INFORME DE EVALUACIÓN DE OFERTAS Nº 16/2016

CONTRATACIÓN DIRECTA Nº 18/2016

"ADQUISICIÓN DE UN EQUIPO DE SEGURIDAD DE RED INFORMÁTICA"

En la Dirección General de Administración y Finanzas de la Secretaria de Prevención de Lavado de Dinero o Bienes (SEPRELAD), sito en la Avenida Federación Rusa y Augusto Roa Bastos, Edificio del Banco Central del Paraguay, sector Cultural, a los siete días del mes de diciembre del año dos mil dieciséis, siendo las 09:00 horas, dando cumplimiento a lo establecido en el Art. 26 y 27 de la Ley 2051/03 "De Contrataciones Públicas" se reúne el Comité de Evaluación de Ofertas de la SEPRELAD, formado según Resolución N° 263 del 22 de junio de 2016, integrado por los siguientes funcionarios: Carlos Humberto Zarza, Director General Interino de la Dirección General de Administración y Finanzas; Raquel Cuevas Arzamendia, Directora General de la Dirección General de Análisis Financiero y Hernán Quiñónez, Jefe del Departamento de Presupuesto, a fin de proceder a la evaluación de las ofertas y documentaciones presentadas para la Contratación Directa Nº 18/2016 "Adquisición de Un Equipo de Seguridad de Red Informática", que será imputado en el Rubro 540 "Adquisiciones de Equipos de Oficina y Computación" del ejercicio Presupuestario año 2016, asignado a la SEPRELAD.

Las evaluaciones se realizan de acuerdo a los siguientes documentos:

ANTECEDENTES:

1. Memorando TI N° 40/2016, del 07 de junio de 2016, por el cual la Dirección de Informática y Tecnología solicita sea considerada la compra de un equipo de seguridad de red informática (Proxi / Firewall).
2. Memorando DGAF N° 209/2016, del 23 de agosto de 2016, por el cual la Dirección General de Administración y Finanzas solicita al Departamento de Presupuesto gestionar una transferencia de crédito presupuestaria para procesar lo solicitado, entre otros.
3. Memorando del Departamento de Presupuesto, de fecha 24 de agosto de 2016, por el cual se remiten los formularios pertinentes para la transferencia de crédito presupuestaria solicitada.
4. Resolución de la Secretaría Ejecutiva N° 387/2016, del 24 de agosto de 2016, por la cual se autoriza la transferencia de crédito y la modificación de las cuotas de ingreso y gastos del Plan Financiero, aprobado por Decreto N° 4931 de fecha 18 de febrero de 2016.
5. Memorando DGAF/UOC N° 164/2016, del 16 de septiembre de 2016, por el cual se solicita la modificación del Programa Anual de Contrataciones, creando el proceso con id 317.428, denominado "Adquisición de un Equipo de seguridad de Red Informático", en la modalidad de Contratación Directa, por un monto total a contratar de guaraníes treinta y cuatro millones trescientos mil (Gs. 34.300.000).
6. Resolución de la Secretaría Ejecutiva N° 422/2016, del 19 de septiembre de 2016, por la cual se autoriza la modificación del Programa Anual de Contrataciones (PAC) del Ejercicio Fiscal 2016.
7. Memorando DGAF/UOC N° 181/2016, del 26 de septiembre de 2016, por el cual la Unidad Operativa de Contratación (UOC) solicita la autorización para el inicio de trámites para la Contratación Directa Nº 18/2016 "Adquisición de un Equipo de seguridad de Red Informática".
8. Resolución de la Secretaría Ejecutiva de la SEPRELAD Nº 446/2016, del 27 de septiembre de 2016, por la cual se autoriza el inicio de trámites para la Contratación Directa Nº 18/2016 "Adquisición de un Equipo de seguridad de Red Informática".

000501

9. Memorando DGAF N° 259/2016, del 04 de octubre de 2016, por el cual la Dirección General de Administración y Finanzas solicita a la Dirección de Informática Tecnología la elaboración de las especificaciones técnicas para la adquisición de un equipo de seguridad de Red Informática.

10. Memorando DIT N° 60/2016, del 07 de octubre de 2016, por el cual la Dirección de Informática y Tecnología remite las especificaciones técnicas solicitadas.

11. Certificado de Disponibilidad Presupuestaria N° 1736/2016, correspondiente al PAC N° 317.428, emitido el 07 de octubre de 2016, por un monto de guaraníes treinta y cuatro millones trescientos mil (Gs. 34.300.000).

12. Nota SEPRELAD/DGAF N° 213/2016, del 13 de octubre de 2016, por la cual se comunica a la Dirección Nacional de Contrataciones Públicas (DNCP), el inicio del llamado a Contratación Directa N° 18/2016 "Adquisición de un Equipo de Seguridad de Red Informática".

13. Fueron invitadas a participar del mencionado procedimiento las siguientes empresas:
    - COMPUSAVER S.A
    - OLAM S.R.L
    - PARASOFT S.R.L
    - CACERES ACOSTA Y ASOCIADOS S.A
    - DATA LAB S.A.

14. Nota DNCP/DNC N° 30.230/2016, del 18 de octubre de 2016 por la cual la Dirección Nacional de Contrataciones Públicas (DNCP), informa que luego de la verificación del Pliego de Bases y Condiciones y los demás documentos remitidos han surgido observaciones y se ha procedido a la difusión a través del Sistema de Información de Contrataciones Públicas (SIPC).

15. Memorando DGAF/UOC N° 196/2016, del 19 de octubre de 2016, por el cual la Unidad Operativa de Contratación (UOC) solicita a la Dirección de Informática Tecnología las aclaraciones referentes al punto 2 de la Nota DNCP/DNC N° 30.230/2016.

16. Memorando DIT N° 62/2016, del 19 de octubre de 2016, por el cual la Dirección de Informática y Tecnología remite las aclaraciones solicitadas.

17. Fue emitida la Adenda N° 1, que forma parte de la Carta de Invitación y sus Anexos y fue difundida en el SICP, correspondiente a la modificación del punto 20 inciso D, Capacidad Técnica, del Anexo B, Datos de la Contratación.

18. Nota SEPRELAD/DGAF N° 215/2016, del 19 de octubre de 2016, por la cual se remite las aclaraciones a las observaciones realizadas por Nota DNCP/DNC/N° 30.230/2016, del 18 de octubre de 2016.

19. Acta de Apertura de Oferta N° 24/2016, del 25/10/2016 en el cual se hace mención que no contando con la cantidad mínima de ofertas para la apertura, conforme lo establecido en la Ley 2015/03; se procederá a la prórroga de la fecha de apertura, según el procedimiento establecido en la Resolución N° 805 de fecha 22/05/2016 y N° 522 de fecha 24/02/2015, emitidas por la Dirección Nacional de Contrataciones Públicas (DNCP).

20. Fue emitida la Adenda N° 2, que forma parte de la Carta de Invitación y sus Anexos y fue difundida en el SICP, correspondiente a la prórroga de la fecha de entrega de apertura de ofertas.

21. Nota SEPRELAD/DGAF N° 221/2016, del 25 de octubre de 2016, por la cual se comunica a la empresa OLAM S.R.L que la apertura programada para el día martes 25 de octubre de 2016, no fue realizada por no contar con la cantidad mínima de ofertas para la apertura, conforme lo establecido en la Ley 2051/03 y se procederá a la prórroga de la fecha de apertura, según el procedimiento establecido en la Resolución N° 805 de fecha 22/05/2016 y N° 522 de fecha 24/02/2015, emitidas por la Dirección Nacional de Contrataciones Públicas (DNCP).

000500

22. Recibo de entrega de oferta cerrada a la empresa OLAM S.R.L., de fecha 01 de noviembre de 2016.
23. Acta de Apertura de Oferta N° 26/2016, del 01/11/2016 en el cual se hace mención que no contando con oferta alguna para la apertura; se procederá a la prórroga de la fecha de apertura, según el procedimiento establecido en la Resolución N° 805 de fecha 22/05/2016 y N° 522 de fecha 24/02/2015, emitidas por la Dirección Nacional de Contrataciones Públicas (DNCP).
24. Fue emitida la Adenda N° 3, que forma parte de la Carta de Invitación y sus Anexos y fue difundida en el SICP, correspondiente a la prórroga de la fecha de entrega de apertura de ofertas
25. Memorando DIT N° 64/2016, del 02 de noviembre de 2016, por el cual la Dirección de Informática y Tecnología solicita la modificación a las especificaciones técnicas en lo referente a la vigencia de actualización de los softwares del equipo.
26. Fue emitida la Adenda N° 4, que forma parte de la Carta de Invitación y sus Anexos y fue difundida en el SICP, correspondiente a la modificación de las Especificaciones Técnicas, en lo referente a la vigencia de actualización de los softwares del equipo.
27. De acuerdo al procedimiento previsto por el Artículo 54 del Decreto Reglamentario N° 21.909/03 y concordantes; se ha llevado a cabo el acto de apertura de sobres y verificación de las ofertas, conforme con lo expresado en el Acta de Apertura N° 29/2016, del 10 de noviembre de 2016, cuyos oferentes y precios totales son los siguientes:

Orden	Empresas	Precios Totales en Guaraníes
1	TEISA	**32.034.600**
2	PYTYVO TELECOMUNICACIONES S.A.	**34.000.000**
3	OLAM S.R.L.	**34.200.000**

ANÁLISIS, ESTUDIO Y EVALUACIÓN DE LAS OFERTAS

A fin de determinar el cumplimiento de los requisitos establecidos en la Carta de Invitación, basados en los procedimientos y criterios establecidos en la Ley N° 2051/03, el Decreto N° 21.909/03 y en las Bases de la Contratación (Carta de Invitación y sus anexos), con el sistema: CUMPLE – NO CUMPLE; en los siguientes criterios:

1. DOCUMENTACIÓN DE CARÁCTER SUSTANCIAL

Se procedió a la verificación de las documentaciones básicas de carácter sustancial presentada:

DOCUMENTOS	TEISA	PYTYVO TELECOM. S.A.	OLAM S.R.L.
Formulario de Presentación de Oferta y Planilla de Precios, debidamente completado y firmado.	CUMPLE	CUMPLE	CUMPLE
Garantía de Mantenimiento de Oferta, debidamente emitida y firmada	CUMPLE	CUMPLE	CUMPLE
Declaración Jurada de no hallarse comprendido en las prohibiciones o limitaciones para contratar establecidas en el artículo 40 y de integridad conforme al artículo 20, inc. "w", ambos de la Ley N° 2051/03, de acuerdo con lo dispuesto en la Resolución N° 330/07 de la Dirección General de Contrataciones Públicas	CUMPLE	CUMPLE	CUMPLE SIPE 1427321

Fotocopia simple de la cedula de identidad del firmante de la oferta	CUMPLE	CUMPLE	CUMPLE SIPE 1427321
Fotocopia simple de los documentos que acrediten la existencia legal de la persona jurídica tales como la Escritura Pública de Constitución y protocolización de los Estatutos Sociales. Los estatutos deberán estar inscriptos en la Sección Personas Jurídicas de la Dirección de Registros Públicos.	CUMPLE SIPE 1427440	CUMPLE	CUMPLE SIPE 1427321
Fotocopia autenticada de los documentos que acrediten la capacidad del firmante, cuando corresponda (poder o documentos estatutarios como acta de asamblea o de directorio)	CUMPLE	CUMPLE|	CUMPLE SIPE 1427321

2. DOCUMENTACIÓN DE CARÁCTER FORMAL

Se procedió a la verificación de las documentaciones de carácter formal presentado por los oferentes y en la misma se ha constatado que algunas empresas no adjuntaron documentaciones y/o se encuentran vencidas en el SIPE, las cuales le son requeridas, conforme al *"Artículo 59. Disconformidades, errores y omisiones"* del Decreto N° 21.909/03, según el siguiente detalle:

- A la empresa TEISA; por nota SEPRELAD/DGAF N° 253/2016, de fecha 11/11/2016, las siguientes documentaciones:
  1) Currículo del o los Técnicos certificados en la marca cotizada.
- A la empresa PYTYVO COMUNICACIONES S.A.; por nota SEPRELAD/DGAF N° 254/2016, de fecha 11/11/2016, las siguientes documentaciones:
  1) Currículo del o los Técnicos certificados en la marca cotizada.
  2) Copias de carta de referencia de clientes y/o contratos y/o comprobantes legales de ventas y/o acta de recepción definitiva ejecutada durante los años (2013 y 2014), deberá presentar por lo menos uno (1) por año.
- A la empresa OLAM S.R.L.; por nota SEPRELAD/DGAF N° 255/2016, de fecha 11/11/2016, las siguientes documentaciones:
  1) Currículo del o los Técnicos certificados en la marca cotizada, acompañado de sus certificados respectivos.
  2) Copias de carta de referencia de clientes y/o contratos y/o comprobantes legales de ventas y/o acta de recepción definitiva ejecutada durante los tres últimos años (2013, 2014 y 2015), deberá presentar por lo menos uno (1) por año.
  3) Folletos, catálogos e impresos descriptivos del equipo ofertado.

Las empresas han cumplido en tiempo y forma lo requerido. Las notas de solicitud y respuestas forman parte de este informe.

DOCUMENTOS	TEISA	PYTYVO TELECOM. S.A.	OLAM S.R.L.
Declaración Jurada por la que el Oferente garantiza que no se encuentra involucrado en prácticas que violen los Derechos de los niños, niñas y adolescentes referentes al trabajo infantil.	CUMPLE	CUMPLE	CUMPLE SIPE 1427321
Fotocopia simple de la cédula tributaria (RUC)	CUMPLE SIPE 1427440	CUMPLE	CUMPLE SIPE 1427321
Constancia de Inscripción en el registro único de contribuyentes - RUC	CUMPLE SIPE 1427440	CUMPLE SIPE 1427310	CUMPLE SIPE 1427321
Fotocopia simple del Certificado de Cumplimiento Tributario vigente.	CUMPLE	CUMPLE	CUMPLE SIPE 1427321
Fotocopia simple de la patente Municipal del Oferente	CUMPLE	CUMPLE	CUMPLE SIPE 1427321

000458

Se procedió a la verificación de la presentación de las documentaciones adicionales, conforme lo solicitado el Anexo E punto V. Otros Documentos de la Carta de Invitación:

DOCUMENTOS	TEISA	PYTYVO TELECOM. S.A.	OLAM S.R.L.
Copia simple del Certificado de Origen Nacional, emitido por la Dirección General de Desarrollo Empresarial del Ministerio de Industria y Comercio (Decreto N° 9649/2012), la no presentación de este documento no es causal de descalificación de la oferta.	NO APLICA	NO APLICA	NO APLICA
Copias de carta de referencia de clientes y/o contratos y/o comprobantes legales de ventas y/o acta de recepción definitiva ejecutada durante los tres últimos años (2013, 2014 y 2015), deberá presentar por lo menos uno (1) por año.	CUMPLE	CUMPLE	CUMPLE
Currículo del o los técnicos certificados en la marca cotizada, acompañados de sus certificados respectivos	CUMPLE	CUMPLE	CUMPLE
Folletos, catálogos e impresos descriptivos del equipo ofertado	CUMPLE	CUMPLE	CUMPLE

3. VERIFICACIÓN ARITMÉTICA DE LAS OFERTAS

Se procedió a la verificación del resultado de los precios unitarios por la cantidad solicitada, de cada una de las ofertas. La propuesta de la firma TEISA fue corregida, en la columna Precio Unitario expresa un monto diferente al Precio Total; las demás ofertas no presentan diferencias con sus propuestas. El detalle se expresa en el Anexo A, que forma parte de este informe. Los precios totales de las ofertas verificadas, en orden de menor a mayor son las siguientes:

Orden	Empresas	Monto Total en Guaraníes
1	PYTYVO TELECOMUNICACIONES S.A.	**34.000.000**
2	TEISA	**34.034.600**
3	OLAM S.R.L.	**34.200.000**

4. ANÁLISIS DE LOS PRECIOS OFERTADOS

Tras la verificación del precio ofertado por las empresas **PYTYVO TELECOMUNICACIONES S.A.; TEISA y OLAM S.R.L.** se ha constatado que no se encuentran situados por debajo del treinta por ciento (30%) y por encima del veinte por ciento (20%) de la estimación del costo difundida con el proceso de contratación.

