JL Security Technologies
JARET NAUN MORAN SORTO
VENTA DE MAQUINARIA Y EQUIPO DE OFICINA COMPUTADORAS Y SUS COMPONENTES INCLUYE SOFTWARE, CONSULTADORES DE EQUIPO Y PROGRAMAS DE INFORMATICA

[redacted]

FACTURA
Serie Autorizada: 17DS000F1 al 17DS000F300
Nº 0246
REG [redacted]
NIT: [redacted]
Autorización de Imprenta No. 599 D.G.I.I. / 18-11-94

FECHA: 09/08/2018

CLIENTE: MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL

DIRECCION: Alameda Juan Pablo II y 17 Av Norte, Edificio 3, Nivel 1, Plan Maestro, Centro de Gobierno

DUI o NIT: _____ CONDICIONES DE PAGO: Crédito 30 días

CANT.	DESCRIPCION	PRECIO UNITARIO	VENTAS NO SUJETAS	VENTAS EXENTAS	VENTAS GRABADAS
1	19 Equipos de Seguridad Perimetral Marca Hillstone 2-modelo T1860 12- modelo E-1700 2Gbps 5-modelo E1700 1.5Gbps	$47,032.00			$47,032.00
1	19 Licencias para Equipos de Seguridad Perimetral Marca Hillstone 2-modelo T1860 12- modelo E-1700 2Gbps 5-modelo E1700 1.5Gbps	$5,225.84			$ 5,225.84
	Según Contrato MTPS 18-2018 Referente a Libre Gestión LG MTPS 12-2018 "ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"				

SON: CINCUENTA Y UN MIL SETECIENTOS NOVENTA Y CINCO DÓLARES 38/100
OPERACIONES SUPERIORES O IGUALES A $200.00

SUMAS	$52,257.84
VENTAS EXENTAS	
VENTAS NO SUJETAS	
SUB-TOTAL	$52,257.84
(-) IVA RETENIDO	$462.46
VENTA TOTAL	$51,795.38

NOMBRE:
DUI ó NIT:
FIRMA RECIBIDO

NOMBRE:
DUI ó NIT:
FIRMA ENTREGADO

[redacted]

ORIGINAL - Blanco - EMISOR
DUPLICADO - Celeste - CLIENTE

421

JL Security Technologies

JARET NAUN MORAN SORTO

VENTA DE MAQUINARIA Y EQUIPO DE OFICINA COMPUTADORAS Y SUS COMPONENTES INCLUYE SOFTWARE, CONSULTADORES DE EQUIPO Y PROGRAMAS DE INFORMATICA

Security Technologies

[redacted]

FACTURA

Serie Autorizada: 17DS000F1 al 17DS000F300

Nº 0246

[redacted]

Autorización de Imprenta No. 599 D.G.I. / 16-11-94

FECHA: 09/08/2018

CLIENTE: MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL

DIRECCION: Alameda Juan Pablo II y 17 Av Norte, Edificio 3, Nivel 1, Plan Maestro, Centro de Gobierno

DUI o NIT: _____ CONDICIONES DE PAGO: Crédito 30 días

CANT.	DESCRIPCION	PRECIO UNITARIO	VENTAS NO SUJETAS	VENTAS EXENTAS	VENTAS GRABADAS
1	19 Equipos de Seguridad Perimetral Marca Hillstone 2-modelo T1860 12- modelo E-1700 2Gbps 5-modelo E1700 1.5Gbps	$47,032.00			$47,032.00
1	19 Licencias para Equipos de Seguridad Perimetral Marca Hillstone 2-modelo T1860 12- modelo E-1700 2Gbps 5-modelo E1700 1.5Gbps	$5,225.84			$ 5,225.84
	Según Contrato MTPS 18-2018 Referente a Libre Gestión LG MTPS 12-2018 "ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"				

SON: CINCUENTA Y UN MIL SETECIENTOS NOVENTA Y CINCO DÓLARES 38/100

OPERACIONES SUPERIORES O IGUALES A $200.00

SUMAS	$52,257.84
VENTAS EXENTAS	
VENTAS NO SUJETAS	
SUB-TOTAL	$52,257.84
(-) IVA RETENIDO	$462.46
VENTA TOTAL	$51,795.38

NOMBRE:
DUI ó NIT: _____ FIRMA RECIBIDO

NOMBRE:
DUI ó NIT: _____ FIRMA ENTREGADO

[redacted]

ORIGINAL - Blanco - EMISOR
DUPLICADO - Celeste - CLIENTE

LA CENTRAL
SEGUROS Y FIANZAS
Su Centro de confianza

LA CENTRAL DE SEGUROS Y FIANZAS, SOCIEDAD ANONIMA

GARANTIA DE BUEN FUNCIONAMIENTO Y CALIDAD DE LOS BIENES

Fianza N°. 317,211 **Monto $ 5,225.78** **Vigencia 08/08/2018 - 08/08/2019**
Solicitud N°. 338,132

Afianzado **JARET NAUN MORAN SORTO**

Beneficiario **MINISTERIO DE TRABAJO Y PREVISION SOCIAL**

[redacted], mayor de edad, [redacted], del domicilio de [redacted] Departamento de [redacted], actuando en nombre y representación en mi carácter de Apoderada Especial de la Sociedad "LA CENTRAL DE SEGUROS Y FIANZAS, SOCIEDAD ANONIMA", de este domicilio, en adelante llamada "La Fiadora", por el presente documento OTORGO: 1) Que la Sociedad que represento, sujetándose a las condiciones particulares más adelante descritas, se constituye FIADORA de: JARET NAUN MORAN SORTO, en favor del MINISTERIO DE TRABAJO Y PREVISION SOCIAL, del domicilio de San Salvador y 2) OBLIGACIONES GARANTIZADAS, MONTO Y CIRCUNSTANCIAS DE LA GARANTIA: La fiadora se constituye garante y principal pagadora hasta por la suma de CINCO MIL DOSCIENTOS VEINTICINCO DOLARES CON SETENTA Y OCHO CENTAVOS DE DOLAR DE LOS ESTADOS UNIDOS DE AMERICA, a favor del MINISTERIO DE TRABAJO Y PREVISION SOCIAL, quien en el curso de esta fianza se denominará "La Institución Contratante", para garantizar que éste reciba a su entera satisfacción y buen funcionamiento y calidad de los Bienes que se encuentran amparados en el CONTRATO MTPS DIECIOCHO-DOS MIL DIECIOCHO, referente a la "ADQUISICIÓN DE DIECINUEVE EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS", derivado de la LIBRE GESTIÓN LG MTPS DOCE-DOS MIL DIECIOCHO, ACTA DE RECEPCIÓN de fecha ocho de agosto de dos mil dieciocho, derivado de las obligaciones contractuales por parte de JARET NAUN MORAN SORTO, mayor de edad, [redacted] del domicilio [redacted], Departamento de [redacted] para con La Institución Contratante. La vigencia de esta fianza será por el plazo de DOCE MESES, contado a partir del OCHO DE AGOSTO DEL DOS MIL DIECIOCHO HASTA EL OCHO DE AGOSTO DEL DOS MIL DIECINUEVE. Es entendido y convenido que en caso de reclamo se cancelará únicamente el valor del equipo defectuoso al momento del reclamo. Vencido el plazo antes mencionado y de no haber reclamo alguno, durante el período, quedará extinguida la responsabilidad de la fiadora, dándose por cancelada la presente garantía aunque el documento original no fuere devuelto. Para los efectos legales de la presente garantía, la fiadora señala como domicilio especial el de esta ciudad, renuncia al beneficio de excusión de bienes, al derecho de apelar del decreto de embargo sentencia de remate y de cualquier otra providencia alzable del juicio, relevando al depositario que nombre La Institución Contratante, de la obligación de rendir fianza. Esta garantía está regulada por las disposiciones de los Artículos del Código de Comercio del 1539 al 1550. En fe de lo cual, firmo la presente en San Salvador, el día nueve de agosto del dos mil dieciocho.

[redacted]

[redacted]

la ciudad de San Salvador, a las once horas y cincuenta y dos minutos del día nueve de agosto del dos mil dieciocho. Ante mí, [redacted] Notario, de este domicilio, comparece [redacted] quien es de [redacted] años de edad, [redacted] del domicilio de San Salvador, Departamento de San Salvador, persona a quien conozco e identifico, por ser portadora de su Documento Único de Identidad NUMERO CERO CERO OCHO CUATRO SEIS CUATRO SEIS UNO-CUATRO, y con Número de Identificación Tributaria cero seiscientos ocho-ciento veinte mil cuatrocientos ochenta-ciento dos-cero, quien actúa en nombre y representación en su carácter de Apoderada Especial de "LA CENTRAL DE SEGUROS Y FIANZAS, SOCIEDAD ANONIMA", que podrá abreviarse "LA CENTRAL DE FIANZAS Y SEGUROS, S.A.", "LA CENTRAL DE SEGUROS, S.A.", "LA CENTRAL DE FIANZAS, S.A." y/o "LA CENTRAL DE SEGUROS Y FIANZAS, S.A.", con Número de Identificación Tributaria cero seiscientos catorce-ciento cuarenta mil setecientos ochenta y tres-cero cero uno-ocho, de este domicilio, de cuya personería DOY FE de ser legítima y suficiente por haber tenido a la vista el Testimonio de Escritura Pública de Poder Especial Administrativo, otorgado en esta ciudad a las once horas y cuarenta minutos del día veinte de abril de dos mil dieciséis, ante los oficios del Notario [redacted] por el Ingeniero [redacted] A, actuando en su calidad de [redacted] de la Junta Directiva y Representante Legal de dicha Sociedad Anónima, a favor de la compareciente para que pueda comparecer a otorgar entre otros, actos como el presente. En dicho Poder, el Notario autorizante dio fe de la personería con que actuó el Ingeniero [redacted] y de la existencia legal de la Sociedad Anónima. El poder relacionado, se encuentra inscrito en el Registro de Comercio, bajo el NUMERO [redacted] del Libro [redacted] del Registro de Otros Contratos Mercantiles; y ME DICE: Que en el carácter y calidad en que comparece a nombre de su representada la cual se constituye FIADORA de: [redacted] mayor de edad, [redacted] del domicilio legal de [redacted] Departamento de [redacted], que en adelante se llamará "El Contratista", a favor del MINISTERIO DE TRABAJO Y PREVISION SOCIAL, del domicilio de [redacted] que se denominará "La Institución Contratante", hasta por la suma de CINCO MIL DOSCIENTOS VEINTICINCO DOLARES CON SETENTA Y OCHO CENTAVOS DE DOLAR DE LOS ESTADOS UNIDOS DE AMERICA, para garantizar que éste reciba a su entera satisfacción y buen Funcionamiento y Calidad de los Bienes, que se encuentran amparados en el CONTRATO MTPS DIECIOCHO-DOS MIL DIECIOCHO, referente a la "ADQUISICIÓN DE DIECINUEVE EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS", derivado de la LIBRE GESTIÓN LG MTPS DOCE-DOS MIL DIECIOCHO, ACTA DE RECEPCIÓN de fecha ocho de agosto de dos mil dieciocho, derivado de las obligaciones contractuales por parte del contratista para con La Institución Contratante; esta fianza estará vigente por el plazo de DOCE MESES, contado a partir del día OCHO DE AGOSTO DEL DOS MIL DIECIOCHO HASTA EL OCHO DE AGOSTO DEL DOS MIL DIECINUEVE; reconociendo los demás conceptos y renuncias que se mencionan en el documento de fianza que se autentica; y yo el Notario también doy fe: Que la firma que se lee "[redacted]", es auténtica por haber sido puesta a mi presencia por la compareciente, a quien expliqué los efectos legales de esta acta notarial que consta de dos hojas útiles y leído que le hube lo escrito íntegramente y en un solo acto, ratifica su contenido y firmamos. DOY FE.-

[redacted]

[redacted]

[redacted]

415

Imprimir
Imprimir para LAIP

	GOBIERNO DE EL SALVADOR	
Ramo de Trabajo y Previsión Social	UNIDAD DE ADQUISICIONES	PREVISION NO:null
UACI del Ministerio de Trabajo	Y CONTRATACIONES INSTITUCIONAL	
	-	

ORDEN DE PEDIDO

Lugar y Fecha:	17 Av. Norte y Alameda Juan Pablo II, Centro de Gobierno Plan Maestro Edificios Numero 2 y 3, San Salvador. 24 de Julio del 2018	No.Orden:180001/2018

RAZON SOCIAL DEL SUMINISTRANTE	NIT
MORAN SORTO, JARET NAUN	[redacted]

CANTIDAD	UNIDAD DE MEDIDA	DESCRIPCION	PRECIO UNITARIO	VALOR TOTAL
1	Unidad	ADQUISICION DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL	$47,032.00	$47,032.00
1	Unidad	ADQUISICION DE 19 LICENCIAS	$5,225.84	$5,225.84
-	-	TOTAL.....	-	$52,257.84

SON: **cincuenta y dos mil doscientos cincuenta y siete 84/100 dolares**

OBSERVACIONES: CONTRATO 18/2018.

LUGAR DE ENTREGA:MINISTERIO DE TRABAJO

Firma del Administrador de Contrato o Encargado de Orden de Pedido	_____
_____	_____

Elaborado por:rosah

MINISTERIO DE TRABAJO Y PREVISION SOCIAL
23 AGO. 2018
RECIBIDO U.A.C.I.
10:54 am.

Rosa María Hernández

MINISTERIO DE TRABAJO Y PREVISION SOCIAL
22 AGO. 2018
RECIBIDO Desarrollo Tecnologico

GOBIERNO DE EL SALVADOR
MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL

ACTA DE RECEPCION

En las instalaciones del Ministerio de Trabajo y Previsión Social, a las trece horas con treinta minutos del dia ocho de agosto de dos mil dieciocho, reunidos el Ingeniero Juan Francisco Sánchez, Administrador del Contrato por parte del Ministerio de Trabajo y Previsión Social y por parte del proveedor el Ingeniero Jaret Naún Morán Sorto, en su calidad de Representante Legal de la Empresa JL Security Technologies. Después de haber recibido a satisfacción los productos establecidos del proceso: **"ADQUISICION DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"**. Se recibe a entera satisfacción en el plazo acordado entre las partes, por lo que se otorga el Visto Bueno y se autoriza el trámite de pago correspondiente.

Ing. Juan Francisco Sánchez Cabrera
Ministerio de Trabajo y Previsión Social
Administrador del Contrato

[redacted]

Ing. Jaret Naún Morán Sorto
Representante Legal
JL Security Technologies

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
GOBIERNO DE EL SALVADOR

ACTA DE RECEPCION

En las instalaciones del Ministerio de Trabajo y Previsión Social, a las trece horas con treinta minutos del día ocho de agosto de dos mil dieciocho, reunidos el Ingeniero Juan Francisco Sánchez, Administrador del Contrato por parte del Ministerio de Trabajo y Previsión Social y por parte del proveedor el Ingeniero Jaret Naún Morán Sorto, en su calidad de Representante Legal de la Empresa JL Security Technologies. Después de haber recibido a satisfacción los productos establecidos del proceso: **"ADQUISICION DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"**. Se recibe a entera satisfacción en el plazo acordado entre las partes, por lo que se otorga el Visto Bueno y se autoriza el trámite de pago correspondiente.

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL DESARROLLO TECNOLÓGICO

Ing. Juan Francisco Sánchez Cabrera
Ministerio de Trabajo y Previsión Social
Administrador del Contrato

[redacted]
Representante Legal
JL Security Technologies

LA CENTRAL
SEGUROS Y FIANZAS
Su Centro de confianza

LA CENTRAL DE SEGUROS Y FIANZAS, SOCIEDAD ANONIMA

GARANTIA DE CUMPLIMIENTO DE CONTRATO

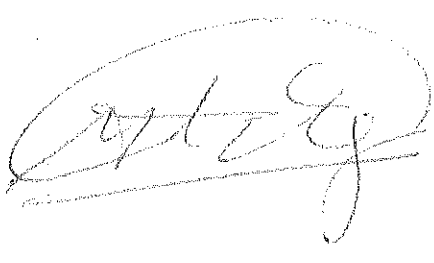
Fianza N°. 317,209 **Monto $ 5,225.78** **Vigencia 25/07/2018 - 09/08/2018**
Solicitud N°. 338,131

Afianzado JARET NAUN MORAN SORTO

Beneficiario MINISTERIO DE TRABAJO Y PREVISION SOCIAL

[redacted] mayor de edad, [redacted] del domicilio de [redacted], Departamento de [redacted] actuando en nombre y representación en mi carácter de Apoderada Especial de la Sociedad "LA CENTRAL DE SEGUROS Y FIANZAS, SOCIEDAD ANONIMA", de este domicilio, en adelante llamada "La Fiadora", por el presente documento OTORGO: 1) Que la Sociedad que represento, sujetándose a las condiciones particulares más adelante descritas, se constituye FIADORA de: JARET NAUN MORAN SORTO, en favor del MINISTERIO DE TRABAJO Y PREVISION SOCIAL, del domicilio de San Salvador y 2) OBLIGACIONES GARANTIZADAS, MONTO Y CIRCUNSTANCIAS DE LA GARANTIA: La fiadora se constituye garante y principal pagadora hasta por la suma de CINCO MIL DOSCIENTOS VEINTICINCO DOLARES CON SETENTA Y OCHO CENTAVOS DE DOLAR DE LOS ESTADOS UNIDOS DE AMERICA, a favor del MINISTERIO DE TRABAJO Y PREVISION SOCIAL, quien en el curso de esta fianza se denominará "La Institución Contratante", para garantizar que en el plazo de QUINCE DIAS CALENDARIO, a partir del VEINTICINCO DE JULIO DEL DOS MIL DIECIOCHO HASTA EL NUEVE DE AGOSTO DEL DOS MIL DIECIOCHO; JARET NAUN MORAN SORTO, mayor de edad, [redacted] del domicilio legal de [redacted] Departamento de [redacted] quien en lo sucesivo se llamará "El Contratista", cumplirá con la "ADQUISICIÓN DE DIECINUEVE EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS", según CONTRATO MTPS DIECIOCHO-DOS MIL DIECIOCHO, autenticado a las catorce horas y treinta y dos minutos del día seis de julio de dos mil dieciocho, ante los oficios del notario [redacted], derivado de la LIBRE GESTIÓN LG MTPS DOCE-DOS MIL DIECIOCHO. Vencido el plazo antes mencionado y de no haber reclamo alguno, durante el período, quedará extinguida la responsabilidad de la fiadora, dándose por cancelada la presente garantía aunque el documento original no fuere devuelto. Es entendido y convenido que en caso de reclamo se procederá a la liquidación respectiva del suministro y se cancelará el porcentaje equivalente al valor del suministro no cumplido, menos el suministro entregado a la fecha del reclamo que no haya sido cancelado. Para los efectos legales de la presente garantía, la fiadora señala como domicilio especial el de esta ciudad, renuncia al beneficio de excusión de bienes, al derecho de apelar del decreto de embargo sentencia de remate y de cualquier otra providencia alzable del juicio, relevando al depositario que nombre La Institución Contratante, de la obligación de rendir fianza. Esta garantía está regulada por las disposiciones de los artículos del Código de Comercio del 1539 al 1550 y del Artículo 35 de la Ley de Adquisiciones y Contrataciones de la Administración Pública. En fe de lo cual, firmo la presente en San Salvador, el día veintiseis de julio del dos mil dieciocho.

[redacted]





72010

En...

la ciudad de San Salvador, a las once horas y cuarenta y siete minutos del día veintiseis de julio del dos mil dieciocho. Ante mí, [redacted], Notario, de este domicilio, comparece [redacted], quien es de [redacted] años de edad, Estudiante, del domicilio de [redacted] Departamento de [redacted] persona a quien conozco e identifico, por ser portadora de su Documento Único de Identidad NUMERO [redacted] y con Número de Identificación Tributaria [redacted], quien actúa en nombre y representación en su carácter de Apoderada Especial de "LA CENTRAL DE SEGUROS Y FIANZAS, SOCIEDAD ANONIMA", que podrá abreviarse "LA CENTRAL DE FIANZAS Y SEGUROS, S.A.", "LA CENTRAL DE SEGUROS, S.A.", "LA CENTRAL DE FIANZAS, S.A." y/o "LA CENTRAL DE SEGUROS Y FIANZAS, S.A.", con Número de Identificación Tributaria [redacted], de este domicilio, de cuya personería DOY FE de ser legítima y suficiente por haber tenido a la vista el Testimonio de Escritura Pública de Poder Especial Administrativo, otorgado en esta ciudad a las once horas y cuarenta minutos del día veinte de abril de dos mil dieciséis, ante los oficios del Notario [redacted] por el Ingeniero [redacted] actuando en su calidad de [redacted] de la Junta Directiva y Representante Legal de dicha Sociedad Anónima, a favor de la compareciente para que pueda comparecer a otorgar entre otros, actos como el presente. En dicho Poder, el Notario autorizante dio fe de la personería con que actuó el Ingeniero [redacted] y de la existencia legal de la Sociedad Anónima. El poder relacionado, se encuentra inscrito en el Registro de Comercio, bajo el NUMERO CUARENTA Y SEIS del Libro MIL SETECIENTOS CINCUENTA Y CINCO del Registro de Otros Contratos Mercantiles; y ME DICE: Que en el carácter y calidad en que comparece a nombre de su representada la cual se constituye FIADORA de: JARET NAUN MORAN SORTO, mayor de edad, [redacted] del domicilio legal de [redacted] Departamento de [redacted], que en adelante se llamará "El Contratista", a favor del MINISTERIO DE TRABAJO Y PREVISION SOCIAL, del domicilio de [redacted] que se denominará "La Institución Contratante", hasta por la suma de CINCO MIL DOSCIENTOS VEINTICINCO DOLARES CON SETENTA Y OCHO CENTAVOS DE DOLAR DE LOS ESTADOS UNIDOS DE AMERICA, para garantizar que en el plazo de QUINCE DIAS CALENDARIO, a partir del VEINTICINCO DE JULIO DEL DOS MIL DIECIOCHO HASTA EL NUEVE DE AGOSTO DEL DOS MIL DIECIOCHO, el contratista cumplirá con la "ADQUISICIÓN DE DIECINUEVE EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS", según CONTRATO MTPS DIECIOCHO-DOS MIL DIECIOCHO, autenticado a las catorce horas y [redacted] y dos minutos del día seis de julio de dos mil dieciocho, ante los oficios del notario [redacted], derivado de la LIBRE GESTIÓN LG MTPS DOCE-DOS MIL DIECIOCHO; reconociendo los demás conceptos y renuncias que se mencionan en el documento de fianza que se autentica; y yo el Notario también doy fe: Que la firma que se lee "[redacted] es auténtica por haber sido puesta a mi presencia por la compareciente, a quien expliqué los efectos legales de esta acta notarial que consta de dos hojas útiles y leído que le hube lo escrito íntegramente y en un solo acto, ratifica su contenido y firmamos. DOY FE.-

[redacted]

[redacted]

Gobierno de El Salvador

Compromiso Presupuestario

Institución Ramo de Trabajo y Previsión Social

No. de Compromiso 1653 Estado : Elaboracion

Proyecto 0 Proyecto

Proveedor 06082210841057 JARET NAUN MORAN SORTO

Unidad Financiera 01 Unidad Financiera Institucional (UFI)

Fte. Financiamiento 1 Fondo General

Fecha Elaboración 24/7/2018

Fecha vencimiento 31/12/2018

Ejercicio Fiscal 2018

Concepto Comp. ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON 19 LICENCIAS

Area de Gestión Desarrollo Social

Tipo de Documento Contrato

Documento de Respaldo MTPS 18-2018

Fuente de Recursos N/A

Agrupación Operacional Recursos de Caracter Ordinario

Total Compromiso 52,257.84

Monto Doc. Respaldo 52,257.84

CLASIFICADOR **CONCEPTO** **MESES**

			Septiembre	Total
	01 Dirección y Administración Institucional **02 Dirección Administrativa**			
61104	Equipos Informáticos	2	47,032.00	**47,032.00**
61403	Derechos de Propiedad Intelectual	1	5,225.84	**5,225.84**
	Total Linea		**52,257.84**	**52,257.84**

MINISTERIO DE TRABAJO Y PREVISION SOCIAL
24 JUL. 2018
Blanca
RECIBIDO
U.A.C.I.
9:17 am.

MINISTERIO DE TRABAJO Y PREVISION SOCIAL
23 JUL. 2018
RECIBIDO
U.A.C.I.
9:17am

419

MINISTERIO DE TRABAJO
Y PREVISIÓN SOCIAL
GOBIERNO DE
EL SALVADOR
UNÁMONOS PARA CRECER

UNIDAD DE ADQUISICIONES Y CONTRATACIONES INSTITUCIONAL

MEMORANDUM

PARA: **Lic. Luis Mario Flores Guillén**
Jefe de la Unidad Financiera Institucional.

DE: **Licda. Blanca Azucena Canizales Ortiz.**
Jefa UACI Ad Honorem.

ASUNTO: Remisión de Contrato

FECHA: 24 de julio de 2018

Estimado Licenciado:

Por este medio hago remisión de Contrato número MTPS 18-2018, en original, derivado del proceso LG MTPS 12 – 2018 "ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS" legalmente formalizado entre la persona natural Jaret Naún Morán Sorto y el MTPS por un monto total de $52,257.84.

Atentamente,

MINISTERIO DE TRABAJO Y PREVISION SOCIAL
24 JUL. 2018
RECIBIDO
DIVISIÓN FINANCIERA INSTITUCIONAL

Gricelda 8:34 am

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
GOBIERNO DE EL SALVADOR

San Salvador, 24 de julio de 2018.

Señor
Jaret Naun Moran Sorto.
Presente.

Referente al proceso de Libre Gestión MTPS 12-2018 "ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"; por este medio se notifica y remite Contrato No. 18-2018 del proceso en mención, el cual se entrega en original a la empresa JL SECURITY TECHNOLOGIES.

De igual forma aprovecho para solicitar la **Garantía de Cumplimiento de Contrato,** según lo indicado en el romano V del contrato.

Atentamente,

[redacted]

Licda. Blanca Azucena Canizales Ortiz.
Jefa Unidad de Adquisiciones y Contrataciones Institucional Ad Honorem.

UAI/MTPS/LG/12-2018/HB/OB

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
UNIDAD DE ADQUISICIONES Y CONTRATACIONES INSTITUCIONAL
San Salvador, El Salvador, C. A.

LIBRE GESTIÓN LG MTPS 12-2018
"ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"
CONTRATO MTPS 18-2018

Nosotros: SANDRA EDIBEL GUEVARA PÉREZ, de [redacted] años de edad, [redacted] del domicilio de [redacted] Departamento de [redacted], con Documento Único de Identidad número [redacted], y Número de Identificación Tributaria [redacted], actuando en nombre y representación del Estado y Gobierno de El Salvador, específicamente del Ministerio de Trabajo y Previsión Social, institución con Número de Identificación Tributaria cero seis uno cuatro - cero uno cero uno dos cinco- cero cero tres - seis, en mi calidad de Ministra de Trabajo y Previsión Social, lo que compruebo con: a) Certificación del Acuerdo Ejecutivo número ocho, emitido por la Presidencia de la República de El Salvador con fecha uno de junio de dos mil catorce, mediante el cual el Presidente de la República me nombró, a partir del día uno de junio de ese año como Ministra de Trabajo y Previsión Social; y b) Certificación del Acta de Juramentación de Funcionarios Públicos que lleva la Presidencia de la República, extendida por el Licenciado Francisco Rubén Alvarado Fuentes, Secretario para Asuntos Legislativos y Jurídicos de la Presidencia de la República de El Salvador, el día uno de junio de dos mil catorce, de la que consta que a folio cuatro vuelto, se encuentra el Acta de Juramentación a través de la cual el señor Presidente de la República tomó protesta constitucional a mi persona como Ministra de Trabajo y Previsión Social; y en nombre y representación del **MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL DE LA REPÚBLICA DE EL SALVADOR**, quien en este instrumento me denominaré "**La Institución Contratante**", y **JARET NAUN MORAN SORTO**, de treinta y tres años de edad, Empleado, del domicilio de Ciudad Delgado, Departamento de San Salvador, con Documento Único de Identidad número cero dos dos cuatro cero uno cero uno - cero y Número de Identificación Tributaria cero seis cero ocho - dos dos uno cero ocho cuatro - uno cero cinco - siete; actuando en nombre y representación en mi calidad de Propietario de la Empresa Comercial cuya denominación es **JL SECURITY TECHNOLOGIES**, con Número de Renovación de Matricula de Empresa dos cero uno uno cero siete uno cuatro uno cero uno tres siete dos cinco cero dos siete cinco dos siete seis, y con Número de Registro de Contribuyente (NRC)

uno nueve nueve tres siete seis - cero, lo que compruebo con la siguiente documentación: a) Copia Certificada de Tarjeta de Identificación Tributaria y Número de Registro (NRC); y b) Copia Certificada de Constancia de Renovación de Matricula de Empresa extendida el trece de abril de dos mil dieciocho y suscrita por el Licenciado [redacted] Registrador del Registro de Comercio, Matriculas de Empresa; quien en este instrumento me denominaré "**La Empresa Contratista**", en las calidades antes expresadas **MANIFESTAMOS**: Que hemos acordado otorgar y en efecto otorgamos proveniente del proceso de Libre Gestión número LG MTPS DOCE - DOS MIL DIECIOCHO, denominado "**ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS**", de conformidad a la Ley de Adquisiciones y Contrataciones de la Administración Pública, que en adelante se denominará LACAP, su Reglamento que en adelante se denominará RELACAP, y a las cláusulas que se detallan a continuación: **I.- OBJETO DEL CONTRATO**: El objeto del presente Contrato es que "La Empresa Contratista" se compromete a brindarnos la adquisición de 19 Equipos de Seguridad Perimetral con Licencias a la "Institución Contratante", las cuales contendrán las siguientes características:

ÍTEM	CANTIDAD	DESCRIPCIÓN	MARCA Y MODELO	MONTO
1	19	EQUIPOS DE SEGURIDAD PERIMETRAL.	HILLSTONE 2 - MODELO T - 1860 12 - MODELO E-1700 2GBPS. 5 - MODELO E-1700 1.5 GBPS	$ 47,032.00
2	19	LICENCIAS PARA EQUIPO DE SEGURIDAD PERIMETRAL.	HILLSTONE 2 - MODELO T - 1860 12 - MODELO E-1700 2GBPS. 5 - MODELO E-1700 1.5 GBPS	$ 5,225.84
TOTAL				**$ 52,257.84**

ESPECIFICACIONES TÉCNICAS.

SITIO PRINCIPAL Y SITIO REMOTO (SANTA ANA)	
CARACTERISTICA	DESCRIPCIÓN
Capacidad de Usuarios	Hasta 1000
Cantidad de Equipos	Dos
Configuración	Contingencia
Almacenamiento	240 GB mínimo
Consumo de Energía	Fuente redundante
Conexiones concurrentes	Mínimo 1 millón
AV rendimiento	Mínimo 1.5 GBPS
IPS rendimiento	Mínimo 2 GBPS
Firewall rendimiento	Mínimo 4 GBPS

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
UNIDAD DE ADQUISICIONES Y CONTRATACIONES INSTITUCIONAL
San Salvador, El Salvador, C. A.

Interfaces	Capacidad de Ampliación
Módulos de protección	1. Firewall 2. Protección de red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPsec.
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES y AES. 4. Autenticación de Certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.
Seguridad Web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS.
Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, IPsec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.
Filtrado de Contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe permitir/restringir/acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL. 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.
IPS	1. Que el UTM soporte motor de IPS para la protección

	contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP, Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de Software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.
Protección de correo electrónico	Especificar
Protección de redes inalámbricas	Especificar
OTRAS	
Soporte Técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestaran un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía de equipo.
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.

CARACTERISTICAS DE EQUIPO AL QUE DEBERÁ ASOCIARSE LICENCIAMIENTO DE SEGURIDAD PERIMETRAL

OFICINAS REGIONALES (A EXCEPCION DE SANTA ANA) Y DEPARTAMENTALES	
CARACTERISTICA	DESCRIPCIÓN
Capacidad de Usuarios	Hasta 100

Cantidad de Equipos	Doce
Almacenamiento	64 GB mínimo
Consumo de Energía	Especificar
Conexiones concurrentes	Mínimo 600K
AV rendimiento	Mínimo 500 MBPS
IPS rendimiento	Mínimo 400 MBPS
Firewall rendimiento	Mínimo 1.5 GBPS
Interfaces	Capacidad de ampliación
Módulos de Protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo Electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPsec
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.
Seguridad Web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: Extensiones de archivos, Flash. 5. Detección de spyware 6. Configuración de perfiles de navegación 7. Autenticación compatible con LDAP y RADIUS
Protección de red	1. Administración web protegido por contraseña personalizada. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS, VPN punto a punto: SSL, IPsec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.
Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http y https. 2. Debe permitir/restringir/acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y Active X 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador.

	7. Control de Aplicaciones.
IPS	1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDos, ICMP Flood, UDP Flood, TCP SYN Flood, Smurt, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.
Protección de correo electrónico	Especificar
Protección de redes inalámbricas	Especificar
OTRAS	
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía de equipo.
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.

CARACTERISTICAS DE EQUIPO AL QUE DEBERÁ ASOCIARSE LICENCIAMIENTO DE SEGURIDAD PERIMETRAL.

CENTROS DE RECREACIÓN Y ARCHIVO GENERAL	
CARACTERISTICA	DESCRIPCIÓN
Capacidad de usuario	Hasta 15
Cantidad de equipos	Cinco
Almacenamiento	64 GB mínimo

Consumo de energía	Especificar
Conexiones concurrentes	Mínimo 600K
AV rendimiento	Mínimo 400MBPS
IPS rendimiento	Mínimo 300 MBPS
Firewall rendimiento	Mínimo 900 MBPS
Interfaces	Capacidad de ampliación
Módulos de protección	1.Firewall 2. Protección de red. 3. Seguridad Web. 4. Protección de Correo electrónico. 5. Protección de redes inalámbricas. 6. Protección para servidor Web. 7. VPN punto a punto: SSK, IPsec.
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.
Seguridad Web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS.
Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, IPsec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.
Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. debe permitir/restringir/acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.

IPS	1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDOS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurt, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS, SQL, MySQL, Cross-site Scripting, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.
Protección de correo electrónico	Especificar
Protección de redes inalámbricas	Especificar
OTRAS	
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía de equipo.
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.

II.- DOCUMENTOS CONTRACTUALES: Forman parte integral del contrato los siguientes documentos: La Garantía de Cumplimiento de Contrato, las especificaciones técnicas, la oferta técnica y económica presentada por "La Empresa Contratista", el acta sobre el informe de evaluación de Ofertas de fecha veintiséis de junio de dos mil dieciocho y otros documentos que emanen del presente contrato, los cuales son complementarios entre sí y serán interpretados en forma conjunta, en caso de discrepancia entre alguno de los documentos contractuales y este contrato, prevaleciendo

el Contrato. **III.- FUENTE DE LOS RECURSOS, PRECIO Y FORMA DE PAGO:** Las obligaciones emanadas del presente instrumento serán cubiertas con cargo de fondos GOES para lo cual se ha verificado la correspondiente asignación presupuestaria dos mil dieciocho. "La Institución Contratante" se compromete a cancelar a "La Empresa Contratista" la cantidad de **CINCUENTA Y DOS MIL DOSCIENTOS CINCUENTA Y SIETE DÓLARES DE LOS ESTADOS UNIDOS DE AMÉRICA CON OCHENTA Y CUATRO CENTAVOS DE DÓLAR ($52,257.84)** en cuyo valor se incluye el Impuesto al Valor Agregado (IVA), dicho pago se realizará mediante la presentación de la factura a la **UNIDAD FINANCIERA INSTITUCIONAL (UFI)** y reporte, siempre y cuando la documentación presentada esté de acuerdo a los requerimientos de "La Institución Contratante" según términos de referencia y estipulaciones contractuales, dichos montos incluyen el trece por ciento (13%) correspondiente al Impuesto a la Transferencia de Bienes Muebles y a la Prestación de Servicios, y "La Institución Contratante" retendrá el uno por ciento (1%) sobre el monto de lo facturado, de conformidad a la Resolución de la Dirección General de Impuestos Internos del Ministerio de Hacienda número doce mil trescientos uno guión NEX guión dos mil ciento noventa y siete guión dos mil siete, de fecha cuatro de diciembre de dos mil siete, mediante la cual se designa al Ministerio de Trabajo y Previsión Social como Agente de Retención. Los montos antes mencionado en calidad de pago se depositarán por parte de la Dirección General de Tesorería del Ministerio de Hacienda a favor de la Empresa Contratista en su Cuenta de Ahorro: a nombre de [redacted] del [redacted], en los plazos y términos estipulados en esta misma cláusula. **IV.- PLAZO DE CONTRATO Y VIGENCIA:** El plazo de ejecución de las obligaciones emanadas del presente contrato será de quince días calendario, después de notificado el referido Contrato y dicho suministro se entregará a través de una única entrega. La prestación del servicio solicitado se llevará a cabo según lo establecido en las oficinas e instalaciones determinadas en las especificaciones técnicas, de igual forma la Institución Contratante verificará el cumplimiento de la calidad y condiciones, en la entrega y el administrador velara por el cumplimiento de los términos establecidos emitiendo el informe oportuno cuando exista irregularidad. La vigencia del presente contrato es a partir de la firma del presente

contrato, pudiendo prorrogarse de conformidad a lo establecido en la Ley de Adquisiciones y Contrataciones de la Administración Pública si las condiciones son favorables para "La Institución Contratante". **V.- GARANTIAS:** Para garantizar el cumplimiento de las obligaciones derivadas del presente Contrato "La Empresa Contratista" otorgará a favor del Estado y Gobierno de El Salvador en el Ramo específicamente del Ministerio de Trabajo y Previsión Social, a) Garantía de Cumplimiento de Contrato, de conformidad al artículo treinta y cinco de la LACAP, equivalente al DIEZ por ciento del valor total contratado, es decir la cantidad de **CINCO MIL DOSCIENTOS VEINTICINCO DÓLARES DE LOS ESTADOS UNIDOS DE AMÉRICA CON SETENTA Y OCHO CENTAVOS DE DÓLAR ($ 5,225.78);** la cual tendrá la misma vigencia del presente contrato y deberá entregarse a la Unidad de Adquisiciones y Contrataciones Institucional del Ministerio de Trabajo y Previsión Social, dentro de los CINCO días hábiles, después de la notificación del Contrato. b) Garantía de buen Funcionamiento y calidad de los bienes de conformidad al artículo treinta y siete bis de la LACAP, equivalente al diez por ciento del valor contratado; la cual tendrá una vigencia de doce meses contados a partir de la entrega formal del suministro. **VI.- ADMINISTRACIÓN DEL CONTRATO:** El seguimiento al cumplimiento de las obligaciones contractuales estará a cargo del Administrador de Contrato, Ingeniero Juan Francisco Sánchez Cabrera, quien se desempeña como Jefe de la Unidad de Desarrollo Tecnológico, de conformidad al Acuerdo Ministerial número cuarenta y nueve de fecha de veinte de junio de dos mil dieciocho. Teniendo como atribuciones las establecidas en los artículos ochenta y dos bis, ciento veintidós de la LACAP, cuarenta y dos inciso tercero, setenta y cuatro, setenta y cinco inciso segundo, setenta y siete, ochenta y ochenta y uno del RELACAP y las funciones establecidas en el Manual de Procedimientos para el Ciclo de Gestión de Adquisiciones y Contrataciones de las Instituciones de la Administración Pública y las demás emanadas del presente contrato. El Administrador del contrato deberá de dar aviso de los desperfectos o irregularidades en las dieciocho licencias para equipo de seguridad perimetral, a efecto que se realicen las diligencias respectivas para solucionar las circunstancias suscitadas. **VII.- ACTA DE RECEPCIÓN:** Corresponderá al administrador del Contrato en coordinación con "La Empresa Contratista", la elaboración y firma del acta de recepción definitiva, la cual contendrá como mínimo lo que

establece el artículo setenta y siete del RELACAP. **VIII.- MODIFICACIÓN:** El presente contrato podrá ser modificado o ampliado en sus plazos y vigencia antes del vencimiento de su plazo, de conformidad a lo establecido en los artículos ochenta y tres A y B de la LACAP, debiendo emitir "La Institución Contratante" la correspondiente resolución modificativa, debiendo "La Empresa Contratista" en caso de ser necesario modificar o ampliar los plazos y montos de las Garantías de Cumplimiento de Contrato, según lo indique "La Institución Contratante" y formará parte integral de ese contrato. Asimismo, estas deberán ser por mutuo acuerdo de las partes, mediante comunicación escrita, con al menos treinta días de anticipación, siempre y cuando concurra una de las situaciones siguientes: a) cuando existan nuevas necesidades, siempre vinculadas al objeto contractual; y b) cuando surjan causas imprevistas. En tales casos "La Institución Contratante" emitirá la correspondiente resolución de Modificación del Contrato, la cual será firmada por la Titular, y notificada a "La Empresa Contratista" en el lugar señalado para recibir notificaciones por las partes, según cláusula XX de este Contrato, "La Empresa Contratista" deberá mostrar su conformidad por escrito y notificarlo a "La Institución Contratante". Los mismos efectos que lo anterior, tendrá, la posterior emisión de la Resolución, y la firma de los documentos contractuales correspondientes. **IX.- PRÓRROGA:** Previo al vencimiento del plazo pactado, el presente contrato podrá ser prorrogado de conformidad a lo establecido en el artículo ochenta y tres de la LACAP y setenta y cinco del RELACAP; en tal caso, se deberá modificar o ampliar los plazos y montos de la Garantía de Cumplimiento de Contrato, debiendo emitir "La Institución Contratante" la correspondiente resolución de prórroga. **X.- CESIÓN:** Salvo autorización expresa del Ministerio de Trabajo y Previsión Social "La Empresa Contratista" no podrá transferir o ceder a ningún título, los derechos y obligaciones que emanan del presente contrato. La transferencia o cesión efectuada sin la autorización antes referida dará lugar a la caducidad del contrato, procediéndose además a hacer efectiva la garantía de cumplimiento de Contrato. **XI.- CONFIDENCIALIDAD:** "La Empresa Contratista" se compromete a guardar la confidencialidad de toda información revelada por "La Institución Contratante", independientemente del medio empleado para transmitirla, ya sea en forma verbal o escrita y se compromete a no revelar dicha información a terceras personas, salvo que "La Institución

Contratante", lo autorice en forma escrita. "La Empresa Contratista" se compromete a hacer del conocimiento únicamente la información que sea estrictamente indispensable para la ejecución encomendada y manejar la reserva de la misma, estableciendo las medidas necesarias para asegurar que la información revelada por "La Institución Contratante" se mantenga con carácter confidencial y que no se utilice para ningún otro fin. **XII.- SANCIONES:** En caso de incumplimiento de las obligaciones contractuales "La Empresa Contratista" se somete a las sanciones que emanaren de la LACAP ya sea imposición de multa por mora, inhabilitación, extinción, las que serán impuestas siguiendo el debido proceso por "La Institución Contratante", a cuya competencia se somete para efectos de su imposición. **XIII.- INCUMPLIMIENTO:** En caso de mora en el cumplimiento por parte de "La Empresa Contratista" de las obligaciones emanadas del presente Contrato, se aplicarán las multas establecidas en el artículo ochenta y cinco de la Ley de Adquisiciones y Contrataciones de la Administración Pública (LACAP). **XIV.- EXTINCIÓN:** Serán causas de extinción del presente Contrato las establecidas en el artículo noventa y tres de la Ley de Adquisiciones y Contrataciones de la Administración Pública (LACAP), y en otras leyes vigentes. **XV.- OTRAS CAUSALES DE EXTINCIÓN CONTRACTUAL:** Sin perjuicio de lo establecido en la LACAP y el RELACAP el presente contrato podrá extinguirse por fuerza mayor, caso fortuito, Resciliación. **XVI.- TERMINACIÓN BILATERAL:** Las partes contratantes podrán acordar la extinción de las obligaciones contractuales en cualquier momento, siempre y cuando no concurra otra causa de terminación imputable a "La Empresa Contratista" y que por razones de interés público hagan innecesario o inconveniente la vigencia del contrato, sin más responsabilidad que la que corresponda a lo recibido. **XVII.- SOLUCIÓN DE CONFLICTOS:** Para resolver las diferencias o conflictos que surgieren durante la ejecución del presente Contrato, se estará a lo dispuesto en el Título VIII, Capítulo I de la Ley de Adquisiciones y Contrataciones de la Administración Pública (LACAP) y previa aceptación de ambas partes podrán dirimir el conflicto por medio de un Arbitraje Ad-Hoc el cual será de Derecho o Técnico, según la naturaleza de la controversia y se someterán a las disposiciones de la Ley de Mediación, Conciliación y Arbitraje. **XVIII) INTERPRETACIÓN DEL CONTRATO:** El Ministerio de Trabajo y Previsión Social, se reserva la facultad de interpretar el presente contrato,

de conformidad a la Constitución de la República, la LACAP, el RELACAP, demás legislación aplicable, y los Principios Generales del Derecho Administrativo y de la forma que más convenga a los intereses del Ministerio de Trabajo y Previsión Social, con respecto a la prestación objeto del presente instrumento, pudiendo en tal caso girar las instrucciones por escrito que al respecto considere convenientes. "La Empresa Contratista" expresamente acepta tal disposición y se obliga a dar estricto cumplimiento a las instrucciones que al respecto dicte el Ministerio de Trabajo y Previsión Social. **XIX.- MARCO LEGAL:** El presente contrato queda sometido en todo a la LACAP, RELACAP, la Constitución de la República, y en forma subsidiaria a las leyes de la República de El Salvador, aplicables a este Contrato. **XX.- NOTIFICACIONES:** "La Institución Contratante" señala como lugar para recibir notificaciones Final diecisiete Avenida Norte y Alameda Juan Pablo II, Edificio tres, Plan Maestro, Centro de Gobierno; y "La Empresa Contratista" señala para el mismo efecto la siguiente dirección Diecinueve Calle Poniente y Primera Avenida Norte, Edificio Niza, Local número doscientos cinco, Barrio San Miguelito, San Salvador. Todas las notificaciones referentes a la ejecución de este contrato serán válidas solamente cuando sean hechas por escrito en las direcciones que las partes han señalado. En fe de lo cual suscribimos el presente contrato, en la ciudad de San Salvador, departamento de San Salvador, a los seis días del mes de julio del año dos mil dieciocho.-

SANDRA EDIBEL GUEVARA PÉREZ
MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL.

[redacted]
en calidad de Propietario de JL SECURITY TECHNOLOGIES

En la ciudad de San Salvador, a las catorce horas y treinta y dos minutos del día seis de julio de dos mil dieciocho. Ante mí, [redacted] Notaria, del domicilio de [redacted] **COMPARECEN:** por una parte, **SANDRA EDIBEL GUEVARA PÉREZ**, quien es de [redacted] años de edad, [redacted] del domicilio de [redacted], Departamento de [redacted] persona a quien no conozco pero identifico por medio de su

Documento Único de Identidad número cero dos siete uno tres nueve cero tres - dos, y Número de Identificación Tributaria cero dos uno cero - uno siete cero cinco seis tres - uno cero tres - dos, actuando en nombre y representación del Estado y Gobierno de El Salvador, específicamente del Ministerio de Trabajo y Previsión Social, institución con Número de Identificación Tributaria cero seis uno cuatro - cero uno cero uno dos cinco- cero cero tres - seis, en mi calidad de Ministra de Trabajo y Previsión Social, personería que doy fe de ser legítima y suficiente por haber tenido a la vista: a) Certificación del Acuerdo Ejecutivo número ocho, emitido por la Presidencia de la República de El Salvador con fecha uno de junio de dos mil catorce, mediante el cual el Presidente de la República la nombró, a partir del día uno de junio de ese año como Ministra de Trabajo y Previsión Social; y b) Certificación del Acta de Juramentación de Funcionarios Públicos que lleva la Presidencia de la República, extendida por el Licenciado [redacted], S[redacted] para [redacted] el día uno de junio de dos mil catorce, de la que consta que a folio cuatro vuelto, se encuentra el Acta de Juramentación a través de la cual el señor Presidente de la República tomó protesta constitucional a su persona como Ministra de Trabajo y Previsión Social; y en nombre y representación del **MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL DE LA REPÚBLICA DE EL SALVADOR**, quien en este instrumento se denominará "**La Institución Contratante**", y **JARET NAUN MORAN SORTO**, quien es de [redacted] años de edad, [redacted] del domicilio de [redacted], Departamento de [redacted] persona a quien en razón de este acto conozco e identifico por medio de su Documento Único de Identidad número [redacted] Número de Identificación Tributaria [redacted] actuando en nombre y representación en su calidad de Propietario de la Empresa Comercial cuya denominación es **JL SECURITY TECHNOLOGIES**, con Número de Renovación de Matrícula de Empresa [redacted], y Número de Registro de Contribuyente (NRC) [redacted] personería que doy fe de ser legítima y suficiente por haber tenido a la vista: a) Copia Certificada de Tarjeta de Identificación Tributaria y Número de Registro (NRC); y b) Copia Certificada

de Constancia de Renovación de Matrícula de Empresa extendida el trece de abril de dos mil dieciocho y suscrita por el Licenciado [redacted] Registrador del Registro de Comercio, Matrículas de Empresa; quien en este instrumento se denominará "La Empresa Contratista"; y **ME DICEN**: Que reconocen como suyas las firmas puestas al pie del Contrato **MTPS DIECIOCHO - DOS MIL DIECIOCHO** derivado de la adjudicación del Proceso de Libre Gestión **LG MTPS doce - dos mil dieciocho** denominada "**ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS**" reconociendo además todos los conceptos vertidos en el mismo y las obligaciones que ampara, Contrato por medio del cual "La Empresa Contratista" se obliga a brindar la adquisición de 19 equipos de seguridad perimetral con licencias, a la "Institución Contratante", con las condiciones establecidas en las cláusulas primera y cuarta del Contrato relacionado. "La Institución Contratante" pagará la cantidad de **CINCUENTA Y DOS MIL DOSCIENTOS CINCUENTA Y SIETE DÓLARES DE LOS ESTADOS UNIDOS DE AMÉRICA CON OCHENTA Y CUATRO CENTAVOS DE DÓLAR**. El pago se hará efectivo durante los treinta días calendario siguientes a la presentación del recibo a la **UNIDAD FINANCIERA INSTITUCIONAL (UFI)**, con anexo de los documentos pertinentes para comprobar que la "La Empresa Contratista" ha hecho la entrega del servicio en los condiciones acordadas en las especificaciones técnicas y estipulaciones contractuales, sujeta a la verificación por parte del Administrador del Contrato; dicho monto incluye el trece por ciento correspondiente al Impuesto a la Transferencia de Bienes Muebles y a la Prestación de Servicios. Los montos antes mencionado en calidad de pago se depositarán por parte de la Dirección General de Tesorería del Ministerio de Hacienda a favor de la Empresa Contratista en su Cuenta de Ahorro: a nombre de [redacted] número [redacted] del [redacted] en los plazos y términos estipulados. Y además me declaran que se someten a las restantes condiciones que se estipulan en el Contrato que se autentica. Así se expresaron las comparecientes a quienes expliqué los efectos legales de la presente acta notarial escrita en dos folios útiles y yo la Notario DOY FE: Que son auténticas las firmas que anteceden por haber sido puestas por las comparecientes en mi presencia de su

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
UNIDAD DE ADQUISICIONES Y CONTRATACIONES INSTITUCIONAL
San Salvador, El Salvador, C. A.

puño y letra, y leído que le fue por mí a los presentes íntegramente todo lo escrito en un solo acto sin interrupción, ratificaron su contenido y para constancia firmamos.

[redacted]

en ca[redacted]

SANDRA EDIBEL GUEVARA PÉREZ
MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL.

LICDA. HAYDEE MARGARITA BOLAÑOS BELTRÁN
NOTARIO

Ministerio de Trabajo
y Previsión Social

EL SALVADOR

DECLARACION JURADA

1.0 DECLARANTE

1.1 PERSONA NATURAL O JURIDICA

Nombres y Apellidos o Razón Social	NIT	DUI O PASAPORTE	TELEFONO
JARET NAUN MORAN SORTO	[redacted]	[redacted]	[redacted]
DIRECCION	CIUDAD	CORREO ELECTRONICO	
[redacted]	[redacted]	[redacted]	

1.2 REPRESENTANTE LEGAL o APODERADO (Solo personas jurídicas)

NOMBRES Y APELLIDOS	NIT	CORREO ELECTRONICO	TELEFONO

Por este medio declaro bajo juramento que la cuenta que declaro a continuación, será utilizada por el estado por medio de la Dirección General de Tesorería para cancelar cualquier tipo obligación legalmente exigible, según lo establecido en el Art. 77, de la Ley Orgánica de Administración Financiera del Estado

La cuenta a declarar es la siguiente

NOMBRE DE LA CUENTA	NUMERO DE CUENTA	CORRIENTE	DE AHORRO	NOMBRE DEL BANCO
Jaret Naun Morán Sorto	[redacted]		X	[redacted]

DECLARO BAJO JURAMENTO LO SIGUIENTE

1-Que los datos que proporciono en este documento son verdaderos y que conozco las Normas Legales y Administrativas que regulan esta declaración jurada.

2-Que en caso de actuar como representante legal, declaro que el poder con el que actúo es suficiente para asumir todas las responsabilidades.

San Salvador, 05 de julio de 2018

FIRMA [redacted]

NOMBRE

DUI

JL Security Technologies
Seguridad en Internet

San Salvador, 05 de julio de 2018

Señores
Ministerio de Trabajo y Previsión Social
Presente

Reciba un cordial saludo de JL Security Technologies.

Referente al proceso de LG MTPS 12-2018"ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMENTRAL CON LICENCIAS" por este medio presentamos la declaración jurada de cuenta bancaria solicitada.

Quedo siempre a sus órdenes por cualquier otro requerimiento.

Sin otro particular por el momento me suscribo de ustedes,

Atentamente,

[redacted]

[redacted]

JARET NAUN MORÁN SORTO
JL SECURITY TECHNOLOGIES

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
06 JUL 2018
RECIBIDO

[redacted]

JL SECURITY TECHNOLOGIES

Seguridad en Internet

Security Technologies

Hillstone NETWORKS

San Salvador, 02 de julio de 2018.

Señores
Ministerio de Trabajo y Previsión Social
Atención: UACI.
Presente.

Luego de recibir notificación de haber sido adjudicados del proceso de Libre Gestión **MTPS 12-2018 "ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"**, presentamos la documentación requerida de acuerdo a carta de notificación de adjudicación del proceso de fecha 26 de junio de 2018, la cual detallamos a continuación:

a) Copia Certificada de DUI de Jaret Naun Morán Sorto.
b) Copia Certificada de NIT de Jaret Naun Morán Sorto.
c) Copia Certificada de Tarjeta de Registro de Contribuyente del Impuesto a la Transferencia de Bienes Muebles y a la Presentación de Servicios (IVA)
d) Copia Certificada de Constancia de Matrícula de Comercio de la empresa mercantil. .
e) Solvencia en original de los Impuestos Municipales del domicilio del establecimiento principal.
f) Solvencia electrónica de la Dirección General de Impuestos Internos.
g) Solvencia electrónica de la Unidad de Pensiones del Instituto Salvadoreño del Seguro Social (UPISSS)
h) Solvencia de pago de cotizaciones Obrero-Patronales del Instituto Salvadoreño del Seguro Social (ISSS)
i) Solvencia en original de las Administradoras de Fondos de Pensiones CRECER y CONFIA.
j) Constancia emitida por el Instituto de Previsión Social de la Fuerza Armada.

Sin otro particular, me suscribo atentamente en la ciudad de San Salvador a los dos días del mes de julio del año dos mil dieciocho.

Atentamente,

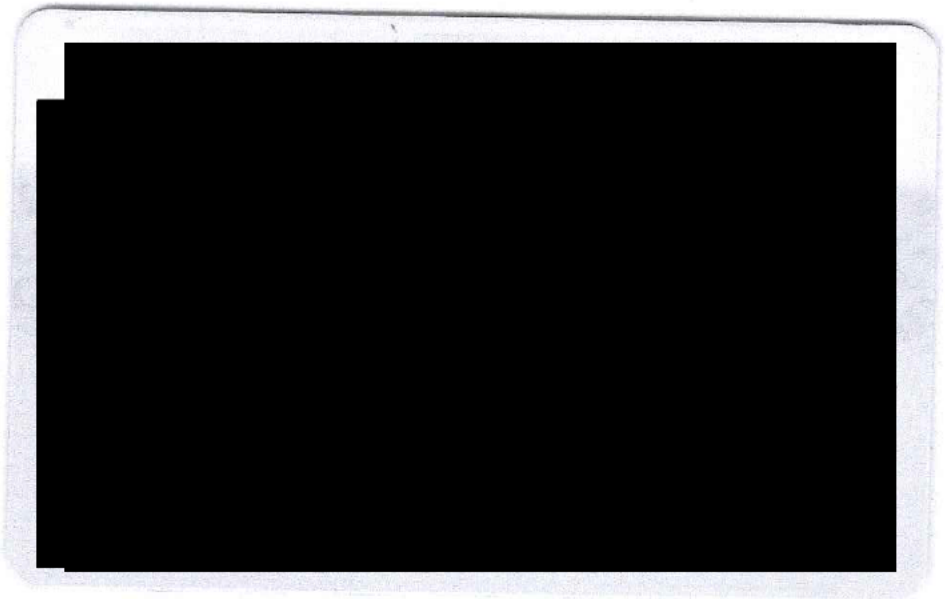
MINISTERIO DE TRABAJO Y PREVISION SOCIAL
02 JUL. 2018
RECIBIDO
UACI

[redacted]

Jaret Naún Morán Sorto
Propietario de JL Security Technologies

[redacted]


RNPN
República de El Salvador
Documento Único de Identidad





[redacted]

[redacted]

396

MINISTERIO DE HACIENDA
DIRECCIÓN GENERAL DE IMPUESTOS INTERNOS
NÚMERO DE REGISTRO DE CONTRIBUYENTES

NOMBRE DEL CONTRIBUYENTE

MORAN SORTO, JARET NAUN

[redacted]

DIRECCION DE CASA MATRIZ

[redacted]

FIRMA DEL FUNCIONARIO AUTORIZADO
LIC. JENDRIX WILMAR PANAMEÑO CASTRO
JEFE SECCIÓN REGISTRO DE CONTRIBUYENTES Y MAQ. EXENTA

ESTA TARJETA ACREDITA LA INSCRIPCIÓN EN EL REGISTRO DE CONTRIBUYENTES DEL IMPUESTO A LA TRANSFERENCIA DE BIENES MUEBLES Y A LA PRESTACIÓN DE SERVICIOS

[redacted]

R.F.210A2098860 delmy calderon

[redacted]

[redacted]

[redacted]

397

MINISTERIO DE HACIENDA
DIRECCIÓN GENERAL DE IMPUESTOS INTERNOS
TARJETA DE IDENTIFICACIÓN TRIBUTARIA

NOMBRE DEL CONTRIBUYENTE

MORAN SORTO, JARET NAUN

NÚMERO DE IDENTIFICACIÓN TRIBUTARIA (NIT)

[redacted]

Fecha
19

DUI

N

PARA TODA GESTIÓN O TRÁMITE RELACIONADO CON LA ADMINISTRACIÓN FISCAL DEBERÁ PRESENTAR ESTA TARJETA O HACER REFERENCIA AL CORRESPONDIENTE NÚMERO DE IDENTIFICACIÓN TRIBUTARIA.

FIRMA DEL FUNCIONARIO AUTORIZADO
LIC. JENDRIX WILMAR PANAMEÑO CASTRO
JEFE SECCIÓN REGISTRO DE CONTRIBUYENTES Y MAG. EXENTA

FIRMA DE CONTRIBUYENTE, REPRESENTANTE LEGAL O APODERADO

R F210A1733788 alexander.martinez

No. 0283122

[redacted]

[redacted]

C 05638

395

REPUBLICA DE EL SALVADOR
CENTRO NACIONAL DE REGISTROS
REGISTRO DE COMERCIO

PRESENTACION 2018005553 AÑO: .2017

RENOVACION DE MATRICULA DE EMPRESA No [redacted]

REGISTRO DE LOCAL No: [redacted]

EL INFRASCRITO REGISTRADOR DEL DEPARTAMENTO DE MATRICULAS DE EMPRESA DEL REGISTRO DE COMERCIO.

[redacted]

Por tanto se expide al titular de dicha Empresa la presente constancia de renovación de conformidad con el Artículo 418 del Código de Comercio.

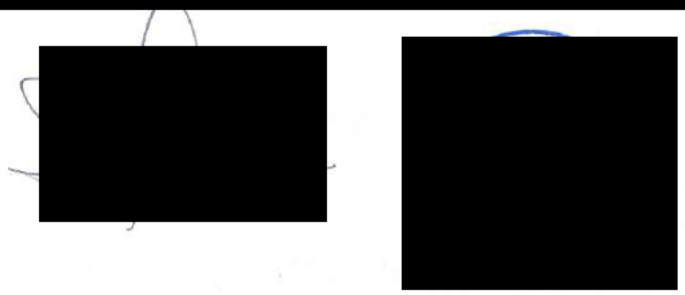
Registro de Comercio. SAN SALVADOR, trece de abril de dos mil dieciocho.

LI[redacted]

RE[redacted]

[redacted]

[redacted]



Dirección General de Impuestos Internos
División Control de Obligaciones Tributarias
Departamento de Cuenta Corriente y Control Tributario

MINISTERIO DE HACIENDA
GOBIERNO DE EL SALVADOR

TRAMITE GRATUITO

La Dirección General de Impuestos Internos, hace constar que el contribuyente

No. 11495038

CÓDIGO ÚNICO : L9DA371U5074

NIT Contribuyente: [redacted]

Posee el siguiente Estado Tributario: Solvente

Fecha y Hora: 27/06/2018 15:42:00

Vigencia: 08/07/2018

En el caso de trámites ante la UACI, Centro Nacional de Registro y/o Instituciones Financieras, dichos entes deberán comprobar a través del Sistema de Consulta Electrónica la validez del Estado Tributario del contribuyente de conformidad a los Artículos 217 y 218 del Código Tributario. Para la inscripción en el Registro de Comercio de acuerdos y escrituras públicas de fusión, disolución y liquidación de sociedades la Administración Tributaria ejercerá su facultad de fiscalización, previo a la emisión de Solvencia Física.

GOBIERNO DE SAN SALVADOR

INSTITUTO SALVADOREÑO DE DESARROLLO MUNICIPAL

SOLVENCIA MUNICIPAL Nº 826287

LA ALCALDÍA MUNICIPAL DE SAN SALVADOR, HACE CONSTAR QUE:

CUENTA Nº: 00000000010310061645 (Negocios)

NOMBRE: JARET NAUN MORAN SORTO

DIRECCIÓN:

[redacted]

ESTA SOLVENTE DEL PAGO DE IMPUESTOS Y SERVICIOS DE ESTA MUNICIPALIDAD

ESTA SOLVENCIA ES VALIDA UNICAMENTE PARA:
LICITACION

FECHA DE EMISIÓN	FECHA DE EXPIRACIÓN
15.06.2018	14.07.2018

NOTA: CUALQUIER ALTERACIÓN EN ESTA SOLVENCIA LA DECLARA SIN VALOR

ALCALDIA DE LA SQUIDAD DE SAN SALVADOR
SUBGERENCIA DE GESTIÓN TRIBUTARIA

TESORERÍA

ORIGINAL - CONTRIBUYENTE

TESORERIA MUNICIPAL SAN SALVADOR

SUB GERENCIA DE GESTIÓN TRIBUTARIA

R.R. DONNELLEY DE EL SALVADOR, S.A. DE C.V. PBX: +503 2297-9400 • NOV/11 14PTT10461.AI • JUL/16

393

27/06/2018 15:19:49

(CONSTANCIA EN EL CASO DE NO EXISTIR REGISTRO DE EMPLEADOR)

CONSTANCIA

La Unidad de Pensiones del Instituto Salvadoreño del Seguro Social, hace constar:

Que el empleador JARET NAUN MORAN SORTO, con número de identificación Tributaria (NIT) [redacted] no se encuentra registrado en la base de datos de empleadores que al efecto posee esta Unidad de Pensiones, en virtud de nunca haberse recibido planillas de declaración de cotizaciones previsionales.

Esta Constancia tiene validez por treinta días a partir de la fecha de emisión; y no exime al empleador de responsabilidad por mora u otros conceptos que a futuro o con carácter retroactivo la Unidad de Pensiones del ISSS determine.

Y para los usos que estime conveniente, se extiende la presente constancia en San Salvador, 27 dias del mes de Junio de Dos mil dieciocho

Jefe de Sección Cobranzas

168511

e6a736caf9c4444c806d489625896214

392

INSTITUTO SALVADOREÑO DEL SEGURO SOCIAL

Alameda Juan Pablo II y 39 Av. Norte, San Salvador, El Salvador, C.A.
Telefax: 2591-3189

EL INSTITUTO SALVADOREÑO DEL SEGURO SOCIAL "HACE CONSTAR" QUE EL PATRONO: JARET NAUN MORAN SORTO , Con Número(s) de identificación [redacted]
Según nuestros Registros a esta fecha está solvente para con este Instituto.

Esta SOLVENCIA, tiene validez por un plazo de treinta dias, a partir del siguiente día de la fecha de emisión. No exime al patrono de responsabilidad de cargos que posteriormente pudieran determinarse conforme lo estipula la Ley del Seguro Social y los reglamentos para su aplicacion.

San Salvador, VEINTE Y SIETE de JUNIO de 2018

A las QUINCE horas con VEINTE Y TRES MINUTOS

Jefe Sección Administracion de Cuentas por Cobrar

NOTA: Cualquier alteración al contenido de ésta la hara invalida

201806-002459

E5312DF6786541BCBBD067CDD5E7D209

391

AFP **Crecer**

CONSTANCIA

La Administradora de Fondos de Pensiones AFP CRECER, S.A., Hace constar:

Que el empleador MORAN SORTO, JARET NAUN con Número de Identificación Tributaria (NIT) [redacted] no se encuentra registrado en la base de datos de empleadores que al efecto posee esta AFP, en virtud de nunca haberse recibido planillas de declaración de cotizaciones previsionales.

Esta constancia tiene validez hasta el día veinticuatro de Julio de dos mil dieciocho.

Y para los usos que estime conveniente, se extiende la presente constancia en SAN SALVADOR, a los dieciocho días del mes de Junio de dos mil dieciocho.

La presente solvencia fue impresa el 18/06/2018.

Código de Validación:
00001510412018061800003300000332

390

AFP CONFIA

Por el mañana que tú quieres

C18062018201806330780

CONSTANCIA

La Administradora de Fondos de Pensiones AFP CONFIA, S.A. hace constar:

Que el empleador MORAN SORTO, JARET NAUN, con número de identificación tributaria (NIT) [redacted] no se encuentra registrado en la base de datos de empleadores que al efecto posee esta AFP, en virtud de nunca haberse recibido planillas de declaración de cotizaciones previsionales.

Esta constancia tiene validez hasta el día 24 de Julio de 2018.

Y para los usos que estime conveniente, se extiende la presente constancia en San Salvador, a los dieciocho días del mes de Junio del año dos mil dieciocho .

[redacted]

Ingrid Lissette Briceño H[redacted]

Ejecutiva De Servicio Al Cliente

EL INSTITUTO DE PREVISIÓN SOCIAL DE LA FUERZA ARMADA (IPSFA)

HACE CONSTAR :

Que el proveedor JARET NAUN MORAN SORTO con el Número de Identificación Tributaria [redacted] no se encuentra registrado en la base de datos de empleadores que al afecto posee este Instituto, en virtud de nunca haberse recibido planillas de cotizaciones previsionales.

Esta solvencia tiene validez 30 días calendario a partir de su fecha de emisión.

Y para los usos que estime conveniente, se extiende la presente constancia en San Salvador, a los 27 días del mes de Junio de 2018 .

Atentamente IPSFA
Código Verificador : NWSFC49670

Blanca Azucena Canizales

De: Blanca Azucena Canizales <blanca.canizales@mtps.gob.sv>
Enviado el: jueves, 28 de junio de 2018 03:53 p.m.
Para: 'Lic. Jemimah Areli Nuñez'
CC: Mayra Palma
Asunto: RE: Notificación de resultados
Datos adjuntos: image001.jpg; image003.jpg; image005.jpg; image006.jpg

Buenas tardes.

Reciban cordiales saludos deseándole éxitos en sus labores cotidianas.

En relación a la consulta realizada y con indicaciones de la jefa UACI se les manifiesta que de la documentación legal solicitada en la nota con fecha 26 de junio de 2018 se deberá de presentar únicamente aquella en la que apliquen , sin otro particular, me despido.

(FAVOR CONFIRMAR DE RECIBIDO ESTE CORREO)

Atentamente,

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
GOBIERNO DE EL SALVADOR
UNÁMONOS PARA CRECER

Blanca Azucena Canizales Ortiz
Colaboradora UACI
Unidad de Adquisiciones y Contrataciones Institucional
Ministerio de Trabajo y Previsión Social
Correo: blanca.canizales@mtps.gob.sv
Teléfonos: *2529-3728/ 2529-3714/ 3740/3760/3727/3771*
Dirección: Alameda Juan Pablo II y 17 Av. Nte. Plan Maestro, Centro de Gobierno, Edificio No.3, Primer Nivel.

De: Lic. Jemimah Areli Nuñez [mailto:areli.nunez@jlsecurity.net]
nviado el: miércoles, 27 de junio de 2018 11:56 a.m.
Para: blanca.canizales@mtps.gob.sv; mpalma@mtps.gob.sv
Asunto: RE: Notificación de resultados

De: Daniel Lemus [mailto:daniel.lemus@jlsecurity.net]
Enviado el: martes, 26 de junio de 2018 05:37 p.m.
Para: areli.nunez@jlsecurity.net
Asunto: RV: Notificación de resultados

Buen día,

Reciba un cordial saludo de JL Security Technologies deseándole éxitos en sus labores diarias.

Primeramente agradecerles por tomar a bien adjudicar el proceso de Libre Gestión MTPS 12-2018 "ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS" para el Ministerio de Trabajo y Previsión Social, a nuestra empresa.

Blanca Azucena Canizales

De: Lic. Jemimah Areli Nuñez <areli.nunez@jlsecurity.net>
Enviado el: miércoles, 27 de junio de 2018 11:56 a.m.
Para: blanca.canizales@mtps.gob.sv; mpalma@mtps.gob.sv
Asunto: RE: Notificación de resultados

De: Daniel Lemus [mailto:daniel.lemus@jlsecurity.net]
Enviado el: martes, 26 de junio de 2018 05:37 p.m.
Para: [redacted]
Asunto: RV: Notificación de resultados

Buen día,

Reciba un cordial saludo de JL Security Technologies deseándole éxitos en sus labores diarias.

Primeramente agradecerles por tomar a bien adjudicar el proceso de Libre Gestión MTPS 12-2018 "ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS" para el Ministerio de Trabajo y Previsión Social, a nuestra empresa.

Seguidamente, estamos preparando la documentación solicitada para proceder a la formalización del contrato; solamente tenemos una consulta en relación al siguiente documento solicitado:

- Copia certificada por notario de Escritura de Poder Especial o General con cláusula especial para ofertar y contratar en procesos de contratación pública, inscrito en el Registro de Comercio.

Nosotros estamos inscritos en el Registro de Comercio como persona natural a nombre de Jaret Naun Morán Sorto, nuestro nombre comercial es JL Security Technologies, y es el señor Jaret Morán quien ha firmado la oferta y quien firmará el correspondiente contrato. Por este motivo surge la pregunta si debemos presentar un documento adicional.

Quedo atenta a sus comentarios, de antemano muchas gracias por su amable atención a nuestra consulta.

Atentamente,

[redacted]

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
GOBIERNO DE EL SALVADOR
UNÁMONOS PARA CRECER

386

San Salvador, 26 de junio de 2018

Señor.
JARET NAUN MORÁN SORTO (JL SECURITY TECHNOLOGIES).
Presente.

En referencia al proceso de Libre Gestión MTPS 12-2018 "ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS" para el Ministerio de Trabajo y Previsión Social; y dado que su oferta ha sido elegida como ganadora del suministro de dicho bienes, con **costo total de** CINCUENTA Y DOS MIL DOSCIENTOS CINCUENTA Y SIETE DÓLARES DE LOS ESTADOS UNIDOS DE AMÉRICA CON OCHENTA Y CUATRO CENTAVOS **($52,257.84)**. Para tal efecto y la formalización del mismo solicito de la manera más atenta tramitar la siguiente documentación:

FOTOCOPIA CERTIFICADA POR NOTARIO DE:

- Copia certificada por notario de DUI y NIT (documentos vigentes a la fecha).
- Copia certificada por notario de constancia de Matricula de Comercio de empresa mercantil, si le fuera aplicable por el monto de sus activos, o en su defecto recibo de pago de la misma o constancia extendida por el Registro de Comercio que la emisión de la matrícula se encuentra en trámite de renovación o primera vez según sea el caso.
- Copia certificada por notario de Escritura de Poder Especial o General con cláusula especial para ofertar y contratar en procesos de contratación pública, inscrito en el Registro de Comercio.

ORIGINALES DE LOS SIGUIENTES DOCUMENTOS:

- Solvencia en original de los Impuestos Municipales del domicilio del establecimiento principal.
- Solvencia en original de la Dirección General de Impuestos Internos.
- Solvencia en original de la Unidad de Pensiones del Instituto Salvadoreño del Seguro Social (UPISSS).
- Solvencia de pago de cotizaciones Obrero-Patronales del Instituto Salvadoreño del Seguro Social (ISSS).
- Solvencias en original de las Administradoras de Fondos de Pensiones CRECER y CONFIA.
- Constancia emitida por el Instituto de Previsión Social de la Fuerza Armada en la que se indique que estás solvente en el pago de cotizaciones y aportes previsionales.

Dichas solvencias y constancias de Registro deberán de **estar vigentes** a la fecha de contratación y los demás documentos solicitados deberán estar **certificados por un notario**. Toda documentación deberá ser presentada, a más tardar, el día 03 de julio de 2018.

Licda. Mayra Yessenia Palma Gutiérrez
Jefe de la Unidad de Adquisiciones y Contrataciones Institucional Ad Honorem

MINISTERIO DE TRABAJO
Y PREVISIÓN SOCIAL

GOBIERNO DE
EL SALVADOR
UNÁMONOS PARA CRECER

385

San Salvador, 26 de junio de 2018

EMPRESA
JARET NAUN MORÁN SORTO (JL SECURITY TECHNOLOGIES).
Presente.

Considerando que se ha dado cumplimiento a los requisitos técnicos y económicos, correspondientes al proceso de **LIBRE GESTIÓN MTPS 12-2018**, para la "ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"

En su oportunidad la Comisión de Evaluación de Ofertas, analizó las propuestas presentadas por las empresas participantes, teniendo en cuenta el cumplimiento de los requerimientos solicitados, a fin de recomendar la adjudicación. De conformidad a lo establecido en el Acta de Evaluación de Ofertas, para este proceso de fecha veintiséis de junio de dos mil dieciocho, la Comisión de Evaluación de Ofertas, recomienda la adjudicación, del proceso de **Libre Gestión MTPS 12-2018** "ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS", de acuerdo a los procedimientos del Ministerio de Trabajo y Previsión Social y de conformidad a la Ley de Adquisiciones y Contrataciones de la Administración Pública. Por lo anterior, SE NOTIFICA LA ADJUDICACIÓN del proceso a:

JARET NAUN MORÁN SORTO, Adjudicado un total de CINCUENTA Y DOS MIL DOSCIENTOS CINCUENTA Y SIETE DÓLARES DE LOS ESTADOS UNIDOS DE AMÉRICA CON OCHENTA Y CUATRO CENTAVOS ($52,257.84). , detallado así:

ÍTEM	CANTIDAD	DESCRIPCIÓN	MARCA Y MODELO	MONTO
1	19	EQUIPOS DE SEGURIDAD PERIMETRAL	**HILLSTONE** **2- modelo T-1860** **12- modelo E-1700 2 Gbps.** **5- modelo E-1700 1.5 Gbps.**	**$47,032.00**
2	19	LICENCIAS PARA EQUIPO DE SEGURIDAD PERIMETRAL	**HILLSTONE** **2- modelo T-1860** **12- modelo E-1700 2 Gbps.** **5- modelo E-1700 1.5 Gbps.**	**$5,225.84**
TOTAL				**$52,257.84**

Para los efectos anteriores se le comunica que la persona designada como Administradora de Contrato y para coordinar este proceso es el ingeniero. Juan Francisco Sánchez, Jefa de Unidad de Desarrollo Tecnológico a quien pueden contactar al **teléfono 2529 – 3725/ 2529 – 3724** o al **correo:** francisco.sanchez@mtps.gob.sv .

Aprovecho la oportunidad para enviarle un atento saludo.

Licda. Mayra Yessenia Palma Gutiérrez
Jefa Unidad de Adquisiciones y Contrataciones Institucional Ad Honorem

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
GOBIERNO DE EL SALVADOR

ACTA SOBRE EL INFORME DE EVALUACIÓN DE OFERTAS

LIBRE GESTIÓN MTPS 12-2018, para la **"ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"**.

En la sala de reuniones de la Dirección Administrativa del Ministerio de Trabajo y Previsión Social, a las catorce horas con treinta minutos del día veintiséis de junio de dos mil dieciocho, reunida la Comisión de Evaluación de Ofertas, nombrada a través de Acuerdo Ministerial número cincuenta de fecha veinte de junio de dos mil dieciocho, constituida por: **Licenciada Yolanda del Carmen Dueñas**, Directora Administrativa; **Licenciada Mayra Yessenia Palma Gutiérrez**, Jefa Ad Honorem de la Unidad de Adquisiciones y Contrataciones Institucional; **Licenciado Luis Mario Flores Guillén**, Jefe de la Unidad Financiera Institucional; **Ingeniero Juan Francisco Sánchez Cabrera**, Jefe de la Unidad de Desarrollo Tecnológico; **Licenciada Sandra Lissette Fuentes Quijano**, Colaboradora Jurídica de la Unidad Jurídica, tomando como referencia las Especificaciones Técnicas requeridas por la Unidad Solicitante, las propuestas técnica y económica presentadas por los oferentes en el proceso de **LIBRE GESTIÓN MTPS 12-2018**, para la **"ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"**. Para dar cumplimiento al Artículo 56 de la Ley de Adquisiciones y Contrataciones de la Administración Pública (LACAP); se procede al análisis y evaluación de las ofertas presentadas en este proceso:

I. Que el día veintidós de junio de dos mil dieciocho, se procedió a la recepción de ofertas del proceso:

NOMBRE DEL OFERENTE	MONTO US $ IVA y CESC Incluido
ACTIVE IT CORP, S.A. DE C.V.	$58,828.10
JARET NAÚN MORÁN SORTO (JL_SECURITY TECNOLOGIES)	$52,257.84
JMTELCOM, S.A. DE C.V.	$58,808.81
DADA DADA Y CIA, S.A. DE C.V.	$56,106.00
DEVEL SECURITY, S.A. DE C.V.	$51,405.90

II. Que la Comisión de Evaluación de Ofertas, verificó el cumplimiento de las **Especificaciones Técnicas y condiciones generales**, determinando que en el resultado de la evaluación técnica, basado en el criterio de cumple y no cumple indicado en el documento de esta Libre Gestión, las empresas participantes obtuvieron el siguiente resultado:

Cuadro de análisis técnico.

"ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS".

ANALISIS TECNICO DE ADQUISICIÓN DE EQUIPO DE SEGURIDAD PERIMETRAL											
SITIO PRINCIPAL Y SITIO REMOTO (SANTA ANA)											
CARACTERISTICA	DESCRIPCIÓN	ACTIVE IT CORP, S.A. DE C.V.		JARET NAÚM MORAN SORTO (JL-SECURITY)		JMTELCOM, S.A. DE C.V.		DADA DADA Y CIA, S.A. DE C.V.		DEVEL SECURITY, S.A. DE C.V.	
		CUMPLE		CUMPLE		CUMPLE		CUMPLE		CUMPLE	
		SI	No	SI	No	SI	No	SI	No	SI	No
Capacidad de usuarios	Hasta 1000	X		X		X		X		X	
Cantidad de equipos	Dos	X		X		X		X		X	
Configuración	Contingencia	X		X		X		X		X	
Almacenamiento	240 GB mínimo	X		X		X		X		X	
Consumo de energía	Fuente redundante	X		X		X		X		X	
Conexiones concurrentes	Mínimo 1 millón	X		X		X		X		X	
AV rendimiento	Mínimo 1.5 GBPS	X		X		X		X			X
IPS rendimiento	Mínimo 2 GBPS	X		X		X		X			X
Firewall rendimiento	Mínimo 4 GBPS	X		X		X		X		X	
Interfaces	Capacidad de ampliación	X		X		X		X		X	
Módulos de protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPsec.	X		X		X		X		X	
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.	X		X		X		X		X	
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.	X		X		X		X		X	
Seguridad web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS.	X		X		X		X		X	
Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, IPsec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.	X		X		X		X		X	

CARACTERISTICA	DESCRIPCIÓN	ACTIVE IT CORP, S.A. DE C.V.		JARET NAÚM MORAN SORTO (IC-SECURITY)		JMTELCOM, S.A. DE C.V.		DADA DADA Y CIA, S.A. DE C.V.		DEVEL SECURITY, S.A. DE C.V.	
		CUMPLE		CUMPLE		CUMPLE		CUMPLE		CUMPLE	
		Si	No	Si	No	Si	No	Si	No	Si	No
Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe permitir / restringir / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador.	X		X		X		X			X
IPS	1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code injection. 5. Bloqueo de actividades relacionadas a P2P e IM.	X		X		X		X		X	
Protección de correo electrónico	Especificar	X		X		X		X		X	
Protección de redes inalámbricas	Especificar	X		X		X		X		X	
		OTRAS									
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.	X		X		X		X		X	
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.	X		X		X		X		X	
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.	X		X		X		X			X
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.	X		X		X		X		X	

ANALISIS TECNICO DE ADQUISICIÓN DE EQUIPO DE SEGURIDAD PERIMETRAL

OFICINAS REGIONALES (A EXCEPCION DE SANTA ANA) Y DEPARTAMENTALES

CARACTERISTICA	DESCRIPCIÓN	ACTIVE IT CORP, S.A. DE C.V.		JARET NAÚM MORAN SORTO (IL-SECURITY)		JMTELCOM, S.A. DE C.V.		DADA DADA Y CIA, S.A. DE C.V.		DEVEL SECURITY, S.A. DE C.V.	
		CUMPLE		CUMPLE		CUMPLE		CUMPLE		CUMPLE	
		SI	No	SI	No	SI	No	SI	No	SI	No
Capacidad de usuarios	Hasta 100	X		X		X		X		X	
Cantidad de equipos	Doce	X		X		X		X		X	
Almacenamiento	64 GB mínimo	X		X		X		X			X
Consumo de energía	Especificar	X		X		X		X		X	
Conexiones concurrentes	Mínimo 600 K	X		X		X		X			X
AV rendimiento	Mínimo 500 MBPS	X		X		X		X			X
IPS rendimiento	Mínimo 400 MBPS	X		X		X		X		X	
Firewall rendimiento	Mínimo 1.5 GBPS	X		X		X		X			X
Interfaces	Capacidad de ampliación	X		X		X		X		X	
Módulos de protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPsec.	X		X		X		X		X	
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.	X		X		X		X		X	
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.	X		X		X		X		X	
Seguridad web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS.	X		X		X		X		X	
Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, IPsec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.	X		X		X		X		X	
Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe permitir / restringir / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.	X		X		X		X		X	
IPS	1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.	X		X		X		X		X	
Protección de correo electrónico	Especificar	X		X		X		X		X	
Protección de redes inalámbricas	Especificar	X		X		X		X		X	

CARACTERISTICA	DESCRIPCIÓN	ACTIVE IT CORP, S.A. DE C.V.		JARET NAÚM MORAN SORTO (JL-SECURITY)		IMTELCOM, S.A. DE C.V.		DADA DADA Y CIA, S.A. DE C.V.		DEVEL SECURITY, S.A. DE C.V.	
		CUMPLE		CUMPLE		CUMPLE		CUMPLE		CUMPLE	
		SI	No	SI	No	SI	No	SI	No	SI	No
OTRAS											
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.	X		X		X		X		X	
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.	X		X		X		X		X	
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.	X		X		X		X			X
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.	X		X		X		X		X	

ANALISIS TECNICO DE ADQUISICIÓN DE EQUIPO DE SEGURIDAD PERIMETRAL

CENTROS DE RECREACIÓN Y ARCHIVO GENERAL

CARACTERISTICA	DESCRIPCIÓN	ACTIVE IT CORP, S.A. DE C.V.		JARET NAÚM MORAN SORTO (JL-SECURITY)		JMTELCOM, S.A. DE C.V.		DADA DADA Y CIA, S.A. DE C.V.		DEVEL SECURITY, S.A. DE C.V.	
		CUMPLE		CUMPLE		CUMPLE		CUMPLE		CUMPLE	
		SI	No	SI	No	SI	No	SI	No	SI	No
Capacidad de usuarios	Hasta 15	X		X		X		X		X	
Cantidad de equipos	Cinco	X		X		X		X		X	
Almacenamiento	64 GB mínimo	X		X		X		X			X
Consumo de energía	Especificar	X		X		X		X		X	
Conexiones concurrentes	Mínimo 600 K	X		X		X		X			X
AV rendimiento	Mínimo 400 MBPS	X		X		X		X			X
IPS rendimiento	Mínimo 300 MBPS	X		X		X		X		X	
Firewall rendimiento	Mínimo 900 MBPS	X		X		X		X			X
Interfaces	Capacidad de ampliación	X		X		X		X		X	
Módulos de protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPsec.	X		X		X		X		X	
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.	X		X		X		X		X	
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.	X		X		X		X		X	
Seguridad web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS.	X		X		X		X		X	
Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, IPsec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.	X		X		X		X		X	
Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe permitir / restringir / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.	X		X		X		X		X	

CARACTERISTICA	DESCRIPCIÓN	ACTIVE IT CORP, S.A. DE C.V.		JARET NAÚM MORAN SORTO (JL-SECURITY)		JMTELCOM, S.A. DE C.V.		DADA DADA Y CIA, S.A. DE C.V.		DEVEL SECURITY, S.A. DE C.V.	
		CUMPLE		CUMPLE		CUMPLE		CUMPLE		CUMPLE	
		SI	No	SI	No	SI	No	SI	No	SI	No
IPS	1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code injection. 5. Bloqueo de actividades relacionadas a P2P e IM.	X		X		X		X		X	
Protección de correo electrónico	Especificar	X		X		X		X		X	
Protección de redes inalámbricas	Especificar	X		X		X		X		X	
OTRAS											
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.	X		X		X		X		X	
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.	X		X		X		X		X	
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.	X		X		X		X			X
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.	X		X		X		X		X	

III. Que los montos propuestos por los oferentes, tiempo de entrega y garantía del producto se detalla de la siguiente manera:

CONDICIONES			ACTIVE IT CORP, S.A. DE C.V.		JARET NAUN MORÁN SORTO (JL SECURITY TECHNOLOGIES)		JMTELCOM, S.A. DE C.V.		DADA DADA Y CIA, S.A. DE C.V.		DEVEL SECURITY, S.A. DE C.V.	
ITEM	CANT	DESCRIPCION	MARCA	TOTAL	MARCA	TOTAL	MARCA	TOTAL	MARCA	TOTAL	MARCA	TOTAL
1	19	EQUIPOS DE SEGURIDAD PERIMETRAL	SOPHOS 2- modelo SG450 12- modelo SG135 5- modelo SG115	$26,472.57	HILLSTONE 2- modelo T-1860 12- modelo E-1700 2 Gbps 5- modelo E-1700 1.5 Gbps	$47,032.00	FORTINET. 2- modelo Fortigate 800D 17- modelo Fortigate 61E	$58,808.81	SOPHOS 2- modelo XG430 12- modelo XG125 5- modelo XG105	$35,952.00	CHECK POINT modelo 5200 modelo 1450 modelo 1430	$51,405.90
2	19	LICENCIAS PARA EQUIPO DE SEGURIDAD PERIMETRAL		$32,355.53		$5,225.84				$20,154.00		
TOTAL DE LA OFERTA			$58,828.10		$52,257.84		$58,808.81		$56,106.00		$51,405.90	
TIEMPO DE ENTREGA			15 días calendario.		Una sola entrega 15 días.		30 días calendario.		35 días calendario.		20 días calendario.	
GARANTIA			Garantía de 1 año y compromiso de presentar garantía de cumplimiento de contrato y buen funcionamiento y calidad de los bienes por el 10% del total adjudicado.		Compromiso de presentar garantía de cumplimiento de contrato y buen funcionamiento y calidad de los bienes por el 10% del total adjudicado.		Garantía 12 meses. Compromiso de presentar garantía de cumplimiento de contrato y buen funcionamiento y calidad de los bienes por el 10% del total adjudicado.		Compromiso de presentar garantía de cumplimiento de contrato y buen funcionamiento y calidad de los bienes por el 10% del total adjudicado.		Compromiso de presentar garantía de cumplimiento de contrato y buen funcionamiento y calidad de los bienes por el 10% del total adjudicado.	

