SEGUNDO INFORME - ACTA DE REEVALUACION Nº 86 / 2015
LICITACIÓN PUBLICA NACIONAL SBE Nº 04/2015
"ADQUISICIÓN DE SOLUCIONES DE SEGURIDAD PARA REDES"
ID 299141

1. Introducción

En la ciudad de Asunción, capital de la República del Paraguay, el 25 de noviembre de 2015, siendo las 14:00 horas, se reúnen los funcionarios designados para integrar el comité de evaluación, con el fin de reevaluar el ITEM N° 2, de acuerdo a lo ordenado por la Resolución DNCP N° 3630/15 de fecha 20 de noviembre del corriente que, en su art. 2° menciona *"Hacer lugar a la protesta promovida por la firma INFOCENTER S.A. contra la adjudicación del Ítem N° 2..."*, y en su Art. 3° *"Anular Parcialmente la Resolución N° 3376/2015 de fecha 30 de octubre de 2015, que resuelve la Adjudicación del ITEM N° 2 a favor de Tecnología en Electrónica e Informática S.A. (TEISA), y en consecuencia retrotraer lo actuado a la etapa de Evaluación de Ofertas con relación al ítem impugnado"*.

2. Análisis del ITEM N° 2

Conforme a lo establecido en el Artículo 61 *"Método de evaluación"* del Decreto Reglamentario Nº 21909/03 *"3. Se seleccionará provisoriamente a la oferta con el precio más bajo,... la que será analizada en detalle para verificar su cumplimiento con otros requisitos de la licitación..."*, se procede a examinar previamente el cumplimiento con las Especificaciones Técnicas del PBC para el ítem N° 2, razón por la cual, para un mejor análisis se detallan los precios de menor a mayor:

OFERENTE	CANTIDAD	PRECIO UNITARIO (IVA incluido)	PRECIO TOTAL (IVA incluido)
DATA LAB S.A.	2	215.000.000	430.000.000
NETLOGIC S.R.L.	2	225.000.000	450.000.000
TEISA	2	275.000.000	550.000.000
INFOCENTER S.A.	2	320.000.000	640.000.000
TECHNOMA S.A.C.I.	2	NO COTIZA	NO COTIZA
LOGICALIS PARAGUAY S.A.	2	NO COTIZA	NO COTIZA

Se deja constancia que mediante el Acta de evaluación N° 64/2015, las ofertas de las firmas **DATA LAB S.A.** y **NETLOGIC S.R.L.** han sido rechazadas debido al incumplimiento con las especificaciones técnicas expuestas en la misma, razón por la cual se pasó a verificar el cumplimiento de la oferta de la firma Tecnología en Electrónica e Informática S.A. (TEISA).

Según lo establecido en el Articulo 59 *"Disconformidades, errores y omisiones"* del Decreto 21909/03, para corroborar el cumplimento con las especificaciones técnicas, en fecha 26/11/2015, se ha solicitado documentación a la firma TEISA, dando plazo para respuesta hasta el 27 de noviembre del corriente. En el plazo solicitado, se ha recibido vía mesa de entrada la respuesta del oferente, cumpliendose así con lo solicitado por la convocante.

Por lo tanto, a continuación se realiza el análisis técnico, detallado en la siguiente planilla:

DIRECCIÓN NACIONAL DE CONTRATACIONES PÚBLICAS * DON * Dirección Administrativa

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

Hugo Araujo
Jefe de Redes - DNCP

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

Solución de Seguridad perimetral para redes		PROPUESTA DEL OFERENTE
Características	**Mínimo Exigido**	**TEISA**
Identificación		
Cantidad	2	**CUMPLE**
Marca	Especificar	**FORTINET**
Modelo	Especificar	**900D**
Numero de Parte	Especificar	**FG-900D-BDL-900-36**
Procedencia	Especificar	**EEUU**
Formato		
La solución deberá ser rackeable en racks estándar de 19", con los que ya cuenta la DNCP.	Exigido	CUMPLE
Los procesadores de los equipos componentes de la solución deben ser de la última generación disponible según la web del fabricante del mismo.	Exigido	CUMPLE
Redundancia		
La solución deberá contemplar redundancia en todos sus componentes (Firewall, IPS, AntiSpam, URL Filter,).	Exigido	CUMPLE
Interfaces		
La solución deberá contar mínimamente con 3 (tres) interfaces de fibra de 1Gbps con sus respectivos módulos SFP y una interfaz dedicada para administración del equipo, por cada equipo que componga la solución	Exigido	CUMPLE
Almacenamiento		
La solución deberá prever la capacidad de Almacenamiento de al menos 120 GB	Exigido	CUMPLE
Soporte de Interfaces		
1000BASE-T, 1000BASE-X, 1000BASE-SX, 1000BASE-LX.	Exigido	CUMPLE
Administración de la Solución		
Interfaz CLI, GUI a través de https además debe soportar conexiones ssh	Exigido	CUMPLE
El sistema operativo de la solución ofertada debe ser de propósito específico y no uno de uso genérico, es decir un SO desarrollado por el fabricante de la solución.	Exigido	CUMPLE
La solución debe permitir la configuración de perfiles de administración, los cuales permitirán la limitación de funciones que pueden ser gerenciados.	Exigido	CUMPLE
Debe soportar snmp v2 y v3, syslog remoto	Exigido	CUMPLE
La solución deberá soportar un agendado de backup de sus configuraciones	Exigido	
Alta Disponibilidad de los componentes de la solución		
Deberá soportar Alta Disponibilidad sin pérdida de conexiones en caso del fallo de uno los nodos, soporte de Modo Activo-Activo, Activo-Pasivo.	Exigido	CUMPLE
Sincronización de sesiones	Exigido	CUMPLE
Firewall		
Firewall de capa 7,4,3 y 2	Exigido	CUMPLE
IEEE 802.1Q VLAN, IEEE 802.ad LACP,	Exigido	CUMPLE
Debe soportar al menos 10.000 mac address	Exigido	CUMPLE
Soporte de ECMP (Equal Cost Multi-Path)	Exigido	CUMPLE
La solución debe permitir la integración con analizadores de tráfico mediante el protocolo sFlow o netflow en su última versión	Exigido	CUMPLE
Soporte de al menos 10.000 rutas IPv4	Exigido	CUMPLE
Ruteo Estático	Exigido	CUMPLE
Funcionamiento en modo Routed y Transparent	Exigido	CUMPLE
NAT, PAT, NAT con PAT, DHCP Server	Exigido	CUMPLE
La solución podrá habilitar políticas de ruteo en IPv6, RIPng, OSPFv2 y 3	Exigido	CUMPLE
La solución deberá poder comunicar direccionamiento IPv6 a servicios con IPv4 y	Exigido	CUMPLE