5. VERIFICACIÓN DE LA CAPACIDAD LEGAL DE LAS EMPRESAS

Se procedió a la verificación de los requisitos en cuanto a la capacidad legal solicitada en el Anexo B – Datos de la Contratación ((DDLC), punto 20 a), de las empresas ofertantes:

5.1. La Declaración Jurada de no hallarse comprendido en las prohibiciones y limitaciones establecidas en el artículo 40 de la Ley 2051/03, se encuentra debidamente emitida y firmada:

TEISA	PYTYVO TELECOM. S.A.	OLAM S.R.L.
CUMPLE	CUMPLE	CUMPLE

5.2. Fueron verificados los registros del personal de la convocante que tienen participación en el proceso de contratación con relación a los socios y representantes legales de las empresas: no fueron detectados supuestos comprendidos en el inciso a) del artículo 40 de la Ley 2051/03, según Memorando DGAF/DPTO. DE ADMINISTRACIÓN DEL

000497

PERSONAL N° 197/2016 del Departamento de Administración del Personal, del 14/11/2016.

5.3. Fueron verificados los socios y representantes legales de las empresas, los mismos no se encuentran registrados como funcionarios públicos en la base de datos del Sistema Integrado de Administración de Recursos Humanos (SINARH), según Memorando DGAF/DPTO. DE ADMINISTRACIÓN DEL PERSONAL N° 197/2016 del Departamento de Administración del Personal, del 14/11/2016.

6. Conforme a lo establecido en el artículo 61 del Decreto N° 3719/15, que modifica parcialmente el Decreto Reglamentario Nº 21.909/03, inciso a) punto 3, que expresa: *"se seleccionará provisoriamente a la oferta con el menor precio como la oferta evaluada como la más baja, la que será analizada en detalle para verificar su cumplimiento con otros requisitos de la licitación, tales como especificaciones técnicas, plazos de entrega, capacidad financiera y técnica para cumplir el contrato".*

6.1. En tal efecto se selecciona la oferta con el menor precio, correspondiente a la empresa **PYTYVO TELECOMUNICACIONES S.A.**, la cual es analizada en detalle en los siguientes criterios:

6.1.1. VERIFICACIÓN DE LA CAPACIDAD TÉCNICA

Se procedió a la verificación de los requisitos en cuanto a la capacidad técnica solicitada en el Anexo B – Datos de la Contratación ((DDLC), punto 20 d):

- El equipo propuesto deberá cumplir como mínimo con las especificaciones técnicas establecidas en el anexo C punto 1 de la Carta de Invitación. Para lo cual será analizado los Folletos, catálogos e impresos descriptivos del equipo ofertado: **CUMPLE** con lo requerido, según Memorando D.I.T. N° 67/2016 del 22/11/2016, de la Dirección de Informática y Tecnología; documento que forma parte de este informe.
- Ser fabricante, representante oficial o distribuidor autorizado para el Paraguay de la marca del equipo ofrecido. En el caso de ser representante o distribuidor, el oferente deberá presentar una carta del fabricante del producto, debidamente membretada y firmada por una autoridad del mismo, emitida cuando menos dentro de los doce (12) meses anteriores a la fecha de presentación de la oferta: **CUMPLE**
- Demostrar que cuenta con la capacidad técnica para instalar y poner en funcionamiento el equipo ofrecido. Para lo cual se considerará la presentación de por lo menos un (1) técnico certificado por el fabricante de la solución ofrecida: **CUMPLE**

6.1.2. VERIFICACIÓN DE LA EXPERIENCIA DE LA EMPRESA

Se procedió a la verificación de los requisitos en cuanto a la experiencia solicitada en el Anexo B – Datos de la Contratación ((DDLC), punto 20 e):

- Demostrar que cuenta con experiencia en la provisión de equipos de seguridad de red informática. Para lo cual se considerarán los siguientes documentos: carta de referencia de clientes y/o contratos y/o comprobantes legales de ventas y/o acta de recepción definitiva ejecutadas durante los tres últimos años (2013, 2014 y 2015) y representen en promedio de los tres años el 80% (ochenta por ciento) del monto total de su oferta. Deberá presentar por lo menos 1 (uno) por cada año: **CUMPLE.**

000496

Realizado el estudio de los documentos presentados por la empresa **PYTYVO TELECOMUNICACIONES S.A.** se han comprobado el cumplimiento de las condiciones establecidas en la Carta de Invitación y sus Anexos, la Ley Nº 2051/03 "de Contrataciones Públicas", su modificatoria la Ley 3.439/07 y el Decreto Reglamentario Nº 21.909/03 modificado por el Decreto Nº 5.174/05.

7. RECOMENDACIÓN

Por las consideraciones expuestas y de conformidad a los artículos 27 y 28 de la Ley Nº 2051/03; los artículos 58 al 59, 62 y 63 del Decreto Reglamentario Nº 21.909/03; su modificatoria el Decreto N° 3719/15, en los artículos 60 y 61; el Comité de Evaluación de Ofertas, recomienda adjudicar por cumplir con la capacidad legal, capacidad técnica y experiencia del llamado a Contratación Directa Nº 18/2016 "Adquisición de un Equipo de Seguridad de Red Informática", a la firma **PYTYVO TELECOMUNICACIONES S.A., con Registro Único del Contribuyente (RUC) Nº 80081010-4,** por un monto total de **Gs. 34.000.000 (guaraníes treinta y cuatro millones),** incluido el impuesto al valor agregado (IVA).

Como prueba de conformidad firman el presente documento, los integrantes del Comité de Evaluación de Ofertas, en tres copias de un solo tenor y a un solo efecto, y se remite a la Secretaría Ejecutiva para su consideración y posterior Resolución, salvo mejor parecer.

HERNAN ARIEL QUIÑONEZ
Jefe del Dpto. de Presupuesto

CARLOS HUMBERTO ZARZA
Director General Interino
Dirección General de Administración y Finanzas

RAQUEL CUEVAS A.
Directora General
Dirección General de Análisis Financiero

000495

INFORME DE EVALUACIÓN DE OFERTAS N° 16/2016

ANEXO A

CUADRO COMPARATIVO DE OFERTAS Y PLANILLA DE VERIFICACIÓN DE CÁLCULOS ARITMÉTICOS

CONTRATACIÓN DIRECTA N° 18/2016 "ADQUISICIÓN DE UN EQUIPO DE SEGURIDAD DE RED INFORMÁTICA"
Id: 317.428

Item	Descripción	Cantidad	OLAM S.R.L.				PYTYVO COMUNICACIONES S.A.				TEISA			
			Precio Unitario	Marca	Procedencia	Precio Total	Precio Unitario	Marca	Procedencia	Precio Total	Precio Unitario	Marca	Procedencia	Precio Total
1	EQUIPO DE SEGURIDAD DE RED INFORMÁTICA	1	34.200.000	FORTINET	USA	34.200.000	34.000.000	FORTINET	EE.UU	34.000.000	34.034.600	FORTINET	EE.UU	34.034.600
		TOTALES				**34.200.000**				**34.000.000**				**34.034.600**

Lic. RAQUEL CUEVAS ARZAMENDIA
Directora General
Dirección General de Análisis Financiero
SEPRELAD

0014694

MEMORANDUM D.I.T. 67/2016

A : Humberto Zarza
Dirección General de Administración y Finanzas
De : Gerardo Fischer
Dirección de Informática y Tecnología
Fecha : 22-11-2016
Asunto : Evaluación Técnicas Firewall UTM

Por el presente cumplo en enviar la correspondiente Evaluación Técnica N°18/2016 "Adquisición de un equipo de seguridad de Red Informatica" (UTM).

Se analiza la oferta técnica presentada por la empresa **TEISA,** con las siguientes consideraciones:

REQUERIMIENTOS TÉCNICOS MÍNIMOS

Provisión del Sistema UTM	Solicitado	Exigido
Características	▪ El dispositivo debe ser un equipo de propósito específico, basado en tecnología ASIC y que sea capaz de brindar una solución de "Complete Content Protection". Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux. ▪ Capacidad de incrementar el rendimiento de VPN a través de soluciones en hardware dentro del mismo dispositivo (mediante el uso de un ASIC). ▪ Capacidad de re ensamblado de paquetes en contenido para buscar ataques o contenido prohibido, basado en hardware (mediante el uso de un ASIC). ▪ El equipo deberá poder ser configurado en modo gateway o en modo transparente en la red. En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP. ▪ El sistema operativo debe incluir un servidor de DNS que permita resolver de forma local ciertas consultas de acuerdo a la configuración del administrador. ▪ El equipo de seguridad debe soportar el uso del protocolo ICAP con el fin de poder delegar tareas a equipos terceros con el fin de liberar procesamiento del mismo.	Cumple
Firewall	• Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs. • Por granularidad y seguridad, el firewall deberá poder especificar políticas tomando en cuenta puerto físico fuente y destino. Esto es, el puerto físico fuente y el puerto físico destino deberán formar parte de la especificación de la regla de firewall. • Será posible definir políticas de firewall que sean independientes del puerto de origen y puerto de destino. • Las reglas del firewall deberán tomar en cuenta 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) de la comunicación que se está analizando. • Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino. • Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a tiempo. • Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a fechas (incluyendo día, mes y año) • Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos. • Debe poder definirse el tiempo de vida de una sesión inactiva de forma independiente por puerto y protocolo (TCP y UDP) • Capacidad de hacer traslación de direcciones estático, uno a uno, NAT. • Capacidad de hacer traslación de direcciones dinámico, muchos a uno, PAT. • Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario). • La solución deberá tener la capacidad de balancear carga entre servidores. Esto es realizar una traslación de una única dirección a múltiples direcciones de forma tal que se distribuya el tráfico entre ellas. • En la solución de balanceo de carga entre servidores, debe soportarse persistencia de sesión al menos mediante HTTP Cookie o SSL Session ID	Cumple

	• En la solución de balanceo de carga de entre servidores deben soportarse mecanismos para detectar la disponibilidad de los servidores, de forma tal de poder evitar enviar tráfico a un servidor no disponible. • El equipo deberá permitir la creación de políticas de tipo Firewall con capacidad de seleccionar campos como dirección, identificador de usuarios o identificador de dispositivos para el caso de dispositivos móviles como smartphones y tabletas. • El equipo deberá permitir la creación de políticas de tipo VPN con capacidad de seleccionar campos como IPSEC o SSL según sea el tipo de VPN. • La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP. • La solución de seguridad deberá permitir la creación de servicios de Firewall para implementar dentro de las políticas de seguridad y categorizarlos de manera personalizada • La solución será capaz de integrar los servicios dentro de las categorías de Firewall predefinidas o personalizadas y ordenarlos alfabéticamente. • El dispositivo de seguridad podrá determinar accesos y denegación a diferentes tipos de tráfico predefinidos dentro de una lista local de políticas • La solución será capaz de habilitar o deshabilitar el paso de tráfico a través de procesadores de propósito específico, si el dispositivo cuenta con estos procesadores integrados dentro del mismo • La solución podrá crear e implementar políticas de tipo Multicast y determinar el sentido de la política, así como también la habilitación del NAT dentro de cada interface del dispositivo • El dispositivo de seguridad será capaz de crear e integrar políticas contra ataques DoS las cuales se deben poder aplicar por interfaces. • El dispositivo de generar logs de cada una de las políticas aplicadas para evitar los ataques de DoS • La solución de seguridad permitirá configurar el mapeo de protocolos a puertos de manera global o especifica • La solución capaz de configurar el bloqueo de archivos o correos electrónicos por tamaño, o por certificados SSL inválidos. • El dispositivo integrara la inspección de tráfico tipo SSL y SSH bajo perfiles predefinidos o personalizados • El dispositivo será capaz de ejecutar inspección de trafico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico • Tendrá la capacidad de hacer escaneo a profundidad de trafico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis • La solución permitirá bloquear o monitorear toda la actividad de tipo Exec, Port-Forward, SSH-Shell, y X-11 SSH.	
Conectividad y Sistema de ruteo	• Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (*Relay*) de solicitudes DHCP. • Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs. • Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas. • Soporte a políticas de ruteo (policy routing). • El soporte a políticas de ruteo deberá permitir que ante la presencia de dos enlaces a Internet, se pueda decidir cuál de tráfico sale por un enlace y qué tráfico sale por otro enlace. • Soporte a ruteo dinámico RIP V1, V2, OSPF, BGP y IS-IS • Soporte a ruteo dinámico RIPng, OSPFv3 • La configuración de BGP debe soportar Autonomous System Path (AS-PATH) de 4 bytes. • Soporte de ECMP (Equal Cost Multi-Path) • Soporte de ECMP con peso. En este modo el tráfico será distribuido entre múltiples rutas pero no en forma equitativa, sino en base a los pesos y preferencias definidas por el administrador. • Soporte de ECMP basado en comportamiento. En este modo, el tráfico será enviado de acuerdo a la definición de una ruta hasta que se alcance un umbral de tráfico. En este punto se comenzará a utilizar en paralelo una ruta alternativa. • Soporte a ruteo de multicast. • La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow. • La solución podrá habilitar políticas de ruteo en IPv6 • La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6 • La solución deberá soportar la creación de políticas de tipo Firewall y VPN y subtipo por dirección IP, tipos de dispositivo y por usuario, con IPv6	Cumple

	• La solución será capaz de habilitar funcionalidades de UTM (Antivirus, Filtrado Web, Control de Aplicaciones, IPS, Filtrado de correo, DLP, ICAP y VoIP) dentro de las políticas creadas con direccionamiento IPv6. • El dispositivo debe integrar la autenticación por usuario o dispositivo en IPv6. • El dispositivo deberá soportar la inspección de tráfico IPv6 en modo proxy explícito. • Deberá ser capaz de integrar políticas con proxy explícito en IPv6 • La solución podrá restringir direcciones IPv6 en modo proxy explicito • Deberá hacer NAT de la red en IPv6 • La solución será capaz de comunicar direccionamiento IPv6 a servicios con IPv4 a través de NAT • Como dispositivo de seguridad deberá soportar la inspección de tráfico IPv6 basada en flujo • La solución deberá ser capaz de habilitar políticas de seguridad con funcionalidades IPS, Filtrado Web, Control de Aplicaciones, Antivirus y DLP, para la inspección de tráfico en IPv6 basado en flujos • La solución contara con una base de administración de información interna generada por sesiones sobre IPv6 • Deberá ser capaz de habilitar la funcionalidad de Traffic Shaper por IP dentro de las políticas creadas en IPv6 • El dispositivo podrá tener la capacidad de transmitir DHCP en IPv6 • La solución tendrá la funcionalidad de habilitar DHCP en IPv6 por interface • La solución deberá contar con soporte para sincronizar por sesiones TCP en IPv6 entre dispositivos para intercambio de configuración en Alta Disponibilidad • El dispositivo podrá ser configurado mediante DHCP en IPv6 para comunicarse con un servidor TFTP donde se encontrara el archivo de configuración • El dispositivo podrá hacer la función como servidor DHCP IPv6 • La solución será capaz de configurar la autenticación por usuario por interface en IPv6.	
VPN IPSec/L2TP/PPTP	• Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site) • Soporte para IKEv2 y IKE Configuration Method • Debe soportar la configuración de túneles PPTP • Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES. • Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits • Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14. • Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256. • Posibilidad de crear VPN's entre gateways y clientes con IPSec. Esto es, VPNs IPSeC site-to-site y VPNs IPSec client-to-site. • La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN) En modo interface, la VPN IPSec deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de firewall. • Tanto para IPSec como para L2TP debe soportarse los clientes terminadores de túneles nativos de Windows y MacOS X.	Cumple
VPN SSL	• Capacidad de realizar SSL VPNs. • Soporte a certificados PKI X.509 para construcción de VPNs SSL. • Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN. • Soporte de renovación de contraseñas para LDAP y RADIUS. • Soporte a asignación de aplicaciones permitidas por grupo de usuarios • Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet. • 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. • Capacidad integrada para eliminar y/o cifrar el contenido descargado al caché de la máquina cliente (caché cleaning) • La VPN SSL integrada deberá soportar a través de algun plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS • Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL • Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente • Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios.	Cumple

