



Federación el 31 de agosto de 1981, el cual se reformó por Decreto publicado en el mismo Diario el 23 de agosto de 2012, y con Registro Federal de Contribuyentes número INE-810901-CP4.

- II. De conformidad al artículo 2 del Decreto de fecha 23 de agosto de 2012, tiene por objeto promover y realizar acciones para organizar e impartir la educación para adultos, a través de la prestación de los servicios de alfabetización, educación primaria y secundaria, la formación para el trabajo y las demás que determinen las disposiciones jurídicas y los programas aplicables, apoyándose en la participación y la solidaridad social.
- III. En los términos señalados en la fracción VII del artículo 22 de la Ley Federal de las Entidades Paraestatales, la Directora General de este organismo público descentralizado de la Administración Pública Federal tiene, entre otras facultades, la de otorgar poderes a nombre de **"EL INEA"**, así como nombrar representantes.
- IV. El Apoderado Legal José Muñoz Gómez, cuenta con las facultades necesarias para formalizar el presente pedido, lo cual se acredita con el testimonio del Poder General, número 175,436 de fecha 01 de julio de 2021, otorgado ante la fe del Notario Público número 42 de la Ciudad de México, Lic. Salvador Godínez Viera, que le confiere entre otras facultades, poderes generales para actos de administración, mismos que no le han sido modificadas ni disminuidas a la presente fecha.
- V. Para los efectos del presente pedido, señala como su domicilio legal el ubicado en la Calle Francisco Márquez número 160, colonia Condesa, alcaldía Cuauhtémoc, Código Postal 06140, Ciudad de México.

"EL PROVEEDOR" declara por conducto de su Administrador Único, que:

- I. Es una persona moral, legalmente constituida conforme a las leyes mexicanas, lo que acredita a través de la Escritura Pública número 21,399 de fecha trece de enero del dos mil cinco, otorgada ante la fe del Licenciado Jorge A. D. Hernández Arias, Titular de la Notaría Pública número ciento cincuenta y dos del Distrito Federal, ahora Ciudad de México, misma que ha sufrido diversas modificaciones, cuenta con el Registro Federal de Contribuyentes ASI0501142C2.
- II. Cuenta con las facultades suficientes para contratar y obligarse a través de su representada, como se acredita con la Póliza número 10,713 de fecha cuatro de diciembre del dos mil dieciocho, otorgada ante la fe del Corredor Público número 74, del Distrito Federal, ahora Ciudad de México, mismas que no le han sido modificadas ni disminuidas a la presente fecha.
- III. Tiene por objeto social, la prestación de servicios en los ramos de la informática, de la computación y del procesamiento de datos; así como en la elaboración, diseño y mantenimiento de sistemas conexos a las actividades antes mencionadas; así como la compra, venta, comisión, importación, exportación, distribución, consignación y en general el ejercicio del comercio en cualquier forma con el equipo, maquinaria, sistemas, partes, accesorios y refacciones de toda clase de equipos de cómputo, entre otros.
- IV. Conoce plenamente el contenido de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, declarando bajo protesta de decir verdad que no se encuentra en ninguno de los supuestos que señalan los artículos 50 y 60 de este ordenamiento.
- V. Cuenta con la experiencia, capacidad jurídica, material y económica, así como con la organización y los elementos técnicos y humanos necesarios para cumplir con las obligaciones derivadas de este pedido.
- VI. Manifiesta bajo protesta de decir verdad, que **"EL INEA"** no es su único cliente.

Francisco Márquez 160, Col. Condesa, CP. 06140, Alcaldía Cuauhtémoc, CDMX.
Tel: (55) 5241 2700 www.gob.mx/inea





- VII. Para los efectos del presente pedido, señala como su domicilio fiscal el ubicado en Calle Nayarit, número interior 101, exterior 85, colonia Roma Sur, Alcaldía Cuauhtémoc, código postal 06760, Ciudad de México.

Declaran "LAS PARTES" que:

- I. Las actividades que realicen de manera conjunta no involucren relaciones de carácter administrativo, laboral o cualquier otra que implique subordinación o que impida el libre desarrollo de sus objetivos.
- II. El presente pedido constituye el acuerdo entre **"LAS PARTES"** en relación con su objeto y deja sin efecto cualquier otra negociación, obligaciones o comunicación entre éstas ya sea verbal o escrita, efectuada con anterioridad en que se firme el mismo.
- III. Se reconocen recíprocamente la calidad con que comparecen y están de acuerdo con los antecedentes y las declaraciones, por lo que manifiestan su conformidad para suscribir el presente instrumento.
- IV. Se deberá considerar que de conformidad con el artículo 54 bis, de la Ley y 102 del reglamento, se procederá a la terminación anticipada, cuando concurren razones de interés general o cuando por causas justificadas se extinga la necesidad de requerir el servicio o se determine la nulidad total o parcial de los actos que dieron origen al pedido con motivo de la resolución de una inconformidad emitida por la Secretaría de la Función Pública, o de así ser necesario conforme a las disposiciones de contratación de la Cabeza de Sector, Secretaría de Educación Pública o el Instituto Nacional Para la Educación de los Adultos.

