejoradas prestaciones y funcionalidades, así como el apoyo técnico ante dudas sobre configuraciones que estuvieran en operación.
- Las licencias necesarias para el correcto funcionamiento de la plataforma deberán estar activas durante un año.
- Se entiende por Tiempo Máximo de Reposición de Hardware (TMRH) aquel que transcurre entre el momento en que se determina que hay que sustituir un elemento hardware y el momento en que llega al destino indicado en la gestión de la sustitución.
- El TMRH variará entre los diferentes componentes o equipos suministrados, tal que:

    1. Los equipos o el hardware dedicado a la plataforma de visualización, detección e inyección de rutas BGP tendrá un TMRH de 4 horas en el caso de que se suministre equipamiento dedicado. En caso de que el licitador opte por suministrar una plataforma virtualizada para albergar las máquinas de servicio el TMRH será de Next Business Day - NBD.

- REDIMadrid tendrá acceso directo, 24 horas al día, todos los días del año, al centro de soporte para consultas hardware y software objeto del suministro vía telefónica, correo electrónico y web, para realizar consultas técnicas, abrir incidencias, acceder a documentación privada, así como obtener parches y actualizaciones o cualquiera de las nuevas versiones software liberadas por el fabricante, que puedan ser descargadas y puestas en operación en dichos equipos.

4. Formación

- Se requiere que le adjudicatario preste un sesión de formación de, al menos, 24 horas basadas en la administración y operación del software y hardware (si se oferta) ofertado, la formación debe estar enfocada a la solución que se va a implantar en REDIMadrid.
- La sesión de formación se realizaran en castellano, aunque la documentación oficial puede estar redactada en ingles o en español.
- La formación estará destinada, al menos, para 6 personas.
- El licitador será responsable del suministro del material de formación a los asistentes a las sesiones.
- Se requiere que la formación sea impartida por personal con conocimientos acorde con la formación que se va a impartir, para este fin se solicitara datos del instructor antes de realizar la formación, REDIMadrid podrá decidir si el instructor esta suficientemente formado.
- La formación se realizará en el lugar y días que a tales efectos designe IMDEA Software.

5. Consultas y Contacto

Cualquier consulta en relación con el presente procedimiento de adjudicación debe dirigirse por correo electrónico a la dirección noc@redimadrid.es indicando:

Asunto: Licitación DDoS.
Cuerpo: nombre de la empresa, datos de la persona que realiza la consulta y texto de la consulta.

El plazo de recepción de consultas finalizará 24 horas antes del fin del plazo de presentación de ofertas. IMDEA Software no tendrá obligación de responder las consultas realizadas transcurrido dicho plazo.

6. Confidencialidad

El adjudicatario garantizará la seguridad y confidencialidad de toda la documentación e información sobre REDIMadrid de la que disponga, disponiendo los medios necesarios para ello. Esta obligación estará en vigor aun cuando el contrato haya llegado a su término o haya sido cancelado.