	• Los portales personalizados deberán soportar al menos la definición de: ○ Widgets a mostrar ○ Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC ○ Esquema de colores ○ Soporte para Escritorio Virtual ○ Política de verificación de la estación de trabajo. • La VPN SSL integrada debe soportar la funcionalidad de Escritorio Virtual, entendiéndose como un entorno de trabajo seguro que previene contra ciertos ataques además de evitar la divulgación de información. • Para la configuración de cluster, en caso de caída de uno de los dispositivos, la VPN SSL que estuviera establecida, debe restablecerse en el otro dispositivo sin solicitar autentificación nuevamente.	
Traffic Shapping / QoS	• Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall • Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión • 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. • Capacidad de poder definir ancho de banda garantizado en KB por segundo • Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KB por segundo • Capacidad de para definir prioridad de tráfico, en al menos tres niveles de importancia.	Cumple
Autenticación y Certificación Digital	• Capacidad de integrarse con Servidores de Autenticación RADIUS. • Capacidad nativa de integrarse con directorios LDAP • Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es, aprovechar las credenciales del dominio de Windows bajo un concepto "Single-Sign-On" • Capacidad de autenticar usuarios para cualquier aplicación que se ejecute bajo los protocolos TCP/UDP/ICMP. Debe de mostrar solicitud de autenticación (Prompt) al menos para Web (HTTP), FTP y Telnet. • Debe ser posible definir puertos alternativos de autenticación para los protocolos http, FTP y Telnet. • Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site) • La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios. • Deben poder definirse usuarios y grupos en un repositorio local del dispositivo. • Para los administradores locales debe poder definirse la política de contraseñas que especificará como mínimo: Longitud mínima permitida, Restricciones de tipo de caracteres: numéricos, alfanuméricos, etc., Expiración de contraseña. • Debe poder limitarse la posibilidad de que dos usuarios o administradores tengan sesiones simultáneas desde distintas direcciones IP.	Cumple
Antivirus	• Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP. • El Antivirus deberá poder configurarse en modo Proxy como en modo de Flujo. En el primer caso, los archivos serán totalmente reconstruidos por el motor antes de hacer la inspección. En el segundo caso, la inspección de antivirus se hará por cada paquete de forma independiente. • Antivirus en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido. • El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6. • La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP deberá estar completamente integrada a la administración del dispositivo appliance, que permita la aplicación de esta protección por política de control de acceso. • El antivirus deberá soportar múltiples bases de datos de virus de forma tal de que el administrador defina cuál es conveniente utilizar para su implementación evaluando desempeño y seguridad. • El appliance deberá de manera opcional poder inspeccionar por todos los virus conocidos. • El Antivirus integrado deberá tener la capacidad de poner en cuarentena archivos encontrados infectados que estén circulando a través de los protocolos http, FTP, IMAP, POP3, SMTP • El Antivirus integrado tendrá la capacidad de poner en cuarentena a los clientes cuando se haya detectado que los mismos envían archivos infectados con virus.	Cumple

000430

	• El Antivirus deberá incluir capacidades de detección y detención de tráfico spyware, adware y otros tipos de malware/grayware que pudieran circular por la red. • El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging) para al menos MSN Messenger. • El antivirus deberá ser capaz de filtrar archivos por extensión • El antivirus deberá ser capaz de filtrar archivos por tipo de archivo (ejecutables por ejemplo) sin importar la extensión que tenga el archivo • Capacidad de actualización automática de firmas Antivirus mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas).	
AntiSpam	• La capacidad anti spam incluida deberá ser capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, decidir rechazar el mensaje. • La capacidad Anti Spam incluida deberá permitir especificar listas blancas (confiables, a los cuales siempre se les deberá pasar) y listas negras (no confiables, a los cuales siempre les deberá bloquear). Las listas blancas y listas negras podrán ser por dirección IP o por dirección de correo electrónico (e-mail address). • La capacidad Anti Spam deberá poder consultar una base de datos donde se revise por lo menos dirección IP del emisor del mensaje, URLs contenidos dentro del mensaje y checksum del mensaje, como mecanismos para detección de SPAM • En el caso de análisis de SMTP, los mensajes encontrados como SPAM podrán ser etiquetados o rechazados (descartados). En el caso de etiquetamiento del mensaje, debe tenerse la flexibilidad para etiquetarse en el motivo (subject) del mensaje o a través un encabezado MIME en el mensaje.	Cumple
Filtraje de URLs (URL Filtering)	• Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 75 categorías y por lo menos 54 millones de sitios web en la base de datos. • Debe poder categorizar contenido Web requerido mediante IPv6. • Filtrado de contenido basado en categorías en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido. • Configurable directamente desde la interfaz de administración del dispositivo appliance. Con capacidad para permitir esta protección por política de control de acceso. • Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al que pertenezca la conexión siendo establecida • La solución debe permitir realizar el filtrado de contenido, tanto realizando reconstrucción de toda la sesión (modo proxy) como realizando inspección paquete a paquete sin realizar reconstrucción de la comunicación (modo flujo). • Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables. Estos mensajes de remplazo deberán poder aplicarse para conexiones http y https, tanto en modo proxy como en modo flujo. • Los mensajes de remplazo deben poder ser personalizados por categoría de filtrado de contenido. • Capacidad de filtrado de scripts en páginas web (JAVA/Active X). • La solución de Filtraje de Contenido debe soportar el forzamiento de "Safe Search" o "Búsqueda Segura" independientemente de la configuración en el browser del usuario. Esta funcionalidad no permitirá que los buscadores retornen resultados considerados como controversiales. Esta funcionalidad se soportará al menos para Google, Yahoo! y Bing. • Será posible definir cuotas de tiempo para la navegación. Dichas cuotas deben poder asignarse por cada categoría y por grupos. • Será posible exceptuar la inspección de HTTPS por categoría. Debe contar con la capacidad de implementar el filtro de Educación de Youtube por Perfil de Filtro de Contenido para trafico HTTP, garantizando de manera centralizada, que todas las sesiones aceptadas por una política de seguridad con este perfil, van a poder acceder solamente a contenido de tipo Educativo en Youtbube, bloqueando cualquier tipo de contenido no Educativo. • El sistema de filtrado de URLs debe tener al menos 3 métodos de inspección: 1. Modo de Flujo: La página es inspeccionada paquete a paquete sin reconstruir la página completa.	Cumple

Fol: 485

	2. Modo Proxy: La página es reconstruida completamente para ser analizada a profundidad. 3. Modo DNS: La inspección se basa únicamente en la categorización del dominio accesado. • Se debe incluir la funcionalidad de reputación basada en filtrado de URLs. • La funcionalidad de reputación busca que, al acceder a páginas de contenido no deseado (tales como Malware, pornografía, consumo de ancho de banda excesivo, etc) se asigne un puntaje a cada usuario o IP cada vez visita una página de esta índole. De acuerdo a esto se extrae los usuarios que infringen las políticas de filtrado con más frecuencia con el fin de detectar zombies dentro de la red. • El sistema de filtrado de URLs debe incluir la capacidad de definir cuotas de navegación basadas en volumen de tráfico consumido. • Se debe incorporar la funcionalidad de filtrado educativo de Youtube (Youtube Education Filter) • En dicho sistema cada organismo obtiene un ID de Youtube para habilitar el contenido educativo del mismo. Se deberá insertar dicho código en la configuración de filtrado de URLs del equipo para poder habilitar únicamente el contenido educativo de Youtube.	
Protección contra intrusos (IPS)	• El Detector y preventor de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror. • Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores. • Capacidad de detección de más de 4000 ataques. • Capacidad de actualización automática de firmas IPS mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas) • El detector y preventor de intrusos deberá estar integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la prevención de intrusos. La interfaz de administración del detector y preventor de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso. • El detector y preventor de intrusos deberá soportar captar ataques por variaciones de protocolo y además por firmas de ataques conocidos (signature based / misuse detection). • Basado en análisis de firmas en el flujo de datos en la red, y deberá permitir configurar firmas nuevas para cualquier protocolo. • Actualización automática de firmas para el detector de intrusos • El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios. • Métodos de notificación: o Alarmas mostradas en la consola de administración del appliance. o Alertas vía correo electrónico. o Debe tener la capacidad de cuarentena, es decir prohibir el tráfico subsiguiente a la detección de un posible ataque. Esta cuarentena debe poder definirse al menos para el tráfico proveniente del atacante o para el tráfico del atacante al atacado. o La capacidad de cuarentena debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma "indefinida", hasta que un administrador tome una acción al respecto. o Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP. • Se debe incluir protección contra amenazas avanzadas y persistentes (Advanced Persistent Threats). Dentro de estos controles se debe incluir: • Protección contra botnets: Se deben 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. • Sandboxing: La funcionalidad de Sandbox hace que el archivo sea ejecutado en un ambiente seguro para analizar su comportamiento y, a base del mismo, tomar una acción sobre el mismo.	Cumple 000488
Prevención de Fuga de Información (DLP)	• La solución debe ofrecer la posibilidad de definir reglas que permitan analizar los distintos archivos que circulan a través de la red en búsqueda de información confidencial.	Cumple

	• La funcionalidad debe soportar el análisis de archivos del tipo: MS-Word, PDF, Texto, Archivos comprimidos. • Debe soportarse el escaneo de archivos en al menos los siguientes protocolos: HTTP, POP3, SMTP, IMAP, NNTP y FTP. • Ante la detección de una posible fuga de información deben poder aplicarse el menos las siguientes acciones: Bloquear el tráfico del usuario, Bloquear el tráfico de la dirección IP de origen, registrar el evento, • En caso del bloqueo de usuarios, la solución debe permitir definir por cuánto tiempo se hará el bloqueo o en su defecto bloquear por tiempo indefinido hasta que el administrador tome una acción. • La solución debe soportar la capacidad de guardar una copia del archivo identificado como posible fuga de información. Esta copia podría ser archivada localmente o en otro dispositivo. • La solución debe permitir la búsqueda de patrones en archivos mediante la definición de expresiones regulares. • Se debe proveer la funcionalidad de filtrado de fuga de información. Dentro de las técnicas de detección se debe considerar como mínimo las siguientes: 1. Filtrado por tipo de archivo 2. Filtrado por nombre de archivo 3. Filtrado por expresiones regulares: Se detectarán los archivos según las expresiones regulares que se encuentren dentro de los mismos. 4. Fingerprinting: Se tomará una muestra del archivo que se considere como confidencial. Según esto se bloquearán archivos que sean iguales a esta muestra. 5. Watermarking: Se insertará un "sello de agua" dentro del archivo considerado como confidencial. De acuerdo a esto se analizarán los archivos en busca de este sello de agua, este se detectará incluso si el archivo sufrió cambios.	
Control de Aplicaciones	• La solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo. • La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico. • La solución debe tener un listado de al menos 1000 aplicaciones ya definidas por el fabricante. • El listado de aplicaciones debe actualizarse periódicamente. • Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log. • Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log. • Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping. • Preferentemente deben soportar mayor granularidad en las acciones.	Cumple
Inspección de Contenido SSL	• La solución debe soportar la capacidad de inspeccionar tráfico que esté siendo encriptado mediante TLS al menos para los siguientes protocolos: HTTPS, IMAPS, SMTPS, POP3S. • La inspección deberá realizarse mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle). • La inspección de contenido encriptado no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario. • Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado. • El equipo debe ser capaz de analizar contenido cifrado (SSL o SSH) para las funcionalidades de Filtrado de URLs, Control de Aplicaciones, Prevención de Fuga de Información, Antivirus e IPS.	Cumple
Controlador Inalámbrico (Wireless Controller)	• El dispositivo debe tener la capacidad de funcionar como Controlador de Wireless • En modo de Controlador de Wireless tendrá la capacidad de configurar múltiples puntos de acceso (Access Points: APs) reales de forma tal de que se comporten como uno solo. Cómo mínimo deberá controlar los SSID, roaming entre APs, configuraciones de cifrado, configuraciones de autenticación. • Debe soportar la funcionalidad de detección y mitigación de puntos de acceso (APs). Rogue Access Point Detection. • El controlador de Wireless tendrá la capacidad de configurar la asignación de direcciones IP mediante DHCP a las estaciones de trabajo conectadas a los APs. • Deberá tener la capacidad de monitorear las estaciones de trabajo, clientes wireless, conectadas a alguno de los APs.	Cumple

00485

	• La solución debe contar con la funcionalidad de WIDS (Wireless IDS), la capacidad de monitorear el trafico wireless para detectar y reportar posibles intentos de intrusión. • Debe contar con un sistema de aprovisionamiento de usuarios invitados para red wifi, que permita la creación sencilla de accesos para invitados, por medio de un portal independiente. • El equipo debe tener capacidad de que estos usuarios invitados con acceso inalámbrico, tengan la opción de colocar o no contraseña, con tiempo limitado y configurable para la expiración de la cuenta. • El controlador inalámbrico debe estar en la capacidad de balancear la carga entre los puntos de acceso (Access Points) soportando por lo menos los siguientes métodos de balanceo: Access Point Hand-off, Frequency Hand-off. • Debe contar con la capacidad de realizar Bridge SSID, permitiendo que una red inalámbrica y un segmento cableado LAN pertenezcan a la misma rubred. • El dispositivo deberá ser capaz de administrar los dispositivos wireless AP de la misma plataforma, tanto en consola CLI como a través de una interfaz grafica (GUI) • El dispositivo debe tener la capacidad de controlar varios puntos de acceso de la misma plataforma de forma remota. • El dispositivo debe poder cifrar la información que se envía hacia los puntos de acceso de la misma plataforma, sobre los cuales se esté teniendo control y gestión. • El dispositivo debe permitir la administración y manejo tanto de redes cableadas como inalámbricos dentro del mismo segmento de red. • El equipo debe tener la capacidad de reconocer y monitorear diferentes tipos de dispositivos de comunicación móvil como Smartphones Androide, Blackberry y Iphone; diferentes tipos de consolas de juego como Xbox, PS2, PS3, Wii, PSP; diferentes tipos de tabletas con SO Androide o tabletas Ipad, • El equipo debe tener la capacidad de controlar el acceso a la red de los diferentes dispositivos antes mencionados a través de ACLs por MAC • El equipo deberá permitir el crear diferentes niveles de acceso a la red en función del tipo de dispositivo que se conecte, siendo estos: Smartphones, Tabletas, Laptoos, PCs (tanto en Windows como en Linux) • El equipo debe permitir la separación de redes al menos entre usuarios internos e invitados, permitiendo la colocación de reglas en función de los dispositivos móviles conectados.	
Filtraje de tráfico VoIP, *Peer-to-Peer* y Mensajería instantánea	• Soporte a aplicaciones multimedia tales como (incluyendo) : SCCP (Skinny), H.323, SIP, Real Time Streaming Protocol (RTSP). • El dispositivo deberá técnicas de detección de P2P y programas de archivos compartidos (peer-to-peer), soportando al menos Yahoo! Messenger, MSN Messenger, ICQ y AOL Messenger para Messenger, y BitTorrent, eDonkey, GNUTella, KaZaa, Skype y WinNY para Peer-to-peer. • 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. • La solución debe contar con un ALG (Application Layer Gateway) de SIP • Debe poder hacerse inspección de encabezados de SIP • Deben poder limitarse la cantidad de requerimientos SIP que se hacen por segundo. Esto debe poder definirse por cada método SIP. • La solución debe soportar SIP HNT (Hosted NAT Transversal). • La solución deberá integrar la inspección de tráfico basado en flujo utilizando un motor de IPS dentro del mismo dispositivo para escaneo de paquetes • Deberá ser capaz de hacer inspección tráfico SSH en modo proxy explicito • La solución de seguridad podrá hacer inspección de tráfico HTTP, HTTPS y FTP sobre HTTP en modalidad proxy explicito con las funcionalidades de IPS, Antivirus, Filtrado Web, Control de Aplicaciones y DLP, todo en un mismo dispositivo • El dispositivo tendrá la opción para configurar sus interfaces integradas en modo Sniffer con funcionalidades de Filtrado Web, Control de Aplicaciones, Antivirus e IPS.	Cumple
Optimización WAN y Web Caching	• La solución deberá permitir la creación de perfiles para la aplicación de Optimización WAN e indicar bajo que protocolos se ejecutará • Deberá ser capaz de activar en modo transparente dentro de los perfiles de Optimización WAN y seleccionar un determinado grupo de usuarios para autenticación de acceso • El dispositivo deberá soportar la desfragmentación dinámica de paquetes para detectar fragmentos persistentes de distintos archivos o datos adjuntos dentro del trafico bajo protocolos desconocidos • La solución debe ser capaz de generar y aplicar perfiles de Optimización WAN para los usuarios	Cumple