Hugo Araujo
Jefe de Redes - DNCP

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

Lic. Nuelia Ricagno
Dirección Administrativa
DNCP

viceversa		
BGP v4. La configuración de BGP debe soportar Autonomous System Path (AS-PATH) de 4 bytes.	Exigido	CUMPLE
Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces o vlans.	Exigido	CUMPLE
Deberá ser posible definir políticas de firewall para puertos tcp y udp independientes en cada interfaz ya sea tráfico entrante o saliente.	Exigido	CUMPLE
Las reglas del firewall deberán poder aplicarse a dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios).	Exigido	CUMPLE
Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar interfaz física origen, interfaz física destino, direcciones IP origen, dirección IP destino.	Exigido	CUMPLE
Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos.	Exigido	CUMPLE
Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a tiempo y fechas (incluyendo día, mes y año).	Exigido	CUMPLE
Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión.	Exigido	CUMPLE
Debe poder definirse el tiempo de vida de una sesión inactiva de forma independiente por puerto y protocolo (TCP y UDP)	Exigido	CUMPLE
Deberá soportar reglas de firewall en IPv6	Exigido	CUMPLE
Deberá será capaz de crear e integrar políticas contra ataques DoS las cuales se deben poder aplicar por interfaces, El dispositivo debe generar logs de cada una de las políticas aplicadas para evitar los ataques de DoS	Exigido	CUMPLE
Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall.	Exigido	CUMPLE
Throughput firewall minima de 1000 Mbps	Exigido	CUMPLE
BOTNET		
La solución ofertada debe incorporar protección contra botnets, debe poder bloquear intentos de conexión a servidores de Botnets, para ello se debe contar con una lista de los servidores de Botnet más utilizado. Dicha lista debe actualizarse de forma periódica por el fabricante, y deberá estar previsto en la oferta la suscripción al servicio durante el periodo de garantía.	Exigido	CUMPLE
VPN		
El oferente en su oferta deberá contemplar al menos 30 licencias para usuarios VPN concurrentes del tipo Client to Site y por lo menos 100 licencias del tipo Site to Site	Exigido	CUMPLE
Deberá soportar conexiones VPN del tipo Site to SIte, client to Site, Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES,	Exigido	CUMPLE
Debe soportar longitudes de llave para AES de 128, 192 y 256 bits, algoritmos de integridad: MD5, SHA-1 y SHA256.	Exigido	CUMPLE
La solución deberá contar una aplicación nativa para dispositivos móviles IOS y Android como mínimo, además deberá poder autenticar usuarios de la VPN con Active Directory 2008 R2.	Exigido	CUMPLE
Deberá poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL.	Exigido	CUMPLE
Sistema de Prevención de Intrusiones		
El oferente en su oferta deberá contemplar la suscripción al servicio de actualización de firmas por la duración del periodo de garantía	Exigido	CUMPLE
El sistema de prevención de Intrusos deberá estar orientado a la protección de redes y servidores.	Exigido	CUMPLE
Deberá soportar la detección de distintos tipos de ataques basándose en firmas actualizables.	Exigido	CUMPLE
Deberá poder mitigar los efectos de ataques de denegación de servicios.	Exigido	CUMPLE
Debe contar con mecanismos de detección de ataques basados en reconocimiento de patrones y análisis de protocolos.	Exigido	CUMPLE
Debe poseer mecanismos de protección contra ataques de RPC (Remote Procedure Call).	Exigido	CUMPLE

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

Hugo Araujo
Jefe de Redes - DNCP

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

Debe permitir bloquear tráfico entrante, saliente o ambos correspondientes a determinados países, sin necesidad de actualizar manualmente los rangos IP correspondientes a cada país.	Exigido	CUMPLE
El ips debe poseer configuraciones o firmas predefinidas para servidores que actúen ya sea como webserver, servidor de dns, servidor de correo o Servidor de Base de Datos	Exigido	CUMPLE
Deberá prevenir amenzas del tipo día 0, A través de sandboxes como un entorno aislado y separado, donde los archivos son monitoreados y ejecutados para determinar si son seguros o maliciosos. La detección puede ser de forma Local o en la Nube	Exigido	CUMPLE
Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6.	Exigido	CUMPLE
Debe poseer mecanismos de protección contra ataques de Windows o Netbios.	Exigido	CUMPLE
Debe poseer mecanismos de protección contra ataques de SMTP IMAP o POP.	Exigido	CUMPLE
Debe poseer mecanismos de protección contra ataques DNS.	Exigido	CUMPLE
El dispositivo debe poder filtrar el tráfico de posibles amenazas con requerimientos inusuales a aplicaciones conocidas o a la arquitectura de red.	Exigido	CUMPLE
Debe ser capaz de reconocer las vulnerabilidades en la red para determinar si puede afectar o no el funcionamiento de esta y sugerir las acciones para protegerla.	Exigido	CUMPLE
Debe proveer información detallada de cada tipo de ataque, Capacidad para manejar perfiles de configuración, Detección de vulnerabilidades, exploits, validacion de protocolos, detección de anormalidades ,detección de ataques basado en conductas, por ej: multiples intentos de logueo ssh en pocos segundos, Capacidad de crear Excepciones.	Exigido	CUMPLE
Protección Antimalware		
La solución deberá poder interceptar la comunicación SSL, desencriptar el trafico inspeccionar el tráfico y aplicar políticas según sea el caso.	Exigido	CUMPLE
La solución deberá permitir instalar un agente para la detección de Malware en los clientes y soportar los siguientes SO: MS Windows 7, 8, MS Windos Server 2008 R2, MS Windows Server 2012, Mac OS X 10.X O superior.	Exigido	CUMPLE
El software instalado en los clientes deberá permitir el bloqueo de archivos maliciosos directamente en la maquina victima sin necesidad de involucrar a otros equipos	Exigido	CUMPLE
La solución deberá de permitir una visibilidad retrospectiva de modo a visualizar y hacer un trazado de los archivos maliciosos una vez ingresado a la red.	Exigido	CUMPLE
La solución deberá ser capaz de integrarse a Directorio Activo Windows para detectar y aplicar políticas basados en usuarios, si la estación de trabajo de un usuario cambia de ip la solución deberá de detectar y aplicar las políticas asociadas a ese usuario.	Exigido	CUMPLE
Filtrado de direcciones URL		
El oferente en su oferta debe contemplar suscripción al servicio de actualizaciones de categorías de filtrado URL para al menos 300 usuarios que deberá estar vigente durante el periodo de garantía	Exigido	CUMPLE
Debe poseer la capacidad de filtrar páginas web (Url Filtering).	Exigido	CUMPLE
Debe poder aplicar restricción de ancho de banda ya sean para cierto tipo de tráfico, streaming de audio o video, p2p.	Exigido	CUMPLE
Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación de las mismas para la regla en general.	Exigido	CUMPLE
Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo.	Exigido	CUMPLE
Capacidad de poder definir prioridad de tráfico, en al menos tres niveles de importancia.	Exigido	CUMPLE
Facilidad de incorporar sitios a los cuales naveguen los usuarios, y establecer mediante categorías el acceso de los mismos.	Exigido	CUMPLE
Filtrado de contenido basado en categorías en tiempo real.	Exigido	CUMPLE
Deberá tener la facilidad de crear perfiles para el acceso web, diferenciando el origen ya sean por dirección ip o segmento de red o por usuarios o grupos de usuarios.	Exigido	CUMPLE
Los mensajes entregados al usuario por parte del URL FILTER (en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables, Facilidad de incorporar sitios a los cuales naveguen los	Exigido	CUMPLE