Se verificó la Disponibilidad Presupuestaria correspondiente a la adquisición de los 19 equipos de seguridad perimetral y las 19 licencias de conformidad a los motos ofertados.

IV. Que técnicamente, por la naturaleza de la contratación, se recomienda que un solo proveedor realice el suministro de equipos y licencias.

V. En los anexos de esta acta: análisis técnico y análisis económico, se detalla el cumplimiento de las Especificaciones Técnicas de los oferentes y los precios ofertados.

La Comisión de Evaluación de Ofertas, después de realizar el análisis y evaluación de las ofertas presentadas y con base a las Especificaciones Técnicas solicitadas, **RECOMIENDA:**

- **ADJUDICAR** en forma total el proceso **LIBRE GESTIÓN MTPS 12-2018**, para la **"ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"** de la siguiente manera:

OFERENTE ADJUDICADO: JARET NAUN MORÁN SORTO (JL SECURITY TECHNOLOGIES)

ÍTEM	CANTIDAD	DESCRIPCIÓN	MARCA Y MODELO	MONTO
1	19	EQUIPOS DE SEGURIDAD PERIMETRAL	**HILLSTONE 2- modelo T-1860 12- modelo E-1700 2 Gbps. 5- modelo E-1700 1.5 Gbps.**	**$47,032.00**
2	19	LICENCIAS PARA EQUIPO DE SEGURIDAD PERIMETRAL	**HILLSTONE 2- modelo T-1860 12- modelo E-1700 2 Gbps. 5- modelo E-1700 1.5 Gbps.**	**$5,225.84**
TOTAL				**$52,257.84**

Lo anterior deberá suministrarse de conformidad a lo ofertado por la empresa adjudicada.

No habiendo más que hacer constar se cierra la presente para constancia firmamos.

San Salvador, 26 de junio de 2018.

Licenciada Yolanda del Carmen Dueñas
Directora Administrativa.

Licenciada Mayra Yessenia Palma Gutiérrez.
Jefa Unidad de Adquisiciones y Contrataciones Institucional (Ad Honorem).

Licenciado Luis Mario Flores Guillén
Jefe Unidad Financiera Institucional.

Ingeniero Juan Francisco Sánchez Cabrera
Jefe Unidad de Desarrollo Tecnológico.

Licenciada Sandra Lissette Fuentes Quijada
Colaboradora Jurídica de la Unidad Jurídica.

CUADRO COMPARATIVO DE OFERTAS
PROCESO LIBRE GESTIÓN MTPS 12-2018 "ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS "
MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
UNIDAD DE ADQUISICIONES Y CONTRATACIONES INSTITUCIONAL
San Salvador, 26 de junio de 2018.

CONDICIONES			ACTIVE IT CORP, S.A. DE C.V.		JARET NAUN MORÁN SORTO (JL SECURITY TECHNOLOGIES)		JMTELCOM, S.A. DE C.V.**		DADA DADA Y CIA, S.A. DE C.V.		DEVEL SECURITY, S.A. DE C.V.**	
ITEM	**CANT.**	**DESCRIPCION**	**MARCA**	**TOTAL**	**MARCA**	**TOTAL**	**MARCA**	**TOTAL**	**MARCA**	**TOTAL**	**MARCA**	**TOTAL**
1	19	EQUIPOS DE SEGURIDAD PERIMETRAL	SOPHOS 2- modelo SG450 12- modelo SG135 5- modelo SG115	$26,472.57	HILLSTONE 2- modelo T-1860 12- modelo E-1700 2 Gbps 5- modelo E-1700 1.5 Gbps	$47,032.00	FORTINET. 2- modelo Fortigate 800D 17- modelo Fortigate 61E	$58,808.81	SOPHOS 2- modelo XG430 12- modelo XG125 5- modelo XG105	$35,952.00	CHECK POINT modelo 5200 modelo 1450 modelo 1430	$51,405.90
2	19	LICENCIAS PARA EQUIPO DE SEGURIDAD PERIMETRAL		$32,355.53		$5,225.84				$20,154.00		
TOTAL DE LA OFERTA			$58,828.10		$52,257.84		$58,808.81		$56,106.00		$51,405.90	
VALIDEZ DE LA OFERTA			30 días calendario.		30 días calendario.		60 días calendario.		30 días calendario.		60 días calendario.	
TIEMPO DE ENTREGA			15 días calendario.		Una sola entrega 15 días.		30 días calendario.		35 días calendario.		20 días calendario.	
FORMA DE PAGO			Crédito 30 días calendario		Crédito 60 días.		Crédito 60 días.		Crédito a 60 días despues de entregado el equipo.		Crédito de 60 días	
GARANTIA			Garantía de 1 año y compromiso de presentar garantía de cumplimiento de contrato y buen funcionamiento y calidad de los bienes por el 10% del total adjudicado.		Compromiso de presentar garantía de cumplimiento de contrato y buen funcionamiento y calidad de los bienes por el 10% del total adjudicado..		Garantía 12 meses. Compromiso de presentar garantía de cumplimiento de contrato y buen funcionamiento y calidad de los bienes por el 10% del total adjudicado.		Compromiso de presentar garantía de cumplimiento de contrato y buen funcionamiento y calidad de los bienes por el 10% del total adjudicado.		Compromiso de presentar garantía de cumplimiento de contrato y buen funcionamiento y calidad de los bienes por el 10% del total adjudicado.	

*Los precios incluyen los impuestos respectivos (IVA y CESC), según solicitado por la Institución.

** Las empresas JMTELCOM, S.A. DE C.V. y DEVEL SECURITY, S.A. DE C.V. no detallan el costo de los equipos y licencias por separado, de igual forma la ésta ultima detalla el costo de soporte tecnico.

MONTO DISPONIBLE:		**$64,500.00**
61104	Equipo	$6,500.00
61403	Licencias	$58,000.00

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL -MTPS-

GOBIERNO DE EL SALVADOR
UNÁMONOS PARA CRECER

Unidad de Desarrollo Tecnológico

MEMORANDUM

UDT/151/2018/ FS

Para: **Licda. Mayra Palma**
Jefa Ad-honorem UACI

De: **Ing. Juan Francisco Sánchez**
Jefe Unidad de Desarrollo Tecnológico

Asunto: **Análisis Técnico**
"Adquisición de 19 Equipos de Seguridad Perimetral con Licencias"

Fecha: **25 de junio de 2018**

En respuesta a memorando de fecha 22 de junio de 2018, referente al proceso de Libre Gestión MTPS 12-2018, sobre la **"Adquisición de 19 Equipos de Seguridad Perimetral con Licencias",** de las ofertas presentadas por las empresas:

- ACTIVE IT CORP, S.A. DE C.V.
- JARET NAUM MORAN SORTO (JL_SECURITY TECNOLOGIES)
- JMTELCOM, S.A DE C.V.
- DADA DADA Y CIA, S.A. DE C.V.
- DEVEL SECURITY, S.A. DE C.V.

De las ofertas presentadas, se ha recibido cuatro marcas (dos empresas presentaron misma marca, distinta familia o modelo), de cinco empresas que han presentado ofertas, cuatro cumplen en todo, de cuatro ofertas que cumplen en todo, dos harían entrega en 15 días, de dos empresas que entregarían en quince días una tiene el costo más bajo.

Remito en anexo análisis técnico del proceso.

Atentamente,

MINISTERIO DE TRABAJO Y PREVISION SOCIAL
25 JUN. 2018
RECIBIDO
UACI
12:10 PM

ANALISIS TECNICO DE ADQUISICIÓN DE EQUIPO DE SEGURIDAD PERIMETRAL

SITIO PRINCIPAL Y SITIO REMOTO (SANTA ANA)

CARACTERISTICA	DESCRIPCIÓN	ACTIVE IT CORP, S.A. DE C.V.		JARET NAÚM MORAN SORTO (JL-SECURITY)		JMTELCOM, S.A. DE C.V.		DADA DADA Y CIA, S.A. DE C.V.		DEVEL SECURITY, S.A. DE C.V.	
		CUMPLE		CUMPLE		CUMPLE		CUMPLE		CUMPLE	
		Si	No	Si	No	Si	No	Si	No	Si	No
Capacidad de usuarios	Hasta 1000	X		X		X		X		X	
Cantidad de equipos	Dos	X		X		X		X		X	
Configuración	Contingencia	X		X		X		X		X	
Almacenamiento	240 GB mínimo	X		X		X		X		X	
Consumo de energía	Fuente redundante	X		X		X		X		X	
Conexiones concurrentes	Mínimo 1 millón	X		X		X		X		X	
AV rendimiento	Mínimo 1.5 GBPS	X		X		X		X			X
IPS rendimiento	Mínimo 2 GBPS	X		X		X		X			X
Firewall rendimiento	Mínimo 4 GBPS	X		X		X		X		X	
Interfaces	Capacidad de ampliación	X		X		X		X		X	
Módulos de protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPsec.	X		X		X		X		X	
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.	X		X		X		X		X	
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.	X		X		X		X		X	
Seguridad web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS.	X		X		X		X		X	
Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, IPsec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.	X		X		X		X		X	

CARACTERISTICA	DESCRIPCIÓN	ACTIVE IT CORP, S.A. DE C.V.		JARET NAÚM MORAN SORTO (JL-SECURITY)		JMTELCOM, S.A. DE C.V.		DADA DADA Y CIA, S.A. DE C.V.		DEVEL SECURITY, S.A. DE C.V.	
		CUMPLE		CUMPLE		CUMPLE		CUMPLE		CUMPLE	
		Si	No	Si	No	Si	No	Si	No	Si	No
Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe permitir / restringir / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador.	X		X		X		X			X
IPS	1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.	X		X		X		X		X	
Protección de correo electrónico	Especificar	X		X		X		X		X	
Protección de redes inalámbricas	Especificar	X		X		X		X		X	
OTRAS											
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.	X		X		X		X		X	
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.	X		X		X		X		X	
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.	X		X		X		X			X
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.	X		X		X		X		X	

ANALISIS TECNICO DE ADQUISICIÓN DE EQUIPO DE SEGURIDAD PERIMETRAL

OFICINAS REGIONALES (A EXCEPCION DE SANTA ANA) Y DEPARTAMENTALES

CARACTERISTICA	DESCRIPCIÓN	ACTIVE IT CORP, S.A. DE C.V.		JARET NAÚM MORAN SORTO (JL-SECURITY)		JMTELCOM, S.A. DE C.V.		DADA DADA Y CIA, S.A. DE C.V.		DEVEL SECURITY, S.A. DE C.V.	
		CUMPLE		CUMPLE		CUMPLE		CUMPLE		CUMPLE	
		SI	No	SI	No	SI	No	SI	No	SI	No
Capacidad de usuarios	Hasta 100	X		X		X		X		X	
Cantidad de equipos	Doce	X		X		X		X		X	
Almacenamiento	64 GB mínimo	X		X		X		X			X
Consumo de energía	Especificar	X		X		X		X		X	
Conexiones concurrentes	Mínimo 600 K	X		X		X		X			X
AV rendimiento	Mínimo 500 MBPS	X		X		X		X			X
IPS rendimiento	Mínimo 400 MBPS	X		X		X		X		X	
Firewall rendimiento	Mínimo 1.5 GBPS	X		X		X		X			X
Interfaces	Capacidad de ampliación	X		X		X		X		X	
Módulos de protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPsec.	X		X		X		X		X	
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.	X		X		X		X		X	
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.	X		X		X		X		X	
Seguridad web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS.	X		X		X		X		X	
Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, IPsec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.	X		X		X		X		X	
Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe permitir / restringir / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.	X		X		X		X		X	
IPS	1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.	X		X		X		X		X	
Protección de correo electrónico	Especificar	X		X		X		X		X	
Protección de redes inalámbricas	Especificar	X		X		X		X		X	

CARACTERISTICA	DESCRIPCIÓN	ACTIVE IT CORP, S.A. DE C.V.		JARET NAÚM MORAN SORTO (JL-SECURITY)		JMTELCOM, S.A. DE C.V.		DADA DADA Y CIA, S.A. DE C.V.		DEVEL SECURITY, S.A. DE C.V.	
		CUMPLE		CUMPLE		CUMPLE		CUMPLE		CUMPLE	
		SI	No	SI	No	SI	No	SI	No	SI	No
OTRAS											
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.	X		X		X		X		X	
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.	X		X		X		X		X	
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.	X		X		X		X			X
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.	X		X		X		X		X	

ANALISIS TECNICO DE ADQUISICIÓN DE EQUIPO DE SEGURIDAD PERIMETRAL

CENTROS DE RECREACIÓN Y ARCHIVO GENERAL

CARACTERISTICA	DESCRIPCIÓN	ACTIVE IT CORP, S.A. DE C.V.		JARET NAÚM MORAN SORTO (JL-SECURITY)		JMTELCOM, S.A. DE C.V.		DADA DADA Y CIA, S.A. DE C.V.		DEVEL SECURITY, S.A. DE C.V.	
		CUMPLE		CUMPLE		CUMPLE		CUMPLE		CUMPLE	
		SI	No	SI	No	SI	No	SI	No	SI	No
Capacidad de usuarios	Hasta 15	X		X		X		X		X	
Cantidad de equipos	Cinco	X		X		X		X		X	
Almacenamiento	64 GB mínimo	X		X		X		X			X
Consumo de energía	Especificar	X		X		X		X		X	
Conexiones concurrentes	Mínimo 600 K	X		X		X		X			X
AV rendimiento	Mínimo 400 MBPS	X		X		X		X			X
IPS rendimiento	Mínimo 300 MBPS	X		X		X		X		X	
Firewall rendimiento	Mínimo 900 MBPS	X		X		X		X			X
Interfaces	Capacidad de ampliación	X		X		X		X		X	
Módulos de protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPsec.	X		X		X		X		X	
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.	X		X		X		X		X	
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.	X		X		X		X		X	
Seguridad web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS.	X		X		X		X		X	
Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, IPsec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.	X		X		X		X		X	
Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe permitir / restringir / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.	X		X		X		X		X	

CARACTERISTICA	DESCRIPCIÓN	ACTIVE IT CORP, S.A. DE C.V.		JARET NAÚM MORAN SORTO (JL-SECURITY)		JMTELCOM, S.A. DE C.V.		DADA DADA Y CIA, S.A. DE C.V.		DEVEL SECURITY, S.A. DE C.V.	
		CUMPLE		CUMPLE		CUMPLE		CUMPLE		CUMPLE	
		Si	No	Si	No	Si	No	Si	No	Si	No
IPS	1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.	X		X		X		X		X	
Protección de correo electrónico	Especificar	X		X		X		X		X	
Protección de redes inalámbricas	Especificar	X		X		X		X		X	
OTRAS											
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.	X		X		X		X		X	
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.	X		X		X		X		X	
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.	X		X		X		X			X
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.	X		X		X		X		X	

Active IT corp

[redacted]

San Salvador, 26 de junio de 2018

Señores
Ministerio de Trabajo y Previsión Social- MTPS
Unidad de Adquisiciones y Contrataciones Institucional- UACI
Presente.

Atención: Licda. Mayra Palma
Jefa UACI Ad Honorem

EstimadaSeñores:

Referente al proceso LG MTPS 12- 2018 denominado "ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS" informamos que nuestra oferta incluye los impuestos de IVA y CESC en los equipos ofertados y el impuesto IVA en las licencias ofertadas.

Sin otro particular, nos suscribimos de ustedes.

Atentamente,

[redacted]

Representante Legal

[redacted]

DevelSecurity
PROFESSIONAL SERVICES

San Salvador, 25 de Junio de 2018.

Ministerio de Trabajo y Previsión Social.
Presente.

Por este medio manifestamos que nuestros clientes pertenecen al sector financiero por motivos de confidencialidad nuestros clientes no proporcionan cartas de referencia, ya que ambas partes firmamos el acuerdo de confidencialidad y no divulgación de información.

Cualquier información adicional o aclaración requerida con gusto estaremos dispuestos a suministrarla.

Atentamente.

[redacted]

Gerente de país.

[redacted]

[redacted]

Check Point
SOFTWARE TECHNOLOGIES, INC.

CLOUD · MOBILE · THREAT PREVENTION

WELCOME TO THE FUTURE OF CYBER SECURITY

Guatemala, Junio 21, 2018

Señores:
Ministerio de Trabajo y Prevision Social
Presente.

Ref. Certificado Canal Autorizado - Check Point Software Technologies.

Por medio de la presente certificamos que la compañía **Devel Security**, es canal de Check Point en **El Salvador**, con un nivel de **2** estrellas, lo cual los autoriza para comercializar nuestro portafolio de soluciones y servicios de seguridad.

Si tiene cualquier consulta, por favor no dude en contactarse con Oswaldo Cuevas, Territory Manager, al correo ocuevas@checkpoint.com o al teléfono móvil +502-5129-6010.

Atentamente,

[redacted]

Territory Manager
Check Point Software Technologies

[redacted]

DevelSecurity
PROFESSIONAL SERVICES

San Salvador, 25 de Junio de 2018.

Ministerio de Trabajo y Previsión Social.
Presente.

Por este medio manifestamos que la propuesta económica incluye IVA y CESC.

El plazo de entrega será de 20 días calendario a partir de la recepción de la orden de compra.

Cualquier información adicional o aclaración requerida con gusto estaremos dispuestos a suministrarla.

Atentamente.

[redacted]

[redacted]

367

DevelSecurity
PROFESSIONAL SERVICES

San Salvador, 25 de Junio de 2018.

Ministerio de Trabajo y Previsión Social.
Presente.

Por este medio manifestamos la clasificación de la categoría:

Nombre del Contribuyente: Devel Security S.A. de C.V.
NIT [redacted]
No de Registro: [redacted]
Giro: [redacted]
Categoría: [redacted]

Cualquier información adicional o aclaración requerida con gusto estaremos dispuestos a suministrarla.

Atentamente.

[redacted]

[redacted]

En la ciudad de San Salvador, departamento de San Salvador, a las diecisiete horas del día veinticinco de junio de dos mil dieciocho. **ANTE MI,** [redacted], Notario, del domicilio de [redacted] Departamento de [redacted] comparece la licenciada [redacted], de [redacted] años de edad, soltera, [redacted], Licenciada en [redacted], del domicilio de [redacted] a quien conozco portadora de su Documento Único de Identidad número [redacted], actuando en su calidad de [redacted] Y APODERADA LEGAL de la Sociedad **DEVEL SECURITY, SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE** entidad constituida y existente de conformidad con las leyes de la República de El Salvador y acredito su personería con Escritura pública de constitución de la sociedad, otorgada en la ciudad de San Salvador, a las diez horas y treinta minutos del día seis de enero de dos mil catorce, ante los oficios de la notario [redacted] inscrita en el Registro de Comercio, el día diez de enero de dos mil catorce, con el número [redacted] del Libro [redacted] del Registro de Sociedades; y en la calidad en que actúa **ME DICE:** Que con el objeto de participar en proceso por Libre Gestión número **LG MTPS doce** relativa a "**Adquisición de diecinueve equipos de seguridad perimetral con licencias ". BAJO JURAMENTO DECLARA: I)** Que en toda la cadena de servicios profesionales en seguridad informática y de la información ofertadas a la institución por la empresa que representa, no se utiliza trabajo realizado por niños, niñas, adolescente por debajo de la edad mínima de adquisición al empleo y se cumple en todo proceso, productivo, con la normativa laboral vigente y con las regulaciones relativas a la protección integral de la niñez y adolescencia, que tienen por objeto garantizar el goce y respeto pleno de los derechos los niños, niñas y adolescentes. **II)** Que se cumpla con la normativa nacional relacionada con la protección de la persona adolescente trabajadora, especialmente aquella relativa a la realización de actividades y trabajos peligrosos. **III)** Que se compromete a vigilar para la empresa que representa, así como sus proveedores, contratistas y subcontratistas en toda la cadena de producción, estén libres de trabajo infantil y se respete el marco legal de protección de la persona adolescente trabajadora. El suscrito notario hace constar que hice el conocimiento al compareciente regulado en el código penal, en cuanto al delito de falsedad ideológica, regulado en el artículo doscientos ochenta y cuatro. El compareciente me manifiesta que para efectos legales de la empresa acta notarial y para los que surgieren en el proceso de licitación, señala como domicilio especial el de esta ciudad a cuyos tribunales se somete expresamente. Así se expresó la compareciente a quien explique los efectos legales de este instrumento notarial que consta de un folio útil y leído que le fue por mí íntegramente en un solo acto sin interrupción, ratifica su contenido y firmamos. **DOY FE.**

.....[redacted].....

[redacted]

[redacted]

JL SECURITY TECHNOLOGIES
Seguridad en Internet

Security Technologies

Hillstone NETWORKS

San Salvador, 26 de junio de 2018

Señores
Ministerio de Trabajo y Previsión Social
Atención: UACI
Presente

Reciba un cordial saludo de JL Security Technologies deseándole éxitos en sus labores.

Me refiero al Proceso de Libre Gestión LG MTPS 12-2018 "ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS", en el cual me encuentro participando, por este medio expreso que el precio ofertado de los equipos incluye el impuesto de Contribución Especial para la Seguridad Ciudadana y Convivencia (CESC).

Sin otro particular por el momento, me suscribo de usted, no sin antes agradecerles el tomar en cuenta nuestra oferta.

Atentamente,

[redacted]

[redacted]

[redacted]

364

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
GOBIERNO DE EL SALVADOR
UNIDOS CRECEMOS TODOS

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
Unidad de Adquisiciones y Contrataciones Institucional

PROCESOS DE LIBRE GESTIÓN
LG MTPS 12-2018 "ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"

San Salvador, 25 de junio de 2018.

Señores:
JARET NAUN MORAN SORTO
Presente.

En relación a la oferta entregada por ustedes el día 22 de junio de 2018 y de acuerdo a lo indicado en el documento de Especificaciones Técnicas: "para facilitar el proceso de revisión, evaluación y comparación de ofertas, el contratante podrá a su discreción solicitar a los oferentes aclaraciones de sus ofertas" por este medio se solicita la siguiente:

Aclarar si dentro del precio oferta se encuentra incluido el impuesto de Contribución Especial para la Seguridad Ciudadana y Convivencia (CESC)

Dicha documentación tiene que ser presentada a la oficina de la UACI del Ministerio de Trabajo y Previsión Social, ubicada en 17 Avenida norte y Alameda Juan Pablo II, Centro de Gobierno, Edificio del Ministerio de Trabajo No. 3, primer nivel, a más tardar **el 26 de junio de 2018**, antes de las **10:30 a.m.**

Atentamente,

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
UACI
EL SALVADOR, C.A.

Licda. Mayra Yessenia Palma Gutiérrez
Jefa de la Unidad de Adquisiciones y Contrataciones Institucional Ad Honorem.
Ministerio de Trabajo y Previsión Social.

363

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
GOBIERNO DE EL SALVADOR
UNIDOS CRECEMOS TODOS

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
Unidad de Adquisiciones y Contrataciones Institucional

PROCESOS DE LIBRE GESTIÓN
LG MTPS 12-2018 "ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"

San Salvador, 25 de junio de 2018.

Señores:
DEVEL SECURITY, S.A. DE C.V.
Presente.

En relación a la oferta entregada por ustedes el día 22 de junio de 2018 y de acuerdo a lo indicado en el documento de Especificaciones Técnicas: "para facilitar el proceso de revisión, evaluación y comparación de ofertas, el contratante podrá a su discreción solicitar a los oferentes aclaraciones de sus ofertas" por este medio se solicita la siguiente:

- Aclarar si dentro del precio oferta se encuentra incluido el impuesto de Contribución Especial para la Seguridad Ciudadana y Convivencia (CESC)
- Plazo de entrega de los bienes ofertados

Dicha documentación tiene que ser presentada a la oficina de la UACI del Ministerio de Trabajo y Previsión Social, ubicada en 17 Avenida norte y Alameda Juan Pablo II, Centro de Gobierno, Edificio del Ministerio de Trabajo No. 3, primer nivel, a más tardar **el 26 de junio de 2018**, antes de las **10:30 a.m.**

Atentamente,

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
UNIDAD DE ADQUISICIONES Y CONTRATACIONES INSTITUCIONAL
UACI
EL SALVADOR, C.A.

Licda. Mayra Yessenia Palma Gutiérrez
Jefa de la Unidad de Adquisiciones y Contrataciones Institucional Ad Honorem.
Ministerio de Trabajo y Previsión Social.

362

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
GOBIERNO DE EL SALVADOR
UNIDOS CRECEMOS TODOS

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
Unidad de Adquisiciones y Contrataciones Institucional

PROCESOS DE LIBRE GESTIÓN
LG MTPS 12-2018 "ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"

San Salvador, 25 de junio de 2018.

Señores:
ACTIVE IT CORP, S.A. DE C.V.
Presente.

En relación a la oferta entregada por ustedes el día 22 de junio de 2018 y de acuerdo a lo indicado en el documento de Especificaciones Técnicas: "para facilitar el proceso de revisión, evaluación y comparación de ofertas, el contratante podrá a su discreción solicitar a los oferentes aclaraciones de sus ofertas" por este medio se solicita la siguiente:

- Aclarar si dentro del precio oferta se encuentra incluido el impuesto de Contribución Especial para la Seguridad Ciudadana y Convivencia (CESC)

Dicha documentación tiene que ser presentada a la oficina de la UACI del Ministerio de Trabajo y Previsión Social, ubicada en 17 Avenida norte y Alameda Juan Pablo II, Centro de Gobierno, Edificio del Ministerio de Trabajo No. 3, primer nivel, a más tardar **el 26 de junio de 2018**, antes de las **10:30 a.m.**

Atentamente,

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
UNIDAD DE ADQUISICIONES Y CONTRATACIONES INSTITUCIONAL
UACI
SAN SALVADOR, EL SALVADOR, C.A.

Licda. Mayra Yessenia Palma Gutiérrez
Jefa de la Unidad de Adquisiciones y Contrataciones Institucional Ad Honorem.
Ministerio de Trabajo y Previsión Social.

Dada Dada & Cia. S.A. de C.V.
Soluciones Integrales de Tecnología

[redacted]

Señores,
Ministerio de Trabajo y Previsión Social
Att. Licda. Mayra Yessenia Palma Gutiérrez
Jefe UACI
Presente.

ASUNTO:
Entrega de documentación subsanable

Estimados Señores:

Nos referimos al Proceso por Libre Gestión LG MTPS 12-2018 "Adquisición de 19 Equipos de Seguridad Perimetral con Licencias"

Por este medio estamos presentando la siguiente documentación solicitada:

- 1 Referencia de empresa pública o privada de acuerdo a Anexo 4, **Se presenta carta emitida por el ISRI.**
- Carta compromiso de presentación de Garantía de Cumplimiento de Contrato y Garantía de Buen Funcionamiento, por el valor del 10% del monto adjudicado.

Sin más que agradecer su atención a la presente,

Atentamente,

[redacted]

MINISTERIO DE TRABAJO Y PREVISION SOCIAL
26 JUN. 2018
RECIBIDO
UACI

[redacted]

NECDM

360

ANEXO No. 4

DADA DADA y COMPAÑÍA S.A. de C.V.

I. DATOS GENERALES DE LA INSTITUCION:

1. Nombre de la Institución: Instituto Salvadoreño de Rehabilitación Integral
2. Dirección: [redacted]
   Número Telefónico [redacted]
   Fax: N/A
   Correo electrónico: informática@isri.gob.sv

3. A continuación proporcionar los siguientes datos:

II. IDENTIFICACION DEL CONTRATO:

NOMBRE DEL CONTRATO: SUMINISTRO DE FIREWALL PARA LA DIFERENTES DEPENDENCIAS DEL ISRI	
FECHA INICIO (DIA, MES, AÑO)	1 de Abril de 2016
FECHA DE FINALIZACION (DIA, MES, AÑO)	31 de Diciembre de 2018
MONTO DEL CONTRATO EN US $	US$ 32,572.96 • 3 Contratos consecutivos.

III. CALIDAD DEL SERVICIO

INDICAR LA CALIDAD DEL SERVICIO RECIBIDO: MARCAR CON UNA "X" UNA SOLA VALORACION:	Regular ( ) Bueno ( ) Muy Bueno ( ) Excelente (X)

Y para ser presentada a la Unidad de Adquisiciones y Contrataciones Institucionales (UACI), del Ministerio de Trabajo y Previsión Social, se extiende la presente constancia en la ciudad de San Salvador a los veintiséis días del mes de junio de dos mil dieciocho.

FIRMA: [redacted]	SELLO DE LA INSTITUCION [redacted]
NOMBRE: [redacted]	
CARGO: Coordinador de Informática.	

[redacted]

Dada Dada & Cia. S.A. de C.V.
Soluciones Integrales de Tecnología

[redacted]

Señores,
Ministerio de Trabajo y Previsión Social
Att. Licda. Mayra Yessenia Palma Gutiérrez
Jefe UACI
Presente.

ASUNTO:
Carta compromiso de presentación de garantías.

Estimados Señores:
r
Nos referimos al Proceso por Libre Gestión LG MTPS 12-2018 "Adquisición de 19 Equipos de Seguridad Perimetral con Licencias"

Por este medio a través de mi persona como Apoderado Especial Administrativo de la empresa DADA DADA Y CIA, S.A. DE C.V. en caso de ser adjudicados en el proceso en mención nos comprometemos a presentar las siguientes garantías.

- Garantía de Cumplimiento de Contrato, por el valor del 10% del monto adjudicado.
- Garantía de Buen Funcionamiento, por el valor del 10% del monto adjudicado

Y para los usos que la Institución estime conveniente extendemos la presente,

Atentamente,

[redacted]

NECDM

[redacted]

358

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
GOBIERNO DE EL SALVADOR
UNIDOS CRECEMOS TODOS

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
Unidad de Adquisiciones y Contrataciones Institucional

PROCESOS DE LIBRE GESTIÓN
LG MTPS 12-2018 "ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"

San Salvador, 25 de junio de 2018.

Señores:
DADA, DADA Y CIA, S.A. C.V.
Presente.

En relación a la oferta entregada por ustedes el día 22 de junio de 2018 y de acuerdo a lo indicado en el documento de Especificaciones Técnicas del proceso se le solicita:

- 1 referencia de empresas públicas o privadas de acuerdo a Anexo 4 del documento.
- Compromiso de presentar garantía de cumplimiento de contrato, por el valor del 10% del monto adjudicado;
- Compromiso de presentar garantía de Buen Funcionamiento, por el valor del 10% del monto adjudicado

Dicha documentación tiene que ser presentada a la oficina de la UACI del Ministerio de Trabajo y Previsión Social, ubicada en 17 Avenida norte y Alameda Juan Pablo II, Centro de Gobierno, Edificio del Ministerio de Trabajo No. 3, primer nivel, a más tardar **el 26 de junio de 2018**, antes de las **9:30 a.m.**

Atentamente,

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL UNIDAD DE ADQUISICIONES Y CONTRATACIONES INSTITUCIONAL UACI EL SALVADOR, C.A.

Licda. Mayra Yessenia Palma Gutiérrez
Jefa de la Unidad de Adquisiciones y Contrataciones Institucional Ad Honorem.
Ministerio de Trabajo y Previsión Social.

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
GOBIERNO DE EL SALVADOR
UNIDOS CRECEMOS TODOS

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
Unidad de Adquisiciones y Contrataciones Institucional

PROCESOS DE LIBRE GESTIÓN
LG MTPS 12-2018 "ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"

San Salvador, 25 de junio de 2018.

Señores:
DEVEL SECURITY, S.A. DE C.V.
Presente.

En relación a la oferta entregada por ustedes el día 22 de junio de 2018 y de acuerdo a lo indicado en el documento de Especificaciones Técnicas del proceso se le solicita:

- 3 referencias de empresas públicas o privadas de acuerdo al Anexo 4 del documento
- Declaración Jurada de tipo de categoría de la empresa emitida por el Ministerio de Hacienda.
- Declaración Jurada de no utilización de trabajo de niñas, niños y adolescentes según anexo 5 del documento.

Dicha documentación tiene que ser presentado a la oficina de la UACI del Ministerio de Trabajo y Previsión Social, ubicada en 17 Avenida norte y Alameda Juan Pablo II, Centro de Gobierno, Edificio del Ministerio de Trabajo No. 3, primer nivel, a más tardar **el 26 de junio de 2018**, antes de las **9:30 a.m.**

Atentamente,

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL - UNIDAD DE ADQUISICIONES Y CONTRATACIONES INSTITUCIONAL - UACI - EL SALVADOR, C.A.

Licda. Mayra Yessenia Palma Gutiérrez
Jefa de la Unidad de Adquisiciones y Contrataciones Institucional Ad Honorem.
Ministerio de Trabajo y Previsión Social.

356

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
GOBIERNO DE EL SALVADOR

UNIDAD DE ADQUISICIONES Y CONTRATACIONES INSTITUCIONAL

MEMORANDUM

Para: **Ing. Juan Francisco Sánchez**
Jefe de la Unidad de Desarrollo Tecnológico.

De: **Licda. Mayra Yessenia Palma Gutiérrez**
Jefa UACI Ad Honorem

ASUNTO: **Remisión de ofertas LG MTPS 12-2018**

FECHA: 22 de junio de 2018

En esta oportunidad me dirijo a usted en referencia al proceso de Libre Gestión MTPS 12-2018, sobre la "adquisición de 19 equipos de seguridad perimetral con licencias", para remitir ofertas presentadas por las siguientes empresas:

- ACTIVE IT CORP, S.A. DE C.V.
- JARET NAÚN MORÁN SORTO (JL_SECURITY TECNOLOGIES)
- JMTELCOM, S.A. DE C.V.
- DADA DADA Y CIA, S.A. DE C.V.
- DEVEL SECURITY, S.A. DE C.V.

Dichas ofertas son remitidas para que se proceda a realizar el análisis técnico de acuerdo a las especificaciones y el criterio de cumple y no cumple, presentar análisis a la brevedad.

Atentamente,

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
22 JUN. 2018
RECIBIDO
Desarrollo Tecnologico
2:20 p.m.

355

DevelSecurity
PROFESSIONAL SERVICES



MTPS
Ministerio de Trabajo y Previsión Social

"Adquisición de 19 equipos de seguridad perimetral con licencias" LG MTPS 12-2018

22/06/2018.

354

Índice

Introducción	3
Certificaciones.	19
Gestión de Escalamiento Técnico en solución de Fallas	21
Carta de distribuidor autorizado.	22
Soporte Premium	23
Propuesta económica.	24
Anexos.	25
Anexo A: Hoja de datos de equipo 5200.	25
Anexo B: Hoja de datos de modelos 1430 y 1450.	28

No se trata de si ocurrirá, sino de cuándo

En cuestión de ciberseguridad no bastan las mejores intenciones, se requiere de los mejores expertos para proteger lo más valioso para su empresa.

Introducción

Las propuestas que se presentan a continuación comprenden la infraestructura identificada para solventar las necesidades de las organizaciones y brindar protección hacia la red corporativa de la misma.

Los productos ofertados, así como los servicios de soporte e implementación reúnen en su totalidad las fortalezas de DEVEL SECURITY mismas que se encuentran concentradas en su experiencia, la cual permite satisfacer las necesidades de su organización. Adicionalmente Devel Security pone a su disposición metodologías exclusivas de implementación, seguimiento y soporte, contamos con personal experto certificado internacionalmente, con altos estándares de calidad que garantizarán un correcto desarrollo de todo el proyecto en sus diferentes etapas y su sostenibilidad en el futuro.

Poseemos un portafolio integral de servicios y soluciones en seguridad de la información, nos se complace en poder ofrecerle la mejor respuesta a su requerimiento, permitiéndole aportar valor a su entidad y ser mucho más competitivo en el mercado.

Lo invitamos a leer el contenido de este documento en donde se detallan los análisis, estudios, fundamentos de las estrategias y acciones a desarrollar, para el sostenimiento de su posición competitiva en el mercado basado en nuestros productos de firewall como servicio gestionado.



"Nuestra excelencia en el servicio, es nuestra propia pasión por la seguridad."

Camilo Fernández
Chief Technology Officer

Objetivos

- Administrar e impider amenazas y ataques en aplicaciones y servicios de su empresa.
- Proveer la experiencia necesaria en seguridad informática para mantenerse al día con las demandas del negocio.
- Proporcionar las herramientas correctas y lo último en tecnología para la resolución de problemas y eventos de seguridad.
- Ingenieros experimentados altamente capacitados.

Especificaciones técnicas

19 equipos de seguridad perimetral con licencias

Características de equipo al que deberá asociarse licenciamiento de seguridad perimetral.

Sitio principal y sitio remoto (Santa Ana)			
Característica	**Descripción**	**Cumple**	
Capacidad de usuarios	Hasta 1000	Sí	
Cantidad de equipos	Dos	Sí	
Configuración	Contingencia	Sí	
Almacenamiento	240 GB mínimo	Sí	
Consumo de energía	Fuente redudante	Sí	
Conexiones concurrentes	Mínimo 1 millón	Sí	
AV rendimiento	Mínimo 1.5 Gbps	No	
IPS rendimiento	Mínimo 2 Gbps	No	
Firewall rendimiento	Mínimo 4 Gbps	Sí	
Interfaces	Capacidad de ampliación	Sí	
Módulos de protección	1. Firewall 2. Protección de red. 3. Seguridad web. 4. Protección de correo electrónico. 5. Protección de redes inalámbricas. 6. Protección para servidor web. 7. VPN punto a punto: SSL, IPSec.	Sí	
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.	Sí	
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, site to site, site to client, y hub and spoke.	Sí	

	3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.		
Seguridad web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como skype, bittorrent, Youtube, etc. 3. Análisis de malware. 4. Filtrado de contenido activo: extensiones de archivos, flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y Radius.	Sí	
Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, Ipsec. 6. Compatibilidad de sistema de autenticación: Radius, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.	Sí	

Filtrado de contenido	1. Sistema de filtrado de contenido web, para http, y https. 2. Debe permitir/restringir/ acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, keyword o frase. 4. Lista de excepción de URL. 5. Bloqueo de Java, Applet, Cookies y ActiveX. 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.	Sí	
IPS	1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP flood, UDP flood, TCP syn flood, smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP,TFTP,NNTP,NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, Oracle, MS SQL, MySQL, Cross-site scripting, code injection. 5. Bloqueo de actividades relacionadas a P2P e IM.	Sí	
Protección de correo electrónico	Especificar	Sí	
Protección de redes inalámbricas	Especificar	No	

Otras			
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.	Sí	
Garantía	Reemplazará en concepto de garantía las veces que sea necesarios que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el	Sí	

	reemplazo en garantía del equipo.		
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.	No	
Capacitación	Brindará capacitación en la configuración y administración de quipo al menos a 4 técnicos del MTPS.	Sí	

Especificaciones técnicas

Características de equipo al que deberá asociarse licenciamiento de seguridad perimetral.

Oficinas regionales (a excepción de Santa Ana) y departamentales.			
Característica	**Descripción**	**Cumple**	
Capacidad de usuarios	Hasta 100	Sí	
Cantidad de equipos	Doce	Sí	
Almacenamiento	64 GB mínimo	No	
Consumo de energía	Especificar	Sí 12V/5.4A 65W	
Conexiones concurrentes	Mínimo 600 K	No	
AV rendimiento	Mínimo 500 Mbps	No	
IPS rendimiento	Mínimo 400 Mbps	Sí	
Firewall rendimiento	Mínimo 1.5 Gbps	No	
Interfaces	Capacidad de ampliación	Sí	
Módulos de protección	1. Firewall 2. Protección de red. 3. Seguridad web. 4. Protección de correo electrónico. 5. Protección de redes inalámbricas. 6. Protección para servidor web. 7. VPN punto a punto: SSL, IPSec.	Sí	
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.	Sí	
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, site to site, site to client, y hub and spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de	Sí	

	certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.		
S ridad web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como skype, bittorrent, Youtube, etc. 3. Análisis de malware. 4. Filtrado de contenido activo: extensiones de archivos, flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y Radius.	Sí	
P ección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, Ipsec. 6. Compatibilidad de sistema de autenticación: Radius, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.	Sí	

Filtrado de contenido	1. Sistema de filtrado de contenido web, para http, y https. 2. Debe permitir/restringir/ acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, keyword o frase. 4. Lista de excepción de URL. 5. Bloqueo de Java, Applet, Cookies y ActiveX. 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.	Sí	
IPS	1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP flood, UDP flood, TCP syn flood, smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP,TFTP,NNTP,NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, Oracle, MS SQL, MySQL, Cross-site scripting, code injection. 5. Bloqueo de actividades relacionadas a P2P e IM.	Sí	

Protección de correo electrónico	Especificar	Sí	
Protección de redes inalámbricas	Especificar	Sí	
Otras			
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.	Sí	
Garantía	Reemplazará en concepto de garantía las veces que sea necesarios que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el	Sí	

	mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.		
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.	No	
Capacitación	Brindará capacitación en la configuración y administración de quipo al menos a 4 técnicos del MTPS.	Sí	

341

Especificaciones técnicas

Características de equipo al que deberá asociarse licenciamiento de seguridad perimetral.

Oficinas regionales (a excepción de Santa Ana) y departamentales.			
Característica	**Descripción**	**Cumple**	
Capacidad de usuarios	Hasta 15	Sí	
Cantidad de equipos	Cinco	Sí	
Almacenamiento	64 GB mínimo	No	
Consumo de energía	Especificar	Sí 12V/5.4A 65W	
Conexiones concurrentes	Mínimo 600 K	No	
AV rendimiento	Mínimo 400 Mbps	No	
IPS rendimiento	Mínimo 300 Mbps	Sí	
Firewall rendimiento	Mínimo 900 Mbps	No	
Interfaces	Capacidad de ampliación	Sí	
Módulos de protección	1. Firewall 2. Protección de red. 3. Seguridad web. 4. Protección de correo electrónico. 5. Protección de redes inalámbricas. 6. Protección para servidor web. 7. VPN punto a punto: SSL, IPSec.	Sí	
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.	Sí	
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, site to site, site to client, y hub and spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de	Sí	

	certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.		
Seguridad web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como skype, bittorrent, Youtube, etc. 3. Análisis de malware. 4. Filtrado de contenido activo: extensiones de archivos, flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y Radius.	Sí	
Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, Ipsec. 6. Compatibilidad de sistema de autenticación: Radius, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.	Sí	

Filtrado de contenido	1. Sistema de filtrado de contenido web, para http, y https. 2. Debe permitir/restringir/ acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, keyword o frase. 4. Lista de excepción de URL. 5. Bloqueo de Java, Applet, Cookies y ActiveX. 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.	Sí		
IPS	1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP flood, UDP flood, TCP syn flood, smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP,TFTP,NNTP,NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, Oracle, MS SQL, MySQL, Cross-site scripting, code injection. 5. Bloqueo de actividades relacionadas a P2P e IM.	Sí		

Protección de correo electrónico	Especificar	Sí	
Protección de redes inalámbricas	Especificar	Sí	
Otras			
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.	Sí	
Garantía	Reemplazará en concepto de garantía las veces que sea necesarios que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el	Sí	

	mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.		
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.	No	
Capacitación	Brindará capacitación en la configuración y administración de quipo al menos a 4 técnicos del MTPS.	Sí	

Certificaciones.



This is to certify that

[redacted]

has demonstrated the knowledge to be a:

Check Point Certified Security Expert

This Day 26th of May , 2015

[redacted]

Check Point
SOFTWARE TECHNOLOGIES LTD.

[redacted]

P/N: 200544 Student ID #: CP0000070205



Check Point Software Technologies Ltd.

This Certifies that

Daniel Suarez

has demonstrated the knowledge to be a

Check Point Certified Security Administrator

This 15 day of October , 2012

Expiration Date: October 15, 2014

[redacted]

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

[redacted]

385

Check Point Software Technologies Ltd.

This Certifies that

Rodrigo Castellanos ID#: CP0000095651

has demonstrated the knowledge to be a

Check Point Certified Security Administrator

This 22 day of May , 2017

Expiration Date: May 22, 2019

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

[redacted]

[redacted]

Check Point Software Technologies Ltd.

This Certifies that

Rodrigo Castellanos ID#: CP0000095651

has demonstrated the knowledge to be a

Check Point Certified Security Expert

This 29 day of May , 2017

Expiration Date: May 29, 2019

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

[redacted]

[redacted]

Gestión de Escalamiento Técnico en solución de Fallas

Como parte de los procesos a considerar, se encuentra el seguimiento de atención a los reportes abiertos. Este proceso determinará la condición que guardan los reportes que están por rebasar o rebasaron los límites establecidos en los SLA's.



Dentro de las mejores prácticas el servicio incorpora políticas de escalamiento sobre las solicitudes que rebasen el límite de tiempo de atención requerido según los acuerdos de niveles de servicio, las cuales generarán notificaciones a los responsables de estas solicitudes por medio de: correo electrónico, telefónico y por el sistema Notificador de la herramienta de Mesa de Servicios.

Dentro del sistema de mesa de ayuda se tendrá toda la información de los responsables de cada nivel (teléfonos de oficina, celulares y particulares) para que puedan estar accesibles para resolver un incidente que se les asigne.

La mesa de ayuda dará seguimiento de problemas y permitirá el escalamiento y notificación de fallas a las diferentes áreas involucradas así:

PRIMER NIVEL DE SOPORTE – Realizado por los ingenieros de gestión de Devel Security en horario 7x24x365. Los tiempos totales de diagnóstico serán especificados como un SLA a definir. Estos tiempos deben tenerse en cuenta para la gestión y administración de todo el proceso de atención de incidentes.

SEGUNDO NIVEL DE SOPORTE – Realizado con apoyo directo de un soporte Interno de Devel Security especializado. Los tiempos totales de diagnóstico serán especificados como un SLA a definir. Estos tiempos deben tenerse en cuenta para la gestión y administración de todo el proceso de atención de incidentes.

TERCER NIVEL DE SOPORTE - El SOC de Devel Security hará el respectivo seguimiento hasta la solución del mismo para documentar el cierre de la falla. Cuando desde un inicio se detecte que hay necesidad de hacer un mantenimiento correctivo que implique el cambio de algún equipo, se hará la respectiva notificación al Cliente.

Nivel de partner CheckPoint 2 estrellas.

333

Carta de distribuidor autorizado.

Check Point
SOFTWARE TECHNOLOGIES, INC.

CLOUD · MOBILE · THREAT PREVENTION
WELCOME TO THE FUTURE OF CYBER SECURITY

Guatemala, Junio 21, 2018

Señores:
Ministerio de Trabajo y Prevision Social
Presente.

Ref. Certificado Canal Autorizado - Check Point Software Technologies.

Por medio de la presente certificamos que la compañía **Devel Security**, es canal de Check Point en **El Salvador**, con un nivel de **2** estrellas, lo cual los autoriza para comercializar nuestro portafolio de soluciones y servicios de seguridad.

Si tiene cualquier consulta, por favor no dude en contactarse con Oswaldo Cuevas, Territory Manager, al correo ocuevas@checkpoint.com o al teléfono móvil +502-5129-6010.

Atentamente,

[redacted]

Territory Manager
Check Point Software Technologies

T 800.429.4391, 650.628.2000 F 650.654.4233 959 Skyway Road, Suite 300, San Carlos, CA 94070 checkpoint.com

Soporte Premium

Este tipo de soporte brinda toda la gestión de la solución adquirida, brindado la administración de la solución por medio de tickets de soporte resueltos dentro del tiempo establecido dentro del contrato de calidad de servicio (SLA). Dentro del soporte técnico Premium se incluyen las siguientes actividades:

Atención en horario hábil (8x5) para nuevos requerimientos o en base al SLA establecido.

- Apoyo en ventanas de mantenimiento y cambios de configuración.
- Generación de nuevos casos de uso bajo demanda.
- Actualizaciones de soluciones e implementación de nuevas funcionalidades.
- Seguimiento, bitácora y plataforma de gestión de cambios solicitados.
- Apoyo y diagnóstico de fallas no críticas.
- Estadísticas de funcionalidad y reportes personalizados.

El soporte Premium viene acompañado de un contrato de calidad de servicio de los más rigurosos del mercado.

Propuesta económica.

Producto o servicio.	Cantidad	Precio unitario	Precio neto
5200 Next Generation Threat Prevention Appliance Firewall, VPN, Advanced Networking and Clustering, Identity Awareness, Mobile Access, IPS, Application Control, URL Filtering, Anti-Virus, Anti-Bot, Anti-Spam, Content Awareness, Network Policy Management, Logging and Status	1	$ 7,971.13	$ 7,971.13
5200 Next Generation Threat Prevention Appliance for High Availability Equipo en alta disponibilidad con productos idénticos al equipo primario.	1	$ 6,376.91	$ 6,376.91
1450 Next Generation Threat Prevention Appliance for 802.11ac WiFi Firewall, VPN, Advanced Networking and Clustering, Identity Awareness, Mobile Access, IPS, Application Control, URL Filtering, Anti-Virus, Anti-Spam, Anti-Bot.	12	$ 1,039.71	$ 12,476.52
1430 Next Generation Threat Prevention Appliance for 802.11ac WiFi Firewall, VPN, Advanced Networking and Clustering, Identity Awareness, Mobile Access, IPS, Application Control, URL Filtering, Anti-Virus, Anti-Spam, Anti-Bot.	5	$ 693.14	$ 3,465.70
Standard Pro Direct Enterprise Support For 1 Year Garantía de hardware para todos los equipos, derecho a actualizaciones de software y nuevos parches e intervención del fabricante en fallas del producto.	1	$ 5,860.64	$ 5,860.64
Devel Security: Servicio de instalación e implementación Instalación, implementación y migración de configuraciones a CheckPoint de oficina central, contingencia y agencias	1	$ 7,910.00	$ 7,910.00
Soporte Técnico - Premium Administración de los firewalls a través de tickets de soporte en tiempos establecidos en el SLA. Las actividades que se incluyen son: - Atención 8x5 para nuevos requerimientos o en base a SLA. - Apoyo en ventanas de mantenimiento y cambios de configuración. - Generación de nuevos casos de uso bajo demanda. - Actualizaciones e implementación de nuevas funcionalidades. - Seguimiento, bitácora y plataforma de gestión de cambios solicitados. - Apoyo y diagnóstico de fallas no criticas. - Estadísticas de funcionalidad y reportes personalizados.	1	$ 7,345.00	$ 7,345.00

Subtotal	$ 51,405.90
Descuento	$ 0.00
IVA (13%)	$ 0.00
Total	**$ 51,405.90**

La presente propuesta tiene una validez de 60 días calendario.
Crédito a 60 días luego de concluir el servicio.
Forma de pago abono a cuenta o cheque.

Nota: Precios ya incluyen IVA.

Anexos.

Anexo A: Hoja de datos de equipo 5200.

CHECK POINT 5200 NEXT GENERATION SECURITY GATEWAY

Small enterprise and branch office security

Product Benefits

- High performance protection against the most advanced cyber attacks
- Unique "first time prevention" for the most sophisticated zero day attack
- Optimized for inspecting SSL encrypted traffic
- Future-proofed technology safeguards against tomorrow's risks
- Centralized control and LOM improves serviceability
- Modular, expandable chassis with flexible I/O options

Product Features

- Simple deployment and management
- Secure remote access to corporate resources from a wide variety of devices
- One network expansion slot to add port density, fiber and fail-open IO card options
- Redundant appliance clustering technologies eliminate a single point of failure

OVERVIEW

The Check Point 5200 Next Generation Security Gateway combines the most comprehensive security protections to safeguard your small enterprise and branch office deployments. The 5200 is a 1U Next Generation Security Gateway with one I/O expansion slot for higher port capacity, a 500GB (HDD) or 240GB (SSD) disk, and optional Lights-Out Management (LOM) for remote management. This powerful Next Generation Security Gateway is optimized to deliver real-world threat prevention to secure your critical assets and environments.

COMPREHENSIVE THREAT PREVENTION

The rapid growth of malware, growing attacker sophistication and the rise of new unknown zero-day threats require a different approach to keep enterprise networks and data secure. Check Point delivers fully integrated, comprehensive Threat Prevention with award-winning SandBlast™ Threat Emulation and Threat Extraction for complete protection against the most sophisticated threats and zero-day vulnerabilities.

Unlike traditional solutions that are subject to evasion techniques, introduce unacceptable delays, or let potential threats through while evaluating files, Check Point SandBlast stops more malware from entering your network. With our solution your employees can work safely no matter where they are and doesn't compromise their productivity.

PERFORMANCE HIGHLIGHTS

Firewall	IPS	NGFW[1]	Threat Prevention[2]
16 Gbps	3 Gbps	2.7 Gbps	1.645 Gbps

Performance measured under ideal testing conditions. Additional performance details on page 4

1. Includes Firewall, Application Control, and IPS Software Blades.

2. Includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection Software Blades using R80.10.

ALL-INCLUSIVE SECURITY SOLUTIONS

Check Point 5200 Next Generation Security Gateways offer a complete and consolidated security solution available in two complete packages:

- NGTP: prevent sophisticated cyber-threats with Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and Email Security.
- NGTX: NGTP with SandBlast Zero-Day Protection, which includes Threat Emulation and Threat Extraction.

PREVENT KNOWN AND ZERO-DAY THREATS

The 5200 Next Generation Security Gateway protects organizations from both known and unknown threats with Antivirus, Anti-Bot, SandBlast Threat Emulation (sandboxing), and SandBlast Threat Extraction technologies.

As part of the Check Point SandBlast Zero-Day Protection solution, the cloud-based Threat Emulation engine detects malware at the exploit phase, even before hackers can apply evasion techniques attempting to bypass the sandbox. Files are quickly quarantined and inspected, running in a virtual sandbox to discover malicious behavior before it enters your network. This innovative solution combines cloud-based CPU-level inspection and OS-level sandboxing to prevent infection from the most dangerous exploits, and zero-day and targeted attacks.

Furthermore, SandBlast Threat Extraction removes exploitable content, including active content and embedded objects, reconstructs files to eliminate potential threats, and promptly delivers sanitized content to users to maintain business flow.

INSPECT ENCRYPTED CONNECTIONS

There is a shift towards more use of HTTPS, SSL and TLS encryption to increase Internet security. At the same time files delivered into the organization over SSL and TLS represent a stealthy attack vector that bypasses traditional security implementations. Check Point Threat Prevention looks inside encrypted SSL and TLS tunnels to detect threats, ensuring users remain in compliance with company policies while surfing the Internet and using corporate data.

INCLUSIVE HIGH PERFORMANCE PACKAGE

Customers with high connection capacity requirements can purchase the affordable High Performance Package (HPP). This includes the base system plus one 4x 1Gb SFP interface card, transceivers, Lights-Out-Management and 16 GB of memory for high connection capacity.

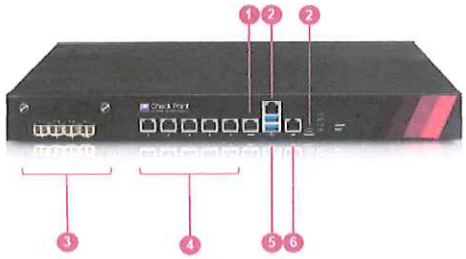
	Base	HPP	Max
1 GbE ports (Copper)	6	6	14
1 GbE ports (Fiber)	0	4	4
Transceivers (SR)	0	4	4
RAM	8GB	16GB	16GB
AC or DC Power Units	1	1	1
Lights Out Management	Optional	Included	Included

REMOTE MANAGEMENT AND MONITORING

An optional Lights-Out-Management (LOM) card provides out-of-band remote management to remotely diagnose, start, restart and manage the Next Generation Security Gateway from a remote location. Administrators can also use the LOM web interface to remotely install an OS image from an ISO file.

5200 SECURITY GATEWAY

1. Management 10/100/1000Base-T RJ45 port
2. RJ45/micro USB console port
3. One network card expansion slot
4. 5x 10/100/1000Base-T RJ45 ports
5. 2x USB ports for ISO installation
6. Lights-Out Management port



328

Performance

Ideal Testing Conditions

- 16 Gbps of UDP 1518 byte packet firewall throughput
- 3 Gbps IPS
- 2.7 Gbps of NGFW[1]
- 1.645 Gbps of Threat Prevention[2]
- 1.88 Gbps of AES-128 VPN throughput
- 125,000 connections per second, 64 byte response
- 3.2/6.4/6.4 million concurrent connections, 64 byte response[3]

Real-World Production Conditions

- 425 SecurityPower Units
- 5.3 Gbps of firewall throughput
- 810 Mbps IPS
- 520 Mbps of NGFW[1]
- 290 Mbps of Threat Prevention[2]

Virtual Systems

- Maximum VS (base/HPP/max memory): 10/20/20

Your performance may vary depending on different factors. Visit www.checkpoint.com/partnerlocator to find an appliance that matches your unique requirements.

1. Includes Firewall, Application Control and IPS Software Blades. 2. Includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection Software Blades using R80.10. 3. Performance measured with default/HPP/maximum memory.

Expansion Options

Base Configuration

- 6 on-board 10/100/1000Base-T RJ-45 ports
- 1x CPUs, 2x physical cores, 2x virtual cores (total)
- 8 GB memory (16 GB option)
- 1x 500GB (HDD) or 1x 240GB (SSD) drive
- 1 power supply (AC or DC)
- Fixed rails (slide rail option)
- (Lights-Out-Management (LOM) option)

Network Expansion Slot Options (1 slot available)

- 8x 10/100/1000Base-T RJ45 port card, up to 14 ports
- 4x 1000Base-F SFP port card, up to 4 ports

Fail-Open/Bypass Network Options

- 4x 10/100/1000Base-T RJ45 port card

Network

Network Connectivity

- Total physical and virtual (VLAN) interfaces per appliance: 1024/4096 (single gateway/with virtual systems)
- 802.3ad passive and active link aggregation
- Layer 2 (transparent) and Layer 3 (routing) mode

High Availability

- Active/Active and Active/Passive - L3 mode
- Session failover for routing change, device and link failure
- ClusterXL or VRRP

IPv6

- NAT66, NAT64
- CoreXL, SecureXL, HA with VRRPv3

Routing

Unicast and Multicast Routing (see SK98226)

- OSPFv2 and v3, BGP, RIP
- Static routes, Multicast routes
- Policy-based routing
- PIM-SM, PIM-SSM, PIM-DM, IGMP v2, and v3

Physical

Power Requirements

- Single Power Supply rating: 250W
- AC power input: 110-240V, (47-63Hz)
- Power consumption maximum: 62.9W
- Maximum thermal output: 214.6 BTU/hr.

Dimensions

- Enclosure: 1RU
- Dimensions (W x D x H): 17.2x16x1.73 in.(438x406.5x44mm)
- Weight: 13.7 lbs. (6.22 kg)

Environmental Conditions

- Operating: 0° to 40°C, humidity 5% to 95%
- Storage: –20° to 70°C, humidity 5% to 95% at 60°C

Certifications

- Safety: UL, CB, CE, TUV GS
- Emissions: FCC, CE, VCCI, RCM/C-Tick
- Environmental: RoHS, WEEE, REACH[1], ISO14001[1]

[1] factory certificate

Anexo B: Hoja de datos de modelos 1430 y 1450.



1400 SECURITY APPLIANCES
BRANCH AND SMALL OFFICE SECURITY

CHECK POINT
1400 APPLIANCES

Branch and Small Office Security

Product Benefits

- All-in-one protection against viruses, spam, bots, dangerous applications, malicious websites and zero-day threats with SandBlast
- Continuous security updates from ThreatCloud™
- Fast set-up, instant protection
- Secure remote access for your mobile workers
- Multiple management options to address any organization's needs

- Simplified web-based local management
-Centralized with our enterprise Security Management or Multi-Domain Management products

Product Features

- Highest ranked Next Generation Firewall
- Profile-based management designed for large-scale deployments
- Multiple internet access options including DSL and support of external 3G/4G/LTE modems
- Integrated 802.11ac wireless security with guest access
- Power over Ethernet (PoE and PoE+) option

THE BRANCH OFFICE CHALLENGE

In the age of global business and a more distributed workforce, remote and branch staff demand access to corporate resources in order to work effectively and efficiently. However, even a small data breach can expose companies to crippling lawsuits, penalties and loss of reputation. Branch offices need an inexpensive, yet effective solution to provide secure access to critical resources from anywhere, while minimizing the risk of a data breach.

OUR SOLUTION

The Check Point 1400 Appliance family is a simple, affordable and easy to deploy all-in-one solution for delivering industry leading security to protect the weakest link in your enterprise network—the remote branch offices. Protect against cyber threats with Check Point Threat Prevention all in a quiet, compact desktop form factor.

	NGTP	+ SandBlast
Firewall	✓	✓
VPN (IPsec)	✓	✓
IPS	✓	✓
Application Control	✓	✓
URL Filtering	✓	✓
Anti-Bot	✓	✓
Anti-Virus	✓	✓
Anti-Spam	✓	✓
SandBlast Threat Emulation	×	✓

* Full SSL/TLS inspection is available when centrally managed

Setup is done in minutes using our step-by-step configuration wizard. The 1400 Appliances are manageable centrally by means of the Check Point enterprise Security Management or Multi-Domain products. Available in two appliances, the 1430/1450 and the 1470/1490, these appliances come standard with eight (8) 1-Gigabit or sixteen (16) Ethernet ports respectively. Connect securely from any device directly or through secure authenticated Wi-Fi.

324

1430/1450 (Wi-Fi DSL options)

1. 802.11n/ac wireless (optional)
2. 6x 1GbE LAN ports
3. 1x 1GbE DMZ port
4. 1x 1GbE WAN port
5. RJ-45/micro USB Console port
6. DSL port
7. 12V power connector
8. USB port



	1430	1450
Ideal Testing Conditions		
Firewall 1518 Byte UDP Packets (Mbps)	2,000	2,500
IPS Throughput (Mbps)	325	575
NGFW Throughput (Mbps) [1]	300	490
Threat Prevention (Mbps) [2]	225	400
VPN AES-128 Throughput (Mbps)	275	500
Connections per Second	20,000	27,000
Concurrent Connections	500,000	500,000
Real-World Production Conditions		
SecurityPower	75	141
Firewall Throughput (Mbps)	900	1,100
IPS Throughput (Mbps)	175	225
NGFW Throughput (Mbps) [1]	100	210
Threat Prevention (Mbps) [2]	90	150
Software		
Security	Firewall, VPN, User Awareness, QoS, Application Control, URL Filtering, IPS, Anti-Bot, Antivirus, Anti-Spam and SandBlast Threat Emulation (sandboxing)	
Unicast, Multicast Routing	OSPFv2, BGPv4 and 4++, RIP, PIM (SM, DM, SSM), IGMP	
Mobile Access User License	100 in default package, 150 maximum	100 in default package, 150 maximum
Hardware		
WAN	1x 10/100/1000Base-T RJ-45 port	
DMZ	1x 10/100/1000Base-T RJ-45 port	
LAN Switch	6x 10/100/1000Base-T RJ-45 ports	
Wi-Fi (optional)	802.11 b/g/n/ac MIMO 3x3	
Radio Band (association rate)	1 radio band: 2.4Ghz (max 450 Mbps) or 5Ghz (max 1300 Mbps)	
Console Port	1x RJ-45, 1x Mini USB	
USB Port	1x USB 3.0	
SD Card Slot	Micro SDHC slot	
3G/4G Modem Support	Yes	
DSL (optional)	VDSL: G.993.1 (VDSL), G.993.2 (VDSL2), G.993.5 (VDSL2 Vectoring), G.998.4 (G.INP) VDSL2 profiles: 8a, 8b, 8c, 8d, 12a, 12b, and 17a ADSL: Annex A (POTS), Annex B (ISDN), G.992.1 (ADSL), G.992.3 (ADSL2), G.992.5 (ADSL2+), Annex M (ADSL2/2+) ,Annex L Reach-extended (ADSL2) Dying Gasp, DSL Forum TR-067, TR-100, TR-114 Conformity	
Dimensions		
Enclosure	Desktop	
Dimensions WxHxD	210 x 42.5 x 155 mm, 8.3 x 1.7 x 6.1 in.	
Weight	1.3 kg (2.8 lbs.)	
Environment		
Operating / Storage	0°C ~ 40°C / -45°C ~ 60°C (5~95%, non-condensing)	
Power Requirements		
AC Input	110 – 240V, 50 – 60 Hz	
Power Supply Rating	12V/3.33A 40W desktop adaptor	
Power Consumption (Max)	25W (non-Wi-Fi), 30W (Wi-Fi option)	
Heat Dissipation	85.3 BTU/hr (non-Wi-Fi), 102.4 BTU/hr (Wi-Fi option)	
Certifications		
Safety / Emissions / Environment	UL/c-UL, IEC 60950 CB / EMC: EN55022 Class B, FCC: Part 15 Class B / RoHS, REACH, WEEE	

[1] Includes Firewall, Application Control and IPS

[2] Includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection

DevelSecurity
PROFESSIONAL SERVICES

San Salvador, 22 de junio de 2018

Señores
Ministerio de Trabajo y Previsión Social
Presente

Yo, Karen Rocio Guzmán Arias , actuando en mi calidad de Representante Legal, de la sociedad Devel Security Sociedad Anónima de Capital Variable, declaro haber leído cada uno de los numerales de las condiciones descritas en las bases de **Licitación Pública No. LG MTPS 12 - 2018,** correspondiente a "**Adquisición de 19 equipos de seguridad perimetral con licencias";** y mediante la presente me comprometo a presentar garantía de cumplimiento de contrato por el valor del 10% del monto adjudicado, en el plazo de cinco días hábiles, posteriores a la entrega y firma del contrato, con una vigencia de quince días calendario. Adicionalmente y en su oportunidad entregaremos también garantía de buen funcionamiento y calidad de los bienes por el valor del 10% del monto adjudicado, en el plazo de cinco días hábiles siguientes a la recepción definitiva de los bienes.

Sin más que expresar
Me suscrito atentamente,

[redacted]

[redacted]

[redacted]

[redacted]

324

Check Point
SOFTWARE TECHNOLOGIES, INC.

CLOUD · MOBILE · THREAT PREVENTION

WELCOME TO THE FUTURE OF CYBER SECURITY

Guatemala, Junio 21, 2018

Señores:
Ministerio de Trabajo y Prevision Social
Presente.

Ref. Certificado Canal Autorizado - Check Point Software Technologies.

Por medio de la presente certificamos que la compañía **Devel Security**, es canal de Check Point en **El Salvador**, con un nivel de **2** estrellas, lo cual los autoriza para comercializar nuestro portafolio de soluciones y servicios de seguridad.

Si tiene cualquier consulta, por favor no dude en contactarse con Oswaldo Cuevas, Territory Manager, al correo ocuevas@checkpoint.com o al teléfono móvil +502-5129-6010.

Atentamente,

[redacted]

[redacted]

DADA-DADA Y COMPAÑÍA S.A. de C.V.

DADA DADA Y CIA.

PRESENTA:

"ADQUICISION DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIA"

REPUBLICA DE EL SALVADOR EN LA AMERICA CENTRAL

Ministerio de Trabajo y Previsión Social

SAN SALVADOR, 22 DE JUNIO DE 2018

[redacted]

DADA DADA & CIA.
Soluciones Integrales de Tecnología

GVP-080A/18

San Salvador, 22 de Junio de 2018

Señores
Ministerio de Trabajo y Previsión Social
Presente.

Atención: Licda. Mayra Palma
Jefe de UACI Ad Honorem

Atentamente sometemos a su consideración nuestra propuesta técnica económica por Suministro y Configuración de una Solución de Firewall con Licencias para Red en el Ministerio de Trabajo y Previsión Social ubicado en San Salvador.

Estamos seguros que la SOLUCION ofrecida a la ***Ministerio de Trabajo y Previsión Social*** *garantizará su correcta operación, convirtiéndose en un excelente aliado tecnológico con el que las necesidades actuales y futuras serán satisfechas.*

Quedamos en espera de sus instrucciones, luego de realizar el correspondiente análisis a la presente propuesta, y aprovechamos para reiterar nuestras más sinceras muestras de respeto y estima.

Atentamente.

[redacted]

[redacted]

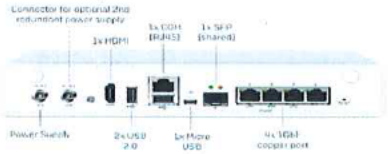
321

INDICE

Descripción	No. de Pagina
Oferta económica	2
Oferta técnica	4
Catálogo de los productos ofertados	12
Carta de fabricante	36
Certificaciones de técnicos	37
Cartas de referencia	41

[redacted]

OFERTA ECONOMICA

Ítem	Cantidad	Precio unitario con IVA y CESC	Descripción	Total con IVA y CESC
1	2	$8,690.00	FIREWALL NGFW SITIO PRINCIPAL Y SITIO REMOTO (SANTA ANA) Marca: **SOPHOS** Modelo: **XG430** País de fabricación: Taiwán/China.  • Precio incluye CESC	**US$ 17,380.00**
1.1	2	$ 7,445.00	Licencia TotalProtect o FullGuard por 1 año para Firewall NGFW marca SOPHOS Modelo **XG430**	**US$ 14,890.00**
2	12	$ 1,236.00	FIREWALL NGFW OFICINAS REGIOMALES (A EXCEPCION SANTA ANA) Y DEPARTAMENTALES Marca: **SOPHOS** Modelo: **XG125** País de fabricación: Taiwán/China.  • Precio incluye CESC	**US$ 14,832.00**
2.1	12	$ 362.00	Licencia EnterpriseProtect por 1 año para Firewall NGFW marca SOPHOS Modelo **XG125**	**US$ 4,344.00**
3	5	$ 748.00	FIREWALL NGFW CENTROS DE RECREACION Y ARCHIVO GENERAL Marca: **SOPHOS** Modelo: **XG105** País de fabricación: Taiwán/China.  • Precio incluye CESC	**US$ 3,740.00**
3.1	5	$ 184.00	Licencia EnterpriseProtect por 1 año para Firewall NGFW marca SOPHOS Modelo **XG105**	**US$ 920.00**
			TOTAL DEL PROYECTO CON IVA Y CESC INCLUIDO...	**US$ 56,106.00**

(Nuestros Precios Totales Incluyen 13% de IVA y 5% de CESC)

DADA-DADA & CIA., S.A. de C.V

[redacted]

De acuerdo a lo establecido en el Art. 26 del Reglamento de la Ley (RELACAP), declaramos que nos encontramos solventes de nuestras obligaciones fiscales, municipales, de seguridad social, provisional y que nos encontramos en capacidad legal de ofertar y contratar con el gobierno.

En nombre de mi representada denominada DADA DADA y CIA. S.A. de C.V. no se emplea a niñas, niños y adolescentes por debajo de la edad mínima de admisión al empleo y se cumple con la normativa que prohíbe el trabajo infantil y de protección de la persona adolescente trabajadora; en caso se comprobare por la Dirección General de Inspección de Trabajo del Ministerio de Trabajo y Previsión Social el incumplimiento a la normativa anterior; reconozco y acepto que la institución contratante iniciará el procedimiento sancionatorio que dispone el art. 160 de la LACAP para determinar el cometimiento o no dentro del procedimiento adquisitivo en el cual estoy participando, de la conducta tipificada como causal de inhabilitación prevista en el art. 158 Romano V literal b) de la LACAP.

CONDICIONES DE LA OFERTA:

Precios estipulados en: Dólares de los Estados Unidos de Norteamérica.

Forma de Pago: Crédito a 60 días después de entregado el equipo.

Lugar de entrega: Según lugares detallados por el cliente.

Validez de la oferta: 30 días calendario después de la fecha de la oferta.

Plazo de entrega: 35 días calendario después de recibir la orden compra.

Notificaciones a: Dirección y Teléfono: 3ª. Calle Pte. Y 21 Av. Nte. Edificio Ericsson, San Salvador.

[redacted]

Correos: [redacted]

Clasificación de la Empresa: Grande_____ **Mediana__X__** Pequeña_____ Micro_____

Agradecemos la oportunidad que nos brinda de poder servirles como ustedes lo merecen.

Atentamente,

[redacted]

[redacted]

[redacted]

ANEXO No. 1

ESPECIFICACIONES TECNICAS

- 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIA

SITIO PRINCIPAL Y SITIO REMOTO (SANTA ANA)				
CARACTERISTICAS	**DESCRIPCION**	**ESPECIFICACIONES TECNICAS OFERTADAS**	**CUMPLE**	
			SI	NO
Capacidad de usuarios	Hasta 1000	**Marca SOPHOS Modelo XG430 Puede soportar hasta 1500 usuarios concurrentes y base de registro de usuario ilimitados. Incluye 1 año de Licencia FullGuard o TotalProtect**	X	
Cantidad de equipos	Dos	2	X	
Configuración	Contingencia	Contingencia y Principal	X	
Almacenamiento	240 GB mínimo	**240 GB tipo SSD**	X	
Consumo de energía	Fuente redundante	**Incluye segunda fuente redundante externa.**	X	
Conexiones concurrentes	Mínimo 1 millón	**20 millones**	X	
AV rendimiento	Mínimo 1.5 GBPS	**6.5 GBPS**	X	
IPS rendimiento	Mínimo 2 GBPS	**9 GBPS**	X	
Firewall rendimiento	Mínimo 4 GBPS	**Hasta 41 GBPS**	X	
Interfaces	Capacidad de ampliación.	**Equipo puede ampliar puertos por medio de flexi port, incluye 8 GbE de Cobre + 2 SFP/SFP+ (no incluye Gbic).**	X	
Módulos de protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPSec	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPSec	X	
Análisis de correlación de amenazas	Correlación de amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.	Correlación de amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.	X	
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client y Hub and Spoke. 3. Soporte de inscripción DES, 3DES y AES 4. Autenticación de certificados IKE 5. El sistema debe tener la capacidad de crear certificados: Locales, CA y CRL.	1. Soporta de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client y Hub and Spoke. 3. Soporta de inscripción DES, 3DES y AES 4. Autenticación de certificados IKE 5. El sistema tiene la capacidad de crear certificados: Locales, CA y CRL.	X	
Seguridad Web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de malware. 4. Filtrado de contenido activo: extensiones de archivos, flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADUIS.	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de malware. 4. Filtrado de contenido activo: extensiones de archivos, flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADUIS.	X	

[redacted]

Protección de red	1. Administración web protegido por contraseña. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces 4. Prevención de intrusos 5. Protección contra DOS. VPN punto a punto: SSL, IPSec. 6. Compatibilidad de sistema de autenticación: RADUIS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.	1. Administración web protegido por contraseña. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces 4. Prevención de intrusos 5. Protección contra DOS. VPN punto a punto: SSL, IPSec. 6. Compatibilidad de sistema de autenticación: RADUIS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico. – Posee suite de reporte iView con multiples tipos de reportes sin costo adicional.	X	
Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http y https. 2. Debe permitir / restringir / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, keyword o Frase. 4. Lista de excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Que permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador 7. Control de aplicaciones.	1. Sistema de filtrado de contenido Web, para http y https. 2. Permite / restringe / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Permite bloqueo de URL, keyword o Frase. 4. Lista de excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permite filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador 7. Control de aplicaciones. 8. QoS de aplicaciones soportado.	X	
IPS	1. Que el UTM Soporte motor IPS para la protección contra ataques. 2. Protección con DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades de protocolos: DNS, FTP, ICMP, IMAP, POP3, RCP, SNMP, TFTP, NNTP. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.	1. El UTM Soporta motor IPS para la protección contra ataques. 2. Protección con DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades de protocolos: DNS, FTP, ICMP, IMAP, POP3, RCP, SNMP, TFTP, NNTP. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.	X	
Protección de correo electrónico	Especificar	Posee modulo anti-spam interno para filtrado de correo no deseado.	X	
Protección de redes inalámbricas	Especificar	Posee controladora de equipos WiFi en marca SOPHOS sin costo adicional (Equipos AP no incluidos)	X	
OTRAS				
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta a fallas en equipo en un máximo de 3 horas posteriores al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días	1. Se instalará y configurará equipo para ponerlo en operación. 2. Se dará respuesta a fallas en equipo en un máximo de 3 horas posteriores al reporte. 3. Se reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Se brindará soporte 24 horas del día, 7 días de la semana, sin costo adicional.	X	

[redacted]

	de la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.	5. Se incluye certificados en la solución ofertada que residen en el país, para atender los requerimientos de soporte técnico.		
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.	Se reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.	X	
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.	1. Se presentan cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Se presenta carta del fabricante para comprobar que es distribuidor autorizado.	X	
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.	Se brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.	X	

OFICINAS REGIOMALES (A EXCEPCION SANTA ANA) Y DEPARTAMENTALES				
CARACTERISTICAS	**DESCRIPCION**	**ESPECIFICACIONES TECNICAS OFERTADAS**	**CUMPLE**	
			SI	NO
Capacidad de usuarios	Hasta 100	**Marca SOPHOS Modelo XG125 Puede soportar hasta 150 usuarios concurrentes, base de registro de usuarios ilimitados. Incluye 1 año de Licencia EnterpriseProtect**	X	
Cantidad de equipos	Doce	12	X	
Almacenamiento	64 GB mínimo	**64 GB tipo SSD**	X	
Consumo de energía	Especificar	100-240 VAC, 50/60 HZ – 36 Watts – Fuente de alimentación eléctrica redundante externa opcional (No Incluida)	X	
Conexiones concurrentes	Mínimo 600 K	**6 millones de conexiones simultáneas.**	X	
AV rendimiento	Mínimo 500 MBPS	**700 MBPS**	X	
IPS rendimiento	Mínimo 400 MBPS	**1.53 GBPS**	X	
Firewall rendimiento	Mínimo 1.5 GBPS	**Hasta 6.5 GBPS**	X	
Interfaces	Capacidad de ampliación.	**Incluye 8 puertos GbE cobre + 1 puerto SPF (Gbic no incluido), se puede realizar ampliación de puertos por medio de 1 slot tipo Flexi Port.**	X	
Módulos de protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas	X	

[redacted]

	6. Protección para servidor Web 7. VPN punto a punto: SSL, IPSec	6. Protección para servidor Web 7. VPN punto a punto: SSL, IPSec		
Análisis de correlación de amenazas	Correlación de amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.	Correlación de amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.	X	
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client y Hub and Spoke. 3. Soporte de inscripción DES, 3DES y AES 4. Autenticación de certificados IKE 5. El sistema debe tener la capacidad de crear certificados: Locales, CA y CRL.	1. Soporta de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client y Hub and Spoke. 3. Soporta de inscripción DES, 3DES y AES 4. Autenticación de certificados IKE 5. El sistema tiene la capacidad de crear certificados: Locales, CA y CRL.	X	
Seguridad Web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de malware. 4. Filtrado de contenido activo: extensiones de archivos, flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADUIS.	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de malware. 4. Filtrado de contenido activo: extensiones de archivos, flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADUIS.	X	
Protección de red	1. Administración web protegido por contraseña. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces 4. Prevención de intrusos 5. Protección contra DOS. VPN punto a punto: SSL, IPSec. 6. Compatibilidad de sistema de autenticación: RADUIS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.	1. Administración web protegido por contraseña. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces 4. Prevención de intrusos 5. Protección contra DOS. VPN punto a punto: SSL, IPSec. 6. Compatibilidad de sistema de autenticación: RADUIS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico. – Posee suite de reporte iView con multiples tipos de reportes sin costo adicional.	X	
Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http y https. 2. Debe permitir / restringir / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, keyword o Frase. 4. Lista de excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Que permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador 7. Control de aplicaciones.	1. Sistema de filtrado de contenido Web, para http y https. 2. Permite / restringe / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Permite bloqueo de URL, keyword o Frase. 4. Lista de excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permite filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador 7. Control de aplicaciones. 8. QoS de aplicaciones soportado.	X	
IPS	1. Que el UTM Soporte motor IPS para la protección contra ataques. 2. Protección con DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades de	1. El UTM Soporta motor IPS para la protección contra ataques. 2. Protección con DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades de	X	

[redacted]

	protocolos: DNS, FTP, ICMP, IMAP, POP3, RCP, SNMP, TFTP, NNTP. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.	protocolos: DNS, FTP, ICMP, IMAP, POP3, RCP, SNMP, TFTP, NNTP. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.		
Protección de correo electrónico	Especificar	Posee modulo anti-spam interno para filtrado de correo no deseado.	X	
Protección de redes inalámbricas	Especificar	Posee controladora de equipos WiFi en marca SOPHOS sin costo adicional (Equipos AP no incluidos)	X	
OTRAS				
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta a fallas en equipo en un máximo de 3 horas posteriores al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días de la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.	1. Se instalará y configurará equipo para ponerlo en operación. 2. Se dará respuesta a fallas en equipo en un máximo de 3 horas posteriores al reporte. 3. Se reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Se brindará soporte 24 horas del día, 7 días de la semana, sin costo adicional. 5. Se incluye certificados en la solución ofertada que residen en el país, para atender los requerimientos de soporte técnico.	X	
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.	Se reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.	X	
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.	1. Se presentan cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Se presenta carta del fabricante para comprobar que es distribuidor autorizado.	X	
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.	Se brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.	X	

[redacted]

[redacted]

[redacted]

CENTROS DE RECREACION Y ARCHIVO GENERAL				
CARACTERISTICAS	**DESCRIPCION**	**ESPECIFICACIONES TECNICAS OFERTADAS**	**CUMPLE**	
			SI	NO
Capacidad de usuarios	Hasta 15	**Marca SOPHOS** **Modelo XG105** **Puede soportar hasta 100 usuarios concurrentes, base de registro de usuarios ilimitados. Incluye 1 año de Licencia EnterpriseProtect**	X	
Cantidad de equipos	Cinco	5	X	
Almacenamiento	64 GB mínimo	64 GB tipo SSD	X	
Consumo de energía	Especificar	100-240 VAC, 50/60 HZ – 36 Watts – Fuente de alimentación eléctrica redundante externa opcional (No Incluida)	X	
Conexiones concurrentes	Mínimo 600 K	**3.2 millones de conexiones simultáneas.**	X	
AV rendimiento	Mínimo 400 MBPS	**450 MBPS**	X	
IPS rendimiento	Mínimo 300 MBPS	**970 GBPS**	X	
Firewall rendimiento	Mínimo 600 MBPS	**Hasta 3.5 GBPS**	X	
Interfaces	Capacidad de ampliación.	**Incluye 4 puertos GbE cobre + 1 puerto SPF (Gbic no incluido),**	X	
Módulos de protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPSec	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPSec	X	
Análisis de correlación de amenazas	Correlación de amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.	Correlación de amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.	X	
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client y Hub and Spoke. 3. Soporte de inscripción DES, 3DES y AES 4. Autenticación de certificados IKE 5. El sistema debe tener la capacidad de crear certificados: Locales, CA y CRL.	1. Soporta de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client y Hub and Spoke. 3. Soporta de inscripción DES, 3DES y AES 4. Autenticación de certificados IKE 5. El sistema tiene la capacidad de crear certificados: Locales, CA y CRL.	X	
Seguridad Web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de malware. 4. Filtrado de contenido activo: extensiones de archivos, flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADUIS.	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de malware. 4. Filtrado de contenido activo: extensiones de archivos, flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADUIS.	X	
Protección de red	1. Administración web protegido por contraseña. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces 4. Prevención de intrusos 5. Protección contra DOS. VPN punto a punto: SSL, IPSec.	1. Administración web protegido por contraseña. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces 4. Prevención de intrusos 5. Protección contra DOS. VPN punto a punto: SSL, IPSec.	X	

[redacted]

	6. Compatibilidad de sistema de autenticación: RADUIS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.	6. Compatibilidad de sistema de autenticación: RADUIS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico. – Posee suite de reporte iView con multiples tipos de reportes sin costo adicional.		
Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http y https. 2. Debe permitir / restringir / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, keyword o Frase. 4. Lista de excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Que permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador 7. Control de aplicaciones.	1. Sistema de filtrado de contenido Web, para http y https. 2. Permite / restringe / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Permite bloqueo de URL, keyword o Frase. 4. Lista de excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permite filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador 7. Control de aplicaciones. 8. QoS de aplicaciones soportado.	X	
IPS	1. Que el UTM Soporte motor IPS para la protección contra ataques. 2. Protección con DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades de protocolos: DNS, FTP, ICMP, IMAP, POP3, RCP, SNMP, TFTP, NNTP. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.	1. El UTM Soporta motor IPS para la protección contra ataques. 2. Protección con DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades de protocolos: DNS, FTP, ICMP, IMAP, POP3, RCP, SNMP, TFTP, NNTP. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.	X	
Protección de correo electrónico	Especificar	Posee modulo anti-spam interno para filtrado de correo no deseado.	X	
Protección de redes inalámbricas	Especificar	Posee controladora de equipos WiFi en marca SOPHOS sin costo adicional (Equipos AP no incluidos)	X	
OTRAS				
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta a fallas en equipo en un máximo de 3 horas posteriores al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días de la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.	1. Se instalará y configurará equipo para ponerlo en operación. 2. Se dará respuesta a fallas en equipo en un máximo de 3 horas posteriores al reporte. 3. Se reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Se brindará soporte 24 horas del día, 7 días de la semana, sin costo adicional. 5. Se incluye certificados en la solución ofertada que residen en el país, para atender los requerimientos de soporte técnico.	X	
Garantía	Reemplazará en concepto de garantía las	Se reemplazará en concepto de garantía las	X	

[redacted]

	veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.	veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.		
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.	1. Se presentan cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Se presenta carta del fabricante para comprobar que es distribuidor autorizado.	X	
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.	Se brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.	X	

[redacted]

[redacted]

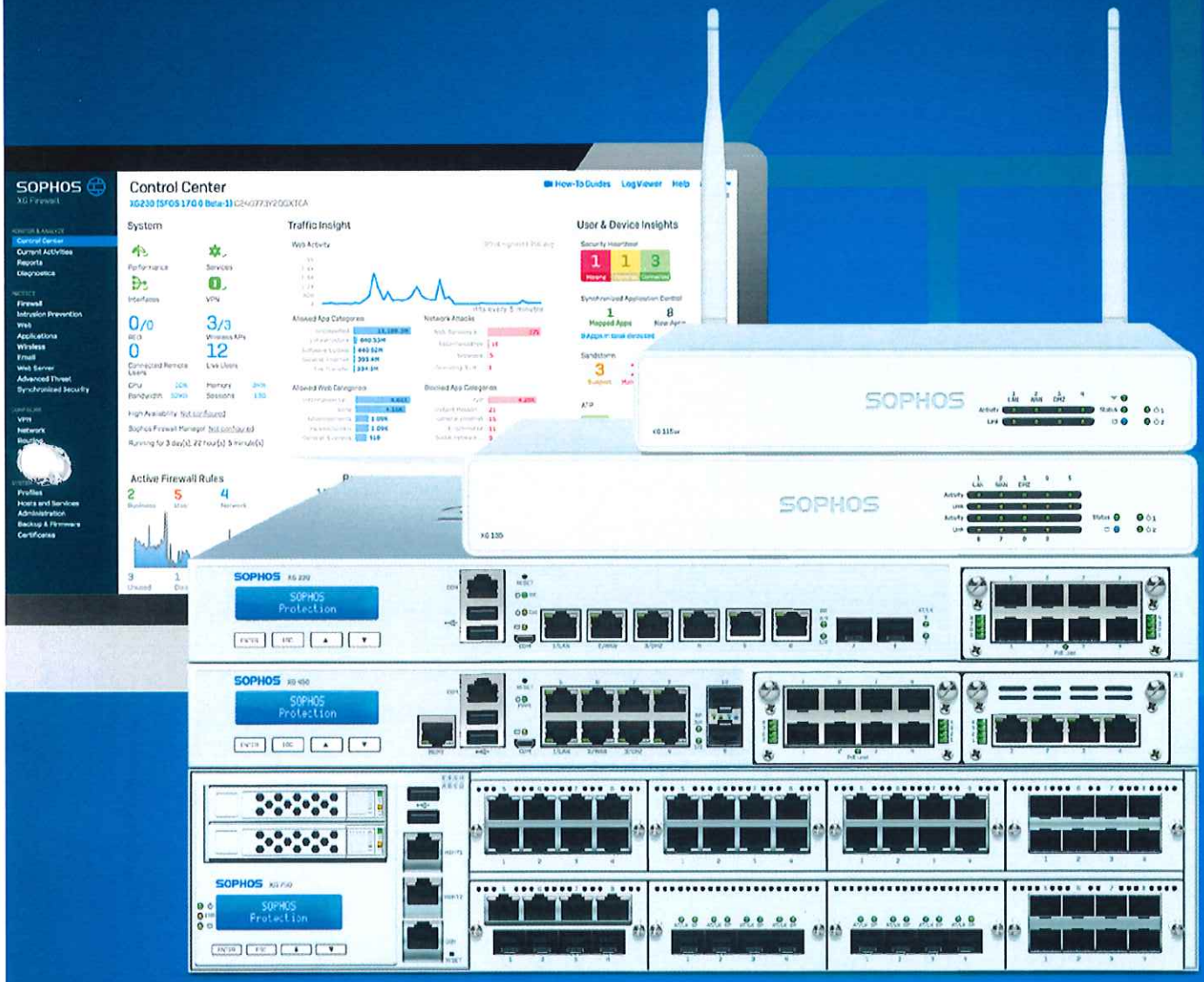
[redacted]

SOPHOS
Security made simple.