600486

	• El dispositivo de seguridad podrá integrar contenido de inspección dentro de sus políticas de seguridad con Optimización WAN • La solución integrara dentro de cada interface la capacidad de hacer túneles de Optimización WAN • Deberá ser capaz de configurar Optimización WAN en modo Activo/Pasivo • Solución capaz de aplicar web cache a tráfico HTTP y HTTPS dentro de las políticas de seguridad incluyendo también Optimización WAN y web proxy cache • Dispositivo capaz de habilitar el almacenamiento en caché web tanto en el lado del cliente y del lado de la solución • La solución podrá recibir el tráfico HTTPS en nombre del cliente, abrirá y extraerá el contenido del tráfico cifrado para inspeccionar y almacenar en cache para el envío al usuario final • El dispositivo tendrá la opción de integrar un certificado SSL determinado para la recifrado de tráfico • La solución capaz de configurar el cache de trafico HTTP y HTTPS bajo distintos puertos a los predeterminados (80 y 443) • La solución debe ser capaz de habilitar opciones para depurar la funcionalidad de Web Cache a determinadas URL.	
Alta Disponibilidad	• El dispositivo deberá soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6 • Alta Disponibilidad en modo Activo-Pasivo • Alta Disponibilidad en modo Activo-Activo • Posibilidad de definir al menos dos interfaces para sincronía • El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red • Será posible definir interfaces de gestión independientes para cada miembro en un clúster.	Cumple
Características de Administración	• Interface gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interface debe soportar SSL sobre HTTP (HTTPS) • La interface gráfica de usuario (GUI) vía Web deberá poder estar en español y en inglés, configurable por el usuario. • Interface basada en línea de comando (CLI) para administración de la solución. • Puerto serial dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto. • Comunicación cifrada y autenticada con usuario y contraseña, tanto como para la interfase gráfica de usuario como la consola de administración de línea de comandos (SSH o telnet) • El administrador del sistema podrá tener las opciones incluidas de autenticarse vía usuario/contraseña y vía certificados digitales. • Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar. • El equipo ofrecerá la flexibilidad para especificar que Los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet,http o HTTPS. • El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional. • Soporte de SNMP versión 2 • Soporte de SNMP versión 3 • Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos • Soporte para almacenamiento de eventos en un repositorio que pueda consultarse luego con SQL. • Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall. • Monitoreo de comportamiento del appliance mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red. • Debe ser posible definir la dirección IP que se utilizará como origen para el tráfico iniciado desde el mismo dispositivo. Esto debe poder hacerse al menos para el tráfico de alertas, SNMP, Log y gestión. • Permitir que el administrador de la plataforma pueda definir qué funcionalidades están disponibles o deshabilitadas para ser mostradas en la interfaz gráfica.	Cumple

	▪ Contar con facilidades de administración a través de la interfaz gráfica como listas de edición a través de click derecho. ▪ Contar con facilidades de administración a través de la interfaz gráfica como ayudantes de configuración (setup wizard). ▪ Contar con la posibilidad de agregar una barra superior (Top Bar) cuando los usuarios estén navegando con información como el ID de usuario, cuota de navegación utilizada, y aplicaciones que vayan en contra de las políticas de la empresa. * Contar con herramientas gráficas para visualizar fácilmente las sesiones en el equipo, que permitan adicionarse por el administrador en la página inicial de la solución (dashboard), incluyendo por lo menos por defecto Top de sesiones por origen, Top de sesiones por destino, y Top de sesiones por aplicación.	
Virtualización	▪ El dispositivo deberá poder virtualizar los servicios de seguridad mediante "Virtual Systems", "Virtual Firewalls" o "Virtual Domains" ▪ La instancia virtual debe soportar por lo menos Firewall, VPN, URL Filtering, IPS y Antivirus ▪ Se debe incluir la licencia para al menos 8 (ocho) instancias virtuales dentro de la solución a proveer. ▪ Cada instancia virtual debe poder tener un administrador independiente ▪ La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales. ▪ Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red ▪ Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual ▪ Debe ser posible definir distintos servidores de log (syslog) para cada instancia virtual. ▪ Debe ser posible definir y modificar los mensajes mostrados por el dispositivo de forma independiente para cada instancia virtual. ▪ Debe ser posible definir enlaces de comunicación entre los sistemas virtuales sin que el trafico deba salir de la solución por medio de enlaces o conexiones virtuales, y estas conexiones deben poder realizarse incluso entre instancias virtuales en modo NAT y en modo Transparente.	Cumple
Análisis de Seguridad y Almacenamiento de Logs en la Nube	▪ La solución de seguridad debe contar con una solución en la nube que permita centralización de reportes, análisis de tráfico, administración de configuraciones, y almacenamiento de logs sin la necesidad de software o hardware adicional para esta función. ▪ Contar con funcionalidad de Análisis de archivos sospechosos en la nube en caso que no se cuente con suficiente información en la solución de seguridad para calificar el tráfico como legitimo o ilegitimo, por medio de técnicas de Caja de Arena o Sandboxing. ▪ Almacenamiento de Logs hasta 1 Giga por equipo incluido con capacidad de crecimiento en caso de requerirse. ▪ Debe permitir administración centralizada de todos los equipos de la solución de seguridad perimetral desde una misma interfaz. ▪ Permitir Monitoreo y alertas en tiempo real. ▪ Debe contar con Reportes predefinidos y la opción de personalización, así como contar con herramientas de análisis. ▪ Debe permitir visualizar de manera sencilla que todos los equipos de seguridad perimetral gestionados cuenten con la misma versión de firmware o sistema operativo para garantizar la homogeneidad en la red.	Cumple
Actualizaciones de plataforma	▪ La solución contara con el servicio de actualización de firmas para dispositivos sobre BYOD ▪ El dispositivo tendrá la opción de conectarse a los servidores NTP de los Laboratorios de Investigación y Actualización propietarios del mismo fabricante para actualización del horario de sistema local ▪ Sera capaz de hacer consultas a los servidores DNS de los Laboratorios de Investigación y Actualización del mismo fabricante para resolución y categorización de sitios web dentro de los perfiles para Filtrado Web ▪ Tendrá la capacidad de hacer consultas a los servidores DNS de los Laboratorios de investigación y actualización mismos del fabricante sobre reputación de direcciones IP. 000484	Cumple
Licencia	El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, cajas de correo, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo.	Cumple
Vigencia de licencia de actualización	La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS y URL Filtering debe proveerse por al menos dos años.	No Cumple

Numero de Interfaces	1 Console Port (RJ45), 2 USB Ports, 2 GE RJ45 Management Ports, 4 GE RJ45 Ports, 4 GE SFP Slots	No Cumple
Throughput de Firewall	3 / 3 / 3 Gbps	No Cumple
Throughput de VPN IPSec	1.3 Gbps	No Cumple
Throughput de Antivirus	600 Mbps	Cumple
Throughput de IPS	350Mbps	Cumple
Tuneles dedicados	2,000	Cumple
Tuneles SSL	10,000	No Cumple
Throughput VPN SSL	400 Mbps	No Cumple
Sesiones Concurrentes	3.2 Mil	No Cumple
Nuevas sesiones / segundo	77.000	No Cumple
Políticas	10,000	Cumple
Dimensiones de Rack	1 RU	Cumple
Numero de Instancias virtuales	10 / 10	Cumple
AC Power	100 – 240V AC, 50 – 60Hz	Cumple
Consumo de poder promedio	49/83 W	Cumple
Implementación	La instalación, capacitación, provisión como así también las licencias y suscripciones a las funcionalidades solicitadas además de parametrización conformes a las licencias y trabajos necesarios para su instalación y funcionamiento correrán por cuenta del Oferente.	Cumple
Certificación Técnica Solicitada	*Al menos 1 técnico certificado, la certificación deberá estar emitida por el fabricante de la marca de la solución ofertada. *Se aceptarán como válidos los certificados emitidos a partir del año 2013.	Cumple
Plazo entrega	45 días corridos.	Cumple

La oferta **no cumple** con las especificaciones técnicas solicitadas en los puntos antes señalados, debido a que la Empresa presenta un equipo de menores prestaciones.

000483

Se analiza la oferta técnica presentada por la empresa **PYTYVO COMUNICACIONES SA**, con las siguientes consideraciones:

REQUERIMIENTOS TÉCNICOS MÍNIMOS

Provisión del Sistema UTM	Solicitado	Exigido
Características	▪ El dispositivo debe ser un equipo de propósito específico, basado en tecnología ASIC y que sea capaz de brindar una solución de "Complete Content Protection". Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux. ▪ Capacidad de incrementar el rendimiento de VPN a través de soluciones en hardware dentro del mismo dispositivo (mediante el uso de un ASIC). ▪ Capacidad de re ensamblado de paquetes en contenido para buscar ataques o contenido prohibido, basado en hardware (mediante el uso de un ASIC). ▪ El equipo deberá poder ser configurado en modo gateway o en modo transparente en la red. En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP. ▪ El sistema operativo debe incluir un servidor de DNS que permita resolver de forma local ciertas consultas de acuerdo a la configuración del administrador. ▪ El equipo de seguridad debe soportar el uso del protocolo ICAP con el fin de poder delegar tareas a equipos terceros con el fin de liberar procesamiento del mismo.	Cumple
Firewall	• Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs. • Por granularidad y seguridad, el firewall deberá poder especificar políticas tomando en cuenta puerto físico fuente y destino. Esto es, el puerto físico fuente y el puerto físico destino deberán formar parte de la especificación de la regla de firewall. • Será posible definir políticas de firewall que sean independientes del puerto de origen y puerto de destino. • Las reglas del firewall deberán tomar en cuenta 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) de la comunicación que se está analizando. • Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino. • Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a tiempo. • Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a fechas (incluyendo día, mes y año) • Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos. • Debe poder definirse el tiempo de vida de una sesión inactiva de forma independiente por puerto y protocolo (TCP y UDP) • Capacidad de hacer traslación de direcciones estático, uno a uno, NAT. • Capacidad de hacer traslación de direcciones dinámico, muchos a uno, PAT. • Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario), • La solución deberá tener la capacidad de balancear carga entre servidores. Esto es realizar una traslación de una única dirección a múltiples direcciones de forma tal que se distribuya el tráfico entre ellas. • En la solución de balanceo de carga entre servidores, debe soportarse persistencia de sesión al menos mediante HTTP Cookie o SSL Session ID • En la solución de balanceo de carga de entre servidores deben soportarse mecanismos para detectar la disponibilidad de los servidores, de forma tal de poder evitar enviar tráfico a un servidor no disponible. • El equipo deberá permitir la creación de políticas de tipo Firewall con capacidad de seleccionar campos como dirección, identificador de usuarios o identificador de dispositivos para el caso de dispositivos móviles como smartphones y tabletas. • El equipo deberá permitir la creación de políticas de tipo VPN con capacidad de seleccionar campos como IPSEC o SSL según sea el tipo de VPN.	Cumple

482

	• La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP. • La solución de seguridad deberá permitir la creación de servicios de Firewall para implementar dentro de las políticas de seguridad y categorizarlos de manera personalizada • La solución será capaz de integrar los servicios dentro de las categorías de Firewall predefinidas o personalizadas y ordenarlos alfabéticamente. • El dispositivo de seguridad podrá determinar accesos y denegación a diferentes tipos de tráfico predefinidos dentro de una lista local de políticas • La solución será capaz de habilitar o deshabilitar el paso de tráfico a través de procesadores de propósito específico, si el dispositivo cuenta con estos procesadores integrados dentro del mismo • La solución podrá crear e implementar políticas de tipo Multicast y determinar el sentido de la política, así como también la habilitación del NAT dentro de cada interface del dispositivo • El dispositivo de seguridad será capaz de crear e integrar políticas contra ataques DoS las cuales se deben poder aplicar por interfaces. • El dispositivo de generar logs de cada una de las políticas aplicadas para evitar los ataques de DoS • La solución de seguridad permitirá configurar el mapeo de protocolos a puertos de manera global o especifica • La solución capaz de configurar el bloqueo de archivos o correos electrónicos por tamaño, o por certificados SSL inválidos. • El dispositivo integrara la inspección de tráfico tipo SSL y SSH bajo perfiles predefinidos o personalizados • El dispositivo será capaz de ejecutar inspección de trafico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico • Tendrá la capacidad de hacer escaneo a profundidad de trafico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis • La solución permitirá bloquear o monitorear toda la actividad de tipo Exec, Port-Forward, SSH-Shell, y X-11 SSH.	
Conectividad y Sistema de ruteo	• Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (*Relay*) de solicitudes DHCP. • Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs. • Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas. • Soporte a políticas de ruteo (policy routing). • El soporte a políticas de ruteo deberá permitir que ante la presencia de dos enlaces a Internet, se pueda decidir cuál de tráfico sale por un enlace y qué tráfico sale por otro enlace. • Soporte a ruteo dinámico RIP V1, V2, OSPF, BGP y IS-IS • Soporte a ruteo dinámico RIPng, OSPFv3 • La configuración de BGP debe soportar Autonomous System Path (AS-PATH) de 4 bytes. • Soporte de ECMP (Equal Cost Multi-Path) • Soporte de ECMP con peso. En este modo el tráfico será distribuido entre múltiples rutas pero no en forma equitativa, sino en base a los pesos y preferencias definidas por el administrador. • Soporte de ECMP basado en comportamiento. En este modo, el tráfico será enviado de acuerdo a la definición de una ruta hasta que se alcance un umbral de tráfico. En este punto se comenzará a utilizar en paralelo una ruta alternativa. • Soporte a ruteo de multicast. • La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow. • La solución podrá habilitar políticas de ruteo en IPv6 • La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6 • La solución deberá soportar la creación de políticas de tipo Firewall y VPN y subtipo por dirección IP, tipos de dispositivo y por usuario, con IPv6 • La solución será capaz de habilitar funcionalidades de UTM (Antivirus, Filtrado Web, Control de Aplicaciones, IPS, Filtrado de correo, DLP, ICAP y VoIP) dentro de las políticas creadas con direccionamiento IPv6. • El dispositivo debe integrar la autenticación por usuario o dispositivo en IPv6. • El dispositivo deberá soportar la inspección de tráfico IPv6 en modo proxy explícito. • Deberá ser capaz de integrar políticas con proxy explícito en IPv6 • La solución podrá restringir direcciones IPv6 en modo proxy explicito • Deberá hacer NAT de la red en IPv6	Cumple 000481

	• La solución será capaz de comunicar direccionamiento IPv6 a servicios con IPv4 a través de NAT • Como dispositivo de seguridad deberá soportar la inspección de tráfico IPv6 basada en flujo • La solución deberá ser capaz de habilitar políticas de seguridad con funcionalidades IPS, Filtrado Web, Control de Aplicaciones, Antivirus y DLP, para la inspección de tráfico en IPv6 basado en flujos • La solución contara con una base de administración de información interna generada por sesiones sobre IPv6 • Deberá ser capaz de habilitar la funcionalidad de Traffic Shaper por IP dentro de las políticas creadas en IPv6 • El dispositivo podrá tener la capacidad de transmitir DHCP en IPv6 • La solución tendrá la funcionalidad de habilitar DHCP en IPv6 por interface • La solución deberá contar con soporte para sincronizar por sesiones TCP en IPv6 entre dispositivos para intercambio de configuración en Alta Disponibilidad • El dispositivo podrá ser configurado mediante DHCP en IPv6 para comunicarse con un servidor TFTP donde se encontrara el archivo de configuración • El dispositivo podrá hacer la función como servidor DHCP IPv6 • La solución será capaz de configurar la autenticación por usuario por interface en IPv6.	
VPN IPSec/L2TP/PPTP	• Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site) • Soporte para IKEv2 y IKE Configuration Method • Debe soportar la configuración de túneles PPTP • Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES. • Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits • Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14. • Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256. • Posibilidad de crear VPN's entre gateways y clientes con IPSec. Esto es, VPNs IPSeC site-to-site y VPNs IPSec client-to-site. • La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN) En modo interface, la VPN IPSec deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de firewall. • Tanto para IPSec como para L2TP debe soportarse los clientes terminadores de túneles nativos de Windows y MacOS X.	Cumple
VPN SSL	• Capacidad de realizar SSL VPNs. • Soporte a certificados PKI X.509 para construcción de VPNs SSL. • Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN. • Soporte de renovación de contraseñas para LDAP y RADIUS. • Soporte a asignación de aplicaciones permitidas por grupo de usuarios • Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet. • 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. • Capacidad integrada para eliminar y/o cifrar el contenido descargado al caché de la máquina cliente (caché cleaning) • La VPN SSL integrada deberá soportar a través de algun plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS • Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL • Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente • Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios. • Los portales personalizados deberán soportar al menos la definición de: ○ Widgets a mostrar ○ Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC ○ Esquema de colores ○ Soporte para Escritorio Virtual ○ Política de verificación de la estación de trabajo.	Cumple