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

Hugo Araujo
Jefe de Redes - DNCP

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

4

usuarios, y establecer mediante categorías el acceso de los mismos.		
Control de Aplicaciones		
El oferente en su oferta debe contemplar suscripción al servicio de control de aplicaciones para al menos 300 usuarios que deberá estar vigente durante el periodo de garantía	Exigido	CUMPLE
Posibilidad de crear políticas granulares para usuarios o grupo de usuarios.	Exigido	CUMPLE
Identificar, bloquear o limitar las aplicaciones y las funciones dentro de las aplicaciones.	Exigido	CUMPLE
Control Granular en streaming de video, debe permitir configurar políticas para la calidad de reproducción, por ej; configurar el streaming de un video 240 p		CUMPLE
Control Granular de Redes Sociales (Facebook, Twitter, YouTube, Instagram, Google+, LinkedIn, Tagged, Flickr, Pinterest, Badoo) Por ejemplo si un usuario accede a la red Social Facebook, la herramienta deberá poder permitirle solo acceso de lectura o debe poder deshabilitar las funciones de chat o Posteo de Publicaciones.	Exigido	CUMPLE
En el caso de los programas para compartir archivos (peer-to-peer) deberá poder limitar el ancho de banda utilizado por ellos, de manera individual.	Exigido	CUMPLE
Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.	Exigido	CUMPLE
La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.	Exigido	CUMPLE
Identificación y Monitoreo de Usuarios		
Debe poseer capacidades de identificación de usuarios en la red por computadora, por dirección ip, o por grupos.	Exigido	CUMPLE
Debe poder monitorear tráfico tanto de usuarios de un Directorio Activo como para usuarios Guest.	Exigido	CUMPLE
Seguridad para Servidor de Correo		
El oferente en su oferta debe incluir subscripciones para soportar las funcionalidades de antispam y antivirus para al menos 300 usuarios durante el periodo de vigencia de la garantía	Exigido	CUMPLE
Debe ser capaz de detectar palabras o url's dentro del contenido del correo.	Exigido	CUMPLE
Debe ser compatible con servidores de Correo Microsoft Exchange 2012	Exigido	CUMPLE
Deberá permitir especificar listas blancas (confiables, a los que siempre se le deberá pasar) y listas negras (no confiables, a los que siempre se les bloqueara), las listas blancas y negras deberán ser configurables por dirección ip o dominio.	Exigido	CUMPLE
Cuando la solución detecta un SPAM tiene que marcarlo.	Exigido	CUMPLE
Debe poseer un antivirus incorporado al proceso de análisis de email	Exigido	CUMPLE
Reportes		
Deberá ser provista una herramienta para correlacionar eventos de todas las funcionalidades de la solución.	Exigido	CUMPLE
Debe poder generar automáticamente gráficos o tablas de distribución de eventos, orígenes y destinos, en la vista del listado de eventos.	Exigido	CUMPLE
La herramienta debe poseer la capacidad de almacenamiento suficiente indicada por el fabricante de conservar los datos por lo menos durante 3 meses Considerando 300 usuarios.	Exigido	CUMPLE
La herramienta de reportes debe soportar la creación de reportes que permita personalizar los reportes predefinidos a las necesidades del administrador (ej. Actividades web de un usuario especifico)	Exigido	CUMPLE
Debe ser capaz de hacer búsquedas por username o dirección IP, para que toda la información almacenada de dicho username o dirección IP sea mostrada en un reporte donde pueda darse seguimiento a su actividad	Exigido	CUMPLE
Debe proveer un reportador basado en una línea de tiempo, para reportes predefinidos o a la medida, permitiendo al administrador realizar análisis de contenido en tiempo real	Exigido	CUMPLE

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

Hugo Araujo
Jefe de Redes - DNCP

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

Dichos reportes deben incluir una explicación acerca de las políticas que fueron violadas y que parte del contenido causó dicha violación.	Exigido	CUMPLE
Debe permitir agrupar los eventos en base a cualquier característica de los mismos, pudiendo agrupar en varios niveles.	Exigido	CUMPLE
Debe permitir la creación de reportes personalizables.	Exigido	CUMPLE
Debe detectar ataques de denegación de servicio, correlacionando eventos de todas las fuentes.	Exigido	CUMPLE
Requisitos eléctricos y de funcionamiento		
Fuentes de poder internas redundantes y hot swap.	Exigido	CUMPLE
Voltaje 220V AC, 50/60 Hz.	Exigido	CUMPLE
Ventiladores redundantes.	Exigido	CUMPLE
La solución deberá poseer fuentes redundates internas con cables que se conecten a PDUs con conectores IEC-60320 C14 que deberán ser provistos por el oferente	Exigido	CUMPLE
Garantía (Escrita)		
Para garantizar a la institución, la garantía así como la asistencia técnica especializada, será un requisito indispensable que la garantía pueda ser ejecutada en cualquiera de los CAS del país. El oferente deberá indicar cuales son los CAS que existen en el país. La gestión de la ejecución de la garantía, deberá poder ser hecha, directamente a través de cualquiera de los CAS del país, o en su defecto, a través del Oferente, corriendo en su caso, por cuenta del Oferente que resulte adjudicado, la gestión de dicha ejecución. La atención del soporte técnico debe tener un nivel de soporte 8x5xNBD durante 3 años	Exigido	CUMPLE
Todos los equipos deben ser nuevos, de fabricación reciente, encontrarse en comercialización activa	Exigido	CUMPLE
Experiencia		
La empresa oferente deberá presentar documentos que acrediten la experiencia propia o de la marca ofertada dentro del territorio nacional en al menos 2 implementaciones de soluciones iguales a las licitadas. Los documentos deberán contener como mínimo el nombre del cliente donde se ha implementado la solución, el número telefónico de contacto y se deberá contar con la posibilidad de poder realizar una visita técnica a dicho cliente.	Exigido	CUMPLE
Capacitación		
Se deberá proveer un curso de capacitación de al menos 40 horas para 2 funcionarios de la DNCP, el contenido del curso deberá contemplar desde la instalación, configuración y puesta a punto de los componentes de la solución.	Exigido	CUMPLE
Instalación		
El personal asignado deberá estar calificado en instalación y configuración de la solución ofertada, y con experiencia comprobable.	Exigido	CUMPLE
Alcance: El servicio contemplará todos los suministros, actividades de montaje, instalación en general, configuración y puesta en funcionamiento de la solución ofertada.	Exigido	CUMPLE
Accesorios: Todos los accesorios necesarios para el buen funcionamiento del equipo serán proveídos por la empresa oferente.	Exigido	CUMPLE
El oferente deberá detallar en una planilla adjunta a la oferta los números de parte del fabricante de cada componente de la solución: 1- El equipo ofertado. 2- Las partes incluidas con la oferta para que el equipo cumpla con todos los requerimientos del pliego de bases y condiciones. Ejemplo: 2 | XXXX | 10 GbE SFP+ SR. 3- El detalle de licencias incluido con cada equipo para habilitar los requerimientos del pbc, tanto de funcionalidad como de performance. Ejemplo: 2 | XXXX | Licencias para habilitar XXX usuarios VPN. 4- Las garantías 5x8 NBD. 2 | XXXX | Soporte 5 x 8 del Fabricante. 5- Las suscripciones de software que se incluyan con los equipos por el periodo de garantía de los equipos. Ejemplo: 2 | XXXX | Licencias para Actualización de Firmas del IPS. La planilla deberá contener mínimamente estos datos: Cantidad, Numero de Parte, Descripción del Producto/Funcionalidades que habilita	Exigido	Presenta

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

Hugo Araujo
Jefe de Redes - DNCP

Hugo Humberto Báez Infante
Asesor Técnico - Legal
DNCP

6

Durante el análisis se realizaron las siguientes consultas:

- Para el ITEM 2, favor indicar detalladamente cuál es la plataforma a ser provista para utilizar el FAZ-VM-BASE FortiAnalyzer.

- Para el ITEM 2, favor remitir documentación que acredite que con el FortiAnalyzer FAZ-VM-BASE se llegara a los periodos de retención solicitados en el PBC.

- Para el ITEM 2, favor remitir documentación que acredite que el equipo ofertado cuenta con: Requisitos eléctricos y de funcionamiento,
  Fuentes de poder internas redundantes y hot swap.

Las mismas fueron respondidas y aclaradas mediante Nota de fecha 27 de Noviembre del corriente, con las que se pudo determinar que la firma Tecnología en Electrónica e Informática S.A. (TEISA) cumple con las condiciones legales, técnicas y económicas establecidas en el Pliego de Bases y Condiciones, por lo que se recomienda su adjudicación.