Sophos XG Firewall

Simplicidad, seguridad y visibilidad sin igual

Sophos XG Firewall ofrece un nuevo enfoque a la forma de gestionar su firewall, responder ante las amenazas y supervisar lo que ocurre en la red.



DADA-DADA & CIA., S.A. de C.V.

Sophos XG Firewall

Sophos XG Firewall ofrece una completa protección de última generación para firewalls que bloquea amenazas desconocidas, responde automáticamente a incidentes y expone riesgos ocultos.

Bloquea amenazas desconocidas

Sophos XG Firewall le ofrece la tecnología avanzada más moderna que necesita para proteger su red contra ransomware y amenazas avanzadas, como IPS de primera categoría, protección contra amenazas avanzadas, espacio seguro en la nube, antivirus dual, control web y de aplicaciones, protección del correo electrónico y un firewall de aplicaciones web integral. Y es fácil de configurar y administrar.

Responde automáticamente a incidentes

XG Firewall es la única solución de seguridad para redes que puede identificar totalmente el origen de una infección en la red y responder limitando el acceso a los otros recursos de red de forma automática. Esto es posible gracias a nuestra tecnología única de Sophos Security Heartbeat™, que comparte el estado y datos de telemetría entre los endpoints de Sophos y su firewall.

Expone riesgos ocultos

Sophos XG Firewall ofrece una visibilidad sin precedentes sobre los usuarios de mayor riesgo, apps desconocidas, amenazas avanzadas, cargas sospechosas y mucho más. También se beneficiará de la generación de informes detallados integrada, incluida sin costes adicionales, y la opción de añadir Sophos iView para la generación de informes centralizada en múltiples firewalls.

Potente ... rápido

Hemos diseñado XG Firewall para que ofrezca una eficiencia de seguridad y un rendimiento excepcionales para un retorno de la inversión óptimo. Nuestros dispositivos están construidos utilizando tecnología multinúcleo de Intel, unidades de estado sólido, y escaneado de contenido en memoria acelerado. Además, la tecnología de optimización de paquetes Sophos FastPath garantiza siempre el máximo rendimiento.

Administre fácilmente múltiples firewalls

Sophos Firewall Manager proporciona una única consola para administrar varios dispositivos XG Firewall de forma centralizada. Y si además desea consolidar la generación de informes en varios dispositivos XG, SG y Cyberoam, podrá hacerlo con Sophos iView.



Características de seguridad que no ofrece nadie más

XG Firewall incluye una serie de innovaciones que no solo le facilitan el trabajo, sino que también garantizan que la red sea más segura.

Una revolución en la protección contra amenazas avanzadas: Seguridad Sincronizada de Sophos

Seguridad Sincronizada, una solución única en el sector, conecta los equipos y el firewall para permitir una coordinación y visibilidad únicas. Security Heartbeat™ informa del estado de mantenimiento de Endpoint y permite que el firewall identifique y responda de forma inmediata a un sistema de la red que corra peligro. El firewall puede aislar los sistemas hasta que puedan investigarse y limpiarse. Otra función de Seguridad Sincronizada, Control de aplicaciones sincronizado, también permite que el firewall consulte el endpoint para determinar el origen del tráfico desconocido en la red.

Control de identidad de nivel 8 patentada

La identidad de usuario lleva el cumplimiento a un nivel totalmente nuevo gracias a nuestra tecnología de políticas basada en la identidad de nivel 8 patentada, que permite realizar controles a nivel de usuario sobre aplicaciones, ancho de banda y otros recursos de red, independientemente de la dirección IP, ubicación, red o dispositivo. Literalmente, lleva la política del firewall a un nivel completamente nuevo.

Las plantillas de políticas le protegen de forma rápida

Las plantillas de políticas predefinidas le permiten proteger aplicaciones comunes como Microsoft Exchange o SharePoint de forma rápida y sencilla. Basta con seleccionarlas de una lista, facilitar algo de información básica y la plantilla se encarga del resto. La plantilla define automáticamente todas las reglas de firewall de entrada/salida y la configuración de seguridad y muestra la política final en un enunciado en lenguaje sencillo.

Informes de riesgos de los usuarios automáticos

El cociente de amenazas por usuario (UTQ) de Sophos es una función única que ofrece información procesable sobre el comportamiento de los usuarios. Nuestro firewall correlaciona los hábitos de navegación y la actividad de cada usuario con desencadenadores de amenazas avanzadas e historial para identificar a usuarios con comportamientos propensos al riesgo.

Implementación flexible sin concesiones

A diferencia de la competencia, no tiene que hacer concesiones en lo que respecta a la elección de hardware, software o virtual. Todas las funciones están disponibles en todos los modelos y formatos.

Para obtener más información, visite www.sophos.com/xgfirewall



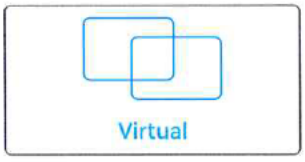
Serie XG

Dispositivos especialmente diseñados para proporcionar lo último en rendimiento.



Software

Instale la imagen de Sophos Firewall OS en su propio hardware Intel o servidor.



Virtual

Instalación en VMware, Citrix, Microsoft Hyper-V y KVM.



Azure

Proteja su infraestructura de red en la nube de Azure.





Protección de redes

Toda la protección que necesita para detener ataques sofisticados y amenazas avanzadas, a la vez que brinda acceso seguro a la red a aquellos en los que confía.

Sistema de prevención contra intrusiones de última generación

Proporciona protección avanzada contra todo tipo de ataques modernos. Va más allá de los recursos tradicionales de red y de servidor para proteger también a los usuarios y aplicaciones en la red.

Protección contra amenazas avanzadas

Identificación instantánea y respuesta inmediata ante los ataques más sofisticados de hoy en día. Una protección multinivel identifica las amenazas al instante y Security Heartbeat™ responde ante las emergencias.

Security Heartbeat

Crea una conexión entre los endpoints protegidos por Sophos Central y el firewall para identificar las amenazas más deprisa, simplificar la investigación y minimizar el impacto de los ataques. Se puede incorporar fácilmente el estado de Security Heartbeat en las políticas del firewall para aislar los sistemas afectados de forma automática.

Tecnologías VPN avanzadas

Añade tecnologías VPN únicas y sencillas, incluido nuestro portal de autoservicio HTML5 sin cliente que facilita enormemente el acceso remoto. También puede utilizar nuestra exclusiva tecnología VPN con dispositivo Ethernet remoto (RED) seguro y ligero.

Protección web

Una protección web completa y un control de aplicaciones con herramientas de políticas potentes y flexibles garantizan que los usuarios de la red estén protegidos y sean productivos.

Políticas web potentes para grupos y usuarios

Proporciona controles de políticas de nivel empresarial de puerta de enlace web segura para gestionar fácilmente controles web sofisticados de grupos y usuarios. Aplique políticas en función de palabras clave web cargadas que indiquen usos o comportamientos inapropiados.

Protección avanzada contra amenazas web

Nuestro motor avanzado, respaldado por SophosLabs, ofrece la máxima protección contra las amenazas web cambiantes y camufladas de hoy en día. Técnicas innovadoras como la emulación en JavaScript, el análisis de comportamiento y la reputación del origen ayudan a garantizar la seguridad de la red.

Proxy transparente de alto rendimiento

Nuestra tecnología de proxy transparente, optimizada para lograr el máximo rendimiento, proporciona inspección de latencia ultrabaja y escaneado HTTPS de todo el tráfico para buscar amenazas y verificar el cumplimiento.

Calidad de servicio y control de aplicaciones de nivel 8

Permite visibilidad y control por usuario sobre miles de aplicaciones con opciones granulares de políticas y dosificación del tráfico (QoS) basadas en la categoría de la aplicación, el grado de riesgo y otras características.

Protección de Sandstorm

Sophos Sandstorm utiliza la tecnología de última generación de espacio seguro en la nube para ofrecer a su organización un nivel de seguridad adicional contra el ransomware y los ataques dirigidos.

Sin hardware adicional

Se integra con XG Firewall y se proporciona en la nube, de forma que no requiere hardware adicional. Sophos Sandstorm bloquea amenazas esquivas como ransomware camufladas como ejecutables, PDF y documentos de Microsoft Office, y las envía a un espacio seguro en la nube para detonarlas y observarlas en un entorno seguro.

Más protección e información

Los datos sobre amenazas se envían a XG Firewall y el archivo se bloquea o admite. El proceso solo tarda un par de minutos y tiene un impacto mínimo en el usuario. Además, Sandstorm proporciona informes de amenazas detallados de cada incidente para que usted sepa exactamente lo que está pasando.

[redacted]

Protección del correo electrónico

Protección completa de SMTP y POP anti-spam, phishing y fuga de datos con nuestra protección todo en uno única que combina cifrado de correo electrónico basado en políticas con DLP y anti-spam.

Agente de transferencia de mensajes integrado

Garantiza la continuidad permanente del correo electrónico al permitir que el firewall ponga en cola automáticamente los mensajes en caso de que los servidores dejen de estar disponibles.

Live Anti-Spam

Ofrece protección contra las últimas campañas de spam, ataques phishing y programas maliciosos en archivos adjuntos.

Cuarentena de autoservicio

Proporciona a los empleados control directo sobre su cuarentena de correo no deseado, lo que ahorra tiempo y esfuerzos.

Cifrado SPX de correo electrónico

Único en Sophos, SPX convierte el envío de correos electrónicos cifrados en algo sencillo, incluso para aquellos que no dispongan de ninguna infraestructura segura, gracias a nuestra tecnología de cifrado mediante contraseña pendiente de patente.

Prevención de fugas de datos

La prevención de fugas de datos (DLP) basada en políticas puede activar automáticamente el cifrado o bloquear/notificar en función de la presencia de datos confidenciales en los mensajes que salen de la empresa.

Protección de servidores web

Refuerce sus servidores web y aplicaciones empresariales contra intentos de ataque con un firewall de aplicaciones web completo, a la vez que proporciona acceso seguro con autenticación de proxy inverso.

Plantillas de políticas de aplicaciones de empresa

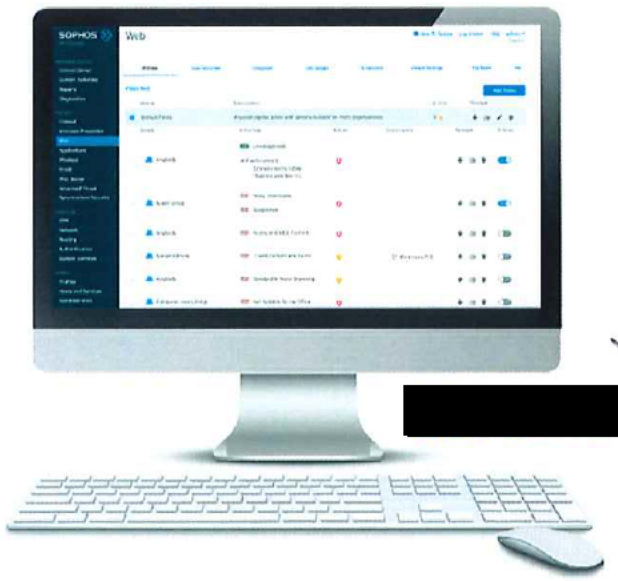
Las plantillas de políticas predefinidas le permiten proteger aplicaciones comunes como Microsoft Exchange Outlook Anywhere o SharePoint de forma rápida y sencilla.

Protección contra los últimos ataques

Con diversas tecnologías de protección avanzada, como el refuerzo de URL y formularios, los enlaces profundos y la prevención de cruces de directorios, la protección contra la inyección de código SQL y la secuencia de comandos, la firma de cookies y mucho más.

Servidor proxy inverso

Con opciones de autenticación, descarga de SSL y equilibrio de cargas de servidores, garantice la máxima protección y rendimiento para los servidores a los que se accede desde Internet.



Formas de compra

Cada dispositivo XG Firewall viene equipado con la funcionalidad de Base Firewall, incluido IPSec, VPN SSL y Wireless Protection. Puede ampliar la protección con nuestros paquetes o añadiendo módulos de protección independientes.



Protección de redes

Toda la protección que necesita para detener ataques sofisticados y amenazas avanzadas, a la vez que brinda acceso seguro a la red a aquellos en los que confía.



Protección de Sandstorm

Sophos Sandstorm utiliza la tecnología de última generación de espacio seguro en la nube para ofrecer a su organización un nivel de seguridad adicional contra el ransomware y los ataques dirigidos.



Protección web

Una protección web completa y un control de aplicaciones con herramientas de políticas potentes y flexibles garantizan que los usuarios de la red estén protegidos y sean productivos.



Security Heartbeat™

Conecta sus endpoint de Sophos con su firewall para proporcionar una protección única contra amenazas avanzadas y una reducción en el tiempo y la complejidad de las respuestas a incidentes de seguridad.



Protección del correo electrónico

Protección completa de SMTP y POP anti-spam, phishing y fuga de datos con nuestra protección todo en uno única que combina cifrado de correo electrónico basado en políticas con DLP y anti-spam.



Protección de servidores web

Refuerce sus servidores web y aplicaciones empresariales contra intentos de ataque, a la vez que proporciona acceso seguro a los usuarios externos con autenticación de proxy inverso.

Un enfoque sencillo para un soporte completo

Construimos productos sencillos, pero completos. Además, usamos este mismo enfoque con nuestro soporte. Con opciones que van desde el soporte técnico básico a opciones que incluyen acceso directo a ingenieros de soporte técnico superiores y prestación personalizada.

Nombres de licencias	Standard Incluido con la compra	Enhanced Incluido en todos los paquetes	Enhanced Plus
Soporte A través de teléfono y correo electrónico	Durante 90 días (solo en horario de oficina)	Incluida (24x7)	Acceso VIP (24x7)
Actualizaciones y parches de seguridad Para el ciclo de vida del producto	Incluido con una suscripción de software activa	Incluido con una suscripción de software activa	Incluido con una suscripción de software activa
Actualizaciones y mejoras de características del software	Incluidos 90 días	Incluido	Incluido
Consultoría Asesoría remota sobre la configuración de su firewall y seguridad con un técnico superior de Soporte de Sophos			Incluida (hasta 4 horas)
Garantía y RMA Para todos los dispositivos de hardware	1 año (devolución / recambio)	Intercambio avanzado (máx. 5 años)	Intercambio avanzado (máx. 5 años)
Responsable técnico de cuenta Responsable técnico de cuenta dedicado		Optativo (coste adicional)	Optativo (coste adicional)

[redacted]

[redacted]

Seguridad Sincronizada

Security Heartbeat™ - Su firewall y sus endpoints por fin se entienden

Sophos XG Firewall es la única solución de seguridad para redes que puede identificar totalmente el usuario y el origen de una infección en la red y responder limitando el acceso a los otros recursos de red de forma automática. Esto es posible gracias a nuestra tecnología única de Sophos Security Heartbeat™, que comparte el estado y datos de telemetría entre los endpoints de Sophos y su firewall.

La buena noticia es que todo esto ocurre automáticamente y está ayudando a numerosas empresas y organizaciones a ahorrar tiempo y dinero a la hora de proteger sus entornos actuales.

Control de aplicaciones sincronizado - Revela lo desconocido

Gracias a Security Heartbeat, podemos hacer mucho más que simplemente observar el estado de un endpoint. También tenemos una solución a uno de los mayores problemas a los que se enfrentan los administradores de redes hoy día: la falta de visibilidad sobre el tráfico de red.

El control de aplicaciones sincronizado identifica, clasifica y controla automáticamente aplicaciones web personalizadas, evasivas y genéricas que actualmente no están siendo identificadas. Puesto que estas aplicaciones se vuelven visibles, es posible aplicarles políticas, lo que le permitirá tenerlas totalmente bajo control.

Para obtener más información, visite es.sophos.com/xgfirewall

Lo que ven los firewalls de última generación hoy día

Que ve XG Firewall



No puede controlar lo que no puede ver. Todos los firewalls actuales dependen de las firmas de aplicaciones estáticas para identificar apps, pero estas no funcionan para la mayoría de apps personalizadas, oscuras, evasivas o de otro tipo que utilicen HTTP o HTTPS genérico.

XG Firewall utiliza Seguridad Sincronizada para identificar, clasificar y controlar automáticamente todas las aplicaciones desconocidas, bloqueando fácilmente las apps no deseadas y priorizando las que sí lo son.

Pero hay más...

Seguridad Sincronizada puede conectar mucho más que solo su firewall y sus endpoints. Mediante Sophos Central como nuestra plataforma de Seguridad Sincronizada, hemos añadido muchas más soluciones para mejorar su protección.

Para obtener más información, visite nuestra página de Seguridad Sincronizada en nuestro sitio web.

[redacted]

Dispositivos de la serie Sophos XG de un vistazo

Nuestros dispositivos de hardware de la serie XG se han diseñado especialmente con la última tecnología multinúcleo de Intel, un aprovisionamiento generoso de RAM y almacenamiento de estado sólido. Tanto si protege una pyme como un centro de datos grande, disfrutará de un rendimiento líder en el sector.

Matriz de productos

Modelo			Especificaciones técnicas			Rendimiento[1]			
	Revisión n.º	Factor de forma	Puertos/ranuras (Máx. puertos)	Modelo w 802.11	Componentes intercambiables	Firewall (Mbps)	VPN (Mbps)	NGFW (Mbps)	AV-proxy (Mbps)
XG 85(w)	3	escritorio	4	a/b/g/n/ac	n/d	3.000	225	310	360
XG 105(w)	3	escritorio	4	a/b/g/n/ac	aliment. ext. opc.	3.500	360	480	450
XG 115(w)	3	escritorio	4	a/b/g/n/ac	aliment. ext. opc.	4.000	490	1.000	600
XG 125(w)	3	escritorio	9/1 (9)	a/b/g/n/ac	aliment. ext. opc., 3G/4G	6.500	700	1.100	700
XG 135(w)	3	escritorio	9/1 (9)	a/b/g/n/ac	aliment. ext. opc., 3G/4G, Wi-Fi*	8.000	1.180	1.200	1.580
XG 210	3	1U	8/1 (16)	n/d	aliment. ext. opc.	16.000	1.450	2.200	2.300
XG 230	2	1U	8/1 (16)	n/d	aliment. ext. opc.	20.000	1.700	3.000	2.800
XG 310	2	1U	12/1 (20)	n/d	aliment. ext. opc.	28.000	2.750	4.000	3.300
XG 330	2	1U	12/1 (20)	n/d	aliment. ext. opc.	33.000	3.200	5.500	6.000
XG 430	2	1U	10/2 (26)	n/d	aliment. ext. opc.	41.000	4.800	6.000	6.500
XG 450	2	1U	10/2 (26)	n/d	int. opc. Potencia	50.000	5.500	7.500	7.000
XG 550	2	2U	8/4 (32)	n/d	Potencia, SSD, Ventilador	65.000	8.400	9.000	10.000
XG 650	2	2U	8/6 (48)	n/d	Potencia, SSD, Ventilador	85.000	9.000	10.000	13.000
XG 750	2	2U	8/8 (64)	n/d	Potencia, SSD, Ventilador	100.000	11.000	11.800	17.000

* opción de 2.º módulo Wi-Fi solo en 135w (requiere XG v17 MR6)

Paquete Sophos XG Firewall TotalProtect Plus

Para disfrutar de la máxima protección, valor y tranquilidad, opte por nuestro práctico paquete TotalProtect Plus.

Funciones incluidas	Paquete TotalProtect Plus
Firewall básico Firewall, IPsec y VPN SSL, protección inalámbrica (los AP se venden por separado)	✓
Protección de redes IPS, RED, VPN HTML5, ATP, Security Heartbeat	✓
Protección web Antimalware, protección, visibilidad y control web y de aplicaciones	✓
Protección del correo electrónico Antispam, cifrado de correo electrónico SPX y DLP	✓
Protección de servidores web Firewall de aplicaciones web y proxy inverso	✓
Protección de Sandstorm Tecnología de última generación de espacio seguro en la nube	✓
Soporte técnico mejorado Soporte 24/7, actualizaciones de seguridad y software, garantía de sustitución por adelantado	✓
Dispositivo de hardware de la serie XG Procesador multinúcleo de Intel, almacenamiento de estado sólido, conectividad flexible	✓

[redacted]

Dispositivos de escritorio de la serie XG de Sophos: XG 85 y XG 85w

Especificaciones técnicas

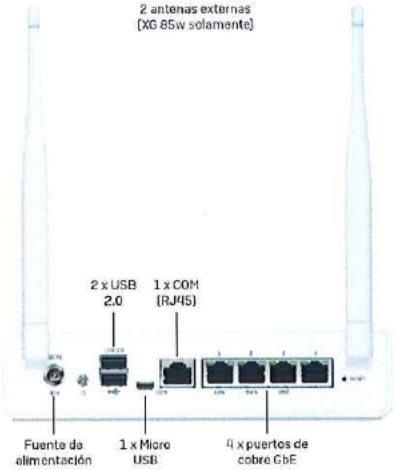
Estos firewalls de escritorio básicos son la opción ideal para pequeñas empresas, tiendas y oficinas pequeñas o domésticas con presupuesto limitado. Están disponibles con y sin LAN inalámbrica 802.11ac integrada, por lo que se puede tener una solución de seguridad de red y punto de acceso todo en uno sin necesidad de hardware adicional. La tecnología de doble núcleo de Intel los hace altamente eficientes y, dado que no usan ventilador, no añadirán ruido no deseado a su espacio de oficina.

Nota: Los modelos XG 85 y 85w no admiten algunas de las funciones avanzadas como la presentación de informes integrada, el escaneado antivirus dual, el escaneado antivirus WAF y la funcionalidad del agente de transferencia de mensajes (MTA) de correo. Si necesita estas funciones, se recomienda el modelo XG 105(w).

Vista frontal



Vista trasera



Entorno	
Consumo de energía	12W, 40,94 BTU/h (inactivo) 20,4W, 69,6 BTU/h (carga completa)
Temperatura en funcionamiento	0-40°C (en funcionamiento) -20 a +80°C (almacenamiento)
Humedad	10%-90%, sin condensación

Certificaciones de productos	
Certificaciones	CB, UL, CE, FCC, ISED, VCCI, MIC (Japón), RCM, CCC, KC Planificado: BIS

Rendimiento[1]	XG 85(w) Rev. 3
Rendimiento del firewall	3 Gbps
IMIX del firewall	800 Mbps
Rendimiento de la VPN	225 Mbps
Rendimiento del IPS	580 Mbps
NGFW (IPS + Control aplic.) máx.	310 Mbps
Rendimiento del antivirus (proxy)	360 Mbps
Conexiones simultáneas	3.200.000
Conexiones nuevas/seg.	15.000
Número máximo de usuarios con licencia	sin restricciones

Especificaciones inalámbricas (XG 85w solo)	
N.º de antenas	2 externas
Funciones MIMO	2 x 2:2
Interfaz inalámbrica	802.11a/b/g/n/ac (2.4 GHz / 5 GHz)

Interfaces físicas	
Almacenamiento	8 GB eMMC
Interfaces Ethernet (fijas)	4 GbE cobre
Puertos de E/S (trasero)	2 x USB 2.0 1 x Micro-USB 1 x COM (RJ45)
Fuente de alimentación	Alcance automático externo de DC: 12V, 100-240 VCA, 24 W@50-60 Hz

Especificaciones físicas	
Montaje	Kit de montaje en bastidor disponible (pedir por separado)
Dimensiones Ancho x Profundidad x Altura	190 x 117 x 43 mm 7,48 x 4,61 x 1,69 pulgadas
Peso	0,75 kg / 1,65 lbs (fuera del paquete) 1,9 kg / 4,19 lbs (en el paquete) (altura del modelo w mínimamente superior)



Dispositivos de escritorio de la serie XG de Sophos: XG 105, XG 105w, XG 115, XG 115w

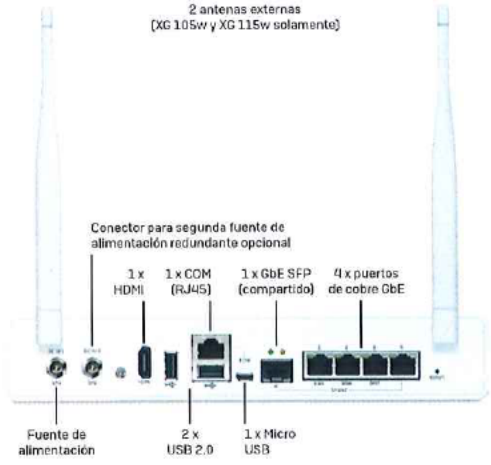
Especificaciones técnicas

Estos dispositivos de firewall de escritorio ofrecen una excelente relación precio-rendimiento, ideal para pequeñas empresas o sucursales. Están disponibles con o sin LAN inalámbrica 802.11ac integrada, por lo que incluso se puede tener una solución de seguridad de red y punto de acceso todo en uno sin necesidad de hardware adicional. Por supuesto, también puede añadir puntos de acceso externos. Junto con la tecnología multinúcleo de Intel, diseñada para un mejor rendimiento y eficacia en un pequeño factor de forma, estos modelos vienen equipados con 4 puertos de cobre GbE y una interfaz SFP compartida, para utilizarse, por ejemplo, con nuestro módem DSL opcional o un transceptor de fibra SFP para conectar el dispositivo a un servidor o un conmutador. La segunda fuente de alimentación opcional ofrece una opción de redundancia sin igual en este segmento de productos.

Vista frontal



Vista trasera



Entorno	
Consumo de energía	8,88W, 30,28 BTU/h (inactivo) 10,44W, 35,6 BTU/h (carga completa)
Temperatura en funcionamiento	0-40°C (en funcionamiento) -20 a +80°C (almacenamiento)
Humedad	10%-90%, sin condensación

Certificaciones de productos	
Certificaciones	CB, UL, CE, FCC, ISED, VCCI, MIC (Japón), RCM, CCC, KC Planificado: BIS

Rendimiento[1]	XG 105(w) Rev. 3	XG 115(w) Rev. 3
Rendimiento del firewall	3,5 Gbps	4 Gbps
IMIX del firewall	1,8 Gbps	2,0 Gbps
Rendimiento de la VPN	360 Mbps	490 Mbps
Rendimiento del IPS	970 Mbps	1,22 Gbps
NGFW (IPS + Control aplic.) máx.	480 Mbps	1 Gbps
Rendimiento del antivirus (proxy)	450 Mbps	600 Mbps
Conexiones simultáneas	3.200.000	6.000.000
Conexiones nuevas/seg.	28.000	35.000
Número máximo de usuarios con licencia	sin restricciones	sin restricciones

Especificaciones inalámbricas (XG 105w y XG 115w solamente)	
N.º de antenas	2 externas
Funciones MIMO	2 x 2:2
Interfaz inalámbrica	802.11a/b/g/n/ac (2,4 GHz / 5 GHz)

Interfaces físicas	
Almacenamiento (cuarentena local/registros)	SSD integrado
Interfaces Ethernet (fijas)	4 GbE cobre 1 GbE SFP (compartido)*
Módulos de conectividad (opcional)	Módulo DSL SFP (VDSL2) Transceptores SFP
Puertos de E/S (trasero)	2 x USB 2.0 1 x Micro-USB 1 x COM (RJ45) 1 x HDMI
Fuente de alimentación	Alcance automático externo de DC: 12 V, 100-240 VCA, 36 W@50-60 Hz Fuente de alimentación redundante opcional (externa)

Especificaciones físicas	
Montaje	Kit de montaje en bastidor disponible (pedir por separado)
Dimensiones Ancho x Profundidad x Altura	245 x 157 x 44 mm 9,65 x 6,18 x 1,73 pulgadas
Peso	1,17 kg / 2,58 lbs (fuera del paquete) 2,4 kg / 5,29 lbs (en el paquete) (altura de los modelos w mínimamente superior)

* Los transceptores SFP se venden por separado

Dispositivos de escritorio de la serie XG de Sophos: XG 125, XG 125w, XG 135, XG 135w

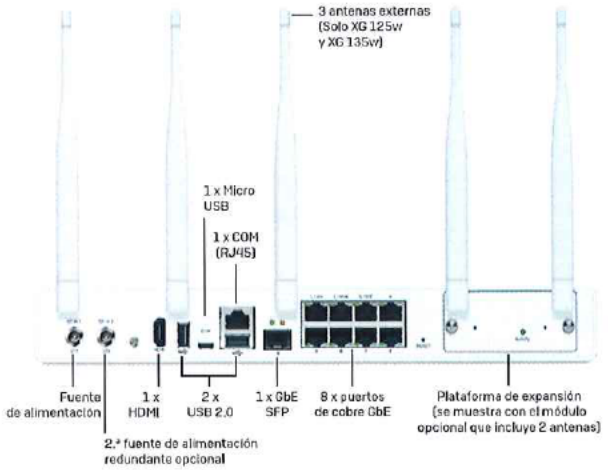
Especificaciones técnicas

Estos potentes dispositivos de firewall ofrecen el rendimiento de un 1U con un factor de forma y precio de un dispositivo de sobremesa. Si necesita proteger un pequeño negocio u oficinas sucursales y trabaja con un presupuesto reducido, estos modelos son la opción ideal. También están disponibles con LAN inalámbrica 802.11ac integrada para proporcionar a sus trabajadores móviles una cobertura y conectividad óptimas. Construido sobre la última arquitectura de Intel, nuestro software hace un uso óptimo de la tecnología multinúcleo para proporcionar un excelente rendimiento para todos sus procesos clave. Estos modelos vienen equipados con 8 puertos de cobre GbE, además de un puerto SFP, para utilizarse, por ejemplo, con nuestro módem DSL opcional o un transceptor de fibra SFP para conectar el dispositivo a un servidor o un conmutador. La plataforma de expansión ofrece la opción de añadir conectividad adicional como nuestro módulo 3G/4G. También está disponible un segundo módulo de radio Wi-Fi para el XG 135w. La segunda fuente de alimentación opcional garantiza la continuidad empresarial para estos modelos.

Vista frontal



Vista trasera



Entorno	
Consumo de energía	18,6W, 63,426 BTU/h (inactivo) 20,04W, 68,336 BTU/h (carga completa)
Temperatura en funcionamiento	0-40°C (en funcionamiento) -20 a +80°C (almacenamiento)
Humedad	10%-90%, sin condensación

Certificaciones de productos	
Certificaciones	CB, UL, CE, FCC, ISED, VCCI, MIC (Japón), RCM, CCC, KC Planificado: BIS

Rendimiento[1]	XG 125(w) Rev. 3	XG 135(w) Rev. 3
Rendimiento del firewall	6,5 Gbps	8 Gbps
IMIX del firewall	2,5 Gbps	5 Gbps
Rendimiento de la VPN	700 Mbps	1,18 Gbps
Rendimiento del IPS	1,53 Gbps	2,48 Gbps
NGFW (IPS + Control aplic + filtro web) máx.	1,1 Gbps	1,2 Gbps
Rendimiento del antivirus (proxy)	700 Mbps	1,58 Gbps
Conexiones simultáneas	6.000.000	6.000.000
Conexiones nuevas/seg.	35.000	85.000
Número máximo de usuarios con licencia	sin restricciones	sin restricciones

Especificaciones inalámbricas (XG 125w y XG 135w solamente)	
N.º de antenas	3 externas
Funciones MIMO	3 x 3:3
Interfaz inalámbrica	802.11a/b/g/n/ac (2.4 GHz / 5 GHz)

Interfaces físicas	
Almacenamiento (cuarentena local/registros)	SSD integrado
Interfaces Ethernet (fijas)	8 GbE cobre 1 GbE SFP*
N.º de ranuras de expansión	1
Módulos de conectividad (opcional)	Módulo DSL SFP (VDSL2) Módulo 3G/4G Radio Wi-Fi 802.11ac 2x2:2 (solo XG 135w) Transceptores SFP
Puertos de E/S (trasero)	2 x USB 2.0 1 x Micro-USB 1 x COM (RJ45) 1 x HDMI
Fuente de alimentación	Alcance automático externo de DC: 12 V, 100-240 VCA, 36 W@50-60 Hz Fuente de alimentación redundante opcional (externa)

Especificaciones físicas	
Montaje	Kit de montaje en bastidor disponible (pedir por separado)
Dimensiones Ancho x Profundidad x Altura	320 x 212 x 44 mm 12,60 x 8,35 x 1,73 pulgadas
Peso	1,9 kg / 4,19 lbs (fuera del paquete) 3,3 kg / 7,27 lbs (en el paquete) (altura de los modelos w mínimamente superior)

* Los transceptores SFP se venden por separado

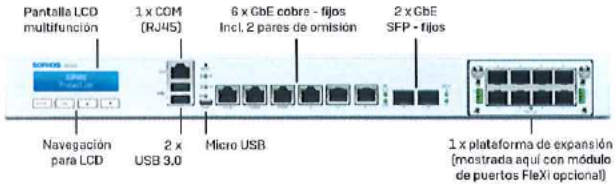
299

Dispositivos montados en bastidor de la serie XG de Sophos: XG 210, XG 230

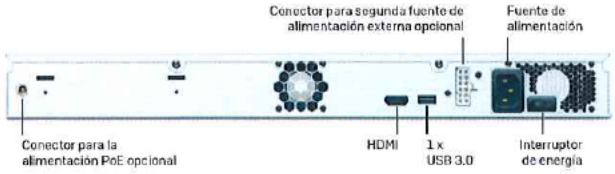
Especificaciones técnicas

Los dispositivos XG 210 y XG 230 de Sophos están diseñados para proteger a empresas pequeñas y medianas y sucursales. Basados en la última tecnología de Intel y equipados con 6 puertos GbE de cobre, 2 puertos de fibra GbE SFP y una ranura FleXi Port para configurarse con un módulo opcional, proporcionan una gran flexibilidad y velocidad con una excelente relación entre precio y rendimiento. Existe la opción de una fuente de alimentación redundante externa para estos modelos.

Vista frontal



Vista trasera



Entorno	
Consumo de energía	XG 210: 19W, 65 BTU/h (inactivo) 35W, 119 BTU/h (carga completa) XG 230: 21W, 72 BTU/h (inactivo) 41W, 141 BTU/h (carga completa)
Temperatura en funcionamiento	0-40°C (en funcionamiento) -20 a +80°C (almacenamiento)
Humedad	10%-90%, sin condensación

Certificaciones de productos	
Certificaciones	CB, UL, CE, FCC Clase A, ISED, VCCI, RCM, CCC, KC, BIS

Rendimiento[1]	XG 210 Rev. 3	XG 230 Rev. 2
Rendimiento del firewall	16 Gbps	20 Gbps
IMIX del firewall	5,5 Gbps	6,8 Gbps
Rendimiento de la VPN	1,45 Gbps	1,7 Gbps
Rendimiento del IPS	2,7 Gbps	4,2 Gbps
NGFW (IPS + Control aplic.) máx.	2,2 Gbps	3 Gbps
Rendimiento del antivirus (proxy)	2,3 Gbps	2,8 Gbps
Conexiones simultáneas	8.200.000	8.200.000
Conexiones nuevas/seg.	135.000	140.000
Número máximo de usuarios con licencia	sin restricciones	sin restricciones

Interfaces físicas	
Almacenamiento (cuarentena local/registros)	SSD integrado
Interfaces Ethernet (fijas)	6 GbE cobre (incl. 2 pares de omisión) 2 GbE SFP*
N.º de ranuras de puertos FleXi	1
Módulos de puertos FleXi (opcional)	GbE cobre de 8 puertos GbE SFP de 8 puertos* 2 puertos de 10 GbE SFP+* 4 puertos de 10 GbE SFP+ 2 puertos de 40 GbE QSFP+* PoE GbE de 4 puertos PoE GbE de 8 puertos GE cobre de 4 puertos con omisión LAN
Puertos de E/S	2 x USB 3.0 (delantero) 1 x micro USB (delantero) 1 x USB 3.0 (trasero) 1 x COM (RJ45) (delantero) 1 x HDMI (trasero)
Pantalla	Módulo LCD multifunción
Fuente de alimentación	Rango automático interno de 100-240VAC, 50-60 Hz Fuente de alimentación redundante opcional (externa)

Especificaciones físicas	
Montaje	Montaje en bastidor 1U (2 orejas de montaje en bastidor incluidas)
Dimensiones Ancho x Profundidad x Altura	438 x 344,4 x 44mm 17,24 x 13,56 x 1,75 pulgadas
Peso	5,2 kg / 11,46 lbs (fuera del paquete)7,7 kg / 16,98 lbs (en el paquete)

* Los transceptores (mini GBICs) se venden por separado

[redacted]

[redacted]

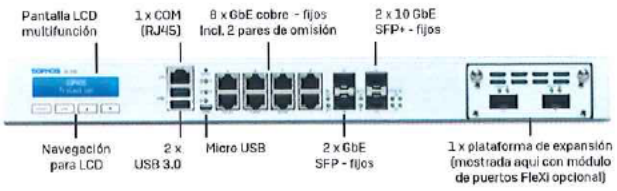
23

Dispositivos montados en bastidor de la serie XG de Sophos: XG 310, XG 330

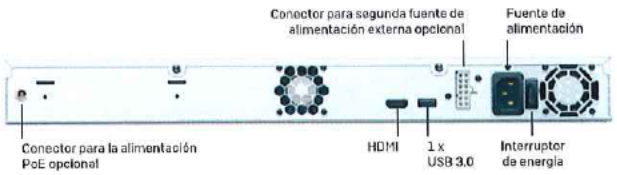
Especificaciones técnicas

Los dispositivos XG 310 y XG 330 de Sophos son escalables y adecuados para organizaciones distribuidas o empresas de tamaño medio. Con unidades de estado sólido para presentación de informes integrada, registros y cuarentena de spam, son muy sensibles, incluso en entornos de alto tráfico. Cada modelo está equipado con 8 puertos de cobre GbE, 2 puertos de fibra GbE SFP+ y 2 puertos de fibra 10 GbE SFP+, más una ranura FleXi Port para la configuración con un módulo opcional. Ofrecen un rendimiento y una flexibilidad óptimos, además de redundancia mediante una fuente de alimentación externa opcional.

Vista frontal



Vista trasera



Entorno

Consumo de energía	XG 310: 32W, 109 BTU/h (inactivo) 49W, 167 BTU/h (carga completa) XG 330: 36W, 122 BTU/h (inactivo) 54W, 184 BTU/h (carga completa)
Temperatura en funcionamiento	0-40°C (en funcionamiento) -20 a +80°C (almacenamiento)
Humedad	10%-90%, sin condensación

Certificaciones de productos

Certificaciones	CB, UL, CE, FCC Clase A, ISED, VCCI, RCM, CCC, KC, BIS

Rendimiento[1]	XG 310 Rev. 2	XG 330 Rev. 2
Rendimiento del firewall	28 Gbps	33 Gbps
IMIX del firewall	9,5 Gbps	12,5 Gbps
Rendimiento de la VPN	2,75 Gbps	3,2 Gbps
Rendimiento del IPS	5,5 Gbps	8,5 Gbps
NGFW (IPS + Control aplic.) máx.	4 Gbps	5,5 Gbps
Rendimiento del antivirus (proxy)	3,3 Gbps	6 Gbps
Conexiones simultáneas	17.500.000	17.500.000
Conexiones nuevas/seg.	200.000	200.000
Número máximo de usuarios con licencia	sin restricciones	sin restricciones

Interfaces físicas

Almacenamiento (cuarentena local/registros)	SSD integrado
Interfaces Ethernet (fijas)	8 GbE cobre (incl. 2 pares de omisión) 2 GbE SFP* 2 10 GbE SFP+*
N.º de ranuras de puertos FleXi	1
Módulos de puertos FleXi (opcional)	GbE cobre de 8 puertos GbE SFP de 8 puertos* 2 puertos de 10 GbE SFP+* 4 puertos de 10 GbE SFP+* 2 puertos de 40 GbE QSFP+* PoE GbE de 4 puertos PoE GbE de 8 puertos GbE cobre de 4 puertos con omisión LAN
Puertos de E/S	2 x USB 3.0 (delantero) 1 x micro USB (delantero) 1 x USB 3.0 (trasero) 1 x COM (RJ45) (delantero) 1 x HDMI (trasero)
Pantalla	Módulo LCD multifunción
Fuente de alimentación	Rango automático interno de 100-240VAC, 50-60 Hz Fuente de alimentación redundante opcional (externa)

Especificaciones físicas

Montaje	Montaje en bastidor 1U (2 orejas de montaje en bastidor incluidas)
Dimensiones Ancho x Profundidad x Altura	438 x 405,5 x 44mm 17,24 x 15,96 x 1,75 pulgadas
Peso	5,8 kg / 12,78 lbs (fuera del paquete) 8,8 kg / 19,4 lbs (en el paquete)

* Los transceptores (mini GBICs) se venden por separado

[redacted]

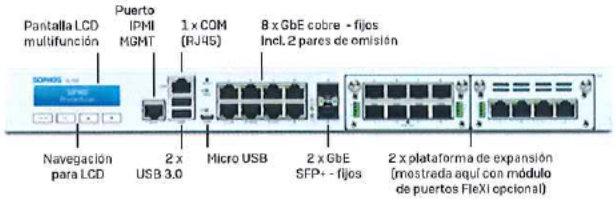
297

Dispositivos de montaje en bastidor de la serie XG de Sophos: XG 430, XG 450

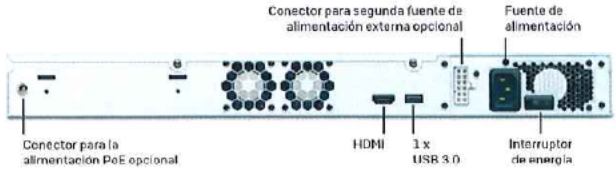
Especificaciones técnicas

Los dispositivos XG 430 y XG 450 de Sophos ofrecen un rendimiento empresarial para organizaciones distribuidas o mayores que las empresas de tamaño medio. Las opciones de conectividad son insuperables para dispositivos montables en bastidor, y cada modelo viene equipado con 8 puertos de cobre GbE, 2 puertos 10 GbE SFP+ y 2 ranuras FleXi Port adicionales que se pueden configurar con su elección de módulos opcionales. Para asegurar una alta disponibilidad, el XG 450 también ofrece características de redundancia sin precedentes en un dispositivo 1U con un segundo SSD (RAID) integrado y una segunda fuente de alimentación opcional disponible para ambos modelos.

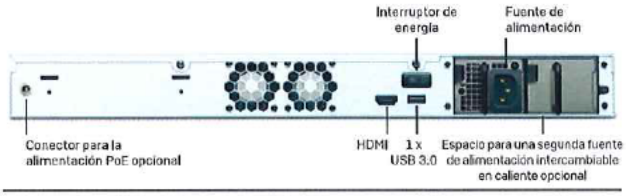
Vista frontal



Vista trasera del XG 430



Vista trasera del XG 450



Entorno	
Consumo de energía	XG 430: 28W, 96 BTU/h (inactivo) 79W, 270 BTU/h (carga completa) XG 450: 31W, 107 BTU/h (inactivo) 83W, 283 BTU/h (carga completa)
Temperatura en funcionamiento	0-40°C (en funcionamiento) -20 a + 80°C (almacenamiento)
Humedad	10%-90%, sin condensación

Certificaciones de productos	
Certificaciones	CB, UL, CE, FCC Clase A, ISED, VCCI, RCM, CCC, KC, BIS

Rendimiento[1]	XG 430 Rev. 2	XG 450 Rev. 2
Rendimiento del firewall	41 Gbps	50 Gbps
IMIX del firewall	14,5 Gbps	17,5 Gbps
Rendimiento de la VPN	4,8 Gbps	5,5 Gbps
Rendimiento del IPS	9 Gbps	10 Gbps
NGFW (IPS + Control aplic.) máx.	6 Gbps	7,5 Gbps
Rendimiento del antivirus (proxy)	6,5 Gbps	7 Gbps
Conexiones simultáneas	20.000.000	20.000.000
Conexiones nuevas/seg.	200.000	200.000
Número máximo de usuarios con licencia	sin restricciones	

Interfaces físicas		
Almacenamiento (cuarentena local/registros)	SSD integrado	2 x SSD integrados
Interfaces Ethernet (fijas)	8 GbE cobre (incl. 2 pares de omisión) 2 10 GbE SFP+*	
N.º de ranuras de puertos FleXi	2	
Módulos de puertos FleXi (opcional)	GbE cobre de 8 puertos GbE SFP de 8 puertos* 2 puertos de 10 GbE SFP+* 4 puertos de 10 GbE SFP+* 2 puertos de 40 GbE QSFP+* PoE GbE de 4 puertos PoE GbE de 8 puertos GbE cobre de 4 puertos con omisión LAN	
Puertos de E/S	2 x USB 3.0 (delantero) 1 x micro USB (delantero) 1 x USB 3.0 (trasero) 1 x COM (RJ45) (delantero) 1 x IPMI (delantero) 1 x HDMI (trasero)	
Pantalla	Módulo LCD multifunción	
Fuente de alimentación	Rango automático interno de 100-240VAC, 50-60 Hz Fuente de alimentación redundante opcional (externa)	Rango automático interno de 100-240VAC, 50-60 Hz Fuente de alimentación redundante de intercambio en caliente opcional (interna)

Especificaciones físicas		
Montaje	Montaje en bastidor 1U (railes deslizantes incluidos)	
Dimensiones Ancho x Profundidad x Altura	438 x 507,7 x 44mm 17,24 x 19,99 x 1,75 pulgadas	
Peso	7,6 kg / 16,76 lbs (fuera del paquete) 13,7 kg / 30,2 lbs (en el paquete)	7,8 kg / 17,2 lbs (fuera del paquete) 14,8 kg / 32,63 lbs (en el paquete)

* Los transceptores (mini GBICs) se venden por separado

[redacted]

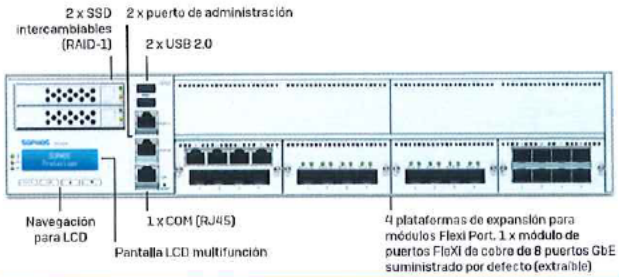
25

Dispositivos montados en bastidor de la serie XG de Sophos: XG 550, XG 650

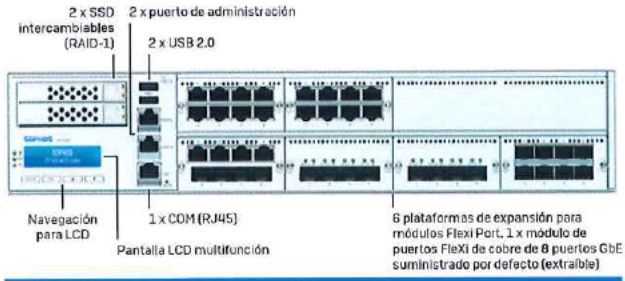
Especificaciones técnicas

Los dispositivos XG 550 y XG 650 de Sophos son firewalls de alto rendimiento equipados para proporcionar protección a grandes organizaciones distribuidas y en crecimiento. Ofrecen tecnología de CPU para poder funcionar sin esfuerzo como una solución "todo en uno" o un potente firewall de última generación. Los modelos ofrecen bien 4 (XG 550) o 6 (XG 650) plataformas de expansión Flexi Port para adaptar su conectividad a su entorno. De fábrica, se suministra un módulo de puertos de cobre de 8 GbE. En esta clase, se proporcionan características de redundancia de fábrica como SSD duales intercambiables y fuentes de alimentación.

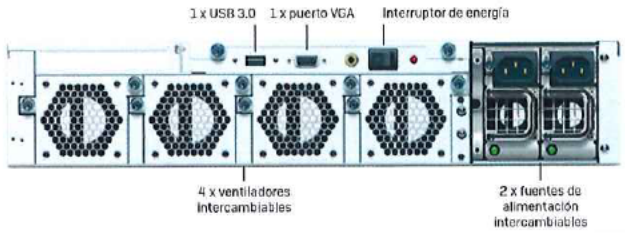
Vista delantera XG 550



Vista delantera XG 650



Vista trasera



Entorno

Consumo de energía	XG 550: 270,5W, 922,98 BTU/h (inactivo) 416,1W, 1419,79 BTU/h (carga completa) XG 650: 320,5W, 1093,59 BTU/h (inactivo) 493,1W, 1682,53 BTU/h (carga completa)
Temperatura en funcionamiento	0-40°C (en funcionamiento) -40 a +70°C (almacenamiento)
Humedad	5%-90%, sin condensación

Certificaciones de productos

Certificaciones	CB, UL, CE, FCC Clase A, ISED, VCCI, RCM, CCC, KC, BIS

Rendimiento[1]	XG 550 Rev. 2	XG 650 Rev. 2
Rendimiento del firewall	65 Gbps	85 Gbps
IMIX del firewall	23 Gbps	28 Gbps
Rendimiento de la VPN	8,4 Gbps	9 Gbps
Rendimiento del IPS	17 Gbps	20 Gbps
NGFW (IPS + Control aplic + filtro web) máx.	9 Gbps	10 Gbps
Rendimiento del antivirus (proxy)	10 Gbps	13 Gbps
Conexiones simultáneas	30.000.000	
Conexiones nuevas/seg.	220.000	240.000
Número máximo de usuarios con licencia	sin restricciones	

Interfaces físicas

Almacenamiento (cuarentena local/registros)	2 x SSD intercambiables integradas (RAID)	
Interfaces Ethernet (extraíbles)	8 GbE cobre	
N.º de ranuras de puertos FleXi	4	6
Módulos de puertos FleXi (opcional)	GbE cobre de 8 puertos GbE SFP de 8 puertos* 2 puertos de 10 GbE SFP+* 2 puertos de 40 GbE QSFP+* 4 puertos de 10 GbE SFP+* SFP* de 4 puertos más GbE cobre de 4 puertos con omisión LAN	
Puertos de E/S	2 x USB 2.0 (delantero) 1 x USB 3.0 (trasero) 2 x puerto admin. (eth0/eth1, frontal) 1 x COM (RJ45) (delantero) 1 x VGA (trasero)	
Pantalla	Módulo LCD multifunción	
Fuente de alimentación	2 x 100-240VAC, 50-60 Hz PSU de alcance automático internas e intercambiables	

Especificaciones físicas

Montaje	Railes deslizantes 2U (incluidos)
Dimensiones Ancho x Profundidad x Altura	438 x 600 x 88 mm 17,24 x 23,62 x 3,46 pulgadas
Peso	17,8 kg / 39,24 lbs (fuera del paquete) 27 kg / 59,53 lbs (en el paquete)

* Los transceptores (mini GBICs) se venden por separado

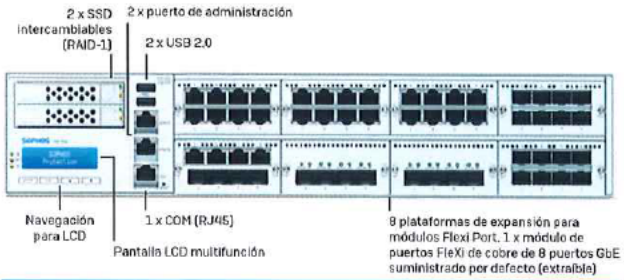
[redacted]

Dispositivos montados en bastidor de la serie XG de Sophos: XG 750

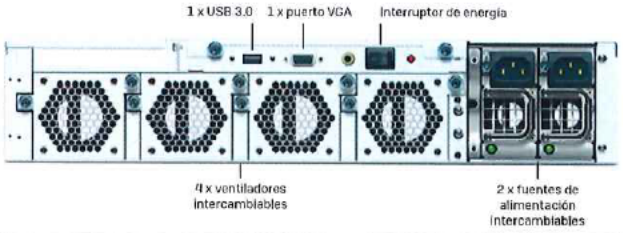
Especificaciones técnicas

El Sophos XG 750 es un firewall de alto rendimiento apto para entornos de centros de datos con un tráfico elevado y grandes empresas. Características como la tecnología multinúcleo de Intel y redundancia como SSD duales, fuentes de alimentación y ventiladores intercambiables, le aseguran una protección en todo momento. Un total de 8 plataformas de FleXi Port, una de las cuales viene equipada con un módulo de cobre de 8 puertos por defecto, permiten llevar más allá la conectividad y puede llegar a un máximo de 64 puertos usando los módulos opcionales..

Vista frontal



Vista trasera



Entorno	
Consumo de energía	326,5W, 1114,01 BTU/h (inactivo) 512,2W, 1747,62 BTU/h (carga completa)
Temperatura en funcionamiento	0-40°C (en funcionamiento) -40 a +70°C (almacenamiento)
Humedad	5%-90%, sin condensación

Certificaciones de productos	
Certificaciones	CB, UL, CE, FCC Clase A, ISED, VCCI, RCM, CCC, KC, BIS

Rendimiento[1]	XG 750 Rev. 2
Rendimiento del firewall	100 Gbps
IMIX del firewall	33,5 Gbps
Rendimiento de la VPN	11 Gbps
Rendimiento del IPS	22 Gbps
NGFW (IPS + Control aplic + filtro web) máx.	11,8 Gbps
Rendimiento del antivirus (proxy)	17 Gbps
Conexiones simultáneas	30.000.000
Conexiones nuevas/seg.	300.000
Número máximo de usuarios con licencia	sin restricciones

Interfaces físicas	
Almacenamiento (cuarentena local/registros)	2 x SSD intercambiables integradas (RAID)
Interfaces Ethernet (extraíbles)	8 GbE cobre
N.º de ranuras de puertos FleXi	8
Módulos de puertos FleXi (opcional)	GbE cobre de 8 puertos GbE SFP de 8 puertos* 2 puertos de 10 GbE SFP+* 2 puertos de 40 GbE QSFP+* 4 puertos de 10 GbE SFP+* SFP* de 4 puertos más GbE cobre de 4 puertos con omisión LAN
Puertos de E/S	2 x USB 2.0 (delantero) 1 x USB 3.0 (trasero) 2 x puerto admin. (eth0/eth1, frontal) 1 x COM (RJ45) (delantero) 1 x VGA (trasero)
Pantalla	Módulo LCD multifunción
Fuente de alimentación	2 x 100-240VAC, 50-60 Hz de alcance automático externas e intercambiables

Especificaciones físicas	
Montaje	Railes deslizantes 2U (incluidos)
Dimensiones Ancho x Profundidad x Altura	438 x 600 x 88 mm 17,24 x 23,62 x 3,46 pulgadas
Peso	17,8 kg / 39,24 lbs (fuera del paquete) 27 kg / 59,53 lbs (en el paquete)

* Los transceptores (mini GBICs) se venden por separado

[redacted]

Adapte la conectividad con módulos opcionales

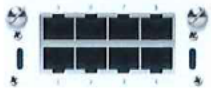
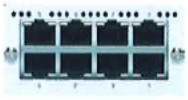
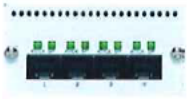
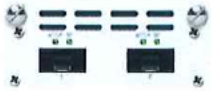
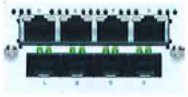
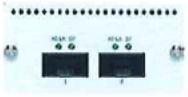
Módulos de conectividad para modelos de escritorio

Añada opciones de conectividad adicionales a sus dispositivos de escritorio para mejorar el alcance y el rendimiento de su red.

Módulos para modelos de escritorio		
Módulo 3G/4G: (para XG/SG 125(w) y 135(w) Rev.3 solamente) 2 antenas externas, ranura de tarjeta SIM Admite LTE (Cat-6)/DC-HSPA+/HSPA+/HSPA/UMTS (WCDMA, versión APAC también TD-SCDMA)	Módem DSL – SFP: (para XG/SG 1xx(w) Rev.3 solamente) El formato SFP admite todos los estándares VDSL2 definidos en ITU –T G.993.2, G.994.1, G.997.1 y los perfiles VDSL2 8a, 8b, 8c, 8d, 12a, 12b, 17a	2.º módulo de radio Wi-Fi: (para XG/SG 135w Rev.3 solamente) 802.11a/b/g/n/ac, 2 x 2 MIMO, 2,4 o 5 GHz, 2 antenas externas

Módulos FleXi Port para 1U y 2U

Configure su hardware para adaptarlo a su infraestructura y cámbielo a medida que usted lo necesite. Nuestros módulos de puerto LAN FleXi opcionales le proporcionan la libertad para seleccionar la conectividad que necesita – cobre, fibra, 10 GbE, 40 GbE. Usted decide.

Módulos FleXi Port para 1U		Módulos FleXi Port para 2U	
	Módulo FleXi Port de 8 puertos GbE de cobre (para SG/XG 2xx/3xx/4xx solamente)		Módulo FleXi Port de 8 puertos GbE de cobre (para XG 750 y SG/XG 550/650 Rev. 2 solamente)
	Módulo FleXi Port de 8 puertos GbE SFP (para SG/XG 2xx/3xx/4xx solamente)		Módulo FleXi Port de 8 puertos GbE SFP (para XG 750 y SG/XG 550/650 Rev. 2 solamente)
	Módulo FleXi Port de 2 puertos de 10 GbE SFP+ (para SG/XG 2xx/3xx/4xx solamente)		Módulo FleXi Port de 2 puertos de 10 GbE SFP+ (para XG 750 y SG/XG 550/650 Rev. 2 solamente)
	Módulo FleXi Port de 4 puertos de 10 GbE SFP+ (para SG/XG 2xx/3xx/4xx solamente)		Módulo FleXi Port de 4 puertos de 10 GbE SFP+ (para XG 750 y SG/XG 550/650 Rev. 2 solamente)
	Módulo FleXi Port de 2 puertos de 40 GbE QSFP+ (para SG/XG 210 Rev. 3 y SG/XG 230, 3xx y 4xx Rev. 2 solamente)		Módulo FleXi Port de 4 puertos GbE SFP más 4 puertos GbE de cobre con omisión LAN (para SG/XG 550/650 Rev. 2 y XG 750 solamente)
	Módulo de puertos PoE FleXi de 4 puertos GbE de cobre (Para SG/XG 210 Rev. 3 y SG/XG 230, 3xx y 4xx Rev. 2 solamente)		Módulo FleXi Port de 2 puertos de 40 GbE QSFP+ (para XG 750 y SG/XG 550/650 Rev.2 solamente)
	Módulo de puertos PoE FleXi de 8 puertos GbE de cobre (Para SG/XG 210 Rev. 3 y SG/XG 230, 3xx y 4xx Rev. 2 solamente)		

Importante: Los transceptores (mini GBICs) se venden por separado.

[redacted]



Protección inalámbrica de Sophos

Disponga de acceso inalámbrico seguro y fiable en toda la oficina

Utilice su Sophos XG Firewall como controlador inalámbrico para centralizar y simplificar la gestión y la seguridad de las conexiones inalámbricas. Sophos Wireless Protection se incluye en la licencia de firewall básica y, por ejemplo, proporciona soporte completo para puntos de acceso inalámbricos para configurar fácilmente el acceso para invitados y visitantes. El firewall configura de forma automática nuestros puntos de acceso opcionales y todos los clientes inalámbricos obtienen también protección completa contra las amenazas.

Elija un punto de acceso

Nuestros puntos de acceso están fabricados con los últimos conjuntos de chips de nivel empresarial y alta velocidad, con antenas especialmente diseñadas, recursos de memoria y CPU adicionales, y cifrado con aceleración de hardware. Obtenga más información.

Dispositivos de hardware con WiFi integrado

Nuestros dispositivos de escritorio de la serie XG están disponibles con un punto de acceso inalámbrico integrado. Es posible ampliar la cobertura añadiendo punto de acceso de Sophos. Consulte la sección sobre Hardware para obtener más información.

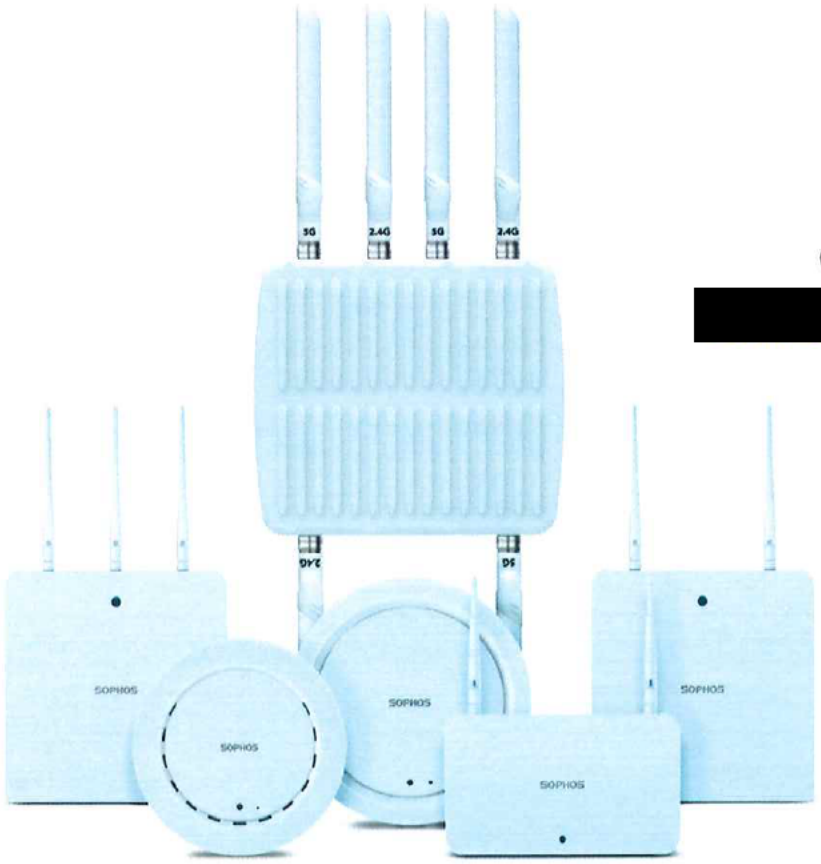
Sophos RED (dispositivo Ethernet remoto)

Convierta cualquier lugar en un lugar seguro con nuestros dispositivos Ethernet remotos (RED)

Si tiene sucursales, puntos de venta, puestos remotos u otros similares, necesita ampliar su red segura de forma fácil y asequible más allá de sus instalaciones principales. Para ello, los dispositivos Ethernet remotos (RED) de Sophos son la solución ideal. Excepcionalmente simples y tremendamente asequibles, los RED proporcionan una solución elegante para la construcción de una red distribuida segura.

Listo para usar

Sophos RED facilita la ampliación de su red segura a otras ubicaciones. No requiere de habilidades técnicas en el sitio remoto; basta con introducir el ID del dispositivo RED en su consola de XG Firewall y enviarlo. Nada más se enchufe y se conecte a Internet, se pondrá en contacto con su firewall y establecerá un túnel VPN seguro dedicado. Es así de fácil.



Sophos Firewall Manager (SFM)

Sophos Firewall Manager (SFM) ofrece una potente administración centralizada para todos sus firewalls de Sophos a través de múltiples sitios o sucursales de clientes, todo desde una única pantalla. Independientemente de si usted es MSP, administrador de seguridad de la red de la empresa o simplemente administra unas pocas oficinas pequeñas, SFM simplifica la gestión de la seguridad ya que permite una imposición de políticas consistente, una fácil implementación de nuevas políticas y supervisión de un vistazo de la salud de los dispositivos. SFM le ahorra tiempo, dinero y facilita las tareas de administración.

Administración centralizada completa

Administre todas las políticas y la configuración del firewall desde una misma consola.

Supervisión intuitiva

Indicadores instantáneos del estado general de la red y los dispositivos.

Amplios controles administrativos

Administración basada en roles, control de cambios y registros.

Opciones de implementación flexibles

Disponibles como dispositivos de hardware, de software o virtuales.

Sophos iView v2

Supervisar una red distribuida en múltiples ubicaciones puede ser todo un desafío. Sophos iView puede ayudarle en esta labor. Le proporciona una visión inteligente e ininterrumpida de la red desde un único panel. Si usted tiene varios dispositivos, necesita informes consolidados o simplemente necesita ayuda con la gestión de registros o con el cumplimiento, Sophos iView es la solución ideal.

Informes consolidados

Informes agregados en múltiples dispositivos de firewall de Sophos y Cyberoam.

Informes basados en los usuarios

Nuestra identidad de usuario patentada de nivel 8 proporciona visibilidad sobre las actividades de los usuarios independientemente de dónde estén trabajando.

Inteligencia de seguridad

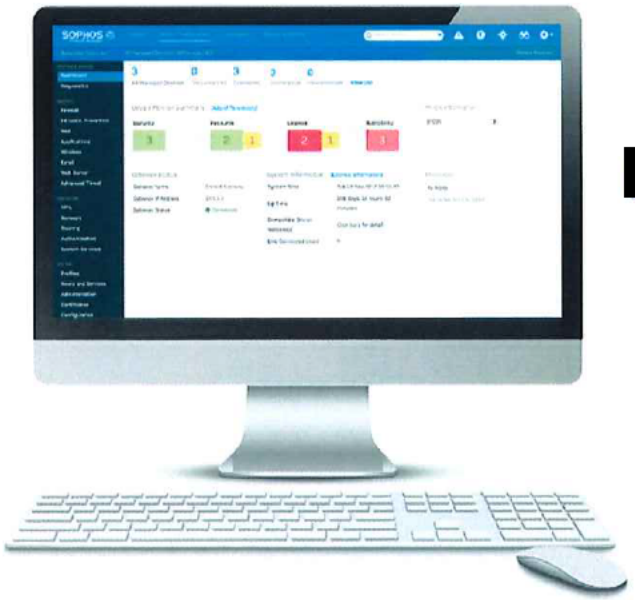
Identifique problemas de red potenciales y posibles ataques en cualquier lugar de la red.

Copia de seguridad y gestión de registros

Registra datos procedentes de múltiples dispositivos en ubicaciones distribuidas con funciones de indexado inteligente y búsqueda sencilla.

Opción de despliegue

Disponible como ISO de software o dispositivo virtual.





291

Pruébelo de forma gratuita - tanto para negocios como para el hogar

Si tiene alguna otra pregunta, visite es.sophos.com o póngase en contacto con uno de nuestros agentes comerciales.

Prueba gratuita de 30 días sin compromiso

Si desea probar el producto, puede obtener una versión completa registrándose en nuestra prueba gratuita de 30 días.

Véalo en acción ahora

Puede recorrer la interfaz de usuario con nuestra demostración interactiva o ver vídeos en los que comprobará cómo ofrecemos seguridad de la red sin complicaciones.
Visite es.sophos.com/xgfirewall

Versión para uso doméstico gratuita

Sophos XG Firewall Home Edition es una versión de software completamente equipada que proporciona protección completa para su red, web, correo y aplicaciones web con funciones de VPN, solo para uso doméstico y limitado a 4 núcleos virtuales y 6GB de RAM.
Visite es.sophos.com/freetools

[1] General: Rendimiento maximo calculado en condiciones de prueba óptimas utilizando SF-OS 17.0 con la clasificación de aplicaciones desactivada utilizando el test de rendimiento Spirent /Avalanche de estándar industrial y herramientas de prueba Ixia. El rendimiento real puede variar en función de las condiciones de la red y de los servicios activados.
- FW: Rendimiento de UDP basado en RFC 2544 utilizando un tamaño de paquete de 1518 bytes.
- FW IMIX: Rendimiento de UDP basado en una combinación de tamaños de paquetes de 48 bytes, 576 bytes y 1518 bytes.
- IPS/NGFW: Rendimiento de HTTP utilizando el conjunto de reglas de IPS predeterminado y un tamaño de objeto de 512 KB (NGFW: con control de aplicaciones activado)
- VPN: Rendimiento de HTTP utilizando múltiples túneles y un tamaño de respuesta HTTP de 512 KB.
- AV: Rendimiento de HTTP utilizando un proxy web y un tamaño de respuesta de 200 KB.

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com

[redacted]

SOPHOS

© Copyright 2016 Sophos Ltd. Todos los derechos reservados.
Constituida en Inglaterra y Gales con el número de registro 2096520. The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP. Reservados todos los derechos. Sophos es una marca registrada de Sophos Ltd. Todos los demás productos y empresas mencionados son marcas comerciales o registradas de sus respectivos propietarios.
Nº de patente de EE. UU. 7.665.130

SOPHOS

Security made simple.

Sophos SG/XG Series Appliances

Technical Specifications

DESKTOP MODELS	Available as XG only	Available as SG and XG	Available as SG and XG	Available as SG and XG	Available as SG and XG
MODEL	**85(w) rev.1**	**105(w) rev.2**	**115(w) rev.2**	**125(w) rev.2**	**135(w) rev.2**
Form factor	desktop	desktop	desktop	desktop	desktop
TECHNICAL SPECS					
Processor	Intel Atom Baytrail Dual Core (1.33 GHz)	Intel Atom Baytrail Dual Core (1.46 GHz)	Intel Atom Baytrail Dual Core (1.75 GHz)	Intel Atom Rangeley Dual Core (1.7 GHz)	Intel Atom Rangeley Quad Core (2.4 GHz)
Memory	2 GB DDR3	2 GB DDR3	4 GB DDR3	4 GB DDR3	6 GB DDR3
Hard Drive	8 GB eMMC	64 GB SSD	64 GB SSD	64 GB SSD	64 GB SSD
Ethernet Ports					
GigEth Copper	4	4	4	8	8
GigEth SFP GBIC	-	-	-	-	-
LAN module slots	-	-	-	-	-
I/O Ports					
USB	2 (rear)	2 (rear)	2 (rear)	2 (rear)	2 (rear)
COM	1 (rear) RJ45	1 (front) RJ45	1 (front) RJ45	1 (front) RJ45	1 (front) RJ45
VGA	-	1 (rear)	1 (rear)	1 (rear)	1 (rear)
PHYSICAL SPECS					
Dimensions w*h*d (mm)	225x44x150	225x44x150	225x44x150	288x44x186.8	288x44x186.8
Weight (kg) unpacked/packed	0.945 / 1.965	1.19 / 2.185	1.19 / 2.185	1.7 / 2.82	1.7 / 2.82
POWER					
Power Supply	External auto-ranging DC:12V 110-240VAC, 50-60 Hz	External auto-ranging DC:12V 110-240VAC, 50-60 Hz	External auto-ranging DC:12V 110-240VAC, 50-60 Hz	External auto-ranging DC:12V 110-240VAC, 50-60 Hz	External auto-ranging DC:12V 110-240VAC, 50-60 Hz
Power Consumption (idle)	3.24W/11.04BTU/h	4.83W, 16.47	4.83W, 16.47BTU/h	12.46W, 49.3BTU/h	12.46W, 49.3BTU/h
Power Consumption (full load)	5.64W/19.232BTU/h	9.84W, 33.55BTU/h	9.84W, 33.55BTU/h	26.16W, 89.2BTU/h	26.16W, 89.2BTU/h
ENVIRONMENT					
Noise level (avg.) (with/without smart fan)	0 dBA (fanless)	0 dBA (fanless)	0 dBA (fanless)	33.9 / 47 dBA	33.9 / 47 dBA
Operating Temperature	0°C - 40°C	0°C - 40°C	0°C - 40°C	0°C - 40°C	0°C - 40°C
Storage Temperature	-20°C - 80°	-20°C - 80°	-20°C - 80°	-20°C - 80°	-20°C - 80°
Humidity	10% - 90% non-condensing	10% - 90% non-condensing	10% - 90% non-condensing	10% - 90% non-condensing	10% - 90% non-condensing
CERTIFICATIONS					
Certifications (Safety, EMC)	CB, CE, FCC Class B, VCCI, RCM, UL, CCC, SRRC, MIC	CB, CE, FCC Class B, VCCI, C- Tick, UL, CCC	CB, CE, FCC Class B, VCCI, C- Tick, UL, CCC	CB, CE, FCC Class B, VCCI, C- Tick, UL, CCC	CB, CE, FCC Class B, VCCI, C- Tick, UL, CCC
MTBF (hours) (MIL-217)	80496 (XG85)	65771 (SG105)	66102 (SG115)	64157 (SG125)	60944 (SG135)
	75220 (XG85w)	62738 (SG105w)	62671 (SG115w)	62944 (SG125w)	59517 (SG135w)

[redacted]

Date first published: 2015

SOPHOS

Security made simple.

Sophos SG/XG Series Appliances

Technical Specifications

2017 1U MODELS	Available as SG and XG	Available as SG and XG	Available as SG and XG	Available as SG and XG	Available as SG and XG	Available as SG and XG
MODEL	**210 Rev.3**	**230 Rev.2**	**310 Rev.2**	**330 Rev.2**	**430 Rev.2**	**450 Rev.2**
Form factor	1U rackmount	1U rackmount	1U rackmount	1U rackmount	1U rackmount	1U rackmount
TECHNICAL SPECS						
Processor	Intel Celeron Dual Core G3900 @ 2.8GHz	Intel Pentium Dual Core G4400 @ 3.3GHz	Intel Core i3 Dual Core 6100 @ 3.7GHz	Intel Core i5 Quad Core 6500 @ 3.2 GHz	Intel Xeon Quad Core E3- 1225v5 @3.3 GHz	Intel Xeon Quad Core E3-1275v5 @3.6 GHz
Memory	8 GB DDR4	8 GB DDR4	12 GB DDR4	12 GB DDR4	16 GB DDR4	16 GB DDR4
Hard Drive[1]	120 GB SSD	120 GB SSD	180 GB SSD	180 GB SSD	240 GB SSD	2*240 GB SSD (RAID-1)
Ethernet Ports						
GigEth Copper	6	6	8	8	8	8
GigEth SFP	2	2	2	2	-	-
GigEth SFP+	-	-	2	2	2	2
LAN module slots	1	1	1	1	2	2
IPMI	-	-	-	-	1	1
I/O Ports						
USB	3 (2 front, 1 rear)	3 (2 front, 1 rear)	3 (2 front, 1 rear)	3 (2 front, 1 rear)	3 (2 front, 1 rear)	3 (2 front, 1 rear)
COM	2 (front) RJ45/Micro USB	2 (front) RJ45/Micro USB	2 (front) RJ45/Micro USB	2 (front) RJ45/Micro USB	2 (front) RJ45/Micro USB	2 (front) RJ45/Micro USB
HDMI	1 (rear)	1 (rear)	1 (rear)	1 (rear)	1 (rear)	1 (rear)
PHYSICAL SPECS						
Dimensions w*h*d (mm)	438x44x344.4	438x44x344.4	438x44x405.5	438x44x405.5	438x44x507.7	438x44x507.7
Weight (kg) unpacked/packed	SG: 5.2 / 7.2 XG: 5.2 / 7.7	SG: 5.2 / 7.2 XG: 5.2 / 7.7	SG: 5.6 / 8.1 XG: 5.8 / 8.8	SG: 5.8 / 8.1 XG: 5.8 / 8.8	SG: 7.6 / 12.7 XG: 7.6 / 13.7	SG: 7.8 / 13.8 XG: 7.8 / 14.8
POWER						
Power Supply	Internal auto-ranging 100-240VAC, 50-60 Hz	Internal auto-ranging 100-240VAC, 50-60 Hz	Internal auto-ranging 100-240VAC, 50-60 Hz	Internal auto-ranging 100-240VAC, 50-60 Hz	Internal auto-ranging 100-240VAC, 50-60 Hz	Internal auto-ranging 100-240VAC, 50-60 Hz
2nd Power Supply Option	External redundant PSU option	External redundant PSU option	External redundant PSU option	External redundant PSU option	External redundant PSU option	Internal hot swap redundant PSU option
Power Consumption (idle)	19W, 65 BTU/h	21W, 72 BTU/h	32W, 109BTU/h	36W, 122BTU/h	28W, 96 BTU/h	31W, 107 BTU/h
Power Consumption (full load)	35W, 119 BTU/h	41W, 141 BTU/h	49W, 167 BTU/h	54W, 184 BTU/h	79W, 270 BTU/h	83W, 283 BTU/h
ENVIRONMENT						
Noise level (avg.) (with/without smart fan)	36.9 / 57.6 dBA	36.9 / 57.6 dBA	25.4 / 58 dBA	25.4 / 58 dBA	37.5 / 55 dBA	37.5 / 55 dBA
Operating Temperature	0°C - 40°C	0°C - 40°C	0°C - 40°C	0°C - 40°C	0°C - 40°C	0°C - 40°C
Storage Temperature	-20°C - 80°	-20°C - 80°	-20°C - 80°	-20°C - 80°	-20°C - 80°	-20°C - 80°
Humidity	10% - 90% non-condensing	10% - 90% non-condensing	10% - 90% non-condensing	10% - 90% non-condensing	10% - 90% non-condensing	10% - 90% non-condensing
CERTIFICATIONS						
Certifications (Safety, EMC)	CB, UL, CE, FCC Class A, ISED, VCCI, RCM, CCC, BIS (planned), MSIP/KCC (planned)	CB, UL, CE, FCC Class A, ISED, VCCI, RCM, CCC, BIS (planned), MSIP/KCC (planned)	CB, UL, CE, FCC Class A, ISED, VCCI, RCM, CCC, BIS (planned), MSIP/KCC (planned)	CB, UL, CE, FCC Class A, ISED, VCCI, RCM, CCC, BIS (planned), MSIP/KCC (planned)	CB, UL, CE, FCC Class A, ISED, VCCI, RCM, CCC, BIS (planned), MSIP/KCC (planned)	CB, UL, CE, FCC Class A, ISED, VCCI, RCM, CCC, BIS (planned), MSIP/KCC (planned)
MTBF (hours) (Bellcore TR-332 Issue 6)	112650 hrs	112650 hrs	109451 hrs	109451 hrs	94332 hrs	88700 hrs

[1] Capacity may vary if in short supply.

[redacted]

Published: July 2017

SOPHOS

Security made simple.

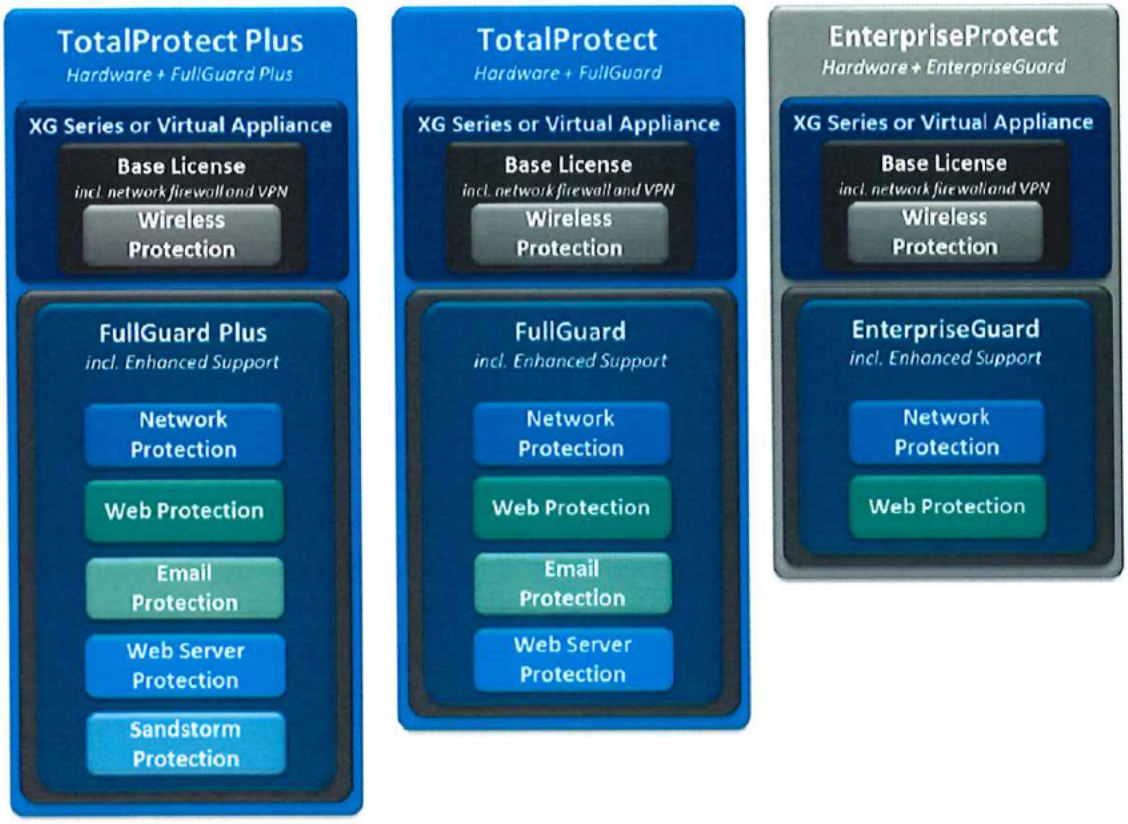
Sophos SG/XG Series Appliances

Technical Specifications

2017 2U MODELS	Available as SG and XG	Available as SG and XG	Available as XG only
Model	**550 Rev.2**	**650 Rev.2**	**750 Rev.2**
Form factor	2U rackmount	2U rackmount	2U rackmount
PHYSICAL SPECS			
Processor	2*Intel Xeon Eight Core E5-2630v3 @ 2.4GHz	2*Intel Xeon Ten Core E5-2660v3 @ 2.6GHz	2*Intel Xeon 12 Core E5-2680v3 @ 2.5GHz + Coleto Creek Co-Proc.
Memory	24 GB DDR4 ECC	48 GB DDR4 ECC	64 GB DDR4 ECC
Hard Drive	2* 480 GB SSD (RAID-1) hot-swap	2*480 GB SSD (RAID-1) hot-swap	2* 480 GB SSD (RAID-1) hot-swap
Ethernet Ports			
GigEth Copper	8 (default module)	8 (default module)	8 (default module)
GigEth SFP GBIC	-	-	-
LAN module slots	4	6	8
GigEth MGMT	2	2	2
I/O Ports			
USB	3 (2 front, 1 rear)	3 (2 front, 1 rear)	3 (2 front, 1 rear)
COM	1 (front) RJ45	1 (front) RJ45	1 (front) RJ45
VGA	1 (rear)	1 (rear)	1 (rear)
PHYSICAL SPECS			
Dimensions w*h*d (mm)	438x88x600	438x88x600	438x88x600
Weight (kg) unpacked/packed	17.8 / 27	17.8 / 27	17.8 / 27
POWER			
Power Supply	2*Internal auto- ranging ATX 100-240VAC, 50-60 Hz hot swap	2*Internal auto- ranging ATX 100-240VAC, 50-60 Hz hot swap	2*Internal auto- ranging ATX 100-240VAC, 50-60 Hz hot swap
Power Consumption (idle)	270.5W, 922.98BTU/h	320.5W, 1093.59BTU/h	326.5W, 1114.01BTU/h
Power Consumption (full load)	416.1W, 1419.79BTU/h	493.1W, 1682.53BTU/h	512.2W, 1747.62BTU/h
ENVIRONMENT			
Noise level (avg.) (with/without smart fan)	57.1 dBA	57.1 dBA	57.1 dBA
Operating Temperature	0°C - 40°C	0°C - 40°C	0°C - 40°C
Storage Temperature	-40°C - 70°	-40°C - 70°	-40°C - 70°
Humidity	5% - 90% non-condensing	5% - 90% non-condensing	5% - 90% non-condensing
CERTIFICATIONS			
Certifications (Safety, EMC)	CE, UL, FCC, ISED, CCC, VCCI, RCM, BIS (CRS)	CE, UL, FCC, ISED, CCC, VCCI, RCM, BIS (CRS)	CE, UL, FCC, ISED, CCC, VCCI, RCM, BIS (CRS)
MTBF (hours) (Telcordia SR-332 Issue 3)	31,258	31,258	31,258

[redacted]

Published: April 2017



XG Firewall Features by Subscription Summary

Features (as listed above)		FullGuard Plus				
			FullGuard			
			EnterpriseGuard			
	Base Firewall	Sandstorm Protection	Network Protection	Web Protection	Email Protection	Web Server Protection
General Management (incl. HA)	●					
Firewall, Networking & Routing	●					
Base Traffic Shaping & Quotas	●					
Secure Wireless	●					
Authentication	●					
Self-Serve User Portal	●					
Base VPN Options	●					
IPSec Client	Sold seperately					
Sandstorm Protection		●				
Intrusion Prevention (IPS)			●			
ATP and Security Heartbeat™			●			
Remote Ethernet Device (RED) VPN			●			
Clientless VPN			●			
Web Protection and Control				●		
Application Protection and Control				●		
Web and App Traffic Shaping				●		
Email Protection and Control					●	
Email Quarantine Management					●	
Email Encryption and DLP					●	
Web Application Firewall Protection						●
Logging and Reporting	●		●	●	●	●

[redacted]

[redacted]

286

SOPHOS
Security made simple.

Burlington, MA, USA
22 de Junio de 2018

Atención:
Señores
Ministerio de Trabajo y Previsión Social
Ciudad de El Salvador, San Salvador

CERTIFICADO DE AUTORIZACION DEL FABRICANTE

Estimado Señores:

El grupo de empresas de Sophos es líder mundial en seguridad informática y protección de datos para empresas. Sophos ofrece complete protección y control a entidades / organizaciones privadas, de educación y gobiernos, y provee protección integral de datos y soluciones de seguridad integradas de red.

Sophos, Inc., cuya casa matriz está en 3 Van de Graaff Drive, Burlington MA, 01803, EEUU, confirma que:

Dada Dada y Cía S.A. de C.V., en Ciudad de San Salvador, El Salvador, es un canal de Nivel Silver autorizado para suministrar productos de Sophos en el territorio de El Salvador.

Sin otro particular y quedando a la espera de poder servirles.

Atentamente,

[redacted]

[redacted]

[redacted]

SOPHOS

Security made simple.

Certificate of Completion

Juan Barahona

has successfully complete the course

Sophos XG Firewall v15 - Certified Engineer

held on Dec 23, 2014

[redacted]

SOPHOS

Security made simple.

Certificate of Completion

Julio Hurtado

has successfully complete the course

Sophos XG Firewall v15 - Certified Engineer

held on Dec 23, 2014

[redacted]

SOPHOS

Security made simple.

Certificate of Completion

Eliseo Soriano

has successfully complete the course

Sophos XG Firewall v16 - Certified Engineer

held on Dec 28, 2015

[redacted]

283

SOPHOS

Security made simple.

Certificate of Completion

Alexander Portillo

has successfully complete the course

Sophos XG Firewall v16 - Certified Engineer

held on Dec 28, 2015

[redacted]

40

282

Señores:
ISRI:
Presentes.

Por este medio extendemos la presente referencia a la empresa DADA DADA y CIA S.A. de C.V. Quienes nos han suministrado Soluciones de Seguridad Perimetral (Firewall UTM) Marca Cyberoam, suministrados al TRIBUNAL SUPREMO ELECTORAL, por un plazo de 10 días hábiles para entregar los equipos, comprendidos Febrero de 2015.

Se emite la siguiente calificación, por el suministro proporcionado:

Excelente	(X)
Muy Bueno	( )
Bueno	( )
Regular	( )

Y para efectos de ser presentada al ISRI, se emite la presente constancia a los Siete días del mes de Marzo de 2016.

[redacted]

[redacted]

[redacted]

Instituto Salvadoreño de
Rehabilitación Integral

CARTA DE REFERENCIA DE SERVICIOS DE FIREWALL

Señores:
ESCUELA NACIONAL DE AGRICULTURA
Presente.

Referencia: Libre Gestión No 11/2016 "SUMINISTRO DE SERVICIO DE FIREWALL PARA LA ESCUELA NACIONAL DE AGRICULTURA

En atención al requerimiento señalado en la Libre Gestión de la referencia y a solicitud de DADA DADA Y CIA, hacemos constar que dicha sociedad, nos suministra los servicios de Firewall UTM señalando que de acuerdo a nuestros registros recibimos la experiencia de acuerdo al detalle siguiente:

No	DESCRIPCION DEL SERVICIO	CALIFICACION		
		EXCELENTE	BUENO	REGULAR
1	CALIDAD DEL SUMINISTRO	X		
2	ENTREGA DEL SERVICIO	X		

Y para los efectos que se estimen convenientes extiendo la presente a los diecinueve días del mes de Julio de dos mil dieciséis.