	• La VPN SSL integrada debe soportar la funcionalidad de Escritorio Virtual, entendiéndose como un entorno de trabajo seguro que previene contra ciertos ataques además de evitar la divulgación de información. • Para la configuración de cluster, en caso de caída de uno de los dispositivos, la VPN SSL que estuviera establecida, debe restablecerse en el otro dispositivo sin solicitar autentificación nuevamente.	
Traffic Shapping / QoS	• Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall • Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión • 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. • Capacidad de poder definir ancho de banda garantizado en KB por segundo • Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KB por segundo • Capacidad de para definir prioridad de tráfico, en al menos tres niveles de importancia.	Cumple
Autenticación y Certificación Digital	• Capacidad de integrarse con Servidores de Autenticación RADIUS. • Capacidad nativa de integrarse con directorios LDAP • Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es, aprovechar las credenciales del dominio de Windows bajo un concepto "Single-Sign-On" • Capacidad de autenticar usuarios para cualquier aplicación que se ejecute bajo los protocolos TCP/UDP/ICMP. Debe de mostrar solicitud de autenticación (Prompt) al menos para Web (HTTP), FTP y Telnet. • Debe ser posible definir puertos alternativos de autenticación para los protocolos http, FTP y Telnet. • Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site) • La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios. • Deben poder definirse usuarios y grupos en un repositorio local del dispositivo. • Para los administradores locales debe poder definirse la política de contraseñas que especificará como mínimo: Longitud mínima permitida, Restricciones de tipo de caracteres: numéricos, alfanuméricos, etc., Expiración de contraseña. • Debe poder limitarse la posibilidad de que dos usuarios o administradores tengan sesiones simultáneas desde distintas direcciones IP.	Cumple
Antivirus	• Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP. • El Antivirus deberá poder configurarse en modo Proxy como en modo de Flujo. En el primer caso, los archivos serán totalmente reconstruidos por el motor antes de hacer la inspección. En el segundo caso, la inspección de antivirus se hará por cada paquete de forma independiente. • Antivirus en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido. • El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6. • La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP deberá estar completamente integrada a la administración del dispositivo appliance, que permita la aplicación de esta protección por política de control de acceso. • El antivirus deberá soportar múltiples bases de datos de virus de forma tal de que el administrador defina cuál es conveniente utilizar para su implementación evaluando desempeño y seguridad. • El appliance deberá de manera opcional poder inspeccionar por todos los virus conocidos. • El Antivirus integrado deberá tener la capacidad de poner en cuarentena archivos encontrados infectados que estén circulando a través de los protocolos http, FTP, IMAP, POP3, SMTP • El Antivirus integrado tendrá la capacidad de poner en cuarentena a los clientes cuando se haya detectado que los mismos envían archivos infectados con virus. • El Antivirus deberá incluir capacidades de detección y detención de tráfico spyware, adware y otros tipos de malware/grayware que pudieran circular por la red. • El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging) para al menos MSN Messenger. • El antivirus deberá ser capaz de filtrar archivos por extensión	Cumple

000479

	• El antivirus deberá ser capaz de filtrar archivos por tipo de archivo (ejecutables por ejemplo) sin importar la extensión que tenga el archivo • Capacidad de actualización automática de firmas Antivirus mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas).	
AntiSpam	• La capacidad anti spam incluida deberá ser capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, decidir rechazar el mensaje. • La capacidad Anti Spam incluida deberá permitir especificar listas blancas (confiables, a los cuales siempre se les deberá pasar) y listas negras (no confiables, a los cuales siempre les deberá bloquear). Las listas blancas y listas negras podrán ser por dirección IP o por dirección de correo electrónico (e-mail address). • La capacidad Anti Spam deberá poder consultar una base de datos donde se revise por lo menos dirección IP del emisor del mensaje, URLs contenidos dentro del mensaje y checksum del mensaje, como mecanismos para detección de SPAM • En el caso de análisis de SMTP, los mensajes encontrados como SPAM podrán ser etiquetados o rechazados (descartados). En el caso de etiquetamiento del mensaje, debe tenerse la flexibilidad para etiquetarse en el motivo (subject) del mensaje o a través un encabezado MIME en el mensaje.	Cumple
Filtraje de URLs (URL Filtering)	• Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 75 categorías y por lo menos 54 millones de sitios web en la base de datos. • Debe poder categorizar contenido Web requerido mediante IPv6. • Filtrado de contenido basado en categorías en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido. • Configurable directamente desde la interfaz de administración del dispositivo appliance. Con capacidad para permitir esta protección por política de control de acceso. • Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al que pertenezca la conexión siendo establecida • La solución debe permitir realizar el filtrado de contenido, tanto realizando reconstrucción de toda la sesión (modo proxy) como realizando inspección paquete a paquete sin realizar reconstrucción de la comunicación (modo flujo). • Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables. Estos mensajes de remplazo deberán poder aplicarse para conexiones http y https, tanto en modo proxy como en modo flujo. • Los mensajes de remplazo deben poder ser personalizados por categoría de filtrado de contenido. • Capacidad de filtrado de scripts en páginas web (JAVA/Active X). • La solución de Filtraje de Contenido debe soportar el forzamiento de "Safe Search" o "Búsqueda Segura" independientemente de la configuración en el browser del usuario. Esta funcionalidad no permitirá que los buscadores retornen resultados considerados como controversiales. Esta funcionalidad se soportará al menos para Google, Yahoo! y Bing. • Será posible definir cuotas de tiempo para la navegación. Dichas cuotas deben poder asignarse por cada categoría y por grupos. • Será posible exceptuar la inspección de HTTPS por categoría. Debe contar con la capacidad de implementar el filtro de Educación de Youtube por Perfil de Filtro de Contenido para trafico HTTP, garantizando de manera centralizada, que todas las sesiones aceptadas por una política de seguridad con este perfil, van a poder acceder solamente a contenido de tipo Educativo en Youtbube, bloqueando cualquier tipo de contenido no Educativo. • El sistema de filtrado de URLs debe tener al menos 3 métodos de inspección: 1. Modo de Flujo: La página es inspeccionada paquete a paquete sin reconstruir la página completa. 2. Modo Proxy: La página es reconstruida completamente para ser analizada a profundidad. 3. Modo DNS: La inspección se basa únicamente en la categorización del dominio accesado. • Se debe incluir la funcionalidad de reputación basada en filtrado de URLs. • La funcionalidad de reputación busca que, al acceder a páginas de contenido no deseado (tales como Malware, pornografía, consumo de ancho de banda excesivo, etc) se asigne un puntaje a	Cumple

000478

	cada usuario o IP cada vez visita una página de esta índole. De acuerdo a esto se extrae los usuarios que infringen las políticas de filtrado con más frecuencia con el fin de detectar zombies dentro de la red. • El sistema de filtrado de URLs debe incluir la capacidad de definir cuotas de navegación basadas en volumen de tráfico consumido. • Se debe incorporar la funcionalidad de filtrado educativo de Youtube (Youtube Education Filter) • En dicho sistema cada organismo obtiene un ID de Youtube para habilitar el contenido educativo del mismo. Se deberá insertar dicho código en la configuración de filtrado de URLs del equipo para poder habilitar únicamente el contenido educativo de Youtube.	
Protección contra intrusos (IPS)	• El Detector y preventor de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror. • Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores. • Capacidad de detección de más de 4000 ataques. • Capacidad de actualización automática de firmas IPS mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas) • El detector y preventor de intrusos deberá estar integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la prevención de intrusos. La interfaz de administración del detector y preventor de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso. • El detector y preventor de intrusos deberá soportar captar ataques por variaciones de protocolo y además por firmas de ataques conocidos (signature based / misuse detection). • Basado en análisis de firmas en el flujo de datos en la red, y deberá permitir configurar firmas nuevas para cualquier protocolo. • Actualización automática de firmas para el detector de intrusos • El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios. • Métodos de notificación: o Alarmas mostradas en la consola de administración del appliance. o Alertas vía correo electrónico. o Debe tener la capacidad de cuarentena, es decir prohibir el tráfico subsiguiente a la detección de un posible ataque. Esta cuarentena debe poder definirse al menos para el tráfico proveniente del atacante o para el tráfico del atacante al atacado. o La capacidad de cuarentena debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma "indefinida", hasta que un administrador tome una acción al respecto. o Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP. • Se debe incluir protección contra amenazas avanzadas y persistentes (Advanced Persistent Threats). Dentro de estos controles se debe incluir: • Protección contra botnets: Se deben 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. • Sandboxing: La funcionalidad de Sandbox hace que el archivo sea ejecutado en un ambiente seguro para analizar su comportamiento y, a base del mismo, tomar una acción sobre el mismo.	Cumple
Prevención de Fuga de Información (DLP)	• La solución debe ofrecer la posibilidad de definir reglas que permitan analizar los distintos archivos que circulan a través de la red en búsqueda de información confidencial. • La funcionalidad debe soportar el análisis de archivos del tipo: MS-Word, PDF, Texto, Archivos comprimidos. • Debe soportarse el escaneo de archivos en al menos los siguientes protocolos: HTTP, POP3, SMTP, IMAP, NNTP y FTP.	Cumple

	• Ante la detección de una posible fuga de información deben poder aplicarse el menos las siguientes acciones: Bloquear el tráfico del usuario, Bloquear el tráfico de la dirección IP de origen, registrar el evento, • En caso del bloqueo de usuarios, la solución debe permitir definir por cuánto tiempo se hará el bloqueo o en su defecto bloquear por tiempo indefinido hasta que el administrador tome una acción. • La solución debe soportar la capacidad de guardar una copia del archivo identificado como posible fuga de información. Esta copia podría ser archivada localmente o en otro dispositivo. • La solución debe permitir la búsqueda de patrones en archivos mediante la definición de expresiones regulares. • Se debe proveer la funcionalidad de filtrado de fuga de información. Dentro de las técnicas de detección se debe considerar como mínimo las siguientes: 1. Filtrado por tipo de archivo 2. Filtrado por nombre de archivo 3. Filtrado por expresiones regulares: Se detectarán los archivos según las expresiones regulares que se encuentren dentro de los mismos. 4. Fingerprinting: Se tomará una muestra del archivo que se considere como confidencial. Según esto se bloquearán archivos que sean iguales a esta muestra. 5. Watermarking: Se insertará un "sello de agua" dentro del archivo considerado como confidencial. De acuerdo a esto se analizarán los archivos en busca de este sello de agua, este se detectará incluso si el archivo sufrió cambios.	
Control de Aplicaciones	• La solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo. • La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico. • La solución debe tener un listado de al menos 1000 aplicaciones ya definidas por el fabricante. • El listado de aplicaciones debe actualizarse periódicamente. • Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log. • Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log. • Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping. • Preferentemente deben soportar mayor granularidad en las acciones.	Cumple
Inspección de Contenido SSL	• La solución debe soportar la capacidad de inspeccionar tráfico que esté siendo encriptado mediante TLS al menos para los siguientes protocolos: HTTPS, IMAPS, SMTPS, POP3S. • La inspección deberá realizarse mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle). • La inspección de contenido encriptado no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario. • Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado. • El equipo debe ser capaz de analizar contenido cifrado (SSL o SSH) para las funcionalidades de Filtrado de URLs, Control de Aplicaciones, Prevención de Fuga de Información, Antivirus e IPS.	Cumple
Controlador Inalámbrico (Wireless Controller)	• El dispositivo debe tener la capacidad de funcionar como Controlador de Wireless • En modo de Controlador de Wireless tendrá la capacidad de configurar múltiples puntos de acceso (Access Points: APs) reales de forma tal de que se comporten como uno solo. Cómo mínimo deberá controlar los SSID, roaming entre APs, configuraciones de cifrado, configuraciones de autenticación. • Debe soportar la funcionalidad de detección y mitigación de puntos de acceso (APs). Rogue Access Point Detection. • El controlador de Wireless tendrá la capacidad de configurar la asignación de direcciones IP mediante DHCP a las estaciones de trabajo conectadas a los APs. • Deberá tener la capacidad de monitorear las estaciones de trabajo, clientes wireless, conectadas a alguno de los APs. • La solución debe contar con la funcionalidad de WIDS (Wireless IDS), la capacidad de monitorear el trafico wireless para detectar y reportar posibles intentos de intrusión. • Debe contar con un sistema de aprovisionamiento de usuarios invitados para red wifi, que permita la creación sencilla de accesos para invitados, por medio de un portal independiente.	Cumple

000476

	• El equipo debe tener capacidad de que estos usuarios invitados con acceso inalámbrico, tengan la opción de colocar o no contraseña, con tiempo limitado y configurable para la expiración de la cuenta. • El controlador inalámbrico debe estar en la capacidad de balancear la carga entre los puntos de acceso (Access Points) soportando por lo menos los siguientes métodos de balanceo: Access Point Hand-off, Frequency Hand-off. • Debe contar con la capacidad de realizar Bridge SSID, permitiendo que una red inalámbrica y un segmento cableado LAN pertenezcan a la misma rubred. • El dispositivo deberá ser capaz de administrar los dispositivos wireless AP de la misma plataforma, tanto en consola CLI como a través de una interfaz grafica (GUI) • El dispositivo debe tener la capacidad de controlar varios puntos de acceso de la misma plataforma de forma remota. • El dispositivo debe poder cifrar la información que se envía hacia los puntos de acceso de la misma plataforma, sobre los cuales se esté teniendo control y gestión. • El dispositivo debe permitir la administración y manejo tanto de redes cableadas como inalámbricos dentro del mismo segmento de red. • El equipo debe tener la capacidad de reconocer y monitorear diferentes tipos de dispositivos de comunicación móvil como Smartphones Androide, Blackberry y Iphone; diferentes tipos de consolas de juego como Xbox, PS2, PS3, Wii, PSP; diferentes tipos de tabletas con SO Androide o tabletas Ipad, • El equipo debe tener la capacidad de controlar el acceso a la red de los diferentes dispositivos antes mencionados a través de ACLs por MAC • El equipo deberá permitir el crear diferentes niveles de acceso a la red en función del tipo de dispositivo que se conecte, siendo estos: Smartphones, Tabletas, Laptoos, PCs (tanto en Windows como en Linux) • El equipo debe permitir la separación de redes al menos entre usuarios internos e invitados, permitiendo la colocación de reglas en función de los dispositivos móviles conectados.	
Filtraje de tráfico VoIP, *Peer-to-Peer* y Mensajería instantánea	• Soporte a aplicaciones multimedia tales como (incluyendo) : SCCP (Skinny), H.323, SIP, Real Time Streaming Protocol (RTSP). • El dispositivo deberá técnicas de detección de P2P y programas de archivos compartidos (peer-to-peer), soportando al menos Yahoo! Messenger, MSN Messenger, ICQ y AOL Messenger para Messenger, y BitTorrent, eDonkey, GNUTella, KaZaa, Skype y WinNY para Peer-to-peer. • 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. • La solución debe contar con un ALG (Application Layer Gateway) de SIP • Debe poder hacerse inspección de encabezados de SIP • Deben poder limitarse la cantidad de requerimientos SIP que se hacen por segundo. Esto debe poder definirse por cada método SIP. • La solución debe soportar SIP HNT (Hosted NAT Transversal). • La solución deberá integrar la inspección de tráfico basado en flujo utilizando un motor de IPS dentro del mismo dispositivo para escaneo de paquetes • Deberá ser capaz de hacer inspección tráfico SSH en modo proxy explicito • La solución de seguridad podrá hacer inspección de tráfico HTTP, HTTPS y FTP sobre HTTP en modalidad proxy explicito con las funcionalidades de IPS, Antivirus, Filtrado Web, Control de Aplicaciones y DLP, todo en un mismo dispositivo • El dispositivo tendrá la opción para configurar sus interfaces integradas en modo Sniffer con funcionalidades de Filtrado Web, Control de Aplicaciones, Antivirus e IPS.	Cumple
Optimización WAN y Web Caching	• La solución deberá permitir la creación de perfiles para la aplicación de Optimización WAN e indicar bajo que protocolos se ejecutará • Deberá ser capaz de activar en modo transparente dentro de los perfiles de Optimización WAN y seleccionar un determinado grupo de usuarios para autenticación de acceso • El dispositivo deberá soportar la desfragmentación dinámica de paquetes para detectar fragmentos persistentes de distintos archivos o datos adjuntos dentro del trafico bajo protocolos desconocidos • La solución debe ser capaz de generar y aplicar perfiles de Optimización WAN para los usuarios • El dispositivo de seguridad podrá integrar contenido de inspección dentro de sus políticas de seguridad con Optimización WAN • La solución integrara dentro de cada interface la capacidad de hacer túneles de Optimización WAN	Cumple