3. Conclusión

En base a las consideraciones expuestas en el presente informe, y de conformidad a los Artículos 27 y 28 de la Ley Nº 2051/03 y los Artículos 58 al 63 del Decreto Reglamentario Nº 21909/03, el Comité de Evaluación recomienda, ADJUDICAR a la firma **TECNOLOGÍA EN ELECTRÓNICA E INFORMÁTICA S.A. (TEISA)** el **ITEM 2** de la **Licitación Pública Nacional SBE Nº 04/2015 "ADQUISICIÓN DE SOLUCIONES DE SEGURIDAD PARA REDES"**, por un monto total de Gs. 550.000.000 (Guaraníes quinientos cincuenta millones); por ser una oferta conveniente a los intereses institucionales, por cumplir con las especificaciones técnicas requeridas, las condiciones legales y la capacidad necesaria para responder a los compromisos asumidos.
Es nuestro informe.

Finaliza el presente, a los 30 días del mes de noviembre del 2015.

DIRECCIÓN NACIONAL DE CONTRATACIONES PÚBLICAS
Dirección Administrativa
UOC

Sr. Hugo Araujo

Lic. Noelia Ricagno

Abg. Humberto Báez

DNCP
DIRECCIÓN NACIONAL DE CONTRATACIONES PÚBLICAS

GOBIERNO NACIONAL
Construyendo el futuro hoy

Asunción, 26 de noviembre de 2015

Señores
TEISA
Presente

Me dirijo a ustedes, de acuerdo a la solicitud realizada por parte del comité evaluador, en referencia a su oferta presentada para el llamado a Licitación Pública Nacional SBE N° 04/2015 **"ADQUISICION DE SOLUCIONES DE SEGURIDAD PARA REDES"**, y teniendo en cuenta las facultades previstas en el Artículo 59 "Disconformidades, errores y omisiones" del Decreto 21909/03, requerimos:

Para el ITEM 2

- Indicar detalladamente cuál es la plataforma a ser provista para utilizar el FAZ-VM-BASE FortiAnalyzer.
- Remitir documentación que acredite que con el FortiAnalyzer FAZ-VM-BASE se llegara a los periodos de retención solicitados en el PBC.
- Remitir documentación que acredite que el equipo ofertado cuenta con:
  Requisitos eléctricos y de funcionamiento
  Fuentes de poder internas redundantes y hot swap.

La documentación requerida deberá ser presentada a esta Dirección Nacional vía mesa de entrada, a más tardar hasta las 13:00 hs. del viernes 27 del corriente, a fin de proseguir con el proceso de evaluación correspondiente.

Atentamente,

C.P. Nathalia Melot
Coordinadora de Adquisiciones

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

Hugo Araujo
Jefe de Redes - DNCP

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

Alba Noelia Ricagno Espinoza

De: Alba Noelia Ricagno Espinoza
Enviado el: jueves, 26 de noviembre de 2015 02:43 p.m.
Para: 'Pablo S. Capo'
Asunto: llamado a Licitación Pública Nacional SBE N° 04/2015 "ADQUISICION DE SOLUCIONES DE SEGURIDAD PARA REDES"
Datos adjuntos: NOTA TEISA 26-11-150000.pdf

En adjunto envío nota.

Favor confirmar recepción del presente.

Atte,

LIC. NOELIA RICAGNO
UOC

DIRECCIÓN NACIONAL DE CONTRATACIONES PÚBLICAS * UOC * Dirección Administrativa

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

Hugo Araujo
Jefe de Redes - DNCP

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

9

Alba Noelia Ricagno Espinoza

De: Pablo S. Capo <pscapo@teisa.com.py>
Enviado el: jueves, 26 de noviembre de 2015 06:14 p.m.
Para: Alba Noelia Ricagno Espinoza
CC: licitaciones@teisa.com.py; Nilda Nathalia Melot Díaz
Asunto: Re: llamado a Licitación Pública Nacional SBE N° 04/2015 "ADQUISICION DE SOLUCIONES DE SEGURIDAD PARA REDES"

Buenas Tardes,

Confirmo recepción.

Saludos Cordiales,

On 11/26/2015 02:43 PM, Alba Noelia Ricagno Espinoza wrote:

En adjunto envío nota.

Favor confirmar recepción del presente.

Atte,

LIC. NOELIA RICAGNO
UOC

Antes de imprimir este mensaje, piense si es necesario hacerlo.
Al reducir el uso de papel se evita la generación de residuos, el consumo de los recursos naturales (madera, agua, energía) y los problemas de contaminación que ocasiona la producción de papel.

--

Pablo Salvador Capo
Ejecutivo de Ventas | Networking | TEISA
Tel: +59521 616 4195 | Cel.: +595 983 103 770
Cecilio Da Silva 1001 | Asunción | Paraguay

TEISA Innovar | Agregar Valor | Ser Confiables

Dirección Nacional de Contrataciones Públicas - Dirección Administrativa - UOC

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

Hugo Araujo
Jefe de Redes - DNCP

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

10

Asunción, 27 de Noviembre de 2015

Señores
DIRECCION NACIONAL DE CONTRATACIONES PÚBLICAS
Ref.: LPN SBE No. 04/2015 – "Adquisición de Soluciones de Seguridad para Redes" – ID No.: 299141

De nuestra mayor consideración:

Por medio de la presente tenemos el agrado de dirigimos a Uds. en respuesta a su Nota de fecha 26/11/2015 donde solicitan informaciones y documentaciones aclaratorias sobre nuestra oferta presentada dentro del marco de la Licitación de Referencia.

A continuación presentamos las respuestas a sus consultas.

1) **Consulta:** Indicar detalladamente cuál es la plataforma a ser provista para utilizar el FAZ-VM-BASE FortiAnalyzer

   Respuesta: Se proveerá un servidor tipo rackeable con las siguientes características:
   - Intel® Xeon® Six-Core: E5-2603v3 (1.6GHz). 15MB Level 3 cache
   - 4Gb RAM DDR4 RDIMM
   - 1TB 6G SATA 7.2k 3.5in SC MDL HDD
   - Tarjeta integrada de cuatro puertos de 1Gb
   - 1 ranura PCI express 3.0
   - 2 Fuentes de poder Hot Plug 800W redundante 1+1.
   - Ventiladores redundantes Hot Plug
   - 3 Años de Garantía

2) **Consulta:** Remitir documentación que acredite que con el FortiAnalyzer FAZ-VM-BASE se llegara a los periodos de retención solicitados en el PBC.

   Respuesta: Adjuntamos documentación del fabricante (FortiAnalyzer-VM.pdf) donde figura la capacidad de GB/día y de almacenamiento del FAZ-VM-BASE.

   Como se puede apreciar, la misma es de 1GB/día con un almacenamiento de 200GB. Esto implica un almacenamiento de 200 días o 6.5 meses.

   Asumiendo un tamaño promedio de 100 bytes por log nos da una capacidad aproximada de 10 millones de logs por día, tomando 300 usuarios generando eventos, esto nos da una capacidad de un poco más 33 mil eventos diarios por usuario.

Aracelii Belén Machuca
Encargada de Mesa de Entrada
DNCP

MESA DE ENTRADA
EXP. 0 0 0 1 3 0 8 5
FECHA 27 NOV 2015
FOJAS 10

Gustavo Egüez
Director Comercial

Abg. Juan Humberto Báez Infante
Asesor Técnico Legal
DNCP

Hugo Araujo
Jefe de Redes - DNCP

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

3) **Consulta:** Remitir documentación que acredite que el equipo ofertado cuenta con:
- Requisitos eléctricos y de funcionamiento
    - Fuentes de poder internas redundantes y hot swap.
    -

Respuesta: Adjuntamos documentación correspondiente al FG-900D (FortiGate-900D.pdf), en donde se puede apreciar que fuente **es redundante y hot-swap**. Esta documentación también puede ser descargada en linea del sitio web de Fortinet: http://www.fortinet.com/sites/default/files/productdatasheets/FortiGate-900D.pdf

Sin otro particular, nos despedimos de Uds. muy atentamente.