[redacted]

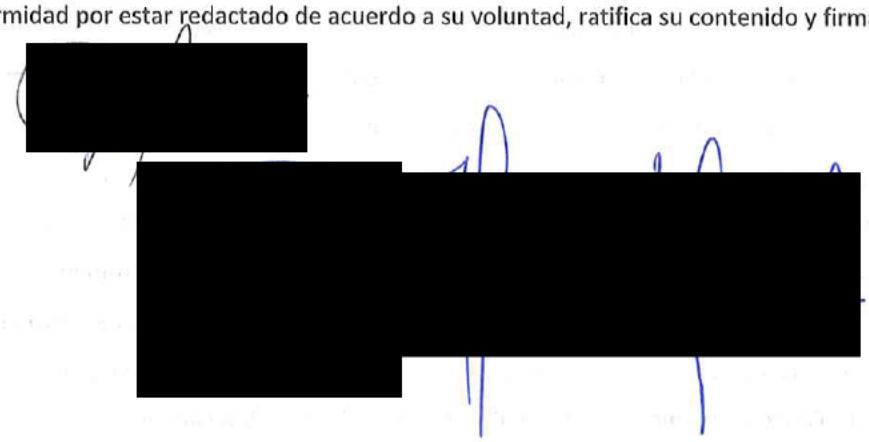
EAMG.-
19/07/2016



DECLARACION JURADA

En la ciudad de San Salvador, a las ocho horas treinta minutos del día veintiuno de junio de dos mil dieciocho.- Ante mí, [redacted] Notario, del domicilio de la ciudad y Departamento de [redacted], comparece el señor [redacted] de [redacted] años de edad, [redacted] del domicilio de [redacted] departamento de [redacted] persona a quien hoy conozco e identifique por medio de su Documento Único de Identidad número [redacted], con Número de Identificación Tributaria [redacted], quien actúa en su calidad de Apoderado Especial Administrativo de "DADA DADA Y COMPAÑÍA, SOCIEDAD ANONIMA DE CAPITAL VARIABLE", que puede abreviarse DADA DADA Y CIA, S. A. DE C. V., del domicilio de la ciudad y Departamento de [redacted] con Número de Identificación Tributaria [redacted], personería que relacionaré al final del presente documento; Y **ME DICE**: Que con el objeto de participar en el proceso por Libre Gestión número LG MTPS DOCE - DOS MIL DIECIOCHO, relativo a "ADQUISICION DE DIECINUEVE EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS", promovido por el MINISTERIO DE TRABAJO Y PREVISION SOCIAL, **BAJO JURAMENTO DECLARA HACE LAS SIGUIENTES DECLARACIONES**: **A)** Que su representada no emplea a niñas, niños, adolescentes por debajo de la edad mínima de admisión al empleo y se cumple con la normativa que prohíbe el trabajo infantil y de protección de la persona adolescente trabajadora; en caso se comprobare por la Dirección General de Inspección de Trabajo del Ministerio de Trabajo y Previsión Social el incumplimiento a la normativa anterior; reconoce y acepta que la institución contratante iniciará el procedimiento sancionatorio que dispone el Art. 160 de la LACAP para determinar el cometimiento o no dentro del procedimiento adquisitivo en el cual está participando, de la conducta tipificada como causal de inhabilitación prevista en el Arto. 158 Romano V literal b) de la LACAP que dispone "Invocar hechos falsos para obtener la adjudicación de la contratación". Se entenderá por comprobado el incumplimiento a la normativa por parte de la Dirección General de Inspección de Trabajo, si durante el trámite de re inspección se determina que hubo subsanación por haber cometido una infracción, o por el contrario si se remitiere a procedimiento sancionatorio, y en este último caso deberá finalizar el procedimiento para conocer la resolución final. El compareciente me manifiesta que para los efectos legales de esta acta notarial y para los demás que surgieren en el proceso de la Libre Gestión, señala como Domicilio esta Ciudad, a cuyos tribunales se somete expresamente. Así se expresó el compareciente, y yo el suscrito Notario, **DOY FE**: **a)** De haberme cerciorado de la identidad del compareciente; **b)** de ser legítima y suficiente la personería con que actúa el compareciente señor Juan Carlos Flores, por haber tenido a la vista: a) Escritura pública de Poder Especial Administrativo otorgado por la sociedad antes mencionada, en la ciudad de San Salvador, a las diez horas y quince minutos del día ocho

de mayo de dos mil diecisiete, ante los oficios notariales del doctor [redacted] e inscrito en el Registro de Comercio bajo el número [redacted] Libro [redacted] del Registro de Otros Contratos Mercantiles, con fecha diecisiete de mayo de dos mil diecisiete, constando en dicho poder que el Licenciado Guillermo Ventura Dada Peña en su calidad de Administrador Único Propietario y representante legal de DADA DADA Y COMPAÑÍA, SOCIEDAD ANONIMA DE CAPITAL VARIABLE confirió a favor del compareciente señor Juan Carlos Flores, Poder Especial Administrativo con facultades para comparecer en instrumentos como el presente; estando en dicha escritura plenamente establecida y comprobada la existencia legal de la sociedad, lo mismo que la personería del Licenciado Guillermo Ventura Dada Peña; y c) De haberle explicado los efectos legales de la presente acta notarial que consta de una hoja; y leída que se la hube íntegramente en un solo acto sin interrupción, manifiesta su conformidad por estar redactado de acuerdo a su voluntad, ratifica su contenido y firmamos. DOY FE.



San Salvador, 21 de Junio de 2018.-

Señores
MINISTERIO DE TRABAJO Y
PREVISION SOCIAL.-
Presente.

Yo, [redacted] de [redacted] años de edad, [redacted] del domicilio de Ciudad [redacted], Departamento de [redacted], con Documento Único de Identidad número [redacted], con Número de Identificación Tributaria [redacted] actuando en nombre y representación en mi calidad de Apoderado Especial Administrativo de "DADA DADA Y COMPAÑÍA, SOCIEDAD ANONIMA DE CAPITAL VARIABLE", que puede abreviarse DADA DADA Y CIA, S. A. DE C. V., del domicilio de la ciudad y Departamento de San Salvador, con Número de Identificación Tributaria cero seiscientos catorce-ciento cincuenta mil trescientos sesenta y dos-cero cero uno-cinco.

Declaro bajo juramento:

Que tomando en consideración las definiciones e indicadores establecidos en los criterios de Clasificación para las Personas Naturales o Jurídicas; afirmo que esta empresa se encuentra dentro del siguiente rango:

MICRO	[ ]
PEQUEÑA	[ ]
MEDIANA	[X]
NINGUNA DE LAS ANTERIORES	[ ]

Asimismo, manifiesto que toda la información declarada es verdad y puede ser verificada oportunamente y acepto que en caso de fraude o faltar a la verdad, los beneficios que pudiera haber logrado en aplicación de la legislación que promueve el desarrollo de las micro, pequeña y mediana empresa (Artículo 39 C., Ley de Adquisiciones y Contrataciones de la Administración Pública), pueden ser anuladas con los efectos legales correspondientes y la responsabilidad legal de mi parte.

[redacted]

Apoderado Especial Administrativo

[redacted]

Sello del Ofertante

El infrascrito Notario DA FE: A) Que la firma que calza al pie del anterior documento es AUTENTICA, por haber sido puesta de su puño y letra a mi presencia por el señor [redacted]; y B) De ser legítima y suficiente la personería con que actúa el señor Juan Carlos Flores, por haber tenido a la vista: a) Escritura pública de Poder Especial Administrativo otorgado por la sociedad antes mencionada, en la ciudad de San Salvador, a las diez horas y quince

minutos del día ocho de mayo de dos mil diecisiete, ante los oficios notariales del doctor [redacted] e inscrito en el Registro de Comercio bajo el número CUARENTA Y CUATRO Libro UN MIL OCHOCIENTOS DIECISEIS del Registro de Otros Contratos Mercantiles, con fecha diecisiete de mayo de dos mil diecisiete, constando en dicho poder que el Licenciado [redacted] en su calidad de Administrador Único Propietario y representante legal de DADA DADA Y COMPAÑÍA, SOCIEDAD ANONIMA DE CAPITAL VARIABLE confirió a favor del compareciente señor Juan Carlos Flores, Poder Especial Administrativo con facultades para comparecer en instrumentos como el presente; estando en dicha escritura plenamente establecida y comprobada la existencia legal de la sociedad, lo mismo que la personería del Licenciado Guillermo Ventura Dada Peña. Y para constancia firmo y sello la presente razón notarial en San Salvador, a los veintiún días del mes de junio de dos mil dieciocho.

[redacted]

JMTELCOM
Toda una RED de Comunicaciones

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL

Unidad de Adquisiciones y Contrataciones Institucional

LIBRE GESTIÓN No. LG MTPS 12-2018

"ADQUISICION DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"

PRESENTADA POR

JMTELCOM, S.A. DE C.V.

SAN SALVADOR, 22 DE JUNIO DE 2018

[redacted]

JMTELCOM
Toda una RED de Comunicaciones

INDICE

OFERTA TÉCNICA - ECONÓMICA

	PAGINA
1. GENERALIDADES DEL OFERTANTE	001
2. DECLARACIÓN JURADA	002
3. ESPECIFICACIONES TÉCNICA	003
4. CARTA DEL FABRICANTE	024
5. CURRICULUM DEL PERSONAL TECNICO	026
6. CARTAS COMPROMISO	044
7. REFERENCIA DE CLIENTES	077
8. OFERTA ECONÓMICA	051
9. HOJAS TÉCNICAS	054

[redacted]

JMTELCOM
Toda una RED de Comunicaciones

GENERALIDADES DE LA EMPRESA

a) Nombre completo de la persona natural o jurídica que está ofertando	JMTelcom, Jesús Martinez y Asociados S.A. de C.V.
b) Nombre comercial de la empresa	JMTelcom S.A. de C.V.
c) Giro o finalidad	Otros servicios de Telecomunicaciones
d) Categoría de Contribuyente	Mediano
e) Número de NIT	[redacted]
f) Domicilio	[redacted]
g) Dirección de oficinas principales	[redacted]
h) Nombre del Representante Legal o Apoderado	Ana Margarita Flores de Martinez
i) Número de teléfono	[redacted]
j) Número de fax	[redacted]
k) Dirección de correo electrónico	[redacted]
l) Fecha de establecimiento de la empresa	09 de diciembre de 1988
m) Nombre, cargo, teléfono fijo y correo electrónico de la persona que será el contacto	[redacted]

[redacted]

[redacted]

0000001

224

En la ciudad de San Salvador, a las diez horas y quince minutos del día diecinueve de junio de dos mil dieciocho. Ante mí, [redacted] Notario, de este domicilio, comparece la Ingeniero [redacted], de [redacted] años de edad, Ingeniero [redacted] del domicilio de [redacted], Departamento de [redacted] a quien conozco portadora de su Documento Único de Identidad Número [redacted]; y Número de Identificación Tributaria: [redacted]; actuando en su calidad de Representante Legal de la Sociedad "JMTELCOM, JESUS MARTINEZ Y ASOCIADOS, SOCIEDAD ANONIMA DE CAPITAL VARIABLE", que puede abreviarse "JMTELCOM, S.A. DE C.V.", del domicilio de [redacted] de este Departamento, con Número de Identificación Tributaria: [redacted] cuya personería doy fe de ser legítima y suficiente por haber tenido a la vista: a) Testimonio de la Escritura Pública de Constitución de la referida Sociedad, otorgada en la ciudad de San Salvador, a las quince horas del día nueve de diciembre de mil novecientos ochenta y ocho, ante los oficios del Notario [redacted] inscrita en el Registro de Comercio al Número VEINTITRES del Libro SEISCIENTOS CUARENTA del Registro de Sociedades; b) Modificación del Pacto Social, otorgado en esta ciudad, a las once horas del día veintiséis de septiembre del año dos mil nueve, ante los oficios del Notario Ulises Antonio Jovel Espinoza, inscrita en el Registro de Comercio al Número [redacted] del Libro [redacted] del Registro de Sociedades de la cual aparece que reformó el domicilio, aumento de capital y se reunió en un mismo instrumento todas las cláusulas que actualmente rigen la Sociedad, constando que la naturaleza, denominación y domicilio social son como se ha expresado, que su plazo es indefinido; que dentro de su objeto social está la de otorgar actos como el presente, que la representación Judicial y Extrajudicial de la sociedad le corresponde conjunta o separadamente al Presidente y Secretario de la Junta Directiva; quienes pueden otorgar instrumentos como el presente; y c) Credencial extendida por la Secretaria de la Junta Directiva de la Sociedad Ingeniero [redacted] el día dieciséis de enero del dos mil dieciocho, en donde consta que se eligió como Presidente al Ingeniero [redacted] como Secretaria a la Ingeniero [redacted] para un período de [redacted] años, contados a partir de su inscripción en el Registro de Comercio; inscrita en el Registro de Comercio al Número VEINTICINCO del Libro [redacted]

JMTELCOM
Toda una RED de Comunicaciones

00000002

ESPECIFICACIONES TÉCNICAS

[redacted]

Cumplimiento de las Especificaciones Técnicas

SITIO PRINCIPAL Y SITIO REMOTO (SANTA ANA)				
CARACTERISTICA	DESCRIPCION	CUMPLE		OBSERVACIONES
		SI	NO	
JMTelcom, S.A. de C.V. incluye en su oferta el equipo Marca Fortinet, modelo FORTIGATE 800D-BDL, que incluye licencias y servicios por 12 meses, y cumple con las siguientes características:				
Capacidad de Usuarios	Hasta 1000	SI		El Equipo cuenta con el rendimiento suficiente para la protección de hasta 1000 usuarios
Cantidad de Equipos	Dos	SI		Se incluyen DOS equipos FortiGate 800D en la oferta económica
Configuración	Contingencia	SI		De resultar adjudicado JMTelcom realizara las configuraciones de contingencias necesarias.
Almacenamiento	240 GB mínimo	SI		Ver Hoja Técnica FORTIGATE 800D, Sección Interfaces y modulos.
Consumo de energía	Fuente redundante	SI		Ver Hoja Técnica FORTIGATE 800D, Sección Dimensiones y Energía.
Conexiones concurrentes	Mínimo 1 millón	SI		Superior característica, Ver Hoja Técnica FORTIGATE 800D, Sección Rendimiento y Capacidad del Sistema.
AV rendimiento	Mínimo 1.5 GBPS	SI		Superior característica, Ver Hoja Técnica FORTIGATE 800D, Sección Rendimiento y Capacidad del Sistema.
IPS rendimiento	Mínimo 2 GBPS	SI		Superior característica, Ver Hoja Técnica FORTIGATE 800D, Sección Rendimiento y Capacidad del Sistema.
Firewall rendimiento	Mínimo 4 GBPS	SI		Superior característica, Ver Hoja Técnica FORTIGATE 800D, Sección Rendimiento y Capacidad del Sistema.
Interfaces	Capacidad de ampliación	SI		Las 26 interfaces que tiene el modelo ofertado son de propósito genérico, por lo que pueden adaptarse a la necesidad del MTPS.
Módulos de Protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo Electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, Ipsec	SI		El equipo ofertado cuenta con todos los módulos requeridos, Ver documento FortiOS™ 6.0 Fortinet's Network Operating System, sección Especificaciones.

[redacted]

SITIO PRINCIPAL Y SITIO REMOTO (SANTA ANA)				
CARACTERISTICA	DESCRIPCION	CUMPLE		OBSERVACIONES
		SI	NO	
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.	SI		Ver documento FortiOS™ 6.0 Fortinet's Network Operating System, sección Especificaciones
VPN	1. Soporte de tuneles VPN en IPSec, VPN en SSL y VPN en PPTP 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES 4. Autenticación de certificados IKE 5. El sistema debe tener la capacidad de crear certificados locales, CA y CRL.	SI		Ver documento FortiOS™ 6.0 Fortinet's Network Operating System, sección Especificaciones.
Seguridad web	1. Bases de datos de filtrado de URL por medio de la categorización de sitios 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware 4. Filtrado de contenido activo: extensiones de archivos Flash. 5. Detección de spyware 6. Configuración de perfiles de navegación 7. Autenticación compatible con LDAP y RADIUS.	SI		Ver documento FortiOS™ 6.0 Fortinet's Network Operating System, sección Especificaciones.
Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de trafico de red 3. Balanceo de enlaces 4. Prevención de intrusos 5. Protección contra DOS. VPN punto a punto: SSL, IPSec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.	SI		Ver documento FortiOS™ 6.0 Fortinet's Network Operating System, sección Especificaciones.

[redacted]

SITIO PRINCIPAL Y SITIO REMOTO (SANTA ANA)				
CARACTERISTICA	DESCRIPCION	CUMPLE		OBSERVACIONES
		SI	NO	
Filtrado de Contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe permitir/ restringir/acceso a categorías tales como Business, Hacking, no productivas, Skyware y Malvare, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.	SI		Ver documento FortiOS™ 6.0 Fortinet's Network Operating System, sección Especificaciones.
IPS	1. Que el UTM soporte motor de IPS para la protección de ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripingg, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM	SI		Ver documento FortiOS™ 6.0 Fortinet's Network Operating System, sección Especificaciones.
Protección de Correo Electrónico	Especificar	SI		El equipo ofertado cuenta con un módulo para Protección de Correo Electrónico, Ver documento FortiOS™ 6.0 Fortinet's Network Operating System, sección Especificaciones.

[redacted]

[redacted]

[redacted]

0000007

SITIO PRINCIPAL Y SITIO REMOTO (SANTA ANA)				
CARACTERISTICA	DESCRIPCION	CUMPLE		OBSERVACIONES
		SI	NO	
Protección de redes inalámbricas	Especificar	SI		El equipo ofertado cuenta con un módulo de Protección de Redes Inalámbricas, llamado Wireless IDS. Ver documento FortiOS™ 6.0 Fortinet's Network Operating System, sección Especificaciones.
OTRAS				
Soporte Técnico	1. Instalara y configurara equipo para ponerlo en operación. 2. Dara respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparara los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestaran un equipo de características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindara soporte 24 horas al día, 7 días a la semana sin costo adicional. 5. Demostrara que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.	SI		Ver carta compromiso, detalles del Servicio de Soporte y currículo del personal técnico.
Garantía	Reemplazara en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o porque las características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.	SI		Ver carta de proceso de garantía.

[redacted]

SITIO PRINCIPAL Y SITIO REMOTO (SANTA ANA)				
CARACTERISTICA	DESCRIPCION	CUMPLE		OBSERVACIONES
		SI	NO	
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia en el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.	SI		Ver cartas de referencia
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS	SI		Ver carta compromiso

[redacted]

[redacted]

OFICINAS REGIONALES (A EXCEPCION DE SANTA ANA) Y DEPARTAMENTALES				
CARACTERISTICA	DESCRIPCION	CUMPLE		REFERENCIA
		SI	NO	
JMTelcom, S.A. de C.V. incluye en su oferta el equipo Marca Fortinet, modelo FG 61E-BDL, que incluye licencias y servicios por 12 meses, y cumple con las siguientes características:				
Capacidad de Usuarios	Hasta 100	SI		El Equipo cuenta con el rendimiento suficiente para la protección de hasta 100 usuarios
Cantidad de Equipos	Doce	SI		Se incluyen DOCE equipos FORTIGATE 61E en la oferta económica
Almacenamiento	64 GB mínimo	SI		El equipo ofertado supera esta característica. Ver Hoja Técnica Series FortiGate / FortiWiFi 60E, Sección Interfaces y módulos.
Consumo de energía	Especificar	SI		Consumo de energía promedio 11.9 y máximo14.3 W Ver Hoja Técnica Series FortiGate / FortiWiFi 60E, Sección Interfaces y módulos.
Conexiones concurrentes	Mínimo 600 K	SI		Superior característica, Ver Hoja Técnica Series FortiGate / FortiWiFi 60E, Sección Rendimiento y Capacidad del Sistema.
AV rendimiento	Mínimo 500 MBPS	NO		La marca Fortinet no considera para sus mediciones el rendimiento de AV aislado, y dicha medición se hace en escenarios más reales haciendo una mezcla de protección con el Antivirus e IPS, por lo que en valores de la hoja técnica no existe un AV Antivirus para FortiGatet, sino un Rendimiento de protección contra amenazas. Ver Hoja Técnica Series FortiGate / FortiWiFi 60E, Sección Rendimiento y Capacidad del Sistema.
IPS rendimiento	Mínimo 400 MBPS	SI		Superior característica, Ver Hoja Técnica Series FortiGate / FortiWiFi 60E, Sección Rendimiento y Capacidad del Sistema.
Firewall rendimiento	Mínimo 1.5 GBPS	SI		Superior característica, Ver Hoja Técnica Series FortiGate / FortiWiFi 60E, Sección Rendimiento y Capacidad del Sistema.
Interfaces	Capacidad de ampliación	SI		Las 10 interfaces que tiene el modelo ofertado son de propósito genérico, por lo que pueden adaptarse a la necesidad del MTPS.

[redacted]

[redacted]

OFICINAS REGIONALES (A EXCEPCION DE SANTA ANA) Y DEPARTAMENTALES				
CARACTERISTICA	DESCRIPCION	CUMPLE		REFERENCIA
		SI	NO	
Módulos de Protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo Electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, Ipsec	SI		El equipo ofertado cuenta con todos los módulos requeridos, Ver documento FortiOS™ 6.0 Fortinet's Network Operating System, sección Especificaciones.
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.	SI		Ver documento FortiOS™ 6.0 Fortinet's Network Operating System, sección Especificaciones.
VPN	1. Soporte de tuneles VPN en IPSec, VPN en SSL y VPN en PPTP 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES 4. Autenticación de certificados IKE 5. El sistema debe tener la capacidad de crear certificados locales, CA y CRL.	SI		Ver documento FortiOS™ 6.0 Fortinet's Network Operating System, sección Especificaciones.
Seguridad web	1. Bases de datos de filtrado de URL por medio de la categorización de sitios 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware 4. Filtrado de contenido activo: extensiones de archivos Flash. 5. Detección de spyware 6. Configuración de perfiles de navegación 7. Autenticación compatible con LDAP y RADIUS.	SI		Ver documento FortiOS™ 6.0 Fortinet's Network Operating System, sección Especificaciones.

[redacted]

[redacted]

265

OFICINAS REGIONALES (A EXCEPCION DE SANTA ANA) Y DEPARTAMENTALES				
CARACTERISTICA	DESCRIPCION	CUMPLE		REFERENCIA
		SI	NO	
Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de trafico de red 3. Balanceo de enlaces 4. Prevención de intrusos 5. Protección contra DOS. VPN punto a punto: SSL, IPSec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.	SI		Ver documento FortiOS™ 6.0 Fortinet's Network Operating System, sección Especificaciones.
Filtrado de Contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe permitir/ restringir/acceso a categorías tales como Business, Hacking, no productivas, Skyware y Malvare, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.	SI		Ver documento FortiOS™ 6.0 Fortinet's Network Operating System, sección Especificaciones.
IPS	1. Que el UTM soporte motor de IPS para la protección de ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3,RPC,SNMP,TFTP,NNTP, NETBIOS.	SI		Ver documento FortiOS™ 6.0 Fortinet's Network Operating System, sección Especificaciones.

[redacted]

OFICINAS REGIONALES (A EXCEPCION DE SANTA ANA) Y DEPARTAMENTALES				
CARACTERISTICA	DESCRIPCION	CUMPLE		REFERENCIA
		SI	NO	
	4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripingg, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM			
Protección de Correo Electrónico	Especificar	SI		El equipo ofertado cuenta con un módulo para Protección de Correo Electrónico, Ver documento FortiOS™ 6.0 Fortinet's Network Operating System, sección Especificaciones.
Protección de redes inalámbricas	Especificar	SI		El equipo ofertado cuenta con un módulo de Protección de Redes Inalámbricas, llamado Wireless IDS. Ver documento FortiOS™ 6.0 Fortinet's Network Operating System, sección Especificaciones.
OTRAS				
Soporte Técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dara respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparara los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestaran un equipo de características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas al día, 7 días a la semana sin costo adicional. 5. Demostrara que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.	SI		Ver carta compromiso, detalles del Servicio de Soporte, y currículo del personal técnico.

[redacted]

[redacted]

OFICINAS REGIONALES (A EXCEPCION DE SANTA ANA) Y DEPARTAMENTALES				
CARACTERISTICA	DESCRIPCION	CUMPLE		REFERENCIA
		SI	NO	
Garantía	Reemplazara en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o porque las características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.	SI		Ver detalles de Servicio de Soporte.
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia en el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.	SI		Ver cartas de referencia
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.	SI		Ver carta compromiso

[redacted]

[redacted]

CENTRO DE RECREACION Y ARCHIVO GENERAL				
CARACTERISTICA	DESCRIPCION	CUMPLE		REFERENCIA
		SI	NO	
JMTelcom, S.A. de C.V. incluye en su oferta el equipo Marca Fortinet, modelo FG 61E-BDL, que incluye licencias y servicios por 12 meses, y cumple con las siguientes características:				
Capacidad de Usuarios	Hasta 15	SI		El Equipo cuenta con el rendimiento suficiente para la protección de hasta 15 usuarios
Cantidad de Equipos	CINCO	SI		Se incluyen CINCO equipos FORTIGATE 61E en la oferta económica
Almacenamiento	64 GB mínimo	SI		El equipo ofertado supera esta característica. Ver Hoja Técnica Series FortiGate / FortiWiFi 60E, Sección Interfaces y módulos.
Consumo de energía	Especificar	SI		Consumo de energía promedio 11.9 y máximo 14.3 W. Ver Hoja Técnica Series FortiGate / FortiWiFi 60E, Sección Interfaces y módulos.
Conexiones concurrentes	Mínimo 600 K	SI		Superior característica, Ver Hoja Técnica Series FortiGate / FortiWiFi 60E, Sección Rendimiento y Capacidad del Sistema.
AV rendimiento	Mínimo 400 MBPS		NO	La marca Fortinet no considera para sus mediciones el rendimiento de AV aislado, y dicha medición se hace en escenarios más reales haciendo una mezcla de protección con el Antivirus e IPS, por lo que en valores de la hoja técnica no existe un rendimiento de AV para FortiGate, sino un Rendimiento de protección contra amenazas. Ver Hoja Técnica Series FortiGate / FortiWiFi 60E, Sección Rendimiento y Capacidad del Sistema.
IPS rendimiento	Mínimo 300 MBPS	SI		Superior característica, Ver Hoja Técnica Series FortiGate / FortiWiFi 60E, Sección Rendimiento y Capacidad del Sistema.
Firewall rendimiento	Mínimo 900 MBPS	SI		Superior característica, Ver Hoja Técnica Series FortiGate / FortiWiFi 60E, Sección Rendimiento y Capacidad del Sistema.
Interfaces	Capacidad de ampliación	SI		Las 10 interfaces que tiene el modelo ofertado son de propósito genérico, por lo que pueden adaptarse a la necesidad del MTPS.

[redacted]

CENTRO DE RECREACION Y ARCHIVO GENERAL				
CARACTERISTICA	DESCRIPCION	CUMPLE		REFERENCIA
		SI	NO	
Módulos de Protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo Electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, Ipsec	SI		El equipo ofertado cuenta con todos los módulos requeridos, Ver documento FortiOS™ 6.0 Fortinet's Network Operating System, sección Especificaciones,
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.	SI		Ver documento FortiOS™ 6.0 Fortinet's Network Operating System, sección Especificaciones,
VPN	1. Soporte de tuneles VPN en IPSec, VPN en SSL y VPN en PPTP 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES 4. Autenticación de certificados IKE 5. El sistema debe tener la capacidad de crear certificados locales, CA y CRL.	SI		Ver documento FortiOS™ 6.0 Fortinet's Network Operating System, sección Especificaciones
Seguridad web	1. Bases de datos de filtrado de URL por medio de la categorización de sitios 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware 4. Filtrado de contenido activo: extensiones de archivos Flash. 5. Detección de spyware 6. Configuración de perfiles de navegación 7. Autenticación compatible con LDAP y RADIUS.	SI		Ver documento FortiOS™ 6.0 Fortinet's Network Operating System, sección Especificaciones.

[redacted]

[redacted]

260

CENTRO DE RECREACION Y ARCHIVO GENERAL				
CARACTERISTICA	DESCRIPCION	CUMPLE		REFERENCIA
		SI	NO	
Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de trafico de red 3. Balanceo de enlaces 4. Prevención de intrusos 5. Protección contra DOS. VPN punto a punto: SSL, IPSec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.	SI		Ver documento FortiOS™ 6.0 Fortinet's Network Operating System, sección Especificaciones,
Filtrado de Contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe permitir/ restringir/acceso a categorías tales como Business, Hacking, no productivas, Skyware y Malvare, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.	SI		Ver documento FortiOS™ 6.0 Fortinet's Network Operating System, sección Especificaciones.
IPS	1. Que el UTM soporte motor de IPS para la protección de ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3,RPC,SNMP,TFTP,NNTP, NETBIOS.	SI		Ver documento FortiOS™ 6.0 Fortinet's Network Operating System, sección Especificaciones,

[redacted]

[redacted]

CENTRO DE RECREACION Y ARCHIVO GENERAL				
CARACTERISTICA	DESCRIPCION	CUMPLE		REFERENCIA
		SI	NO	
	4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripingg, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM			
Protección de Correo Electrónico	Especificar	SI		El equipo ofertado cuenta con un módulo para Protección de Correo Electrónico, Ver documento FortiOS™ 6.0 Fortinet's Network Operating System, sección Especificaciones, folio xxxx.
Protección de redes inalámbricas	Especificar	SI		El equipo ofertado cuenta con un módulo de Protección de Redes Inalámbricas, llamado Wireless IDS. Ver documento FortiOS™ 6.0 Fortinet's Network Operating System, sección Especificaciones.
OTRAS				
Soporte Técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dara respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparara los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestaran un equipo de características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas al día, 7 días a la semana sin costo adicional. 5. Demostrara que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.	SI		Ver carta compromiso, detalles del Servicio de Soporte y Currículo del personal técnico.

[redacted]

[redacted]

CENTRO DE RECREACION Y ARCHIVO GENERAL				
CARACTERISTICA	DESCRIPCION	CUMPLE		REFERENCIA
		SI	NO	
Garantía	Reemplazara en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o porque las características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.	SI		Ver detalles de Servicio de Soporte
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia en el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.	SI		Ver cartas de referencia
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.	SI		Ver carta compromiso

[redacted]

[redacted]

JMTELCOM
Toda una RED de Comunicaciones

SERVICIOS TECNICOS 24X7

Cobertura de Lunes a Domingo a cualquier hora

Al adquirir un contrato anual de Soporte su equipo cuenta con:

A. Soporte técnico local
B. Proceso administrativo de RMA[1]
C. Garantía

A- SOPORTE TECNICO LOCAL

Beneficios

- ✓ Soporte Técnico personalizado las 24 horas del día los 365 días del año.
- ✓ Acceso al soporte vía web, telefónico o por correo electrónico.
- ✓ Solución de problemas más comunes relacionados con sus equipos de comunicación Fortinet: caídas de sistemas, errores o fallas en configuraciones, puestas en marcha, actualizaciones, etc.
- ✓ Actualización de Firmware de los equipos.
- ✓ Priorizar (determinar la urgencia) y categorizar (evaluar los riesgos) en cada caso.
- ✓ Escalar a un soporte de segundo o tercer nivel si fuera necesario.
- ✓ Estrategias de planificaciones en la resolución de problemas para minimizar las interrupciones del servicio y/u optimizar su estructura de comunicación para desarrollar el máximo potencial.
- ✓ 4 horas de mensuales dedicadas a mantenimiento de la infraestructura de la FGR.

Servicio de soporte preventivo y correctivo incluye:

- Visita en sitio bajo las siguientes condiciones:
  - Que el equipo no encienda, ninguna luz indicadora este activa.
  - Que el equipo esté totalmente inaccesible, encienda, pero no funciona.
  - Pérdida de Password.
  - Si el equipo no tiene acceso remoto y no funcione el apoyo telefónico.
  - Por desperfectos de fábrica según criterio del ingeniero de servicio.
  - Restaurar back up de configuración en los equipos.
  - Otros que el ingeniero de servicio considere necesario.

[1] RMA: Return Material Autorization (Autorización de Retorno de Equipo)

[redacted]

- En caso de falla de hardware:

  - Revisión de equipo.
  - Evaluación y diagnóstico de la falla del equipo.
  - Retirar el equipo dañado.
  - Instalar un equipo de similares características durante el periodo de diagnóstico de la falla.
  - Instalación del back up de la configuración del equipo prestado.
  - Instalar el equipo de remplazo e instalar el back up correspondiente.

- En caso de falla de sistema operativo:

- Revisión del sistema de forma periódica según el tiempo de vida del proyecto.
  - ***Diaria** durante 15 días mientras se está realizando la implementación (De forma remota o en sitio de ser necesario)
  - ***Quincenal** posterior a la implementación (De forma Remota).
- Monitorización permanente (JMTELCOM cuenta con sistemas de monitoreo que permiten garantizar la observación del comportamiento de la plataforma a nivel de comunicación.)

Acceso al soporte

a) Sitio de Gestión de JMTelcom

Levantar un ticket definiendo la prioridad del mismo en el portal de soporte: http://support.mayabits.com, en donde se le dará un número de caso y será asignado un Ingeniero de Servicio el cual se comunicará con usted y le dará seguimiento al problema.

b) Atención Telefónica

Marcar al teléfono del Call Center 2246-6046, donde contestará nuestro personal de HelpDesk, quien determinará la criticidad del problema y abrirá un ticket de soporte donde se le asignará un número para dicho ticket. Posteriormente un Ingeniero de Servicio se comunicará con usted y le dará seguimiento al problema.

c) Atención por Correo

Enviar un correo electrónico a la cuenta support@mayabits.com donde nuestro personal de HelpDesk determinará la criticidad del problema y abrirá un ticket, será asignado a un Ingeniero de Servicio el cual se comunicará con usted y le dará seguimiento al problema reportado.'

d) Conexión Remota

Se requiere que el cliente brinde un acceso al equipo para poder realizar las configuraciones vía remota ya sea de manera directa o por medio de una conexión remota a la máquina del cliente. El acceso podría ser temporal o permanente, siempre y cuando al momento de realizar alguna configuración esté activa con su respectivo usuario y password.

[redacted]

[redacted]

Tipos de incidentes y tiempos de respuesta – PLAN 24x7

Tipo de Incidencia	Estatus del Sistema	Impacto en la Productividad	Tiempos de Respuesta
Crítica	Sistema fuera de servicio	Alto	1-3 horas
Media	Problemas intermitentes No causa interrupción inmediata de labores.	Impacto a largo plazo	3-6 horas
Leve	No hay impacto en el sistema. Actualizaciones, preguntas, instalaciones o nuevas configuraciones.	No hay impacto	6-8 horas

Nota. Los tiempos aplican para zona Metropolitana, y para zonas occidental y oriental los tiempos de respuesta en sitio sería de 4 - 8 horas máximo.

- **Configuraciones Nivel 1, 2 y 3:**

	**Nivel 1** Configuraciones Básicas	• Creación y configuración de: o Objetos, o Direcciones o Usuarios, o Cuentas, o Perfiles, o Creación de políticas,
	**Nivel 2** Configuraciones Intermedias	• Autenticación, • Encripción, • Interpretación de logs, • Troubleshooting básico,
	**Nivel 3** Configuraciones Avanzadas	• Troubleshooting avanzado, • Diagnóstico de problemas, • Captura de tráfico.

B- **PROCESO ADMINISTRATIVO DE RMA**

Al contar con un contrato de soporte técnico o de administración de equipo, si fuera necesario, JMTelcom se encargará del proceso administrativo y costos relacionados al trámite de RMA para el cambio del equipo dañado, y pondrá a disposición del cliente un equipo de iguales o similares características (en calidad de préstamo) para garantizar la continuidad de sus procesos y de la seguridad de su red mientras el nuevo equipo es instalado.

[redacted]

JMTELCOM
Toda una RED de Comunicaciones

C- SERVICIO ADMINISTRATIVO PARA CAMBIO POR GARANTIA

Este servicio aplica únicamente para aquellos equipos vendidos por JMTELCOM y que posean garantía de fábrica y corresponde a todas las actividades necesarias para gestionar el reemplazo o reparación del equipo que presenta fallas, las cuales se describen a continuación:

- Gestionar con fábrica el RMA correspondiente.
- Instalar un equipo de similares características en calidad de préstamo, mientras se solventa el RMA con fábrica
- Realizar los trámites para envío del equipo con RMA.
- Pago de Flete, seguro y tramite aduanal por JMTELCOM como parte del Servicio
- Seguimiento al RMA.
- Realizar trámites de recepción del equipo enviado por fábrica.
- Instalación del equipo reparado o sustituido por fábrica.

RMA:

1. Return Material Autorización (Autorización de Retorno de Equipo) No incluye flete, seguro y trámite aduanal por el fabricante.

LIMITACIONES DEL SERVICIO:

Entendiéndose por limitaciones a cualquier servicio que no corresponda con lo estipulado en este documento, tales como: adiciones o modificaciones a nivel de hardware, adiciones o modificaciones a nivel de equipos o aplicaciones periféricas proveídos o no por JMTELCOM configuraciones o nuevos cambios en los enlaces de internet y/o datos, incluyendo aparatos telefónicos, computadoras, Software, etc.

CASOS FORTUITOS O FUERZA MAYOR:

JMTELCOM no tendrá responsabilidad de reparar los equipos que hayan sido dañados o no funcionen por motivos de fuerza mayor o caso fortuito, como:

- Fenómenos naturales tales como: inundaciones, terremotos, descargas eléctricas, humedad.
- Accidentes tales como: fuego, explosiones, fallas en la corriente eléctrica, pérdidas.
- Actos de los hombres como: sabotaje, vandalismo, robo.
- Actos u omisiones tales como: negligencia o mal uso de los equipos.
- Instalaciones, reparaciones o modificaciones no efectuadas por JMTELCOM
- Fenómenos radioeléctricos como: interferencias, ruidos, propagación.
- Cualquier otro caso que no se mencione en el presente documento pero que encaje en el concepto de fuerza mayor o caso fortuito.
- Daños debido a condiciones ambientales, no apropiadas para el equipo: Polvo, Plagas, Insectos, Humedad, Etc.

[redacted]

[redacted]

JMTELCOM
Toda una RED de Comunicaciones

CARTA DEL FABRICANTE

[redacted]

[redacted]

Confirmación de Distribuidor Autorizado

Fecha: 06/20/2018

Señores.
MINISTERIO DE TRABAJO Y PREVISION SOCIAL
Presente.

Referencia: Libre Gestión LG MTPS 12-2018: "ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"

Fortinet, Inc. opera a través de un canal de distribuidores y revendedores independientes. Por lo tanto, Fortinet confirma por la presente que: Jesus Martínez y Asociados S.A. de C.V.

Quien tiene como dirección:
[redacted]

Es un integrador autorizado a nivel Platinum de aquí en adelante "FortiPartner" y actualmente está autorizado para revender los productos de Fortinet en El Salvador, Guatemala and Honduras.

Este certificado se emite a partir de la fecha indicada anteriormente, y es válido por 180 días a partir de esta fecha.

Siempre que el FortiPartner identificado anteriormente compre los servicios de soporte y estos hayan sido registrados y contratados con Fortinet, Fortinet está de acuerdo y se compromete a proporcionar los soportes aplicables a los términos del contrato de soporte de Fortinet disponible en https://support.fortinet.com. La garantía de equipos Fortinet se limita a las garantías del fabricante las cuales están ubicadas en el sitio de web, http://www.fortinet.com/doc/legal/EULA.pdf.

Este Certificado se da a condición de que el FortiPartner mantenga su contrato vigente con Fortinet y que siga las políticas y lineamientos de Fortinet. El programa de partners de Fortinet y sus lineamientos están disponibles en http://www.fortinet.com/partners/partner_program/fpp.html. No obstante que son integradores autorizados, los FortiPartner no representan a Fortinet y por consiguiente no pueden hacer declaraciones a nombre de Fortinet.

[redacted]

Samantha Symonds
Vicepresidente Legal y de Compliance, Americas

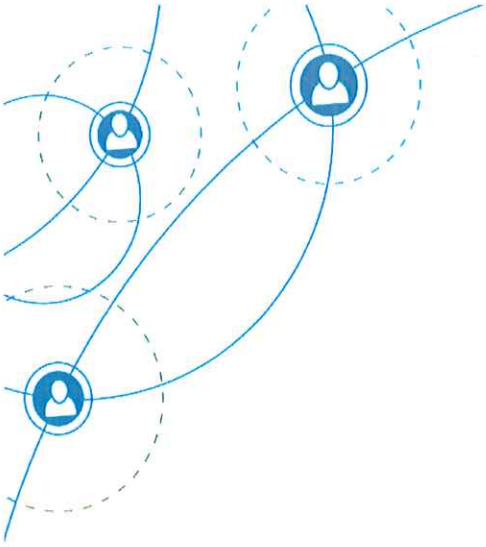
[redacted]

[redacted]

[redacted]

[redacted]

00000025



JMTELCOM
Toda una RED de Comunicaciones

25L

CURRICULUM DEL PERSONAL TÉCNICO

JMTELCOM
Toda una RED de Comunicaciones

San Salvador, 22 de junio de 2018

Señores
MINISTERIO DE TABAJO Y PREVISION SOCIAL
Presente.

Referencia: Libre Gestión LG MTPS 12-2018: **"Adquisición de 19 equipos de seguridad perimetral con licencias"**

Estimados Señores:

Por este medio les informamos que JMTELCOM, S.A. de C.V. con el propósito de brindar mayor calidad y eficiencia a nuestros clientes en cuanto a Servicios de Soporte Técnico Preventivo y Correctivo se refiere, toma a bien el surgimiento de nuestra División de Ingeniería Especializada en Soluciones de Seguridad de Redes y Networking denominada MAYA BITS, S.A. de C.V., la cual cuenta con toda la experiencia y respaldo de JMTelcom con 29 años en el mercado de la Tecnología, razón por la cual anexamos la planilla de Maya Bits del personal de Soporte Técnico que establece la relación permanente del mismo.

Atentamente,

[redacted]

Representante Legal
JMTelcom S.A de C.V.

[redacted]

00000027

JMTELCOM
Toda una RED de Comunicaciones

CURRICULUM DEL PERSONAL TECNICO QUE PROPORCIONARA SOPORTE Y MANTENIMIENTO LOCAL DURANTE LA VIGENCIA DEL CONTRATO

Nombre:	[redacted]		
Profesión:	Ingeniero en [redacted]		
Años de trabajo en la empresa:	[redacted]ños	**Años de experiencia en soluciones similares a la ofertada**	[redacted]años
Cargo en la empresa:	[redacted]		

Educación

INSTITUCION	TITULO OBTENIDO	FECHA
Universidad Don Bosco	Ingeniero en Electrónica	2005
BlueCoat	Blue Coat Certified Proxy Administrator, v.3.2.1 +v.3.3.1	Mayo 2009
Motorola	Curso Técnico Canopy & OFDM	Mayo 2006
BlueCoat	Certified Pre-Sales Systems Engineers Boot-Camp	Agosto 2009
DLink	Certificación DBC	Mayo 2007
DLink	Certificación DBCex	Mayo 2007
Fortinet	Fortigate Multi-Threat Security System I – Administration and Content Inspection	Junio 2007
Fortinet	Fortigate Multi-Threat Security System II – Secured Network Deployment & Virtual Private Networks	Junio 2007
RedLine	Certificate of Attendance RedLine's AN-80i product training	Febrero 2008
Extreme Networks	ECF-200/5 Extreme Configuration Fundamentals	Abril 2008
Extreme Networks	Extreme Networks Associate	Abril 2008
March Networks	Aplicaciones Técnicas de NVR 5.5	Febrero 2010
Fortinet	Fortinet Certified Network Security Administrator (V4.X)	Marzo 2011
BlueCoat	Certified Partner SE-Acceleration	Diciembre 2011
BlueCoat	Certified Partner SE- Security	Marzo 2012
Fortinet	Fortinet Certified Network Security Professional (V4.X)	Marzo 2012
Fortinet	Network Security Expert 4, Security Professional	Marzo 2012
Fortinet	Reconocimiento por su destacada participación en el entrenamiento Xtreme Team Engineering- PANAMÁ	Octubre 2014
Fortinet	Reconocimiento por su destacada participación en el entrenamiento Xtreme Team Engineering- CANCUN	Octubre 2015
Cambium Networks	Certificación Técnica sobre línea de Productos	Enero 2016
Fortinet	Network Security Expert 1, Network Security Associate	Julio 2017
Fortinet	Network Security Expert 2, Network Security Associate	Julio 2017
Fortinet	Network Security Expert 3, Network Security Associate	Julio 2017
Fortinet	Network Security Expert 4, Network Security Professional	Agosto 2017
Fortinet	Fortimail Specialist	Octubre 2017
Fortinet	Network Security Expert 5, Network Security Analyst	Agosto 2017
Fortinet	FortiADC, Aplication Delivery Specialist	Diciembre 2017

[redacted]

[redacted]

JMTELCOM
Toda una RED de Comunicaciones

Experiencia Profesional

Empresa	Fecha	Cargo	Función
Maya Bits, S.A. de C.V.	Agosto 2012 a la fecha.	Jefe de Tecnologías Avanzadas	Soporte del Área Comercial y Técnica.
JMTelcom S.A de C.V.	Diciembre 2005 a Agosto 2012.	Ingeniero de Soporte Senior	Soporte del Área Comercial y Técnica.
Asociación de Radios y programas participativos de El Salvador	Marzo de 2005- Noviembre 2005	Técnico de Mantenimiento	Servicio de Soporte Técnico en Reparación de transmisores

Certificación
Yo, el abajo firmante, certifico que, según mi anteceder, estos datos describen correctamente mi persona, mis calificaciones y mi experiencia.

[redacted]

[redacted]

[redacted]

FORTINET

NSE CERTIFIED

This certifies that

Carlos Zelaya

has successfully completed

NSE 5 Network Security Analyst

DATE: November 17, 2017

[redacted]
CHIEF EXECUTIVE OFFICER
FORTINET

[redacted]
CHIEF TECHNOLOGY OFFICER
FORTINET

FORTINET
NSE Certification Program

00000030

JMTELCOM
Toda una RED de Comunicaciones

CURRICULUM DEL PERSONAL TECNICO QUE PROPORCIONARA SOPORTE Y MANTENIMIENTO LOCAL DURANTE LA VIGENCIA DEL CONTRATO

Nombre:	[redacted]		
Profesión:	Bachiller General		
Años de trabajo en la empresa:	[redacted]os	**Años de experiencia en soluciones similares a la ofertada**	[redacted]años
Cargo en la empresa:	[redacted]		

Educación

INSTITUCION	TITULO OBTENIDO	FECHA
Universidad Politécnica de El Salvador	Estudiante de 5to año	2000 a la fecha
Liceo Salvadoreño	Bachiller General	1997
Blue Coat	Blue Coat Certified Proxy Administrator	Noviembre 2011
Fortinet	Fortinet Certified Network Security Administrator	Diciembre 2009
Fortinet	Fortinet Certified Network Security Professional (V4.X)	Marzo 2012
Fortinet	Reconocimiento por su destacada participación en el entrenamiento Xtreme Team Engineering- CANCUN	Octubre 2015
Fortinet	Certificación de Ingeniería en Network Security Expert - NSE6 advanced security technologies	Diciembre 2016
Fortinet	Reconocimiento por su destacada participación en el entrenamiento Xtreme Team Engineering- CANCUN	Octubre 2016
Fortinet	Certificación de Ingeniería en Network Security Expert – NSE4 Network Security Professional	Agosto 2017

Experiencia Profesional

Empresa	Fecha	Cargo	Función
Maya Bits, S.A. de C.V.	Noviembre 2012 a la fecha.	Jefe de Ingeniería y Soporte	Soporte del Área Comercial y Técnica.
JMTelcom S.A de C.V.	Diciembre 2005 a Noviembre 2012.	Ingeniero de Soporte Senior	Soporte del Área Comercial y Técnica.
Sistemas Aplicativos de El Salvador S.A	Junio 2005 –Agosto 2009	Pre-Venta	Soporte Técnico y pre-ventas en el área de seguridad de información en proyectos empresariales a nivel corporativo
Next Genesis Technologies S.A. de C.V.	Febrero 2003- Junio 2005	Experto en Seguridad Informática	Instalaciones de Firewalls, IPS, AntiVirus Corporativos, Filtrados de contenido, Proxys, Antispam, UTM. Etc.

Certificación

Yo, el abajo firmante, certifico que, según mi anteceder, estos datos describen correctamente mi persona, mis calificaciones y mi experiencia.

[redacted]

[redacted]

[redacted]

FORTINET
FAST. SECURE. GLOBAL.

NSE Certified

This certifies that

Alvaro Mancia

has successfully certified for

NSE 6 Security Specialist

6/12/2016

[redacted]
CHIEF EXECUTIVE OFFICER
FORTINET

[redacted]
CHIEF TECHNOLOGY OFFICER
FORTINET

FORTINET
Network Security Expert Program

00000032

JMTELCOM
Toda una RED de Comunicaciones

CURRICULUM DEL PERSONAL TECNICO QUE PROPORCIONARA SOPORTE Y MANTENIMIENTO LOCAL DURANTE LA VIGENCIA DEL CONTRATO

Nombre:	[redacted]		
Profesión:	[redacted]		
Años de trabajo en la empresa:	[redacted]ño	**Años de experiencia en soluciones similares a la ofertada**	[redacted]año
Cargo en la empresa:	[redacted]		

Educación

INSTITUCION	TITULO OBTENIDO	FECHA
Universidad Don Bosco	Ingeniero en Telecomunicaciones	2015
Colegio Español Padre Arrupe	Bachiller Técnico Industrial Electrónica	2009
Fortinet	Fortinet Certified Network Security Specialist (NSE6)	Junio 2016
Fortinet	Fortinet Certified Network Security Architect (NSE7)	Noviembre 2017

Experiencia Profesional

Empresa	Fecha	Cargo	Función
Maya Bits, S.A. de C.V.	Enero 2016 a la fecha.	Ingeniero de Soporte	Soporte del Área Técnica.
Aldeas Infantiles SOS	Marzo 2015 a Diciembre 2015.	Asistente TIC & MEL	Soporte Técnico del Área TIC y de Monitoreo y Evaluación

Certificación

Yo, el abajo firmante, certifico que, según mi anteceder, estos datos describen correctamente mi persona, mis calificaciones y mi experiencia.

[redacted]

[redacted]

FORTINET

NSE CERTIFIED

This certifies that

Herbert Zapata

has successfully completed

NSE 7 Network Security Architect

DATE: November 7, 2017

CERTIFICATE NUMBER: TMExi4WGZN

[redacted]

FICER
FORTINET

[redacted]

CHIEF TECHNOLOGY OFFICER
FORTINET

FORTINET
NSE Certification Program

00000034

243

JMTELCOM
Toda una RED de Comunicaciones

CURRICULUM DEL PERSONAL TECNICO QUE PROPORCIONARA SOPORTE Y MANTENIMIENTO LOCAL DURANTE LA VIGENCIA DEL CONTRATO

Nombre:	[redacted]		
Profesión:	Ingeniero en Telecomunicaciones.		
Años de trabajo en la empresa:	3 años	**Años de experiencia en soluciones similares a la ofertada**	4 años
Cargo en la empresa:	[redacted]		

Educación

INSTITUCION	TITULO OBTENIDO	FECHA
Universidad Don Bosco	Ingeniero en telecomunicaciones.	2012
Colegio Anglo Americano	Bachiller general	2005
Fortinet	Fortinet Certified Network Security Specialist (NSE6)	Junio 2016
Fortinet	Fortinet Certified Network Security Architect (NSE7)	Noviembre 2017

Experiencia Profesional

Empresa	Fecha	Cargo	Función
Maya Bits, S.A. de C.V.	Junio 2014 a la fecha.	Ingeniero de soporte nivel 2	Soporte del Área Técnica.
Disatel	Junio 2013 a junio 2014.	Helpdesk	Administración de firewall y soporte a usuarios finales.

Certificación

Yo, el abajo firmante, certifico que, según mi anteceder, estos datos describen correctamente mi persona, mis calificaciones y mi experiencia.

[redacted]

[redacted]

FORTINET

NSE CERTIFIED

This certifies that

Fernando Díaz

has successfully completed

NSE 7 Network Security Architect

DATE: November 6, 2017

CERTIFICATE NUMBER: fjXNJw9foA

[redacted]

CHIEF EXECUTIVE OFFICER
FORTINET

[redacted]

CHIEF TECHNOLOGY OFFICER
FORTINET

FORTINET
NSE Certification Program

[redacted]

0000036

241

JMTELCOM
Toda una RED de Comunicaciones

2H0

CURRICULUM DEL PERSONAL TECNICO QUE PROPORCIONARA SOPORTE Y MANTENIMIENTO LOCAL DURANTE LA VIGENCIA DEL CONTRATO

Nombre:	[redacted]		
Profesión:	[redacted]		
Años de trabajo en la empresa:	[redacted]	**Años de experiencia en soluciones similares a la ofertada**	[redacted]
Cargo en la empresa:	[redacted]		

Educación

INSTITUCION	TITULO OBTENIDO	FECHA
Universidad Don Bosco	Ingeniero en Telecomunicaciones	Noviembre 2013
Colegio de España Padre Arrupe	Bachiller Técnico Industrial (opción Electrónica)	2007
Fortinet	Network Security Expert (NSE1)	Enero 2016
Fortinet	Network Security Expert (NSE2-3)	Marzo 2016
Fortinet	Network Security Expert (NSE4)	Abril 2016
Fortinet	Fortinet Certified Network Security Architect (NSE7)	Mayo 2018
Cambium Networks	Certificación Técnica sobre línea de Productos	Enero 2016

Experiencia Profesional

Empresa	Fecha	Cargo	Función
Maya Bits, S.A. de C.V.	Julio 2015 a la fecha.	Ingeniero de Soporte	Soporte Remoto y en campo con soluciones de Networking
JMTelcom S.A de C.V.	Enero 2014 a Julio 2015.	Ingeniero de Soporte IT	Soporte del Área Comercial y Técnica.
ITS INFOCOM	Septiembre 2013 – Diciembre 2013	Técnico Nivel 1	Soporte Técnico remoto en instalaciones y documentación proyecto de integración 2G/3G para la empresa Claro El Salvador.

Certificación

Yo, el abajo firmante, certifico que, según mi anteceder, estos datos describen correctamente mi persona, mis calificaciones y mi experiencia.

[redacted]

[redacted]

[redacted]

00000037

FORTINET

NSE CERTIFIED

This certifies that

Amadeo Alvarez

has successfully completed

NSE 7 Network Security Architect

DATE: May 2, 2018

CERTIFICATE NUMBER: MAVoiVyBrF

[redacted]

CHIEF EXECUTIVE OFFICER
FORTINET

[redacted]

CHIEF TECHNOLOGY OFFICER
FORTINET

FORTINET
NSE Certification Program

[redacted]

00000038

239

JMTELCOM
Toda una RED de Comunicaciones

CURRICULUM DEL PERSONAL TECNICO QUE PROPORCIONARA SOPORTE Y MANTENIMIENTO LOCAL DURANTE LA VIGENCIA DEL CONTRATO

Nombre:	[redacted]		
Profesión:	[redacted]		
Años de trabajo en la empresa:	[redacted]	**Años de experiencia en soluciones similares a la ofertada**	[redacted]
Cargo en la empresa:	[redacted]		

Educación

INSTITUCION	TITULO OBTENIDO	FECHA
Mile2	Certified Penetration Testing Engineer	2018
Universidad Francisco Gavidia	Estudiante de 3to año	2016 a la fecha
Fortinet	Fortinet Certified Network Security Specialist (NSE6)	Junio 2016
Cambium Networks	Certificación Técnica sobre línea de Productos	Enero 2016
Instituto Técnico Ricaldone	Bachiller Técnico Industrial Electromecánica	2008

Experiencia Profesional

Empresa	Fecha	Cargo	Función
Maya Bits, S.A. de C.V.	Enero 2016 a la fecha.	Técnico de Soporte	Soporte del Área Técnica.
JMTelcom S.A de C.V.	Octubre 2009 a Diciembre 2015.	Técnico de Soporte	Instalación y soporte del Área Técnica

Certificación

Yo, el abajo firmante, certifico que, según mi anteceder, estos datos describen correctamente mi persona, mis calificaciones y mi experiencia.

[redacted]

[redacted]

FORTINET
FAST. SECURE. GLOBAL.

NSE Certified

This certifies that

Bryan Quezada

has successfully certified for

NSE 6 Security Specialist

6/26/2016

[redacted]

CHIEF EXECUTIVE OFFICER
FORTINET

[redacted]

CHIEF TECHNOLOGY OFFICER
FORTINET

FORTINET
Network Security Expert Program

[redacted]

0000040

232

JMTELCOM
Toda una RED de Comunicaciones

236

CURRICULUM DEL PERSONAL TECNICO QUE PROPORCIONARA SOPORTE Y MANTENIMIENTO LOCAL DURANTE LA VIGENCIA DEL CONTRATO

Nombre:	[redacted]		
Profesión:	[redacted]		
Años de trabajo en la empresa:	[redacted]	**Años de experiencia en servicios similares a la ofertada**	[redacted]
Cargo en la empresa:	[redacted]		

Educación

INSTITUCION	TITULO OBTENIDO	FECHA
Fortinet	Network Security Expert (NSE1, NSE2, NSE3 y NSE4) (certificación)	2016 -2017
VIDYO	Vidyo Certified Deployment & Support Engineer (VC-DSE) (certificación)	2016
INSAFORM	Curso de Preparación para Certificación de Ethical Hacking	2016
Fortinet	Fortinet Certified Network Security Professional (certificación)	2015
Ubiquiti	Enterprise Wireless Admin (UEWA) (certificación)	2014
Ubiquiti	Broadband Wireless Admin (UBWA) (certificación)	2014
Fortinet	Fortinet Certified Network Security Administrator (certificación)	2014
Universidad Don Bosco	Técnico en Computación	2012
Cisco Networking Academy Universidad Don Bosco	CCNA1, CCNA2, CCNA3 y CCNA4	2009-2010
Surtielectric Energía	Seminario: "Instalación de cableado estructurado y bandeja porta cable"	2009
Universidad Don Bosco	Curso Administración GNU/Linux	2009
EDUSYSTEMS, Honduras	Curso de Mantenimiento y configuración de PC e Instalación de Redes y comunicaciones.	2008
Colegio Génesis	Bachillerato General	2002

[redacted]

JMTELCOM
Toda una RED de Comunicaciones

Experiencia Profesional

Empresa	Fecha	Cargo	Función
Maya Bits, S.A. de C.V.	Febrero 2014 a la fecha	Técnico de Soporte	Soporte del Área Comercial y Técnica.
Universidad Don Bosco	Febrero 2014 – junio 2013	Docente hora clase	Docente de Materia Redes de Área Amplia y Redes de Área local
Bellmart S.A de C.V.	Diciembre 2012 a febrero 2014	Encargado de informática	Garantizar el correcto funcionamiento de equipos y sistemas informáticos, apoyo a usuarios, backup y restauración de Información.
Ministerio de Trabajo y Previsión Social	Abril 2012 – Diciembre 2012	Administrador de red y Seguridad de red	Administrar equipos de Comunicación y seguridad de red, control de accesos de usuario, administración de servicios de red, monitoreo de enlaces de Comunicación y VPN
Servintegra – proyecto **Claro**	Septiembre 2011– Febrero - 2012	Analista de sistemas	Administrador de Mediación e Interconexión de Claro Costa Rica. Administrar las aplicaciones encargadas de la Mediación entre las centrales de comunicación de: (GSM,MMS,GPRS y SMS) y el sistema de Facturación para Claro Costa Rica. Administrador de Aplicación para gestionar la Interconexión de Claro Costa Rica con otros operadores.
Proyecto Cumple y Gana "Ministerio de Trabajo"	Abril 2011 – Septiembre 2011	Técnico de soporte	Soporte a equipos y usuarios del Ministerio de Trabajo

Certificación
Yo, el abajo firmante, certifico que, según mi anteceder, estos datos describen correctamente mi persona, mis calificaciones y mi experiencia.

[redacted]

[redacted]

[redacted]

FORTINET
FAST. SECURE. GLOBAL.

NSE Certified

This certifies that

Mario Brito

has successfully certified for

NSE 4 Security Professional

1/19/2015

[redacted]

CHIEF EXECUTIVE OFFICER
FORTINET

[redacted]

CHIEF TECHNOLOGY OFFICER
FORTINET

FORTINET
Network Security Expert Program

[redacted]

00000043

JMTELCOM
Toda una RED de Comunicaciones

CARTAS COMPROMISO

[redacted]

[redacted]

JMTELCOM
Toda una RED de Comunicaciones

232

San Salvador, 22 de Junio de 2018.

Señores
MINISTERIO DE TRABAJO Y PREVISION SOCIAL
Presente.

Referencia: LG MTPS 12-2018 denominada "Adquisición de 19 Equipos de Seguridad Perimetral con Licencias"

Estimados señores:

De resultar adjudicados, JMTelcom, S.A. de C.V. se compromete a presentar solvencias o constancias fiscales, municipales y de seguridad social, vigentes a la fecha de ser requeridas por la UACI. Del mismo modo, si fuera requerido nos comprometemos a presentar garantía de cumplimiento de contrato por el valor del 10% del monto adjudicado y garantía de buen funcionamiento y calidad de bienes por el valor del 10% del monto adjudicado, en términos establecidos en los documentos de contratación.

Atentamente,

[redacted]

[redacted]

JMTELCOM
Toda una RED de Comunicaciones

231

San Salvador, 22 de junio de 2018

Señores
MINISTERIO DE TABAJO Y PREVISION SOCIAL
Presente.

Referencia: Libre Gestión LG MTPS 12-2018: **"Adquisición de 19 equipos de seguridad perimetral con licencias"**

Estimados Señores:

JMTelcom, S.A. de C.V. confirma que de ser adjudicado cumplirá con lo siguiente:

- Instalará y configurará equipo para ponerlo en operación.
- Dara respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte.
- Reparara los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestaran un equipo de características similares mientras se hace efectivo el reemplazo total del equipo en garantía.
- Brindará soporte 24 horas al día, 7 días a la semana sin costo adicional.
- Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.
- Reemplazara en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o porque las características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.

Atentamente,

[redacted]

[redacted]

00000046



JMTELCOM
Toda una RED de Comunicaciones

230

REFERENCIAS DE CLIENTES

[redacted]

00000047

MINISTERIO DE TRABAJO

I. DATOS GENERALES DE LA INSTITUCIÓN:

1. Nombre de la Institución: **MINISTERIO DE GOBERNACION Y DESARROLLO TERRITORIAL**
2. Dirección: [redacted]
   Número telefónico:
   Fax: NA
   Correo Electrónico: [redacted]
3. A continuación, proporcionar los siguientes datos:

II. IDENTIFICACIÓN DEL CONTRATO:

NOMBRE DEL CONTRATO:	Suministro, instalación, configuración, soporte y capacitación de equipo para seguridad perimetral del Ministerio de Gobernación
FECHA DE INICIO	JULIO- 2014
FECHA DE FINALIZACIÓN	JULIO- 2015
MONTO DEL CONTRATO EN US $	$21,607.42

III. CALIDAD DEL SERVICIO:

INDICAR LA CALIDAD DE SERVICIO RECIBIDO: **MARCAR CON UNA "X" UNA SOLA VALORACIÓN:**	**Regular ( )** **Bueno ( )** **Muy bueno ( )** **Excelente (X)**

Y para ser presentada a la Unidad de Adquisiciones y Contrataciones Institucional (UACI), del Ministerio de Trabajo y Previsión Social, se extiende la presente constancia, en la ciudad de San Salvador, a los diecinueve días del mes de junio de dos mil dieciocho.

Atentamente,

MINISTERIO DE GOBERNACIÓN Y DESARROLLO TERRITORIAL
DIRECTOR DE DESARROLLO TECNOLÓGICO

Ing. Eduardo López
Director de Desarrollo Tecnológico
Ministerio de Gobernación y Desarrollo Territorial
MAIL: eduardo.lopez@gobernacion.gob.sv
Tel: 2527-7004

[redacted]

00000048

228

MINISTERIO DE TRABAJO

I. DATOS GENERALES DE LA INSTITUCIÓN:

1. Nombre de la Institución:
   BANCO DE DESARROLLO DE EL SALVADOR
2. Dirección: [redacted]

   Número telefónico:
   Fax: **NA**
   Correo Electrónico: **Rogelio.guevara@bandesal.gob.sv**

3. A continuación, proporcionar los siguientes datos:

II. IDENTIFICACIÓN DEL CONTRATO:

NOMBRE DEL CONTRATO:	**"SUMINISTRO DE SOFTWARE Y HARDWARE DE SEGURIDAD INFORMATICA PARA BANDESAL"**
FECHA DE INICIO	DICIEMBRE- 2017
FECHA DE FINALIZACIÓN	DICIEMBRE- 2020
MONTO DEL CONTRATO EN US $	$34,055.85

III. CALIDAD DEL SERVICIO:

INDICAR LA CALIDAD DE SERVICIO RECIBIDO: **MARCAR CON UNA "X" UNA SOLA VALORACIÓN:**	**Regular ( )** **Bueno ( )** **Muy bueno ( )** **Excelente (X)**

Y para ser presentada a la Unidad de Adquisiciones y Contrataciones Institucional (UACI), del Ministerio de Trabajo y Previsión Social, se extiende la presente constancia, en la ciudad de San Salvador, a los diecinueve días del mes de junio de dos mil dieciocho.

FIRMA: [redacted]	SELLO DE LA INSTITUCION [redacted]
NOMBRE: Lic. Rogelio Guevara	
CARGO: Jefe de Soporte e Infraestructura TI	

[redacted]

00000049

22

MINISTERIO DE TRABAJO

I. DATOS GENERALES DE LA INSTITUCIÓN:

1. Nombre de la Institución:
   MINISTERIO DE ECONOMIA
2. Dirección:
   Alameda Juan Pablo II y Calle Guadalupe Edificio C1 - C2, Centro de Gobierno. San Salvador
   Número telefónico: [redacted]
   Fax:
   Correo Electrónico:
3. A continuación, proporcionar los siguientes datos:

II. IDENTIFICACIÓN DEL CONTRATO:

NOMBRE DEL CONTRATO:	Soporte Técnico Local 7x24 para equipo FortiGate Cluster 1240B que incluye: Mantenimiento Preventivo y Correctivo
FECHA DE INICIO	**03/2018**
FECHA DE FINALIZACIÓN	**03/2019**
MONTO DEL CONTRATO EN US $	**$20,906.00**

III. CALIDAD DEL SERVICIO:

INDICAR LA CALIDAD DE SERVICIO RECIBIDO: **MARCAR CON UNA "X" UNA SOLA VALORACIÓN:**	**Regular ( )** **Bueno ( )** **Muy bueno ( )** **Excelente (x)**

Y para ser presentada a la Unidad de Adquisiciones y Contrataciones Institucional (UACI), del Ministerio de Trabajo y Previsión Social, se extiende la presente constancia, en la ciudad de San Salvador, a los dieciocho días del mes de junio de dos mil dieciocho.

FIRMA: [redacted]	SELLO DE LA INSTITUCION [redacted]
NOMBRE: Ir[redacted]	
CARGO: Jefe de Infraestructura y Soporte	

[redacted]

00000050



JMTELCOM
Toda una RED de Comunicaciones

226

OFERTA ECONÓMICA

[redacted]

[redacted]

00000051

JMTELCOM
Toda una RED de Comunicaciones

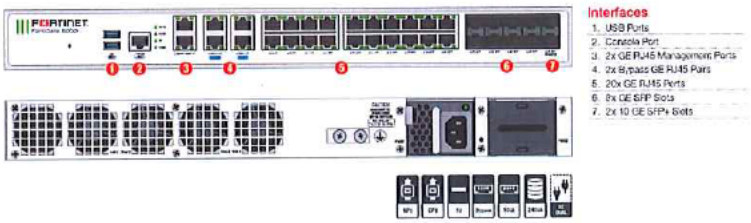
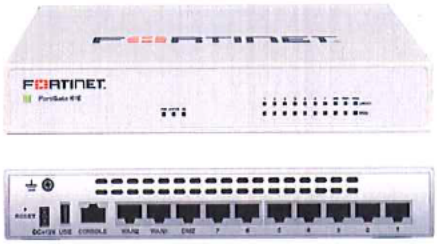
225

San Salvador, 22 de junio de 2018

Señores
MINISTERIO DE TABAJO Y PREVISION SOCIAL
Presente.

Referencia: Libre Gestión LG MTPS 12-2018: **"Adquisición de 19 equipos de seguridad perimetral con licencias"**

OFERTA ECONÓMICA

Cantidad	Descripción	Precio unitario con IVA y CESC Incluido	Total
2	 Firewall marca FORTINET, modelo FORTIGATE 800D en Bundle Pack, incluye instalación, licencias y soporte por 12 meses	$17,699.99	$35,399.98
17	 Firewall marca FORTINET, modelo FORTIGATE 61E en Bundle Pack, incluye instalación, licencias y soporte por 12 meses	$1,376.99	$23,408.83
		TOTAL CON IVA Y CESC	$58,808.81

SON: CINCUENTA Y OCHO MIL OCHOCIENTOS OCHO 81/100 DÓLARES DE LOS ESTADOS UNIDOS DE AMÉRICA INCLUYENDO IVA Y CESC

[redacted]

[redacted]

[redacted]

00000052

224

CONDICIONES GENERALES

Validez de la oferta:	Oferta válida por 60 días Calendario a partir de la presentación de la oferta.
Forma de pago:	Pago único con Crédito 60 días.
Tiempo de entrega:	Equipos con licenciamiento: 30 días calendario
Duración del servicio:	12 meses
Tiempo de Garantía:	12 meses

F. [redacted]

[redacted]

JMTELCOM
Toda una RED de Comunicaciones

HOJAS TÉCNICAS

[redacted]

[redacted]

222

En la ciudad de San Salvador, a las trece horas del día veinte de junio del año dos mil dieciocho.- Ante mí, [redacted], Notario, de este domicilio, comparece la Ingeniero [redacted], de [redacted] años de edad, [redacted] del domicilio de [redacted], Departamento de [redacted], a quien conozco e identifico portadora de su Documento Único de Identidad Número [redacted]; y ME DICE: Que comparece ante mis oficios Notariales para que de conformidad con el artículo veinticuatro de la Ley del Ejercicio Notarial de la Jurisdicción Voluntaria y de Otras Diligencias se nombre un perito traductor, para que vierta al castellano los pasajes escritos en Idioma Inglés, contenidos en el documento que me presenta.- Así se expresó la compareciente, a quien expliqué los efectos legales de la presente acta notarial que consta de una hoja y leída que le hube íntegramente lo escrito en solo acto ininterrumpido, ratifica su contenido y firmamos. DOY FE.

[redacted]

[redacted]

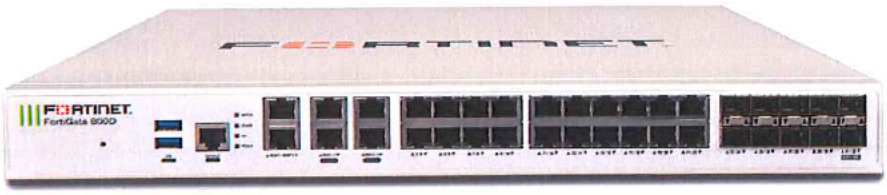
[redacted]

[redacted]

00000055

FORTINET

FortiGate® 800D



The Fortinet Enterprise Firewall Solution delivers end-to-end network security with one platform, one network security operating system and unified policy management with a single pane of glass — for **the industry's best protection against the most advanced security threats and targeted attacks.**

Security Fabric Integration

FortiGate appliances, interconnected with the Fortinet Security Fabric, form the backbone of the Fortinet Enterprise Solution.

36 Gbps
Firewall

5 Million
Concurrent Sessions

4.2 Gbps
IPS

3.5 Gbps
NGFW

2.4 Gbps
Threat Protection

Multiple GE RJ45, GE SFP,10 GE SFP+ slots and Bypass GE RJ45 Pairs

Deployment Modes

Next Generation Firewall
Internal Segmentation Firewall

Hardware Acceleration

SPU NP6 and CP8



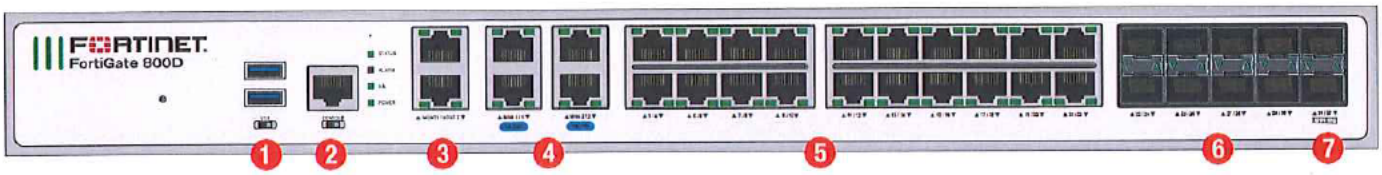
Third-Party Certifications

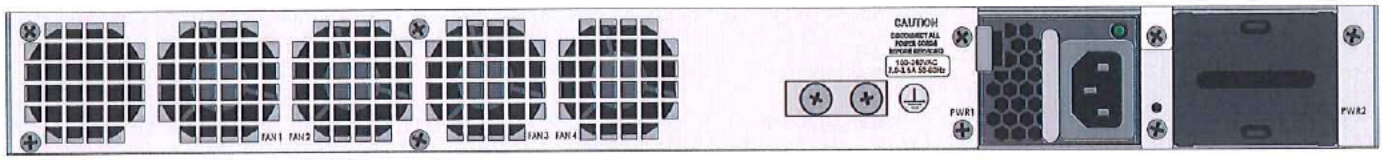
ICSA labs ICSA labs ICSA labs ICSA labs

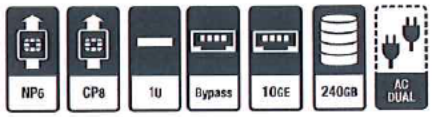
[redacted]

HARDWARE

FortiGate 800D







Interfaces

1. USB Ports
2. Console Port
3. 2x GE RJ45 Management Ports
4. 2x Bypass GE RJ45 Pairs
5. 20x GE RJ45 Ports
6. 8x GE SFP Slots
7. 2x 10 GE SFP+ Slots

Powered by SPU



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

Network Processor

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

- Superior firewall performance for IPv4/IPv6, SCTP and multicast traffic with ultra-low latency down to 2 microseconds
- VPN, CAPWAP and IP tunnel acceleration
- Anomaly-based intrusion prevention, checksum offload and packet defragmentation
- Traffic shaping and priority queuing

Content Processor

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

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

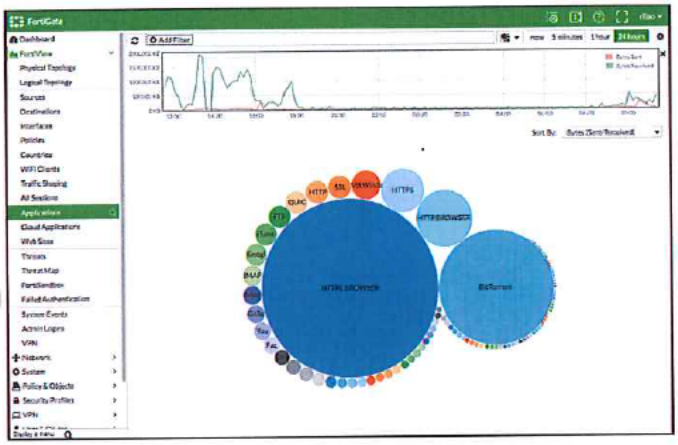
10 GE Connectivity

High speed connectivity is essential for network security segmentation. The FortiGate 800D provides 10 GE slots that simplify network designs without relying on additional devices to bridge desired connectivity.

SOFTWARE

FortiOS

Control all the security and networking capabilities across the entire FortiGate platform with one intuitive operating system. Reduce operating expenses and save time with a truly consolidated next generation security platform.



- A truly consolidated platform with one OS for all security and networking services for all FortiGate platforms.
- Industry-leading protection: NSS Labs Recommended, VB100, AV Comparatives and ICSA validated security and performance.
- Control thousands of applications, block the latest exploits, and filter web traffic based on millions of real-time URL ratings.
- Detect, contain and block advanced attacks automatically in minutes with integrated advanced threat protection framework.
- Solve your networking needs with extensive routing, switching, WiFi, LAN and WAN capabilities.
- Activate all the SPU-boosted capabilities you need on the fastest firewall platform available.

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

SERVICES

FortiGuard™ Security Services

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

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

FortiCare™ Support Services

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

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

Enterprise Bundle

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with the FortiGuard Enterprise Bundle. This bundle contains the full set of FortiGuard security services plus FortiCare service and support offering the most flexibility and broadest range of protection all in one package.

[redacted]

SPECIFICATIONS

	FORTIGATE 800D
Interfaces and Modules	
Hardware Accelerated 10 GE SFP+ Slots	2
Hardware Accelerated GE SFP Slots	8
Hardware Accelerated GE RJ45 Ports	20
Accelerated GE RJ45 Bypass Interfaces	4
GE RJ45 Management / HA Ports	2
USB Ports (Client / Server)	1 / 2
Console Port	1
Onboard Storage	240 GB
Included Transceivers	2x SFP (SX 1 GE)
System Performance and Capacity	
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	36 / 36 / 22 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	36 / 36 / 22 Gbps
Firewall Latency (64 byte, UDP)	3 µs
Firewall Throughput (Packet per Second)	33 Mpps
Concurrent Sessions (TCP)	5 Million
New Sessions/Second (TCP)	280,000
Firewall Policies	10,000
IPsec VPN Throughput (512 byte)	20 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	2,000
Client-to-Gateway IPsec VPN Tunnels	10,000
SSL-VPN Throughput	2.2 Gbps
Concurrent SSL-VPN Users (Recommended Maximum)	5,000
IPS Throughput (HTTP / Enterprise Mix) [1]	8 / 4.2 Gbps
SSL Inspection Throughput [2]	4 Gbps
Application Control Throughput [3]	6 Gbps
NGFW Throughput [4]	3.5 Gbps
Threat Protection Throughput [5]	2.4 Gbps
CAPWAP Throughput [6]	5.5 Gbps
Virtual Domains (Default / Maximum)	10 / 10

	FORTIGATE 800D
Maximum Number of FortiAPs (Total / Tunnel)	1024 / 512
Maximum Number of FortiTokens	1,000
Maximum Number of Registered Endpoints	2,000
High Availability Configurations	Active-Active, Active-Passive, Clustering
Dimensions and Power	
Height x Width x Length (inches)	1.77 x 17.0 x 16.4
Height x Width x Length (mm)	45 x 432 x 416
Weight	19.0 lbs (8.6 kg)
Form Factor	1 RU
Wall Mountable	No
AC Power Supply	100–240V AC, 60–50 Hz
Power Consumption (Average / Maximum)	128 W / 187 W
Current (Maximum)	110V/7A, 220V/3.5A
Heat Dissipation	636 BTU/h
Redundant Power Supplies	(Hot Swappable) optional
Operating Environment and Certifications	
Operating Temperature	32–104°F (0–40°C)
Storage Temperature	-31–158°F (-35–70°C)
Humidity	20–90% non-condensing
Operating Altitude	Up to 7,400 ft (2,250 m)
Compliance	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; USGv6/IPv6

Note: All performance values are "up to" and vary depending on system configuration. IPsec VPN performance is based on 512 byte UDP packets using AES-256+SHA1. 1. IPS performance is measured using 1 Meyte HTTP and Enterprise Traffic Mix. 2. SSL Inspection is measured with IPS enabled and HTTP traffic using TLS v1.2 with AES256-SHA. 3. Application Control performance is measured with 64 Kbytes HTTP traffic. 4. NGFW performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix. 5. Threat Protection performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix. 6. CAPWAP performance is based on 1444 byte UDP packets.

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

ORDER INFORMATION

Product	SKU	Description
FortiGate 800D	FG-800D	22x GE RJ45 ports, 4x GE RJ45 with Bypass Protection, 8x GE SFP slots, 2x 10 GE SFP+ slots, SPU NP6 and CP8 hardware accelerated, 240 GB internal onboard SSD storage.

Optional Accessories/Spares	SKU	Description
1 GE SFP LX Transceiver Module	FG-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 Transceiver Module	FG-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP SX Transceiver Module	FG-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FG-TRAN-SFP+SR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Long Range	FG-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Active Direct Attach Cable, 10m / 32.8 ft	SP-CABLE-ADASFP+	10 GE SFP+ active direct attach cable, 10m / 32.8 ft for all systems with SFP+ and SFP/SFP+ slots.
AC Power Supply	SP-FG600C-PS	AC power supply for FG-600C, FG-800C, FG-800D and FG-1000C.

FORTINET

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

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6395.2788

LATIN AMERICA SALES OFFICE
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
United States
Tel: +1.954.368.9990

[redacted]

Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

FST-FG0D-DS-GTGH

FG-800D-DAT-R9-201703

la ciudad de San Salvador, a las trece horas y diez minutos del día veinte de junio del año dos mil dieciocho.-

Agréguese el documento presentado por la Ingeniero [redacted] nómbrese perito traductor para que vierta al Idioma Castellano a [redacted] los pasajes escritos en Idioma Inglés, a quien se le hará saber este nombramiento para su aceptación y demás efectos legales. DOY FE.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

TRADUCCION

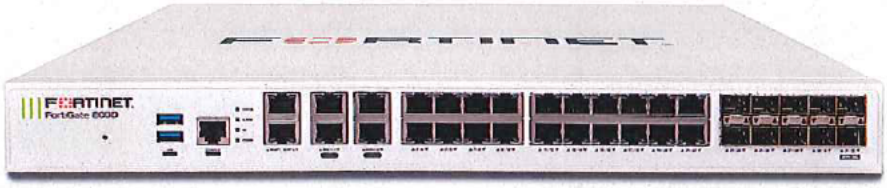
[redacted]

00000062

FORTINET

FortiGate® 800D

[redacted]



La solución de FireWall Fortinet Empresarial ofrece Seguridad en la Red de Extremo a Extremo en una sola plataforma, un sistema operativo de seguridad de red y administración unificada de políticas con un único panel de Administracion, **siendo la mejor protección en la industria contra las amenazas de seguridad más avanzadas y ataques dirigidos.**

Integración del Tejido de Seguridad

Los dispositivos FortiGate, interconectados con el Tejido de Seguridad Fortinet, forman la columna vertebral de la solución Empresarial de Fortinet.

36 Gbps
Firewall

5 Millones
Sesiones concurrentes

4.2 Gbps
IPS

3.5 Gbps
Firewall de Siguiente Generacion

2.4 Gbps
Proteccion de Amenazas

Puertos Multiples RJ45, Puertos SFP, 10 Puertos SFP + ranuras y puertos RJ45 de Derivación

Modos de implementación
Firewall de Proxima Generación
de Segmentación Interna.

Aceleradores de Hardware
SPU NPS y CPS



Certificaciones de Terceros

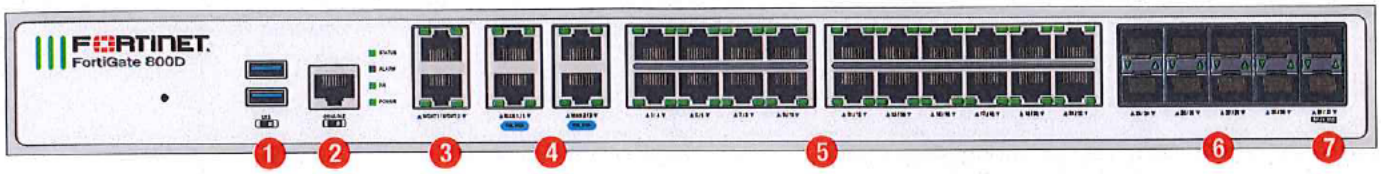
[redacted]

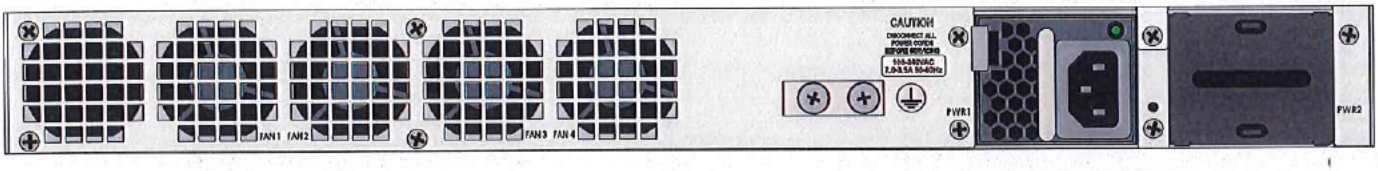
00000063

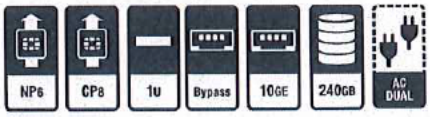
[redacted]

ConstruccionFisica HARDWARE

FortiGate 800D







Interfaces

1. Puertos USB
2. Puerto de Consola
3. 2x Puertos de Administracion RJ45 GE
4. 2x pares RJ45 de Derivacion
5. 20x Puertos RJ45 GE
6. 8x Ranuras SFP GE
7. 2x 10 SFP+ ranuras GE

Alimentado con Procesadores SPU



▪Los procesadores SPU personalizados ofrecen la potencia que necesita para detectar contenido malicioso a velocidades de varios Gigabit

• Otras tecnologías de seguridad no pueden proteger contra la amplia gama actual de amenazas basadas en contenido y conexión, ya que dependen de un procesador CPU de propósito general, lo que provoca una brecha de rendimiento peligroso.

• Los procesadores SPU brindan el rendimiento necesario para bloquear las amenazas emergentes, cumplir con las rigurosas certificaciones de terceros y garantizar que su solución de seguridad de red no se convierta en un cuello de botella de su red.

Procesador de Red

El nuevo y revolucionario procesador de red SPU NP6 de Fortinet funciona en línea con las funciones de FortiOS y ofrece:

• Rendimiento de firewall superior para IPv4 / IPv6, SCTP y tráfico de multidifusión con latencia ultrabaja de hasta 2 microsegundos

• VPN, CAPWAP y aceleración de túnel IP

• Prevención de intrusiones basadas en anomalías, descarga de suma de comprobación y desfragmentación de paquetes

• Modelado del tráfico y colas de prioridad

Procesador de Contenido

El procesador de contenido SPU CP8 funciona fuera del flujo directo de tráfico, proporcionando servicios de criptografía e inspección de contenido de alta velocidad, que incluyen:

• Aprobación de inspección de contenido basada en firmas

• Descarga de cifrado y descifrado

[redacted]

10 Conectividad de GE

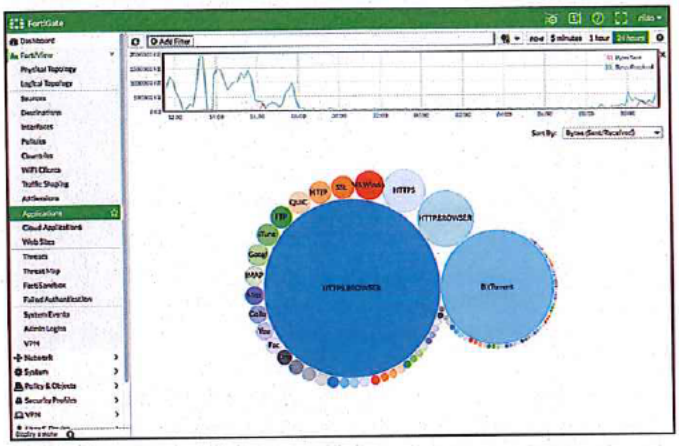
La conectividad de alta velocidad es esencial para la segmentación de la seguridad de la red. El FortiGate 800D proporciona 10 ranuras GE que simplifican los diseños de red sin depender de dispositivos adicionales para unir la conectividad deseada.

00000064

SOFTWARE

FortiOS

Controle todas las capacidades de seguridad y de red en toda la plataforma FortiGate con un sistema operativo intuitivo. Reduzca los gastos operativos y ahorre tiempo con una plataforma de seguridad de próxima generación verdaderamente consolidada.



- Una plataforma verdaderamente consolidada con un sistema operativo para todos los servicios de seguridad y redes para todas las plataformas FortiGate.
- Protección líder en el sector: NSS Labs la recomienda, VB100, comparaciones AV y ICSA valida la seguridad y rendimiento.
- Controla miles de aplicaciones, bloquea las últimas vulnerabilidades y filtrar el tráfico web en función de millones de valoraciones de URL en tiempo real.
- Detecta, contiene y bloquea ataques avanzados automáticamente en minutos con un marco de protección de amenazas avanzado integrado.
- Resuelva sus necesidades de red con amplias capacidades de enrutamiento, conmutación, WiFi, LAN y WAN.
- Activa todas las capacidades SPU-Mejoradas que necesita en la plataforma de firewall más rápida disponible.

Para obtener más información, consulte la hoja de datos FortiOS disponible en www.fortinet.com

SERVICIOS

Servicios de Seguridad Fortiguard

FortiGuard Labs ofrece inteligencia en tiempo real sobre el panorama de las amenazas, ofreciendo actualizaciones de seguridad integrales en toda la gama de soluciones de Fortinet. Formado por investigadores, ingenieros y especialistas forenses especializados en amenazas de seguridad, el equipo colabora con las organizaciones de monitoreo de amenazas más importantes del mundo, otros proveedores de seguridad y redes, así como también agencias de aplicación de la ley:

- Actualizaciones en Tiempo Real: investigación de operaciones globales 24x7x365 inteligencia de seguridad, distribuida a través de la red distribuida Fortinet a todas las plataformas de Fortinet.
- Investigaciones en Seguridad - FortiGuard Labs ha descubierto más de 170 vulnerabilidades únicas de día cero hasta la fecha, que suman millones de actualizaciones automáticas de firmas mensualmente.
- Inteligencia de Seguridad Validada: con base en la inteligencia de FortiGuard, la plataforma de seguridad de red de Fortinet es probada y validada por los laboratorios de pruebas y clientes de terceros más importantes del mundo.