	• Deberá ser capaz de configurar Optimización WAN en modo Activo/Pasivo • Solución capaz de aplicar web cache a tráfico HTTP y HTTPS dentro de las políticas de seguridad incluyendo también Optimización WAN y web proxy cache • Dispositivo capaz de habilitar el almacenamiento en caché web tanto en el lado del cliente y del lado de la solución • La solución podrá recibir el tráfico HTTPS en nombre del cliente, abrirá y extraerá el contenido del tráfico cifrado para inspeccionar y almacenar en cache para el envío al usuario final • El dispositivo tendrá la opción de integrar un certificado SSL determinado para la recifrado de tráfico • La solución capaz de configurar el cache de trafico HTTP y HTTPS bajo distintos puertos a los predeterminados (80 y 443) • La solución debe ser capaz de habilitar opciones para depurar la funcionalidad de Web Cache a determinadas URL.	
Alta Disponibilidad	• El dispositivo deberá soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6 • Alta Disponibilidad en modo Activo-Pasivo • Alta Disponibilidad en modo Activo-Activo • Posibilidad de definir al menos dos interfaces para sincronía • El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red • Será posible definir interfaces de gestión independientes para cada miembro en un clúster.	Cumple
Características de Administración	▪ Interface gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interface debe soportar SSL sobre HTTP (HTTPS) ▪ La interface gráfica de usuario (GUI) vía Web deberá poder estar en español y en inglés, configurable por el usuario. ▪ Interface basada en línea de comando (CLI) para administración de la solución. ▪ Puerto serial dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto. ▪ Comunicación cifrada y autenticada con usuario y contraseña, tanto como para la interfase gráfica de usuario como la consola de administración de línea de comandos (SSH o telnet) ▪ El administrador del sistema podrá tener las opciones incluidas de autenticarse vía usuario/contraseña y vía certificados digitales. ▪ Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar. ▪ El equipo ofrecerá la flexibilidad para especificar que Los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet,http o HTTPS. ▪ El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional. ▪ Soporte de SNMP versión 2 ▪ Soporte de SNMP versión 3 ▪ Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos ▪ Soporte para almacenamiento de eventos en un repositorio que pueda consultarse luego con SQL. ▪ Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall. ▪ Monitoreo de comportamiento del appliance mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red. ▪ Debe ser posible definir la dirección IP que se utilizará como origen para el tráfico iniciado desde el mismo dispositivo. Esto debe poder hacerse al menos para el tráfico de alertas, SNMP, Log y gestión. ▪ Permitir que el administrador de la plataforma pueda definir qué funcionalidades están disponibles o deshabilitadas para ser mostradas en la interfaz gráfica. ▪ Contar con facilidades de administración a través de la interfaz gráfica como listas de edición a través de click derecho. ▪ Contar con facilidades de administración a través de la interfaz gráfica como ayudantes de configuración (setup wizard).	Cumple

	▪ Contar con la posibilidad de agregar una barra superior (Top Bar) cuando los usuarios estén navegando con información como el ID de usuario, cuota de navegación utilizada, y aplicaciones que vayan en contra de las políticas de la empresa. ▪ Contar con herramientas gráficas para visualizar fácilmente las sesiones en el equipo, que permitan adicionarse por el administrador en la página inicial de la solución (dashboard), incluyendo por lo menos por defecto Top de sesiones por origen, Top de sesiones por destino, y Top de sesiones por aplicación.	
Virtualización	▪ El dispositivo deberá poder virtualizar los servicios de seguridad mediante "Virtual Systems", "Virtual Firewalls" o "Virtual Domains" ▪ La instancia virtual debe soportar por lo menos Firewall, VPN, URL Filtering, IPS y Antivirus ▪ Se debe incluir la licencia para al menos 8 (ocho) instancias virtuales dentro de la solución a proveer. ▪ Cada instancia virtual debe poder tener un administrador independiente ▪ La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales. ▪ Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red ▪ Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual ▪ Debe ser posible definir distintos servidores de log (syslog) para cada instancia virtual. ▪ Debe ser posible definir y modificar los mensajes mostrados por el dispositivo de forma independiente para cada instancia virtual. ▪ Debe ser posible definir enlaces de comunicación entre los sistemas virtuales sin que el trafico deba salir de la solución por medio de enlaces o conexiones virtuales, y estas conexiones deben poder realizarse incluso entre instancias virtuales en modo NAT y en modo Transparente.	Cumple
Análisis de Seguridad y Almacenamiento de Logs en la Nube	▪ La solución de seguridad debe contar con una solución en la nube que permita centralización de reportes, análisis de tráfico, administración de configuraciones, y almacenamiento de logs sin la necesidad de software o hardware adicional para esta función. ▪ Contar con funcionalidad de Análisis de archivos sospechosos en la nube en caso que no se cuente con suficiente información en la solución de seguridad para calificar el tráfico como legitimo o ilegitimo, por medio de técnicas de Caja de Arena o Sandboxing. ▪ Almacenamiento de Logs hasta 1 Giga por equipo incluido con capacidad de crecimiento en caso de requerirse. ▪ Debe permitir administración centralizada de todos los equipos de la solución de seguridad perimetral desde una misma interfaz. ▪ Permitir Monitoreo y alertas en tiempo real. ▪ Debe contar con Reportes predefinidos y la opción de personalización, así como contar con herramientas de análisis. ▪ Debe permitir visualizar de manera sencilla que todos los equipos de seguridad perimetral gestionados cuenten con la misma versión de firmware o sistema operativo para garantizar la homogeneidad en la red.	Cumple
Actualizaciones de plataforma	▪ La solución contara con el servicio de actualización de firmas para dispositivos sobre BYOD ▪ El dispositivo tendrá la opción de conectarse a los servidores NTP de los Laboratorios de Investigación y Actualización propietarios del mismo fabricante para actualización del horario de sistema local ▪ Sera capaz de hacer consultas a los servidores DNS de los Laboratorios de Investigación y Actualización del mismo fabricante para resolución y categorización de sitios web dentro de los perfiles para Filtrado Web ▪ Tendrá la capacidad de hacer consultas a los servidores DNS de los Laboratorios de investigación y actualización mismos del fabricante sobre reputación de direcciones IP.	Cumple
Licencia	El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, cajas de correo, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo.	Cumple
Vigencia de licencia de actualización	La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS y URL Filtering debe proveerse por al menos dos años.	Cumple
Numero de Interfaces	1 Console Port (RJ45), 2 USB Ports, 2 GE RJ45 Management Ports, 4 GE RJ45 Ports, 4 GE SFP Slots	Cumple

Throughput de Firewall	3 / 3 / 3 Gbps	Cumple
Throughput de VPN IPSec	1.3 Gbps	Cumple
Throughput de Antivirus	600 Mbps	Cumple
Throughput de IPS	350Mbps	Cumple
Tuneles dedicados	2,000	Cumple
Tuneles SSL	10,000	Cumple
Throughput VPN SSL	400 Mbps	Cumple
Sesiones Concurrentes	3.2 Mil	Cumple
Nuevas sesiones / segundo	77.000	Cumple
Políticas	10,000	Cumple
Dimensiones de Rack	1 RU	Cumple
Numero de Instancias virtuales	10 / 10	Cumple
AC Power	100 – 240V AC, 50 – 60Hz	Cumple
Consumo de poder promedio	49/83 W	Cumple
Implementación	La instalación, capacitación, provisión como así también las licencias y suscripciones a las funcionalidades solicitadas además de parametrización conformes a las licencias y trabajos necesarios para su instalación y funcionamiento correrán por cuenta del Oferente.	Cumple
Certificación Técnica Solicitada	*Al menos 1 técnico certificado, la certificación deberá estar emitida por el fabricante de la marca de la solución ofertada. *Se aceptarán como válidos los certificados emitidos a partir del año 2013.	Cumple
Plazo entrega	45 días corridos.	Cumple

La Oferta presentada por **PYTYVO COMUNICACIONES, cumple** con las especificaciones técnicas solicitadas.

000472

Se analiza la oferta técnica presentada por la empresa OLAM SRL, con las siguientes consideraciones:

REQUERIMIENTOS TÉCNICOS MÍNIMOS

Provisión del Sistema UTM	Solicitado	Exigido
Características	▪ El dispositivo debe ser un equipo de propósito específico, basado en tecnología ASIC y que sea capaz de brindar una solución de "Complete Content Protection". Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux. ▪ Capacidad de incrementar el rendimiento de VPN a través de soluciones en hardware dentro del mismo dispositivo (mediante el uso de un ASIC). ▪ Capacidad de re ensamblado de paquetes en contenido para buscar ataques o contenido prohibido, basado en hardware (mediante el uso de un ASIC). ▪ El equipo deberá poder ser configurado en modo gateway o en modo transparente en la red. En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP. ▪ El sistema operativo debe incluir un servidor de DNS que permita resolver de forma local ciertas consultas de acuerdo a la configuración del administrador. ▪ El equipo de seguridad debe soportar el uso del protocolo ICAP con el fin de poder delegar tareas a equipos terceros con el fin de liberar procesamiento del mismo.	Cumple
Firewall	• Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs. • Por granularidad y seguridad, el firewall deberá poder especificar políticas tomando en cuenta puerto físico fuente y destino. Esto es, el puerto físico fuente y el puerto físico destino deberán formar parte de la especificación de la regla de firewall. • Será posible definir políticas de firewall que sean independientes del puerto de origen y puerto de destino. • Las reglas del firewall deberán tomar en cuenta 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) de la comunicación que se está analizando. • Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino. • Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a tiempo. • Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a fechas (incluyendo día, mes y año) • Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos. • Debe poder definirse el tiempo de vida de una sesión inactiva de forma independiente por puerto y protocolo (TCP y UDP) • Capacidad de hacer traslación de direcciones estático, uno a uno, NAT. • Capacidad de hacer traslación de direcciones dinámico, muchos a uno, PAT. • Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario), • La solución deberá tener la capacidad de balancear carga entre servidores. Esto es realizar una traslación de una única dirección a múltiples direcciones de forma tal que se distribuya el tráfico entre ellas. • En la solución de balanceo de carga entre servidores, debe soportarse persistencia de sesión al menos mediante HTTP Cookie o SSL Session ID • En la solución de balanceo de carga de entre servidores deben soportarse mecanismos para detectar la disponibilidad de los servidores, de forma tal de poder evitar enviar tráfico a un servidor no disponible. • El equipo deberá permitir la creación de políticas de tipo Firewall con capacidad de seleccionar campos como dirección, identificador de usuarios o identificador de dispositivos para el caso de dispositivos móviles como smartphones y tabletas. • El equipo deberá permitir la creación de políticas de tipo VPN con capacidad de seleccionar campos como IPSEC o SSL según sea el tipo de VPN.	Cumple

	• La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP. • La solución de seguridad deberá permitir la creación de servicios de Firewall para implementar dentro de las políticas de seguridad y categorizarlos de manera personalizada • La solución será capaz de integrar los servicios dentro de las categorías de Firewall predefinidas o personalizadas y ordenarlos alfabéticamente. • El dispositivo de seguridad podrá determinar accesos y denegación a diferentes tipos de tráfico predefinidos dentro de una lista local de políticas • La solución será capaz de habilitar o deshabilitar el paso de tráfico a través de procesadores de propósito específico, si el dispositivo cuenta con estos procesadores integrados dentro del mismo • La solución podrá crear e implementar políticas de tipo Multicast y determinar el sentido de la política, así como también la habilitación del NAT dentro de cada interface del dispositivo • El dispositivo de seguridad será capaz de crear e integrar políticas contra ataques DoS las cuales se deben poder aplicar por interfaces. • El dispositivo de generar logs de cada una de las políticas aplicadas para evitar los ataques de DoS • La solución de seguridad permitirá configurar el mapeo de protocolos a puertos de manera global o especifica • La solución capaz de configurar el bloqueo de archivos o correos electrónicos por tamaño, o por certificados SSL inválidos. • El dispositivo integrara la inspección de tráfico tipo SSL y SSH bajo perfiles predefinidos o personalizados • El dispositivo será capaz de ejecutar inspección de trafico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico • Tendrá la capacidad de hacer escaneo a profundidad de trafico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis • La solución permitirá bloquear o monitorear toda la actividad de tipo Exec, Port-Forward, SSH-Shell, y X-11 SSH.	
Conectividad y Sistema de ruteo	• Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (*Relay*) de solicitudes DHCP. • Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs. • Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas. • Soporte a políticas de ruteo (policy routing). • El soporte a políticas de ruteo deberá permitir que ante la presencia de dos enlaces a Internet, se pueda decidir cuál de tráfico sale por un enlace y qué tráfico sale por otro enlace. • Soporte a ruteo dinámico RIP V1, V2, OSPF, BGP y IS-IS • Soporte a ruteo dinámico RIPng, OSPFv3 • La configuración de BGP debe soportar Autonomous System Path (AS-PATH) de 4 bytes. • Soporte de ECMP (Equal Cost Multi-Path) • Soporte de ECMP con peso. En este modo el tráfico será distribuido entre múltiples rutas pero no en forma equitativa, sino en base a los pesos y preferencias definidas por el administrador. • Soporte de ECMP basado en comportamiento. En este modo, el tráfico será enviado de acuerdo a la definición de una ruta hasta que se alcance un umbral de tráfico. En este punto se comenzará a utilizar en paralelo una ruta alternativa. • Soporte a ruteo de multicast. • La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow. • La solución podrá habilitar políticas de ruteo en IPv6 • La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6 • La solución deberá soportar la creación de políticas de tipo Firewall y VPN y subtipo por dirección IP, tipos de dispositivo y por usuario, con IPv6 • La solución será capaz de habilitar funcionalidades de UTM (Antivirus, Filtrado Web, Control de Aplicaciones, IPS, Filtrado de correo, DLP, ICAP y VoIP) dentro de las políticas creadas con direccionamiento IPv6. • El dispositivo debe integrar la autenticación por usuario o dispositivo en IPv6. • El dispositivo deberá soportar la inspección de tráfico IPv6 en modo proxy explícito. • Deberá ser capaz de integrar políticas con proxy explícito en IPv6 • La solución podrá restringir direcciones IPv6 en modo proxy explicito • Deberá hacer NAT de la red en IPv6	Cumple 000470

	• La solución será capaz de comunicar direccionamiento IPv6 a servicios con IPv4 a través de NAT • Como dispositivo de seguridad deberá soportar la inspección de tráfico IPv6 basada en flujo • La solución deberá ser capaz de habilitar políticas de seguridad con funcionalidades IPS, Filtrado Web, Control de Aplicaciones, Antivirus y DLP, para la inspección de tráfico en IPv6 basado en flujos • La solución contara con una base de administración de información interna generada por sesiones sobre IPv6 • Deberá ser capaz de habilitar la funcionalidad de Traffic Shaper por IP dentro de las políticas creadas en IPv6 • El dispositivo podrá tener la capacidad de transmitir DHCP en IPv6 • La solución tendrá la funcionalidad de habilitar DHCP en IPv6 por interface • La solución deberá contar con soporte para sincronizar por sesiones TCP en IPv6 entre dispositivos para intercambio de configuración en Alta Disponibilidad • El dispositivo podrá ser configurado mediante DHCP en IPv6 para comunicarse con un servidor TFTP donde se encontrara el archivo de configuración • El dispositivo podrá hacer la función como servidor DHCP IPv6 • La solución será capaz de configurar la autenticación por usuario por interface en IPv6.	
VPN IPSec/L2TP/PPTP	• Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site) • Soporte para IKEv2 y IKE Configuration Method • Debe soportar la configuración de túneles PPTP • Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES. • Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits • Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14. • Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256. • Posibilidad de crear VPN's entre gateways y clientes con IPSec. Esto es, VPNs IPSeC site-to-site y VPNs IPSec client-to-site. • La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN) En modo interface, la VPN IPSec deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de firewall. • Tanto para IPSec como para L2TP debe soportarse los clientes terminadores de túneles nativos de Windows y MacOS X.	Cumple
VPN SSL	• Capacidad de realizar SSL VPNs. • Soporte a certificados PKI X.509 para construcción de VPNs SSL. • Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN. • Soporte de renovación de contraseñas para LDAP y RADIUS. • Soporte a asignación de aplicaciones permitidas por grupo de usuarios • Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet. • 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. • Capacidad integrada para eliminar y/o cifrar el contenido descargado al caché de la máquina cliente (caché cleaning) • La VPN SSL integrada deberá soportar a través de algun plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS • Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL • Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente • Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios. • Los portales personalizados deberán soportar al menos la definición de: o Widgets a mostrar o Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC o Esquema de colores o Soporte para Escritorio Virtual o Política de verificación de la estación de trabajo.	Cumple