Gustavo Egüez
Director Comercial

Gustavo Egüez
Director Comercial

Abg. Juan Humberto Báez Infante
Asesor Jurídico Legal
DNCP

Hugo Araujo
Jefe de Redes - DNCP

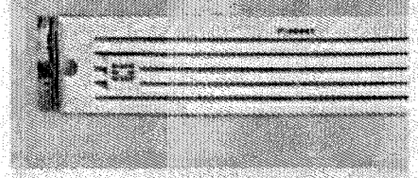
Lic. Noelia Ricagno
Dirección Administrativa
DNCP

12

FORTINET.

DATA SHEET

FortiAnalyzer™
Centralized logging, analytics and reporting



FortiAnalyzer

FortiAnalyzer 200D, 300D, 1000D, 2000B, 3000E, 3500E, 3900E and FAZ-VM

Centralized logging, analytics and reporting

Comprehensive Visualization of Your Network

FortiAnalyzer platforms integrate network logging, analytics, and reporting into a single system, delivering increased knowledge of security events throughout your network. The FortiAnalyzer family minimizes the effort required to monitor and maintain acceptable use policies, as well as identify attack patterns to help you fine tune your policies. Organizations of any size will benefit from centralized security event logging, forensic research, reporting, content archiving, data mining and malicious file quarantining.

You can deploy FortiAnalyzer physical or virtual appliances to collect, correlate, and analyze geographically and chronologically diverse security data. Aggregate alerts and log information from Fortinet appliances and third-party devices in a single location, providing a simplified, consolidated view of your security posture. In addition, FortiAnalyzer platforms provide detailed data capture for forensic purposes to comply with policies regarding privacy and disclosure of information security breaches.

Key Features & Benefits

Graphical Summary Reports	Provides network-wide reporting of events, activities and trends occurring on FortiGate® and third-party devices.
Network Event Correlation	Allows IT administrators to quickly identify and react to network security threats across the network.
Scalable Performance and Capacity	FortiAnalyzer family models support thousands of FortiGate and FortiClient™ agents, and can dynamically scale storage based on retention/compliance requirements.
Choice of Standalone, Collector or Analyzer mode	Can be deployed as an individual unit or optimized for a specific operation (such as store & forward or analytics).
Seamless Integration with the Fortinet Product Portfolio	Tight integration allows FortiAnalyzer resources to be managed from FortiGate or FortiManager™ user interfaces.

Fortinet's Versatile Management Solution

Networks are constantly evolving due to threats, organizational growth or new regulatory/business requirements. Traditional analysis products focus on recording and identifying company-wide threats through logging, analysis and reporting over time.

FortiAnalyzer offers enterprise class features to identify these threats, but also provides flexibility to evolve along with your ever-changing network. FortiAnalyzer can generate highly customized reports for your business requirements while aggregating logs in a hierarchical, tiered logging topology.

Key tenets of Fortinet's management versatility:

- Diversity of form factors
- Architectural flexibility
- Highly customizable
- Simple licensing

FortiCare Worldwide 24x7 Support
support.fortinet.com

FortiGuard Security Services
www.fortiguard.com

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

Hugo Araujo
Jefe de Redes - DNCP

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

3

13

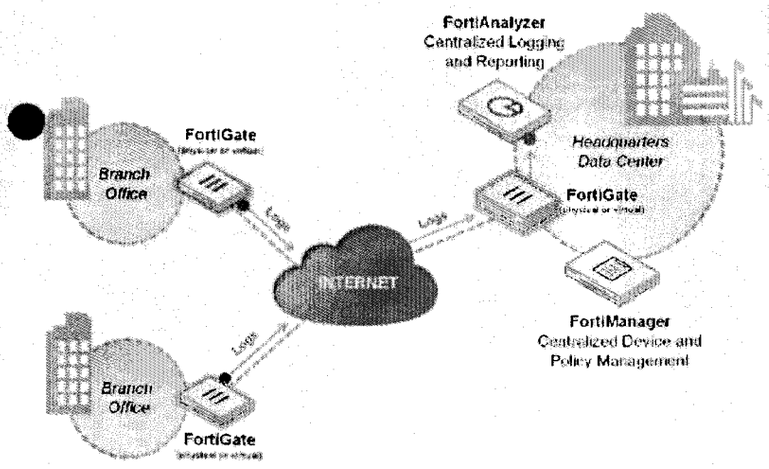
HIGHLIGHTS

Reporting and Visualization Tools

- **FortiView Summary**
  Views Generation ad-hoc graphical, filterable views of top users, applications, destinations, websites, threats, VPN usage and more.
- **Built-in Report Templates**
  Utilize or modify the PDF templates to display colorful, comphrehensive, graphical network security and usage reports.
- **UTM & Traffic Summary Reports**
  Regularly analyze the security profile and traffic/bandwidth patterns with a new consolidated UTM/Traffic report.
- **Event Management**
  Raise and monitor important events to present the IT administrator with unprecedented insight into potentially anomalous behavior.
- **Import/Export Templates**
  After building a report, export and modify the configuration on another FortiAnalyzer or different ADOM.

JSON and XML (Web Services) APIs

- APIs are available on all FortiAnalyzer hardware models and virtual machines
- JSON API — Allows MSSPs/large enterprises to manipulate FortiAnalyzer reports, charts/datasets and objects
- XML API — Enables IT administrators to quickly provision/configure FortiAnalyzer and generate reports
- Access tools, sample code, documentation and interact with the Fortinet developer community by subscribing to the Fortinet Developer Network (FNDN)



Log Viewer

- View logs in real-time or historical
- Select from traffic, event and full security logs
- Browse by device, ADOM or in aggregate
- Log filtering and search capabilities
- Granular inspection with the log details pane
- Intuitive icons for countries, applications, etc.

Event Management

- Comprehensive alert builder
- Trigger off of severity levels, specific events, actions and destinations
- Set varying threshholds by number of events within a certain timeframe
- View or search through historical alerts
- Notify via email/SNMP or raise a syslog event

Better with FortiManager

- Enterprise-class device management
- Familiar GUI for full network control
- Available as integrated solution with FortiAnalyzer

DLP Archiving

- Investigate DLP content archives
- Supported archive types include: email, HTTP, FTP, IM
- View archive text or download files

FortiAnalyzer Supported Devices

- FortiGate Multi-Threat Security Systems
- FortiMail Messaging Security Systems
- FortiClient Endpoint Security Suite
- FortiWeb Web Application Security
- FortiManager Centralized Management
- FortiSandbox Threat Protection
- FortiCache Web Caching
- Any Syslog-Compatible Device