Servicios de Soporte Forticare

Nuestro equipo de atención al cliente de FortiCare proporciona asistencia técnica global para todos los productos de Fortinet. Con personal de apoyo en América, Europa, Medio Oriente y Asia, FortiCare ofrece servicios para satisfacer las necesidades de empresas de todos los tamaños:

- Soporte Mejorado: para clientes que solo necesitan asistencia durante el horario comercial local.
- Soporte Integral: para clientes que necesitan soporte de misión crítica las 24 horas, incluido el reemplazo de hardware de intercambio avanzado.
- Servicios Avanzados: para clientes globales o regionales que necesitan un Administrador de cuentas técnico asignado, acuerdos de nivel de servicio mejorados, soporte de software extendido, escalamiento de prioridades, visitas in situ y más.
- Servicios Profesionales: para clientes con implementaciones de seguridad más complejas que requieren servicios de arquitectura y diseño, servicios de implementación e implementación, servicios operativos y más.

[redacted]

Paquete Empresarial

FortiGuard Labs ofrece una Serie de Servicios de Inteligencia de seguridad para aumentar la plataforma de firewall FortiGate. Puede optimizar fácilmente las capacidades de protección de su FortiGate con el FortiGuard Enterprise Bundle. Este paquete contiene el conjunto completo de servicios de seguridad FortiGuard más el servicio y soporte de FortiCare que ofrece la mayor flexibilidad y la más amplia gama de protección, todo en un solo paquete.

[redacted]

211

Especificaciones

	FORTIGATE 800D
Interfaces and Modules	
Hardware Accelerated 10 GE SFP+ Slots	2
Hardware Accelerated GE SFP Slots	8
Hardware Accelerated GE RJ45 Ports	20
Accelerated GE RJ45 Bypass Interfaces	4
GE RJ45 Management / HA Ports	2
USB Ports (Client / Server)	1 / 2
Console Port	1
Onboard Storage	240 GB
Included Transceivers	2x SFP (SX 1 GE)
System Performance and Capacity	
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	36 / 36 / 22 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	36 / 36 / 22 Gbps
Firewall Latency (64 byte, UDP)	3 µs
Firewall Throughput (Packet per Second)	33 Mpps
Concurrent Sessions (TCP)	5 Million
New Sessions/Second (TCP)	280,000
Firewall Policies	10,000
IPsec VPN Throughput (512 byte)	20 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	2,000
Client-to-Gateway IPsec VPN Tunnels	10,000
SSL-VPN Throughput	2.2 Gbps
Concurrent SSL-VPN Users (Recommended Maximum)	5,000
IPS Throughput (HTTP / Enterprise Mix) [1]	8 / 4.2 Gbps
SSL Inspection Throughput [2]	4 Gbps
Application Control Throughput [3]	6 Gbps
NGFW Throughput [4]	3.5 Gbps
Threat Protection Throughput [5]	2.4 Gbps
CAPWAP Throughput [6]	5.5 Gbps
Virtual Domains (Default / Maximum)	10 / 10

	FORTIGATE 800D
Maximum Number of FortiAPs (Total / Tunnel)	1024 / 512
Maximum Number of FortiTokens	1,000
Maximum Number of Registered Endpoints	2,000
High Availability Configurations	Active-Active, Active-Passive, Clustering
Dimensions and Power	
Height x Width x Length (inches)	1.77 x 17.0 x 16.4
Height x Width x Length (mm)	45 x 432 x 416
Weight	19.0 lbs (8.6 kg)
Form Factor	1 RU
Wall Mountable	No
AC Power Supply	100–240V AC, 60–50 Hz
Power Consumption (Average / Maximum)	128 W / 187 W
Current (Maximum)	110V/7A, 220V/3.5A
Heat Dissipation	636 BTU/h
Redundant Power Supplies	(Hot Swappable) optional
Operating Environment and Certifications	
Operating Temperature	32–104°F (0–40°C)
Storage Temperature	-31–158°F (-35–70°C)
Humidity	20–90% non-condensing
Operating Altitude	Up to 7,400 ft (2,250 m)
Compliance	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; USGv6/IPv6

Note: All performance values are "up to" and vary depending on system configuration. IPsec VPN performance is based on 512 byte UDP packets using AES-256+SHA1. 1. IPS performance is measured using 1 Mbyte HTTP and Enterprise Traffic Mix. 2. SSL Inspection is measured with IPS enabled and HTTP traffic using TLS v1.2 with AES256-SHA. 3. Application Control performance is measured with 64 Kbytes HTTP traffic. 4. NGFW performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix. 5. Threat Protection performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix. 6. CAPWAP performance is based on 1444 byte UDP packets.

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

Información de como ordenar

Product	SKU	Description
FortiGate 800D	FG-800D	22x GE RJ45 ports, 4x GE RJ45 with Bypass Protection, 8x GE SFP slots, 2x 10 GE SFP+ slots, SPU NP6 and CP8 hardware accelerated, 240 GB Internal onboard SSD storage.
Optional Accessories/Spares	**SKU**	**Description**
1 GE SFP LX Transceiver Module	FG-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 Transceiver Module	FG-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+slots.
1 GE SFP SX Transceiver Module	FG-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FG-TRAN-SFP+SR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Long Range	FG-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Active Direct Attach Cable, 10m / 32.8 ft	SP-CABLE-ADASFP+	10 GE SFP+ active direct attach cable, 10m / 32.8 ft for all systems with SFP+ and SFP/SFP+ slots.
AC Power Supply	SP-FG600C-PS	AC power supply for FG-600C, FG-800C, FG-800D and FG-1000C.

FORTINET

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

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6395.2788

LATIN AMERICA SALES OFFICE
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
United States
Tel: +1.954.368.99[redacted]

Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

FST-PROD-DS-GT8-I

FG-800D-DAT-R8-201703

000000 66

la ciudad de San salvador, a las trece horas y veinticinco minutos del día veinte de junio del año dos mil dieciocho. Ante mí, [redacted], Notario, de este domicilio, con Documento Único de Identidad Número [redacted]

Vista la anterior traducción del idioma inglés al Castellano por la Ingeniera [redacted] se da por aprobada firmada y sellada por la suscrita Notario. Devuélvanse a la interesada las presentes diligencias para los efectos consiguientes. DOY FE.

[redacted]

[redacted]

[redacted]

En la ciudad de San Salvador, a las catorce horas del día veinte de junio del año dos mil dieciocho.- Ante mí, [redacted], Notario, de este domicilio, comparece la Ingeniero [redacted] de s[redacted] años de edad, [redacted], del domicilio de [redacted], Departamento de [redacted] a quien conozco e identifico portadora de su Documento Único de Identidad Número [redacted] y ME DICE: Que comparece ante mis oficios Notariales para que de conformidad con el artículo veinticuatro de la Ley del Ejercicio Notarial de la Jurisdicción Voluntaria y de Otras Diligencias se nombre un perito traductor, para que vierta al castellano los pasajes escritos en Idioma Inglés, contenidos en el documento que me presenta.- Así se expresó la compareciente, a quien expliqué los efectos legales de la presente acta notarial que consta de una hoja y leída que le hube íntegramente lo escrito en solo acto ininterrumpido, ratifica su contenido y firmamos. DOY FE.

[redacted]

[redacted]

[redacted]

[redacted]

00000068

[redacted]

FortiGate/FortiWiFi® 60E Series

FortiGate 60E, FortiWiFi 60E, FortiGate 61E and FortiWiFi 61E



The Fortinet Enterprise Firewall Solution delivers end-to-end network security with one platform, one network security operating system and unified policy management with a single pane of glass — for **the industry's best protection against the most advanced security threats and targeted attacks.**

Security Fabric Integration

FortiGate appliances, interconnected with the Fortinet Security Fabric, form the backbone of the Fortinet Enterprise Solution.

3 Gbps
Firewall

1.3 Million
Concurrent Sessions

350 Mbps
IPS

250 Mbps
NGFW

180 Mbps
Threat Protection

Multiple GE RJ45 | WiFi Variants | Variants with internal storage

Deployment Modes

Distributed Enterprise Firewall

Hardware Acceleration

SPU SoC3



Third-Party Certifications

ICSA labs ICSA labs ICSA labs

[redacted]

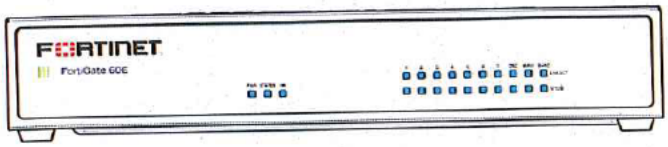
ICSA labs ICSA labs

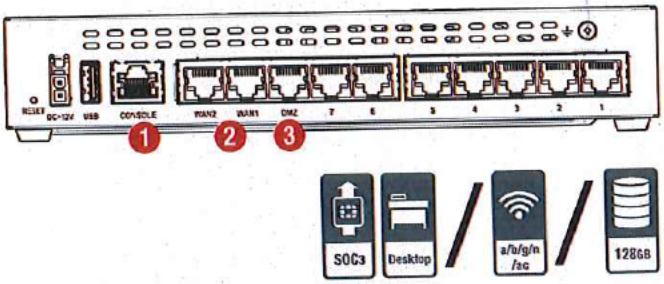
00000069

[redacted]

HARDWARE

FortiGate/FortiWiFi 60E/61E





Interfaces

1. Console Port
2. 2x GE RJ45 WAN Ports
3. 1x GE RJ45 DMZ Ports
4. 7x GE RJ45 Internal Ports

Powered by SPU SoC3



- Combines a RISC-based CPU with Fortinet's proprietary SPU content and network processors for unmatched performance
- Simplifies appliance design and enables breakthrough performance for smaller networks
- Supports firewall acceleration across all packet sizes for maximum throughput
- Delivers accelerated UTM content processing for superior performance and protection
- Accelerates VPN performance for high speed, secure remote access

3G/4G WAN Connectivity

The FortiGate/FortiWiFi 60E Series includes a USB port that allows you to plug in a compatible third-party 3G/4G USB modem, providing additional WAN connectivity or a redundant link for maximum reliability.

Compact and Reliable Form Factor

Designed for small environments, you can place it on a desktop or wall-mount it. It is small, lightweight yet highly reliable with superior MTBF (Mean Time Between Failure), minimizing the chance of a network disruption.

Superior Wireless Coverage

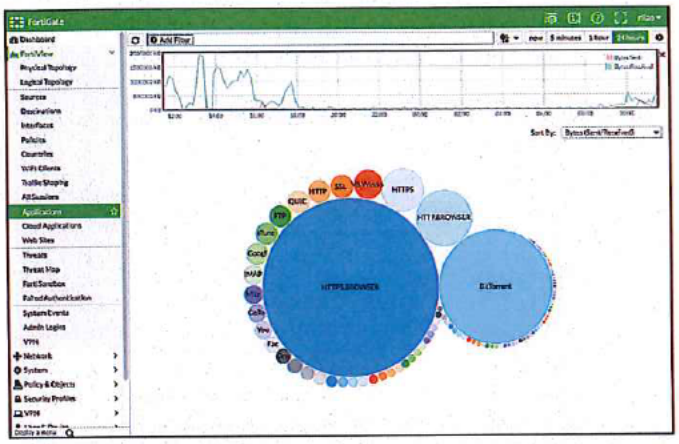
A built-in dual-band, dual-stream access point with internal antennas is integrated on the FortiWiFi 60E and provides speedy 802.11ac wireless access. The dual-band chipset addresses the PCI-DSS compliance requirement for rogue AP wireless scanning, providing maximum protection for regulated environments.

[redacted]

SOFTWARE

FortiOS

Control all the security and networking capabilities across the entire FortiGate platform with one intuitive operating system. Reduce operating expenses and save time with a truly consolidated next generation security platform.



- A truly consolidated platform with one OS for all security and networking services for all FortiGate platforms.
- Industry-leading protection: NSS Labs Recommended, VB100, AV Comparatives and ICSA validated security and performance.
- Control thousands of applications, block the latest exploits, and filter web traffic based on millions of real-time URL ratings.
- Detect, contain and block advanced attacks automatically in minutes with integrated advanced threat protection framework.
- Solve your networking needs with extensive routing, switching, WiFi, LAN and WAN capabilities.
- Activate all the SPU-boosted capabilities you need on the fastest firewall platform available.

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

SERVICES

FortiGuard™ Security Services

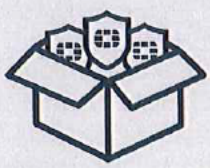
FortiGuard Labs offers real-time intelligence on the threat landscape, delivering comprehensive security updates across the full range of Fortinet's solutions. Comprised of security threat researchers, engineers, and forensic specialists, the team collaborates with the world's leading threat monitoring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

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

FortiCare™ Support Services

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

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



Enterprise Bundle

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with the FortiGuard Enterprise Bundle. This bundle contains the full set of FortiGuard security services plus FortiCare service and support offering the most flexibility and broadest range of protection all in one package.

[redacted]

SPECIFICATIONS

	FORTIGATE 60E	FORTIWIFI 60E	FORTIGATE 61E	FORTIWIFI 61E
Hardware Specifications				
GE RJ45 WAN Ports	2		2	
GE RJ45 Internal Ports	7		7	
GE RJ45 PoE Ports	–		–	
GE RJ45 DMZ Ports	1		1	
Wireless Interface	–	802.11 a/b/g/n/ac	–	802.11 a/b/g/n/ac
USB Ports	1		1	
Console (RJ45)	1		1	
Internal Storage	–		128 GB	
System Performance				
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	3 / 3 / 3 Gbps			
Firewall Latency (64 byte UDP packets)	3 µs			
Firewall Throughput (Packets Per Second)	4.5 Mpps			
Concurrent Sessions (TCP)	1.3 Million			
New Sessions/Second (TCP)	30,000			
Firewall Policies	5,000			
IPsec VPN Throughput (512 byte packets)	2 Gbps			
Gateway-to-Gateway IPsec VPN Tunnels	200			
Client-to-Gateway IPsec VPN Tunnels	500			
SSL-VPN Throughput	150 Mbps			
Concurrent SSL-VPN Users (Recommended Maximum)	100			
IPS Throughput (HTTP / Enterprise Mix) [1]	1,400 / 350 Mbps			
SSL Inspection Throughput [2]	340 Mbps			
Application Control Throughput [3]	550 Mbps			
NGFW Throughput [4]	250 Mbps			
Threat Protection Throughput [5]	180 Mbps			
CAPWAP Throughput [6]	1.5 Gbps			
Virtual Domains (Default / Maximum)	10 / 10			
Maximum Number of FortiAPs (Total / Tunnel Mode)	10 / 5			
Maximum Number of FortiTokens	100			
Maximum Number of Registered FortiClients	200			
High Availability Configurations	Active / Active, Active / Passive, Clustering			
Dimensions				
Height x Width x Length (inches)	1.5 x 8.5 x 6.3			
Height x Width x Length (mm)	38 x 216 x 160			
Weight	1.9 lbs (0.9 kg)			
Form Factor	Desktop			
Environment				
Power Required	100–240V AC, 50–60 Hz			
Maximum Current	110V AC / 1.5 A, 220V AC / 0.75 A	115V AC / 0.9A, 230V AC / 0.6A	115V AC / 0.9A, 230V AC / 0.6A	115V AC / 0.9A, 230V AC / 0.6A
Power Consumption (Average / Maximum)	11.7 / 14 W	12.6 / 15.2 W	11.9 / 14.3 W	13 / 16 W
Heat Dissipation	40 BTU/h	52 BTU/h	49 BTU/h	55 BTU/h
Operating Temperature	32–104°F (0–40°C)			
Storage Temperature	-31–158°F (-35–70°C)			
Humidity	20–90% non-condensing			
Operating Altitude	Up to 7,400 ft (2,250 m)			
Compliance				
Safety	FCC Part 15 Class B, C-Tick, VCCI, CE, UL/cUL, CB			
Certifications				
	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN			

Note: All performance values are "up to" and vary depending on system configuration. IPsec VPN performance is based on 512 byte UDP packets using AES-256+SHA1. 1. IPS performance is measured using 1 Mbyte HTTP and Enterprise Traffic Mix. 2. SSL Inspection is measured with IPS enabled and HTTP traffic, using TLS v1.2 with AES256-SHA. 3. Application Control performance is measured with 64 Kbytes HTTP traffic. 4. NGFW performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix. 5. Threat Protection performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix. 6. CAPWAP performance is based on 1444 byte UDP packets.

ORDER INFORMATION

Product	SKU	Description
FortiGate 60E	FG-60E	10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port). Maximum managed FortiAPs (Total / Tunnel) 10 / 5.
FortiWiFi 60E	FWF-60E	10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port), Wireless (802.11a/b/g/n/ac). Maximum managed FortiAPs (Total / Tunnel) 10 / 5.
FortiGate 61E	FG-61E	10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port), 128 GB SSD onboard storage. Maximum managed FortiAPs (Total / Tunnel) 10 / 5.
FortiWiFi 61E	FWF-61E	10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port), Wireless (802.11a/b/g/n/ac), 128 GB SSD onboard storage. Maximum managed FortiAPs (Total / Tunnel) 10 / 5.

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

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6395.2788

LATIN AMERICA SALES OFFICE
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
United States
Tel: +1.954.368.9990

Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

FST-PROD-DS-GT60E

FGFWF-60E-DAT-R6-201702

la ciudad de San Salvador, a las catorce horas y diez minutos del día veinte de junio del año dos mil dieciocho.-

Agréguese el documento presentado por la Ingeniero [redacted] nómbrese perito traductor para que vierta al Idioma Castellano a [redacted], los pasajes escritos en Idioma Inglés, a quien se le hará saber este nombramiento para su aceptación y demás efectos legales. DOY FE.

[redacted]

[redacted]

202

En la ciudad de San Salvador, a las catorce horas y quince minutos del día veinte de junio del año dos mil dieciocho.- Hice saber, leyéndole el auto anterior al [redacted] de sesenta y tres años de edad, Ingeniero [redacted] del domicilio de [redacted], departamento de [redacted] con Documento Único de Identidad Número ce[redacted]; a quien luego de impuesto de su cargo, manifiesta aceptarlo y jura cumplirlo fiel y legalmente y para constancia firma. DOY FE.

[redacted]

[redacted]

[redacted]

[redacted]

00000075

[redacted]

201

[redacted]

TRADUCCION

[redacted]

00000076

[redacted]

FortiGate/FortiWiFi Serie 60E

FortiGate 60E, FortiWiFi 60E, FortiGate 61E and FortiWiFi 61E



La solución Empresarial de FireWall Fortinet ofrece seguridad de red de extremo a extremo con una plataforma, un sistema operativo de seguridad de red y administración unificada de políticas con un único panel de Administración, para la mejor protección de la industria contra las amenazas de seguridad más avanzadas y ataques dirigidos.

Integración del Tejido de Seguridad

Los dispositivos FortiGate, interconectados con el Tejido de Seguridad Fortinet Security Fabric, forman la columna vertebral de la solución Fortinet Enterprise.

3 Gbps
Firewall

1.3 Million
Sesiones concurrentes

350 Mbps
IPS

250 Mbps
NGFW

180 Mbps
Proteccion de amenazas

Puertos Multiples RJ45, Puertos SFP, 10 Puertos SFP+ ranuras y puertos RJ45 de Derivación

Modos de Implementación

Firewall Empresarial Distribuido

Acelerador de Hardware

SPU SoC3



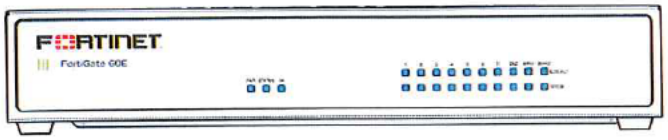
Certificaciones de Terceros Certificación

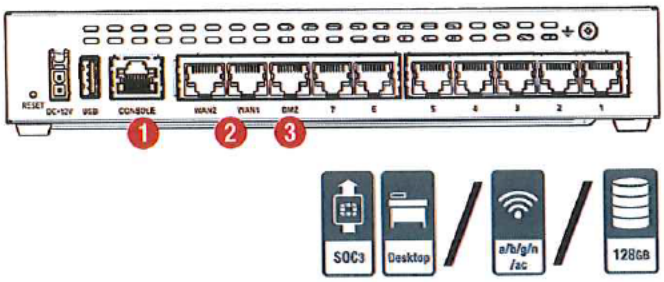
[redacted]

[redacted]

Construcción Física (Hardware)

FortiGate/FortiWiFi 60E/61E





Interfaces

1. Puerto de Consola
2. 2X Puertos WAN RJ45 GE
3. 1x Puerto DMZ RJ45 GE
4. 7x Puertos Internos RJ45 GE

Alimentado con Procesadores SPU SoC3

SPU

- Combina una CPU basada en RISC con contenido patentado de Fortinet y procesadores de red para un rendimiento sin igual
- Simplifica el diseño del dispositivo y permite un rendimiento innovador para redes más pequeñas
- Admite la aceleración del FireWall en todos los tamaños de paquetes para un rendimiento máximo
- Ofrece procesamiento acelerado de contenido UTM para un rendimiento y protección superiores
- Acelera el rendimiento de VPN para acceso remoto seguro de alta velocidad

Conectividad 3G / 4G WAN

La serie FortiGate / FortiWiFi 60E incluye un puerto USB que le permite conectar un módem USB 3G / 4G de terceros compatible, que brinda conectividad WAN adicional o un enlace redundante para una máxima confiabilidad.

Factor de Forma Compacto y Confiable

Diseñado para entornos pequeños, puede colocarlo en un escritorio o montarlo en la pared. Es pequeño, liviano pero altamente confiable con un MTBF (Mean Time Between Failure) superior, lo que minimiza la posibilidad de una interrupción de la red.

Cobertura Inalámbrica Superior

El FortiWiFi 60E incorpora un punto de acceso de doble banda incorporado con antenas internas y proporciona un acceso inalámbrico 802.11ac rápido. El chipset de doble banda satisface el requisito de cumplimiento de PCI-DSS para el escaneo inalámbrico AP eficiente, proporcionando la máxima protección para entornos regulados.

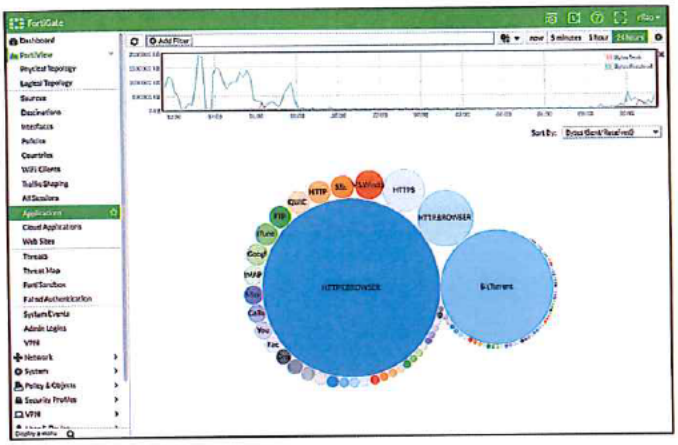
[redacted]

00000078

SOFTWARE

FortiOS

Controle todas las capacidades de seguridad y de red en toda la plataforma FortiGate con un sistema operativo intuitivo. Reduzca los gastos operativos y ahorre tiempo con una plataforma de seguridad de próxima generación verdaderamente consolidada.



▪Una plataforma verdaderamente consolidada con un sistema operativo para todos los servicios de seguridad y redes para todas las plataformas FortiGate.
• Protección líder en el sector: NSS Labs la recomienda, VB100, comparaciones AV y ICSA valida la seguridad y rendimiento.
• Controla miles de aplicaciones, bloquea las últimas vulnerabilidades y filtrar el tráfico web en función de millones de valoraciones de URL en tiempo real.
• Detecta, contiene y bloquea ataques avanzados automáticamente en minutos con un marco de protección de amenazas avanzado integrado.
• Resuelva sus necesidades de red con amplias capacidades de enrutamiento, conmutación, WiFi, LAN y WAN.
• Activa todas las capacidades SPU-Mejoradas que necesita en la plataforma de firewall más rápida disponible.

Para obtener más información, consulte la hoja de datos FortiOS disponible en www.fortinet.com

SERVICIOS

Servicios de Seguridad FortiGuardTM

FortiGuard Labs ofrece inteligencia en tiempo real sobre el panorama de las amenazas, ofreciendo actualizaciones de seguridad integrales en toda la gama de soluciones de Fortinet. Formado por investigadores, ingenieros y especialistas forenses especializados en amenazas de seguridad, el equipo colabora con las organizaciones de monitoreo de amenazas más importantes del mundo, otros proveedores de seguridad y redes, así como también agencias de aplicación de la ley:

• Actualizaciones en Tiempo Real: investigación de operaciones globales 24x7x365 inteligencia de seguridad, distribuida a través de la red distribuida Fortinet a todas las plataformas de Fortinet.
• Investigaciones en Seguridad - FortiGuard Labs ha descubierto más de 170 vulnerabilidades únicas de día cero hasta la fecha, que suman millones de actualizaciones automáticas de firmas mensualmente.
• Inteligencia de Seguridad Validada: con base en la inteligencia de FortiGuard, la plataforma de seguridad de red de Fortinet es probada y validada por los laboratorios de pruebas y clientes de terceros más importantes del mundo.

Servicios de Soporte FortiCareTM

Nuestro equipo de atención al cliente de FortiCare proporciona asistencia técnica global para todos los productos de Fortinet. Con personal de apoyo en América, Europa, Medio Oriente y Asia, FortiCare ofrece servicios para satisfacer las necesidades de empresas de todos los tamaños:

•**Soporte Mejorado:** para clientes que solo necesitan asistencia durante el horario comercial local.
• **Soporte Integral:** para clientes que necesitan soporte de misión crítica las 24 horas, incluido el reemplazo de hardware de intercambio avanzado.
•**Servicios Avanzados:** para clientes globales o regionales que necesitan un Administrador de cuentas técnico asignado, acuerdos de nivel de servicio mejorados, soporte de software extendido, escalamiento de prioridades, visitas in situ y más.
•**Servicios Profesionales:** para clientes con implementaciones de seguridad más complejas que requieren servicios de arquitectura y diseño, servicios de implementación e implementación, servicios operativos y más.



Enterprise Bundle (Paquete Empresarial)
FortiGuard Labs ofrece una Serie de Servicios de Inteligencia de seguridad para aumentar la plataforma de firewall FortiGate. Puede optimizar fácilmente las capacidades de protección de su FortiGate con el FortiGuard Enterprise Bundle. Este paquete contiene el conjunto completo de servicios de seguridad FortiGuard más el servicio y soporte FortiCare que ofrece la mayor flexibilidad y la más amplia gama de protección, todo en un solo paquete.

ESPECIFICACIONES

	FORTIGATE 60E	FORTIWIFI 60E	FORTIGATE 61E	FORTIWIFI 61E
Hardware Specifications				
GE RJ45 WAN Ports	2		2	
GE RJ45 Internal Ports	7		7	
GE RJ45 PoE Ports	–		–	
GE RJ45 DMZ Ports	1		1	
Wireless Interface	–	802.11 a/b/g/n/ac	–	802.11 a/b/g/n/ac
USB Ports	1		1	
Console (RJ45)	1		1	
Internal Storage	–		128 GB	
System Performance				
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	3 / 3 / 3 Gbps			
Firewall Latency (64 byte UDP packets)	3 µs			
Firewall Throughput (Packets Per Second)	4.5 Mpps			
Concurrent Sessions (TCP)	1.3 Million			
New Sessions/Second (TCP)	30,000			
Firewall Policies	5,000			
IPsec VPN Throughput (512 byte packets)	2 Gbps			
Gateway-to-Gateway IPsec VPN Tunnels	200			
Client-to-Gateway IPsec VPN Tunnels	500			
SSL-VPN Throughput	150 Mbps			
Concurrent SSL-VPN Users (Recommended Maximum)	100			
IPS Throughput (HTTP / Enterprise Mix) [1]	1,400 / 350 Mbps			
SSL Inspection Throughput [2]	340 Mbps			
Application Control Throughput [3]	550 Mbps			
NGFW Throughput [4]	250 Mbps			
Threat Protection Throughput [5]	180 Mbps			
CAPWAP Throughput [6]	1.5 Gbps			
Virtual Domains (Default / Maximum)	10 / 10			
Maximum Number of FortiAPs (Total / Tunnel Mode)	10 / 5			
Maximum Number of FortiTokens	100			
Maximum Number of Registered FortiClients	200			
High Availability Configurations	Active / Active, Active / Passive, Clustering			
Dimensions				
Height x Width x Length (inches)	1.5 x 8.5 x 8.3			
Height x Width x Length (mm)	38 x 216 x 160			
Weight	1.9 lbs (0.9 kg)			
Form Factor	Desktop			
Environment				
Power Required	100–240V AC, 50–60 Hz			
Maximum Current	110V AC / 1.5 A, 220V AC / 0.75 A	115V AC / 0.9A, 230V AC / 0.8A	115V AC / 0.9A, 230V AC / 0.6A	115V AC / 0.9A, 230V AC / 0.6A
Power Consumption (Average / Maximum)	11.7 / 14 W	12.8 / 15.2 W	11.9 / 14.3 W	13 / 16 W
Heat Dissipation	40 BTU/h	52 BTU/h	49 BTU/h	55 BTU/h
Operating Temperature	32–104°F (0–40°C)			
Storage Temperature	-31–158°F (-35–70°C)			
Humidity	20–90% non-condensing			
Operating Altitude	Up to 7,400 ft (2,250 m)			
Compliance				
Safety	FCC Part 15 Class B, C-Tick, VCCI, CE, UL/cUL, CB			
Certifications				
	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN			

Note: All performance values are "up to" and vary depending on system configuration. IPsec VPN performance is based on 512 byte UDP packets using AES-256+SHA1. 1. IPS performance is measured using 1 Mbyte HTTP and Enterprise Traffic Mix. 2. SSL Inspection is measured with IPS enabled and HTTP traffic, using TLS v1.2 with AES256-SHA. 3. Application Control performance is measured with 64 Kbytes HTTP traffic. 4. NGFW performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix. 5. Threat Protection performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix. 6. CAPWAP performance is based on 1444 byte UDP packets.

INFORMACION DE COMO ORDENAR

Product	SKU	Description
FortiGate 60E	FG-60E	10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port). Maximum managed FortiAPs (Total / Tunnel) 10 / 5.
FortiWiFi 60E	FWF-60E	10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port), Wireless (802.11a/b/g/n/ac). Maximum managed FortiAPs (Total / Tunnel) 10 / 5.
FortiGate 61E	FG-61E	10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port), 128 GB SSD onboard storage. Maximum managed FortiAPs (Total / Tunnel) 10 / 5.
FortiWiFi 61E	FWF-61E	10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port), Wireless (802.11a/b/g/n/ac), 128 GB SSD onboard storage. Maximum managed FortiAPs (Total / Tunnel) 10 / 5.

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

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6395.2788

LATIN AMERICA SALES OFFICE
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
United States
Tel: +1.954.368.9990

Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

FST-PROD-DS-GT6OE
FGFWF-60E-DAT-R6-201702

la ciudad de San salvador, a las catorce horas y veinticinco minutos del día veinte de junio del año dos mil dieciocho. Ante mí, [redacted], Notario, de este domicilio, con Documento Único de Identidad Número [redacted].

Vista la anterior traducción del idioma Inglés al Castellano por la Ingeniera [redacted] se da por aprobada firmada y sellada por la suscrita Notario. Devuélvanse a la interesada las presentes diligencias para los efectos consiguientes. DOY FE.

[redacted]

[redacted]

[redacted]

00000082

FortiOS™ 6.0

Sistema Operativo de Red Fortinet



Controle todas las capacidades de seguridad y de red en todos sus elementos de Fortinet Security Fabric con un sistema operativo intuitivo. Mejore su protección y visibilidad a la vez que reduce los gastos operativos y ahorro de tiempo con una solución de firewall empresarial de próxima generación verdaderamente consolidada. FortiOS permite la visión de Fortinet Security Fabric para una protección mejorada del IoT hacia la nube.

Amplia visibilidad

FortiOS ofrece a los equipos de TI una visión integral de los dispositivos, el tráfico, las aplicaciones y los eventos, y la capacidad de detener una amenaza en cualquier punto de su cadena de ataque.

Deteccion Integrada

Admite la detección coordinada de amenazas avanzadas a través de análisis sofisticados y centralizados.

Respuestas Automatizadas

Como parte de la última versión de Fortinet Security Fabric, FortiGate puede proporcionar automáticamente una evaluación de confianza continua para brindar respuesta inmediata a las amenazas detectadas.

¿Qué hay de nuevo? Lo más destacado

- Automatización de la tela de seguridad
- Indicador de cuarentena de compromiso (IOC) y prohibición de IP
- Ranking de calificaciones de seguridad y reglas de calificación ampliadas
- Etiquetado de Activos
- Inteligencia de múltiples rutas para SD-WAN
- Compatibilidad con varias nubes con conectores de Fabrica
- Listas negras de filtro web externo
- Nuevos Servicios FortiGuard

[redacted]

00000083

VISIÓN EN CONJUNTO

Introducción a FortiOS 6.0



A medida que las empresas buscan transformar todo, desde sus modelos operativos empresariales hasta los métodos de prestación de servicios, están adoptando tecnologías como la informática móvil, la IoT y las redes de múltiples nubes para lograr la agilidad, la automatización y la escala del negocio.

El aumento de la conectividad digital de las organizaciones está impulsando el requisito de una transformación de seguridad, donde la seguridad se integra en aplicaciones, dispositivos y redes en la nube para proteger los datos empresariales distribuidos en estos entornos complejos.

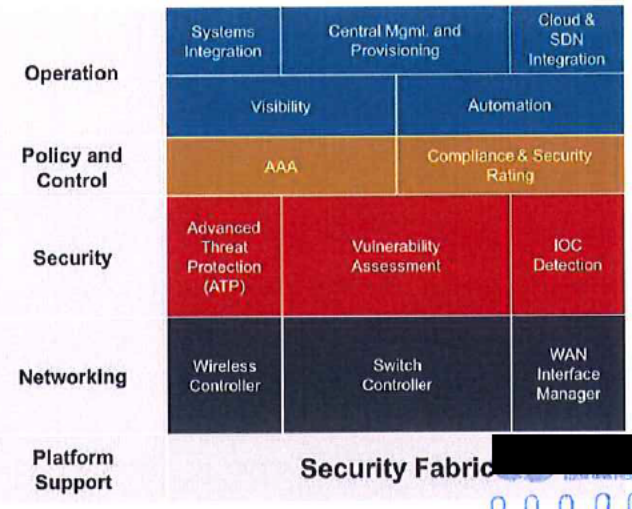
FortiOS ™ 6.0 ofrece cientos de nuevas características y capacidades que fueron diseñadas para proporcionar una amplia visibilidad, inteligencia de amenaza integrada y respuesta automatizada requerida para el negocio digital.

Fortinet Security Fabric, fortalecido por FortiOS 6.0, es un marco inteligente diseñado para seguridad escalable e interconectada combinada con alta conciencia, inteligencia de amenazas procesable y estándares API abiertos para máxima flexibilidad e integración para proteger incluso los entornos empresariales más exigentes. Las tecnologías de seguridad de Fortinet han obtenido las certificaciones independientes sobre eficacia y el rendimiento de la seguridad en la industria. Fortinet Security Fabric cierra las brechas dejadas por productos y plataformas de puntos heredados al proporcionar la protección amplia, potente y automatizada que las organizaciones de hoy en día requieren en sus entornos físicos y virtuales, desde el punto final hasta la nube.

FortiOS 6.0 Anatomia

FortiOS es un sistema operativo reforzado y especialmente diseñado que es la base de software de FortiGate. Controle todas las capacidades de seguridad y de red en todos sus FortiGates en toda su red con un sistema operativo intuitivo. FortiOS ofrece un amplio conjunto de funciones que permite a las organizaciones de todos los tamaños implementar la configuración de puerta de enlace de seguridad que mejor se adapte a sus entornos. A medida que evolucionan los requisitos, puede modificarlos con interrupciones y costos mínimos.

Configuration	Log & Report	Diagnostics	Monitoring
Policy Objects	Device Identification	SSL Inspection	Actions
Anti-Malware	IPS & DoS	Application Control	Web Filtering
Firewall	VPN	DLP	Email Filtering
SD WAN	Explicit Proxy	IPv6	High Availability
Routing/NAT	L2/Switching	Offline Inspection	Essential Network Services
Physical Appliance (+SPU)	Virtual System	Hypervisor	Cloud



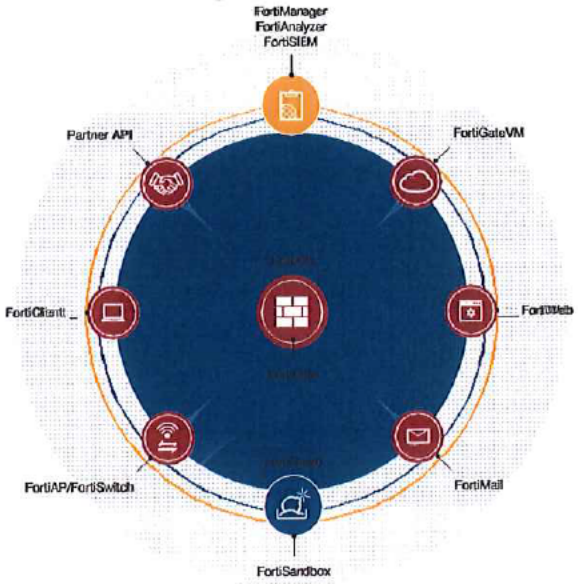
CARACTERISTICAS

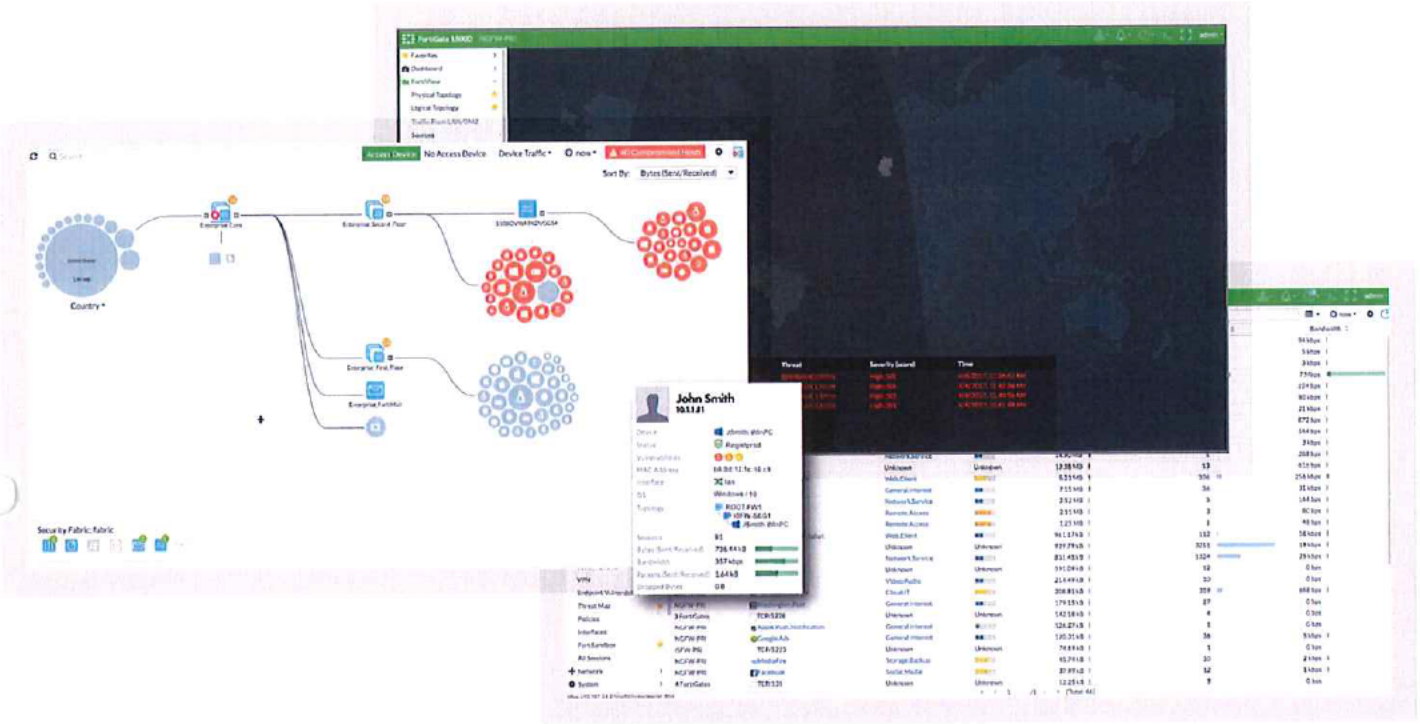
Fábrica de Seguridad

Integración con FortiGate

Fábrica de Seguridad permite que la seguridad se expanda y se adapte dinámicamente a medida que se agregan más cargas de trabajo y datos, y al mismo tiempo, sigue y protege datos, usuarios y aplicaciones a medida que avanzan y retroceden entre IoT, dispositivos inteligentes y la nube. En todo el entorno de la red.

Se puede implementar un firewall FortiGate en el corazón de Security Fabric, expandiendo su alcance de seguridad a través de la visibilidad y el control, mediante la estrecha integración con otros productos FortiGates y Fortinet, además de soluciones Fabric-Ready.





FortiView, Topología y Mapa de Amenazas

Visibilidad

FortiView, en FortiOS 6.0, le proporciona una visibilidad de 360 ° del tráfico de su red. Con un solo clic, puede ver el tráfico por origen, destino, aplicación, amenaza, interfaz, dispositivo, política y país. Las visualizaciones gráficas, como los mapas de país y de topología y los gráficos de burbujas basados en el volumen, están disponibles además de las vistas completas de tablas. Estos le permiten identificar problemas de forma rápida e intuitiva.

ASPECTOS SOBRESALIENTES

Calificación de Seguridad

La auditoría de Security Fabric es una característica que le permite analizar su despliegue de Security Fabricpara identificar vulnerabilidades potenciales y resaltar las mejores prácticas que usted puede usar para mejorar la seguridad y el desempeño en general de su red. También, al chequear su puntaje de Security Fabric, el cual está determinado en base a cuantos chequeos su red pase o falle durante la auditoría, usted puede estar seguro de que su red está volviéndose más segura con el tiempo.



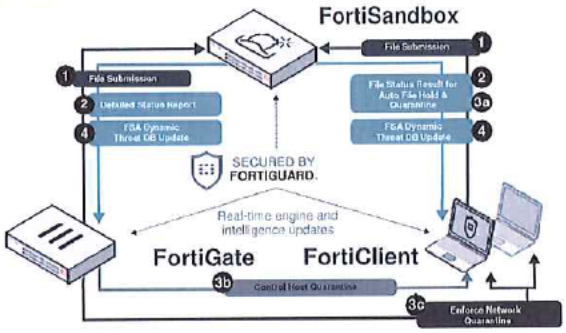


Automatización

Puntadas y nuevos flujos de trabajo automatizados definidos por el administrador que usan declaraciones if/then para hacer que el FortiOS responda automáticamente a un evento en una forma preprogramada. Porque las puntadas son parte de la security fabric, usted puede establecer puntadas para cualquier dispositivo en la Security Fabric.

Protección de Amenazas Avanzada

Fortinet ofrece la Protección Contra Amenazad Avanzadas automatizada más integrada (ATP)disponible a través de un marco ATP que incluyeal FortiGate, FortiSandbox, FortiMail, FortiClient y FortiWeb. Estos productos trabajan fácilmente, juntos, para proveer protección de bucle cerrado a través de todos los vectores de ataque más comunes.



Consulta

1. Envío de Archivo para análisis
2. Los análisis de resultados respectivos son regresados

Remediación

3a. Auto cuarentena de archivos en el host con la opción de mantener el resultado de la unidad de archivo

3b. Cuarentena de Host Manual por el administrador

3c. Cuarentena de IP origen manual usando el firawall

Protección

4. Actualización de base de datos de amenazas dinámica proactiva para el Gateway y el Host

CARACTERÍSTICA	ASPECTOS SOBRESALIENTES	LA VENTAJA DE FORTINET
Integración del sistema	▪ Salida de monitoreo basada en estándares – Netflow/Sflow SNMP, soporte de Syslog para sistemas SIEM y de almacenamiento de logs externos (de terceros)	§ logs y salidas detalladas proveen más vistas de modo que las organizaciones puedan identificar de forma precisa y rápida y resolver los incidentes o problemas.
	▪ Integración con el Security Fabric con una alianza de productos y tecnologías Fortinet	§ Habilidad para reusar los sistemas existentes de la red baja el TCO y optimiza los procesos.
Administración y provisionamiento centrales	▪ Soporte de Automatización de Fortinet/terceros y servicios de portal a través de APIs y secuencias de comandos CLI	§ APIs exhaustivos y comandos CLI ofrecen la habilitación de servicios ricos en características.
	▪ Características de despliegue rápido incluyendo soluciones de provisionamiento basadas en la nube	§ Opciones de despliegue raídos exhaustivas ahorran tiempo y costos.
	▪ Plataforma de comunidad de desarrolladores y opciones de servicios profesionales para integraciones complejas	§ La red de desarrolladores de Fortinet (FNDN) empodera a los proveedores de servicios y las empresas, grandes, con la implementación compartida/personalización/integración de conocimiento.
Integración de Nube y SDN	▪ Soporte multi nube a través de la integración con Openstack, NSXde VMware, Los servicios virtualizados Nuage y la infraestructura ACI de Cisco	§ Integración de capacidades SDN robustas y exhaustivas le permite a las organizaciones implementar soluciones de nube seguras sin comprometer la agilidad.
	▪ Nuevo: Facilidad de configuración con soporte de GUI y objetos de dirección dinámicos	

ASPECTOS SOBRESALIENTES

CARACTERÍSTICA	ASPECTOS SOBRESALIENTES	LA VENTAJA DE FORTINET
Visibilidad	§ Visores profundos y de topología ilustran el estatus en tiempo real y en forma histórica de las amenazas y el uso de la red con información contextual exhaustiva ▪ Vistas de datos agregadas con un control remoto de los FortiGates descendientes	Remediación de un clic contra orígenes/destinatinos listados ofrece una protección precisa y rápida contra amenazas y abusos ▪ Sistema de puntaje de amenazas único correlaciona las amenazas con usuarios particulares para priorizar las investigaciones. ▪ Vistas con la amplitud de la Security Fabric expanden la visibilidad más allá de una entidad de seguridad única, permitiéndole a las organizaciones encontrar los problemas rápidamente y resolverlos.
Automatización	§ NUEVO: Automatización del flujo de trabajo basada en Wizard que desempeña las acciones apropiadas en base a desencadenadores definidos, a través de la Security Fabric ▪ NUEVO: Pone en cuarentena a los hosts comprometidos de forma automática usando el FortiClient a través de EMS o una conexión a través de un FortiSwitch y FortiAP	▪ Reduciendo la exposición a riesgos, y reemplazando los procesos de seguridad manuales con automatización, también le ayuda a solventar los desafíos organizacionales de presupuestos más estrechos y el hecho de no poseer personal calificado.
Autenticación Autorización y Contabilidad (AAA por sus siglas en inglés)	▪ Interactúa con el FortiAuthenticator y una amplia variedad de sistema de administración de identidad externos para facilitar los procesos de autenticación de usuarios. ▪ Métodos de adquisición de identidad de un solo inicio de sesión amplios, incluyendo Windows AD, servidores terminales, portales de acceso y servicios de correo ▪ Servidor de token integrado que administra tanto tokens físicos como móviles para usarlos con varios requerimientos de autenticación FortiOS tales y como el acceso VPN y la administración de un FortiGate.	▪ FortiOS se integra con una gran variedad de servicios AAA para facilitar el control de admisión de usuario desde varios puntos de entrada, dando a los usuarios una experiencia simplificada mientras se implementa una seguridad mejor. ▪ Implementa fácilmente la autenticación de dos factores para el acceso de usuarios y administradores a bajo costo.
Calificación de cumplimiento y seguridad	§ Chequeo periódico de la configuración del sistema usando una lista de chequeo de cumplimiento PCI predefinida ▪ Cumplimiento de dispositivo final: asignación de perfil de chequeo de postura en base a dispositivos/grupos de usuarios ▪ Chequeo del estatus de la configuración de seguridad FortiGate y la vulnerabilidad del cliente, en la amplitud completa de la Security Fabric ▪ NUEVO: Clasificaciones de las calificaciones de seguridad contra los pares	▪ Automatiza la auditoría de cumplimiento, lo cual libera recursos de administración. ▪ Ejecución de seguridad de usuarios móviles simplificada al distribuir y actualizar los perfiles de seguridad de los clientes, que se encuentran acordes a la protección Gateway, fácilmente. ▪ Verifica rápidamente el estatus y la conectividad de sus dispositivos configurados y conectados dentro de la Security Fabric e identifica cualquier brecha que pudiera dejarlo potencialmente en un riesgo mayor.
Protección de Amenazas Avanzadas	§ Opciones de Antivirus basado en flujo y en proxy para poder elegir entre protección y desempeño ▪ Cuarentena de archivos local (para modelos con almacenamiento) ▪ Capacidad antibot usando una base de datos de reputación IP corta la comunicación Botnet a servidores C&C ▪ Recibe remediaciones dinámicas, (checksums de archivos y URLs maliciosas) actualizaciones de bases de datos y reportes de análisis detallados desde la solución de análisis de archivos de Fortinet, externa. (FortiSandbox)	▪ Apoyado por servicios de investigación de antivirus probados y validados por la industria ▪ Habilidad para adoptar un marco ATP robusto que llega a los usuarios móviles y las oficinas de sucursal, detectando y previniendo ataques avanzados que pudieran traspasar las barreras tradicionales, al examinaar archivos desde varios vectores, incluyendo archivos cifrados
Evaluación de Vulnerabilidades	§ Vistas de vulnerabilidad de dispositivos finales que presentan a los clientes considerados como vulnerables, con detalle.	▪ Identifica fácilmente hosts vulnerables a través de la Security Fabric.
Detección IOC	§ NUEVO: La integración del servicio IOC muestra datos de detección IOC desde un FortiAnalyzer en la FortiView y bs mapas de topología	▪ Los administradores pueden identificar fácilmente hosts sospechosos y ponerlos en cuarentena rápida o automáticamente.
Controlador Inalámbrico	§ Controlador inalámbrico integrado para el amplio rango de factores de forma de APs de Fortinet, incluyendo para interiores, exteriores y modelos remotos, sin licencias adicionales o cargos por componente ▪ Funcionalidad de administración inalámbrica de clase empresarial, incluyendo protección de APs bandidos, seguridad inalámbrica, monitoreo, y reportería ▪ Soporte de 802.3az en los APs Wifi de onda 2 ▪ Administra FortiAPs basados en la nube, distribuidos	▪ El controlador inalámbrico integrado en la consola FortiGate provee una verdadera administración de un solo panel para obtener facilidad de uso y un TCO más bajo.
Controlador de Conmutador	§ Controlador de conmutador integrado para los conmutadores de acceso de Fortinet sin licencias adicionales o cargos por componente § Soporte de configuración GUI mejorado	▪ Expande la seguridad al nivel de acceso para detener a las amenazas y proteger a las terminales entre sí
Administrador de Interfaz WAN	§ Soporta el uso de módems 3G/4G a través del puerto USB o FortiExtender	§ Les permite a las organizaciones usar o agregar conectividad 3G/4G para conexiones WAN mientras mantiene el control de acceso y la definición de uso para esos enlaces

ASPECTOS SOBRESALIENTES

Operación

FortiOS provee un amplio set de herramientas de operación que hace que la identificación y la respuesta a problemas de seguridad y red, sean efectivas. Las operaciones de seguridad están más optimizadas con automatizaciones, que contribuyen a resoluciones de problemas más rápidas y más precisas.

CARACTERÍSTICA	ASPECTOS SOBRESALIENTES	LA VENTAJA DE FORTINET
Configuración	§ Amplia variedad de herramientas de configuración — Software de , cliente, UI Web UI y CLI ▪ Facilidad de uso con una GUI y Wizards intuitivos ▪ Acceso de un solo clic y acciones entre visores de logs, FortiView tablas de políticas y más ▪ Panel de objetos inteligente para la configuración y edición de políticas ▪ NUEVO: Etiquetación de recursos	▪ La herramienta de configuración única: FortiExplorer le permite a los administradores accesar rápidamente a las configuraciones, incluyendo el acceso mediante teléfonos y tablets. ▪ Wizards VPN facilitan una configuración fácil, incluyendo clientes móviles populares y otros gateways VPN de otros proveedores. ▪ Acceso de un solo clic y acciones útiles llevan a los administradores a los siguientes pasos rápida y precisamente para mitigar a las amenazas o resolver los problemas velozmente
Almacenamiento de logs y reportería	§ Logs detallados y reportes fuera de la caja que son esenciales para el cumplimiento, auditorías y propósitos de diagnóstico ▪ Almacenamiento de logs en tiempo real hacia el FortiAnalyzer y la FortiCloud ▪ Soporte del formato de eventos común (CEF) ▪ Consolidación del almacenamiento de logs dentro de la Security Fabric	▪ Incluye información contextual profunda, incluyendo los detalles del dispositivo de origen y un fuerte rastreo de auditoría ▪ Un editor de reportes GUI ofrece reportes altamente personalizables ▪ La administración de logs holística simplifica la configuración y garantiza que la información crítica de cada FortiGate sea recolectada centralmente y esté disponible para el análisis. Esto cierra cualquier brecha en inteligencia. ▪ Herramientas de diagnóstico exhaustivas le ayudan a las organizaciones a remediar rápidamente los problemas e investigar situaciones anormales
Diagnostics	§ Comandos de diagnóstico CLI, rastreador de sesiones y captura de paquetes para resolver los problemas de hardware, del sistema, y la red ▪ Conjunto de pruebas de hardware en la CLI ▪ Rastreador GUI de políticas y enrutamiento	▪ Vista de tablero NOC le permite mantener la información de misión crítica a la vista en todo momento. Widgets interactivos evaden los finales muertos durante sus investigaciones manteniendo al análisis moviéndose rápida y fluidamente.
Monitoring	§ Monitores en tiempo real ▪ Tablero NOC ▪ NUEVO: Notificación de IOS por empuje mediante la aplicación FortiExplorer	

Políticas y Control

Un FortiGate le provee un punto de ejecución de políticas valioso en su red, donde usted puede controlar su tráfico de red y aplicar tecnologías de seguridad. Con FortiOS usted puede configurar políticas consolidadas que integran controles de seguridad granulares. Cada servicio de seguridad es administrado a través de un paradigma de control similar y puede instalarse fácilmente en una política consolidada. Controles de jalar y soltar le permiten crear políticas fácilmente, y los atajos de navegación de un solo clic le permiten poner dispositivos finales en cuarentena o editar políticas, rápidamente.

CARACTERÍSTICA	ASPECTOS SOBRESALIENTES	LA VENTAJA DE FORTINET
Objetos de Política	▪ Objetos de dirección definidos por IP Geográfica y FQDN para rastrear inteligentemente IPs dinámicas/Rangos de IP ▪ Base de datos de servicio de Internet: Base de datos actualizada dinámicamente que provee una lista de aplicaciones de nube populares con su información vital que usted puede usar para la configuración de políticas, enrutamiento y configuraciones de balanceo de carga	§ Rango exhaustivo de tipos de objeto que facilitan los requerimientos de red dinámicos y granulares de hoy en día
Identificación de dispositivos	▪ Identificación y control del acceso de red para distintos tipos de dispositivos presentes en la red ▪ Identificación y administración de dispositivos mejorada	§ Empodera a las organizaciones para agregar seguridad crítica a los entornos BYOD de hoy en día al identificar y controlar dispositivos personales
Inspección SSL	▪ Examina efectivamente el tráfico cifrado SSL con varios controles de seguridad, tales y como AV y DLP ▪ Inspección SSL de alto desempeño con procesadores de contenido ▪ Base de daros de sitios con buena reputación, para las excepciones	§ Identifica y bloquea amenazas escondidas dentro del tráfico cifrado si impactar significativamente en el desempeño
Acciones	▪ Implementa políticas de seguridad que usan una combinación de objetos de origen, IPs, usuarios y/o dispositivos ▪ Notificaciones altamente personalizables son enviadas cuando las actividades de los usuarios no están permitidas ▪ Pone en cuarentena a los Usuarios/Atacantes de forma manual o automática ▪ Direcciona a los Forticlient registrados hacia la cuarentena de host	§ Política de configuración flexible usando elementos identificados adicionales y notificaciones de usuarios activos asisten a la seguridad de las organizaciones, mientras robustas características de cuarentena le ayudan a mitigar las amenazas [redacted]

ASPECTOS SOBRESALIENTES

Seguridad

Los laboratorios FortiGuard proveen los servicios de seguridad líderes de la industria y la inteligencia de amenazas entregada a través de las soluciones Fortinet. FortiOS administra el amplio rango de servicios FortiGuard disponibles para la plataforma FortiGate, incluyendo control de aplicaciones, prevención de intrusiones, filtrado web, antivirus, protección contra amenazas avanzadas, inspección SSL y seguridad móvil. Licencias de servicio están disponibles a la carta o en un bundle efectivo en relación con el costo para obtener un despliegue de flexibilidad máxima.

Efectividad de seguridad líder en la industria

Las soluciones Fortinet están validadas consistentemente para una seguridad líder en la industria en las pruebas de la industria hechas por los laboratorios NSS para IPS y el control de aplicaciones, por Virus Bulletin en la comparativa VB100 de pruebas de la industria para antimalware y por AV Comparatives.

- Firewall de Próxima Generación recomendado con una calificación de seguridad casi perfecta, 99.47%. (Prueba de NGFW realizada por los laboratorios NSS en el 2017 para el FortiGate 600D y 3200D)
- Sistema de Prevención de Brechas Recomendado con una detección en general del 99%. (Prueba de Sistemas de Prevención de Brechas realizada por los laboratorios NSS en el 2017 para el FortiGate con FortiSandbox)
- Gateway de Seguridad para Centro de Datos Recomendado con una efectividad de seguridad del 97.87% y 97.97%. (Prueba para Gateway de Seguridad para Centro de Datos realizada por los laboratorios NSS en el 2017 con los FortiGate 7060E y 3000D)
- IPS de Próxima Generación recomendado con una efectividad de seguridad en general del 99.71%. (Prueba de IPS de Próxima Generación realizada por los laboratorios NSS en el 2017 con el FortiGate 600D)
- Firewalls de red certificados por ICSA, IPS de red, IPsec, VPN SSL-TLS y antivirus

CARACTERÍSTICA	ASPECTOS PRINCIPALES	LA VENTAJA DE FORTINET
Anti-Malware	§ Opciones de Antivirus basado en flujo y basado en proxy para poder elegir entre protección y desempeño ▪ Capacidad anti-bot usando una base de datos de reputación IP que finaliza la comunicación botnet a servidores C&C ▪ Reciba remediación dinámica. (checksum de archivos maliciosos y URLs) Actualizaciones de base de datos y reportes de análisis detallados provenientes de la solución de análisis de archivos de Fortinet, externa (FortiSandbox) ▪ NUEVO: Protección de Brote de Virus como una capa adicional de protección proactiva que se dirige al malware nuevo; comparación y detección de amenazas usando una base de datos de checksums en tiempo real de FortiGuard ▪ NUEVO: El Desarme y Reconstrucción de contenido (CDR) remueve el contenido que puede ser víctima de un exploit antes de que llegue a los usuarios	▪ Soportado por servicios de investigación de AntiVirus probados y validados por la industria ▪ Habilidad para adoptar un marco ATP robusto que alcanza a los usuarios móviles y las oficinas sucursales detectando y previniendo ataques avanzados que podría evitar las defensas tradicionales al examinar los archivos provenientes de varios vectores, incluyendo archivos cifrados
IPS y DoS	§ Firmas regulares y basadas en velocidad, soportadas por protección de amenazas de cero días e investigación para una efectiva implementación de IPS ▪ Una protección de DoS integrada le defiende contra las conductas de tráfico anormales ▪ Referencia CVE para firmas de IPS	▪ Calidad de protección probada con el premio "Recomendado por NSS" por una cobertura y una relación costo/desempeño superior ▪ Se adapta a las necesidades de la empresa con características de IPS y capacidades NGIPS completas tal y como visibilidad contextual ▪ Soporta varios requerimientos de despliegue de red, tal y como el modo de sniffer Y es completamente compatible con el FortiBridge Activo-Pasivo o los puertos de bypass integrados para un modelo seleccionado
Control de Aplicaciones	§ Detecta y actúa contra el tráfico en base a aplicaciones mientras provee visibilidad sobre el uso de la red ▪ Control altamente granular sobre aplicaciones de nube populares, tales como SalesForce, Google Docs y Dropbox	▪ Cobertura superior, incluyendo tanto aplicaciones de escritorio como móviles, permitiendo una mejor administración de las políticas de acceso de red. ▪ Aplica inspecciones de aplicación más profundad para obtener mejor control y visibilidad mientras más empresas confían en los servicios de nube pública
Filtrado Web	§ Solución de filtrado URL de clase empresarial que incluye cuotas, anulaciones por usuario, búsqueda segura transparente y almacenamiento de logs de palabras clave ingresadas en un motor de búsqueda ▪ Cobertura superior con calificaciones de URL de más de 70 lenguajes e identifica sitios redirigidos (en cache y traducidos)	▪ Capacidades de evasión anti-proxy multicapa con control de aplicaciones e IPS integrados le permiten a las organizaciones implementar controles de uso web estrictos

[redacted]

00000089

ASPECTOS SOBRESALIENTES

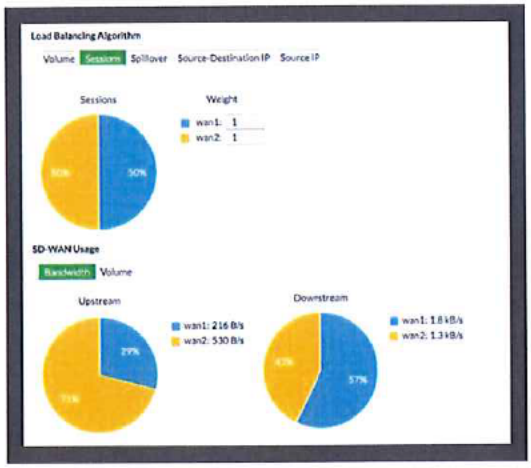
CARACTERÍSTICA	ASPECTOS SOBRESALIENTES	LA VENTAJA DE FORTINET
Firewall	§ Firewall de alto desempeño con dispositivo empoderado por SPU ▪ Administrador de políticas fácil de usar con opciones de Vista de sección Única o Global ▪ NGFW con modo basado en políticas	▪ El mejor dispositivo de Firewall de la industria con un radio de costo-desempeño superior
VPN	§ Características de clase empresarial únicas para varios tipos de configuración de VPN ▪ Wizards de VPN SSL e IPsec ▪ NUEVO: VPN de un solo clic asistida por la nube	▪ El desempeño inigualable del FortiGate para las VPN le permite a las organizaciones establecer comunicaciones seguras y privacidad de datos entre múltiples redes y hosts al aprovechar procesadores de seguridad a la medida (SPUs) para acelerar el cifrado y el descifrado del tráfico de red
DLP	§ Monitoree el tráfico de red y no permita que la información sensible deje la red al comparar contra definiciones de formato de archivo y contenido ▪ La Herramienta de Marca de Agua FortiExplorer le permite a los organizadores aplicar el marcado de documentos para DLP	▪ Prevenga que la información sensible deje la red, fácilmente y de forma efectiva en relación al costo
Filtrado de Email	§ Filtros de spam altamente efectivos multicapa con bajos falsos positivos	§ Solución antispam eficiente en relación con el costo para las organizaciones pequeñas o o las oficinas sin que se requiera invertir en un sistema adicional

Redes

Con FortiOS usted puede administrar sus redes y su seguridad en un OS nativo consistente en el FortiGate. FortiOS entrega un amplio rango de capacidades de red, incluyendo un enrutamiento exhaustivo, NAT, conmutación, Wi-Fi, WAN, balanceo de carga, y alta disponibilidad, haciendo al FortiGate una elección popular para las organizaciones que quieren consolidar sus funciones de redes y seguridad.

SD WAN

El SD-WAN de FortiGate integra capacidades de WAN de próxima generación y seguridad en una única solución de borde WAN multi-camino. Un SD-WAN seguro detecta a las aplicaciones en los dispositivos de borde y mantiene el desempeño de las aplicaciones alto con una automatización de controlador de camino WAN integrada. Con un NGFW, integrado, es más fácil permitir el acceso de Internet directo y continúa manteniendo una postura de seguridad alta con una complejidad reducida.



CARACTERÍSTICA	ASPECTOS SOBRESALIENTES	LA VENTAJA DE FORTINET
Enrutamiento / NAT	▪ Soporte de protocolos de enrutamiento exhaustivos y NAT ▪ Redirección de tráfico con soporte de ICAP y WCCP	§ Características de enrutamiento de alto rango que cumplen con los requerimientos de resistencia de red de carriers y empresas
L2 / Conmutación	▪ Habilidad para elaborar conmutadores de software o emular conmutadores VLAN a partir de las interfaces ▪ Soporta puertos SPAN y agregación de puertos con múltiples interfaces ▪ Implementa modos de control de admisión en las interfaces tales y como 802.1x o el portal captivo ▪ WiFi exhaustivo y opciones de configuración de interfaz WAN ▪ Soporte de VXLAN ▪ NEW: Soporte de VLAN EMAC	§ Configuraciones de interfaz flexibles ofrecen varias posibilidades de configuración que se adaptan mejor a los requerimientos de red de una organización mientras proveen seguridad de acceso opcional
Inspección fuera de línea	▪ El modo de sniffer permite el monitoreo de las amenazas y el uso, en relación con las actividades de red, fuera de línea	§ El modo fuera de línea provee flexibilidad cuando se despliega en redes críticas existentes, donde una solución de seguridad en línea aún no es apropiada

CARACTERÍSTICA	ASPECTOS SOBRESALIENTES	LA VENTAJA DE FORTINET
SD WAN	§ Control de camino WAN inteligente con la habilidad de dirigir el tráfico entre los enlaces WAN basado en aplicaciones y usuarios/grupos de usuarios (más de 3,000) ▪ Mide las transacciones de las aplicaciones tal y como la latencia, dijitter y la perdida de paquetes, más una conmutación por error automática, integrada, para determinar los caminos preferidos y mantener un desempeño de aplicaciones, óptimo, para las aplicaciones críticas del negocio ▪ Usa QoS, Modelado de tráfico y enrutamiento de políticas para la administración del ancho de banda ▪ Permite VPN IPSEC para los enlaces WAN y saca ventaja del desempeño de VPN más alto de la industria y una alta escalabilidad de túnel ▪ Optimización WAN de par a par y usuario remoto y tecnologías de almacenamiento en memoria cache de byte	▪ Amplia cobertura de la visibilidad de aplicaciones y clasificación de primer paquete para una eficiente adopción de SD-WAN ▪ NGFW y SD-WAN integrados en el mismo dispositivo reducen aún más el TCO y la complejidad ▪ La automatización del controlador de camino WAN continúa proveyendo un alto desempeño de aplicaciones ▪ El desempeño de VPN IPSEC más alto de la industria ▪ Despliegue de cero toques para un SD-WAN de Borde
Alta Disponibilidad	§ Soporte para VRRP estándar de la industria y varias soluciones propietarias con la habilidad de combinar más de una solución de alta disponibilidad en una configuración única	▪ Ofertas de alta disponibilidad flexibles le permiten a las organizaciones elegir las soluciones más adecuadas en base a los entornos de red y los requerimientos de SLA
IPv6	§ Soporte IPv6 exhaustivo para enrutamiento, NAT, políticas de seguridad y más	▪ Opciones de modo de operación proveen flexibilidad cuando se despliegan en redes existentes o nuevas, reduciendo los requerimientos de cambio de red
Proxy Explicito	§ HTTP y HTTPS explícitos, FTP sobre HTTP, o uso de proxy SOCKS del tráfico IPv4 e IPV6 en una o más interfaces ▪ Proxy web transparente	▪ Un proxy web explícito de clase empresarial, integrado, provee el uso de proxys HTTP y HTTPS con los beneficios agregados de la seguridad UTM y la identidad de usuario
Servicios de Red Esenciales	§ Una amplia variedad de servicios de red tales y como DHCP, servidor DNS, servidor NTP, etc.	▪ Capacidades integradas, listas para usarse, les permiten a las organizaciones proveer rápidamente los servicios de red necesarios a las terminales internas o integrarse con otros dispositivos de red

Soporte de Plataforma

Desempeño



Los dispositivos FortiGate entregan hasta 5 veces el desempeño de firewall de próxima generación y 10 veces el desempeño de firewall que las plataformas con precios equivalentes de otros proveedores. Los altos niveles de desempeño en el FortiGate están basados en una arquitectura de Procesamiento de Camino Paralelo en el FortiOS que aprovecha el desempeño, los motores de seguridad optimizados, y los procesadores de red y contenido desarrollados a la medida. Por lo tanto, el FortiGate ha alcanzado el mejor resultado en el valor de costo por desempeño en Mbps.

Flexibilidad de Despliegue Suprema

Proteja su red entera adentro y afuera a través de una estrategia de segmentación de red dirigida por políticas haciendo uso de la solución Fortinet. Es fácil desplegar Firewall optimizados por segmento, aprovechando el amplio rango de plataformas FortiGate y la flexibilidad del FortiOS para proteger los segmentos de red internos, el perímetro de red, las ubicaciones distribuidas, las nubes públicas y privadas y el centro de datos — asegurando que usted tenga la mezcla correcta de capacidades y desempeño para cada modo de despliegue

CARACTERÍSTICA	ASPECTOS SOBRESALIENTES	LA VENTAJA DE FORTINET
Dispositivo Físico (+SPU)	▪ Integración con arquitecturas de hardware propietario que incluye componentes de aceleración (SPU) y procesadores multi-núcleo	▪ Una integración de Software y Hardware superior, asegura el uso más óptimo de los componentes de hardware, proveyendo la mejor relación costo-desempeño para los clientes
Sistemas Virtuales	▪ Dominios Virtuales (VDOMs): Componentes de FortiOS virtualizados para múltiples sistemas lógicos en un dispositivo virtual único o un dispositivo físico ▪ Opciones de VDOM Proxy y basadas en flujo para simplificar las configuraciones del perfil de seguridad ▪ NUEVO: Perfiles de Seguridad Globales	▪ Ofrece a los MSSPs y a las organizaciones grandes la habilidad de ejecutar instancias separadas de FortiOS para un entorno multi-inquilino o para consolidar varias gateways de seguridad para obtener un TCO menor
Hipervisor	▪ Soporte para plataformas de hipervisor populares, incluyendo vSphere de VMware, Citrix y Xen de fuente abierta, KVM, e Hiper-V de MS	▪ Una administración y características consistentes entre los dispositivos físicos y virtuales reduce el costo de administración y simplifica los despliegues
Nube	▪ Soporte de servicios de nube pública: Servicios Web de Amazon (AWS por sus siglas en inglés) y Microsoft Azure	▪ Una administración y características consistentes entre plataformas locales y en la nube reduce el costo de administración y simplifica los despliegues

[redacted]

00000091

ESPECIFICACIONES

Security Fabric

INTEGRACIÓN DEL SISTEMA

Monitoreo del Sistema SNMP:
- Soporte de SNMP v1 y v2c t
- La implementación de SNMP v3 incluye el soporte para consultas, trampas, autenticación y privacidad
- Trampas SNMP brindan alertas de eventos como un disco lleno de logs o un virus detectado

Monitoreo de Tráfico:
- sFlow version 5 y Netflow V9.0

Almacenamiento de logs externo:
- Syslog
- Syslog confiable (Perfil RAW) basado en el RFC 3195
- Tendencias Web compatible con WELF

El ecosistema de tecnología abarca a los socios líderes en los mercados de la Administración de Firewall y Riesgo de Red, SDN y Virtualización, Administración de la seguridad de la información y los eventos (SIEM por sus siglas en inglés), Integración de Sistemas, Pruebas y Entrenamiento y Redes Inalámbricas

Integración Nativa con FortiSandbox, FortiSandbox en la nube, FortiMail, FortiMail en la nube, FortiCache, y FortiWeb

Almacenamiento de logs de La Security Fabric
- Configuraciones de FortiAnalyzer para el almacenamiento de logs sincronizado entre FortiGates
- Intercambio de Datos (información tal y como etiquetas de activos de topología y dispositivos) con un FortiAnalyzer

ADMINISTRACIÓN Y PROVISIONAMIENTO CENTRAL

Soporte de Administración Central: FortiManager, Servicio FortiCloud alojado en la nube, APIs de servicios Web

Despliegue rápido de: Wizards de instalación, Auto instalación de USB, ejecución de secuencias de código, local y remota

INTEGRACIÓN DE NUBE Y SDN

Integración con Openstack, NSX de VMWare, y la infraestructura ACI de Cisco

VISIBILIDAD

Visualizador Interactivo y Gráfico para el usuario, dispositivo, red y actividades de seguridad (FortiView):
- Una variedad de consolas GUI muestran el estatus actual e histórico usando diferentes perspectivas tales y como 'orígenes', 'destinos', 'interfaces', 'aplicaciones', 'amenazas', etc.
- Mapa de Amenazas y VPN
- Opciones de Vista de Datos: Tabla, gráfico de burbuja o mapa mundial si es aplicable
- Vista de Resultados de análisis de archivo/sandbox (Integración con FortiSandbox requerida)
- Vista de Vulnerabilidad de Dispositivos Finales (Integración con FortiClient requerida)
- Indicación de sesiones aceleradas en la Consola FortiView todas las sesiones'
- Búsqueda WHOIS para Direcciones IP Públicas dentro de FortiView y las tablas de logs

Visores de topología física y lógica que ilustran:
- la ubicación de hosts dentro de la red del Security Fabric
- acceso a cuarentena de un solo clic, prohibición de IP o acceso detallado a la información contextual de los dispositivos
- conexiones entre las entidades del security fabric
- información relacionada el SD-WAN tal y como el uso de enlace

Vistas de datos agregados con FortiGates descendentes dentro de una Security Fabric
- presentado en FortiView, mapas de topología y monitores

AUTOMATIZACIÓN

Define automatizaciones dentro de la Security Fabric usando una configuración simple de if-then

Ponga en cuarentena hosts remotos, automáticamente, en la capa de acceso, con FortiAP y/o FortiSwitch, o FortiClient a través EMS

AUTENTICACIÓN AUTORIZACIÓN Y CONTABILIDAD (AAA POR SUS SIGLAS EN INGLÉS)

Base de datos de usuario local y soporte de servicio de autenticación de servicio remoto: LDAP, Radius y TACACS+, autenticación de dos factores

Inicio de Sesión Simple: Integración con el AD de Windows, el servidor Microsoft Exchange, el eDirectory de Novell, FortiClient, El Agente de Servidor Citrix y de Terminal, Radius (mensaje de contabilidad), POP3/POP3S, acceso a usuario (802.1x, autenticación por portal captivo)

PKI y certificados: certificados X.509, soporte de SCEP, Creación de Solicitud de Firma de Certificado (CSR, auto renovación de certificados antes de que expiren, soporte de OCSP

Servidor de Token, Integrado, que provisiona y administra tokens físicos, SMS y de Contraseña de Una Sola Vez (OTP por sus siglas en inglés) Suave

CALIFICACIÓN DE CUMPLIMIENTO Y SEGURIDAD

Ejecuta una serie de chequeos de cumplimiento de la configuración del sistema y resultados de logs periódicamente o bajo demanda

Calificación de Security Fabric: audita los componentes dentro de la Security Fabric contra las mejores prácticas, provee resultados y recomendaciones, luego les permite a los usuarios aplicar fácilmente remedios para ciertos ítems

Administra el cumplimiento de los dispositivos de red a través de software de cliente:
- Chequeo de postura: Hace cumplir la instalación de software de cliente y las configuraciones deseadas de acuerdo con el tipo de dispositivo/grupo y/o usuario/grupo de usuario y/o ubicaciones (IPs)
- Pone en Cuarentena a los clientes si se llega al umbral de nivel de vulnerabilidad

PROTECCIÓN CONTRA AMENAZAS AVANZADAS (ATP)

Análisis de archivos basado en la nube, externo, o integración local (OS de sandbox):
- Envío de archivos (con la selección de seleccionar tipos)
- Recepción de reportes de análisis de archivos
- Recepción de actualizaciones de firmas dinámicas de un sistema de análisis de archivos (checksum de archivos y base de dato de URLs maliciosas)

EVALUACIÓN DE VULNERABILIDADES

Muestra una lista de hosts vulnerables y sus vulnerabilidades a través de telemetría con FortiClient

DETECCIÓN DE IOC

Muestra una lista de hosts comprometidos a través de la información proveída por un FortiAnalyzer

CONTROLADOR INALÁMBRICO

Administra y provisiona las configuraciones para Puntos de Acceso Ligeros o Conmutadores locales y remotos (modelos seleccionados)

Configure los métodos de acceso y autenticación para los SSIDs y VLANs, soporta un portal activo integrado o externo, 802.1x y llaves precompartidas

Múltiples PSK para WPA Personal

Seguridad WiFi: Supresión de AP bandido, IDS inalámbrico

Soporte de topología inalámbrica: Roaming rápido, balanceo de carga de AP, Malla Inalámbrica y Bridging

Conmutación por error controlada entre los controladores inalámbricos

CONTROLADOR DE CONMUTADOR

Extienda el control de acceso y la seguridad a los dispositivos cableados al administrar los conmutadores Fortinet (FortiSwitch) a través de una comunicación tipo CAPWAP.

Habilidad para configurar las características de puerto de conmutador tal y como PoE y la asignación de VLAN desde la GUI

ADMINISTRADOR DE INTERFAZ WAN

Soporta módems WAN inalámbricos USB 3G/4G

Operación

CONFIGURACIÓN

Acceso de Administración: HTTPS a través de un navegador Web, SSH, telnet y consola

FortiExplorer:
- Cliente de administración en las plataformas IOS
- Facilidad de uso al utilizar conectividad USB
- Provee notificación móvil (como parte de la característica de automatización)

Almacén de Características: Cambie las visualizaciones de los componentes de GUI

Cree etiquetas (en base a múltiples categorías definidas por el administrador) para separar y categorizar objetos de red, interfaces y dispositivos

Configuración de GUI:
- Acceso de 'Un solo clic' que transfiere rápidamente a los administradores a los paneles del siguiente paso
- Selectores de objetos dinámicos y consultas de búsqueda predictivas

Soporte del lenguaje de administración de la Interfaz de Usuario web: Inglés, Español, Francés, Portugués, Japonés, Chino Simplificado, Chino Tradicional y Coreano

ALMACENAMIENTO DE LOGS Y REPORTES

Soporte de infraestructura de almacenamiento de logs: Memoria y almacenamiento local (si se encuentra disponible), múltiples servidores syslog, múltiples FortiAnalyzers, servidores de Tendencias Web, Servicio de FortiCloud alojado

Almacenamiento de lots confiable, haciendo uso de la opción TCP (RFC 3195)

Almacenamiento de logs cifrado e integridad de logs con un FortiAnalyzer

Carga de lotes de logs programada o almacenamiento de logs en tiempo real

Tráfico de logs detallado: enviado, sesiones violadas, tráfico local, paquetes inválidos

Logs de eventos, exhaustivos: auditorías de los sistemas y la actividad de los administradores, enrutamiento y redes, VPN, autenticaciones de usuario, eventos relacionados al WiFi

Opción de formato del tráfico de logs, breve

Envía logs a los servidores syslog en Formato de Evento Común (CEF)

Opción de resolución de nombres para IPs y puertos de servicio

DIAGNÓSTICOS

Comandos CLI de diagnóstico, trazador de sesiones y captura de paquetes para resolver problemas de hardware, sistema y red.

Trazador GUI de políticas y enrutamiento

Trazador CLI del flujo de paqueles

ESPECIFICACIONES

Conjunto de pruebas de hardware en la CLI

MONITOREO

Monitores Gráficos: Sistema en tiempo real, servicio de red y visores del estatus de los usuarios

Dashboard: widgets y diseño personalizados

Política y Control

OBJETOS DE POLÍTICA

Objetos de política: predefinidos, personalizados, agrupación de objetos, etiquetado y coloreado

Objetos de dirección: subred, IP, rango de IPs, GeoIP (Geografía), FQDN

Servicio de Base de Datos de Internet: Base de datos actualizada automáticamente que provee una lista de aplicaciones de nube populares con su información vital, que puede ser usada para la configuración de políticas, enrutamiento y configuraciones de balanceo de carga de enlace.

IDENTIFICACIÓN DE DISPOSITIVO

Identificación de Dispositivo: Creación de huellas digitales de dispositivo y OS, clasificación automática y soporte de administración de inventario

Soporte de aplicación y bypass de la autenticación MAC

INSPECCIÓN SSL

Inspecciona la opción de tráfico cifrado SSL para el IPS, el control de aplicaciones, el antivirus, el filtrado web y el DLP

Mirroring de MITM SSL DLP

Opciones de Método de Inspección SSL: Inspección de certificado SSL o inspección de SSL completa

Exceptuación de inspección SSL por base de datos de reputación del sitio, categorías web y/o direcciones de política

ACCIONES

Notificaciones de usuario: mensaje de reemplazo personalizable para bloquear sitios y archivos adjuntos

Inserción de banner superior de explorador web (Fortinet Bar): muestra las violaciones del control de aplicaciones, el cumplimiento del control de dispositivos finales, la cuota de exploración web, etc.

Cuarentena de usuarios:
- Manualmente asignada con una duración personalizable o perpetua
- Automáticamente cuando es desencadenada por una firma IPS violada

Seguridad

ANTI-MALWARE

Bloqueo de IP de servidor Botnet con una base de datos de reputación IP global

Selección del tipo de base de datos de Antivirus (en modelos seleccionados)

Consulta de Base de Datos de Prevención de Brote de Virus: usa una base de datos de checksums en tiempo real de las nuevas amenazas detectadas antes de que las firmas de Antivirus estén disponibles

Opción de Desarme y Reconstrucción de contenido:
- Un motor de Antivirus remueve todo el contenido activo en tiempo real antes de pasarlo al usuario
- Envía el archivo original a un sandbox para un análisis adicional, ser puesto en cuarentena o descartado

Opción de Antivirus basada en flujo o basada en proxy:
- Soporte para protocolos populares: web, correo y FTP
- Escanea el tráfico cifrado con inspección SSL

Opción para tratar los ejecutables de Windows en archivos de email adjuntos como virus

Cuarentena de archivos (almacenamiento local requerido)

IPS Y DOS

Motor de IPS: más de 7,000 firmas actualizadas, detección de anomalía de protocolo, detección basada en velocidad, firmas personalizadas, manuales, actualización de firmas por tirón o empuje, integración con la enciclopedia de amenazas

Acciones de IPS: Por defecto, monitor, bloquear, resetear, o poner en cuarentena (IP de atacantes, e IP de víctimas, interfaz de entrada) con tiempo de expiración

Selección Basada en Filtro: Severidad, objetivo, OS, aplicación y/o protocolo

Opción de almacenamiento de logs de paquetes

Excepciones de IPs de firmas de IPS específicas

Protección DOS IPv4 e IPv6 basada en velocidad (disponible en la mayoría de modelos) con configuración de umbral contra la inundación de Syn TCP, escáneo de puertos TCP/UDP/SCTP, barrido ICMP, inundación de sesiones TCP/UDP/SCTP/ICMP (origen/destino)

Modo de Sniffer IDS

Bypass activo con interfaces de bypass (modelos seleccionados) y FortiBridge

CONTROL DE APLICACIONES

Detecta miles de aplicaciones en 8 categorías: Negocios, Nube IT, Colaboración, Email, Juegos, Interés General, Móvil, Servicio de Red, P2P, Proxy, Acceso Remoto, Medios Sociales, Almacenamiento/Respaldo, Actualizaciones, Video/ Audio, VoIP, Chat Web e Industrial.

Soporte de firmas, personalizables, de aplicaciones

Soporta la detección de tráfico usando el protocolo HTTP/2 y es capaz de bloquear el tráfico QUIC de modo que el navegador automáticamente retrocede a HTTP/2 + TLS 1.2

Anulaciones basadas en filtro por: conducta, categoría, popularidad, tecnología, riesgo, proveedor y/o protocolo

Acciones: Permite, bloquea, resetea sesión (solo por CLI), solo monitor

Inspección SSH

Control de aplicaciones, profunda, a través de servicios de nube pública tales como SalesForce, Google Docs y Dropbox

FILTRADO WEB

Soporte de modo de inspección de filtrado web: Basado en proxy, basado en flujo y DNS Filtrado

web manualmente definido basado en URL, contenido web y encabezado MIME

Filtrado web dinámico con una base de datos de categorización en tiempo real basada en la nube:
- Más de 250 millones de URLs clasificadas en 78 categorías, en 70 lenguajes

Cumplimiento de búsqueda segura: inserta transparentemente el parámetro de Búsqueda Segura a las consultas. Soporta Google, Yahoo!, Bing y Yandex. Filtro de Educación YouTube definible

Prevención de evasión Proxy: Bloquea de categoría de sitios proxy, clasifica URLs por dominio y dirección IP, bloquea redirecciones provenientes de sitios cache y de traslación, bloqueo de aplicaciones de evasión de proxy (control de aplicaciones), bloqueo de comportamiento proxy (IPS)

Filtrado Web de categorías locales y anulación de clasificación de categorías

Anulación de perfil de filtrado web: Le permite al administrador asignar temporalmente diferentes perfiles a múltiples usuarios/grupos de usuario/IPs

Soporta lista negras externas

Restringe el acceso a solamente las Cuentas de Google Corporativo

Características adicionales ofrecidas por el filtrado web basado en proxy:
- Filtro de Java Applet, ActiveX y/o cookie
- Bloquea el POST de HTTP
- Almacena logs de palabras clave de búsqueda
- Clasifica imágenes por URL
- Bloquea las redirecciones HTTP por clasificación
- Exceptúa el escaneo de conexiones cifradas en ciertas categorías, por privacidad
- Cuota de navegación web por categorías

FIREWALL

Modos de Operación: NAT/route y transparente (puente)

Horarios: una vez, recurrente

Auxiliares de Sesión (Session Helpers) y ALGs: DCE/RPC, DNS-TCP, DNS-UDP, FTP, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS (Oracle)

Soporte de tráfico VoIP: SIP/H.323 /SCCP NAT transversal, creación de agujeros RTP de aguja

Soporte de tipo de protocolo: SCTP, TCP, UDP, ICMP e IP

Políticas basadas en Usuario y Dispositivo

Administración de políticas: Vista de administración de secciones o de la política global

Modo de política de NGFW: configura políticas con aplicaciones y URLs como objetos

VPN

Portal de VPN SSL personalizable: temas de color, diseño, marcadores, herramientas de conexión, descarga de cliente

Soporte de reino VPN SSL: permite múltiples inicios de sesión SSL VPN personalizables asociados con grupos de usuarios (caminos URL, diseño)

Marcadores de inicio de sesión único: reúsa inicios de sesión previos o credenciales predefinidas para acceder a los recursos

Administración de marcadores personales: les permite a los administradores ver y mantener marcadores de cliente remoto

Limita el número de usuarios concurrentes del portal SSL

Un único inicio de sesión por opciones de usuario: Previene los inicios de sesión concurrentes usando el mismo nombre de usuario

Modo Web de VPN SSL: Para clientes remotos equipados solamente con un navegador Web y soporte de Aplicaciones Web, tales y como HTTP/HTTPS Proxy, FTP, Telnet, SMB/CIFS, SSH, VNC, RDP y Citrix

Modo de Túnel VPN SSL: para computadoras remotas que ejecutan una variedad de aplicaciones de cliente y servidor, el cliente de VPN SSL soporta MAC OSX, Linux, Windows Vista y sistemas operativos Windows de 64-bit

Modo de envío de puerto VPN SSL: usa un Applet de Java que escucha en los puertos locales en la computadora del usuario. Cuando este recibe datos desde una aplicación de cliente, el módulo de envío del puerto cifra y envía los datos al dispositivo VPN SSL, el cual entonces envía el tráfico al servidor de aplicación.