	• La VPN SSL integrada debe soportar la funcionalidad de Escritorio Virtual, entendiéndose como un entorno de trabajo seguro que previene contra ciertos ataques además de evitar la divulgación de información. • Para la configuración de cluster, en caso de caída de uno de los dispositivos, la VPN SSL que estuviera establecida, debe restablecerse en el otro dispositivo sin solicitar autentificación nuevamente.	
Traffic Shapping / QoS	• Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall • Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión • 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. • Capacidad de poder definir ancho de banda garantizado en KB por segundo • Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KB por segundo • Capacidad de para definir prioridad de tráfico, en al menos tres niveles de importancia.	Cumple
Autenticación y Certificación Digital	• Capacidad de integrarse con Servidores de Autenticación RADIUS. • Capacidad nativa de integrarse con directorios LDAP • Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es, aprovechar las credenciales del dominio de Windows bajo un concepto "Single-Sign-On" • Capacidad de autenticar usuarios para cualquier aplicación que se ejecute bajo los protocolos TCP/UDP/ICMP. Debe de mostrar solicitud de autenticación (Prompt) al menos para Web (HTTP), FTP y Telnet. • Debe ser posible definir puertos alternativos de autenticación para los protocolos http, FTP y Telnet. • Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site) • La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios. • Deben poder definirse usuarios y grupos en un repositorio local del dispositivo. • Para los administradores locales debe poder definirse la política de contraseñas que especificará como mínimo: Longitud mínima permitida, Restricciones de tipo de caracteres: numéricos, alfanuméricos, etc., Expiración de contraseña. • Debe poder limitarse la posibilidad de que dos usuarios o administradores tengan sesiones simultáneas desde distintas direcciones IP.	Cumple
Antivirus	• Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP. • El Antivirus deberá poder configurarse en modo Proxy como en modo de Flujo. En el primer caso, los archivos serán totalmente reconstruidos por el motor antes de hacer la inspección. En el segundo caso, la inspección de antivirus se hará por cada paquete de forma independiente. • Antivirus en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido. • El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6. • La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP deberá estar completamente integrada a la administración del dispositivo appliance, que permita la aplicación de esta protección por política de control de acceso. • El antivirus deberá soportar múltiples bases de datos de virus de forma tal de que el administrador defina cuál es conveniente utilizar para su implementación evaluando desempeño y seguridad. • El appliance deberá de manera opcional poder inspeccionar por todos los virus conocidos. • El Antivirus integrado deberá tener la capacidad de poner en cuarentena archivos encontrados infectados que estén circulando a través de los protocolos http, FTP, IMAP, POP3, SMTP • El Antivirus integrado tendrá la capacidad de poner en cuarentena a los clientes cuando se haya detectado que los mismos envían archivos infectados con virus. • El Antivirus deberá incluir capacidades de detección y detención de tráfico spyware, adware y otros tipos de malware/grayware que pudieran circular por la red. • El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging) para al menos MSN Messenger. • El antivirus deberá ser capaz de filtrar archivos por extensión	Cumple

000468

	• El antivirus deberá ser capaz de filtrar archivos por tipo de archivo (ejecutables por ejemplo) sin importar la extensión que tenga el archivo • Capacidad de actualización automática de firmas Antivirus mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas).	
AntiSpam	• La capacidad anti spam incluida deberá ser capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, decidir rechazar el mensaje. • La capacidad Anti Spam incluida deberá permitir especificar listas blancas (confiables, a los cuales siempre se les deberá pasar) y listas negras (no confiables, a los cuales siempre les deberá bloquear). Las listas blancas y listas negras podrán ser por dirección IP o por dirección de correo electrónico (e-mail address). • La capacidad Anti Spam deberá poder consultar una base de datos donde se revise por lo menos dirección IP del emisor del mensaje, URLs contenidos dentro del mensaje y checksum del mensaje, como mecanismos para detección de SPAM • En el caso de análisis de SMTP, los mensajes encontrados como SPAM podrán ser etiquetados o rechazados (descartados). En el caso de etiquetamiento del mensaje, debe tenerse la flexibilidad para etiquetarse en el motivo (subject) del mensaje o a través un encabezado MIME en el mensaje.	Cumple
Filtraje de URLs (URL Filtering)	• Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 75 categorías y por lo menos 54 millones de sitios web en la base de datos. • Debe poder categorizar contenido Web requerido mediante IPv6. • Filtrado de contenido basado en categorías en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido. • Configurable directamente desde la interfaz de administración del dispositivo appliance. Con capacidad para permitir esta protección por política de control de acceso. • Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al que pertenezca la conexión siendo establecida • La solución debe permitir realizar el filtrado de contenido, tanto realizando reconstrucción de toda la sesión (modo proxy) como realizando inspección paquete a paquete sin realizar reconstrucción de la comunicación (modo flujo). • Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables. Estos mensajes de remplazo deberán poder aplicarse para conexiones http y https, tanto en modo proxy como en modo flujo. • Los mensajes de remplazo deben poder ser personalizados por categoría de filtrado de contenido. • Capacidad de filtrado de scripts en páginas web (JAVA/Active X). • La solución de Filtraje de Contenido debe soportar el forzamiento de "Safe Search" o "Búsqueda Segura" independientemente de la configuración en el browser del usuario. Esta funcionalidad no permitirá que los buscadores retornen resultados considerados como controversiales. Esta funcionalidad se soportará al menos para Google, Yahoo! y Bing. • Será posible definir cuotas de tiempo para la navegación. Dichas cuotas deben poder asignarse por cada categoría y por grupos. • Será posible exceptuar la inspección de HTTPS por categoría. Debe contar con la capacidad de implementar el filtro de Educación de Youtube por Perfil de Filtro de Contenido para trafico HTTP, garantizando de manera centralizada, que todas las sesiones aceptadas por una política de seguridad con este perfil, van a poder acceder solamente a contenido de tipo Educativo en Youtbube, bloqueando cualquier tipo de contenido no Educativo. • El sistema de filtrado de URLs debe tener al menos 3 métodos de inspección: 1. Modo de Flujo: La página es inspeccionada paquete a paquete sin reconstruir la página completa. 2. Modo Proxy: La página es reconstruida completamente para ser analizada a profundidad. 3. Modo DNS: La inspección se basa únicamente en la categorización del dominio accesado. • Se debe incluir la funcionalidad de reputación basada en filtrado de URLs. • La funcionalidad de reputación busca que, al acceder a páginas de contenido no deseado (tales como Malware, pornografía, consumo de ancho de banda excesivo, etc) se asigne un puntaje a	Cumple

	cada usuario o IP cada vez visita una página de esta índole. De acuerdo a esto se extrae los usuarios que infringen las políticas de filtrado con más frecuencia con el fin de detectar zombies dentro de la red. • El sistema de filtrado de URLs debe incluir la capacidad de definir cuotas de navegación basadas en volumen de tráfico consumido. • Se debe incorporar la funcionalidad de filtrado educativo de Youtube (Youtube Education Filter) • En dicho sistema cada organismo obtiene un ID de Youtube para habilitar el contenido educativo del mismo. Se deberá insertar dicho código en la configuración de filtrado de URLs del equipo para poder habilitar únicamente el contenido educativo de Youtube.	
Protección contra intrusos (IPS)	• El Detector y preventor de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror. • Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores. • Capacidad de detección de más de 4000 ataques. • Capacidad de actualización automática de firmas IPS mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas) • El detector y preventor de intrusos deberá estar integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la prevención de intrusos. La interfaz de administración del detector y preventor de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso. • El detector y preventor de intrusos deberá soportar captar ataques por variaciones de protocolo y además por firmas de ataques conocidos (signature based / misuse detection). • Basado en análisis de firmas en el flujo de datos en la red, y deberá permitir configurar firmas nuevas para cualquier protocolo. • Actualización automática de firmas para el detector de intrusos • El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios. • Métodos de notificación: o Alarmas mostradas en la consola de administración del appliance. o Alertas vía correo electrónico. o Debe tener la capacidad de cuarentena, es decir prohibir el tráfico subsiguiente a la detección de un posible ataque. Esta cuarentena debe poder definirse al menos para el tráfico proveniente del atacante o para el tráfico del atacante al atacado. o La capacidad de cuarentena debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma "indefinida", hasta que un administrador tome una acción al respecto. o Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP. • Se debe incluir protección contra amenazas avanzadas y persistentes (Advanced Persistent Threats). Dentro de estos controles se debe incluir: • Protección contra botnets: Se deben 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. • Sandboxing: La funcionalidad de Sandbox hace que el archivo sea ejecutado en un ambiente seguro para analizar su comportamiento y, a base del mismo, tomar una acción sobre el mismo.	Cumple
Prevención de Fuga de Información (DLP)	• La solución debe ofrecer la posibilidad de definir reglas que permitan analizar los distintos archivos que circulan a través de la red en búsqueda de información confidencial. ▪ La funcionalidad debe soportar el análisis de archivos del tipo: MS-Word, PDF, Texto, Archivos comprimidos. • Debe soportarse el escaneo de archivos en al menos los siguientes protocolos: HTTP, POP3, SMTP, IMAP, NNTP y FTP.	Cumple

	• Ante la detección de una posible fuga de información deben poder aplicarse el menos las siguientes acciones: Bloquear el tráfico del usuario, Bloquear el tráfico de la dirección IP de origen, registrar el evento, • En caso del bloqueo de usuarios, la solución debe permitir definir por cuánto tiempo se hará el bloqueo o en su defecto bloquear por tiempo indefinido hasta que el administrador tome una acción. • La solución debe soportar la capacidad de guardar una copia del archivo identificado como posible fuga de información. Esta copia podría ser archivada localmente o en otro dispositivo. • La solución debe permitir la búsqueda de patrones en archivos mediante la definición de expresiones regulares. • Se debe proveer la funcionalidad de filtrado de fuga de información. Dentro de las técnicas de detección se debe considerar como mínimo las siguientes: 1. Filtrado por tipo de archivo 2. Filtrado por nombre de archivo 3. Filtrado por expresiones regulares: Se detectarán los archivos según las expresiones regulares que se encuentren dentro de los mismos. 4. Fingerprinting: Se tomará una muestra del archivo que se considere como confidencial. Según esto se bloquearán archivos que sean iguales a esta muestra. 5. Watermarking: Se insertará un "sello de agua" dentro del archivo considerado como confidencial. De acuerdo a esto se analizarán los archivos en busca de este sello de agua, este se detectará incluso si el archivo sufrió cambios.	
Control de Aplicaciones	• La solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo. • La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico. • La solución debe tener un listado de al menos 1000 aplicaciones ya definidas por el fabricante. • El listado de aplicaciones debe actualizarse periódicamente. • Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log. • Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log. • Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping. • Preferentemente deben soportar mayor granularidad en las acciones.	Cumple
Inspección de Contenido SSL	• La solución debe soportar la capacidad de inspeccionar tráfico que esté siendo encriptado mediante TLS al menos para los siguientes protocolos: HTTPS, IMAPS, SMTPS, POP3S. • La inspección deberá realizarse mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle). • La inspección de contenido encriptado no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario. • Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado. • El equipo debe ser capaz de analizar contenido cifrado (SSL o SSH) para las funcionalidades de Filtrado de URLs, Control de Aplicaciones, Prevención de Fuga de Información, Antivirus e IPS.	Cumple
Controlador Inalámbrico (Wireless Controller)	• El dispositivo debe tener la capacidad de funcionar como Controlador de Wireless • En modo de Controlador de Wireless tendrá la capacidad de configurar múltiples puntos de acceso (Access Points: APs) reales de forma tal de que se comporten como uno solo. Cómo mínimo deberá controlar los SSID, roaming entre APs, configuraciones de cifrado, configuraciones de autenticación. • Debe soportar la funcionalidad de detección y mitigación de puntos de acceso (APs). Rogue Access Point Detection. • El controlador de Wireless tendrá la capacidad de configurar la asignación de direcciones IP mediante DHCP a las estaciones de trabajo conectadas a los APs. • Deberá tener la capacidad de monitorear las estaciones de trabajo, clientes wireless, conectadas a alguno de los APs. • La solución debe contar con la funcionalidad de WIDS (Wireless IDS), la capacidad de monitorear el trafico wireless para detectar y reportar posibles intentos de intrusión. • Debe contar con un sistema de aprovisionamiento de usuarios invitados para red wifi, que permita la creación sencilla de accesos para invitados, por medio de un portal independiente.	Cumple

	• El equipo debe tener capacidad de que estos usuarios invitados con acceso inalámbrico, tengan la opción de colocar o no contraseña, con tiempo limitado y configurable para la expiración de la cuenta. • El controlador inalámbrico debe estar en la capacidad de balancear la carga entre los puntos de acceso (Access Points) soportando por lo menos los siguientes métodos de balanceo: Access Point Hand-off, Frequency Hand-off. • Debe contar con la capacidad de realizar Bridge SSID, permitiendo que una red inalámbrica y un segmento cableado LAN pertenezcan a la misma rubred. • El dispositivo deberá ser capaz de administrar los dispositivos wireless AP de la misma plataforma, tanto en consola CLI como a través de una interfaz grafica (GUI) • El dispositivo debe tener la capacidad de controlar varios puntos de acceso de la misma plataforma de forma remota. • El dispositivo debe poder cifrar la información que se envía hacia los puntos de acceso de la misma plataforma, sobre los cuales se esté teniendo control y gestión. • El dispositivo debe permitir la administración y manejo tanto de redes cableadas como inalámbricos dentro del mismo segmento de red. • El equipo debe tener la capacidad de reconocer y monitorear diferentes tipos de dispositivos de comunicación móvil como Smartphones Androide, Blackberry y Iphone; diferentes tipos de consolas de juego como Xbox, PS2, PS3, Wii, PSP; diferentes tipos de tabletas con SO Androide o tabletas Ipad, • El equipo debe tener la capacidad de controlar el acceso a la red de los diferentes dispositivos antes mencionados a través de ACLs por MAC • El equipo deberá permitir el crear diferentes niveles de acceso a la red en función del tipo de dispositivo que se conecte, siendo estos: Smartphones, Tabletas, Laptoos, PCs (tanto en Windows como en Linux) • El equipo debe permitir la separación de redes al menos entre usuarios internos e invitados, permitiendo la colocación de reglas en función de los dispositivos móviles conectados.	
Filtraje de tráfico VoIP, *Peer-to-Peer* y Mensajería instantánea	• Soporte a aplicaciones multimedia tales como (incluyendo) : SCCP (Skinny), H.323, SIP, Real Time Streaming Protocol (RTSP). • El dispositivo deberá técnicas de detección de P2P y programas de archivos compartidos (peer-to-peer), soportando al menos Yahoo! Messenger, MSN Messenger, ICQ y AOL Messenger para Messenger, y BitTorrent, eDonkey, GNUTella, KaZaa, Skype y WinNY para Peer-to-peer. • 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. • La solución debe contar con un ALG (Application Layer Gateway) de SIP • Debe poder hacerse inspección de encabezados de SIP • Deben poder limitarse la cantidad de requerimientos SIP que se hacen por segundo. Esto debe poder definirse por cada método SIP. • La solución debe soportar SIP HNT (Hosted NAT Transversal). • La solución deberá integrar la inspección de tráfico basado en flujo utilizando un motor de IPS dentro del mismo dispositivo para escaneo de paquetes • Deberá ser capaz de hacer inspección tráfico SSH en modo proxy explicito • La solución de seguridad podrá hacer inspección de tráfico HTTP, HTTPS y FTP sobre HTTP en modalidad proxy explicito con las funcionalidades de IPS, Antivirus, Filtrado Web, Control de Aplicaciones y DLP, todo en un mismo dispositivo • El dispositivo tendrá la opción para configurar sus interfaces integradas en modo Sniffer con funcionalidades de Filtrado Web, Control de Aplicaciones, Antivirus e IPS.	Cumple
Optimización WAN y Web Caching	• La solución deberá permitir la creación de perfiles para la aplicación de Optimización WAN e indicar bajo que protocolos se ejecutará • Deberá ser capaz de activar en modo transparente dentro de los perfiles de Optimización WAN y seleccionar un determinado grupo de usuarios para autenticación de acceso • El dispositivo deberá soportar la desfragmentación dinámica de paquetes para detectar fragmentos persistentes de distintos archivos o datos adjuntos dentro del trafico bajo protocolos desconocidos • La solución debe ser capaz de generar y aplicar perfiles de Optimización WAN para los usuarios • El dispositivo de seguridad podrá integrar contenido de inspección dentro de sus políticas de seguridad con Optimización WAN • La solución integrara dentro de cada interface la capacidad de hacer túneles de Optimización WAN	Cumple