DIRECCIÓN NACIONAL DE CONTRATACIONES PÚBLICAS
Dirección Administrativa
DNCP

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

Hugo Araujo
Jefe de Redes - DNCP

Gustavo Báez
Director Comercial
www.fortinet.com

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

SPECIFICATIONS

	FORTIANALYZER 200D	FORTIANALYZER 300D	FORTIANALYZER 1000D	FORTIANALYZER 2000B
Capacity and Performance				
GB/Day of Logs	5	15	75	200
Sustained Log Rate (Standalone Mode)	120	200	350	1,500
Peak Log Rate (Standalone Mode)*	350	625	1,000	5,000
Devices/VDOMs/ADOMs (Maximum)	150	175	2,000	2,000
Hardware Specifications				
Form Factor	1 RU Rackmount	1 RU Rackmount	2 RU Rackmount	2 RU Rackmount
Total Interfaces	4x GE	4x GE	6x GE, 2x GE SFP	6x GE
Storage Capacity	1 TB (1x 1 TB)	4 TB (2x 2 TB)	8 TB (4x 2 TB)	4 TB (2x 2 TB – 12 TB maximum)
Removable Hard Drives	No	No	Yes	Yes
RAID Levels Supported	None	RAID 0/1	RAID 0/1/5/10	RAID 0/1/5/10/50
Default RAID Level	–	1	10	10
Redundant Hot Swap Power Supplies	No	No	Yes	Yes
Dimensions				
Height x Width x Length (inches)	1.8 x 17.1 x 13.9	1.7 x 17.1 x 14.3	3.5 x 17.2 x 14.5	3.4 x 17.4 x 26.8
Height x Width x Length (cm)	4.5 x 43.3 x 35.2	4.4 x 43.5 x 36.4	9 x 43.8 x 36.2	8.6 x 44.2 x 68.1
Weight	13.4 lbs (6.1 kg)	15.9 lbs (7.2 kg)	30.6 lbs (13.9 kg)	63 lbs (28.6 kg)
Environment				
AC Power Supply	100–240V AC, 50–60 Hz, 6 Amp Max	100–240V AC, 50–60 Hz, 4 Amp Max	100–240V AC, 50–60 Hz, 5 Amp Max	100–240V AC, 50–60 Hz, 9 Amp Max
Power Consumption (Average)	60 W	182 W	133 W	200 W
Heat Dissipation	205 BTU/h	686 BTU/h	546 BTU/h	519 BTU/h
Operating Temperature	32–104°F (0–40°C)	50–95°F (10–35°C)	32–104°F (0–40°C)	50–95°F (10–35°C)
Storage Temperature	-13–158°F (-35–70°C)	-40–158°F (-40–70°C)	-13–158°F (-25–70°C)	-40–149°F (-40–65°C)
Humidity	5–95% non-condensing	5–95% non-condensing	5–95% non-condensing	5–95% non-condensing
Operating Altitude	Up to 7,400 ft (2,250 m)	Up to 7,400 ft (2,250 m)	Up to 7,400 ft (2,250 m)	Up to 7,400 ft (2,250 m)
Compliance				
Safety Certifications	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, C-Tick, VCCI, CE, BSMI, UL/cUL, CB	FCC Part 15 Class A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST

	FORTIANALYZER 800B	FORTIANALYZER 3500E	FORTIANALYZER 3900E
Capacity and Performance			
GB/Day of Logs	800	3,000	4,000
Sustained Log Rate (Standalone Mode)	15,000	36,000	48,000
Peak Log Rate (Standalone Mode)*	50,000	60,000	75,000
Devices/VDOMs/ADOMs (Maximum)	4,000	4,000	4,000
Hardware Specifications			
Form Factor	2 RU Rackmount	4 RU Rackmount	2 RU Rackmount
Total Interfaces	4x GE, 2x GE SFP	2x GE, 2x GE SFP	2x GE, 2x GE SFP+
Storage Capacity	16 TB (8x 2 TB)	24 TB (12x 2 TB – 48 TB maximum)	15 TB SSD (15x 1 TB SSD)
Removable Hard Drives	Yes	Yes	Yes
RAID Storage Management	RAID 0/1/5/6/10/50/60	RAID 0/1/5/6/10/50/60	RAID 0/1/5/6/10/50/60
Default RAID Level	10	10	10
Redundant Hot Swap Power Supplies	Yes	Yes	Yes
Dimensions			
Height x Width x Length (inches)	3.4 x 18 x 29.7	6.9 x 19.1 x 27.2	3.5 x 17.2 x 26.9
Height x Width x Length (cm)	8.7 x 46.2 x 75.5	17.5 x 48.5 x 69.0	8.9 x 43.7 x 68.4
Weight	71.5 lbs (32.5 kg)	77 lbs (34.9 kg)	52 lbs (23.6 kg)
Environment			
AC Power Supply	100–240V AC, 50–60 Hz, 10 Amp Maximum	100–240V AC, 50–60 Hz, 11.5 Amp Maximum	100–240V AC, 50–60 Hz, 11.5 Amp Maximum
Power Consumption (Average)	375.6 W	465 W for 12 HDD	470 W for 15 HDD
Heat Dissipation	1947 BTU/h	1904 BTU/h	1637 BTU/h
Operating Temperature	50–95°F (10–35°C)	32–104°F (0–40°C)	50–95°F (10–35°C)
Storage Temperature	-40–149°F (-40–65°C)	-13–158°F (-25–70°C)	-40–60°C (-40–140°F)
Humidity	20–90% non-condensing	10–90% non-condensing	5–95% (non-condensing)
Operating Altitude	Up to 7,400 ft (2,250 m)	Up to 7,400 ft (2,250 m)	Up to 7,400 ft (2,250 m)
Compliance			
Safety Certifications	FCC Part 15 Class A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB (GOST)	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB

* Peak rate can hold for up to 30 minutes

DIRECCIÓN NACIONAL DE CONTRATACIONES PÚBLICAS
Dirección Administrativa
DNCP

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

Hugo Araujo
Jefe de Redes - DNCP

Gustavo Báez
Director Comercial

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

5

15

SPECIFICATIONS

	FAZ-VM-BASE	FAZ-VM-GB1	FAZ-VM-GB5	FAZ-VM-GB25	FAZ-VM-GB100
Capacity and Performance					
GB/Day of Logs	1 (unl.)**	+1	+5	+25	+100
Storage Capacity	200 GB	+200 GB	+1 TB	+8 TB	+16 TB
Devices/ADOMs/VDOMs Supported (Maximum)	10,000	10,000	10,000	10,000	10,000
Hypervisor Support	VMware ESX/ESXi 4.0/4.1/5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS)				
Network Interface Support (Minimum / Maximum)	1 / 4				
vCPUs (Minimum / Maximum)	1 / Unlimited				
Memory Support (Minimum / Maximum)	1 GB / Unlimited				

** Unlimited GB/Day when deployed in collector mode

ORDER INFORMATION

Product	SKU	Description
FortiAnalyzer 200D	FAZ-200D	Centralized log and analysis appliance — 4x GE RJ45, 1 TB storage, up to 5 GB/Day of logs.
FortiAnalyzer 300D	FAZ-300D	Centralized log and analysis appliance — 4x GE RJ45, 4 TB storage, up to 15 GB/Day of logs.
FortiAnalyzer 1000D	FAZ-1000D	Centralized log and analysis appliance — 6x GE RJ45, 2x SFP slots, 8 TB storage, up to 75 GB/Day of Logs.
FortiAnalyzer 2000B	FAZ-2000B-BO3S	Centralized log and analysis appliance — 6x GE RJ45, 12 TB storage, dual power supplies, up to 200 GB/Day of Logs.
FortiAnalyzer 3000E	FAZ-3000E	Centralized log and analysis appliance — 4x GE RJ45, 2x GE SFP slots, 16 TB storage, dual power supplies, up to 800 GB/Day of Logs.
FortiAnalyzer 3500E	FAZ-3500E-E02S	Centralized log and analysis appliance — 2x GE RJ45, 2x GE SFP slots, 48 TB storage, dual power supplies, up to 3,000 GB/Day of Logs.
FortiAnalyzer 3900E	FAZ-3900E	Centralized log and analysis appliance — 2x GE RJ45, 2x 10 GE SFP+ slots, flash-based 15 TB SSD storage, dual power supplies, up to 4,000 GB/Day of Logs.
FortiAnalyzer VM Base	FAZ-VM-Base	Base license for stackable FortiAnalyzer-VM; 1 GB/Day of Logs and 200 GB storage capacity. Unlimited GB/Day when used in collector mode only. Designed for AWS, VMware vSphere, Xen, KVM and Hyper-V platforms.
FortiAnalyzer VM GB1	FAZ-VM-GB1	Upgrade license for adding 1 GB/Day of Logs and 200 GB storage capacity.
FortiAnalyzer VM GB5	FAZ-VM-GB5	Upgrade license for adding 5 GB/Day of Logs and 1 TB storage capacity.
FortiAnalyzer VM GB25	FAZ-VM-GB25	Upgrade license for adding 25 GB/Day of Logs and 8 TB storage capacity.
FortiAnalyzer VM GB100	FAZ-VM-GB100	Upgrade license for adding 100 GB/Day of Logs and 16 TB storage capacity.