Chequeo de integridad de Host y chequeo de OS (solo para las terminales windows) anterior a las conexiones en modo túnel

SSL Chequeo de Host por MAC y por portal [redacted]

Opción de limpieza de cache justo antes de que la sesión de VPN SSL termine

ESPECIFICACIONES

Opción de escritorio virtual para aislar la sesión de VPN SSL del entorno de escritorio de la computadora del cliente

VPN IPsec:
- Soporte de par remoto: Clientes de marcado que cumplen con IPsec, pares con DNS de IP estática/dinámica
- Método de Autenticación: Certificado, llave precompartida
- Modo de Fase 1 IPsec: Modos agresivo y principal (protección de ID)
- Opciones de aceptación de par: Cualquier ID, un ID específico, un ID en un grupo de usuario de marcado
- Soporte de IKEv1 e IKEv2 (RFC 4306)
- Soporte de configuración de modo IKE (como servidor o cliente), DHCP sobre IPsec
- Cifrado de propuesta de Fase 1/Fase 2: DES, 3DES, AES128, AES192 y AES256
- Autenticación de propuesta de Fase 1/Fase 2: MD5, SHA1, SHA256, SHA384 y SHA512
- Soporte del grupo Diffie-Hellman de Fase 1/Fase 2: 1, 2, 5 y 14
- Soporte de XAuth como modo de cliente o servidor
- XAuth para usuarios de marcación: Opción de tipo de servidor (PAP, CHAP, Auto), opción de NAT Transversal
- Expiración de llave de cifrado IKE Configurable, frecuencia de keep-alive de NAT transversal
- Detección de par muerto
- Detección de repetición
- Keep-alive de clave automática para el SA de fase 2

Wizard de configuración IPsec para la terminación con populares dispositivos de terceros

VPN de un clic asistida por la nube: VPN de estrella fácilmente configurable para múltiples sitios de FortiGate con la ayuda de un portal de nube

Modos de despliegue de VPN IPsec: Gateway-a-gateway, estrella, malla completa, túnel redundante, terminación VPN en modo transparente

Opciones de Configuración de VPN IPsec: basado en rutas o basado en políticas

Monitoreo VPN: Vea y administre las conexiones de VPN IPsec y SSL, actuales, detalladamente

Otras VPN Soportadas: cliente L2TP (en modelos seleccionados) y modo de servidor, L2TP sobre IPsec, PPTP, GRE sobre IPEC

DLP

El modo de inspección de filtrado web soporta: basado en proxy, basado en flujo y DNS

Filtro de Mensaje DLP:
- Protocolos soportados: HTTP-POST, SMTP, POP3, IMAP, MAPI y NNTP
- Acciones: Solo almacenar logs, bloquear y/o poner en cuarentena a un usuario/IP/Interfaz
- Filtro predefinido: Número de tarjeta de crédito, ID de Seguridad Social

Filtro de Archivo DLP:
- Protocolos Soportados: HTTP-POST, HTTP-GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP
- Opciones de Filtro: tamaño, tipo de archivo, marca de agua, contenido, si se encuentra encriptado o no

Marcado de agua DLP: Permite filtrar los archivos que pasa a través de la unidad FortiGate y contiene un identificador corporativo (una cadena de texto) y un nivel de sensibilidad (Crítico, Privado y Advertencia) escondido en la marca de agua. Soporta las herramientas de marcado de agua gratis de Windows y Linux

Toma de huella digital DLP: Genera una huella digital de checksum a partir de los archivos interceptados y la compara con aquellas en la base de datos de huella digital

Archivado DLP: Registra el contenido completo del tráfico de email, FTP, IM, NNTP, y Web

FILTRADO DE EMAIL

Soporte de protocolos de correo: IMAP(S), POP3(S), y SMTP(S)

Consulta de base de datos Anti-Spam: chequeo de dirección IP, chequeo URL y checksum de email

Filtrado de Spam Local: Búsqueda de HELO DNS, chequeo DNS del email de retorno y Lista Negra/Blanca

Redes

ENRUTAMIENTO/NAT

Enrutamiento estático y por políticas

Protocolos de enrutamiento dinámico: RIPv1 y v2, OSPF v2 y v3, ISIS, BGP4

Enrutamiento de contenido: WCCP e ICAP

Configuración NAT: Basado en políticas y la tabla NAT central

Soporte de NAT: NAT64, NAT46, NAT estático, NAT dinámico, PAT, NAT de cono lleno, STUN

Tráfico Multicast: modo disperso y denso, soporte de PIM

L2/CONMUTACIÓN

Modos de interfaz de capa 2: Puertos agregados, bucle, VLANs (802.1Q y Troncalización), hardware virtual, software y conmutadores VLAN

Soporte de VXLAN:
- interVTEP (Punto Final de Túnel VXLAN)
- Soporte de múltiples IPs remotas, estas IPs remotas pueden ser IPv4 unicast, IPv6 unicast, IPv4 multicast o IPv6 multicast

Soporte de EMAC-VLAN: permite la adición de direcciones de capa 2, múltiples, (o Direcciones MAC de Ethernet) a una sola interfaz física

Par de Cable Virtual:
- Procesa el tráfico, solo entre 2 interfaces asignadas en el mismo segmento de red
- Disponible tanto en modo transparente como en modo NAT/route
- Opción para implementar una configuración de VLANs de wildcard

INSPECCIÓN FUERA DE LÍNEA

Modo de sniffer: Dedica una interfaz exclusivamente, en la que todo el tráfico entrando a la interfaz es procesado por el sniffer

Inspección de Seguridad Fuera de Línea: AV, Filtrado Web, Control de Aplicaciones, IPS y Anti-spam

SD-WAN

Balanceo de carga WAN (ponderado) algoritmos por: volumen, sesiones, IP de origen-destino, IP de origen y excedente

Chequeos de enlace WAN para SLAs:
- Ping o pruebas HTTP
- El criterio de monitoreo incluye latencia, jitter y pérdida de paquetes
- Intervalo de chequeo configurable, umbrales de fallas y conmutación por recuperación

Inteligencia Multi-Camino usando reglas definidas por:
- Dirección y/o Grupo de Usuario de origen
- Dirección de destino y/o una selección de más de 3,000 aplicaciones
- Selección de camino usando un criterio de calidad de enlace particular o definido por SLAs

Modelado de tráfico y QoS por políticas o aplicaciones: Modelado de políticas compartidas, modelado por IP, ancho de banda máximo y garantizado, número máximo de conexiones concurrentes por IP, priorización de tráfico, Tipo de Servicio (TOS), y soporte de servicios diferenciados (DiffServ)

Opción para configurar un perfil de modelado de tráfico al definir el porcentaje de ancho de banda de interfaz para cada tráfico clasificado y entonces vincularlo a las interfaces

Políticas de Modelado de Tráfico: Asigna un perfil de modelado de tráfico de acuerdo a la política que encaje en base al origen, destino, servicio, aplicación, categoría de aplicación, y/o categoría de URL.

Soporte de DSCP:
- Coincidencia DSCP en las reglas SD-WAN
- Etiquetado DSCP de los paquetes enviados en base a las aplicaciones identificadas

Topología de optimización WAN en línea y fuera de camino, par a par y soporte de cliente remoto

Opción de Modo Transparente: mantiene la dirección de origen, original, de los paquetes, de modo que los servidores parezcan recibir tráfico directamente de los clientes

Técnicas de optimización WAN: Optimización de protocolo y almacenamiento en memoria cache de Bytes

Protocolos de optimización WAN soportados: CIFS, FTP, HTTP(S), MAPI y TCP

Opción de Tunelización Segura: Usa SSL con AES-128bit-CBC para cifrar el tráfico en el túnel de optimización WAN

Opción de distribución de túnel: Múltiples sesiones de optimización WAN comparten el mismo túnel

Almacenamiento en memoria cache, Web: Almacenamiento en memoria cache de objetos, que acelera las aplicaciones y los servidores web al reducir el uso del ancho de banda, la carga de servidor, y la latencia percibida. Soporta el almacenamiento en memoria cache de sitios web HTTP 1.0 y HTTP 1.1

Descarga SSL con almacenamiento en memoria cache, Web:
- Modo completo: realiza tanto el descifrado y el cifrado del tráfico HTTPS
- Modo medio: realiza solo la acción de cifrado o descifrado

Opción para exceptuar ciertos sitios web del almacenamiento en memoria cache mediante patrones de URL

Soporta configuraciones y opciones de almacenamiento en memoria cache, avanzados:
- Siempre revalidar, Máximo tamaño de objeto en cache, duración de respuesta negativa, factor fresco, TTL Máximo/Mínimo/Por defecto, FQDN proxy, Número máximo de solicitudes/longitud de mensajes HTTP, ignorar opciones, objetos en cache expirados, pragma-no-cache revalidado

Monitor de optimización WAN y cache web

PROXY EXPLÍCITO

Proxy Web y FTP explícito: Creación de proxy FTP, HTTP y HTTPS en una o más interfaces

Proxy auto-config (PAC): Provee configuraciones de proxy automáticas para usuarios de proxy web explícito

Concatenación de Proxy: Envío de proxy web para redirigir las sesiones de proxy web a otros servidores proxy Web

Chequeo del estado de enlace y monitoreo del servidor de envío de proxy

Capacidad de reflejar IP

Balanceo de carga para el envío de proxy y la concatenación de proxy

Autenticación de proxy web explícito: autenticación basada en IP y por proxy Web transparente de autenticación de sesión

IPV6

Soporte de IPv6: Administración a través de IPv6, protocolos de enrutamiento IPv6, tunelización IPv6, firewall y UTM para el tráfico IPv6, NAT46, NAT64 y VPN Ipsec IPv6 [redacted]

Soporte de SD-WAN IPv6: Monitor de enlace Ping6, objetos de origen y destino IPv6

183
00000095

ESPECIFICACIONES

ALTA DISPONIBILIDAD

Modos de Alta Disponibilidad: Activo-pasivo, activo-activo, clusters virtuales, VRRP, agrupamiento de la serie FG-5000

Interfaces de Monitoreo de Estado de un Miembro de Cluster (Heartbeat Interfaces) Redundantes

Interfaz de Administración Reservada de HA

Conmutación por error:
- Monitoreo de enlace de puerto, local y remoto
- Conmutación por error con estado
- Conmutación por error de menos de segundos
- Notificación de Detección de Fallas

Opciones de Despliegue:
- HA con agregación de enlace
- HA de Malla Completa
- HA Geográficamente Dispersa

- Sincronización de sesiones independiente

SERVICIOS DE RED ESENCIALES

DHCP integrado, NTP, Servidor DNS y proxy DNS

FortiGuard NTP, DDNS y servicio DNS

Soporte de Plataforma

DISPOSITIVO FÍSICO (+SPU)

Se integra con los componentes SPU para obtener una aceleración del procesamiento del tráfico.

SISTEMAS VIRTUALES

Sistemas Virtuales (Dominios Virtuales FortiOS) dividen una sola unidad FortiGate en dos o más instancias virtuales de FortiOS que funcionan separadamente y pueden ser administradas independientemente.

Limitación y administración de los recursos de los sistemas virtuales, configurable, tales como los valores máximos/garantizado de 'sesiones activas' y cuota de disco de log

Modos de operación por VDOM: NAT/Route o VDOM

Modos de inspección de seguridad por VDOM: Proxy o basados en flujo

HIPERVISOR

Soporta las plataformas de Hipervisor populares, incluyendo el vSphere de VMWare, Citrix y Xen de fuente abierta, KVM, y hyper-V de MS

NUBE

Soporta los servicios de nube pública: Amazon AWS y Microsoft Azure

Otros

OTROS

Firewall de Aplicaciones Web:
- Basado en firmas, restricciones URL y política de método HTTP

Balanceo de Carga de Servidor: el tráfico puede ser distribuido a través de múltiples servidores backend:
- Basado en múltiples métodos incluyendo: estático (conmutación por error), round robin, ponderado o basado en el tiempo de viaje de vuelta y número de conexiones.
- Soporta los protocolos IP o TCP/UDP genéricos: TTP, HTTPS, IMAPS, POP3S, SMTPS, SSL
- La persistencia de sesión es soportada en base al ID de sesión SSL o en base a una cookie HTTP inyectada.

NOTA: Conjunto de características basado en el FortiOS V6.0 GA, algunas características podrían no aplicar a todos los modelos. Para la disponibilidad, por favor refiérase a la Matriz de Características de Software disponible en docs.fortinet.com

REFERENCIAS

RECURSO	URL
The FortiOS Handbook — The Complete Guide	http://docs.fortinet.com/fgt.html
Fortinet Knowledge Base	http://kb.fortinet.com/

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

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6395.2788

LATIN AMERICA SALES OFFICE
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
United States
Tel: +1.954.368.9990

Derechos de autor© de La Corporación Fortinet, 2017. Todos los derechos reservados. Fortinet®, FortiGate®, FortiCare® y FortiGuard®, y ciertas otras marcas son marcas registradas de La Corporación Fortinet, en los Estados Unidos y en otras jurisdicciones, y otros nombres de Fortinet aquí presentados podrían también estar registrados, así como las marcas de ley común de Fortinet. Todos los otros productos o nombres de compañía podrían ser marcas de sus respectivos dueños. El desempeño y otras métricas contenidas aquí fueron obtenidos en pruebas de laboratorio internas bajo condiciones ideales, y el desempeño actual y otros resultados podrían variar. Variables de red, distintos entornos de red y otras condiciones podrían afectar los resultados del desempeño. Nada aquí representa un compromiso vinculante para Fortinet y Fortinet rechaza todas las garantías, ya sea expresadas o implícitas, excepto al grado que Fortinet entre en un contrato escrito vinculante, firmado por el Consejo General de Fortinet, con un comprador que expresamente garantice que el producto identificado se desempeñará de acuerdo a ciertas métricas desempeño identificadas expresamente y en tal evento, solo las métricas de desempeño específicas expresamente identificadas en tal contrato escrito vinculante serán vinculantes para Fortinet. Para claridad absoluta, tal garantía estará limitada al desempeño en las mismas condiciones ideales que se tienen en los laboratorios de pruebas internas de Fortinet. En ningún momento Fortinet hace ningún compromiso relacionado a entregables futuros, características o desarrollo, y las circunstancias pueden cambiar de modo que cualquier declaración aquí contenida no sea precisa. Fortinet rechaza por completo cualquier convenio, representación, y la garantía acorde a lo aquí expresado, ya sea expresa o implícita. Fortinet se reserva el derecho a cambiar, modificar, transferir o de alguna forma revisar esta publicación sin aviso alguno, y la versión más actual de la publicación será la aplicable.

FST-PROD-DS-FOS

FOS-DAT-R6-201804

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL

PROCESO DE LIBRE GESTIÓN LG MTPS 12-2018
PARA: "ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"

Security Technologies

OFERTANTE:
JARET NAUN MORÁN SORTO/JL SECURITY TECHNOLOGIES

ORIGINAL

SAN SALVADOR, JUNIO DE 2018

[redacted]

[redacted]

ÍNDICE

	Página.
Oferta Técnica	1
Cuadros Comparativos	13
Soporte Técnico	14
Ficha Técnica Serie T	17
Ficha Técnica Serie E	21
Imagen 1	26
Imagen 2	27
Imagen 3	28
Imagen 4	29
Imagen 5	30
Imagen 6	31
Imagen 7	32
Oferta Económica	33
Cartas de referencia	37
Cartas Compromiso	43
Carta de Distribuidor Autorizado	46
Certificaciones de los Técnicos	48
Carta para Gestionar Garantía	56
Declaración Jurada	58

Security Technologies

[redacted]

JL SECURITY TECHNOLOGIES
Seguridad en Internet

San Salvador, viernes 22 de Junio de 2018

Señores.
Ministerio de Trabajo y Previsión Social
Atención: Licenciada Mayra Palma jefa UACI ad Honorem
Presente.

Reciba un cordial saludo de JL Security Technologies y nuestros mejores deseos de éxito en sus labores diarias. Presentamos a su consideración y evaluación la siguiente cotización de acuerdo a sus requerimientos:

OFERTA TÉCNICA.

ÍTEM 1 SITIO PRINCIPAL Y SITIO REMOTO (SANTA ANA)				
CARACTERISTICA	**DESCRIPCIÓN**	**CUMPLE**		**OBSERVACIONES**
Capacidad de usuarios	Hasta 1000	SI		En nuestra solución ofrecemos 8GB de rendimiento de firewall + 1.5 Millones de sesiones concurrentes + cada parámetro de seguridad (AV, IPS, APP, URL, etc) ofrecemos un porcesamiento independiente de X cantidad de acuerdo a la ficha técnica independiente a los 8GB de rendimiento.
Cantidad de equipos	Dos	SI		
Configuración	Contingencia	SI		
Almacenamiento	240 GB mínimo	SI		Hillstone Serie T, pág. 20 N° 3
Consumo de energía	Fuente redundante	SI		Hillstone Serie T, pág. 20 N° 4
Conexiones concurrentes	Mínimo 1 millones	SI		Hillstone Serie T, pág. 20 N° 5
AV rendimiento	Mínimo 1.5 GBPS	SI		Hillstone Serie T, pág. 20 N° 6

[redacted]

IPS rendimiento	Mínimo 2 GBPS	SI		Hillstone Serie T, pág. 20 N° 7
Firewall rendimiento	Mínimo 4 GBPS	SI		Hillstone Serie T, pág. 20 N° 8
Interfaces	Capacidad de ampliación	SI		Hillstone Serie T, pág. 20 N° 9
Módulos de protección	"1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPSec."	SI		Hillstone Serie T, pág. 18 N° 10
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.	SI		Hillstone Serie T, pág. 18 N° 11
VPN	"1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: SI Locales, CA y CRL."	SI		Hillstone Serie T, pág. 19 N° 12
Seguridad web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, YouTube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS."	SI		Hillstone Serie T, pág. 17, 18, 19 e imagen 4, pág. 29 N° 13
Protección de red	"1. Administración web protegido	SI		Hillstone Serie T,

[redacted]

	por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, IPSec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico."			pág. 18 y 19 N° 14
Filtrado de contenido	"1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe permitir / restringir / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones."	SI		Hillstone Serie T, pág. 18, 19 e imagen 5, pág. 30 N° 15
IPS	"1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code Injection.	SI		Hillstone Serie T, pág. 23 N° 16 NOTA: nuestra solución es un firewall Hillstone de próxima generación

	5. Bloqueo de actividades relacionadas a P2P e IM."			
Protección de correo electrónico	Especificar	SI		Hillstone Serie T, pág. 18 e imagen 1, pág. 26 N° 17,
Protección de redes inalámbricas	Especificar	SI		Imagen 2 pág. 27 y 28 N° 18
Soporte técnico	"1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico."	SI		JL Security Technologies de ser adjudicado instalará y configurará los equipos por técnicos certificados de la marca. JL Security Technologies Se compromete a brindar un soporte técnico según las características descritas en la página 14 de este documento
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.	SI		JL Security Technologies ofrece una garantía por desperfectos de fábrica por un año renovable con las licencias del equipo. Ver cuadro de Garantía pag. 56
Experiencia	"1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al	SI		JL Security Technologies cuenta con una amplia cartera de clientes tanto del

[redacted]

	menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado."			sector privado como del gobierno para lo cual presentamos las cartas de referencia dentro del presente documento.
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.	SI		JL Security Technologies ofrece capacitación en la configuración y administración de los equipos Hillstone de 20 horas para 4 técnicos

ÍTEM 2 REGIONALES Y DEPARTAMENTALES (A EXCEPCION DE SANTA ANA)				
CARACTERISTICA	DESCRIPCIÓN	CUMPLE		OBSERVACIONES
Capacidad de usuarios	Hasta 100	SI		
Cantidad de equipos	Doce	SI		
Almacenamiento	64GB Mínimo	SI		Cuadro Comparativo pág. 13
Consumo de energía	Especificar	SI		Hillstone Serie E pág. 24 N° 3
Conexiones concurrentes	Mínimo 600K	SI		Hillstone Serie E pág. 24 N° 4
AV rendimiento	Mínimo 500 Mbps	SI		Hillstone Serie E pág. 24 N° 5
IPS rendimiento	Mínimo 400 Mbps	SI		Hillstone Serie E pág. 24 N° 6
Firewall rendimiento	Mínimo 1.5 Gbps	SI		Hillstone Serie E pág. 24 N° 7
Interfaces	Capacidad de Ampliación	SI		Cuadro comparativo pág. 13
Módulos de protección	"1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes	SI		Hillstone Serie E pág. 22, imagen 1, pág. 26, imagen 2 pág. 27 y 28 N° 9

[redacted]

	inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPSec."			
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.	SI		Hillstone Serie E pág. 21 N° 10
VPN	"1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL."	SI		Hillstone Serie E pág. 23 N° 11
Seguridad web	"1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, YouTube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS."	SI		Hillstone Serie E pág. 22 imagen 4 pág. 29 N° 12
Protección de red	"1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, IPSec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico."	SI		Hillstone Serie E pág. 22 y 23 N° 13
Filtrado de contenido	"1. Sistema de filtrado de	SI		Hillstone Serie E

[redacted]

	contenido Web, para http, y https. 2. Debe permitir / restringir / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones."			pág. 22 y 23 e imagen 6 pág. 31 N° 14
IPS	"1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM."	SI		Hillstone Serie E pág. 21 y 22 imagen 4, pág. 29 N° 15 NOTA: nuestra solución es un firewall Hillstone de próxima generación
Protección de correo electrónico	Especificar	SI		imagen 1 pág. 26 N° 16
Protección de redes inalámbricas	Especificar	SI		imagen 2 pág. 27 N° 17
Soporte técnico	"1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas	SI		JL Security Technologies de ser adjudicado instalará y configurará los equipos por

[redacted]

	que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico."			técnicos certificados de la marca. JL Security Technologies Se compromete a brindar un soporte técnico según las características descritas en la página 14 de este documento.
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.	SI		JL Security Technologies ofrece una garantía por desperfectos de fábrica por un año renovable con las licencias del equipo. Ver cuadro de gestión de garantía pág. 56
Experiencia	"1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado."	SI		JL Security Technologies cuenta con una amplia cartera de clientes tanto del sector privado como del gobierno para lo cual presentamos las cartas de referencia dentro del presente documento.
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.	SI		JL Security Technologies ofrece capacitación en la configuración y administración

[redacted]

				de los equipos Hillstone de 20 horas para 4 técnicos.

ÍTEM 3 CENTROS DE RECREACIÓN Y ARCHIVO GENERAL				
CARACTERISTICA	DESCRIPCIÓN	CUMPLE		OBSERVACIONES
Capacidad de usuarios	Hasta 15	SI		
Cantidad de equipos	Cinco	SI		
Almacenamiento	64GB Mínimo	SI		Cuadro Comparativo pág. 13
Consumo de energía	Especificar	SI		Hillstone Serie E pág. 24 N° 3
Conexiones concurrentes	Mínimo 600K	SI		Hillstone Serie E pág. 24 N° 4
AV rendimiento	Mínimo 400 Mbps	SI		Hillstone Serie E pág. 24 N° 5
IPS rendimiento	Mínimo 300 Mbps	SI		Hillstone Serie E pág. 24 N° 6
Firewall rendimiento	Mínimo 900 Mbps	SI		Hillstone Serie E pág. 24 N° 7
Interfaces	Capacidad de Ampliación	SI		Cuadro comparativo pág. 13
Módulos de protección	"1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPSec."	SI		Hillstone Serie E pág. 22, imagen 1, pág. 26, imagen 2 pág. 27 y 28 N° 9
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.	SI		Hillstone Serie E pág. 21 N° 10
VPN	"1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP.	SI		Hillstone Serie pág. 23 N° 11

[redacted]

	2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL."			
Seguridad web	"1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, YouTube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS."	SI		Hillstone Serie E pág. 22 imagen 4 pág. 29 N° 12
Protección de red	"1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, IPSec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico."	SI		Hillstone Serie E pág. 22 y 23 N° 13
Filtrado de contenido	"1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe permitir / restringir / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet,	SI		Hillstone Serie E pág. 22 y 23 e imagen 6 pág. 31 N° 14

	Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones."			
IPS	"1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM."	SI		Hillstone Serie E pág. 21 y 22 imagen 4, pág. 29 N° 15 NOTA: nuestra solución es un firewall Hillstone de próxima generación
Protección de correo electrónico	Especificar	SI		imagen 1 pág. 26 N° 16
Protección de redes inalámbricas	Especificar	SI		imagen 2 pág. 27 N° 17
Soporte técnico	"1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff	SI		JL Security Technologies de ser adjudicado instalará y configurará los equipos por técnicos certificados de la marca. JL Security Technologies Se compromete a brindar un soporte técnico según las características descritas en la

	certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico."			página 14 de este documento.
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.	SI		JL Security Technologies ofrece una garantía por desperfectos de fábrica por un año renovable con las licencias del equipo. Ver cuadro de gestión de garantía pág. 56
Experiencia	"1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado."	SI		JL Security Technologies cuenta con una amplia cartera de clientes tanto del sector privado como del gobierno para lo cual presentamos las cartas de referencia dentro del presente documento.
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.	SI		JL Security Technologies ofrece capacitación en la configuración y administración de los equipos Hillstone de 20 horas para 4 técnicos.

[redacted]

[redacted]

CUADROS COMPARATIVOS

CUADRO COMPARATIVO FIREWALL PRINCIPAL (ÍTEM 1)		
N°	REQUERIMIENTO SOLICITADO	CARACTERISTICAS OFERTADAS
1	Almacenamiento 240 GB	El equipo Hillstone de la serie T está equipado con un Disco Duro de 480 GB en estado solido
2	Consumo de Energía: fuente redundante	El equipo Hillstone de la serie T está equipado con una fuente redundante de 150Watts
3	Conexiones Concurrentes: 1 Millón	El equipo Hillstone de la serie T tiene un alcance de hasta 1.5 Millones de sesiones concurrentes
4	AV Rendimiento: 1.5 Gbps	El equipo Hillstone de la serie T cuenta con 1.6 Gbps de AV Throughput para una mejor defensa contra virus
5	IPS Rendimiento: 2 Gbps	El equipo Hillstone de la serie T cuenta con 3 Gbps de IPS Throughput para un mejor bloqueo de intrusos
6	Firewall Rendimiento: 4 Gbps	El equipo Hillstone de la serie T cuenta con 8 Gbps de Firewall Throughput para un máximo rendimiento de procesamiento de información de tráfico en la red
7	Interface: Capacidad de ampliación	El equipo Hillstone de la serie T cuenta con dos slots de 8 puertos cada uno (puede ser cobre o fibra)

CUADRO COMPARATIVO FIREWALL DEPENDENCIAS (ÍTEM 2)		
N°	REQUERIMIENTO SOLICITADO	CARACTERISTICAS OFERTADAS
1	Almacenamiento 64 GB	Hillstone ofrece la solución VHSM de 80GB para todos los equipos de la Serie E.
2	Consumo de Energía: fuente redundante	El equipo Hillstone de la serie E está equipado con una fuente redundante de 45 Watts
3	Conexiones Concurrentes: 600 Mil	El equipo Hillstone de la serie E tiene un alcance de hasta 1.5 Millones de sesiones concurrentes
4	AV Rendimiento: 500 Mbps	El equipo Hillstone de la serie E cuenta con 500 Mbps de AV Throughput para una mejor defensa contra virus
5	IPS Rendimiento: 400 Mbps	El equipo Hillstone de la serie E cuenta con 600 Mbps de IPS Throughput para un mejor bloqueo de intrusos
6	Firewall Rendimiento: 1.5 Gbps	El equipo Hillstone de la serie E cuenta con 1.5 Gbps de Firewall Throughput para un máximo rendimiento de procesamiento de información de tráfico en la red
7	Interface: Capacidad de ampliación	Para la ampliación puede soportar un switch de 24 o 48 puertos configurado como extensión al firewall por medio de VLAN y enlaces troncales.

[redacted]

SOPORTE TÉCNICO.

Soporte para Equipos Firewall Marca Hillstone

Descripción del servicio:

* JL SECURITY TECHNOLOGIES, ofrece brindar soporte local para equipos Firewall, de la siguiente manera:
* El servicio se brindará de lunes a domingo en horario 24 horas.
* El soporte ofrecido tiene las siguientes modalidades, de acuerdo a las fallas técnicas que pudieran presentarse o despejar consultas que puedan surgir en el manejo del equipo:

1. Soporte vía Telefónica: por medio del teléfono: 2225-0951 y a los celulares 7610-2425 y 7011-6022 con servicio las 24 horas del día, los siete días de la semana, los 365 días del año (365/7/24). Atendiendo situaciones como:
    i. Consultas de Actualizaciones de firmware.
    ii. Consultas acerca de usuarios, password, direcciones IP de equipos a los cuales necesita entrar.
2. Soporte Remoto: En casos como:
    i. Modificación de Políticas
    ii. Introducción de nuevas IP de computadores.
    iii. Traslado de usuarios entre políticas
    iv. Creación de Nuevas Políticas.
    v. Creación de rutas nuevas entre los departamentales
    vi. Calidad de servicio.
3. Soporte en el sitio.
    i. Equipos no encienden
    ii. Falla en comunicación entre los equipos.
    iii. Cambio de direccionamiento IP Privada o Pública
    iv. Actualización de equipo.
    v. Realización de montajes de backup.

* Estos son algunos Ítem de lo que se pueda recurrir en estos tres servicios, pero la determinación la hará el encargado de sistemas.

4. JL Security Technologies se compromete a reparar los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestar un equipo de características similares mientras se hace efectivo el reemplazo total del equipo en garantía.

Soporte Técnico para Servidor de Correo y Sitio Web

- JL Security Technologies al ser adjudicado ofrece brindar soporte y asistencia técnica al servidor de correo y sitio web del Ministerio de Trabajo y Previsión Social sin costo adicional.

[redacted]

TIEMPOS DE RESPUESTA AREA METROPOLITANA DE SAN SALVADOR			
Tipo de llamada	**Tiempo máximo para respuesta telefónica**	**Tiempo máximo para respuesta en sitio**	**Tiempo máximo para habilitar el sistema**
Urgente (Problema de Hardware)	10 minutos	1 hora 30 minutos	3 horas
Grave (Sistema no Controlado)	45 minutos	3 horas	6 horas
No critica (Consultas o asistencia técnica)	1 hora 30 minutos	12 horas o a una hora mutuamente convenida después de 12 horas	1 Día o día y medio según sea la gravedad

TIEMPOS DE RESPUESTA FUERA DE SAN SALVADOR			
Tipo de llamada	**Tiempo máximo para respuesta telefónica**	**Tiempo máximo para respuesta en sitio**	**Tiempo máximo para habilitar el sistema**
Urgente (Problema de Hardware)	10 minutos	Max. 6 Horas (dependiendo la distancia desde San Salvador)	3 horas
Grave (Sistema no Controlado)	45 minutos	12 horas o un máximo de 24 horas (dependiendo la distancia desde San Salvador)	6 horas
No critica (Consultas o asistencia técnica)	1 hora 30 minutos	24 horas o a una hora mutuamente convenida después de 24 horas (dependiendo la distancia desde San Salvador)	1 Día o día y medio según sea la gravedad

Security Technologies

[redacted]

[redacted]

FICHAS TÉCNICAS

Security Technologies

[redacted]

[redacted]

163

Hillstone NETWORKS

Hillstone Serie-T Firewall Inteligente de Próxima Generación

NSS LABS RECOMMENDED

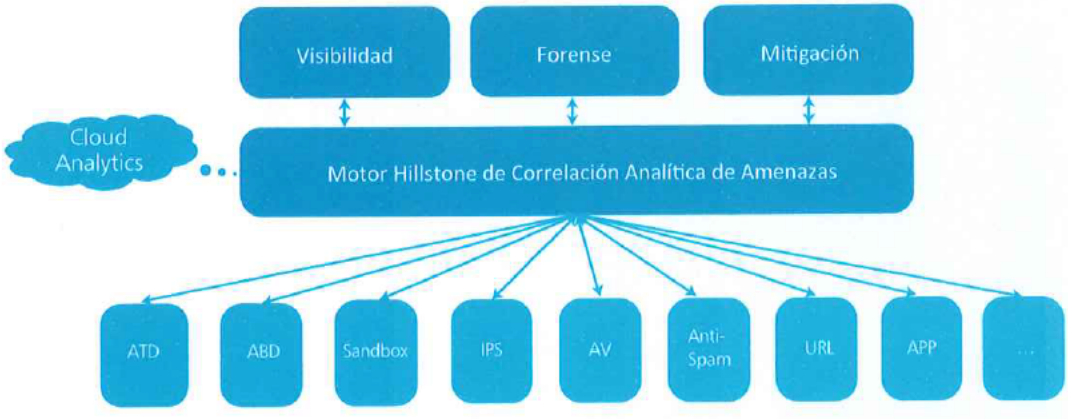
ICSA labs CERTIFIED FIREWALL - CORPORATE

T1860 / T2860 / T3860 / T5060 / T5860



El Firewall Serie-T inteligente de Hillstone de Próxima Generación (iNGFW) utiliza tres tecnologías clave para detectar ataques avanzados y proporcionar una defensa continua para las redes de hoy en día. En primer lugar, utiliza
Nº 13 agrupamiento estadístico para detectar malware desconocido, aprovechando el motor patentado de detección de amenazas Hillstone Advanced Threat Detection Engine (ATD). En segundo lugar, utiliza análisis comportamental para detectar comportamiento anómalo en la red, basado en el motor de detección de Hillstone Advanced Behavior Detection engine (ABD) Por último, apalanca la correlación del motor Hillstone de análisis de amenazas para correlacionar eventos de amenazas detectadas por los motores dispares - incluyendo ATD, ABD, sandbox y otras tecnologías para la detección de amenazas tradicionales basadas en firmas - junto con la información de contexto para identificar las amenazas avanzadas.

Con capacidades de detección y análisis de amenazas profundas, el iNGFW de Hillstone ofrece a los clientes una visibilidad completa de la situación de riesgo en la red, así como los detalles de amenaza para cada huésped. El Hillstone iNGFW proporciona a los administradores la información forense con diferentes herramientas y caminos, con el fin de profundizar en la causa raíz de un ataque. Además, el Hillstone iNGFW faculta al administrador con funciones de mitigación de gran alcance, que pueden ganar tiempo para los administradores al examinar los datos forenses, tomar una decisión informada acerca de la autenticidad del ataque, y reducir al mínimo los daños al negocio.



www.hillstonenet.com
Phone: 1-800-889-9860

Detalles del Producto

Detección de malware desconocido

Hillstone ha construido un motor propio que ha analizado cerca de un millón de muestras de malware "conocidas." Cada muestra ha sido clasificada y caracterizada basado en múltiples dimensiones que describen sus acciones, activos y atributos. En un entorno de producción, cuando se encuentra un nuevo malware, también se analiza, se caracteriza y se clasifica. Luego, se compara con la base de datos de muestras de malware conocidos que ya han sido analizados. Cuanto más cerca coincida con una muestras conocidas - mayor será la certeza de que se trata de una variante de una muestra de malware conocido. Este proceso se denomina "agrupamiento estadístico" y proporciona un método preciso para la identificación de nuevos programas maliciosos.

Análisis Forense Detallado

Hillstone ofrece una nueva forma de visualizar y analizar los ataques. Cada acción tomada por un código potencialmente malicioso se vincula automáticamente a los pasos dentro de "Kill Chain." Se complementa con información forense rica que permite que el analista determine el origen del ataque, la gravedad de la crisis, y la metodología empleada. Hillstone también proporciona archivos de captura de paquetes, que, cuando se combinan con el registro del sistema y con registros de tráfico, proporcionan al administrador una gran cantidad de información adicional. Además, de los datos del usuario, tales como los sitios web visitados, aplicaciones utilizadas, y el nivel de riesgo de las aplicaciones, para enfocar mejor la explotación. Lo más importante, Hillstone identifica la política de Firewall exacta que le permitió al atacante penetrarlo.

Detección de Comportamiento Anormal

El motor de comportamiento anormal de Hillstone supervisa continuamente la red para aprender como luce el tráfico normal de la red día a día, a cierta hora y en tal mes; proporcionando alertas cuando la actividad de la red supera los umbrales calculados. Se utiliza una matriz dimensional de 50+ para calcular el tráfico normal de la red en la capa L4-L7, llamado "modelado de comportamiento." Además, se ha entrenado con herramientas de piratería reales para asegurar que reconocerá fácilmente la actividad maliciosa. Estas técnicas limitan los falsos positivos y proporcionan al usuario múltiples oportunidades para detener un ataque.

Mitigación Prioritaria

Además de la posibilidad de realizar un cambio de política para prevenir un ataque, Hillstone ha incorporado varias funciones automáticas de mitigación. Estas funciones consisten en plantillas predefinidas que desaceleran automáticamente o bloquean un ataque si se detecta un comportamiento sospechoso. El administrador puede modificar las plantillas para limitar el ancho de banda o el número de sesiones disponibles para el atacante. También puede ajustar las limitaciones que introduce en los recursos de la red según el tipo de ataque y el nivel de gravedad. En los casos en que el ataque es crítico y el nivel de confianza es alto, la mitigación puede incluir un bloqueo completo de todos los recursos de la red. Y, si una plantilla no existe o no está activa, el administrador puede configurar rápidamente una mitigación temporal para ese evento.

Caracteristicas

Análisis de correlación de amenazas

- Correlación entre las amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales N° 11
- Reglas de correlación multidimensional, actualización diaria automática en la nube

Detección Avanzada de Amenazas

- Detección avanzada de malware basada en el comportamiento N° 13
- Detección de más de 2000 familias de programas maliciosos conocidos y desconocidos, incluyendo virus, desbordamiento, gusanos, troyanos, etc.
- En tiempo real, en línea, comportamiento del malware, actualización de base de datos modelo

Detección de Comportamiento Anormal

- Modelado de comportamiento basado en L3-L7 tráfico de la línea de base para revelar comportamientos anómalos en la red, tales como análisis HTTP, spiders, spam, SSH/FTP contraseña débil
- La detección de ataques DDoS incluyendo por inundación, Sockstress, zip de la muerte, reflexión, consultas DNS, DDos SSL y aplicaciones DDoS
- Apoya la inspección del tráfico de un túnel encriptado para aplicaciones desconocidas
- En tiempo real, en línea, comportamiento anormal de la actualización de la base de datos modelo

Visibilidad y Mitigación de Amenazas

- Índice de riesgo de red, activos críticos y riesgo del estado del anfitrión, gravedad del riesgo de amenaza para la seguridad del anfitrión
- Mapeo del Kill Chain sobre los eventos de amenaza en cada anfitrión N° 16
- Amenaza forense que incluye el análisis de las amenazas, base de conocimientos, la historia y los PCAP
- Normas de mitigación predefinidos y personalizados

Servicios de Red N° 10

- Enrutamiento dinámico (OSPF, BGP, RIPv2) N° 14
- Enrutamiento estático y por políticas
- Rutas controladas por la aplicación
- DHCP, NTP, Servidor DNS y proxy DNS incorporados
- Modo Tap - se conecta al puerto SPAN
- Modos de interface: sniffer, puerto agregado, loopback, VLAN (802.1Q y Trunking)
- Conmutación y enrutamiento de L2/L3
- Cable virtual (Capa 1) despliegue transparente en línea

Firewall N° 10

- Modos operativos: NAT/ruta, (puente) transparente, y modo mixto
- Objetos de política: predefinidos, personalizados y por agrupación de objetos
- Política de seguridad basada en la aplicación, el papel y la geolocalización
- Gateways a nivel de aplicación y soporte de sesiones: MSRCP, PPTP, RAS, RSH, SIP, FTP, TFTP, HTTP, dcerpc, dns-tcp, dns-udp, H.245 0, H.245 1, H.323
- Soporte NAT y ALG: NAT46, NAT64, NAT444, SNAT, DNAT, PAT, Full Cone NAT, STUN
- Configuración de NAT: por política y por tabla NAT central
- VoIP: SIP/H.323/SCCP NAT traversal, RTP pin holing
- Vista de gestión de políticas globales
- Política de seguridad para inspección de redundancias
- Agendamiento: de una sola vez y recurrente

Prevención de Intrusiones

- Detección de anomalías de protocolo, detección basada en tasas, firmas personalizadas, actualización manual o automática de firmas, enciclopedia de amenazas integrada N° 14
- Acciones IPS: por defecto, monitoreo, bloqueado, reinicio (IP de los atacantes o de la víctima, interfaz de entrada) con tiempo de caducidad N° 16
- Opción de registro de paquetes
- Selección basada en filtros: gravedad, destino, sistema operativo, aplicación o protocolo N° 16
- Exención de IP de firmas específicas de IPS
- Modo rastreo IDS
- Protección DoS basada en tasas IPv4 e IPv6 con configuración de umbral contra inundaciones de TCP Syn, escaneo de puertos TCP/UDP/SCTP, barrido de ICMP, N° 14
  inundación de sesiones TCP/UDP/SCTP/ICMP (origen/destino) N° 16
- Bypass activo con interfaces de bypass
- Configuraciones de prevención predefinidas

Anti-Virus

- Manual, actualización automática de firmas push o pull
- Antivirus basado en flujos: protocolos que incluyen HTTP, SMTP, POP3, IMAP, FTP/SFTP N° 16
- Escaneo de virus en archivos compreso

Defensa contra Ataques

- Defensa contra ataques de protocolo anormal
- Anti-DoS/DDoS, incluyendo SYN Flood, defensa contra inundación de consultas DNS N° 16
- Defensa contra ataques ARP

Filtrado por URL N° 10

- Inspección de filtrado web basado en el flujo N° 13
- Filtrado web definido manualmente basado en URL, contenidos web y por cabecera MIME N° 15 N° 13
- Filtrado web dinámico con base en datos de categorización en tiempo real, basados en la nube: más de 140 millones de URLs con 64 categorías (8 de los cuales están relacionados con la seguridad)
- Características adicionales del filtrado web:
  - Filtrado de Applets de Java, ActiveX o de cookies N° 13 y 15
  - Bloqueo a Posteos HTTP
  - Registro de palabras clave de búsqueda
  - Por privacidad, conexiones cifradas exentas de exploración en ciertas categorías
- Anulación del perfil web de filtrado: permite que el administrador asigne temporalmente diferentes perfiles de usuario/grupo/IP
- Filtro Web para categorías locales y anulación de categorías calificadas

Anti-Spam N° 10

- Clasificación y prevención de spam en tiempo real
- Correo no deseado confirmado, correo no deseado sospechoso, correo no deseado masivo, bulto válido N° 17
- Protección Independientemente del idioma, formato o contenido del mensaje
- Admite protocolos de correo electrónico SMTP y POP3
- Detección de entrada y salida
- Listas blancas para permitir correos electrónicos de dominios de confianza

Cloud-Sandbox

- Carga archivos maliciosos a la nube en una sandbox para su análisis, incluyendo

tráfico cifrado HTTPS
- Se incluye el soporte de los siguientes protocolos HTTP/HTTPS, POP3, IMAP, SMTP y FTP
- Se incluye el soporte de los siguientes protocolos PE, ZIP, RAR, Office, PDF, APK, JAR y SWF
- Soporte de Transferencia de Archivos y Control de Tamaño de Archivos
- Proporciona un informe completo sobre el análisis del comportamiento de los archivos maliciosos
- Compartir la inteligencia de amenazas reales. Bloqueo de amenazas en tiempo real

Reputación de IP
- Bloqueo del IP del servidor Botnet con base de datos IP de reputación global

Descifrado SSL
- Identificación de la aplicación para el tráfico cifrado SSL
- Habilitación IPS para el tráfico cifrado SSL
- Habilitación AV para el tráfico cifrado SSL
- Filtro URL para tráfico cifrado SSL
- tráfico cifrado SSL y lista blanca
- Modo proxy por descarga SSL

Identificación de Puntos Finales
- Soporte e Identificación de Puntos Finales por Dirección IP, Identificación de Puntos Finales por Cantidad , Identificación de Puntos Finales por tiempo de Actividad en línea , Identificación de Puntos Finales por duración en el tiempo de Actividad en línea
- Soporte de 10 Sistemas Operativos
- Soporte de Búsquedas basadas en Dirección IP y Basadas en la Cantidades de Puntos Finales

Seguridad de datos
- Control de transferencia de archivos basado en el tipo de archivo
- Identificación del protocolo de archivos, incluidos HTTP, FTP, SMTP y POP3
- Identificación de firmas y sufijos de archivos para más de 100 tipos de archivos
- Filtrado de contenido para los protocolos HTTP-GET, HTTP-POST, FTP y SMTP
- Identificación de IM y auditoría de comportamiento de la red

Control de Aplicaciones
- Más de 3.000 aplicaciones se pueden filtrar por nombre, categoría, subcategoría, tecnología y por riesgo N° 13
- Cada aplicación contiene una descripción, sus factores de riesgo, dependencias, puertos típicos utilizados, y las URL de referencia adicionales
- Acciones: bloqueo, reinicio de la sesión, monitoreo, modulación del tráfico
- Identifica y controla aplicaciones en la nube
- Proporciona monitoreo multidimensional y estadísticas para las aplicaciones en la nube, incluyendo la categoría de los riesgos y sus características

Calidad de Servicio (QoS)
- Número máximo de túneles/ancho de banda garantizados o por IP/usuario
- Asignación de túnel basada en dominio de seguridad, interfaz, dirección, usuario/grupo, servidor/grupo de servidores, app/grupo de apps, TOS, VLAN
- Ancho de banda asignado por hora, prioridad, o reparto equitativo del ancho de banda
- Tipo de Servicio (TOS) y el soporte a servicios diferenciados (DiffServ)
- Asignación de prioridades de ancho de banda restante
- Número máximo de conexiones simultáneas por IP
- Asignación de ancho de banda según la categoría de URL

Servidores de Balanceo de Carga
- Hash ponderada, menor conexión ponderada y round-robin ponderado
- Protección de la sesión, persistencia de sesión y estado de la sesión de monitoreo
- Comprueba el estado del servidor, supervisión de sesiones y protección de sesiones

Balanceo de Carga en Enlaces
- Equilibrio de carga del enlace bidireccional N° 14
- Equilibrio de carga del enlace de salida que incluye política de enrutamiento, ECMP y ponderada, enrutamiento ISP integrado y detección dinámica
- Equilibrio de carga de enlaces de entrada soporta SmartDNS y detección dinámica
- Cambio de Enlace Automática basada en Anchos de Banda, Latencia, Variación, Conectividad, Aplicación , etc.
- Inspección del enlace con ARP, PING, y DNS

VPN
- VPN IPSec
- IPSEC Fase 1: Modo de protección agresiva y de ID principal
- Opciones de aceptación de colegas: cualquier ID, ID específica, ID en el grupo usuario de acceso telefónico

N° 12
- Soporta IKEv1 e IKEv2 (RFC 4306)
- Método de autenticación: certificado y una clave pre-compartida
- Configuración a modo de IKE (como servidor o cliente)
- DHCP por IPSec
- Caducidad de clave cifrada IKE configurable, NAT transversal para mantener viva la frecuencia N° 12
- Cifrado propuesto para Fase 1/Fase 2: DES, 3DES, AES128, AES192, AES256
- Autenticación propuesta para Fase 1/Fase 2: MD5, SHA1, SHA256, SHA384, SHA512
- Soporte Diffie-Hellman para Fase 1/Fase 2: 1,2,5
- XAuth como modo de servidor y para usuarios de acceso telefónico
- Detección de Punto Muerto
- Detección de Replay
- Autokey para mantener la conexión en la Fase 2 SA N° 12
- Apoyo total a IPSEC VPN: permite múltiples inicios de sesión SSL VPN personalizados asociados a grupos de usuarios (rutas de URL, diseño)
- Opciones de configuración IPSEC VPN: por rutas o por políticas N° 12
- Modos de implementación de VPN IPSec: puerta de enlace a puerta de enlace, malla

N° 12 completa, hub-and-spoke, túnel redundante, terminación de VPN en modo transparente
- Una sola entrada de tiempo impide conexiones concurrentes con el mismo nombre de usuario
- Limita usuarios concurrentes en portal SSL
- Módulo VPN SSL para reenvío de puertos encripta los datos del cliente y envía los datos al servidor de aplicaciones
- Acepta clientes que ejecutan iOS, Android y Windows XP/Vista, incluyendo el sistema operativo Windows de 64 bits
- Comprueba la integridad del host y del sistema operativo antes de conectar al túnel SSL
- Comprueba equipos MAC por portal
- Opción de limpieza del caché antes de finalizar la sesión SSL VPN
- Modo de servidor y cliente L2TP, L2TP sobre IPSec y GRE sobre IPSec N° 12
- Visualiza y administra conexiones IPSEC y SSL VPN
- PnPVPN

IPv6
- Gestión sobre IPv6, logueo IPv6 y HA
- Túneles IPv6, DNS64/NAT64 etc.
- Protocolos de enrutamiento IPv6, enrutamiento estático, enrutamiento por política, ISIS, RIPng, OSPFv3 y BGP4 +
- IPS, identificación de aplicaciones, filtrado de URL, antivirus, control de acceso, defensa contra ataques ND

VSYS
- Asignación de recursos del sistema para cada vSYS
- Virtualización de la CPU
- Soporte de Firewall No-root VSYS, IPSec VPN, VPN SSL, IPS, filtrado de URL
- Monitoreo vSYS y estadístico

Alta Disponibilidad
- Interfaces heartbeat redundantes
- Activo/Activo y Activo/Pasivo
- Sincronización de sesión autónoma
- Interfaz HA de gestión reservada
- Conmutación por error:
- Puerto, monitoreo de vínculos locales y remotos
- Con estado de conmutación por error
- Conmutación por error, inferior a un segundo
- Notificación de fallas
- Opciones de Implementación:
- HA con agregación de enlaces
- HA con malla completa
- HA geográficamente dispersa

Identidad de Usuario y Dispositivo N° 15
- Base de datos de usuario local
- Autenticación de usuario remoto: TACACS +, LDAP, Radius, Active N° 13 y 14
- Single-Sign-on: Windows AD
- Autenticación de 2 factores: Apoyo a terceros, servidor de contador integrado con token físico y SMS
- Políticas de usuario y por dispositivo
- Sincronización de grupos de usuarios basada en AD y LDAP
- Soporte para Proxy 802.1X, SSO
- Personalización de la página Web por medio de WebAuth
- Autenticación basada en interfaz
- Sin agente ADSSO (Polling AD)
- Usar sincronización de autenticación basada en SSO-monitor

Administración
- Acceso administrativo: HTTP/HTTPS, SSH, Telnet, consola
- Administración Central: Administrador de seguridad Hillstone (HSM), API de servicios web N° 14
- Integración de Sistemas: SNMP, Syslog, alianzas
- Despliegue rápido: Instalación automática de USB, ejecución local y remota del script
- Estado dinámico, en tiempo real del tablero de instrumentos y widgets de monitoreo drill-in
- Soporte de idiomas: Inglés

Registros e Informes
- Instalaciones para Registros: memoria y almacenamiento locales (si está disponible), múltiples servidores syslog y varias plataformas Hillstone para Auditoría de Seguridad (HSA)
- Cifrado de registros e integridad de registros con subida programada de lotes HSA
- Registro fiable utilizando la opción TCP (RFC 3195)
- Registros detallados del tráfico: reenviados, sesiones violadas, tráfico local, paquetes inválidos, URL, etc.
- Registro detallado de eventos: auditorías del sistema y de la actividad administrativa, enrutamiento y trabajo en red, VPN, autenticaciones de usuario, eventos relacionados con WiFi
- Opción de IP y servicio de resolución de nombres de puerto
- Opción de formato para breves registros del tráfico
- Tres informes predefinidos: Informes de seguridad, de flujo y de red
- Generación de informes definidos por el usuario
- Los informes se pueden exportar en formato PDF, a través de correo electrónico y FTP

CloudView
- Monitoreo de seguridad basado en la nube
- Acceso desde la web 7x24 o por medio de Aplicación móvil
- Estado del dispositivo, tráfico y monitoreo de amenazas
- Retención de logs e informes de registros basados en la nube

Detalles del Producto

Especificaciones	SG-6000-T1860	SG-6000-T2860	SG-6000-T3860	SG-6000-T5060	SG-6000-T5860
					
FW Throughput[1]	8Gbps N° 8	10Gbps	20Gbps	25Gbps	40Gbps
IPS Throughput[2]	3Gbps N° 7	4Gbps	8Gbps	12Gbps	18Gbps
AV Throughput[3]	1.6Gbps N° 6	2Gbps	6Gbps	7Gbps	10Gbps
IPSec Throughput[4]	3Gbps	3.8Gbps	12Gbps	15Gbps	28Gbps
IMIX Throughput[5]	1.6Gbps	2.1Gbps	8.2Gbps	10.9Gbps	17.4Gbps
NGFW Throughput[6]	1Gbps	1.5Gbps	5Gbps	8Gbps	12Gbps
Threat Protection Throughput[7]	600Mbps	900Mbps	2.5Gbps	4Gbps	6Gbps
New Sessions/s [8]	80K	100K	250K	300K	450K
Maximum Concurrent Sessions	1.5M N° 5	3M	4M	5M	6M
IPSec Tunnel Number	6,000	10,000	20,000	20,000	20,000
SSL VPN Users (Default/Max)	8/4,000	8/6,000	128/10,000	128/10,000	128/10,000
Integrated I/O	6 × GE, 4 × SFP	6 × GE(1 pair bypass port), 4 × SFP, 2 × SFP+	2 × GE, 4 × SFP	2 × GE, 4 × SFP	2 × GE, 4 × SFP
Maximum I/O	26 × GE	26 × GE, 2 × 10GE	22 × GE, 4 × 10GE	38 × GE, 8 × 10GE	38 × GE, 8 × 10GE
Expansion Modules	2 × Generic Slot N° 9	2 × Generic Slot	2 × Generic Slot	4 × Generic Slot	4 × Generic Slot
Expansion Module Option	IOC-4GE-B-M, IOC-8GE-M, IOC-8SFP-M	IOC-4GE-B-M, IOC-8GE-M, IOC-8SFP-M	IOC-8GE-M, IOC-8SFP-M, IOC-4GE-B-M, IOC-2XFP-Lite-M	IOC-8GE-M, IOC-8SFP-M, IOC-4GE-B-M, IOC-4XFP, IOC-8SFP+, IOC-4SFP+, IOC-2XFP-Lite-M(only supported at Slot-3/4) ,	IOC-8GE-M, IOC-8SFP-M, IOC-4GE-B-M, IOC-4XFP, IOC-8SFP+, IOC-4SFP+, IOC-2XFP-Lite-M (only supported at Slot-3/4)
Management Ports	1 × Concole Port, 1 × HA, 1 × MGT, 1 × USB 2.0, 1 × AUX Port N° 4	1 × Concole Port, 1 × HA, 1 × MGT, 1 × USB 2.0, 1 × AUX Port	1 × Console Port, 1 × AUX Port, 1 × USB 2.0 Port, 2 × HA, 1 × MGT	1 × Console Port, 1 × AUX Port, 1 × USB 2.0 Port, 2 × HA, 1 × MGT	1 × Console Port, 1 × AUX Port, 1 × USB 2.0 Port, 2 × HA, 1 × MGT
Maximum Power Consumption	1 × 150w Redundancy 1 + 1	1 × 150w Redundancy 1 + 1	2 × 450W Redundancy 1 + 1	2 × 450W Redundancy 1 + 1	2 × 450W Redundancy 1 + 1
Storage	N° 3 480G SSD (960G SSD Optional)	480G SSD (960G SSD Optional)	Dual Storage: 120G (480G or 960G SSD Optional) +480G SSD (960G SSD Optional)	Dual Storage: 120G (480G or 960G SSD Optional) +480G SSD (960G SSD Optional)	Dual Storage: 120G (480G or 960G SSD Optional) + 1T HDD (960G SSD Optional)
Power Supply	AC 100~240V 50/60Hz DC -40~-60V	AC 100~240V 50/60Hz DC -40~-60V	AC 100-240V 50/60Hz DC -40 ~ -60V	AC 100-240V 50/60Hz DC -40 ~ -60V	AC 100-240V 50/60Hz DC -40 ~ -60V
Dimension (W × D × H)	1U 17.2 × 14.4 × 1.7 in (436 × 366 × 44 mm)	1U 17.2 × 14.4 × 1.7 in (436 × 366 × 44 mm)	2 U 17.3 × 20.5 × 3.5 in (440 × 520 × 88 mm)	2 U 17.3 × 20.5 × 3.5 in (440 × 520 × 88 mm)	2 U 17.3 × 20.5 × 3.5 in (440 × 520 × 88 mm)
Weight	12.3 lb (5.6KG)	12.3 lb (5.6KG)	34.2 lb (15.5KG)	34.8 lb (15.8 KG)	34.8 lb (15.8 KG)
Temperature	32-104 F (0-40°C)	32-104 F (0-40°C)	32-104 F (0-40°C)	32-104 F (0-40°C)	32-104 F (0-40°C)
Relative Humidity	10-95%	10-95%	10-95%	10-95%	10-95%
Compliance and Certificate	CE, CB, FCC, UL/cUL, ROHS, IEC/EN61000-4-5 Power Surge Protection, ISO 9001:2015, ISO 14001:2015, CVE Compatibility, IPv6 Ready, ICSA Firewalls				

Opciones del Módulo

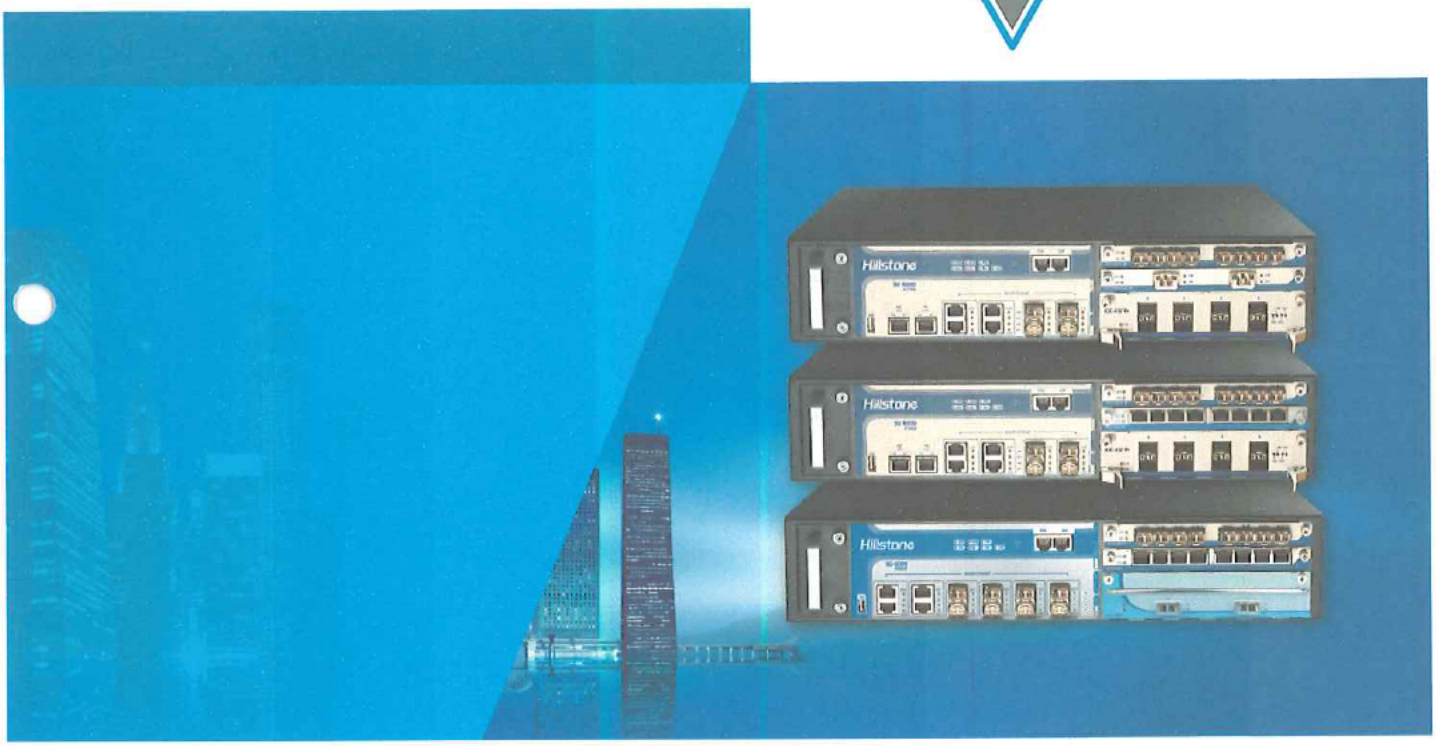
Especificaciones	IOC-8GE-M	IOC-8SFP-M	IOC-4GE-B-M	IOC-2XFP-Lite-M	IOC-4XFP	IOC-4SFP+	IOC-8SFP+
							
Name	8GE Extension Module	8SFP Extension Module	4GE Bypass Extension Module	2XFP Extension Module	4XFP Extension Module	4SFP+ Extension Module	8SFP+ Extension Module
I/O Ports	8 x GE	8 x SFP, SFP module not included	4 x GE Bypass (2 pair bypass ports)	2 x XFP, XFP module not included	4 x XFP, XFP module not included	4 x SFP+, SFP+ module not included	8 x SFP+, SFP+ module not included
Dimension	½ U (Occupies 1 generic slots)	½ U (Occupies 1 generic slot)	½ U (Occupies 1 generic slot)	½ U (Occupies 1 generic slot)	1 U (Occupies 2 generic slots)	1 U (Occupies 2 generic slots)	1 U (Occupies 2 generic slots)
Weight	1.8 lb (0.8kg)	2.0 lb (0.9kg)	1.8 lb (0.8kg)	2.0 lb (0.9kg)	2.0 lb (0.9kg)	1.5 lb (0.7kg)	1.5 lb (0.7kg)

A menos que se especifique lo contrario, todo el rendimiento, la capacidad y funcionalidad se basan en StoneOS 5.5R5. Los resultados pueden variar en función del StoneOS® versión y despliegue.

NOTAS: (1) Se obtuvieron datos FW rendimiento bajo tráfico UDP de sola pila con paquetes de 1518 bytes (2) se obtuvieron los datos de rendimiento IPSec bajo Preshare configuración AES256 + SHA-1 y paquetes 1400 bytes; (3) datos de rendimiento AV se obtuvieron bajo tráfico HTTP con el archivo adjunto; (4) para IPS se obtuvieron los datos de rendimiento bajo de detección de tráfico HTTP bi-direccional con todas las normas de IPS activadas; (5) Las capacidades de trougtput es obtenido de la siguiente manera (64 byte : 512 byte : 1518 byte = 5:7:1); (6) Los datos de rendimiento de NGFW se obtienen por debajo de 64 Kbytes de tráfico HTTP con control de aplicaciones e IPS habilitado; (7) Los datos de rendimiento de protección de amenazas se obtienen por debajo de 64 Kbytes de tráfico HTTP con control de aplicaciones, IPS, AV y filtrado de URL habilitados; (8) las Nuevas Sesiones se obtuvieron en virtud de tráfico TCP.

Hillstone™
NETWORKS

Firewall Hillstone Serie-E de Próxima Generación



El Firewall Hillstone Serie-E (NGFW) de Próxima Generación proporciona completa visibilidad y control granular sobre las aplicaciones. Puede identificar y prevenir amenazas potenciales asociadas con las aplicaciones de alto riesgo mientras que ofrece control basado en políticas para aplicaciones, usuarios y grupos. Se pueden definir políticas para garantizar el ancho de banda para aplicaciones de misión crítica mientras que se restringen o se bloquean las aplicaciones no autorizadas. El Hillstone Serie-E NGFW incorpora completa seguridad de red, características avanzadas como firewall, proporciona un rendimiento superior por precio, excelente eficiencia energética, y la capacidad integral para la prevención de amenazas.

Detalles del Producto

Identificación Granular y Control de Aplicaciones

El Hillstone Serie-E NGFW proporciona un control detallado de las aplicaciones web independientemente del puerto, protocolo o acción evasiva. Puede identificar y prevenir amenazas potenciales asociadas con las aplicaciones de alto riesgo mientras que ofrece control basado en políticas para aplicaciones, usuarios y grupos. Se pueden definir políticas de seguridad para garantizar el ancho de banda para aplicaciones de misión crítica mientras que se restringen o se bloquean las aplicaciones no autorizadas o maliciosas.

Detección Integral y Prevención de Amenazas

El Hillstone Serie-E NGFW, en tiempo real, proporciona protección para aplicaciones de ataques en la red como virus, spyware, gusanos, botnets, ARP Spoofing, DoS/DDoS, troyanos, desbordamientos de búfer, e inyecciones SQL. Incorpora un motor de detección de amenazas unificado que comparte los detalles del paquete con múltiples motores de seguridad (AD, IPS, filtrado por URL, anti-virus, sandbox, etc.), lo que mejora significativamente la eficacia de la protección y reduce la latencia de la red.

www.hillstonenet.com
Phone: 1-800-889-9860

Caracteristicas

Servicios de Red N° 9

* Enrutamiento dinámico (OSPF, BGP, RIPv2)
* Enrutamiento estático y por políticas N° 13
* Rutas controladas por la aplicación
- DHCP, NTP, Servidor DNS y proxy DNS incorporados
- Modo Tap - se conecta al puerto SPAN
- Modos de interface: sniffer, puerto agregado, loopback, VLAN (802.1Q y Trunking)
- Conmutación y enrutamiento de L2/L3
- Cable virtual (Capa 1) despliegue transparente en línea

Firewall N° 9

- Modos operativos: NAT/ruta, (puente) transparente, y modo mixto
- Objetos de política: predefinidos, personalizados y por agrupación de objetos
- Política de seguridad basada en la aplicación, el papel y la geolocalización
- Gateways a nivel de aplicación y soporte de sesiones: MSRCP, PPTP, RAS, RSH, SIP, FTP, TFTP, HTTP, dcerpc, dns-tcp, dns-udp, H.245 0, H.245 1, H.323
- Soporte NAT y ALG: NAT46, NAT64, NAT444, SNAT, DNAT, PAT, Full Cone NAT, STUN
- Configuración de NAT: por política y por tabla NAT central
- VoIP: SIP/H.323/SCCP NAT traversal, RTP pin holing
- Vista de gestión de políticas globales
- Política de seguridad para inspección de redundancias
- Agendamiento: de una sola vez y recurrente

Prevención de Intrusiones N° 13 y 15

* Detección de anomalías de protocolo, detección basada en tasas, firmas personalizadas, actualización manual o automática de firmas, enciclopedia de amenazas integrada N° 13
- Acciones IPS: por defecto, monitoreo, bloqueado, reinicio (IP de los atacantes o de la víctima, interfaz de entrada) (1)con tiempo de caducidad
- Opción de registro de paquetes
- Selección basada en filtros: gravedad, destino, sistema operativo, aplicación o protocolo
- Exención de IP de firmas específicas de IPS
- Modo rastreo IDS
* Protección DoS basada en tasas IPv4 e IPv6 con configuración de umbral N° 15 contra inundaciones de TCP Syn, escaneo de puertos TCP/UDP/SCTP, barrido de ICMP, inundación de sesiones TCP/UDP/SCIP/ICMP (origen/destino)
- Bypass activo con interfaces de bypass
- Configuraciones de prevención predefinidas

Anti-Virus N° 12

- Manual, actualización automática de firmas push o pull
* Antivirus basado en flujos: protocolos que incluyen HTTP, SMTP, POP3, IMAP, FTP/SFTP N° 15
- Escaneo de virus en archivos compreso

Defensa contra Ataques

* Defensa contra ataques de protocolo anormal N° 15
* Anti-DoS/DDoS, incluyendo SYN Flood, defensa contra inundación de consultas DNS N° 13 y 15
- Defensa contra ataques ARP

Filtrado por URL N° 9 y 12

- Inspección de filtrado web basado en el flujo
* Filtrado web definido manualmente basado en URL, contenidos web y por cabecera MIME N° 14
- Filtrado web dinámico basado en la nube para bases de datos con categorización en tiempo real: más de 140 millones de URLs con 64 categorías (8 de los cuales están relacionados con la seguridad) N° 14
- Características adicionales del filtrado web:

- Filtrado de Applets de Java, ActiveX o de cookies N° 12 y 14
- Bloqueo a Posteos HTTP
- Registro de palabras clave de búsqueda
- Por privacidad, conexiones cifradas exentas de exploración en ciertas categorías
* Anulación del perfil web de filtrado: permite que el administrador asigne temporalmente diferentes perfiles de usuario/grupo/IP N° 12
* Filtro Web para categorías locales y anulación de categorías calificadas

Cloud-Sandbox

- Carga archivos maliciosos a la nube en una sandbox para su análisis, incluyendo el tráfico cifrado HTTPS
- Se incluye el soporte de los siguientes protocolos HTTP/HTTPS, POP3, IMAP, SMTP y FTP
- Se incluye el soporte de los siguientes protocolos PE, ZIP, RAR, Office, PDF, APK, JAR y SWF
- Soporte de Transferencia de Archivos y Control de Tamaño de Archivos
- Proporciona un informe completo sobre el análisis del comportamiento de los archivos maliciosos
- Compartir la inteligencia de amenazas reales. Bloqueo de amenazas en tiempo real

Reputación de IP

- Bloqueo del IP del servidor Botnet basado en datos IP de reputación global

Descifrado SSL

- Identificación de la aplicación para el tráfico cifrado SSL
- Habilitación IPS para el tráfico cifrado SSL
- Habilitación AV para el tráfico cifrado SSL
* Filtro URL para tráfico cifrado SSL N° 14
- Tráfico cifrado SSL y de lista blanca
- Modo proxy por descarga SSL

Identificación de Puntos Finales

- Soporte e Identificación de Puntos Finales por Dirección IP, Identificación de Puntos Finales por Cantidad , Identificación de Puntos Finales por tiempo de Actividad en línea , Identificación de Puntos Finales por duración en el tiempo de Actividad en línea
- Soporte de 10 Sistemas Operativos
- Soporte de Búsquedas basadas en Dirección IP y Basadas en la Cantidades de Puntos Finales

Seguridad de datos

- Control de transferencia de archivos basado en el tipo de archivo
- Identificación del protocolo de archivos, incluidos HTTP, FTP, SMTP y POP3
- Identificación de firmas y sufijos de archivos para más de 100 tipos de archivos
- Filtrado de contenido para los protocolos HTTP-GET, HTTP-POST, FTP y SMTP
- Identificación de IM y auditoría de comportamiento de la red

Control de Aplicaciones N° 14

* Más de 3.000 aplicaciones se pueden filtrar por nombre, categoría, subcategoría, tecnología y por riesgo N° 12
* Cada aplicación contiene una descripción, sus factores de riesgo, dependencias, puertos típicos utilizados, y las URL de referencia adicionales
* Acciones: bloqueo, reinicio de la sesión, monitoreo, modulación del tráfico N° 15
- Identifica y controla aplicaciones en la nube
- Proporciona monitoreo multidimensional y estadísticas para las aplicaciones en la nube, incluyendo la categoría de los riesgos y sus características

Calidad de Servicio (QoS)

- Número máximo de túneles/ancho de banda garantizados o por IP/usuario
- Asignación de túnel basada en dominio de seguridad, interfaz, dirección, usuario/grupo, servidor/grupo de servidores, app/grupo de apps, TOS, VLAN
- Ancho de banda asignado por hora, prioridad, o reparto equitativo del ancho de banda

- Tipo de Servicio (TOS) y el soporte a servicios diferenciados (DiffServ)
- Asignación de prioridades de ancho de banda restante
- Número máximo de conexiones simultáneas por IP
- Asignación de ancho de banda según la categoría de URL

Servidores de Balanceo de Carga

- Hash ponderada, menor conexión ponderada y round-robin ponderado
- Protección de la sesión, persistencia de sesión y estado de la sesión de monitoreo
- Comprueba el estado del servidor, supervisión de sesiones y protección de sesiones

Balanceo de Carga en Enlaces

- Equilibrio de carga del enlace bidireccional N° 13
- Equilibrio de carga del enlace de salida que incluye política de enrutamiento, ECMP y ponderada, enrutamiento ISP integrado y detección dinámica
- Equilibrio de carga de enlaces de entrada soporta SmartDNS y detección dinámica
- Cambio de Enlace Automática basada en Anchos de Banda, Latencia, Variación, Conectividad, Aplicación , etc.
- Inspección del enlace con ARP, PING, y DNS

VPN

- VPN IPSec
- IPSEC Fase 1: Modo de protección agresiva y de ID principal
- Opciones de aceptación de colegas: cualquier ID, ID específica, ID en el grupo usuario de acceso telefónico
- Soporta IKEv1 e IKEv2 (RFC 4306)
- Método de autenticación: certificado y una clave pre-compartida
- Configuración a modo de IKE (como servidor o cliente) N° 11
- DHCP por IPSec
- Caducidad de clave cifrada IKE configurable, NAT transversal para mantener viva la frecuencia
- Cifrado propuesto para Fase 1/Fase 2: DES, 3DES, AES128, AES192, AES256 N° 11
- Autenticación propuesta para Fase 1/Fase 2: MD5, SHA1, SHA256, SHA384, SHA512
- Soporte Diffie-Hellman para Fase 1/Fase 2: 1,2,5
- XAuth como modo de servidor y para usuarios de acceso telefónico
- Detección de Punto Muerto
- Detección Replay
- Autokey para mantener la conexión en la Fase 2 SA N° 11
- Apoyo total a IPSEC VPN: permite múltiples inicios de sesión SSL VPN personalizados asociados a grupos de usuarios (rutas de URL, diseño)
- Opciones de configuración IPSEC VPN: por rutas o por políticas
- Modos de implementación de VPN IPSec: puerta de enlace a puerta de enlace, malla completa, hub-and-spoke, túnel redundante, terminación de VPN en modo transparente N° 11
- Una sola entrada de tiempo impide conexiones concurrentes con el mismo nombre de usuario
- Limita usuarios concurrentes en portal SSL
- Módulo VPN SSL para reenvío de puertos encripta los datos del cliente y envía los datos al servidor de aplicaciones
- Acepta clientes que ejecutan iOS, Android y Windows XP/Vista, incluyendo el sistema operativo Windows de 64 bits
- Comprueba la integridad del host y del sistema operativo antes de conectar al túnel SSL
- Comprueba equipos MAC por portal
- Opción de limpieza del caché antes de finalizar la sesión SSL VPN
- Modo de servidor y cliente L2TP, L2TP sobre IPSec y GRE sobre IPSec N° 11
- Visualiza y administra conexiones IPSEC y SSL VPN
- PnPVPN

IPv6

- Gestión sobre IPv6, logueo IPv6 y HA
- Túneles IPv6, DNS64/NAT64 etc.
- Protocolos de enrutamiento IPv6, enrutamiento estático, enrutamiento por política, ISIS, RIPng, OSPFv3 y BGP4 +
- IPS, identificación de aplicaciones, filtrado de URL, antivirus, control de acceso, defensa contra ataques ND

VSYS

- Asignación de recursos del sistema para cada vSYS
- Virtualización de la CPU
- Soporte de Firewall No-root VSYS, IPSec VPN, VPN SSL, IPS, filtrado de URL
- Monitoreo vSYS y estadístico
- No compatible con E1600, E1100W y E1100W3Gw

Alta Disponibilidad

- Interfaces heartbeat redundantes
- Activo/Activo y Activo/Pasivo
- Sincronización de sesión autónoma
- Interfaz HA de gestión reservada
- Conmutación por error:
- Puerto, monitoreo de vínculos locales y remotos
- Con estado de conmutación por error
- Conmutación por error, inferior a un segundo
- Notificación de fallas
- Opciones de Implementación:
- HA con agregación de enlaces
- HA con malla completa
- HA geográficamente dispersa

Identidad de Usuarios y Dispositivos N° 12 y 14

- Base de datos de usuario local N° 12 y 13
- Autenticación de usuario remoto: TACACS +, LDAP, Radius, Active
- Single-Sign-on: Windows AD
- Autenticación de 2 factores: Apoyo a terceros, servidor de contador integrado con token físico y SMS
- Políticas de usuario y por dispositivo
- Sincronización de grupos de usuarios basada en AD y LDAP
- Soporte para Proxy 802.1X, SSO
- Personalización de la página Web por medio de WebAuth N° 13
- Autenticación basada en interfaz
- Sin agente ADSSO (Polling AD)
- Usar sincronización de autenticación basada en SSO-monitor

Administración

- Acceso administrativo: HTTP/HTTPS, SSH, Telnet, consola
- Administración Central: Administrador de seguridad Hillstone (HSM), API de servicios web
- Integración de Sistemas: SNMP, Syslog, alianzas
- Despliegue rápido: Instalación automática de USB, ejecución local y remota del script
- Estado dinámico, en tiempo real del tablero de instrumentos y widgets de monitoreo drill-in
- Soporte de idiomas: Inglés

Registros e Informes

- Instalaciones para Registros: memoria y almacenamiento locales (si está disponible), múltiples servidores syslog y varias plataformas Hillstone para Auditoría de Seguridad (HSA)
- Cifrado de registros e integridad de registros con subida programada de lotes HSA
- Registro fiable utilizando la opción TCP (RFC 3195)
- Registros detallados del tráfico: reenviados, sesiones violadas, tráfico local, paquetes inválidos, URL, etc.
- Registro detallado de eventos: auditorías del sistema y de la actividad administrativa, enrutamiento y trabajo en red, VPN, autenticaciones de usuario, eventos relacionados con WiFi
- Opción de IP y servicio de resolución de nombres de puerto
- Opción de formato para breves registros del tráfico
- Tres informes predefinidos: Informes de seguridad, de flujo y de red
- Generación de informes definidos por el usuario
- Los informes se pueden exportar en formato PDF, a través de correo electrónico y FTP N° 13

156

CloudView

- Monitoreo de seguridad basado en la nube
- Acceso desde la web 7x24 o por medio de Aplicación móvil
- Estado del dispositivo, tráfico y monitoreo de amenazas
- Retención de logs e informes de registros basados en la nube

Inalámbrico

- Multi-SSID y control del tráfico inalámbrico (sólo en E1100W y E1100WG3w)
- Enlace de alambre y enlace WCDMA para copia de seguridad (Sólo el E1100WG3w)
- WCDMA VPN IPSec (Sólo el E1100WG3w)

Especificaciones del Producto

Especificaciones	SG-6000-E1100W	SG-6000-E1100WG3w	SG-6000-E1600	SG-6000-E1606	SG-6000-E1700
					
FW Throughput [1]	1Gbps	1Gbps	1Gbps	1Gbps	1.5Gbps/2Gbps N° 7
IPSec Throughput[2]	600Mbps	600Mbps	600Mbps	600Mbps	700Mbps
AV Throughput[3]	300Mbps	300Mbps	300Mbps	300Mbps	500Mbps N° 5
IPS Throughput [4]	400Mbps	400Mbps	400Mbps	400Mbps	600Mbps N° 6
IMIX Throughput [5]	200Mbps	200Mbps	200Mbps	200Mbps	600Mbps
NGFW Throughput[6]	350Mbps	350Mbps	350Mbps	350Mbps	450Mbps
Threat Protection Throughput[7]	300Mbps	300Mbps	300Mbps	300Mbps	400Mbps
New Sessions/s[8]	10,000	10,000	10,000	12,000	25,000
Maximum Concurrent Sessions (Default/Max)	200k	200k	200k	400k	600K/1M N° 4
IPSec Tunnel Number	512	512	512	1,000	2,000
SSL VPN Users (Default/Max)	8/128	8/128	8/128	8/500	8/500
Management Ports	1 x Console Port 1 x USB Port	1 x Console Port 1 x USB Port	1 x Console Port 1 x USB Port	1 x Console Port 1 x USB Port	1 x Console Port 1 x USB Port
Fixed I/O Ports	9 x GE	9 x GE	9 x GE	9 x GE	9 x GE
WiFi	IEEE802.11a/b/g/n	IEEE802.11a/b/g/n	N/A	N/A	N/A
3G	NA	WCDMA	N/A	N/A	N/A
Maximum Power Consumption	30W	30W	30W	1×45W Redundancy 1+1	1×45W Redundancy 1+1 N° 3
Power Supply	AC 100-240V 50/60Hz	AC 100-240V 50/60Hz	AC 100-240V 50/60Hz	AC:100-240V 50/60Hz	AC:100-240V 50/60Hz DC-40~-60V
Dimension (W×D×H, mm)	Desktop 12.6 × 5.91 × 1.7 in (320×150×44 mm)	Desktop 12.6 × 5.91 × 1.7 in (320×150×44 mm)	Desktop 12.6 × 5.91 × 1.7 in (320×150×44 mm)	1U 17.4 x 9.5 x 1.7in (442 x 241 x 44mm)	1U 17.4 x 9.5 x 1.7in (442 x 241 x 44mm)
Weight	3.3lb (1.5KG)	3.3lb (1.5KG)	3.3lb (1.5KG)	5.5lb (2.5kg)	5.5lb (2.5kg)
Temperature	32-104 F (0-40°C)	32-104 F (0-40°C)	32-104 F (0-40°C)	32-104F (0-40°C)	32-104F (0-40°C)
Relative Humidity	10-95% (no dew)	10-95% (no dew)	10-95% (no dew)	10-95% (no dew)	10-95% (no dew)
Compliance and Certificate	CE, CB, FCC, UL/cUL, ROHS, IEC/EN61000-4-5 Power Surge Protection, ISO 9001:2015, ISO 14001:2015, CVE Compatibility, IPv6 Ready, ICSA Firewalls				

IMAGENES

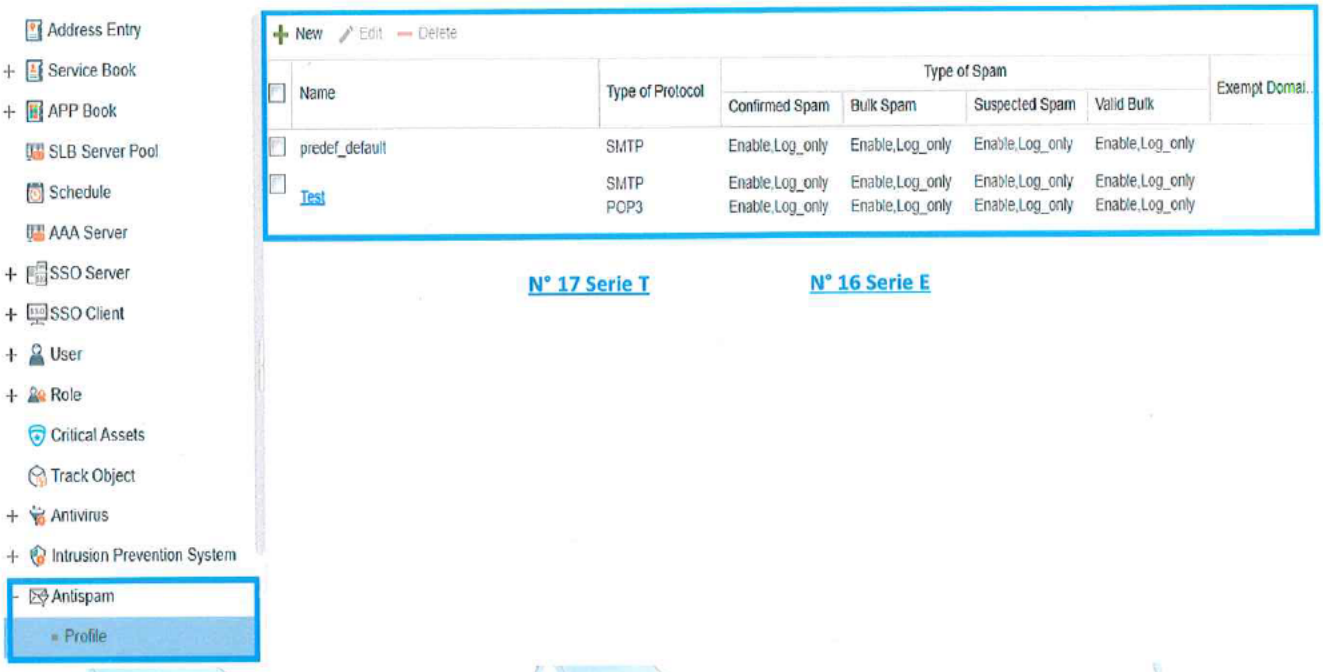
Security Technologies

[redacted]

[redacted]

IMAGEN 1 PROTECCIÓN DE CORREO ELECTRÓNICO

1 Protección de correo electrónico



N° 17 Serie T

N° 16 Serie E

Security Technologies

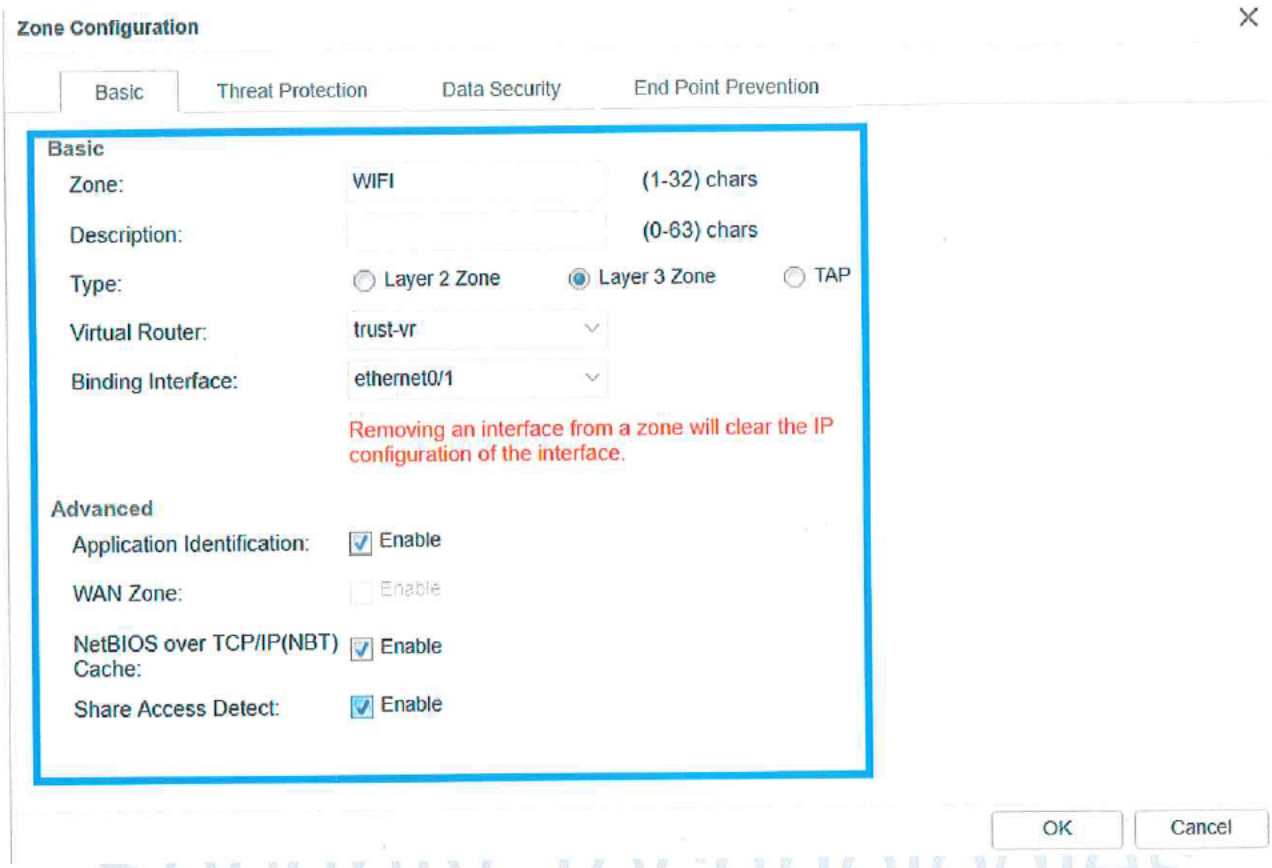
[redacted]

[redacted]

[redacted]

IMAGEN 2 PROTECCIÓN DE REDES INÁLAMBRICAS

2 Protección de redes inalámbricas N° 18 Serie T N° 17 Serie E



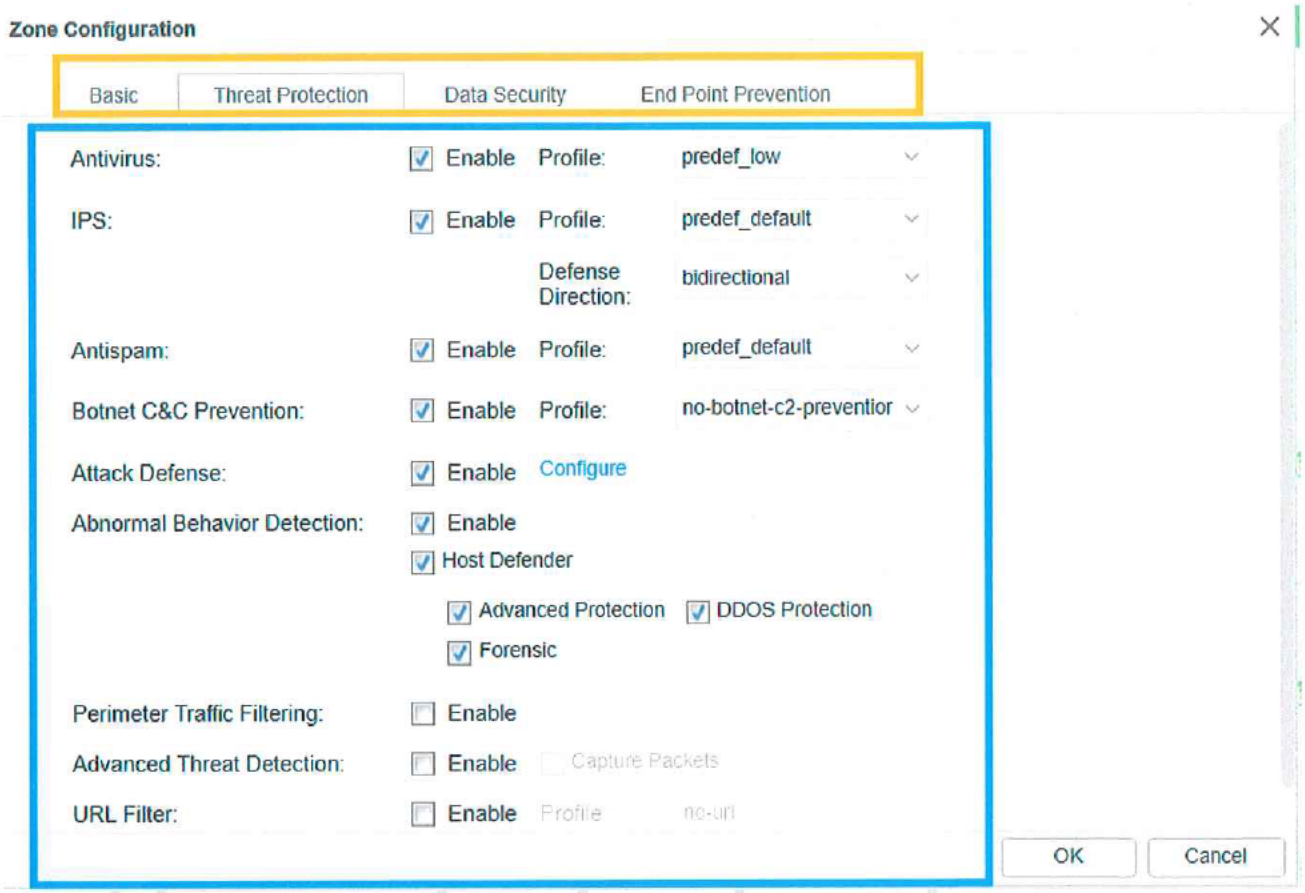
Security Technologies

[redacted]

[redacted]

[redacted]

IMAGEN 2.1 PROTECCIÓN DE REDES INÁLAMBRICAS



Security Technologies

[redacted]

Hillstone Next Generation Firewall

N° 13 Serie T N° 12 Serie E

- Identify applications regardless of port, protocol, or evasive action
- Identify users regardless of IP address
- Identify and prevent potential threats associated with high risk applications
- Policy-based control over applications, users, and functionality
- Policy based routing and bandwidth management

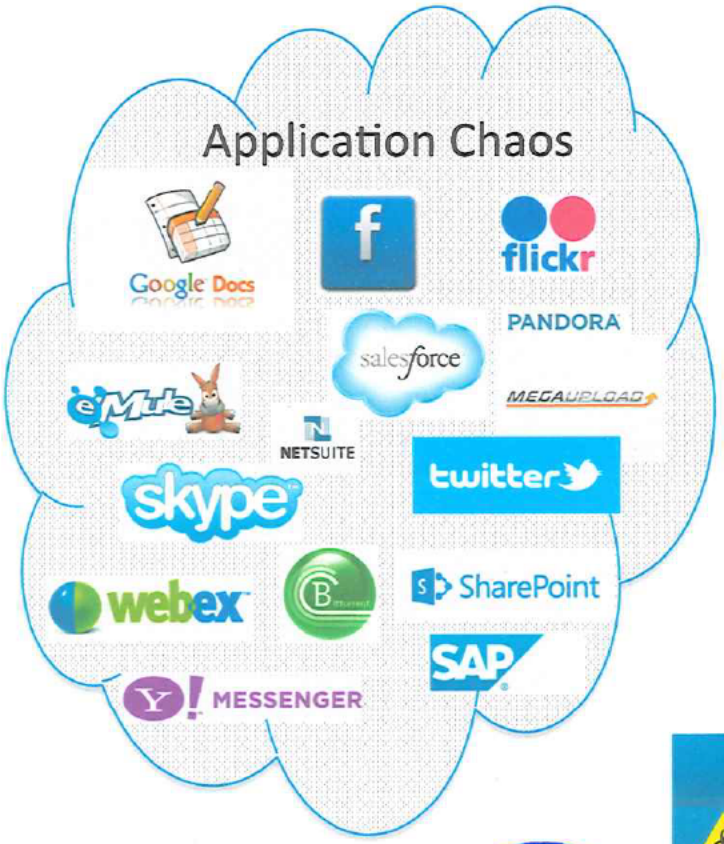


[redacted]

Visibility and Control

Hillstone NETWORKS

Identify



Categorize

N°15 Serie T

Users & Groups

N° 14 Serie E

Policies

Deep Packet Inspection

Blocked Malware

Viruses | Worms | Spyware | Trojans

Control

Critical Apps
Prioritized Bandwidth

salesforce SAP ORACLE ✔

Acceptable Apps
Managed Bandwidth

YouTube f twitter ✔

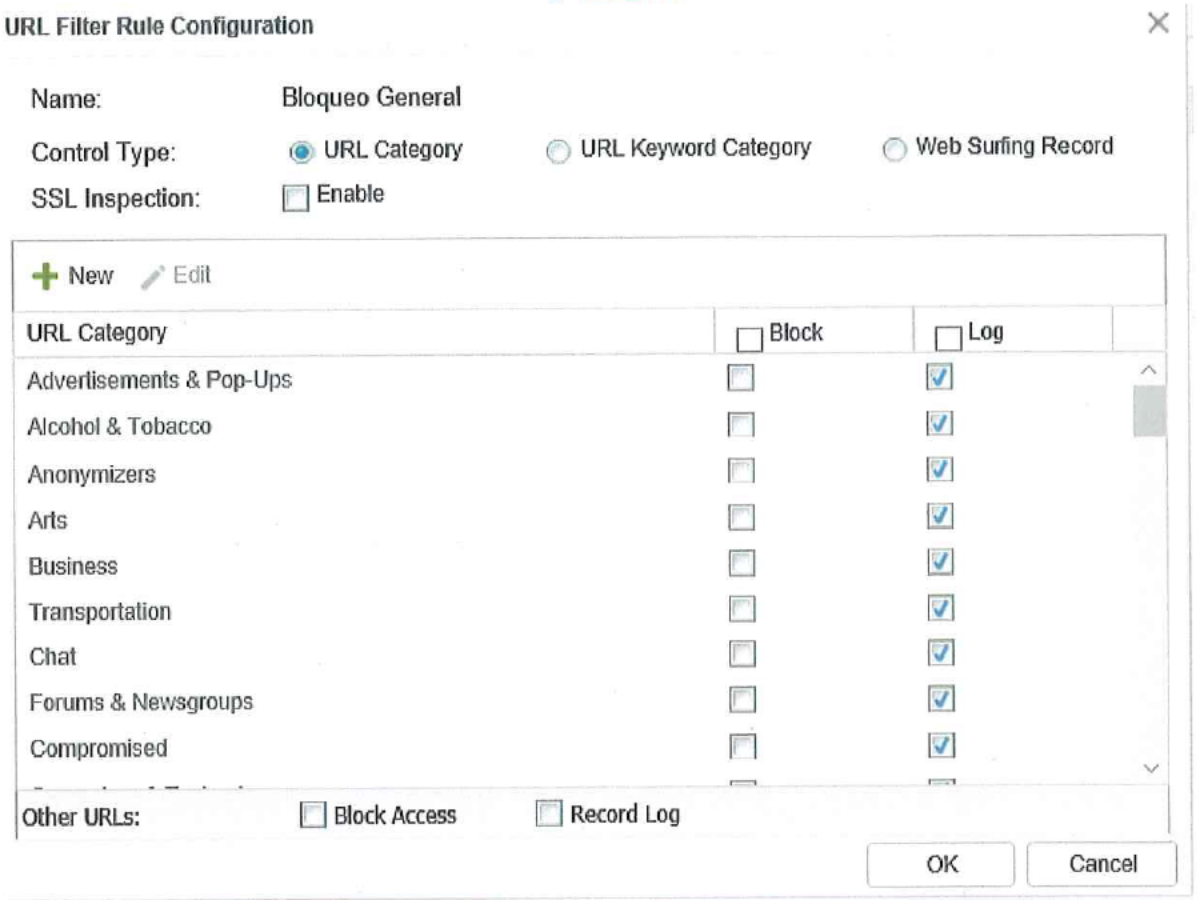
Unacceptable Apps
Blocked

eMule MEGAUPLOAD ✖

[redacted]

IMAGEN 6 LISTA DE EXCEPCIONES DE URL

N° 15 Serie T

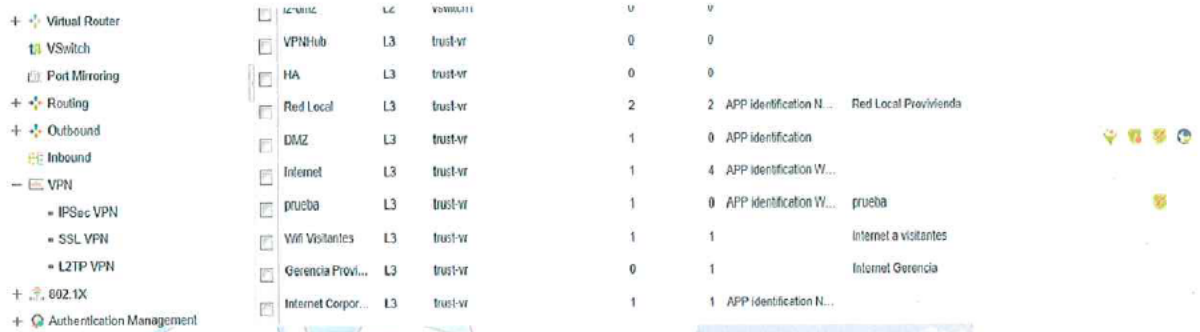


Security Technologies

[redacted]

[redacted]

IMAGEN 7 CERTIFICACIONES VPN



Security Technologies

[redacted]

Security Technologies

JL SECURITY TECHNOLOGIES

Seguridad en Internet

Hillstone NETWORKS

OFERTA ECONOMICA

ÍTEM	CANT.	DESCRIPCIÓN	PRECIO UNITARIO	PRECIO TOTAL
1	2	Equipo de Seguridad Hillstone T-1860 	$10,351.58	$20,703.16
	2	Licencia Equipo de Seguridad Hillstone T-1860 *	$1,150.18	$2,300.36
2	12	Equipo de Seguridad Hillstone E-1700 2 Gbps 	$1,618.97	$19,427.64
	12	Licencia Equipo de Seguridad Hillstone E-1700 2 Gbps *	$179.89	$2,158.68
3	5	Equipo de Seguridad Hillstone E-1700 1.5 Gbps 	$1,380.24	$6,901.20
	5	Licencia Equipo de Seguridad Hillstone E-1700 1.5 Gbps *	$153.36	$766.80
			TOTAL	**$52,257.84**

NOTA: * Hillstone Networks ha otorgado a JL Security para este proyecto un descuento especial. Vale aclarar que el costo de renovación de licencias para el próximo año no será el mismo que el contemplado en la presente oferta

Security Technologies

[redacted]

TERMINOS Y CONDICIONES DE OFERTA.