Gu 464

	• Deberá ser capaz de configurar Optimización WAN en modo Activo/Pasivo • Solución capaz de aplicar web cache a tráfico HTTP y HTTPS dentro de las políticas de seguridad incluyendo también Optimización WAN y web proxy cache • Dispositivo capaz de habilitar el almacenamiento en caché web tanto en el lado del cliente y del lado de la solución • La solución podrá recibir el tráfico HTTPS en nombre del cliente, abrirá y extraerá el contenido del tráfico cifrado para inspeccionar y almacenar en cache para el envío al usuario final • El dispositivo tendrá la opción de integrar un certificado SSL determinado para la recifrado de tráfico • La solución capaz de configurar el cache de trafico HTTP y HTTPS bajo distintos puertos a los predeterminados (80 y 443) • La solución debe ser capaz de habilitar opciones para depurar la funcionalidad de Web Cache a determinadas URL.	
Alta Disponibilidad	• El dispositivo deberá soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6 • Alta Disponibilidad en modo Activo-Pasivo • Alta Disponibilidad en modo Activo-Activo • Posibilidad de definir al menos dos interfaces para sincronía • El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red • Será posible definir interfaces de gestión independientes para cada miembro en un clúster.	Cumple
Características de Administración	▪ Interface gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interface debe soportar SSL sobre HTTP (HTTPS) ▪ La interface gráfica de usuario (GUI) vía Web deberá poder estar en español y en inglés, configurable por el usuario. ▪ Interface basada en línea de comando (CLI) para administración de la solución. ▪ Puerto serial dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto. ▪ Comunicación cifrada y autenticada con usuario y contraseña, tanto como para la interfase gráfica de usuario como la consola de administración de línea de comandos (SSH o telnet) ▪ El administrador del sistema podrá tener las opciones incluidas de autenticarse vía usuario/contraseña y vía certificados digitales. ▪ Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar. ▪ El equipo ofrecerá la flexibilidad para especificar que Los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet,http o HTTPS. ▪ El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional. ▪ Soporte de SNMP versión 2 ▪ Soporte de SNMP versión 3 ▪ Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos ▪ Soporte para almacenamiento de eventos en un repositorio que pueda consultarse luego con SQL. ▪ Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall. ▪ Monitoreo de comportamiento del appliance mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red. ▪ Debe ser posible definir la dirección IP que se utilizará como origen para el tráfico iniciado desde el mismo dispositivo. Esto debe poder hacerse al menos para el tráfico de alertas, SNMP, Log y gestión. ▪ Permitir que el administrador de la plataforma pueda definir qué funcionalidades están disponibles o deshabilitadas para ser mostradas en la interfaz gráfica. ▪ Contar con facilidades de administración a través de la interfaz gráfica como listas de edición a través de click derecho. ▪ Contar con facilidades de administración a través de la interfaz gráfica como ayudantes de configuración (setup wizard).	Cumple

000463

	▪ Contar con la posibilidad de agregar una barra superior (Top Bar) cuando los usuarios estén navegando con información como el ID de usuario, cuota de navegación utilizada, y aplicaciones que vayan en contra de las políticas de la empresa. ▪ Contar con herramientas gráficas para visualizar fácilmente las sesiones en el equipo, que permitan adicionarse por el administrador en la página inicial de la solución (dashboard), incluyendo por lo menos por defecto Top de sesiones por origen, Top de sesiones por destino, y Top de sesiones por aplicación.	
Virtualización	▪ El dispositivo deberá poder virtualizar los servicios de seguridad mediante "Virtual Systems", "Virtual Firewalls" o "Virtual Domains" ▪ La instancia virtual debe soportar por lo menos Firewall, VPN, URL Filtering, IPS y Antivirus ▪ Se debe incluir la licencia para al menos 8 (ocho) instancias virtuales dentro de la solución a proveer. ▪ Cada instancia virtual debe poder tener un administrador independiente ▪ La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales. ▪ Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red ▪ Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual ▪ Debe ser posible definir distintos servidores de log (syslog) para cada instancia virtual. ▪ Debe ser posible definir y modificar los mensajes mostrados por el dispositivo de forma independiente para cada instancia virtual. ▪ Debe ser posible definir enlaces de comunicación entre los sistemas virtuales sin que el trafico deba salir de la solución por medio de enlaces o conexiones virtuales, y estas conexiones deben poder realizarse incluso entre instancias virtuales en modo NAT y en modo Transparente.	Cumple
Análisis de Seguridad y Almacenamiento de Logs en la Nube	▪ La solución de seguridad debe contar con una solución en la nube que permita centralización de reportes, análisis de tráfico, administración de configuraciones, y almacenamiento de logs sin la necesidad de software o hardware adicional para esta función. ▪ Contar con funcionalidad de Análisis de archivos sospechosos en la nube en caso que no se cuente con suficiente información en la solución de seguridad para calificar el tráfico como legitimo o llegitimo, por medio de técnicas de Caja de Arena o Sandboxing. ▪ Almacenamiento de Logs hasta 1 Giga por equipo incluido con capacidad de crecimiento en caso de requerirse. ▪ Debe permitir administración centralizada de todos los equipos de la solución de seguridad perimetral desde una misma interfaz. ▪ Permitir Monitoreo y alertas en tiempo real. ▪ Debe contar con Reportes predefinidos y la opción de personalización, así como contar con herramientas de análisis. ▪ Debe permitir visualizar de manera sencilla que todos los equipos de seguridad perimetral gestionados cuenten con la misma versión de firmware o sistema operativo para garantizar la homogeneidad en la red.	Cumple
Actualizaciones de plataforma	▪ La solución contara con el servicio de actualización de firmas para dispositivos sobre BYOD ▪ El dispositivo tendrá la opción de conectarse a los servidores NTP de los Laboratorios de Investigación y Actualización propietarios del mismo fabricante para actualización del horario de sistema local ▪ Sera capaz de hacer consultas a los servidores DNS de los Laboratorios de Investigación y Actualización del mismo fabricante para resolución y categorización de sitios web dentro de los perfiles para Filtrado Web ▪ Tendrá la capacidad de hacer consultas a los servidores DNS de los Laboratorios de investigación y actualización mismos del fabricante sobre reputación de direcciones IP.	Cumple
Licencia	El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, cajas de correo, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo.	Cumple
Vigencia de licencia de actualización	La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS y URL Filtering debe proveerse por al menos dos años.	Cumple
Numero de Interfaces	1 Console Port (RJ45), 2 USB Ports, 2 GE RJ45 Management Ports, 4 GE RJ45 Ports, 4 GE SFP Slots	Cumple

000462

Numero de Interfaces	1 Console Port (RJ45), 2 USB Ports, 2 GE RJ45 Management Ports, 4 GE RJ45 Ports, 4 GE SFP Slots	Cumple
Throughput de Firewall	3 / 3 / 3 Gbps	Cumple
Throughput de VPN IPSec	1.3 Gbps	Cumple
Throughput de Antivirus	600 Mbps	Cumple
Throughput de IPS	350Mbps	Cumple
Tuneles dedicados	2,000	Cumple
Tuneles SSL	10,000	Cumple
Throughput VPN SSL	400 Mbps	Cumple
Sesiones Concurrentes	3.2 Mil	Cumple
Nuevas sesiones / segundo	77.000	Cumple
Politicas	10,000	Cumple
Dimensiones de Rack	1 RU	Cumple
Numero de Instancias virtuales	10 / 10	Cumple
AC Power	100 – 240V AC, 50 – 60Hz	Cumple
Consumo de poder promedio	49/83 W	Cumple
Implementación	La instalación, capacitación, provisión como así también las licencias y suscripciones a las funcionalidades solicitadas además de parametrización conformes a las licencias y trabajos necesarios para su instalación y funcionamiento correrán por cuenta del Oferente.	Cumple
Certificación Técnica Solicitada	*Al menos 1 técnico certificado, la certificación deberá estar emitida por el fabricante de la marca de la solución ofertada. *Se aceptarán como válidos los certificados emitidos a partir del año 2013. *Certificaciones adicionales relacionadas a la función requerida;	Cumple
Plazo entrega	45 días corridos.	Cumple

La Oferta presentada por la empresa **OLAM SRL, cumple** con las especificaciones técnicas solicitadas.

Atentamente,

GERARDO FISCHER
Director
Dirección de Informática
y Tecnología

000461

Nota SEPRELAD/DGAF N° 253/2016

Asunción, 11 de noviembre de 2016

Señores
TEISA
Teléfono: 6164000
Cecilio Da Silva N° 1001
Asunción – Paraguay

Ref.: Llamado a Contratación Directa N° 18/2016 "Adquisición de un Equipo de Seguridad de Red Informática", Id: 317.428

Tengo el agrado de dirigirme usted, con relación a la oferta presentada por vuestra empresa, en el marco del llamado de referencia, de manera a solicitar la presentación de los siguientes documentos exigida en la Carta de Invitación y sus Anexos:

1) Currículo del o los técnicos certificados en la marca cotizada

Las mismas deberán ser entregadas en un plazo de 48 horas, contadas a partir de la recepción de esta notificación, en las oficinas de la SEPRELAD, sito en la Avenida Federación Rusa y Augusto Roa Bastos, Edificio del Banco Central del Paraguay, Sector Cultural.

Sin otro particular, aprovecho la oportunidad para saludarlo muy atentamente.

SECRETARIA DE PREVENCION DE LAVADO DE DINERO O BIENES
DIRECCION GENERAL DE ADMINISTRACION Y FINANZAS
SEPRELAD

CARLOS HUMBERTO ZARZA
Director General Interino
Dirección General de Administración y Finanzas

00344

Asunción, 14 de Noviembre del 2016

Señores
Secretaría de Prevención de Lavado de Dinero o Bienes
Att.: Sr. Carlos Humberto Zarza, Director General Interirno
Dirección General de Administración y Finanazas
Presente

Ref.: Contratación Directa Nº 18/2016 – "Adquisición de un Equipo de Seguridad de Red Informática" – ID Nro. 317.428

De nuestra mayor consideración:

Por medio de la presente tenemos el agrado de dirigimos a Uds. en respuesta a su Nota SEPRELAD/DGAF Nº 253/2016 de fecha 11/11/2016 donde solicitan la presentación de documentos dentro del marco de la Contratación de referencia, y para dar cumplimiento a lo solicitados adjuntamos lo siguiente:

- Copias de Curriculo de los técnicos certificados en la marca ofertada.

Sin otro particular saludamos a ustedes muy atentamente,

Elbio Oviedo
Representante Legal

DIRECCIÓN GENERAL DE ADMINISTRACIÓN Y FINANZAS
Expediente Nº: 1421 Fecha: 14/11/16 Hora: 09:44
Recibido por: Derlis Delgado Firma:
☐ Secretaría Ejecutiva ☐ Presupuesto ☐ Contabilidad
☒ UOC ☐ Adm. del Personal ☐ Tesorería
☐ Patrimonio ☐ Rendición de Cuentas ☐ Servicios Generales
☐ Capacitación y Bien. ☐ Inventario y Ctrol. de Bien. ☐ Otros
☐ Informar ☐ Procesar ☐ Archivar
☐

CARLOS HUMBERTO ZARZA
Director General Interino
Dirección General de Administración y Finanzas
SEPRELAD

000388

Cecilio Da Silva 1001 esq/ Federación Rusa - Teléfono + 595 21 616 40 00 Fax : +595 21 616 41 09
Web: www.teisa.com.py Email: info@teisa.com.py
Asunción – Paraguay

000346

Pytyvo Telecomunicaciones S. A.

11 de setiembre 860 c/ Soldado Ovelar
Teléfono: 021 237-6485
ventas@pytyvo.com
www.pytyvo.com

PARA: SEPRELAD - Dirección General de Administración y Finanzas

ATENCION: Sra. Araceli Figueredo - UOC

FECHA: 15 de noviembre de 2016

REFERENCIA: Entrega de documentos

De nuestra consideración;

Hacemos entrega de los siguientes documentos solicitados;

- ✓ 3 copias de Facturas de venta de equipos Fortinet
- ✓ 1 constancia de haber proveído equipos Fortinet de la Empresa EMERSA
- ✓ 1 constancia de haber proveído equipos a Aldeas Infantiles SOS Paraguay
- ✓ Certificado Técnico Fortinet.

Atentamente.

Marcelo Fernández Robles
Gerente Comercial

DIRECCIÓN GENERAL DE ADMINISTRACIÓN Y FINANZAS
Expediente N°: 1962 Fecha: 15.11.16 Hora: 11:55
Recibido por: Hugo Vera Firma:
☐ Secretaría Ejecutiva ☐ Presupuesto ☐ Contabilidad
☒ UOC ☐ Adm. del Personal ☐ Tesorería
☐ Patrimonio ☐ Rendición de Cuentas ☐ Servicios Generales
☐ Capacitación y Bien. ☐ Inventario y Ctrol. de Bien. ☐ Otros
☐ Informar ☐ Procesar ☐ Archivar
☐

Pytyvo Telecomunicaciones S. A.

CARLOS HUMBERTO ZARZA
Director General Interino
Dirección General de Administración y Finanzas
SEPRELAD

000459

Microsoft GOLD CERTIFIED Partner

GFi GOLD Authorised reseller

www.olam.com OLAM SRL

symantec.

NetSupport Incorporated

00001

Asunción; 14 de noviembre de 2016

Señores

SECRETARÍA DE PREVENCIÓN DE LAVADO DE DINERO O BIENES (SEPRELAD)

Unidad Operativa de Contrataciones

REF.: NOTA SEPRELAD DGAF N° 255/2016

Por medio de la presente, en representación de la empresa OLAM SRL con RUC N° 80013217-3, en mi carácter de Apoderado Legal, condición que acredito con los documentos en estado activo en la constancia **SIPE N° 1427928** En el marco del llamado ***CD 18/2016 "ADQUISICIÓN DE UN EQUIPO DE SEGURIDAD DE RED INFORMÁTICA".*** **ID N° 317.428,** remitimos los siguientes documentos formales solicitados;

- Curriculo del técnico certificado en la marca cotizada, acompañados de sus certificados respectivos.
- Copias de Contratos años (2013, 2014 y 2015).
- Catálogos e impresos descriptivos del equipo ofertado.

Sin otro particular, me despido atentamente.

Manfredo Deligdisch
Apoderado Legal
OLAM SRL

DIRECCIÓN GENERAL DE ADMINISTRACIÓN Y FINANZAS
Expediente N°: 1944 Fecha: 15-11-16 Hora: 10-25
Recibido por: Hugo Vera Firma:
☐ Secretaria Ejecutiva ☐ Presupuesto ☐ Contabilidad
☒ UOC ☐ Adm. del Personal ☐ Tesorería
☐ Patrimonio ☐ Rendición de Cuentas ☐ Servicios Generales
☐ Capacitación y Bien. ☐ Inventario y Ctrol. de Bien. ☐ Otros
☐ Informar ☐ Procesar ☐ Archivar
☐

OLAM S.R.L. – Prof. Francisco Chávez N° 189 - Tel/Fax: 595 (21) 605 074 – Asunción – Paraguay
http://www.olam.com – email licitaciones@olam.com.py

CARLOS HUMBERTO ZARZA
Director General Interino
Dirección General de Administración y Finanzas
SEPRELAD

Fo. 450