FORTINET.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480

Copyright © 2016 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary and may be significantly less effective than the metrics stated herein. Network variables, different network environments and other conditions may negatively affect performance results and other metrics stated herein. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet and any such commitment shall be limited by the disclaimers in this paragraph and other limitations in the written contract. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests, and in no event will Fortinet be responsible for events or issues that are outside of its reasonable control. Notwithstanding anything to the contrary, Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

FAZ-DATASH-20160

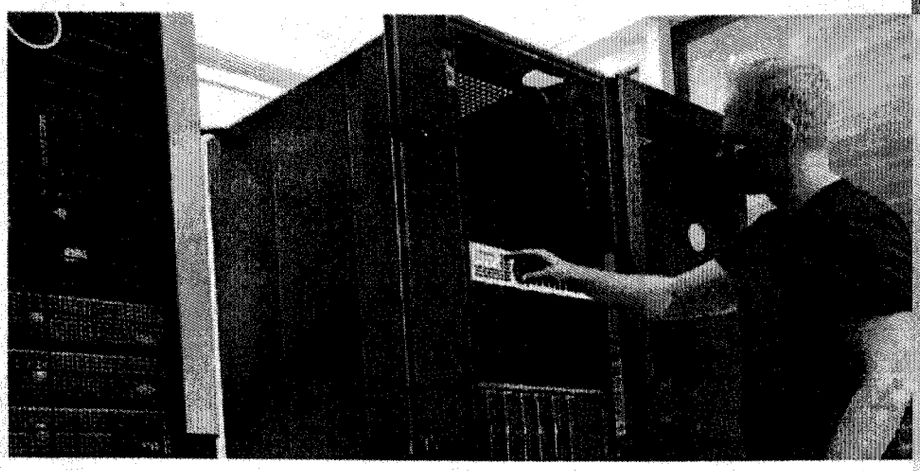
Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

Hugo Araujo
Jefe de Redes - DNCP

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

FORTINET.

DATA SHEET



FortiGate® 900D
High Performance Enterprise Firewall for Large Branch Offices

FortiGate 900D

With network bandwidth requirements doubling every 18 months and increases in sophisticated cyber threats, enterprise organizations with large branch offices know they need high-speed network security that also delivers highly effective next generation security.

5 Times Next Generation Firewall Performance

The FortiGate 900D appliance delivers superior performance through a combination of purpose-built FortiASIC™ processors, high port density with 10 GE ports and consolidated security features from the FortiOS™ operating system. It delivers 5 times better next generation firewall performance compared to alternate products and provides the best price/performance in the industry.

Deeper Visibility and Top-rated Security

This breakthrough threat prevention performance allows organizations to run NSS Labs Recommended intrusion prevention and application control and VB100 certified antimalware capabilities for deeper inspection. Rich console views and reports together with a flexible policy engine provide the visibility and control to empower employees yet secure your enterprise.

Finally, these features of the FortiGate FortiOS Network Security Platform are routinely validated by independent real-world tests and are consistently getting superior ratings in security effectiveness.

Highlights

Firewall Performance	IPS Performance	Interfaces
52 Gbps	8 Gbps	Multiple 10 GE SFP+, GE SFP and GE RJ45

Features & Benefits

- 5 times faster hardware accelerated next generation firewall offers best-in-class price/performance ratio
- Integrated high port density delivers maximum flexibility and scalability
- NSS Labs Recommended NGFW and NGIPS with consolidated security delivers top-rated protection
- Application control plus identity and device-based policy enforcement provides more granular protection
- Intuitive management interface enables broad and deep visibility that scales from a single FortiGate to thousands

FortiCare Worldwide 24x7 Support
support.fortinet.com

FortiGuard Security Services
www.fortiguard.com

Ing. Humberto Báez Infante
Asesor Técnico - Legal
DNCP

Hugo Araujo
Jefe de Redes - DNCP

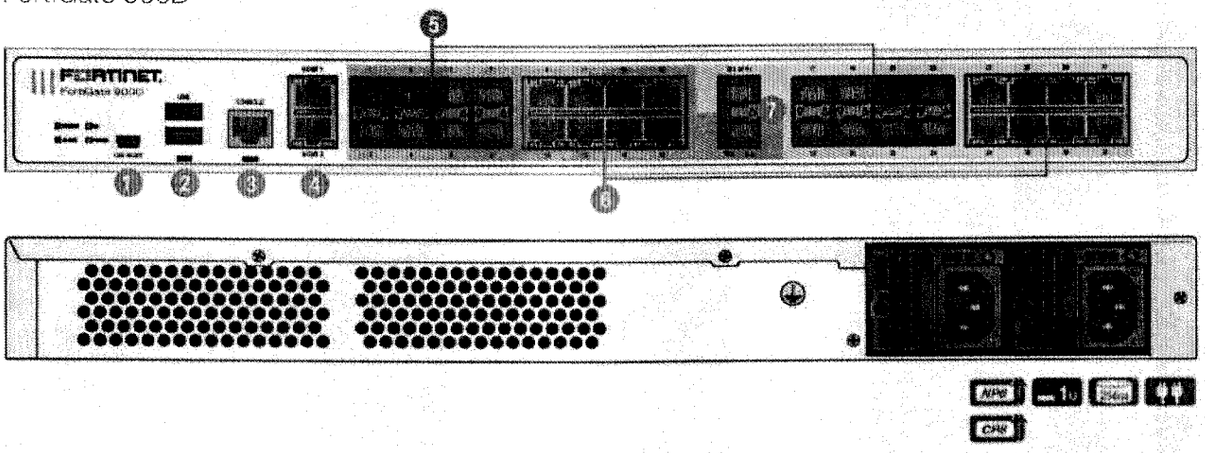
Lic. Noelia Ricagno
Dirección Administrativa
DNCP

7

17

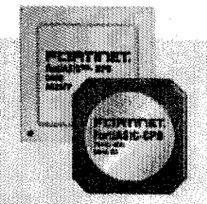
HARDWARE

FortiGate 900D



Interfaces

1. USB Management Port
2. USB Ports
3. Console Port
4. 2x GE RJ45 Management Ports
5. 16x GE SFP Slots
6. 16x GE RJ45 Ports
7. 2x 10 GE SFP+ Slots



Powered by FortiASICs

- Custom FortiASIC™ processors deliver the power you need to detect malicious content at multi-Gigabit speeds
- Other security technologies cannot protect against today's wide range of content and connection-based threats because they rely on general-purpose CPUs, causing a dangerous performance gap
- FortiASIC processors provide the performance needed to block emerging threats, meet rigorous third-party certifications, and ensure that your network security solution does not become a network bottleneck

Network Processor

Fortinet's new, breakthrough FortiASIC NP6 network processor works inline with FortiOS functions delivering:

- Superior firewall performance for IPv4/IPv6, SCTP and multicast traffic with ultra-low latency down to 3 microseconds
- VPN, CAPWAP and IP tunnel acceleration
- Anomaly-based intrusion prevention, checksum offload and packet defragmentation
- Traffic shaping and priority queuing

Content Processor

The FortiASIC CP8 content processor works outside of the direct flow of traffic, providing high-speed cryptography and content inspection services including:

- Signature-based content inspection acceleration
- Encryption and decryption offloading

10 GE Connectivity

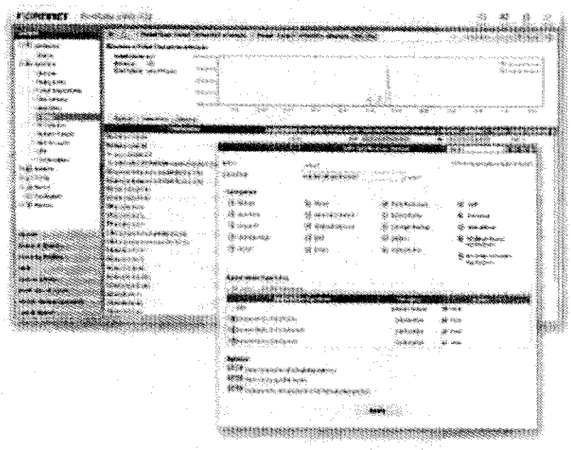
High speed connectivity is essential for network security segmentation. The FortiGate 900D provides 10 GE slots that simplify network designs without relying on additional devices to bridge desired connectivity.