- Todos los precios están expresados en Dólares de los Estados Unidos de América
- Precios incluyen 13% de IVA
- Forma de pago: Crédito: 60 días.
- Validez de la oferta: 30 días calendario.
- Tiempo de entrega: Se realizará una sola entrega 15 días después de recibida la orden de compra.

FORMAS DE PAGO A LJ SECURITY TECHNOLOGIES.

- Depósito en cuenta bancaria:
  - [redacted]

INFORMACIÓN GENERAL DE JL SECURITY TECHNOLOGIES.

- Razón Social: [redacted]
- Nombre Com[redacted]
- N° de Identifi[redacted]
- N° de Registro[redacted]
- Giro o Actividad Económica: [redacted]
- Categoría de Contribuyente: Otro.
- Categoría de Empresa: Micro Empresa.

"Posee capacidad legal para ofertar y contratar por el Estado, y se encuentra solvente en el cumplimiento de todas las obligaciones fiscales, municipales, de seguridad social y previsional, además de no estar incapacitado, ni inhabilitado para ofertar de acuerdo a lo establecido en los artículos 25, 26 y 158 de la Ley de Adquisiciones y Contrataciones de la Administración Pública (LACAP)"

"No empleo a niños, niñas y adolescentes por debajo de la edad mínima de admisión al empleo y se cumple con la normativa que prohíbe el trabajo infantil y de la protección a la persona adolecente trabajadora; en caso se comprobare por la Dirección General de Inspección de Trabajo del Ministerio de Trabajo y Previsión Social el incumplimiento de la normativa anterior; reconozco y acepto que la Institución contratante iniciará el procedimiento sancionatorio que dispone el Art. 160 de la LACAP para determinar el sometimiento o no del procedimiento adquisitivo en el cual estoy participando, de la conducta tipificada como casual de inhabilitación prevista en el Art. 158 Romano V literal b) de la LACAP que dispone "invocar hechos falsos para obtener la Adjudicación de la Contratación" se entenderá por comprado el incumplimiento a la normativa por parte de la Dirección General de Inspección de Trabajo, si durante el trámite de la re inspección se determinara que hubo subsanación por haber cometido una infracción, o por el contrario si se remitiere a procedimiento sancionatorio, y en este último caso deberá finalizar el procedimiento para conocer la Resolución Final"

[redacted]

[redacted]

A sus órdenes.

[redacted]

Security Technologies

[redacted]

CARTAS DE REFERENCIA

Security Technologies

[redacted]

[redacted]

COMISION EJECUTIVA PORTUARIA AUTONOMA

Gerencia de Sistemas de Información

REFERENCIAS-GASI-153/2018

CARTA DE REFERENCIA

I. DATOS GENERALES DE LA INSTITUCIÓN:

1. Nombre de la Institución: **Comisión Ejecutiva Portuaria Autónoma (CEPA)**
2. Dirección: Boulevard de los Héroes, Colonia Miramonte Centro Comercial Metrocentro, Edificio Torre Roble, San Salvador.
   Número de teléfono: [redacted]
   Correo electrónico: [redacted]

3. A continuación proporcionar los siguientes datos.

II. IDENTIFICACIÓN DEL CONTRATO:

NOMBRE DEL CONTRATO: Contrato N° 21450 Derivado del Proceso de Compra CEPA MB-07/2015 "Suministro de Equipos de Seguridad Perimetral Informática y Equipos y Materiales de Comunicación para las empresas de CEPA"	
FECHA INICIO (DÍA, MES,AÑO)	Día: 11 Mes: Noviembre Año: 2015
FECHA FINALIZACION (DÍA, MES, AÑO)	Día: 09 Mes: enero Año: 2016
MONTO DEL CONTRATO EN US $	**$39,577.40 (Treinta y nueve mil quinientos setenta y siete 40/100 dólares.**

III. CALIDAD DEL SERVICIO:

INDICAR LA CALIDAD DEL SERVICIO RECIBIDO: **MARCAR CON UN "X" UNA SOLA VALORACIÓN.**	**REGULAR ( )** **BUENO ( )** **MUY BUENO ( )** **EXCELENTE (X)**

Y para ser presentada a la Unidad de Adquisiciones y Contrataciones Institucional (UACI), del Ministerio de Trabajo y Previsión Social, se extiende la presente constancia en la ciudad de San Salvador, a los veintiún días del mes de junio del dos mil dieciocho.

[redacted]

[redacted]

[redacted]

Cc. Archivo.

SIGAMOS creando futuro

GOBIERNO DE EL SALVADOR

142

San Salvador 21 de junio de 2018

Señores:
Ministerio de Trabajo y Previsión Social
Presente.

En atención al requerimiento señalado en la referencia y a solicitud de Jaret Naun Morán Sorto propietario de la empresa JL SECURITY TECHNOLOGIES, hacemos constar que dicha empresa, nos suministra los servicios de "Suministro, Instalación, Configuración y Soporte de Hillstone Next Generation Firewall modelos SG-6000-T1860 y SG-6000-E1100", señalando que de acuerdo a nuestros registros recibimos la experiencia de acuerdo al detalle siguiente:

NOMBRE DEL CONTRATO: Proceso de Libre Gestión N°11/2017 "Suministro de un dispositivo de Seguridad Perimetral (Firewall) para la red Informática de Oficina Central" Marca Hillstone modelo: SG-6000-T1860	
FECHA INICIO (DÍA, MES,AÑO)	Día: 30 Mes: Enero Año: 2017
FECHA FINALIZACION (DÍA, MES, AÑO)	Día: 03 Mes: Febrero Año: 2017
MONTO DEL CONTRATO EN US $	**$9,956.00 (Nueve mil novecientos cincuenta y seis 00/100 dólares)**

Nº	**DESCRIPCION DEL SERVICIO**	**CALIFICACION**		
		EXCELENTE	**BUENO**	**REGULAR**
1	**CALIDAD DEL SUMINISTRO**	X		
2	**ENTREGA DEL SERVICIO**	X		

Y para los efectos que se estimen convenientes extiendo la presente a los veintiún días del mes de junio de 2018.

[redacted]

141

N·CONACYT
CONSEJO NACIONAL DE CIENCIA Y TECNOLOGÍA
VICEMINISTERIO DE CIENCIA Y TECNOLOGÍA

Viceministerio Ciencia y Tecnología
MINISTERIO DE EDUCACIÓN

San Salvador, 21 de junio de 2018

CARTA DE REFERENCIA

I. DATOS GENERALES DE LA INSTITUCIÓN:

1. Nombre de la Institución: Consejo Nacional de Ciencia y Tecnología. N-CONACYT
   Dirección: Colonia Médica Avenida Dr. Emilio Álvarez, y Pasaje Dr. Guillermo Rodríguez Pacas, Edificio Espinoza #51, San Salvador.
   Número de teléfono: (503) 2234-8407
   Fax:
   Correo electrónico: dsalinas@conacyt.gob.sv

2. A continuación proporcionar los siguientes datos.

II. IDENTIFICACIÓN DEL CONTRATO:

NOMBRE DEL CONTRATO: Proceso de Libre Gestión N° 55-2017-ME –N CONACYT referente a la "Adquisición e instalación de Equipo Firewall, para el N-CONACYT", Marca Hillstone, Modelo: SG-6000-E2300.	
FECHA INICIO (DÍA, MES,AÑO)	Día: 16 Mes: Noviembre Año: 2017
FECHA FINALIZACION (DÍA, MES, AÑO)	Día: 15 Mes: Diciembre Año: 2017
MONTO DEL CONTRATO EN US $	**$3,815.00 (Tres mil ochocientos quince 00/100 dólares)**

III. CALIDAD DEL SERVICIO:

INDICAR LA CALIDAD DEL SERVICIO RECIBIDO: **MARCAR CON UN "X" UNA SOLA VALORACIÓN.**	**REGULAR** **BUENO** **MUY BUENO** **EXCELENTE**	( ) ( ) ( ) (✓)

Y para ser presentada a la Unidad de Adquisiciones y Contrataciones Institucional (UACI), del Ministerio de Trabajo y Previsión Social, se extiende la presente constancia en la ciudad de San Salvador, a los 21 días del mes de junio del 2018.

[redacted]

FIRMA: [redacted]	SELLO DE LA INSTITUCIÓN: [redacted]
NOMBRE [redacted]	
CARGO: Gestora en Indicadores ICT Nuevo Consejo de Ciencia y Tecnología	

[redacted]

CARTA DE REFERENCIA

I. DATOS GENERALES DE LA INSTITUCIÓN:

1. Nombre de la Institución: MULTI INVERSIONES MI BANCO [redacted]
   Número de teléfono: (503) 2212-1810
   Fax: (503) 2212-1850
   Correo electrónico: [redacted]

2. A continuación proporcionar los siguientes datos.

II. IDENTIFICACIÓN DEL CONTRATO:

NOMBRE DEL CONTRATO: SUMINISTRO, INSTALACIÓN Y CONFIGURACIÓN DE EQUIPO FIREWALL PARA NUEVA AGENCIA.	
FECHA INICIO (DÍA, MES,AÑO)	Día: 21 Mes: Marzo Año: 2018
FECHA FINALIZACION (DÍA, MES, AÑO)	Día: 21 Mes: Abril Año: 2018
MONTO DEL CONTRATO EN US $	**$1,700 (Un mil setecientos 00/100 dólares).**

III. CALIDAD DEL SERVICIO:

INDICAR LA CALIDAD DEL SERVICIO RECIBIDO: **MARCAR CON UN "X" UNA SOLA VALORACIÓN.**	**REGULAR ( )** **BUENO ( )** **MUY BUENO ( )** **EXCELENTE (X)**

Y para ser presentada a la Unidad de Adquisiciones y Contrataciones Institucional (UACI), del Ministerio de Trabajo y Previsión Social, se extiende la presente constancia en la ciudad de San Salvador, a los 21 días del mes de junio del 2018.

FIRMA: [redacted]	SELLO DE LA INSTITUCIÓN: [redacted]
NOMBRE: [redacted]	
CARGO: Jefe de Informática	

[redacted]

CARTAS COMPROMISO

Security Technologies

[redacted]

Security Technologies

JL SECURITY TECHNOLOGIES
Seguridad en Internet

Hillstone NETWORKS

COMPROMISO DE PRESENTAR GARANTÍA DE CUMPLIMIENTO DE CONTRATO

San Salvador, 22 de junio de 2018.

Señores:
Ministerio de Trabajo y Previsión Social
Presente.

Por este medio me comprometo a presentar una Garantía de Cumplimiento de Contrato, por el valor del 10% del monto adjudicado, vigente por un período de 15 días calendario. Así mismo, presentar dicha garantía dentro de los cinco días hábiles posteriores a la entrega y firma del contrato.

[redacted]

[redacted]

COMPROMISO DE PRESENTAR GARANTÍA DE BUEN FUNCIONAMIENTO Y CALIDAD DE LOS BIENES

San Salvador, 22 de junio de 2018.

Señores:
Ministerio de Trabajo y Previsión Social
Presente.

Por este medio me comprometo a presentar una Garantía de Buen Funcionamiento y Calidad de los Bienes, por el valor del 10% del monto adjudicado, vigente por un período de 1 año. Así mismo, presentar dicha garantía dentro de los cinco días hábiles posteriores a la recepción definitiva de los bienes.

[redacted]

[redacted]

CARTA DE DISTRIBUIDOR AUTORIZADO

JARET NAUN MORAN SORTO
TEL: 2225-0951
JL SEGURITY

[redacted]

[redacted]

20 de Junio de 2018

Señores
Ministerio de Trabajo
Presente.-

REF: "CERTIFICACIÓN DE CANAL DE VENTA HILLSTONE"

Estimados Señores:

Por la presente, y conforme a la relación contractual con **Hillstone Networks** y en el marco del proyecto de referencia, nos dirigimos a ustedes con el fin de informales que, para la fecha de esta comunicación, **Hillstone Networks** mantiene contratos suscritos con **JL Secuity Technologies** (el "Partner").

Para la fecha de esta comunicación, el Partner tiene la designación de **SILVER** estando autorizado a vender, instalar, soportar técnicamente y cumplir con la garantía de los productos de **Hillstone Networks** en todo el territorio de **El Salvador**.

Quedamos a sus órdenes ante cualquier aclaración o duda.

Atentamente,

[redacted]

[redacted]

[redacted]

CERTIFICACIONES DE TÉCNICOS

Security Technologies

[redacted]

[redacted]

Hillstone NETWORKS

This certifies that

Jaret Moran - Hillstone

has successfully completed

the requirements and is recognized as a

Hillstone Certified Security Associate

HCSA

HCSA0864

Valid From: Jul.8,2015

[redacted]

[redacted]

Hillstone NETWORKS

This certifies that

Otoniel Moran - Hillstone

has successfully completed

the requirements and is recognized as a

Hillstone Certified Security Associate

[redacted]

HCSA

HCSA0864
Valid From: Jul.8,2015

[redacted]

[redacted]

[redacted]

50

Hillstone NETWORKS

This certifies that

Nelson Aguirre - Hillstone

has successfully completed

the requirements and is recognized as a

Hillstone Certified Security Associate

[redacted]

HCSA0864
Valid From: Jul.8,2015

[redacted]

[redacted]

130

51

Hillstone™
NETWORKS

This certifies that

Jaret Moran - ***Hillstone***

has successfully completed

the requirements and is recognized as a

Hillstone Certified Security Professional

[redacted]

HCSP0723
Valid From: Sep.26,2015

[redacted]

[redacted]

129

Hillstone™
NETWORKS

This certifies that

Otoniel Moran - ***Hillstone***

has successfully completed

the requirements and is recognized as a

Hillstone Certified Security Professional



HCSP0723
Valid From: Sep.26,2015

[redacted]

[redacted]

53

Hillstone™
NETWORKS

This certifies that

Nelson Aguirre - ***Hillstone***

has successfully completed

the requirements and is recognized as a

Hillstone Certified Security Professional

HCSP

HCSP0723
Valid From: Sep.26,2015

[redacted]

[redacted]

127

05/06/2018
02:58:47 PM

INSTITUTO SALVADOREÑO DEL SEGURO SOCIAL

PLANILLA PREELABORADA PARA EL PAGO MENSUAL DE COTIZACIONES CON FACTURACIÓN DIRECTA REGIMEN DE SALUD

No. Recibo: 4996990
201806016456
FACTURACIÓN DIRECTA
MENSUAL
N° 0

1. Nombre Patrono	2. Fecha De Emisión	3. Número Patronal	4. Corr. Planilla	5. Hoja
JARET NAUN MORAN SORTO	05/06/2018	[redacted]	1	1
6. Dirección Del Patrono	7. Departamento y Municipio			8. Teléfono
[redacted]	SAN SALVADOR / MEJICANOS			22826511
9. Nombre Del Centro De Trabajo	10. NIT	11. Actividad Económica		12. Período De Pago
J L SECURITY TECHNOLOGIES	[redacted]	Otras actividades de tecnología de la información y de servicios informático		MAYO - 2018
13. Dirección Centro Trabajo		14. Departamento y Municipio		15. Teléfono
[redacted]		SAN SALVADOR / MEJICANOS		22826511

16. Corr.	17. Número De Afiliación	18. Nombre Según Tarjeta De Afiliación	19. Salario Devengado	20. Pago Adicional	21. Pago Vacaciones	22. Hrs. Jor.	23. Días Rem.	24. Días Vacación	25. Cod Obs.	26. Aporte Laboral	27. Aporte Patronal	28. Total Aporte
1	116890894	MENENDEZ RAMIREZ EDGARDO ALEXIS	310.00	0.00	0.00	8	31	0	0	9.30	23.25	32.55
2	112640053	MARTINEZ DIMAS MILTON ARNOLDO	310.00	0.00	0.00	8	31	0	0	9.30	23.25	32.55
3	113640036	ARGUETA MARIA ESTER GOMEZ	310.00	0.00	0.00	8	31	0	0	9.30	23.25	32.55
4	109885655	AGUIRRE AGUILAR NELSON JAIME	310.00	0.00	0.00	8	31	0	0	9.30	23.25	32.55
5	108820542	MORAN SORTO LUIS OTONIEL	310.00	0.00	0.00	8	31	0	0	9.30	23.25	32.55
6	108822970	NUÑEZ JEMIMAH ARELI DE MORAN	310.00	0.00	0.00	8	31	0	0	9.30	23.25	32.55
7	112873296	ROSALES TEJADA JOSE ANGEL	310.00	0.00	0.00	8	31	0	0	9.30	23.25	32.55
8	107844722	MORAN SORTO JARET NAUN	310.00	0.00	0.00	8	31	0	10	9.30	23.25	32.55
			2,480.00	0.00	0.00					74.40	186.00	260.40

RESERVADO AL ISSS

	APORTACIONES	MULTAS (25%)
SALUD	$ 260.40	$ 0.00
INSAFORP	$ 0.00	$ 0.00
TOTAL	$ 260.40	$ 0.00

TOTAL PLANILLA

TOTAL PLANILLA:	$ 260.40
MULTAS Y RECARGOS:	$ 0.00
TOTAL A PAGAR:	$ 260.40

[redacted]

N° 1 / 1

126

CARTA DE GESTIÓN DE GARANTÍA.

Security Technologies

[redacted]

[redacted]

San Salvador, 22 de junio de 2018

Señores
Ministerio de Trabajo y Previsión Social
Presente.

Yo Jaret Naún Morán Sorto, actuando como propietario de la empresa JL Security Technologies, por este medio hago constar que, de ser adjudicado en el proceso de Libre Gestión LG MTPS 12-2018 "ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS" para los equipos entregados según contrato se detalla en el siguiente cuadro el tiempo de garantía que se ofrece:

Equipo	Tiempo de garantía
• Item 1. 2 FIREWALL HILLSTONE MODELO SG-6000-T1860 • Item 2. 12 FIREWALL HILLSTONE MODELO SG-6000-E1700 • Item 3. 5 FIREWALL HILLSTONE MODELO SG-6000-E1700	1 año. Prorrogable con la renovación de las Licencias de cada Equipo.

Cuadro 1. Detalle de tiempos de garantía para equipos

La garantía ofrecida será aplicable por desperfectos de fabricación que presenten los equipos con las siguientes excepciones:

- ✓ Daños ocasionados por roedores o cualquier tipo de plagas.
- ✓ Fenómenos naturales tales como: inundaciones, terremotos, descargas eléctricas (rayos), incendios, etc.
- ✓ Por instalaciones eléctricas defectuosas o mala polarización en tomacorrientes de alimentación de los equipos.
- ✓ Ventilación deficiente o condiciones ambientales fuera del rango de trabajo que indican los fabricantes.
- ✓ Por derrames de líquidos y emanaciones químicas.
- ✓ Cualquier tipo de modificaciones o alteraciones al hardware interno.
- ✓ Mal uso de los equipos por parte de los usuarios o terceros.

[redacted]

19 calle poniente y 1ª Av. Norte, Edificio Niza local #205 Barrio San Miguelito, San Salvador. Tel. 2225-[redacted]

[redacted]

- ✓ Golpes o caídas de los equipos (intencionales o no).

En caso que los equipos presenten desperfectos de fabricación bastará con que El Ministerio de Trabajo y Previsión Social notifique por escrito a JL Security Technologies, se procederá a enviar un técnico para revisión del equipo, si la falla no puede ser solventada se procederá a solicitar el retiro del equipo para hacer pruebas y determinar la causa de la falla, entregando un equipo similar o de características mayores mientras dure la revisión del equipo, para que el Ministerio de Trabajo y Previsión Social pueda seguir laborando sin interrupciones.

Si el equipo no pasa las pruebas en el taller y presenta fallas que ameriten cambio de equipo se procederá a tramitar la garantía con el fabricante, para lo cual se requerirá de un período de 30 días calendario para contar con el equipo nuevo y poder llevar a cabo la entrega del equipo que el fabricante envíe en sustitución del dañado a el Ministerio de Trabajo y Previsión Social.

Para los usos pertinentes, me suscribo atentamente en la ciudad de San Salvador a los Veintidós días del mes de junio del año dos mil dieciocho.

[redacted]

Propietario de JL Security Technologies

Security Technologies

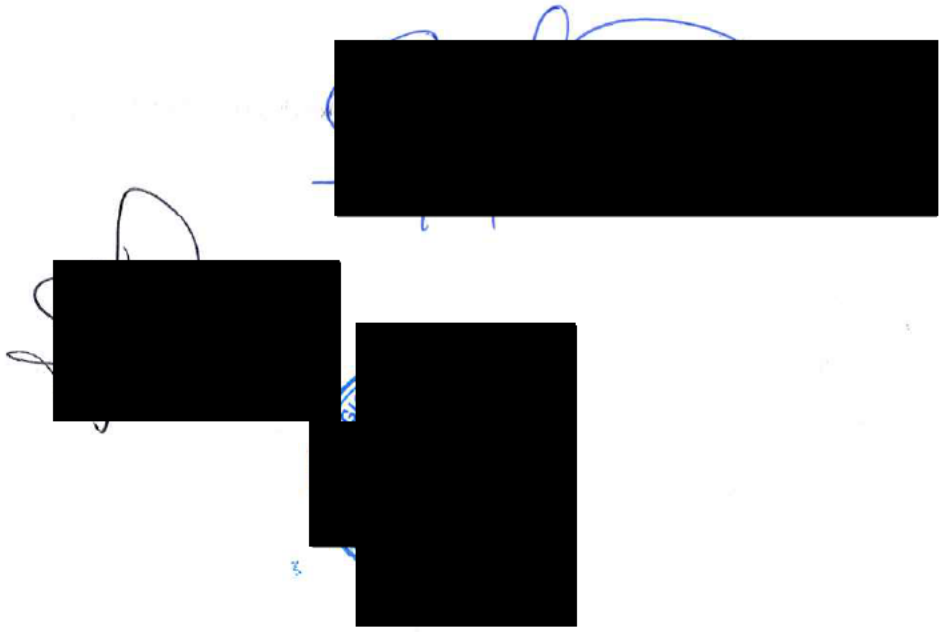
[redacted]

122

En la ciudad de San Salvador, a las diez horas del día veinte de junio dos mil dieciocho. Ante mí, [redacted] Notario, del domicilio de [redacted] comparece el señor J[redacted] de [redacted] años de edad, [redacted] del domicilio de [redacted] departamento de San Salvador, a quien conozco e identifico por medio de su Documento Único de Identidad número: [redacted]; actuando en su carácter personal; **Y ME DICE:** Que con el objeto de participar en el proceso de Libre Gestión número LG MTPS 12-2018 relativa a "ADQUISICION DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS" **BAJO JURAMENTO DECLARA: I)** Que en toda la cadena de producción de EQUIPO DE SEGURIDAD PERIMETRAL, ofertados a la institución por su empresa, no se utiliza en ningún trabajo a niñas, niños y adolescentes por debajo de la edad mínima de admisión al empleo y se cumple en todo el proceso, productivo, con la normativa laboral vigente y con las regulaciones relativas a la protección integral de la niñez y la adolescencia, que tienen por objeto garantizar el goce y respeto pleno de los derechos de los niños, niñas y adolescentes. **II)** Me declara el compareciente que cumple con la normativa nacional relacionada con la protección de la persona adolescente trabajadora, especialmente aquella relativa a la realización de actividades y trabajos peligrosos. **III)** Me continua manifestando el declarante que se compromete a vigilar que su empresa, así como sus proveedores, contratistas o subcontratistas, en toda la cadena de producción, estén libres de trabajo infantil y se respete el marco legal de protección de

[redacted]

la persona adolescente trabajadora. El suscrito Notario, hace constar que hice del conocimiento al compareciente lo regulado en el Código Penal, en cuanto al delito de falsedad ideológica, regulado en el artículo doscientos ochenta y cuatro. El compareciente me manifiesta que para los efectos legales de la presente acta notarial y para los que surgieren en el proceso de licitación, señala como domicilio especial el de esta ciudad a cuyos tribunales se somete expresamente. Así se expresó el compareciente a quien expliqué los efectos legales de esta acta notarial que consta de un folio útil y leído que le fue por mí íntegramente en un acto sin interrupción, ratifica su contenido y firmamos. DOY FE.



[redacted]

San Salvador, 22 de junio de 2018

Solicitud de Cotización para:

"ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"

LG MTPS 12- 2018

CLIENTE:

MINISTERIO DE TRABAJO Y PREVISION SOCIAL

[redacted]

[redacted]

Contenido

CARTA DE PRESENTACIÓN 3

OFERTA TÉCNICA 4

ESPECIFICACIONES TÉCNICAS 4

HOJAS TÉCNICAS DE LOS PRODUCTOS OFERTADOS 19

OFERTA ECONÒMICA 28

NUESTRO SERVICIO OFERTADO INCLUYE COMO VALOR AGREGADO (SIN COSTO ALGUNO): 30

MECANISMOS Y CONDICIONES A SEGUIR PARA HACER EFECTIVO EL REEMPLAZO EN GARANTÍA DEL EQUIPO: 31

CARTA DE COMPROMISO SOBRE COBERTURA DE EQUIPOS ACTUALES DURANTE IMPLEMENTACIÓN 32

CARTA DE COMPROMISO SOBRE GARANTÍA FIEL CUMPLIMIENTO 33

CARTA DE COMPROMISO SOBRE GARANTÍA BUEN FUNCIONAMIENTO 34

CARTA SOBRE PLAN DE PAGOS DE HACIENDA 35

DATOS GENERALES ACTIVE IT CORP 36

DECLARACIÓN JURADA 37

CARTAS DE REFERENCIA 39

CARTA DE AUTORIZACIÓN DEL FABRICANTE 43

CERTIFICACIONES DE NUESTRO PERSONAL TECNICO 45

[redacted]

[redacted]

CARTA DE PRESENTACIÓN

San Salvador, 22 de junio de 2018

Señores
Ministerio de Trabajo y Previsión Social- MTPS
Unidad de Adquisiciones y Contrataciones Institucional- UACI
Presente.

Atención: Licda. Mayra Palma
Jefa UACI Ad Honorem

Estimados Señores:

Agradeciendo la oportunidad que nos brindan de prestarles nuestros servicios les estamos presentando para su amable consideración la inversión a realizar para nuestra siguiente solución:

"ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"

No omitimos comentarles que nuestro servicio es realizado por Staff de Consultores Certificados en SOPHOS.

Aprovechamos la oportunidad para saludarles, quedando a su disposición para cualquier consulta o información adicional que deseen obtener.

Atentamente,

[redacted]

Active IT corp

[redacted]

OFERTA TÉCNICA

ESPECIFICACIONES TÉCNICAS

- **19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS**

CARACTERÍSTICAS DE EQUIPO AL QUE DEBERÁ ASOCIARSE LICENCIAMIENTO DE SEGURIDAD PERIMETRAL

SITIO PRINCIPAL Y SITIO REMOTO (SANTA ANA)			
CARACTERÍSTICA	**DESCRIPCIÓN**	**CUMPLE**	
Capacidad de usuarios	Hasta 1000	SI	
Cantidad de equipos	Dos	SI	
Configuración	Contingencia	SI	
Almacenamiento	240 GB mínimo	SI	
Consumo de energía	Fuente redundante 83W, 283 BTU/hr	SI	
Conexiones concurrentes	Mínimo 1 millón	SI	
AV rendimiento	Mínimo 1.5 GBPS	SI	
IPS rendimiento	Mínimo 2 GBPS	SI	
Firewall rendimiento	Mínimo 4 GBPS	SI	
Interfaces	Capacidad de ampliación	SI	
Módulos de protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPsec.	SI	
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.	SI	

[redacted]

[redacted]

VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.	SI	
Seguridad Web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS.	SI	
Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS.VPN punto a punto: SSL, IPsec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.	SI	
Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe de permitir / restringir / acceso a diferentes categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL	SI	

[redacted]

(503) 2510-7100
info@activesystems.com.sv
Residencial Villas de Santa Elena,
Calle Alegría, Casa 13-A.
Antiguo Cuscatlán.

	5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.		
IPS	1. Que el UTM soporte un motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.	SI	
Protección de correo electrónico	• Protección de correo electrónico contra spam • Protección contra suplantación de identidades y fuga de datos • Protección de la puerta de enlace del servidor de correo • Detección de correos no deseado en varias capas • Protección contra la suplantación de sitios web • Doble motor de Antirus • Escaneo profundo de archivos adjuntos • Cifrado SPX • Portal de usuario para gestionar correos no deseado del usuario final • Bloquear contenido expresiones y mime • Protección de TLS capa de transporte • Sincronización de Active Directory • Capacidad de crear informes integrados	SI	

[redacted]

[redacted]

	• Creación de política DLP a nivel de Correos		
Protección de redes inalámbricas	• Capacidad de centralizar y administrar AP desde el UTM • Configurar al menos 8 SSID por Estándar 2.4 – 5 GHz • Capacidad de Crear SSID fiables con acceso a la red local • Capacidad de Filtrar contenido a todos los SSID • Capacidad de crear redes mallas • Capacidad de crear varios perfiles de hotspot • Portal de administración de hotspot • Capacidad de Crear hotspot gestionado por ticket y correo electrónico • Capacidad de limitar ancho de banda y descarga por cada uno de los hotspot • Protección para los clientes conectados a las redes inalámbricas • Compatibilidad con Microsoft Lync y voz sobre ip • Capacidad de utilizar los estándares de cifrado WPA2-Enterprise y IEEE 802.1X • Capacidad de utilizar los estándares de autenticación RADIUS • Capacidad de utilizar Servidores de autenticación back-end AD, LDAP y LOCAL DEL UTM • Capacidad de personalizar la página de inicio de los clientes conectador • Compatibilidad con los estándares inalámbricos 802.11ac y 802.11n	SI	

[redacted]

Active IT corp

[redacted]

OTRAS			
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratados, para atender los requerimientos de soporte técnico.	SI	
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantías del equipo.	SI	
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.	SI	
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.	SI	

[redacted]

Active IT corp

[redacted]

CARACTERÍSTICAS DE EQUIPO AL QUE DEBERÁ ASOCIARSE LICENCIAMIENTO DE SEGURIDAD PERIMETRAL

OFICINAS REGIONALES (A EXCEPCIÓN DE SANTA ANA) Y DEPARTAMENTALES			
CARACTERÍSTICA	**DESCRIPCIÓN**	**CUMPLE**	
Capacidad de usuarios	Hasta 100	SI	
Cantidad de equipos	Doce	SI	
Almacenamiento	64 GB mínimo	SI	
Consumo de energía	20.04W, 68.336 BTU/hr	SI	
Conexiones concurrentes	Mínimo 600 K	SI	
AV rendimiento	Mínimo 500 MBPS	SI	
IPS rendimiento	Mínimo 400 MBPS	SI	
Firewall rendimiento	Mínimo 1.5 GBPS	SI	
Interfaces	Capacidad de ampliación	SI	
Módulos de protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPsec.	SI	
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.	SI	
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.	SI	

[redacted]

[redacted]

Seguridad Web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS.	SI	
Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS.VPN punto a punto: SSL, IPsec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.	SI	
Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe de permitir / restringir / acceso a diferentes categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.	SI	

[redacted]

[redacted]

IPS	1. Que el UTM soporte un motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.	SI	
Protección de correo electrónico	• Protección de correo electrónico contra spam • Protección contra suplantación de identidades y fuga de datos • Protección de la puerta de enlace del servidor de correo • Detección de correos no deseado en varias capas • Protección contra la suplantación de sitios web • Doble motor de Antirus • Escaneo profundo de archivos adjuntos • Cifrado SPX • Portal de usuario para gestionar correos no deseado del usuario final • Bloquear contenido expresiones y mime • Protección de TLS capa de transporte • Sincronización de Active Directory • Capacidad de crear informes integrados • Creación de política DLP a nivel de Correos	SI	

[redacted]

[redacted]

Protección de redes inalámbricas	• Capacidad de centralizar y administrar AP desde el UTM • Configurar al menos 8 SSID por Estándar 2.4 – 5 GHz • Capacidad de Crear SSID fiables con acceso a la red local • Capacidad de Filtrar contenido a todos los SSID • Capacidad de crear redes mallas • Capacidad de crear varios perfiles de hotspot • Portal de administración de hotspot • Capacidad de Crear hotspot gestionado por ticket y correo electrónico • Capacidad de limitar ancho de banda y descarga por cada uno de los hotspot • Protección para los clientes conectados a las redes inalámbricas • Compatibilidad con Microsoft Lync y voz sobre ip • Capacidad de utilizar los estándares de cifrado WPA2-Enterprise y IEEE 802.1X • Capacidad de utilizar los estándares de autenticación RADIUS • Capacidad de utilizar Servidores de autenticación back-end AD, LDAP y LOCAL DEL UTM • Capacidad de personalizar la página de inicio de los clientes conectador • Compatibilidad con los estándares inalámbricos 802.11ac y 802.11n	SI	

[redacted]

[redacted]

OTRAS			
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratados, para atender los requerimientos de soporte técnico.	SI	
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantías del equipo.	SI	
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.	SI	
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.	SI	

[redacted]

Active IT corp

[redacted]

CARACTERÍSTICAS DE EQUIPO AL QUE DEBERÁ ASOCIARSE LICENCIAMIENTO DE SEGURIDAD PERIMETRAL

CENTROS DE RECREACIÓN Y ARCHIVO GENERAL			
CARACTERÍSTICA	**DESCRIPCIÓN**	**CUMPLE**	
Capacidad de usuarios	Hasta 15	SI	
Cantidad de equipos	Cinco	SI	
Almacenamiento	64 GB mínimo	SI	
Consumo de energía	10.44W, 35.6 BTU/hr	SI	
Conexiones concurrentes	Mínimo 600 K	SI	
AV rendimiento	Mínimo 400 MBPS	SI	
IPS rendimiento	Mínimo 300 MBPS	SI	
Firewall rendimiento	Mínimo 900 MBPS	SI	
Interfaces	Capacidad de ampliación	SI	
Módulos de protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPsec.	SI	
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.	SI	
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.	SI	

[redacted]

Active IT corp

[redacted]

Seguridad Web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS.	SI	
Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS.VPN punto a punto: SSL, IPsec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.	SI	
Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe de permitir / restringir / acceso a diferentes categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.	SI	

[redacted]

[redacted]

IPS	1. Que el UTM soporte un motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.	SI	
Protección de correo electrónico	• Protección de correo electrónico contra spam • Protección contra suplantación de identidades y fuga de datos • Protección de la puerta de enlace del servidor de correo • Detección de correos no deseado en varias capas • Protección contra la suplantación de sitios web • Doble motor de Antirus • Escaneo profundo de archivos adjuntos • Cifrado SPX • Portal de usuario para gestionar correos no deseado del usuario final • Bloquear contenido expresiones y mime • Protección de TLS capa de transporte • Sincronización de Active Directory • Capacidad de crear informes integrados • Creación de política DLP a nivel de Correos	SI	

[redacted]

Active IT corp

[redacted]

Protección de redes inalámbricas	• Capacidad de centralizar y administrar AP desde el UTM • Configurar al menos 8 SSID por Estándar 2.4 – 5 GHz • Capacidad de Crear SSID fiables con acceso a la red local • Capacidad de Filtrar contenido a todos los SSID • Capacidad de crear redes mallas • Capacidad de crear varios perfiles de hotspot • Portal de administración de hotspot • Capacidad de Crear hotspot gestionado por ticket y correo electrónico • Capacidad de limitar ancho de banda y descarga por cada uno de los hotspot • Protección para los clientes conectados a las redes inalámbricas • Compatibilidad con Microsoft Lync y voz sobre ip • Capacidad de utilizar los estándares de cifrado WPA2-Enterprise y IEEE 802.1X • Capacidad de utilizar los estándares de autenticación RADIUS • Capacidad de utilizar Servidores de autenticación back-end AD, LDAP y LOCAL DEL UTM • Capacidad de personalizar la página de inicio de los clientes conectador • Compatibilidad con los estándares inalámbricos 802.11ac y 802.11n	SI	

[redacted]

Active IT corp

[redacted]

OTRAS			
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratados, para atender los requerimientos de soporte técnico.	SI	
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantías del equipo.	SI	
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.	SI	
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.	SI	

[redacted]

Active IT corp



HOJAS TÉCNICAS DE LOS PRODUCTOS OFERTADOS



Active IT corp

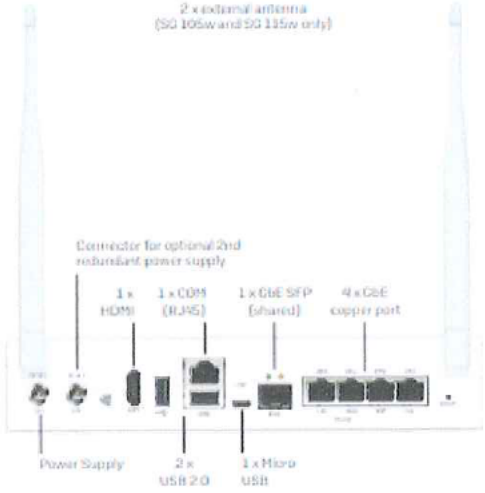
[redacted]

SOPHOS SG 115 SIN ANTENAS WIRELESS PARA LOS CINCO (5) FIREWALL DE CENTROS DE RECREACIÓN Y ARCHIVO GENERAL

Front View



Back View



Performance	SG 105(w) Rev. 3	SG 115(w) Rev. 3
Firewall throughput	2,500 Mbps	2,700 Mbps
VPN throughput	325 Mbps	425 Mbps
IPS throughput	350 Mbps	500 Mbps
Antivirus throughput (proxy)	380 Mbps	500 Mbps
Concurrent connections	1,000,000	1,000,000
New connections/sec	17,000	21,000
Maximum licensed users	unrestricted	unrestricted

Wireless Specification (SG 105w and SG 115w only)	
No. of antennas	2 external
MIMO capabilities	2 x 2:2
Wireless interface	802.11a/b/g/n /ac (2.4 GHz / 5 GHz)

Physical interfaces	
Storage (local quarantine/logs)	integrated SSD
Ethernet interfaces (fixed)	4 GbE copper 1 GbE SFP (shared)*
Connectivity modules (optional)	SFP DSL module (VDSL2) SFP transceivers
I/O ports (rear)	2 x USB 2.0 1 x Micro-USB 1 x COM (RJ45) 1 x HDMI
Power supply	External auto ranging DC: 12V, 100-240VAC, 36W@50-60 Hz Redundant PSU optional (external)

Environment	
Power consumption	8.88W, 30.28 BTU/hr (idle) 104W, 35.6 BTU/hr (full load)
Operating temperature	0-40°C (operating) -20 to +80°C (storage)
Humidity	10%-90%, non-condensing

Physical specifications	
Mounting	Rackmount kit available (to be ordered separately)
Dimensions Width x Depth x Height	225 x 150 x 44 mm 8.86 x 5.91 x 1.73 inches
Weight	1.11 kg / 2.45 lbs (unpacked) 1.84 kg / 4.06 lbs (packed)

Product Certifications	
Certifications	CB, UL, CE, FCC, ISED, VCCI, MIC (Japan), RCM, CCC, KC Planned: BIS

* SFP transceivers sold separately

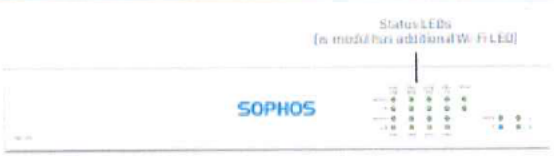
[redacted]

Active IT corp

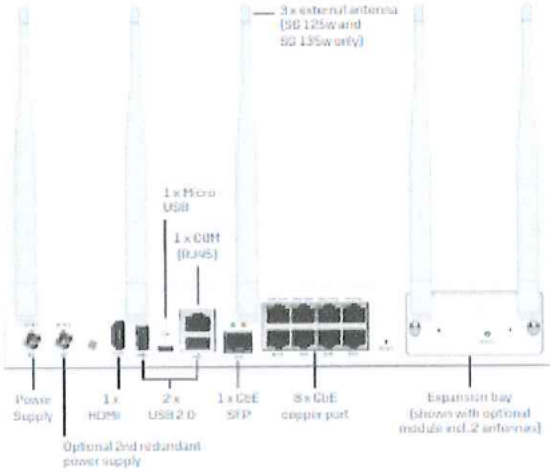
[redacted]

SOPHOS SG 135 SIN ANTENAS WIRELESS PARA LOS DOCE (12) FIREWALL DE **OFICINAS REGIONALES (A EXCEPCIÓN DE SANTA ANA) Y DEPARTAMENTALES** **RECOMENDADO POR TENER 8 INTERFACES DE COBRE GBE. ACTUALMENTE EN LAS OFICINAS REGIONALES SE UTILIZAN APROXIMADAMENTE 7 PUERTOS DE COBRE GBE**

Front View



Back View



Performance	SG 125(w) Rev. 3	SG 135(w) Rev. 3
Firewall throughput	3,100 Mbps	6,000 Mbps
VPN throughput	500 Mbps	1,000 Mbps
IPS throughput	750 Mbps	1,500 Mbps
Antivirus throughput (proxy)	700 Mbps	900 Mbps
Concurrent connections	2,002,930	2,002,930
New connections/sec	25,000	36,000
Maximum licensed users	unrestricted	unrestricted

Wireless Specification (SG 125w and SG 135w only)	
No. of antennas	3 external
MIMO capabilities	3 x 3:3
Wireless interface	802.11a/b/g/n/ac (2.4 GHz / 5 GHz)

Physical interfaces	
Storage (local quarantine/logs)	integrated SSD
Ethernet interfaces (fixed)	8 GbE copper 1 GbE SFP*
I/O ports (rear)	2 x USB 2.0 1 x Micro-USB 1 x COM (RJ45) 1 x HDMI
No. of expansion slots:	1
Connectivity Modules (optional):	SFP DSL module (VDSL2) 3G/4G module 802.11ac Wi-Fi radio 2x2:2 (SG 135w only) SFP transceivers
Power supply	External auto ranging DC: 12V, 100-240VAC, 36W@50-60 Hz Redundant PSU optional (external)

Environment	
Power consumption	18.6W, 63.426 BTU/hr (idle) 20.04W, 68.336 BTU/hr (full load)
Operating temperature	0-40°C (operating) -20 to +80°C (storage)
Humidity	10%-90%, non-condensing

Product Certifications	
Certifications	CB, UL, CE, FCC, ISED, VCCI, MIC (Japan), RCM, CCC, KC Planned: BIS

Physical specifications	
Mounting	Rackmount kit available (to be ordered separately)
Dimensions Width x Depth x Height	305 x 205 x 44 mm 12 x 8.07 x 1.73 inches
Weight	1.8 kg / 3.97 lbs (unpacked) 2.7 kg / 5.95 lbs (packed)

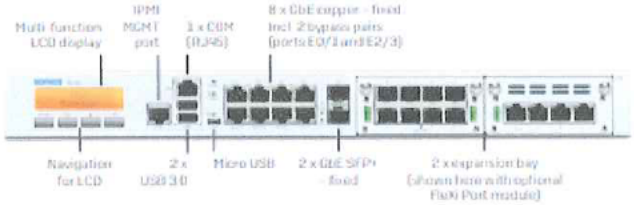
[redacted]

Active IT corp

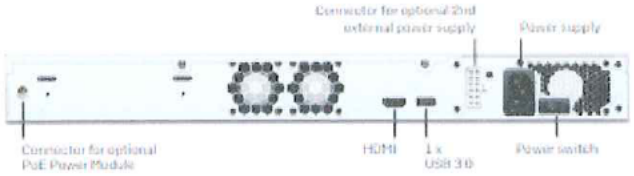
[redacted]

SOPHOS SG 450 PARA LOS DOS (2) FIREWALL DE **SITIO PRINCIPAL Y SITIO REMOTO (SANTA ANA)**

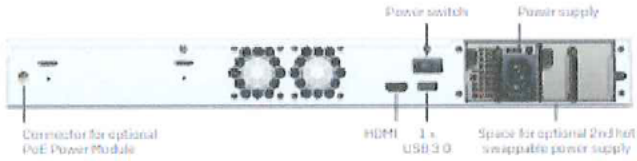
Front View



Back View SG 430



Back View SG 450



Environment

Power consumption	SG 430: 28W, 96 BTU/hr (idle) 79W, 270 BTU/hr (full load) SG 450: 31W, 107 BTU/hr (idle) 83W, 283 BTU/hr (full load)
Operating temperature	0-40°C (operating) -20 to +80°C (storage)
Humidity	10%-90%, non-condensing

Product Certifications

Certifications	CB, UL, CE, FCC Class A, ISED, VCCI, RCM, CCC, KC, BIS

Performance	SG 430 Rev. 2	SG 450 Rev. 2
Firewall throughput	28 Gbps	30 Gbps
VPN throughput	4 Gbps	5 Gbps
IPS throughput	7 Gbps	8 Gbps
Antivirus throughput (proxy)	2 Gbps	2.5 Gbps
Concurrent connections	8,000,000	8,000,000
New connections/sec	130,000	140,000
Maximum licensed users	unrestricted	unrestricted

Physical interfaces		
Storage (local quarantine/logs)	integrated SSD	integrated SSD x2
Ethernet interfaces (fixed)	8 GbE copper (incl. 2 bypass pairs) 2 10 GbE SFP+	
No. of FleXi Port slots	2	
FleXi Port modules (optional)	8 port GbE copper 8 port GbE SFP* 2 port 10 GbE SFP+* 4 port 10 GbE SFP+* 2 port 40 GbE QSFP+* 4 port GbE PoE 8 port GbE PoE	
I/O ports	2 x USB 3.0 (front) 1 x Micro USB (front) 1 x USB 3.0 (rear) 1 x COM (RJ45) (front) 1 x IPMI (front) 1 x HDMI (rear)	
Display	Multi-function LCD module	
Power supply	Internal auto-ranging 90-264VAC, 50-60 Hz Redundant PSU optional (external)	Internal auto-ranging 90-264VAC, 50-60 Hz Hot Swap Redundant PSU optional (internal)

Physical specifications		
Mounting	1U rackmount (sliding rails incl.)	
Dimensions Width x Depth x Height	438 x 483 x 44mm 17.24 x 19 x 1.75 inches	
Weight	7.6 kg / 16.76 lbs (unpacked) 12.7 kg / 28 lbs (packed)	7.8 kg / 17.2 lbs (unpacked) 13.8 kg / 30.42 lbs (packed)

* Transceivers (mini GBICs) sold separately

[redacted]

Active IT corp

[redacted]

Lista de funciones de Sophos UTM

Administración general

- Panel de control personalizable
- Administración delegada: auditor, solo lectura y administrador para todas las funciones
- Administración centralizada y gratuita de varios dispositivos de UTM a través de Sophos UTM Manager (SUM)
- Servicio de actualización configurable
- Definiciones reutilizables de objetos del sistema para redes, servicios, hosts, períodos temporales, usuarios y grupos, clientes y servidores
- Gestión rápida de reglas del sistema de prevención de intrusiones
- Portal de autoservicio para usuarios para configurar la VPN con un solo clic
- Seguimiento de cambios de configuraciones
- Opciones de restauración y copia de seguridad manuales o totalmente automatizadas
- Opciones de notificación de destinos SNMP o correo electrónico
- Compatible con SNMP
- Contraseña de un solo uso (OTP) y autenticación de doble factor (2FA) compatibles con el protocolo OATH para iniciar sesión en WebAdmin, el portal de usuarios, VPN SSL, VPN IPSec, el portal HTML5 y SSH*

Servicios y enrutamiento de red

- Enrutamiento: estático, multidifusión (PIM-SM) y dinámico (BGP, OSPF)
- Estático de NAT, camuflaje (dinámico)
- Enrutamiento de multidifusión independiente del protocolo con IGMP snooping
- Puentes compatibles con STP y reenvío de emisiones de ARP
- Equilibrio de enlaces de WAN: 32 conexiones a Internet, comprobación automática del estado de los enlaces, conmutación automática por error, equilibrio automático y ponderado, y reglas multi ruta granulares
- Alta disponibilidad activa y pasiva sin necesidad de configuraciones
- Clústeres activo-activo de hasta 10 dispositivos
- Agregación de enlaces de interfaces 802.3ad
- Calidad del servicio con control total de bloques del ancho de banda y límite de descargas mediante SFQ y RED del tráfico entrante
- Configuración total de DNS, DHCP y NTP
- Equilibrio de cargas de servidores
- Compatible con el protocolo IPv6
- Compatible con RED

Protección de redes

- Protección contra intrusiones: Motor de inspección detallada de paquetes, más de 18.000 patrones
- Patrones de IPS selectivos para una protección y un rendimiento máximos
- Algoritmo de vencimiento de patrones del IPS para un rendimiento óptimo*
- Protección contra avalanchas: Bloqueo de ataques de denegación de servicio y denegación de servicio distribuido, y exploración de puertos
- Bloqueo de países individuales o por zonas (más de 360 países) con opciones y excepciones separadas para el tráfico entrante y saliente
- VPN de sitio a sitio: SSL, IPSec, AES/3DES de 256 bits, PFS, RSA, certificados X.509, clave compartida previamente
- Acceso remoto: Compatible con clientes VPN de SSL, IPsec, iPhone/iPad/Cisco
- Gestión de VoIP para conexiones SIP y H.323
- Auxiliares de seguimiento de conexiones: FTP, IRC, PPTP, TFTP
- Configuración y reglas basadas en identidades con agente de autenticación para usuarios

Protección avanzada contra amenazas*

- Detecte y bloquee el tráfico de red que intenta ponerse en contacto con servidores de comando y control mediante cortafuegos y servidores proxy HTTP, ATC y DNS
- Identifique servidores infectados en la red y contenga sus actividades
- Espacios seguros selectivos de código sospechoso para determinar intenciones maliciosas

[redacted]

Active IT corp

[redacted]

Lista de funciones de Sophos UTM

Autenticación

- Autenticación de cliente o servidor proxy (NTLM/Kerberos) transparente
- Autenticación a través de: Active Directory, eDirectory, RADIUS, LDAP y TACACS+
- Inicio de sesión único: Active Directory, eDirectory
- Compatible con SSL
- Herramientas: comprobación de la configuración del servidor, prueba de nombres de usuario y contraseñas, y eliminación de la caché de autenticación
- Navegador gráfico para usuarios y grupos
- Creación automática de usuarios
- Capturas previas de sincronizaciones base programadas
- Imposición de contraseñas complejas

Protección web

- Base de datos de filtrado de direcciones web con más de 35 millones de sitios en 96 categorías y en más de 65 idiomas
- Restricción de aplicaciones: Listas precisas y patrones de Capa 7 para miles de aplicaciones
- Restricción dinámica de aplicaciones basada en la productividad o tarjetas de riesgo
- Visualización del tráfico en tiempo real, bloqueo o gestión
- Escaneado de programas maliciosos: Correo electrónico web, HTTP/S y FTP mediante dos motores antivirus independientes (Sophos y Avira) para bloquear todo tipo de virus, programas maliciosos web, troyanos y programas espía
- Filtrado HTTPS de direcciones web totalmente transparente*
- Protección web avanzada contra programas maliciosos con simulación de JavaScript*
- Búsquedas de Live Protection en tiempo real en la nube con la información más reciente sobre amenazas
- Bloqueo de descargas de aplicaciones no deseadas*
- Filtrado de direcciones web maliciosas por reputación con el respaldo de SophosLabs
- Umbral de reputación: establezca los umbrales de reputación que los sitios web deben alcanzar para estar disponibles desde la red interna
- Filtro activo del contenido: Extensiones de archivos, tipo MIME, JavaScript, ActiveX, Java y Flash
- Imposición de YouTube para centros educativos
- Imposición de SafeSearch
- Imposición de Google Apps*
- Único y transparente con SSO de AD*
- Portal cautivo transparente con autenticación
- Compatible con otros servidores proxy de filtrado en modos diferentes
- Políticas de acceso por tiempo, usuarios o grupos
- Anulación temporal del filtro de direcciones web con autenticación
- Agente de autenticación de clientes para seguimientos especiales por usuario
- Clonación de perfiles de seguridad
- Mensajes de usuario personalizables para eventos en diferentes idiomas
- Compatibilidad con CA de verificación especial de HTTPS
- Asistente de configuración y ayuda contextual online
- Páginas de bloqueo personalizables
- Categorización a medida para anular categorías o crear categorías personalizadas*
- Opciones de filtrado y autenticación por tipo de dispositivo para iOS, Android, Mac y Windows, entre otros*
- Herramienta de prueba de políticas para direcciones web, horas, usuarios y otros parámetros*

Protección del correo electrónico

- Servicio de reputación con vigilancia de brotes de correo no deseado basado en tecnología patentada de detección de patrones recurrentes
- Técnicas avanzadas de detección de correo no deseado: Listas de Blackhole en tiempo real (RBL), heurística, comprobación de SPF, BATV, escaneado de direcciones web, listas grises, comprobaciones de RDNS/HELO, filtro de expresiones y comprobación de destinatarios
- Bloqueo de correo no deseado y programas maliciosos durante la transacción SMTP
- Detecta direcciones web de suplantación de identidad en mensajes de correo electrónico
- Listas de direcciones y dominios permitidas y prohibidas por usuario y globales
- Comprobación de destinatarios en función a cuentas de Active Directory
- Escaneado de correo electrónico compatible con SMTP y POP3
- Motores antivirus dobles (Sophos y Avira)
- Escaneado de adjuntos comprimidos y archivados con soporte de nivel profundo
- Escaneado de formatos de correo incrustados

[redacted]

Active IT corp

[redacted]

Lista de funciones de Sophos UTM

Cifrado del correo electrónico y DLP

- Cifrado SPX (pendiente de patente) de mensajes de sentido único*
- Cifrado y descifrado transparente, y firmas digitales para mensajes de SMTP
- Totalmente transparente, sin necesidad de software ni clientes adicionales
- Compatible con los estándares S/MIME, OpenPGP y TLS
- Compatible con servidores de claves PGP
- Permite escanear el contenido y detectar virus incluso en mensajes cifrados
- Administración centralizada de todas las claves y certificados, sin necesidad de distribución
- Motor DLP con escaneado automático de mensajes de correo electrónico y adjuntos para detectar datos sensibles*
- Listas de control del contenido con tipos de datos sensibles predefinidos para PII, PCI, HIPAA, entre otros estándares, actualizadas por SophosLabs*

Administración del correo electrónico

- Informes de cuarentenas de usuarios enviados a diario por correo a la hora elegida
- Compatible con el servicio de administración de registros
- Portal de usuarios personalizable para gestión del correo en 15 idiomas
- Convierte en anónimos los datos de informes para el cumplimiento de políticas de privacidad
- Más de 50 informes integrados
- Exportación de informes a archivos PDF y CSV
- Pies de página y exenciones de responsabilidad personalizables para mensajes de correo electrónico
- Asistente de configuración y ayuda contextual en línea

Portal de usuarios

- Cuarentena de SMTP, visualización y liberación de mensajes en cuarentena
- Lista de remitentes permitidos y prohibidos
- Información de acceso a puntos inalámbricos
- Descarga del agente de autenticación de Sophos (SAA)
- Descarga de software cliente de acceso remoto y archivos de configuración
- Portal VPN HTML5 para abrir conexiones VPN sin cliente con servidores predefinidos, utilizando servicios predefinidos
- Descarga de certificados de CA de servidores proxy HTTPS

Opciones de VPN

- VPN de uso remoto basadas en clientes de Cisco y HTML5, PPTP, L2TP, SSL, IPsec, así como túneles de sitio a sitio de Amazon VPC, SSL e IPsec, y VPN lista para usar del dispositivo Ethernet remoto (RED) de Sophos

Cliente VPN IPsec

- Autenticación: Clave previamente compartida (PSK), PKI (X.509), tarjetas inteligentes, token y XAUTH
- Cifrado: AES (128/192/256), DES, 3DES (112/168), Blowfish, RSA (hasta 2048 bits), grupos DH 1/2/5/14, MD5 y SHA-256/384/512
- Túneles divididos inteligentes para conseguir un enrutamiento óptimo del tráfico
- Compatibilidad de recurso NAT
- Resumen gráfico del estado de las conexiones gracias al monitor de clientes
- Multilingüe: Alemán, inglés y francés
- Exclusivo de túneles IPsec

Cliente VPN SSL

- Seguridad probada basada en SSL (TLS)
- Requisitos mínimos del sistema
- Compatible con perfiles con diferentes niveles de acceso
- Compatible con MD5, SHA, DES, 3DES y AES
- Funciona a través de todos los cortafuegos, independientemente de los servidores proxy y NAT
- Compatible con iOS y Android

VPN sin cliente

- Portal VPN HTML5 sin cliente para acceder a aplicaciones de forma segura desde navegadores en cualquier dispositivo

VPN con un solo clic

- Instalación y configuración sencillas de cada cliente en pocos minutos
- Descarga de software cliente, archivos de configuración individuales, claves y certificados con un solo clic desde el portal de usuarios de la puerta de enlace de seguridad
- Instalación y configuración automáticas del cliente
- Sin necesidad de configuración por parte del usuario

[redacted]

Active IT corp

[redacted]

Lista de funciones de Sophos UTM

VPN de RED

- Administración centralizada de todos los dispositivos RED desde Sophos UTM
- Sin configuraciones: Se conecta de forma automática mediante un servicio de aprovisionamiento basado en la nube
- Túnel cifrado protegido mediante certificados digitales X.509 y AES256
- Las oficinas de RED están totalmente protegidas con las suscripciones de protección web, de redes y de correo del dispositivo UTM central.
- Ethernet virtual para transferencias fiables de todo el tráfico entre ubicaciones
- Administración de direcciones IP con configuración de servidores DNS y DHCP definida de forma central
- Desautorización remota de dispositivos RED tras el período elegido de inactividad
- Compresión del tráfico de túneles* (RED 50, RED 10 revisión 2.3)
- Opciones de configuración de puertos de VLAN* (RED 50)

Wifi segura

- Implementación sencilla y visualización automática en el dispositivo de UTM
- Vigilancia y administración centralizada de todos los puntos de acceso y clientes inalámbricos a través del controlador inalámbrico incorporado
- Seguridad integrada: Todo el tráfico de wifi atraviesa de forma automática el dispositivo de UTM
- 802.11 b/g/n inalámbrico a 2,4 GHz y 5 GHz (AP 50)
- Alimentación a través de Ethernet 802.3af (AP 30/50)
- Compatible con varios SSID: Hasta 8
- Cifrado potente compatible con tecnologías de autenticación inalámbrica punteras, incluidas WPA2-Enterprise y IEEE 802.1X (autenticación RADIUS)
- Acceso inalámbrico a Internet para invitados con páginas de inicio personalizables en el portal cautivo
- Acceso diario o semanal para invitados mediante vales
- Acceso por tiempo a la red inalámbrica
- Modo de red en malla de puentes y repetidores inalámbricos con AP 50
- Compatible con autenticación base de puntos de acceso* (RADIUS, TACACS, LDAP, AD)

Protección del cortafuegos de aplicaciones web

- Servidor proxy inverso
- Motor de refuerzo de direcciones web
- Motor de refuerzo de formularios
- Control de enlaces profundos
- Prevención de cruces de directorios
- Protección contra inyecciones de SQL
- Protección contra secuencias de comandos entre sitios
- Motor antivirus doble (Sophos y Avira)
- Descarga de cifrado de HTTPS (SSL)
- Firma digital de cookies
- Enrutamiento basado en rutas
- Compatible con el protocolo Outlook en cualquier lugar
- Autenticación inversa (descarga) básica y basada en formularios para acceder a servidores*

Administración del cortafuegos de aplicaciones web

- La detección automática de servidores escanea las redes adjuntas e identifica servidores web
- El equilibrio de carga integrado distribuye todos los visitantes entre los distintos servidores
- Perfiles de cortafuegos predefinidos para Microsoft Outlook Web Access (OWA)
- El cambio rápido de servidores facilita el mantenimiento
- Anulación granular de comprobaciones individuales según las necesidades
- Cumplimiento de solicitudes de redes de origen o direcciones web de destino especificadas
- Compatibilidad con operadores y lógica
- Contribuye a la compatibilidad con diferentes configuraciones e implementaciones no estándar

[redacted]

Active IT corp

[redacted]

Lista de funciones de Sophos UTM

UTM Endpoint Protection

- Protección de estaciones Windows con Sophos Antivirus y control de dispositivos
- Escaneados en acceso, en demanda y programados para detectar programas maliciosos, virus, programas espía y troyanos
- Detección de aplicaciones no deseadas
- Live Protection Antivirus realiza búsquedas en tiempo real en la información más reciente sobre amenazas en la nube
- HIPS con detección de comportamientos sospechosos
- Protección web con protección contra sitios maliciosos
- Escaneado de descargas
- Control de dispositivos para cientos de tipos de dispositivos populares, incluidos medios ópticos, modems, almacenamiento extraíble, Bluetooth, inalámbricos, infrarrojos, etc.
- Imposición de políticas web para grupos y usuarios en puestos de trabajo , y detección de programas maliciosos con sincronización total de informes y políticas

UTM Endpoint Management

- Administrado totalmente desde el dispositivo de UTM
- Despliegue sencillo con el programa de instalación desde el dispositivo de UTM
- Vigilancia de estaciones conectadas, amenazas y uso de dispositivos con acceso total al registro
- Alertas sobre estaciones infectadas*

Integración con estaciones de SEC*

- La integración con la gestión de estaciones de Sophos Enterprise Console proporciona informes y políticas web de UTM para la protección web en las estaciones

Registro e informes

- Registro: Registro remoto del sistema, rotación nocturna, servicio de administración de registros y archivos de email/ftp/SMB/SSH
- Creación de informes incorporada: Filtro de paquetes, protección contra intrusiones, ancho de banda y escalas diarias, semanales, mensuales y anuales
- Informes basados en identidades
- Exportación de informes a archivos PDF y CSV
- Programación y archivado de informes ejecutivos
- El motor reactivo compone los informes a medida que hace clic en los datos
- Inscriba destinatarios a cualquier informe, guárdelos o envíelos al instante
- Exportación de informes a archivos PDF y CSV
- Rotación y compresión nocturna de registros
- Archivación de registros: Incorporada, FTP, SMB, SSH, correo electrónico y registro del sistema
- Cientos de informes incorporados
- Informes de actividades diarias
- Informe de anulación del filtro de direcciones web
- Seguimiento y auditorías por usuario
- Anonimización de datos de informes para el cumplimiento de políticas de privacidad
- Registro completo de transacciones de todas las actividades en formato legible
- Parámetros de búsqueda en registros web por usuario, dirección web o acción*

[redacted]

Active IT corp

[redacted]

OFERTA ECONÒMICA

CANT	DESCRIPCION	PRECIO UNITARIO C/IVA US$	TOTAL C/IVA US$
2	EQUIPO **MARCA SOPHOS MODELO SG450** APPLIANCE QUE INCLUYE: • 16 GB RAM • 2 X 240 GB SSD DE ALMACENAMIENTO • 2 X FUENTE DE PODER REDUNDANTE • 8 INTERFACES DE COBRE GBE • 2 INTERFACES 2 10 GBE FSP • CAPACIDAD DE AMPLIACION DE PUERTOS CON FLEXI PORTS • GARANTÌA: 1 AÑO	$ 7,107.05	$ 14,214.10
2	LICENCIAMIENTO **SOPHOS SG450** FULLGUARD QUE INCLUYE TODAS LAS FUNCIONES DE LA LISTA DE FUNCIONES SOPHOS UTM QUE SE ENCUENTRA EN LA OFERTA TÉCNICA	$8,686.39	$17,372.78
12	EQUIPO **MARCA SOPHOS MODELO SG135** APPLIANCE QUE INCLUYE • 6 GB RAM • 1 X 64 GB SSD DE ALMACENAMIENTO • 8 INTERFACES DE COBRE GBE • CAPACIDAD DE AMPLIACION DE PUERTOS CON FLEXI PORTS • GARANTÌA: 1 AÑO	$ 825.66	$9,907.92
12	LICENCIAMIENTO **SOPHOS SG135** FULLGUARD QUE INCLUYE TODAS LAS FUNCIONES DE LA LISTA DE FUNCIONES SOPHOS UTM QUE SE ENCUENTRA EN LA OFERTA TÉCNICA	$1,009.15	$ 12,109.80
5	EQUIPO **MARCA SOPHOS MODELO SG115** APPLIANCE QUE INCLUYE: • 4 GB RAM • 1 X 64 GB SSD DE ALMACENAMIENTO • 4 INTERFACES DE COBRE GBE • CAPACIDAD DE AMPLIACION DE 1 PUERTO CON TRANSCEIVERS • GARANTIA: 1 AÑO	$ 470.11	$ 2,350.55
5	LICENCIAMIENTO **SOPHOS SG115** FULLGUARD QUE INCLUYE TODAS LAS FUNCIONES DE LA LISTA DE FUNCIONES SOPHOS UTM QUE SE ENCUENTRA EN LA OFERTA TÉCNICA	$574.59	$2,872.95
		TOTAL	**$58,828.10**

[redacted]

Active IT corp

[redacted]

PERÍODO DE VIGENCIA (VALIDEZ DE LA OFERTA):

- 30 Días Calendario

INCLUYE:

- Servicio de Soporte técnico 24x7 durante un año
- Capacitación a Técnicos sobre uso y administración del producto
- Instalación y Configuración de Consola de Administración

NOTAS DE LA COTIZACION:

- Los precios incluyen implementación y configuración de nuevas versiones del Equipo
- Los precios están expresados en Dólares de Estado Unidos de Norteamérica.
- Precios Incluyen IVA.
- Garantía de la licencias y equipos: 1 año.

FORMA DE PAGO:

- Crédito a 30 días calendario.

FUENTE DE FINANCIAMIENTO

- GOES

TIEMPO DE ENTREGA DE EQUIPOS Y LICENCIAS

- 15 dias calendario

LUGAR DE ENTREGA:

- Una sola entrega, oficina de Ministerio de Trabajo y Previsión Social Ubicada en final 17 Avenida Nte. y Alameda Juan Pablo II, Centro de Gobierno, Edificio del Ministerio de Trabajo No.3 Primer nivel.

[redacted]

Active IT corp

[redacted]

NUESTRO SERVICIO OFERTADO INCLUYE COMO VALOR AGREGADO (SIN COSTO ALGUNO):

- Capacitación en la configuración y administración del "**FIREWALL SOPHOS**" de 12 horas para 4 Técnicos de MINISTERIO DE TRABAJO Y PREVISION SOCIAL – MTPS.
- Soporte Técnico 24x7x365 durante el periodo contratado de los productos SOPHOS brindado por Consultores Certificados por el Fabricante. Los incidentes se atenderán o reportarán vía telefónica o por correo electrónico o visita presencial dependiendo del caso, dando respuesta por fallas en equipos en un máximo de 3 horas posterior al reporte.
- Actualización de las nuevas versiones liberadas por el Fabricante SOPHOS
- Equipos disponibles para el inmediato reemplazo en concepto de garantía as veces que sea necesario con un máximo de cuatro horas para el área de Occidente y seis horas para el área de Oriente por equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional, garantizando el respaldo de la información en instruyendo al personal de Informática **de MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL -MTPS** para luego ser instalado en el nuevo equipo.

- **SE ENTREGARÀN OCHO (8) AP15C PARA EL FORTALECIMIENTO DE LA RED WIRELESS INSTITUCIONAL.**

AP 15C	
	1 x 10/100/1000 Base TX
	802.11 b/g/n 2.4 GHz and 5 GHz
✔(from v9.4)	-
✔	802.3af
SOHO Ceiling mount	2 internal
300 Mbps	1
8	2x2:2

- **SE ENTREGARÁ SERVICIO DE SOPORTE TÉCNICO PARA EL SERVIDOR DE CORREO ELECTRÓNICO INSTITUCIONAL ZIMBRA VALORADO EN PRECIO DE MERCADO DE $10,000.00. ESTE SERVICIO DE ENTREGARÁ POR EL PERÍODO DE 1 AÑO Y SIN COSTO ALGUNO.**

[redacted]

Active IT corp



MECANISMOS Y CONDICIONES A SEGUIR PARA HACER EFECTIVO EL REEMPLAZO EN GARANTÍA DEL EQUIPO:

1. MTPS reporta falla técnica del equipo
    a. Medios de notificación:
        i. Teléfono
        ii. Correo electrónico
2. Se coordina visita con el MTPS para revisión de equipo y falla técnica
    a. Escenarios de falla técnica
        i. Si es problema de software se somete ticket a helpdesk del fabricante
            1. Si el problema afecta la operatividad del cliente, se procede a paso 3.
        ii. Si es problema de hardware se procede al paso 3
3. Se hace entrega inmediata de un equipo de la misma capacidad al MTPS para solventar problemas temporalmente
4. Se abre una solicitud de reclamo de garantía al fabricante para el envío de nuevo equipo en reemplazo del dañado (8 días hábiles)
5. Se revisa el nuevo equipo exhaustivamente para garantizar que no tenga ningún desperfecto.
6. Se coordina con MTPS la entrega del equipo nuevo de reemplazo y la implementación.
7. Cliente hace entrega de equipo dañado salvo que sea institución de gobierno y se entregue carta explicativa de activo fijo que limite su entrega.



Active IT corp

[redacted]

CARTA DE COMPROMISO SOBRE COBERTURA DE EQUIPOS ACTUALES DURANTE IMPLEMENTACIÓN

San Salvador, 22 de junio de 2018

Señores
Ministerio de Trabajo y Previsión Social- MTPS
Unidad de Adquisiciones y Contrataciones Institucional- UACI
Presente.

Atención: Licda. Mayra Palma
Jefa UACI Ad Honorem

Estimados Señores:

De ser adjudicados, nos comprometemos a dar cobertura de la seguridad perimetral en todos los equipos actuales durante el tiempo que tarde la implementación de los nuevos equipos con el fin de evitar cualquier inconveniente con alguna interrupción en los servicios de la institución.

Atentamente,

[redacted]

Representante Legal
Active IT Corp

[redacted]

[redacted]

[redacted]

CARTA DE COMPROMISO SOBRE GARANTÍA FIEL CUMPLIMIENTO

San Salvador, 22 de junio de 2018

Señores
Ministerio de Trabajo y Previsión Social- MTPS
Unidad de Adquisiciones y Contrataciones Institucional- UACI
Presente.

Atención: Licda. Mayra Palma
Jefa UACI Ad Honorem

Nos comprometemos a presentar la garantía de fiel cumplimiento de contrato por el valor de 10% del monto adjudicado, la cual será presentada cinco días hábiles siguientes posterior a la entrega y firma del contrato y estará vigente por un periodo de 15 días calendario.

Atentamente,

[redacted]

[redacted]

[redacted]

Active IT corp

[redacted]

CARTA DE COMPROMISO SOBRE GARANTÍA BUEN FUNCIONAMIENTO

San Salvador, 22 de junio de 2018

Señores
Ministerio de Trabajo y Previsión Social- MTPS
Unidad de Adquisiciones y Contrataciones Institucional- UACI
Presente.

Atención: Licda. Mayra Palma
Jefa UACI Ad Honorem

Nos comprometemos a presentar la garantía buen funcionamiento y calidad de los bienes por un valor de 10% del monto adjudicado, y la cual será presentada cinco días hábiles siguientes a la recepción definitiva de los bienes.

Atentamente,

[redacted]

[redacted]

[redacted]

Active IT corp

[redacted]

CARTA SOBRE PLAN DE PAGOS DE HACIENDA

San Salvador, 22 de junio de 2018

Señores
Ministerio de Trabajo y Previsión Social- MTPS
Unidad de Adquisiciones y Contrataciones Institucional- UACI
Presente.

Atención: Licda. Mayra Palma
Jefa UACI Ad Honorem

Estimados Señores:

Por este medio hacemos de su conocimiento que nuestra empresa Active IT Corp. S.A de C.V cuenta con un plan de pago autorizado por el Ministerio de Hacienda para extender solvencias. De ser adjudicado tardaremos en un periodo de 5 días hábiles para entregarla.

Atentamente,

[redacted]

[redacted]

[redacted]

[redacted]

DATOS GENERALES ACTIVE IT CORP

RAZÓN SOCIAL:	**Active It Corp, SA de CV**
NIT:	[redacted]
NRC:	[redacted]
DOMICILIO:	
PÁGINA WEB:	
CORREO ELECTRÓNICO:	
TELÉFONO:	
FAX:	
REPRESENTANTE LEGAL:	
NIT DEL REPRESENTANTE LEGAL:	[redacted]
DUI DEL REPRESENTANTE LEGAL:	
PERSONA CONTACTO:	
DIRECCIÓN DE LA PERSONA CONTACTO:	
TELÉFONO DE LA PERSONA CONTACTO:	
DATOS DE QUIEN FIRMA CONTRATO U ORDEN DE COMPRA EN CASO DE SER ADJUDICADO	
CLASIFICACION DE LA EMPRESA	[redacted]
EMITIR ORDEN DE COMPRA / QUEDAN / CHEQUE A NOMBRE DE:	

[redacted]

Active IT corp



DECLARACIÓN JURADA



En la ciudad de San Salvador, departamento de San Salvador, a las once horas del día veintiuno de Junio del año dos mil dieciocho. **ANTE MI,** [redacted] otario, del domicilio de [redacted], comparece el señor [redacted] años de edad, [redacted] del domicilio de [redacted] con Documento Unico de Identidad Número [redacted] con número de identificación tributaria [redacted], actuando en su calidad de Representante Legal de la sociedad **ACTIVE IT CORP, SOCIEDAD ANONIMA DE CAPITAL VARIABLE,** de cuya personería DOY FE de ser legítima y suficiente por haber tenido a la vista: Escritura de constitución de dicha sociedad, otorgada en San Salvador, a las diez horas del día veintiuno de junio del año dos mil trece, ante los oficios de la notario [redacted], e inscrita en el Registro de Comercio al [redacted] del Registro de Sociedades, el día veintiséis de junio del año dos mil trece, de la que consta que el nombre es como se ha dicho; de nacionalidad salvadoreña, del domicilio de San Salvador, para un plazo indeterminado; que su finalidad entre otras está la prestación de servicios de consultoría empresarial y capacitación en informática; que la administración y representación legal, y el uso de la firma social estará confiada a un Administrador Unico Propietario y Suplente; y haber tenido a la vista también Certificación extendida por el Secretario de la Junta General Ordinaria de Accionistas de dicha sociedad, el día dieciocho de abril del año dos mil dieciséis, e inscrita en el Registro de Sociedades del Registro de Comercio al [redacted] el día veinticuatro de Mayo del año dos mil dieciséis, de la que consta que se eligió como Administrador Unico Propietario al señor [redacted] para un período comprendido del dieciocho de abril del año dos mil dieciséis, al dieciocho de abril del año dos mil veintidós, y en la calidad en que actúa **ME DICE** : Que con el objeto de participar en Proceso por Libre Gestión número **DOCE/DOS MIL DIECIOCHO**, relativa a **"ADQUISICION DE DIECINUEVE EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS", BAJO JURAMENTO DECLARA: I)** Que toda la cadena de producción de Equipos Firewall ofertados a la Institución por la empresa que representa, no se utiliza trabajo realizado por niños y niñas y adolescente por debajo de la edad mínima de admisión al empleo y se cumple en todo el proceso productivo, con la normativa

[redacted]

laboral vigente y con las regulaciones relativas a la protección integral de la niñez y la adolescencia, que tienen por objeto garantizar el goce y respeto pleno de los derechos los niños, niñas y adolescentes. **II)** Que se cumple con la normativa nacional relacionada con la protección de la persona adolescente trabajadora, especialmente aquella relativa a la realización de actividades y trabajos peligrosos. **III)** Que se compromete a vigilar para que la empresa que representa, así como sus proveedores, contratistas y subcontratistas, en toda la cadena de producción estén libres de trabajo infantil y se respete el marco legal de protección de la persona adolescente trabajadora. La suscrita Notario hace constar que hice del conocimiento al compareciente lo regulado en el Código Penal, en cuanto al delito de falsedad ideológica, regulado en el Artículo doscientos ochenta y cuatro. El compareciente me manifiesta que para los efectos legales de la presente acta notarial y para los que sugieren en el proceso de licitación, señala como domicilio especial el de esta ciudad a cuyos tribunales se somete expresamente. Así se expresó el compareciente quien expliqué los efectos legales de esta acta notarial que consta de un folio útil y leído que le fue por mí íntegramente en un solo acto sin interrupción, ratifica su contenido y firmamos. **DOY FE.-**

[redacted]

[redacted]

Active IT corp

[redacted]

CARTAS DE REFERENCIA

[redacted]

Active IT corp

[redacted]

EL SALVADOR
UNÁMONOS PARA CRECER

Active IT Corp S.A de C.V

I. DATOS GENERALES DE LA INSTITUCIÓN

1. Nombre de la institución: Ministerio de Obras Públicas, Transporte, Vivienda y Desarrollo Urbano
2. Dirección: [redacted]
   Número Telefónico: 2528-3000
   Fax:
   Correo Electrónico: paul.ramos@mop.gob.sv

3. A continuación, proporcionar los siguientes datos:

II. IDENTIFICACIÓN DEL CONTRATO

NOMBRE DEL CONTRATO/ ORDEN DE COMPRA: No. 000015	
FECHA INICIO	6 Febrero 2018
FECHA FINALIZACIÓN	6 Febrero 2019
MONTO DEL CONTRATO EN US$	$20,954.44

III. CALIDAD DEL SERVICIO

INDICAR LA CALIDAD DEL SERVICIO RECIBIDO: MARCAR CON UNA "X" UNA SOLA VALORACIÓN:	Regular	( )
	Bueno	( )
	Muy Bueno	( )
	Excelente	(x)

NOTA: Hacemos constar que la empresa Grupo Active Systems- Active IT Corp S.A de C.V., ha sido nuestro proveedor de servicios de seguridad firewall SOPHOS UTM por más de 3 años.
Y para ser presentada a la Unidad de Adquisiciones y Contrataciones Institucional (UACI), del Ministerio de Trabajo y Previsión Social, se extiende la presente constancia, en la ciudad de San Salvador, a los diecinueve días del mes de junio de dos mil dieciocho

[redacted]

[redacted]

[redacted]

Active IT corp

[redacted]

Active IT Corp S.A de C.V

I. DATOS GENERALES DE LA INSTITUCIÓN

1. Nombre de la Institución: Consejo Nacional de la Judicatura
2. Dirección: [redacted]
   Número Telefónico [redacted]
   Correo Electrónico: [redacted]
3. A continuación, proporcionar los siguientes datos:

II. IDENTIFICACIÓN DEL CONTRATO

NOMBRE DEL CONTRATO/ ORDEN DE COMPRA: No. 384/2017	
FECHA INICIO	13 Septiembre 2017
FECHA FINALIZACIÓN	13 Septiembre 2018
MONTO DEL CONTRATO EN US$	$13,000.00

III. CALIDAD DEL SERVICIO

INDICAR LA CALIDAD DEL SERVICIO RECIBIDO: MARCAR CON UNA "X" UNA SOLA VALORACIÓN:	Regular	( )
	Bueno	( )
	Muy Bueno	( )
	Excelente	(X)

NOTA: Hacemos constar que la empresa Grupo Active Systems- Active IT Corp S.A de C.V., ha sido nuestro proveedor de servicios de seguridad firewall SOPHOS UTM por más de 3 años.