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

Hugo Araujo
Jefe de Redes - DNCP

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

SOFTWARE



FortiOS Managment UI — FortiView and Application Control Panel

FortiOS

FortiOS helps you protect your organization against advanced threats, configure and deploy your network security faster and see deep into what's happening inside your network. It enables organization to set up policies specific to types of devices, users and applications with industry-leading security capabilities. FortiOS leverages custom FortiASICs and the Optimum Path Processing architecture of FortiGate to deliver 5 times faster throughput performance. In essence, FortiOS delivers:

- **Comprehensive Security** — Control thousands of applications and stop more threats with NSS Labs Recommended IPS, sandboxing, VB100 certified antimalware and more.
- **Superior Control and Visibility** — Stay in control with rich visibility over network traffic, granular policy control, and intuitive, scalable security and network management.
- **Robust Networking Capabilities** — Optimize your network with extensive switching and routing, high availability, WAN optimization, embedded WiFi controller, and a range of virtual options.

For more information, please refer to the FortiOS data sheet available at www.fortinet.com

SERVICES

FortiGuard™ Security Services

FortiGuard Labs offers real-time intelligence on the threat landscape, delivering comprehensive security updates across the full range of Fortinet's solutions. Comprised of security threat researchers, engineers, and forensic specialists, the team collaborates with the world's leading threat monitoring organizations, other network and security vendors, as well as law enforcement agencies:

- **Real-time Updates** — 24x7x365 Global Operations research security intelligence, distributed via Fortinet Distributed Network to all Fortinet platforms.
- **Security Research** — FortiGuard Labs have discovered over 170 unique zero-day vulnerabilities to date, totaling millions of automated signature updates monthly.
- **Validated Security Intelligence** — Based on FortiGuard intelligence, Fortinet's network security platform is tested and validated by the world's leading third-party testing labs and customers globally.

For more information, please refer to http://forti.net/guard

FortiCare™ Support Services

Our FortiCare customer support team provides global technical support for all Fortinet products. With support staff in the Americas, Europe, Middle East and Asia, FortiCare offers services to meet the needs of enterprises of all sizes:

- **Enhanced Support** — For customers who need support during local business hours only.
- **Comprehensive Support** — For customers who need around-the-clock mission critical support, including advanced exchange hardware replacement.
- **Premium Services** — For global or regional customers who need an assigned Technical Account Manager, enhanced service level agreements, extended software support, priority escalation, on-site visits and more.
- **Professional Services** — For customers with more complex security implementations that require architecture and design services, implementation and deployment services, operational services and more.

For more information, please refer to http://forti.net/care

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

Hugo Araujo
DNCP

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

SPECIFICATIONS

	FORTIGATE 900D
Interfaces and Modules	
Hardware Accelerated 10 GE SFP+ Slots	2
Hardware Accelerated GE SFP Slots	16
Hardware Accelerated GE RJ45 Ports	16
GE RJ45 Management / HA Ports	2
USB Ports (Client / Server)	1 / 2
Console Port	1
Onboard Storage	256 GB
Included Transceivers	0
System Performance and Capacity	
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	52 / 52 / 33 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	52 / 52 / 33 Gbps
Firewall Latency (64 byte, UDP)	3 µs
Firewall Throughput (Packet per Second)	49.5 Mpps
Concurrent Sessions (TCP)	11 Million
New Sessions/Second (TCP)	280,000
Firewall Policies	100,000
IPsec VPN Throughput (512 byte)	25 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	2,000
Client-to-Gateway IPsec VPN Tunnels	10,000
SSL-VPN Throughput	3.6 Gbps
Concurrent SSL-VPN Users (Recommended Maximum)	10,000
IPS Throughput	8 Gbps
Antivirus Throughput	3.5 Gbps
CAPWAP Clear-text Throughput (HTTP)	8 Gbps
Virtual Domains (Default / Maximum)	10 / 10
Maximum Number of FortiAPs (Total / Tunnel)	1024 / 512
Maximum Number of FortiTokens	1,000
Maximum Number of Registered Endpoints	2,000
High Availability Configurations	Active-Active, Active-Passive, Clustering

	FORTIGATE 900D
Dimensions and Power	
Height x Width x Length (inches)	1.74 x 17.22 x 18.24
Height x Width x Length (mm)	44.2 x 437.5 x 463.2
Weight	20.24 lbs (9.18 kg)
Form Factor	1 RU
AC Power Supply	100–240V AC, 60–50 Hz, 300 W Redundant
Power Consumption (Average / Maximum)	135 W / 187.2 W
Current (Maximum)	100V/5A, 240V/3A
Heat Dissipation	638.75 BTU/h
Redundant Power Supplies	Yes (Hot Swappable)
Operating Environment and Certifications	
Operating Temperature	32–104°F (0–40°C)
Storage Temperature	-31–158°F (-35–70°C)
Humidity	20–90% non-condensing
Operating Altitude	Up to 7,400 ft (2,250 m)
Compliance	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN

Note: All performance values are "up to" and vary depending on system configuration. Antivirus performance is measured using 44 Kbyte HTTP files in proxy mode. IPS performance is measured using 1 Mbyte HTTP files. IPsec VPN performance is based on 512 byte UDP packets using AES-256+SHA1. LAG support and redundant interfaces are limited to certain port configurations, please refer to technical documentation.

For complete, up-to-date and detailed feature set, please refer to the Administration Handbook and FortiOS Datasheet.

ORDER INFORMATION

Product	SKU	Description
FortiGate 900D	FG-900D	2x 10 GE SFP+ slots, 16x GE SFP slots, 16x GE RJ45 ports, 2x GE RJ45 Management ports, FortiASIC NP6 and CP8 hardware accelerated, 1x 256 GB SSD onboard storage, dual AC power supplies

Optional Accessories/Spares	SKU	Description
1 GE SFP LX Transceiver Module	FG-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots
1 GE SFP RJ45 Transceiver Module	FG-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots
1 GE SFP SX Transceiver Module	FG-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots
10 GE SFP+ Transceiver Module, Short Range	FG-TRAN-SFP+SR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots
10 GE SFP+ Transceiver Module, Long Range	FG-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots
10 GE SFP+ Active Direct Attach Cable, 10m / 32.8 ft	SP-CABLE-ADASFP+	10 GE SFP+ active direct attach cable 10m / 32.8 ft for all systems with SFP+ and SFP/SFP+ slots
AC Power Supply	SP-FXX1000D	AC power supply for FG-900D, FG-1000D and FXX-1000D

FORTINET

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480

Copyright© 2015 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary and may be significantly less effective than the metrics stated herein. Network variables, different network environments and other conditions may negatively affect performance results and other metrics stated herein. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet and any such commitment shall be limited by the disclaimers in this paragraph and other limitations in the written contract. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests, and in no event will Fortinet be responsible for events or issues that are outside of its reasonable control. Notwithstanding anything to the contrary, Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of publication shall be applicable.

SP PROD-DS-G

FG-900D-DAT-R6-(2015)

Gustavo Báez
Director Comercial

10

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

Hugo Araujo
Jefe de Redes - DNCP

Lic. Noelia Rivaldo
Dirección Administrativa
DNCP

20