Y para ser presentada a la Unidad de Adquisiciones y Contrataciones Institucional (UACI), del Ministerio de Trabajo y Previsión Social, se extiende la presente constancia, en la ciudad de San Salvador, a los 20 días del mes de junio de 2018

[redacted]

[redacted]

[redacted]

Active IT Corp S.A de C.V

I. DATOS GENERALES DE LA INSTITUCIÓN

1. Nombre de la institución: Comisión Ejecutiva Hidroeléctrica del Río Lempa
2. Dirección [redacted]
   San Salvador, El Salvador
   Número Telefónico: [redacted]
   Fax:
   Correo Electrónico: [redacted]
3. A continuación, proporcionar los siguientes datos:

II. IDENTIFICACIÓN DEL CONTRATO

NOMBRE DEL CONTRATO/ORDEN DE COMPRA: No. 23- 1 Año: 2017	
FECHA INICIO	7 Noviembre 2017
FECHA FINALIZACIÓN	7 Noviembre 2018
MONTO DEL CONTRATO EN US$	$10,603.92

III. CALIDAD DEL SERVICIO

INDICAR LA CALIDAD DEL SERVICIO RECIBIDO: MARCAR CON UNA "X" UNA SOLA VALORACIÓN:	Regular	( )
	Bueno	( )
	Muy Bueno	( )
	Excelente	(X)

NOTA: Hacemos constar que la empresa Grupo Active Systems- Active IT Corp S.A de C.V., ha sido nuestro proveedor de servicios de seguridad firewall por más de 3 años.

Y para ser presentada a la Unidad de Adquisiciones y Contrataciones Institucional (UACI), del Ministerio de Trabajo y Previsión Social, se extiende la presente constancia, en la ciudad de San Salvador, a los 19 día de Junio 2018

[redacted]

[redacted]

Active IT corp

[redacted]

CARTA DE AUTORIZACIÓN DEL FABRICANTE

[redacted]

Active IT corp

[redacted]

SOPHOS
Security made simple.

[redacted]

A quien concierna:
San Salvador
El Salvador

CERTIFICADO DE AUTORIZACIÓN DEL FABRICANTE

Estimados Señores:

El grupo de empresas de Sophos es líder mundial en seguridad informática y protección de datos para empresas. Sophos ofrece completa protección y control a entidades / organizaciones privadas, de educación y gobiernos y provee protección integral de datos y soluciones de seguridad integradas de red.

Sophos, Inc., cuya casa matriz está en 3 Van de Graaff Drive, Burlington MA, 01803, EEUU, confirma que:

Active IT Corp, S.A., en San Salvador, El Salvador, es un **Canal Sophos, Nivel Platino** autorizado para suministrar productos, servicios e instalaciones de Sophos en el territorio de Republica de El Salvador.

Sin otro particular y quedando a la espera de poder servirles.

Atentamente,

[redacted]

Sophos Inc., 3 Van de Graaff Drive, 2nd Floor, Burlington, MA, 01803, USA
Tel 781-494-5800 Fax 781-494-5801 Email latamteam@sophos.com www.sophos.com

[redacted]

Active IT corp

[redacted]

CERTIFICACIONES DE NUESTRO PERSONAL TECNICO

[redacted]

Active IT corp

(503) 2510-7100
info@activesystems.com.sv
Residencial Villas de Santa Elena,
Calle Alegría, Casa 13-A.
Antiguo Cuscatlán.

SOPHOS
Security made simple.

Certificate of Completion

Manuel Claros
has successfully completed the course
UTM v9.5 - Certified Engineer

held on Sep 01, 2017

[redacted]

[redacted]

94

Active IT corp

(503) 2510-7100
info@activesystems.com.sv
Residencial Villas de Santa Elena,
Calle Alegría, Casa 13-A.
Antiguo Cuscatlán.

SOPHOS
Security made simple.

Certificate of Completion

Carlos Echeverria
has successfully completed the course

UTM v9.5 - Certified Engineer

held on Sep 05, 2017

[redacted]

Active IT corp

(503) 2510-7100
info@activesystems.com.sv
Residencial Villas de Santa Elena,
Calle Alegría, Casa 13-A.
Antiguo Cuscatlán.

SOPHOS
Security made simple.

Certificate of Completion

Milton Palacios
has successfully completed the course

UTM v9.5 - Certified Engineer

held on Sep 04, 2017

[redacted]

Active IT corp

[redacted]

[redacted]





[redacted]

Active IT corp

[redacted]

[redacted]





[redacted]

Active IT corp

[redacted]

[redacted]





[redacted]

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
UNIDAD DE ADQUISICIONES Y CONTRATACIONES INSTITUCIONAL
LIBRE GESTIÓN MTPS 12- 2018
"ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"
DÍA: 22 DE JUNIO DE 2018 HORA: DE 8:30 A.M A 12:30 P.M.

FECHA	HORA	NOMBRE DE LA EMPRESA	DIRECCIÓN DE LA EMPRESA	NOMBRE DE QUIÉN PRESENTA LA OFERTA	TELÉFONO Y CORREO ELECTRÓNICO	FIRMA Y SELLO
22 JUNIO 2018	9:55 Am	Active it corp	[redacted]	[redacted]	[redacted]	[redacted]
22 Junio 2018	11:20 Am	JL - Security Technologies				
22/06/18	11:30 am	JMTelcom SA de CV				
2206 18	11:45 am	DADA DADA Y CIA, S.A. de C.V.				

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
UNIDAD DE ADQUISICIONES Y CONTRATACIONES INSTITUCIONAL
LIBRE GESTIÓN MTPS 12- 2018
"ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"
DÍA: 22 DE JUNIO DE 2018 HORA: DE 8:30 A.M A 12:30 P.M.

FECHA	HORA	NOMBRE DE LA EMPRESA	DIRECCIÓN DE LA EMPRESA	NOMBRE DE QUIÉN PRESENTA LA OFERTA	TELÉFONO Y CORREO ELECTRÓNICO	FIRMA Y SELLO
22/06/18	12:30 MD	Devel Security S.A de C.V	[redacted]	[redacted]	[redacted]	[redacted]

69

MINISTERIO DE TRABAJO
Y PREVISIÓN SOCIAL

GOBIERNO DE
EL SALVADOR
UNÁMONOS PARA CRECER

Unidad de Adquisiciones y Contrataciones Institucional

MEMORANDUM

PARA: **LICDA. SANDRA EDIBEL GUEVARA PÉREZ**
Ministra de Trabajo y Previsión Social

DE: **LICDA. MAYRA YESSENIA PALMA GUTIERREZ**
Jefa UACI Ad Honorem.

ASUNTO: Solicitud de firma de acuerdos.

FECHA: 20 de junio de 2018.

Respetable Señora Ministra:

Referente a proceso de Libre Gestión MTPS 12-2018 **"Adquisición de 19 equipos de seguridad perimetral con licencias"**; muy atentamente estoy solicitando, de no haber objeción alguna, su autorización y firma a acuerdos Nos. 50 y 49 de conformación de Comisión de Evaluación de Ofertas y Administrador de Contrato respectivamente.

No omito manifestarle que este documento cuenta con el Visto Bueno de la Unidad Jurídica.

Atentamente,

1:30 pm

MINISTERIO DE TRABAJO Y PREVISION SOCIAL
20 JUN. 2018
DESPACHO MINISTERIAL

ASUNTO: Nombramiento de Comisión de Evaluación de Ofertas.

ACUERDO No. 50.-

SANDRA EDIBEL GUEVARA PÉREZ
Ministra de Trabajo y Previsión Social

En uso de sus facultades legales y de conformidad con lo dispuesto en el Artículo 20 incisos segundo y tercero de la Ley de Adquisiciones y Contrataciones de la Administración Pública, **ACUERDA:**

Nombrar, como miembros de la Comisión de Evaluación de Ofertas a partir de esta fecha, para el proceso de Libre Gestión MTPS 12-2018 **"ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"**, a las personas siguientes:

- Licenciada Yolanda del Carmen Dueñas Figueroa, Directora Administrativa;
- Licenciada Mayra Yessenia Palma Gutiérrez, Jefa de la Unidad de Adquisiciones y Contrataciones Institucional Ad-honorem;
- Licenciado Luis Mario Flores Guillén, Jefe de la Unidad Financiera Institucional;
- Ingeniero Juan Francisco Sánchez Cabrera, Jefe de la Unidad de Desarrollo Tecnológico; y,
- Licenciada Sandra Lissette Fuentes Quijano, Colaboradora Jurídica de la Unidad Jurídica.

COMUNIQUESE.

Unidad de Adquisiciones y Contrataciones Institucional, Ministerio de Trabajo y Previsión Social: San Salvador, a los veinte días del mes de junio de dos mil dieciocho.

MINISTRA DE TRABAJO Y PREVISIÓN SOCIAL

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
GOBIERNO DE EL SALVADOR

Fecha : 20-06-18 *Procedencia:* ***UACI***
adem

Extracto: **Se recibe:** para firma, acuerdos de conformación de Comisión de Evaluación de Ofertas y de Administrador de Contrato del proceso "Adquisición de 19 equipos de seguridad perimetral con licencias"

De: Lic. Mayra Palma.

SRA. MINISTRA:

V/B
22/06/2018

dad perimetral con licencias"

Original a Leda Palma.

MINISTERIO DE TRABAJO Y PREVISION SOCIAL
25 JUN. 2018
RECIBIDO
8:53am
Rosa María Hernández

65

MINISTERIO DE TRABAJO
Y PREVISIÓN SOCIAL

GOBIERNO DE
EL SALVADOR
UNÁMONOS PARA CRECER

Unidad de Adquisiciones y Contrataciones Institucional

MEMORANDUM

PARA: **LICDA. SANDRA EDIBEL GUEVARA PÉREZ**
Ministra de Trabajo y Previsión Social

DE: **LICDA. MAYRA YESSENIA PALMA GUTIERREZ**
Jefa UACI Ad Honorem.

ASUNTO: Solicitud de firma de acuerdos.

FECHA: 20 de junio de 2018.

Respetable Señora Ministra:

Referente a proceso de Libre Gestión MTPS 12-2018 **"Adquisición de 19 equipos de seguridad perimetral con licencias"**; muy atentamente estoy solicitando, de no haber objeción alguna, su autorización y firma a acuerdos Nos. 50 y 49 de conformación de Comisión de Evaluación de Ofertas y Administrador de Contrato respectivamente.

No omito manifestarle que este documento cuenta con el Visto Bueno de la Unidad Jurídica.

Atentamente,

1:30 pm
MINISTERIO DE TRABAJO Y PREVISION SOCIAL
20 JUN. 2018
DESPACHO MINISTERIAL

MINISTERIO DE TRABAJO
Y PREVISIÓN SOCIAL
GOBIERNO DE
EL SALVADOR
UNÁMONOS PARA CRECER

Unidad Jurídica

MEMORÁNDUM

PARA : **Licda. Mayra Yessenia Palma Gutiérrez.**
Jefa UACI Ad-Honorem.

DE : **Licdo. Walter de Jesús Zúniga Reyes.**
Jefe de la Unidad Jurídica.

ASUNTO : Remisión de Acuerdos del Proceso de LG MTPS 12-2018.

FECHA : San Salvador, 20 de junio de 2018.

Respetable Licenciada:

En virtud de haber recibido Memorándum el día 18 de los corrientes, mediante el cual solicita elaboración de Acuerdo para nombrar Administrador de Contrato al Ingeniero Juan Francisco Sánchez Cabrera y Acuerdo de Comisión de Evaluación de Ofertas, del Proceso de Libre Gestión MTPS 12-2018 "ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS", remito los Acuerdos N° 49 y N° 50.

Atentamente.-

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
20 JUN. 2018 2:14 pm
RECIBIDO U.A.C.I.

ASUNTO: Nombramiento de Administrador de Contrato.

ACUERDO No. 49.-

SANDRA EDIBEL GUEVARA PÉREZ,
Ministra de Trabajo y Previsión Social,

En uso de sus facultades legales y de conformidad con lo dispuesto en el Artículo 82 Bis de la Ley de Adquisiciones y Contrataciones de la Administración Pública, y Artículo 74 del Reglamento de la Ley de Adquisiciones y Contrataciones de la Administración Pública **ACUERDA:**

I. Nombrar al Ingeniero **Juan Francisco Sánchez Cabrera,** quien se desempeña como Jefe de la Unidad de Desarrollo Tecnológico del Ministerio de Trabajo y Previsión Social; como Administrador de Contrato, referente al proceso de contratación de Libre Gestión número MTPS 12-2018 denominado: **"ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"**, lo que deberá consignarse en el contrato respectivo, en cumplimiento a lo establecido en la letra "h" del artículo 23 del Reglamento de la Ley de Adquisiciones y Contrataciones de la Administración Pública.

II. El Administrador de Contrato nombrado en el presente acuerdo, deberá de observar y cumplir con las obligaciones legales establecidas en: la Ley de Adquisiciones y Contrataciones de la Administración Pública, el Reglamento de la Ley de Adquisiciones y Contrataciones de la Administración Pública, y el Manual de Procedimientos para el Ciclo de Gestión de Adquisiciones y Contrataciones de las Instituciones de la Administración Pública, y demás deberes que la ley, normas y contrato instruyan. Todo esto a efecto de dar fiel cumplimiento a los términos legales de la ejecución de los contratos.

COMUNIQUESE.

Unidad de Adquisiciones y Contrataciones Institucional, Ministerio de Trabajo y Previsión Social: San Salvador, a los veinte días del mes de junio de dos mil dieciocho.

MINISTRA DE TRABAJO Y PREVISIÓN SOCIAL

MINISTERIO DE TRABAJO
Y PREVISIÓN SOCIAL
GOBIERNO DE
EL SALVADOR
UNÁMONOS PARA CRECER

Unidad de Adquisiciones y Contrataciones Institucional

MEMORANDUM

PARA: **Lic. Walter de Jesús Zúniga Reyes**
Jefe de la Unidad Jurídica

DE: **Licda. Mayra Yessenia Palma Gutiérrez.**
Jefa UACI Ad Honorem.

ASUNTO: **Elaboración de Acuerdo de CEO y Administrador de Orden de Compra.**

FECHA: 18 de junio de 2018.

Estimado Licenciado:

Referente al proceso de **Libre Gestión MTPS 12-2018 "ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS";** muy atentamente estoy solicitando la elaboración de acuerdo para nombrar como miembros de la Comisión de Evaluación de Ofertas a las siguientes personas:

- **Licda. Yolanda del Carmen Dueñas Figueroa**, Directora Administrativa;
- **Licda. Mayra Yessenia Palma Gutiérrez,** Jefa Unidad de Adquisiciones y Contrataciones Institucional Ad Honorem;
- **Lic. Luis Mario Flores Guillén**, Jefe Unidad Financiera Institucional;
- **Ing. Juan Francisco Sánchez**; Jefe de la Unidad de Desarrollo Tecnológico;
- **Y la persona que sea designa de la Unidad Jurídica para integrar esta comisión.**

De igual forma se solicita la elaboración de acuerdo para nombrar como Administrador de Contrato al **INGENIERO JUAN FRANCISCO SANCHEZ;** Jefe de la Unidad de Desarrollo Tecnológico.

Atentamente,

MINISTERIO DE TRABAJO Y PREVISION SOCIAL
18 JUN. 2018
2:42 pm
RECIBIDO
UNIDAD DE ASESORÍA JURIDICA

ASUNTO: Nombramiento de Administrador de Contrato.

ACUERDO No. 49.-

SANDRA EDIBEL GUEVARA PÉREZ,
Ministra de Trabajo y Previsión Social,

En uso de sus facultades legales y de conformidad con lo dispuesto en el Artículo 82 Bis de la Ley de Adquisiciones y Contrataciones de la Administración Pública, y Artículo 74 del Reglamento de la Ley de Adquisiciones y Contrataciones de la Administración Pública **ACUERDA:**

I. Nombrar al Ingeniero **Juan Francisco Sánchez Cabrera,** quien se desempeña como Jefe de la Unidad de Desarrollo Tecnológico del Ministerio de Trabajo y Previsión Social; como Administrador de Contrato, referente al proceso de contratación de Libre Gestión número MTPS 12-2018 denominado: **"ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"**, lo que deberá consignarse en el contrato respectivo, en cumplimiento a lo establecido en la letra "h" del artículo 23 del Reglamento de la Ley de Adquisiciones y Contrataciones de la Administración Pública.

II. El Administrador de Contrato nombrado en el presente acuerdo, deberá de observar y cumplir con las obligaciones legales establecidas en: la Ley de Adquisiciones y Contrataciones de la Administración Pública, el Reglamento de la Ley de Adquisiciones y Contrataciones de la Administración Pública, y el Manual de Procedimientos para el Ciclo de Gestión de Adquisiciones y Contrataciones de las Instituciones de la Administración Pública, y demás deberes que la ley, normas y contrato instruyan. Todo esto a efecto de dar fiel cumplimiento a los términos legales de la ejecución de los contratos.

COMUNIQUESE.

Unidad de Adquisiciones y Contrataciones Institucional, Ministerio de Trabajo y Previsión Social: San Salvador, a los veinte días del mes de junio de dos mil dieciocho.

MINISTRA DE TRABAJO Y PREVISIÓN SOCIAL

MINISTERIO DE TRABAJO
Y PREVISIÓN SOCIAL
GOBIERNO DE
EL SALVADOR
UNÁMONOS PARA CRECER

Unidad de Adquisiciones y Contrataciones Institucional

MEMORANDUM

PARA: **Lic. Walter de Jesús Zúniga Reyes**
Jefe de la Unidad Jurídica

DE: **Licda. Mayra Yessenia Palma Gutiérrez.**
Jefa UACI Ad Honorem.

ASUNTO: **Elaboración de Acuerdo de CEO y Administrador de Orden de Compra.**

FECHA: 18 de junio de 2018.

Estimado Licenciado:

Referente al proceso de **Libre Gestión MTPS 12-2018 "ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS";** muy atentamente estoy solicitando la elaboración de acuerdo para nombrar como miembros de la Comisión de Evaluación de Ofertas a las siguientes personas:

- **Licda. Yolanda del Carmen Dueñas Figueroa**, Directora Administrativa;
- **Licda. Mayra Yessenia Palma Gutiérrez,** Jefa Unidad de Adquisiciones y Contrataciones Institucional Ad Honorem;
- **Lic. Luis Mario Flores Guillén**, Jefe Unidad Financiera Institucional;
- **Ing. Juan Francisco Sánchez**; Jefe de la Unidad de Desarrollo Tecnológico;
- **Y la persona que sea designa de la Unidad Jurídica para integrar esta comisión.**

De igual forma se solicita la elaboración de acuerdo para nombrar como Administrador de Contrato al **INGENIERO JUAN FRANCISCO SANCHEZ;** Jefe de la Unidad de Desarrollo Tecnológico.

Atentamente,

MINISTERIO DE TRABAJO Y PREVISION SOCIAL
18 JUN. 2018
2:42 pm
RECIBIDO
UNIDAD DE ASESORÍA JURIDICA

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
Unidad de Adquisiciones y contrataciones Institucional
San Salvador, El Salvador, C.A.

San Salvador, 15 de junio de 2018

Empresas:
JMTELCOM, S.A. DE C.V.
RYASA, S.A. DE C.V.
JL SECURITY TECHNOLOGIES
Presente.-

Respetables Empresas:

Reciban un cordial saludo deseándoles éxito en sus labores cotidianas. El motivo de la presente es para hacerles la atenta invitación a participar en el proceso por Libre Gestión: **LG MTPS 12-2018 "ADQUISICIÓN DE EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"**, Para lo cual se les adjuntan Documento de Especificaciones Técnicas.

Esperando contar con su participación.

Atentamente,

Licda. Mayra Yessenia Palma Gutiérrez
Jefa de la Unidad de Adquisiciones
y Contrataciones Institucional Ad Honorem

Recibido 18.06.18

JMTELCOM

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
Unidad de Adquisiciones y contrataciones Institucional
San Salvador, El Salvador, C.A.

San Salvador, 15 de junio de 2018

Empresas:
JMTELCOM, S.A. DE C.V.
RYASA, S.A. DE C.V.
JL SECURITY TECHNOLOGIES
Presente.-

Respetables Empresas:

Reciban un cordial saludo deseándoles éxito en sus labores cotidianas. El motivo de la presente es para hacerles la atenta invitación a participar en el proceso por Libre Gestión: **LG MTPS 12-2018 "ADQUISICIÓN DE EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"**, Para lo cual se les adjuntan Documento de Especificaciones Técnicas.

Recibida
15-06-2018
5:02 p.m.
Jaret Moran

Esperando contar con su participación.

Atentamente,

Licda. Mayra Yessenia Palma Gutiérrez
Jefa de la Unidad de Adquisiciones
y Contrataciones Institucional Ad Honorem

JARET NAUN MORAN SORTO
TEL: 2226-0951
JL SEGURITY

Blanca Azucena Canizales

De: Edgardo Alexis Menendez Ramirez <jl_alexis.menendez@yahoo.com>
Enviado el: viernes, 15 de junio de 2018 05:49 p.m.
Para: Blanca Azucena Canizales
Asunto: Re: Invitación a presentar ofertas

muy buenas tardes Licda. Blanca

muchas gracias por la invitación con gusto trabajaremos para presentar nuestra oferta

saludos cordiales

El Viernes, 15 de junio, 2018 17:01:55, Blanca Azucena Canizales <blanca.canizales@mtps.gob.sv> escribió:

Buenas tardes.

Reciba cordiales saludos deseándole éxitos en sus actividades cotidianas.

*Por este medio la Unidad de Adquisiciones y Contrataciones Institucional les invita a participar en el proceso de Libre Gestión MTPS 12-2018 sobre el "**Adquisición de equipos de seguridad perimetral con licencias**" de acuerdo a las condiciones, especificaciones técnicas e información adjunta, favor **leer detalladamente** el documento de invitación, y empezar a tramitar las cartas de referencias. Las consultas se estarán recibiendo hasta la fecha indicada en el documento.*

Importante:
*Les solicito **reenviar NOTA DE INVITACIÓN adjunta con firma, sellos, fecha y hora de recibida**, para confirmar la recepción de la nota y la participación en el proceso, dicha confirmación también es importante para el control de expediente. De antemano agradezco su ayuda y esperando contar con su participación, me despido.*

(FAVOR CONFIRMAR DE RECIBIDO ESTE CORREO)

Atentamente,

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
GOBIERNO DE EL SALVADOR
UNÁMONOS PARA CRECER

Blanca Azucena Canizales Ortiz
Colaboradora UACI
Unidad de Adquisiciones y Contrataciones Institucional
Ministerio de Trabajo y Previsión Social
Correo: blanca.canizales@mtps.gob.sv
***Teléfonos:** 2529-3728/ 2529-3714/ 3740/3760/3727/3771*
Dirección: Alameda Juan Pablo II y 17 Av. Nte. Plan Maestro, Centro de Gobierno, Edificio No.3, Primer Nivel.

Blanca Azucena Canizales

De: Blanca Azucena Canizales <blanca.canizales@mtps.gob.sv>
Enviado el: viernes, 15 de junio de 2018 05:01 p.m.
Para: 'jl_alexis.menendez@yahoo.com'; 'flor.ramirez@ryasa.com.sv'; 'florramirez.ryasa@yahoo.com'; rocio.guardado@jmtelcom.com
CC: Mayra Palma
Asunto: Invitación a presentar ofertas
Datos adjuntos: LG MTPS 12-2018.pdf; INVITACIÓN LG MTPS 12-2018.pdf; image001.jpg; image003.jpg

Buenas tardes.

Reciba cordiales saludos deseándole éxitos en sus actividades cotidianas.

*Por este medio la Unidad de Adquisiciones y Contrataciones Institucional les invita a participar en el proceso de Libre Gestión MTPS 12-2018 sobre el "**Adquisición de equipos de seguridad perimetral con licencias**" de acuerdo a las condiciones, especificaciones técnicas e información adjunta, favor **leer detalladamente** el documento de invitación, y empezar a tramitar las cartas de referencias. Las consultas se estarán recibiendo hasta la fecha indicada en el documento.*

Importante:
*Les solicito **reenviar NOTA DE INVITACIÓN adjunta con firma, sellos, fecha y hora de recibida**, para confirmar la recepción de la nota y la participación en el proceso, dicha confirmación también es importante para el control de expediente. De antemano agradezco su ayuda y esperando contar con su participación, me despido.*

(FAVOR CONFIRMAR DE RECIBIDO ESTE CORREO)

Atentamente,

MINISTERIO DE TRABAJO
Y PREVISIÓN SOCIAL
GOBIERNO DE
EL SALVADOR
¡NÁMONOS PARA CRECER

Blanca Azucena Canizales Ortiz
Colaboradora UACI
Unidad de Adquisiciones y Contrataciones Institucional
Ministerio de Trabajo y Previsión Social
Correo: blanca.canizales@mtps.gob.sv
***Teléfonos:** 2529-3728/ 2529-3714/ 3740/3760/3727/3771*
Dirección: Alameda Juan Pablo II y 17 Av. Nte. Plan Maestro, Centro de Gobierno, Edificio No.3, Primer Nivel.

57

COMPRASal
Sistema Electrónico de Compras Públicas de El Salvador

UNAC

(index.jsf)

Regresar a la lista

Generales del proceso | Documentos Anexos

Forma ofertar:	Presencial
Institución	Ministerio de Trabajo y Previsión Social (MTPS)
Correlativo COMPRASAL	20180156
Oficina gestora de la convocatoria	UACI de Ministerio de Trabajo y Previsión Social 2529-3760, 25293740
Horario de atención de la oficina gest ora	07:30 PM a 12:30 PM 01:15 PM a 03:30 PM
Nombre del contacto	ROSA MARIA HERNANDEZ
Descripción	ADQUISICION DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS.
Período de vigencia	15/06/2018 - 16/06/2018
Condiciones de compra	VER TDR

MINISTERIO DE HACIENDA
GOBIERNO DE EL SALVADOR

Copyright © 2013. Ministerio de Hacienda. Gobierno de la República de El Salvador. Todos los derechos reservados.

54

COMPRASal
Sistema Electrónico de Compras Públicas de El Salvador

UNAC

(index.jsf)

Inicio Convocatorias Resultados Búsqueda Sanciones PAAC Estadísticas Marco normativo Noticias Enlaces Contáctenos

LIBRE GESTIÓN

Búsqueda de convocatorias

Período | Fecha inicial | Fecha final | Ministerio de Trabajo y Previsión Social (MTPS) | Buscar

Institución	Correlativo de compra	Descripción	Condiciones de compra	Fecha de publicación	Tipo Cotizacion
Ministerio de Trabajo y Previsión Social (MTPS)	20180156	ADQUISICION DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS.	VER TDR	15/06/2018	Presencial
Ministerio de Trabajo y Previsión Social (MTPS)	20180155	COMPRA DE 949 LICENCIAS	VER TDR	14/06/2018	Presencial

(1 of 1)

MINISTERIO DE HACIENDA
GOBIERNO DE EL SALVADOR

Contáctenos: unac.solicitudes@mh.gob.sv (mailto:unac.solicitudes@mh.gob.sv), (503) 2244-3171 Horarios: 8:30am a 12:00m y 12:40pm a 4:30pm
Edificio Ministerio de Hacienda 3er. Nivel, Blvd. de los Heroes,1231, San Salvador, El Salvador.
Copyright © 2013. Ministerio de Hacienda. Gobierno de la República de El Salvador. Todos los derechos reservados.
Version:PR_V2.037
15/06/2018 05:10 PM

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL
Unidad de Adquisiciones y contrataciones Institucional
San Salvador, El Salvador, C.A.

San Salvador, 15 de junio de 2018

Empresas:
JMTELCOM, S.A. DE C.V.
RYASA, S.A. DE C.V.
JL SECURITY TECHNOLOGIES
Presente.-

Respetables Empresas:

Reciban un cordial saludo deseándoles éxito en sus labores cotidianas. El motivo de la presente es para hacerles la atenta invitación a participar en el proceso por Libre Gestión: **LG MTPS 12-2018 "ADQUISICIÓN DE EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"**, Para lo cual se les adjuntan Documento de Especificaciones Técnicas.

Esperando contar con su participación.

Atentamente,

Licda. Mayra Yessenia Palma Gutiérrez
Jefa de la Unidad de Adquisiciones
y Contrataciones Institucional Ad Honorem

MINISTERIO DE TRABAJO

Y PREVISION SOCIAL

MINISTERIO DE TRABAJO
Y PREVISIÓN SOCIAL
GOBIERNO DE
EL SALVADOR
UNÁMONOS PARA CRECER

UNIDAD DE ADQUISICIONES Y CONTRATACIONES INSTITUCIONAL (UACI)

DOCUMENTO DE ESPECIFICACIONES TECNICAS

LIBRE GESTIÓN

"ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS"

LG MTPS 12 – 2018

San Salvador, junio 2018

Alameda Juan Pablo Segundo y 17 Avenida Norte, Edificio Nos. 2,3 y 4, Plan Maestro Centro de Gobierno: 2529-3728, 2529-3740, 2529-3760, 2529-3761, 2529-3762; Fax 2529-3747, 2529-3748

ÍNDICE

Página

INSTRUCCIONES A LOS OFERENTES 4

1. GENERALIDADES 4

1.1. Objeto de la Libre Gestión 4

1.2. Dirección del Contratante 4

1.3. Prácticas Corruptivas 4

1.4. Oferentes Hábiles para Ofertar 4

2.CONTENIDO DE LOS DOCUMENTOS DE LIBRE GESTIÓN 5

2.1 Secciones de los Documentos de Contratación 5

2.2 Aclaraciones sobre Documentos de Contratación 5

3.PREPARACIÓN DE LAS OFERTAS 5

3.1 Costos de las Ofertas 5

3.2 Idioma de la Oferta 5

3.3 Documentos que Componen la Oferta 6

3.4 Formularios de Presentación de Ofertas 6

3.5 Moneda de la Oferta o Cotización y Financiamiento 7

3.6 Plazo y Forma de Pago 7

3.7 Documentos que establecen la conformidad de documentos de contratación 7

3.8 Periodo de Validez de las Ofertas 7

3.9 Presentación de la Oferta 7

4.PRESENTACIÓN Y APERTURA DE OFERTAS 8

4.1. Identificación de Ofertas 8

4.2. Plazo para la presentación de ofertas 8

5.EVALUACIÓN Y COMPARACIÓN DE OFERTAS 8

5.1. Confidencialidad 8

5.2. Aclaración de Ofertas 8

5.3. Evaluación de Ofertas 8

5.4. Recomendación de Oferta Ganadora 9

6.CRITERIOS DE SELECCIÓN 9

6.1. Criterios de Selección de Oferta ganadora 9

6.2. Firma de Contrato. 10

6.3. Garantía de Fiel Cumplimiento. 10

6.4. Garantía de Buen Funcionamiento y Calidad de los Bienes. 10
6.5. Declaración Jurada del tipo de categoría de la empresa 10
6.6. Declaración Jurada 10
6.7. FORMATO DE OFERTA 11

ANEXO N° 1 ESPECIFICACIONES TÉCNICAS. 12
ANEXO N° 2 FORMULARIO PARA PERSONAS JURIDICAS 18
ANEXO N° 3 FORMULARIO PARA PERSONAS NATURALES 19
ANEXO N° 4 CARTA DE REFERENCIA 20
ANEXO N° 5 DECLARACIÓN JURADA 21

DOCUMENTO DE ESPECIFICACIONES TÉCNICAS

Instrucciones a los Oferentes	
1. GENERALIDADES	
1.1. Objeto de la Libre Gestión	De conformidad con la solicitud de cotización, el Contratante emite los documentos de contratación para el proceso No. **LG MTPS 12 - 2018, para "ADQUISICIÓN DE 19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS".** De conformidad a lo detallado en estos documentos.
1.2. Dirección del Contratante	Para el propósito de aclaración y presentación de oferta se establece que la dirección de la Institución contratante es la siguiente: Dirección: Alameda Juan Pablo II, y 17 Av. Nte. Plan Maestro Centro de Gobierno, Edificio 3, Nivel 1. Ciudad: San Salvador País: El Salvador Tel. 2529-3760, 2529-3740, 2529-3761, fax Directo 2529-3747, 2529-3748
1.3. Prácticas Corruptivas	Si se comprueba que en procedimientos administrativos de contratación pública, un funcionario o empleado público o un particular han incurrido en cualquiera de las infracciones establecidas en los Artículos 151, 152, 153 y 158 de la LACAP, se aplicará las sanciones que correspondan, agotados los procedimientos establecidos en los Arts, 156 y 160 LACAP.
1.4. Oferentes Hábiles para Ofertar	• Persona natural o jurídica, nacional o extranjera o cualquier combinación de ellas, en forma de Participación Conjunta. A menos que se indique de otra manera en los Términos de Referencia, en este caso las partes deberán ser solidariamente responsables. • El Participante hará prevalecer los intereses del Contratante, evitando conflictos con otros o con sus propios intereses. • Aquellos que no estén en conflicto con sus obligaciones previas o actuales con respecto a los intereses del Contratante. • El participante no deberá estar incluido en las incapacidades, impedimentos e inhabilidades establecidas en los Arts. 25, 26 y 158 de la LACAP.

2. CONTENIDO DE LOS DOCUMENTOS DE LIBRE GESTIÓN	
2.1 Secciones de los Documentos de Contratación	Los documentos de contratación para Libre Gestión están compuestos por: Sección incluyendo las Especificaciones Técnicas, los documentos comprenden además cualquier aclaración o corrección que emita el contratante en relación al proceso de Libre Gestión. El Contratante no acepta responsabilidad alguna en cuanto a que sus documentos de contratación y sus aclaraciones estén completas, a menos que estas se hayan obtenido directamente del contratante o del sistema COMPRASAL. Es responsabilidad del participante examinar todas las instrucciones, formularios y condiciones de los documentos de contratación y de proporcionar toda la información o documentación requerida al presentar su oferta o cotización.
2.2 Aclaraciones sobre Documentos de Contratación	El oferente que requiere alguna aclaración sobre los Documentos de la Libre Gestión deberá solicitarlo por escrito a la UACI quién responderá también por escrito, cualquier solicitud de aclaración que reciba a más tardar el día **18 de junio de 2018 hasta las 12:30p.m.,** el contratante enviará copia de las respuestas, incluyendo una descripción de las consultas realizadas, sin identificar su fuente, a todos los oferentes que hubiesen obtenido las especificaciones técnicas, directamente del contratante o de COMPRASAL.
3. PREPARACIÓN DE LAS OFERTAS	
3.1 Costos de las Ofertas	El oferente sufragará todos los gastos relacionados con la preparación y presentación de su oferta, independientemente de su resultado. El contratante no será responsable en ningún caso de dichos costos, independientemente de la forma en que se lleve a cabo la contratación o de su resultado.
3.2 Idioma de la Oferta	La oferta que prepare el participante, así como toda la correspondencia y documentos relativos intercambiados por el participante y el contratante, deberán redactarse en el idioma castellano. Los documentos complementarios y textos impresos que formen parte de la oferta podrán estar escritos en otro idioma, con la condición de que las partes relevantes de dicho material vayan acompañados de las correspondientes diligencias notariales de traducción al idioma castellano.

3.3 Documentos que Componen la Oferta	Oferta Técnica • Especificaciones Técnicas, Anexo 1 Detalle de las especificaciones técnicas ofrecidas por el participante. • Otros documentos técnicos, tales como manuales, brochures, permisos, etc. que se estimen necesarios requerir, en atención del tipo de bien o servicio ofrecido, de carácter obligatorio. Oferta Económica • Oferta económica precios unitarios y totales con IVA incluido. Documentos legales **(aplica únicamente al adjudicado)** • La documentación legal será solicitada oportunamente al ofertante que resultare adjudicado. • Documentos contenidos en el Formulario Anexo 2 para personas jurídicas. • Documentos contenidos en el Formulario Anexo 3 para personas naturales. **Nota: Se deberá ofertar la totalidad de los bienes solicitados (equipos y licencias).**
3.4 Formularios de Presentación de Ofertas	El oferente deberá presentar la oferta y sus documentos en la forma establecida por el contratante. La oferta incluye: a) Manifestación expresa de conocimiento y aceptación de cada una de las aclaraciones, emitidas de los documentos de contratación, si las hay. b) Descripción detallada de las especificaciones técnicas de los bienes o servicios y cualquier otro requisito necesario; c) Precios unitarios y total de la oferta, con IVA incluido; d) Período de vigencia de la oferta (mínimo 30 días calendario); e) 3 referencias de empresas públicas o privadas, Anexo 4. f) Compromiso de presentar garantía de cumplimiento de contrato, por el valor del 10% del monto adjudicado. El adjudicatario dispondrá de cinco días hábiles, posteriores a la entrega y firma del contrato, para la presentación de esta, y estará vigente por un periodo de 15 días calendario. g) Compromiso de presentar garantía de buen funcionamiento y calidad de los bienes por el valor del 10% del monto adjudicado. La cual deberá de ser presentada cinco días hábiles siguientes a la recepción definitiva de los bienes.

3.5 Moneda de la Oferta o Cotización y Financiamiento	Los precios de la oferta serán cotizados en dólares de los Estados Unidos de Norte América; serán financiados con fondos GOES.
3.6 Plazo y Forma de Pago	Se realizará contrato y el suministro de los bienes se realizará en una sola entrega. Se realizará un solo pago cuando se compruebe que el contratista ha hecho la entrega del suministro solicitado de acuerdo a lo pactado en el contrato. Dicho pago se hará efectivo dependiendo de la clasificación de la empresa, de conformidad al artículo N°32 de la "Ley de Protección, Fomento y Desarrollo de la Micro, Pequeña Empresa y otros contribuyentes", se hará efectivo a treinta (30) días calendarios siguientes a la presentación de la factura; para la Mediana y Gran empresa se hará efectivo a 60 días calendarios siguientes a la presentación de la factura siempre y cuando la documentación presentada esté de acuerdo a los requerimientos del contratante, entregando factura y acta de recepción, con visto bueno del administrador de contrato en ambos casos.
3.7 Documentos que establecen la conformidad de documentos de contratación	El oferente deberá presentar la evidencia documentada señalados en los Documentos de la Libre Gestión, que demuestren un cumplimiento sustancial con los requerimientos del contratante.
3.8 Periodo de Validez de las Ofertas	Las ofertas deberán permanecer validas por un periodo de 30 días a partir de la fecha de presentación de las mismas.
3.9 Presentación de la Oferta	El oferente deberá prepara un original de su oferta y marcar claramente en dicho ejemplar la palabra **"ORIGINAL".** Adicionalmente el oferente deberá presentar una copia de la oferta, y marcarla con la palabra **"COPIA".** En caso de cualquier discrepancia entre original y copia prevalecerá el original. La oferta original deberá ser firmada por el oferente o por su apoderado; para el caso de persona jurídica, por el representante legal o su apoderado. El documento que acredita la facultad de la persona que firme deberá adjudicarse la oferta según lo indicado en los Documentos de esta Libre Gestión. Las páginas de las ofertas deberán ser presentadas por índice y numeradas correlativamente, de igual forma cualquier información técnica, legal o broshures adicionales. Y deberán llevar la firma o

	rubrica de las personas que firman las ofertas. Si la documentación es emitida en el extranjero ésta deberá presentarse debidamente apostillada tratándose de país subscriptores del convenio de la Haya. Para los países no suscriptores del convenio deberán seguir el trámite de legalización de firmas establecidos en el Código Procesal Civil y Mercantil de El Salvador.
4. PRESENTACIÓN Y APERTURA DE OFERTAS	
4.1. Identificación de Ofertas	El oferente presentará el original y una copia de la oferta en sobres separados y cerrados. Cada sobre deberá estar claramente identificado con los términos original y copia según corresponda, **"ORIGINAL", o "COPIA",** los sobres en su exterior deberán: • Indicar el nombre y dirección del oferente • Estar dirigidos al Ministerio de Trabajo y Previsión Social • Indicar la Identificación de la Libre Gestión
4.2. Plazo para la presentación de ofertas	Presentación de Ofertas: día **22 de junio de 2018**, desde las **8:30 a.m. hasta las 12:30 p.m.**, en la Unidad de Adquisiciones y Contrataciones Institucional del Ministerio de Trabajo y Previsión Social, en la dirección: final 17 Av. Nte. y Alameda Juan Pablo II, Centro de Gobierno, Edificio Número tres, primer nivel, San Salvador. Con atención a la Licda. Mayra Palma; Jefa UACI Ad Honorem. No se consideraran, las ofertas presentadas posteriores a la hora y fecha limite señalada.
5. EVALUACIÓN Y COMPARACIÓN DE OFERTAS	
5.1. Confidencialidad	No se divulgara a los ofertantes ni a cualquier otra persona que no esté oficialmente involucrada en el proceso de esta contratación, ninguna información relacionada con la revisión, evaluación y comparación de las ofertas o cotizaciones, ni las recomendaciones para la adjudicación.
5.2. Aclaración de Ofertas	Para facilitar el proceso de revisión, evaluación y comparación de ofertas, el contratante podrá a su discreción, solicitar a los oferentes aclaraciones acerca de sus ofertas. No serán consideradas las aclaraciones presentadas por los oferentes que no sean en respuesta a aclaraciones solicitadas por el contratante.
5.3. Evaluación de	La determinación por parte del Contratante de si una oferta se ajusta a los Documentos de Contratación, se basara solamente en el

Ofertas	contenido de la propia oferta. Si en la oferta económica se detectaren errores aritméticos, estos serán corregidos por la Unidad solicitante o la Comisión de Evaluación de Ofertas (CEO), prevaleciendo en todo caso el precio unitario. A estos efectos, se reajustara el precio de la oferta a fin de reflejar el precio resultante. La unidad solicitante o la Comisión de Evaluación de Ofertas, según corresponda, examinaran las ofertas, para confirmar que todos los términos y condiciones que se especifiquen en los Documentos de Contratación, han sido aceptados por el oferente sin reservas. Se deberán evaluar los aspectos técnicos de la oferta, presentados para confirmar que cumple con todos los requisitos especificados. La Unidad solicitante o la CEO, evaluara aquellas ofertas o cotizaciones que haya determinado que cumplen con los documentos de contratación. En la evaluación de una oferta, se tomara en cuenta lo siguiente: • El Precio de la Oferta. • Ajustes de precios por corrección de errores aritméticos. • Aplicación de todos los factores de evaluación. La CEO deberá comparar todas las ofertas que se ajustan a los documentos de contratación para determinar cuál es la oferta mejor evaluada. Para la evaluación técnica se tomará en cuenta la calidad de los productos que ofrece la empresa, esta evaluación técnica será bajo los criterios de "Cumple" y "No cumple". La Institución seleccionará la oferta que en su evaluación cumpla con las especificaciones técnicas requeridas por la Institución y que presente el precio más bajo.
5.4. Recomendación de Oferta Ganadora	La Comisión de Evaluación de Ofertas, deberá informar a la UACI, el resultado de la evaluación y recomendación de la oferta o cotización ganadora. Dicha recomendación no creara derechos en favor de ningún oferente.
6. Criterios de Selección	
6.1. Criterios de Selección de Oferta ganadora.	El contratante seleccionará al oferente cuya oferta haya sido mejor evaluada y que cumple sustancialmente con los documentos de contratación. Durante el análisis de las ofertas, el contratante podrá aumentar o disminuir la cantidad a contratar, por lo cual, se deberá

	mantener el precio unitario si así conviene a los intereses del contratante. **Por la naturaleza de la contratación la adjudicación será a un solo oferente.**
6.2. Firma de Contrato.	Después de comunicado el resultado del proceso de contratación LG MTPS 12-2018, la UACI solicitará la documentación legal para la elaboración del Contrato, los cuales deberán ser presentados en un plazo no mayor de 5 días hábiles. Posteriormente la UACI convocará al oferente seleccionado ganador para la firma del contrato. La no presentación del adjudicatario para la firma de Contrato en el plazo establecido, sin justa causa, será suficiente para cerrar el proceso. En tal caso el contratante podrá seleccionar al siguiente mejor evaluado, y se iniciara el procedimiento sancionatorio correspondiente. El contratista dispondrá, del plazo establecido en los documentos de contratación para la presentación de las garantías.
6.3. Garantía de Fiel Cumplimiento.	El adjudicatario dispondrá de cinco días, posteriores a la formalización y entrega del contrato, para la presentación de la garantía de Fiel Cumplimiento, la que se constituirá por un 10% del monto total, para garantizar el cumplimiento de la misma, y estará vigente por un periodo de 15 días calendario, después de firmado y entregado el contrato.
6.4. Garantía de Buen Funcionamiento y Calidad de los Bienes.	El adjudicatario dispondrá de cinco días hábiles siguientes a la recepción definitiva de los bienes, para la presentación de garantía de buen funcionamiento y calidad de los bienes, que se constituirá por un 10% del monto total y estará vigente por 12 meses, contados a partir de la entrega formal del suministro.
6.5. Declaración Jurada del tipo de categoría de la empresa	El Representante legal o el propietario, deberá presentar Declaración Jurada en la cual se detalle el tipo de categoría de la empresa emitida por el Ministerio de Hacienda.
6.6. Declaración Jurada	El Representante legal o propietario deberá presentar Declaración Jurada en la cual se detalle la no utilización de trabajo de niñas, niños y adolescentes por debajo de la edad mínima de admisión al empleo. Ver anexo 5.

6.7. FORMATO DE OFERTA

CANTIDAD	DESCRIPCIÓN (Detallar: Imagen, marca, modelo)	PRECIO UNITARIO IVA INCLUIDO	TOTAL

NOTA: Detallar precio de licencias y equipo por separado

MINISTERIO DE TRABAJO Y PREVISION SOCIAL
UNIDAD DE ADQUISICIONES Y CONTRATACIONES INSTITUCIONAL
UACI

Licenciada Mayra Yessenia Palma Gutiérrez
Jefa de la Unidad de Adquisiciones y Contrataciones
Institucional Ad Honorem

ANEXO N° 1
ESPECIFICACIONES TÉCNICAS.

- **19 EQUIPOS DE SEGURIDAD PERIMETRAL CON LICENCIAS**

CARACTERÍSTICAS DE EQUIPO AL QUE DEBERÁ ASOCIARSE LICENCIAMIENTO DE SEGURIDAD PERIMERAL

SITIO PRINCIPAL Y SITIO REMOTO (SANTA ANA)			
CARACTERISTICA	**DESCRIPCIÓN**	**CUMPLE**	
Capacidad de usuarios	Hasta 1000		
Cantidad de equipos	Dos		
Configuración	Contingencia		
Almacenamiento	240 GB mínimo		
Consumo de energía	Fuente redundante		
Conexiones concurrentes	Mínimo 1 millón		
AV rendimiento	Mínimo 1.5 GBPS		
IPS rendimiento	Mínimo 2 GBPS		
Firewall rendimiento	Mínimo 4 GBPS		
Interfaces	Capacidad de ampliación		
Módulos de protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPsec.		
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.		
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.		
Seguridad web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS.		
Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, IPsec. 6. Compatibilidad de sistema de autenticación: RADIUS,		

	LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.		
Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe permitir / restringir / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.		
IPS	1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.		
Protección de correo electrónico	Especificar		
Protección de redes inalámbricas	Especificar		
	OTRAS		
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.		
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.		

Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.		
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.		

CARACTERÍSTICAS DE EQUIPO AL QUE DEBERÁ ASOCIARSE LICENCIAMIENTO DE SEGURIDAD PERIMERAL

OFICINAS REGIONALES (A EXCEPCION DE SANTA ANA) Y DEPARTAMENTALES			
CARACTERISTICA	**DESCRIPCIÓN**	**CUMPLE**	
Capacidad de usuarios	Hasta 100		
Cantidad de equipos	Doce		
Almacenamiento	64 GB mínimo		
Consumo de energía	Especificar		
Conexiones concurrentes	Mínimo 600 K		
AV rendimiento	Mínimo 500 MBPS		
IPS rendimiento	Mínimo 400 MBPS		
Firewall rendimiento	Mínimo 1.5 GBPS		
Interfaces	Capacidad de ampliación		
Módulos de protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPsec.		
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.		
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.		
Seguridad web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS.		
Protección de red	1. Administración web protegido por contraseña personalizable.2. Enrutamiento de tráfico de red.3. Balanceo de enlaces.4. Prevención de Intrusos.5. Protección contra DOS. VPN punto a punto: SSL, IPsec.6. Compatibilidad de sistema de autenticación: RADIUS, LDAP.7. Generación de reportes		

	automáticos enviados por medio de correo electrónico.		
Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe permitir / restringir / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.		
IPS	1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.		
Protección de correo electrónico	Especificar		
Protección de redes inalámbricas	Especificar		
OTRAS			
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.		
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.		
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.		
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.		

CARACTERÍSTICAS DE EQUIPO AL QUE DEBERÁ ASOCIARSE LICENCIAMIENTO DE SEGURIDAD PERIMERAL

CENTROS DE RECREACIÓN Y ARCHIVO GENERAL			
CARACTERISTICA	**DESCRIPCIÓN**	**CUMPLE**	
Capacidad de usuarios	Hasta 15		
Cantidad de equipos	Cinco		
Almacenamiento	64 GB mínimo		
Consumo de energía	Especificar		
Conexiones concurrentes	Mínimo 600 K		
AV rendimiento	Mínimo 400 MBPS		
IPS rendimiento	Mínimo 300 MBPS		
Firewall rendimiento	Mínimo 900 MBPS		
Interfaces	Capacidad de ampliación		
Módulos de protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPsec.		
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.		
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.		
Seguridad web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS.		
Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, IPsec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.		
Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http, y https.2. Debe permitir / restringir / acceso a categorías		

	tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc.3. Que permita bloqueo de URL, Keyword o Frase.4. Lista de Excepción de URL5. Bloqueo de Java, Applet, Cookies y ActiveX6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador.7. Control de aplicaciones.		
IPS	1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.		
Protección de correo electrónico	Especificar		
Protección de redes inalámbricas	Especificar		
OTRAS			
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.		
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.		
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.		
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.		

Nota: La entrega de las licencias y equipo se deberá realizar en un máximo de 15 días calendario.

ANEXO No. 2

FORMULARIO PARA PERSONA JURÍDICA

N°	DETALLE	CUMPLE	
		SI	NO
1	Copia certificada por notario de Escritura de Constitución, inscrito en el Registro de Comercio. Para extranjeros, Estatutos o Documento Constitutivo, según sea el caso, debidamente legalizado deacuerdo a loqueestablece supaís de origen, Apostillado o consularizado.		
2	Copia certificada por notario de la Escritura de Modificación, Transformación o Fusión de la Sociedad inscrita en el Registro de Comercio. Para extranjeros, el documento que contenga los modificaciones o transformaciones de sus estatutos, legalizandose acuerdo a lo que establece su país de origen, apostillado o consularizado.		
3	Copia certificada por notario de Matrícula de Comercio de empresa mercantil o en su defecto recibo de pago de la misma o constancia extendida por el Registro de Comercio que la emisión de la matrícula se encuentra en trámite de renovación o primera vez según sea el caso. Para extranjeros, su documento Equivalente a la matrícula de comercio, debidamente apostillado o consularizado.		
4	Copiacertificada por notario de Credencial vigente de nombramiento de Representante legal u otro documento que lo acredite como tal. Para extranjeros, el documento que acredite la representación legal, apostillado o consularizado.		
5	Copia certificada por notario de Escritura de Poder Especial o General con cláusula especial para ofertar y contratar en procesos de contratación pública, Inscrito en el Registro de Comercio. Para extranjeros, el Poder debidamente apostillado o consularizado.		
6	Copla certificada por notario de DUI y NIT, del representante legal de la sociedad. Pasaporte o Carné de Residente de extranjeros que deben estar vigentes a la fecha.		
7	Copla certificada por notario de Tarjeta del Número de Identificación Tributaria (NIT).		
8	Solvencia en original de los Impuestos Municipales del domicilio de la sociedad, vigente a la fecha de la apertura de ofertas.		
9	Solvencia en original de la Unidad de Pensiones del Instituto Salvadoreño del Seguro Social (UPISSS), vigente a la fecha de la apertura de ofertas.		
10	Solvencia en original de pago de cotizaciones Obrero-Patronales del Instituto Salvadoreño del Seguro Social(ISSS), vigente a la fecha de la apertura de ofertas.		
11	Solvencias en original de las Administradoras de Fondos de Pensiones CRECER y CONFIA, vigentes a la fecha de la apertura de ofertas. En caso de no cotizar para alguna de las referidas instituciones, deberá presentar constancia emitida por la AFP en que se establezca dicha circunstancia.		
12	Constancia en original emitida por el Instituto de Previsión Social de la Fuerza Armada en la que se indique que estás solvente en el pago de cotizaciones y aportes previsionales, en caso de no cotizar, deberá presentar constancia de del Instituto en la que se establezca que no cotizo para dicha entidad.		

ANEXO N° 3

FORMULARIO PARA PERSONA NATURAL

No.	DETALLE	CUMPLE	
		SI	NO
1	Copia certificada por notario de DUI o Pasaporteo Carné de Residente, documentos que deben estar vigentes a la fecha		
2	Copia certificada por notario de Tarjeta del Número de Identificación Tributaria (NIT).		
3	Copia certificada por notario de constancia de Matrícula de Comercio de empresa mercantil, si les fuere aplicable por el monto de sus activos, o en su defecto del recibo de pago de la misma, o constancia extendida por el Registro de Comercio que la emisión de la matrícula se encuentra en trámite de renovación o primera vez según sea el caso. Para extranjeros, su documento equivalente o la matrícula de comercio, debidamente apostillado o consularizado.		
4	Copia certificada por notario de Escritura de Poder Especial o General con cláusula especial paro ofertar y contratar en procesos de contratación pública, inscrito en el Registro de Comercio. Para extranjeros, el Poder debidamente apostillado o consularizado.		
5	Solvencia en original de los Impuestos Municipales del domicilio del establecimiento principal, vigente a la fecha de la apertura de ofertas.		
6	Solvencia en original de la Unidad de Pensiones del Instituto Salvadoreño del Seguro Social (UPISSS), vigente a la fecha de la apertura de ofertas.		
7	Solvencia en original de Pago de cotizaciones Obrero Patronales del Instituto Salvadoreño del Seguro Social (ISSS), vigente a la fecha de la apertura de oferta.		
8	Solvencias en original de las Administradoras de Fondos de Pensiones **CRECER** y CONFIA, vigentes a la fecha de la apertura de ofertas. En caso de no cotizar para alguna de las referidas Instituciones, deberá presentar constancia emitida por la AFP en que se establezca dicha circunstancia.		
9	Constancia en original emitida por el Instituto de Previsión Social de la Fuerza Armada en la que se indique que está solvente en el pago de cotizaciones y aportes previsionales, en caso de no cotizar, deberá presentar constancia de Instituto en la que se establezco que no cotiza para dicha entidad.		

ANEXO No. 4

Nombre o Razón Social del Oferente:

_____

I. DATOS GENERALES DE LA INSTITUCIÓN:

1. Nombre de la Institución:

   _____

2. Dirección:

   _____

   Número Telefónico: _____
   Fax: _____
   Correo Electrónico: _____

3. A continuación proporcionar los siguientes datos:

II. IDENTIFICACIÓN DEL CONTRATO:

NOMBRE DEL CONTRATO:	
FECHA INICIO(DIA, MES, AÑO)	Día _____ Mes _____ Año _____
FECHA FINALIZACIÓN (DIA, MES, AÑO)	Día_____ Mes _____ Año _____
MONTO DEL CONTRATO EN US $	

III. CALIDAD DEL SERVICIO

INDICAR LA CALIDAD DEL SERVICIO RECIBIDO: **MARCAR CON UNA "X" UNA SOLA VALORACIÓN:**	**Regular** ( ) **Bueno** ( ) **Muy Bueno** ( ) **Excelente** ( )

Y para ser presentada a la Unidad de Adquisiciones y Contrataciones Institucional (UACI), del Ministerio de Trabajo y Previsión Social, se extiende la presente constancia, en la ciudad de San Salvador, a los _____

FIRMA:	SELLO DE LA INSTITUCION
NOMBRE:	
CARGO:	

ANEXO 5

En la ciudad de San Salvador, departamento de San Salvador, a las _____horas del día _____de _____dos mil _____ **ANTE MI,** _____ Notario, del domicilio de _____ comparece el señor (especificar generales completas), quien actúa en su calidad de _____ (consignar si es Representante Legal o Apoderado y relacionar la personaría según el caso) y en la calidad en que actúa **ME DICE**: Que con el objeto de participar en Proceso por Libre Gestión numero ---------- relativa a "----------". **BAJO JURAMENTO DECLARA**: **I)** Que en toda la cadena de producción de _____(obra, bienes o servicios) ofertados a la Institución por la empresa que represento, no se utiliza trabajo realizado por niños, niñas y adolescente por debajo de la edad mínima de admisión al empleo y se cumple en todo el proceso, productivo, con la normativa laboral vigente y con las regulaciones relativas a la protección integral de la niñez y la adolescencia, que tienen por objeto garantizar el goce y respeto pleno de los derechos los niños, niñas y adolescentes.

II) Que se cumple con la normativa nacional relacionada con la protección de la persona adolescente trabajadora, especialmente aquella relativa a la realización de actividades y trabajos peligrosos. **III)** Que se compromete a vigilar para que la empresa que representa, así como sus proveedores, contratistas y subcontratistas, en toda la cadena de producción, estén libres de trabajo infantil y se respete el marco legal de protección de la persona adolescente trabajadora. El suscrito Notario, hace constar que hice del conocimiento al compareciente lo regulado en el Código Penal, en cuanto al delito de falsedad ideológica, regulado en el Artículo doscientos ochenta y cuatro. El compareciente me manifiesta que para los efectos legales de la presente acta notarial y para los que surgieren en el proceso de licitación, señala como domicilio especial el de esta ciudad a cuyos tribunales se somete expresamente. Así se expresó el compareciente a quien expliqué los efectos legales de este instrumento notarial que consta de un folio útil y leído que le fue por mí íntegramente en un solo acto sin interrupción, ratifica su contenido y firmamos. **DOY FE.-**

MINISTERIO DE TRABAJO Y PREVISION SOCIAL
14 JUN. 2018
RECIBIDO
UACI
2:32pm

EL SALVADOR
UNAMONOS PARA CRECER

San Salvador, 13 de junio de 2018

Señores
Jefe de la Unidad Financiera
Presente.

En atención a los artículos 10 literal e) y 11 de la Ley de Adquis iciones y Contrataciones de la Administración Pública (LACAP), solicito su colaboración en el sentido de verificar la asignación presupuestaria para dar inicio a los procesos de compras siguientes:

UNIDAD DE ADQUISICIONES Y CONTRATACIONES INSTITUCIONAL				
Código del Proceso	**Descripción del Proceso**	**Unidad Presupuestaria Línea de Trabajo (Unidad Solicitante)**	**Objeto Específico de Gasto Presupuestario**	**Monto**
356	COMPRA DE 19 EQUIPOS SE ANEXAN ESPECIFICACIONES TECNICAS PARA EQUIPOS DE SEGURIDAD PERIMETRAL. SERA UTILIZADO PARA LA SEGURIDAD DE INFORMACION, FILTRADO DE CONTENIDO Y REDES VIRTUALES, SEGURIDAD DE DE SITIOS PUBLICOS INSTITUCIONALES EN TODAS LAS OFICINAS DEL MINISTERIO DE TRABAJO Y P.S. POR UN AÑO	UNIDAD DE DESARROLLO TECNOLOGICO 01/01	61104	$7,000.00
			TOTAL US $	$ 7,000.00

Licenciada Mayra Yessenia Palma Gutíerrez
Jefa UACI (ad-Honorem)

MINISTERIO DE TRABAJO Y PREVISION SOCIAL
UNIDAD DE ADQUISICIONES Y CONTRATACIONES INSTITUCIONAL
UACI
EL SALVADOR, C.A.

UNIDAD FINANCIERA			
Confirmación de asignación prespuestaria No. 356 Fecha: 14-06-18			
UP: 01	LT- 02	OBJ. ESP.: 61104	Monto: $ 6.500,-
UP:	LT-	OBJ. ESP.:	Monto: $
UP:	LT-	OBJ. ESP.:	Monto: $
		TOTAL	US $ 6.500,-
Observaciones:			

Lic. Luis Mario Flores Guillén,
Jefe UFI

MINISTERIO DE TRABAJO Y PREVISION SOCIAL
UNIDAD FINANCIERA INSTITUCIONAL
UFI
JEFE
EL SALVADOR, C.A.

MINISTERIO DE TRABAJO Y PREVISION SOCIAL
12 JUN. 2018 2:25pm.
RECIBIDO

42

GOBIERNO DE EL SALVADOR
UNÁMONOS PARA CRECER

No. de Requerimiento.	356

FECHA:	08 DE JUNIO DE 2018		
NOMBRE DEL SOLICITANTE:	ING. JUAN FRANCISCO SANCHEZ		
CARGO:	JEFE UNIDAD DE DESARROLLO TECNOLOGICO		
DEPENDENCIA:	DIRECCION EJECUTIVA	FIRMA DEL SOLICITANTE:	
NOMBRE DEL AUTORIZANTE:	LICDA. BEATRIZ DE PAUL	FIRMA DEL AUTORIZANTE	
CARGO:	DIRECTORA EJECUTIVA		
DEPENDENCIA:	OFICINAS CENTRALES DEL MTPS		

JUSTIFICACIÓN DE LA SOLICITUD

SERA UTILIZADO PARA LA SEGURIDAD DE INFORMACION, FILTRADO DE CONTENIDO Y REDES VIRTUALES, SEGURIDAD DE SITIOS PUBLICOS INSTITUCIONALES

EN TODOS LAS OFICINAS DEL MINISTERIO DE TRABAJO Y PREVISION SOCIAL POR UN AÑO.

ITEM	CÓDIGO	DETALLE			
		CANTIDAD	UNIDAD DE MEDIDA	OBRA, BIEN O SERVICIO SOLCIITADO	ESPECIFICACIONES TÉCNICAS (Material, color, medida, otras características requeridas. En caso de ser necesario adjuntar ducmento con esta información):
1	61104	19	UNIDAD	EQUIPO	Se anexan especificaciones técnicas para equipos de seguridad perimetral.

CONDICIONES:

VALOR ESTIMADO DE LA COMPRA:	$7,000.00
FORMA DE ENTREGA:	UNA SOLA ENTREGA
LUGAR DE ENTREGA:	OFICINA CENTRAL DEL MTPS
OTRAS CONDICIONES NECESARIAS	
OBSERVACIONES:	

PROPUESTA DE ADMINISTRADOR DE CONTRATO U ORDEN DE COMPRA

NOMBRE:	ING. FRANCISCO SANCHEZ
CARGO:	JEFE UNIDAD DE DESARROLLO TECNOLOGICO
DEPENDENCIA:	DIRECCION EJECUTIVA

ADQUISICIÓN DE EQUIPO DE SEGURIDAD PERIMETRAL			
SITIO PRINCIPAL Y SITIO REMOTO (SANTA ANA)			
CARACTERISTICA	DESCRIPCIÓN	CUMPLE	
Capacidad de usuarios	Hasta 1000		
Cantidad de equipos	Dos		
Configuración	Contingencia		
Almacenamiento	240 GB mínimo		
Consumo de energía	Fuente redundante		
Conexiones concurrentes	Mínimo 1 millón		
AV rendimiento	Mínimo 1.5 GBPS		
IPS rendimiento	Mínimo 2 GBPS		
Firewall rendimiento	Mínimo 4 GBPS		
Interfaces	Capacidad de ampliación		
Módulos de protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPsec.		
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.		
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.		
Seguridad web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS.		

Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, IPsec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.		
Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe permitir / restringir / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.		
IPS	1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.		
Protección de correo electrónico	Especificar		
Protección de redes inalámbricas	Especificar		

OTRAS			
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.		
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.		
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.		
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.		

ADQUISICIÓN DE EQUIPO DE SEGURIDAD PERIMETRAL			
OFICINAS REGIONALES (A EXCEPCION DE SANTA ANA) Y DEPARTAMENTALES			
CARACTERISTICA	**DESCRIPCIÓN**	**CUMPLE**	
Capacidad de usuarios	Hasta 100		
Cantidad de equipos	Doce		
Almacenamiento	64 GB mínimo		
Consumo de energía	Especificar		
Conexiones concurrentes	Mínimo 600 K		
AV rendimiento	Mínimo 500 MBPS		
IPS rendimiento	Mínimo 400 MBPS		
Firewall rendimiento	Mínimo 1.5 GBPS		
Interfaces	Capacidad de ampliación		
Módulos de protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPsec.		
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.		
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.		
Seguridad web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS.		

Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, IPsec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.		
Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe permitir / restringir / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.		
IPS	1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.		
Protección de correo electrónico	Especificar		
Protección de redes inalámbricas	Especificar		

OTRAS			
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.		
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.		
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.		
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.		

ADQUISICIÓN DE EQUIPO DE SEGURIDAD PERIMETRAL			
CENTROS DE RECREACIÓN Y ARCHIVO GENERAL			
CARACTERÍSTICA	DESCRIPCIÓN	CUMPLE	
Capacidad de usuarios	Hasta 15		
Cantidad de equipos	Cinco		
Almacenamiento	64 GB mínimo		
Consumo de energía	Especificar		
Conexiones concurrentes	Mínimo 600 K		
AV rendimiento	Mínimo 400 MBPS		
IPS rendimiento	Mínimo 300 MBPS		
Firewall rendimiento	Mínimo 900 MBPS		
Interfaces	Capacidad de ampliación		
Módulos de protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPsec.		
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.		
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.		
Seguridad web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS.		
Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, IPsec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.		

Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe permitir / restringir / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.		
IPS	1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code injection. 5. Bloqueo de actividades relacionadas a P2P e IM.		
Protección de correo electrónico	Especificar		
Protección de redes inalámbricas	Especificar		
OTRAS			
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.		
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.		

Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.		
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.		

MINISTERIO DE TRABAJO Y PREVISION SOCIAL
14 JUN. 2018
Blanca
RECIBIDO
2:32pm.

EL SALVADOR

San Salvador, 13 de Junio de 2018.

Señores
Jefe de la Unidad
Financiera
Presente.

En atención a los articulos 10 literal e) y 11 de la ley de Adquisiciones y Contrataciones de la Administracion Pública (LACAP), solicito su colaboracion en el sentido de verificar la asignacion presupuestaria para dar inicio a los procesos de compras siguiente:

Código del Proceso	DESCRIPCION DEL PROCESO	UNIDAD PRESUPUESTARIA LINEA DE TRABAJO (UNIDAD SOLICITANTE)	OBJETO ESPECIFICO GASTO PRESUPUESTARIO	MONTO
355	COMPRA DE 19 LICENCIAS , SERA UTILIZADO PARA LA SEGURIDAD DE INFORMACION, FILTRADO DE CONTENIDO Y REDES VIRTUALES, SEGURIDAD DE SITIOS PUBLICOS INSTITUCIONALES EN TODOS LAS OFICINAS DEL MTPS POR UN AÑO.	UNIDAD DE DESARROLLO TECNOLOGICO 01-01	61403	$58,000.00

MINISTERIO DE TRABAJO Y PREVISION SOCIAL
UNIDAD DE ADQUISICIONES Y CONTRATACIONES INSTITUCIONAL
UACI
San Salvador, C.A.

Licenciada Mayra Yessenia Palma Gutiérrez
Jefa UACI (Ad-Honorem)

UNIDAD FINANCIERA

Confirmación de asignación prespuestaria No. 355 Fecha: 14-06-18

UP: 01 LT- 02		OBJ. ESP.: 61403	Monto: $ 58.000.--
UP:	LT-	OBJ. ESP.:	Monto: $
UP:		OBJ. ESP.:	Monto: $
		TOTAL	US $ 58.000.--

Observaciones:

MINISTERIO DE TRABAJO Y PREVISION SOCIAL
U F I
UNIDAD FINANCIERA INSTITUCIONAL
SAN SALVADOR, C.A.

Lic. Luis Mario Flores Guillén,
Jefe UFI

GOBIERNO DE EL SALVADOR
UNÁMONOS PARA CRECER

MINISTERIO DE TRABAJO Y PREVISION SOCIAL
12 JUN. 2018 2:24 pm.
Blancca
RECIBIDO
UACI

No. de Requerimiento. 355

FECHA:	08 DE JUNIO DE 2018		
NOMBRE DEL SOLICITANTE:	ING. JUAN FRANCISCO SANCHEZ		
CARGO:	JEFE UNIDAD DE DESARROLLO TECNOLOGICO		
DEPENDENCIA:	DIRECCION EJECUTIVA	FIRMA DEL SOLICITANTE:	
NOMBRE DEL AUTORIZANTE:	LICDA. BEATRIZ DE PAUL	FIRMA DEL AUTORIZANTE	
CARGO:	DIRECTORA EJECUTIVA		
DEPENDENCIA:	OFICINAS CENTRALES DEL MTPS		

JUSTIFICACIÓN DE LA SOLICITUD

SERA UTILIZADO PARA LA SEGURIDAD DE INFORMACION, FILTRADO DE CONTENIDO Y REDES VIRTUALES, SEGURIDAD DE SITIOS PUBLICOS INSTITUCIONALES

EN TODOS LAS OFICINAS DEL MINISTERIO DE TRABAJO Y PREVISION SOCIAL POR UN AÑO.

ITEM	CÓDIGO	DETALLE			
		CANTIDAD	UNIDAD DE MEDIDA	OBRA, BIEN O SERVICIO SOLCIITADO	ESPECIFICACIONES TÉCNICAS (Material, color, medida, otras características requeridas. En caso de ser necesario adjuntar ducmento con esta información):
1	61403	19	UNIDAD	LICENCIAS	Se anexan especificaciones técnicas mínimas que deberán tener los equipos a los que se asocie licencias.

CONDICIONES:

VALOR ESTIMADO DE LA COMPRA:	$58,000.00
FORMA DE ENTREGA:	UNA SOLA ENTREGA
LUGAR DE ENTREGA:	OFICINA CENTRAL DEL MTPS
OTRAS CONDICIONES NECESARIAS	
OBSERVACIONES:	

PROPUESTA DE ADMINISTRADOR DE CONTRATO U ORDEN DE COMPRA

NOMBRE:	ING. FRANCISCO SANCHEZ
CARGO:	JEFE UNIDAD DE DESARROLLO TECNOLOGICO
DEPENDENCIA:	DIRECCION EJECUTIVA

CARACTERÍSTICAS DE EQUIPO AL QUE DEBERÁ ASOCIARSE LICENCIAMIENTO DE SEGURIDAD PERIMERAL			
SITIO PRINCIPAL Y SITIO REMOTO (SANTA ANA)			
CARACTERISTICA	DESCRIPCIÓN	CUMPLE	
Capacidad de usuarios	Hasta 1000		
Cantidad de equipos	Dos		
Configuración	Contingencia		
Almacenamiento	240 GB mínimo		
Consumo de energía	Fuente redundante		
Conexiones concurrentes	Mínimo 1 millón		
AV rendimiento	Mínimo 1.5 GBPS		
IPS rendimiento	Mínimo 2 GBPS		
Firewall rendimiento	Mínimo 4 GBPS		
Interfaces	Capacidad de ampliación		
Módulos de protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPsec.		
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.		
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.		
Seguridad web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS.		

Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, IPsec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.		
Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe permitir / restringir / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.		
IPS	1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.		
Protección de correo electrónico	Especificar		
Protección de redes inalámbricas	Especificar		

OTRAS			
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.		
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.		
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.		
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.		

CARACTERÍSTICAS DE EQUIPO AL QUE DEBERÁ ASOCIARSE LICENCIAMIENTO DE SEGURIDAD PERIMERAL			
OFICINAS REGIONALES (A EXCEPCIÓN DE SANTA ANA) Y DEPARTAMENTALES			
CARACTERISTICA	DESCRIPCIÓN	CUMPLE	
Capacidad de usuarios	Hasta 100		
Cantidad de equipos	Doce		
Almacenamiento	64 GB mínimo		
Consumo de energía	Especificar		
Conexiones concurrentes	Mínimo 600 K		
AV rendimiento	Mínimo 500 MBPS		
IPS rendimiento	Mínimo 400 MBPS		
Firewall rendimiento	Mínimo 1.5 GBPS		
Interfaces	Capacidad de ampliación		
Módulos de protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPsec.		
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.		
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.		
Seguridad web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS.		

Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, IPsec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.		
Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe permitir / restringir / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.		
IPS	1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.		
Protección de correo electrónico	Especificar		
Protección de redes inalámbricas	Especificar		

OTRAS			
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.		
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.		
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.		
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.		

RACTERÍSTICAS DE EQUIPO AL QUE DEBERÁ ASOCIARSE LICENCIAMIENTO DE SEGURIDAD PERIMER			
CENTROS DE RECREACIÓN Y ARCHIVO GENERAL			
CARACTERISTICA	DESCRIPCIÓN	CUMPLE	
Capacidad de usuarios	Hasta 15		
Cantidad de equipos	Cinco		
Almacenamiento	64 GB mínimo		
Consumo de energía	Especificar		
Conexiones concurrentes	Mínimo 600 K		
AV rendimiento	Mínimo 400 MBPS		
IPS rendimiento	Mínimo 300 MBPS		
Firewall rendimiento	Mínimo 900 MBPS		
Interfaces	Capacidad de ampliación		
Módulos de protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPsec.		
Análisis de correlación de amenazas	correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.		
VPN	en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.		
Seguridad web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS.		
Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, IPsec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.		

Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe permitir / restringir / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.		
IPS	1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.		
Protección de correo electrónico	Especificar		
Protección de redes inalámbricas	Especificar		
OTRAS			
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.		

Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.		
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.		
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.		

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL -MTPS-

GOBIERNO DE EL SALVADOR
UNÁMONOS PARA CRECER

Unidad de Desarrollo Tecnológico

MEMORANDUM

UDT/127/2018/ FS

Para: **Licda. Mayra Palma**
Jefa Ad Honorem

De: **Ing. Juan Francisco Sánchez**
Jefe Unidad de Desarrollo Tecnológico

Asunto: **Equipo y Licenciamiento de Seguridad Perimetral**

Fecha: **12 de junio de 2018**

Remito en anexo Requerimiento para la adquisición de:

1. **Licencias de Seguridad Perimetral**
2. **Equipo para alojar licenciamiento de Seguridad Perimetral**

Consideraciones:

La solución para resolver la necesidad de Seguridad Perimetral, es la adquisición de equipo con las especificaciones descritas en el primer requerimiento y el licenciamiento para garantizar la seguridad de información, sitios públicos institucionales, filtrado y contenido; y redes virtuales en el segundo. En consecuencia no hay opción a adjudicación parcial, el mismo proveedor deberá satisfacer ambos requerimientos.

Atentamente,

MINISTERIO DE TRABAJO Y PREVISION SOCIAL
12 JUN. 2018
RECIBIDO
UACI
2:20 p.m.

MINISTERIO DE TRABAJO Y PREVISION SOCIAL
12 JUN. 2018 2:45pm.
RECIBIDO

GOBIERNO DE EL SALVADOR
UNÁMONOS PARA CRECER

No. de Requerimiento. 356

FECHA:	08 DE JUNIO DE 2018		
NOMBRE DEL SOLICITANTE:	ING. JUAN FRANCISCO SANCHEZ		
CARGO:	JEFE UNIDAD DE DESARROLLO TECNOLOGICO		
DEPENDENCIA:	DIRECCION EJECUTIVA	FIRMA DEL SOLICITANTE:	
NOMBRE DEL AUTORIZANTE:	LICDA. BEATRIZ DE PAUL	FIRMA DEL AUTORIZANTE	
CARGO:	DIRECTORA EJECUTIVA		
DEPENDENCIA:	OFICINAS CENTRALES DEL MTPS		

JUSTIFICACIÓN DE LA SOLICITUD

SERA UTILIZADO PARA LA SEGURIDAD DE INFORMACION, FILTRADO DE CONTENIDO Y REDES VIRTUALES, SEGURIDAD DE SITIOS PUBLICOS INSTITUCIONALES

EN TODOS LAS OFICINAS DEL MINISTERIO DE TRABAJO Y PREVISION SOCIAL POR UN AÑO.

ITEM	CÓDIGO	DETALLE			
		CANTIDAD	UNIDAD DE MEDIDA	OBRA, BIEN O SERVICIO SOLCIITADO	ESPECIFICACIONES TÉCNICAS (Material, color, medida, otras características requeridas. En caso de ser necesario adjuntar ducmento con esta información):
1	61104	19	UNIDAD	EQUIPO	Se anexan especificaciones técnicas para equipos de seguridad perimetral.

CONDICIONES:

VALOR ESTIMADO DE LA COMPRA:	$7,000.00
FORMA DE ENTREGA:	UNA SOLA ENTREGA
LUGAR DE ENTREGA:	OFICINA CENTRAL DEL MTPS
OTRAS CONDICIONES NECESARIAS	
OBSERVACIONES:	

PROPUESTA DE ADMINISTRADOR DE CONTRATO U ORDEN DE COMPRA

NOMBRE:	ING. FRANCISCO SANCHEZ
CARGO:	JEFE UNIDAD DE DESARROLLO TECNOLOGICO
DEPENDENCIA:	DIRECCION EJECUTIVA

ADQUISICIÓN DE EQUIPO DE SEGURIDAD PERIMETRAL			
SITIO PRINCIPAL Y SITIO REMOTO (SANTA ANA)			
CARACTERISTICA	**DESCRIPCIÓN**	**CUMPLE**	
Capacidad de usuarios	Hasta 1000		
Cantidad de equipos	Dos		
Configuración	Contingencia		
Almacenamiento	240 GB mínimo		
Consumo de energía	Fuente redundante		
Conexiones concurrentes	Mínimo 1 millón		
AV rendimiento	Mínimo 1.5 GBPS		
IPS rendimiento	Mínimo 2 GBPS		
Firewall rendimiento	Mínimo 4 GBPS		
Interfaces	Capacidad de ampliación		
Módulos de protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPsec.		
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.		
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.		
Seguridad web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS.		

Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, IPsec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.		
Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe permitir / restringir / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.		
IPS	1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.		
Protección de correo electrónico	Especificar		
Protección de redes inalámbricas	Especificar		

OTRAS			
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.		
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.		
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.		
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.		

ADQUISICIÓN DE EQUIPO DE SEGURIDAD PERIMETRAL			
OFICINAS REGIONALES (A EXCEPCION DE SANTA ANA) Y DEPARTAMENTALES			
CARACTERISTICA	**DESCRIPCIÓN**	**CUMPLE**	
Capacidad de usuarios	Hasta 100		
Cantidad de equipos	Doce		
Almacenamiento	64 GB mínimo		
Consumo de energía	Especificar		
Conexiones concurrentes	Mínimo 600 K		
AV rendimiento	Mínimo 500 MBPS		
IPS rendimiento	Mínimo 400 MBPS		
Firewall rendimiento	Mínimo 1.5 GBPS		
Interfaces	Capacidad de ampliación		
Módulos de protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPsec.		
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.		
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.		
Seguridad web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS.		

Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, IPsec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.		
Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe permitir / restringir / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.		
IPS	1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.		
Protección de correo electrónico	Especificar		
Protección de redes inalámbricas	Especificar		

OTRAS			
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.		
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.		
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.		
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.		

ADQUISICIÓN DE EQUIPO DE SEGURIDAD PERIMETRAL			
CENTROS DE RECREACIÓN Y ARCHIVO GENERAL			
CARACTERISTICA	DESCRIPCIÓN	CUMPLE	
Capacidad de usuarios	Hasta 15		
Cantidad de equipos	Cinco		
Almacenamiento	64 GB mínimo		
Consumo de energía	Especificar		
Conexiones concurrentes	Mínimo 600 K		
AV rendimiento	Mínimo 400 MBPS		
IPS rendimiento	Mínimo 300 MBPS		
Firewall rendimiento	Mínimo 900 MBPS		
Interfaces	Capacidad de ampliación		
Módulos de protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPsec.		
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.		
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.		
Seguridad web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS.		
Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, IPsec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.		

Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe permitir / restringir / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.		
IPS	1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.		
Protección de correo electrónico	Especificar		
Protección de redes inalámbricas	Especificar		
OTRAS			
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.		
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.		

Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.		
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.		

10

MINISTERIO DE TRABAJO Y PREVISION SOCIAL
12 JUN. 2018 2:24pm.
Blanca
RECIBIDO

GOBIERNO DE EL SALVADOR
UNÁMONOS PARA CRECER

No. de Requerimiento. 355

FECHA:	08 DE JUNIO DE 2018		
NOMBRE DEL SOLICITANTE:	ING. JUAN FRANCISCO SANCHEZ		
CARGO:	JEFE UNIDAD DE DESARROLLO TECNOLOGICO		
DEPENDENCIA:	DIRECCION EJECUTIVA	FIRMA DEL SOLICITANTE:	
NOMBRE DEL AUTORIZANTE:	LICDA. BEATRIZ DE PAUL	FIRMA DEL AUTORIZANTE	
CARGO:	DIRECTORA EJECUTIVA		
DEPENDENCIA:	OFICINAS CENTRALES DEL MTPS		

JUSTIFICACIÓN DE LA SOLICITUD

SERA UTILIZADO PARA LA SEGURIDAD DE INFORMACION, FILTRADO DE CONTENIDO Y REDES VIRTUALES, SEGURIDAD DE SITIOS PUBLICOS INSTITUCIONALES

EN TODOS LAS OFICINAS DEL MINISTERIO DE TRABAJO Y PREVISION SOCIAL POR UN AÑO.

		DETALLE			
ITEM	CÓDIGO	CANTIDAD	UNIDAD DE MEDIDA	OBRA, BIEN O SERVICIO SOLCIITADO	ESPECIFICACIONES TÉCNICAS (Material, color, medida, otras características requeridas. En caso de ser necesario adjuntar ducmento con esta información):
1	61403	19	UNIDAD	LICENCIAS	Se anexan especificaciones técnicas mínimas que deberán tener los equipos a los que se asocie licencias.

CONDICIONES:

VALOR ESTIMADO DE LA COMPRA:	$58,000.00
FORMA DE ENTREGA:	UNA SOLA ENTREGA
LUGAR DE ENTREGA:	OFICINA CENTRAL DEL MTPS
OTRAS CONDICIONES NECESARIAS	
OBSERVACIONES:	

PROPUESTA DE ADMINISTRADOR DE CONTRATO U ORDEN DE COMPRA

NOMBRE:	ING. FRANCISCO SANCHEZ
CARGO:	JEFE UNIDAD DE DESARROLLO TECNOLOGICO
DEPENDENCIA:	DIRECCION EJECUTIVA

CARACTERÍSTICAS DE EQUIPO AL QUE DEBERÁ ASOCIARSE LICENCIAMIENTO DE SEGURIDAD PERIMERAL			
SITIO PRINCIPAL Y SITIO REMOTO (SANTA ANA)			
CARACTERISTICA	**DESCRIPCIÓN**	**CUMPLE**	
Capacidad de usuarios	Hasta 1000		
Cantidad de equipos	Dos		
Configuración	Contingencia		
Almacenamiento	240 GB mínimo		
Consumo de energía	Fuente redundante		
Conexiones concurrentes	Mínimo 1 millón		
AV rendimiento	Mínimo 1.5 GBPS		
IPS rendimiento	Mínimo 2 GBPS		
Firewall rendimiento	Mínimo 4 GBPS		
Interfaces	Capacidad de ampliación		
Módulos de protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPsec.		
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.		
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.		
Seguridad web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS.		

Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, IPsec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.		
Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe permitir / restringir / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.		
IPS	1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.		
Protección de correo electrónico	Especificar		
Protección de redes inalámbricas	Especificar		

OTRAS			
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.		
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.		
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.		
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.		

CARACTERÍSTICAS DE EQUIPO AL QUE DEBERÁ ASOCIARSE LICENCIAMIENTO DE SEGURIDAD PERIMERAL			
OFICINAS REGIONALES (A EXCEPCION DE SANTA ANA) Y DEPARTAMENTALES			
CARACTERISTICA	**DESCRIPCIÓN**	**CUMPLE**	
Capacidad de usuarios	Hasta 100		
Cantidad de equipos	Doce		
Almacenamiento	64 GB mínimo		
Consumo de energía	Especificar		
Conexiones concurrentes	Mínimo 600 K		
AV rendimiento	Mínimo 500 MBPS		
IPS rendimiento	Mínimo 400 MBPS		
Firewall rendimiento	Mínimo 1.5 GBPS		
Interfaces	Capacidad de ampliación		
Módulos de protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPsec.		
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.		
VPN	1. Soporte de túneles VPN en IPSec, VPN en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.		
Seguridad web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS.		

Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, IPsec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.		
Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe permitir / restringir / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.		
IPS	1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.		
Protección de correo electrónico	Especificar		
Protección de redes inalámbricas	Especificar		

OTRAS			
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.		
Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.		
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.		
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.		

RACTERÍSTICAS DE EQUIPO AL QUE DEBERÁ ASOCIARSE LICENCIAMIENTO DE SEGURIDAD PERIMER			
CENTROS DE RECREACIÓN Y ARCHIVO GENERAL			
CARACTERISTICA	DESCRIPCIÓN	CUMPLE	
Capacidad de usuarios	Hasta 15		
Cantidad de equipos	Cinco		
Almacenamiento	64 GB mínimo		
Consumo de energía	Especificar		
Conexiones concurrentes	Mínimo 600 K		
AV rendimiento	Mínimo 400 MBPS		
IPS rendimiento	Mínimo 300 MBPS		
Firewall rendimiento	Mínimo 900 MBPS		
Interfaces	Capacidad de ampliación		
Módulos de protección	1. Firewall 2. Protección de Red 3. Seguridad Web 4. Protección de Correo electrónico 5. Protección de redes inalámbricas 6. Protección para servidor Web 7. VPN punto a punto: SSL, IPsec.		
Análisis de correlación de amenazas	Correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales.		
VPN	[illegible] en SSL y VPN en PPTP. 2. VPN en modo, Site to Site, Site to Client, y Hub and Spoke. 3. Soporte de inscripción DES, 3DES, y AES. 4. Autenticación de certificados IKE. 5. El sistema debe tener capacidad de crear certificados: Locales, CA y CRL.		
Seguridad web	1. Base de datos de filtrado de URL por medio de la categorización de sitios. 2. Control de aplicaciones como Skype, Bittorent, Youtube, etc. 3. Análisis de Malware. 4. Filtrado de contenido activo: extensiones de archivos, Flash. 5. Detección de spyware. 6. Configuración de perfiles de navegación. 7. Autenticación compatible con LDAP y RADIUS.		
Protección de red	1. Administración web protegido por contraseña personalizable. 2. Enrutamiento de tráfico de red. 3. Balanceo de enlaces. 4. Prevención de Intrusos. 5. Protección contra DOS. VPN punto a punto: SSL, IPsec. 6. Compatibilidad de sistema de autenticación: RADIUS, LDAP. 7. Generación de reportes automáticos enviados por medio de correo electrónico.		

Filtrado de contenido	1. Sistema de filtrado de contenido Web, para http, y https. 2. Debe permitir / restringir / acceso a categorías tales como: Business, Hacking, no productivas, Spyware y Malware, controversiales, finanzas, etc. 3. Que permita bloqueo de URL, Keyword o Frase. 4. Lista de Excepción de URL 5. Bloqueo de Java, Applet, Cookies y ActiveX 6. Permita filtrado de forma transparente o por autenticación mediante agente, active directory (SSO) o navegador. 7. Control de aplicaciones.		
IPS	1. Que el UTM soporte motor de IPS para la protección contra ataques. 2. Protección contra DDoS, ICMP Flood, UDP Flood, TCP SYN Flood, Smurf, IP Spoofing, Port Scan, Exploit, Backdoors. 3. Protección contra vulnerabilidades en protocolos: DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, TFTP, NNTP, NETBIOS. 4. Protección contra vulnerabilidades de software en: IIS, ORACLE, MS SQL, MySQL, Cross-site Scripting, code Injection. 5. Bloqueo de actividades relacionadas a P2P e IM.		
Protección de correo electrónico	Especificar		
Protección de redes inalámbricas	Especificar		
OTRAS			
Soporte técnico	1. Instalará y configurará equipo para ponerlo en operación. 2. Dará respuesta por fallas en equipo en un máximo de 3 horas posterior al reporte. 3. Reparará los equipos con fallas que imposibiliten o degraden su funcionamiento o en su defecto prestarán un equipo características similares mientras se hace efectivo el reemplazo total del equipo en garantía. 4. Brindará soporte 24 horas del día, 7 días a la semana, sin costo adicional. 5. Demostrará que cuenta con al menos 3 técnicos de staff certificados en la solución ofertada que residan en el país, no subcontratado, para atender los requerimientos de soporte técnico.		

Garantía	Reemplazará en concepto de garantía las veces que sea necesario que equipos que estén: defectuosos, en mal estado o que por sus características de hardware imposibiliten la actualización a una nueva versión sin costo adicional. Deberá definir en su oferta, el mecanismo y las condiciones a seguir para hacer efectivo el reemplazo en garantía del equipo.		
Experiencia	1. Deberá presentar 3 cartas de referencia del sector gobierno en servicios de equipos de similares características o superiores que deberán demostrar que posee al menos 3 años de experiencia con el producto ofertado. 2. Deberá presentar carta del fabricante que compruebe que es distribuidor autorizado.		
Capacitación	Brindará capacitación en la configuración y administración de equipo al menos a 4 técnicos del MTPS.		