Expuesto lo anterior, **"LAS PARTES"** otorgan las siguientes:

CLÁUSULAS

Primera. - Objeto.

"EL PROVEEDOR" se obliga con **"EL INEA"** en la **"Contratación del licenciamiento de software para el año 2021"**.

La contratación del servicio antes referido se desarrollará de acuerdo con la programación que determine **"EL INEA"** a través del administrador y/o supervisor del pedido, y que se enuncia con mayor amplitud en el Anexo Único que se integra por el Anexo Técnico de la Convocatoria, Propuesta Técnica y Propuesta Económica aceptadas y que determinaron el fallo de la Invitación a cuando menos Tres Personas. **"LAS PARTES"** convienen en agregar éste Anexo Único al pedido como parte íntegra del mismo.

Segunda. - Monto.

"LAS PARTES" acuerdan que el monto total por la prestación del servicio objeto del presente pedido, es por la cantidad de **\$2'651,495.52 (Dos millones seiscientos cincuenta y un mil cuatrocientos noventa y cinco pesos 52/100 M.N.)**, que incluye el Impuesto al Valor Agregado, que se cubrirá contra entrega de los servicios contratados como se detalla en el Anexo Único, conforme a lo siguiente:





PARTIDA	CONCEPTO	CANTIDAD DE LICENCIAS	IMPORTE POR PARTIDA O CONCEPTO (INCLUYE I.V.A.)
3	Renovación de licencia por 1 año de Firewall FORTINET modelo FORTIGATE 600C (2 licencias) y FG100D (33 licencias, para Oficinas Centrales, Institutos Estatales y Unidades de Operación. Incluye para los FORTIGATE, servicio de FORTICARE 8X5 y FORTIGUARD UTM que incluye devolución y remplazo por fallas de hardware.	35	\$2,273,600.00
	Renovación de licencia por 1 año de software para reporte de análisis de seguridad FORTIANALYZER 200F.	2	\$222,019.36
	Renovación de licencia por 1 año de software para la administración y control de los dispositivos de seguridad de un FORTIMANAGER modelo 300D la renovación incluye la actualización tecnológica del appliance donde se renueva la licencia del producto.	1	\$155,876.16
TOTAL DE LOS CONCEPTOS DE LA PARTIDA 3			\$2,651,495.52

Así mismo convienen **"LAS PARTES"** que por ninguna circunstancia el precio pactado variará durante la vigencia del presente pedido.

Si **"EL PROVEEDOR"** recibiera pagos en exceso deberá reintegrar las cantidades entregadas más los intereses que se calcularán conforme a una tasa que será igual a la establecida en el Código Fiscal de la Federación como si se tratara del supuesto de prórroga para el pago de créditos fiscales. Los cargos se calcularán sobre las cantidades pagadas en exceso en cada caso y se computará por días naturales, desde la fecha del pago hasta que se ponga a disposición de **"EL INEA"**.

"EL INEA" se obliga a realizar el pago como se detalla en el Anexo Único, por los servicios realizados conforme a las características y especificaciones contratadas.

Tercera. - Obligaciones de "EL PROVEEDOR".

Prestar los servicios objeto de este pedido, de acuerdo con las normas, tiempos, requerimientos, instrucciones, programas, especificaciones y datos que le indique **"EL INEA"** a través del administrador del pedido y/o del supervisor del mismo y en su caso, ajustarse a las indicaciones que éstos le otorguen por escrito.

Aceptar, de ser el caso, que **"EL INEA"** efectúe las retenciones, deducciones o descuentos previstos en las disposiciones fiscales aplicables.

Entregar al administrador y/o al supervisor del pedido, en caso de que se lo soliciten, un informe del avance de la prestación del servicio.

Cuarta. - Condiciones de pago.

"EL INEA" realizará el pago a través depósito bancario, mediante una transferencia electrónica de recursos a la cuenta bancaria señalada por **"EL PROVEEDOR"**, por el importe del servicio proporcionado. **"EL PROVEEDOR"** deberá presentar un Comprobante (s) Fiscal (es) Digital (es) por internet (CFDI'S) en el cual especificará el importe del pedido.

Francisco Márquez 160, Col. Condesa, CP. 06140, Alcaldía Cuauhtémoc, CDMX.
Tel: (55) 5241 2700 www.gob.mx/inea





El pago se realizará, conforme a las características y especificaciones contratadas establecidas en el Anexo Único, en un plazo que no podrá exceder de veinte días naturales contados a partir de la entrega del (los) Comprobante (s) Fiscal (es) respectivo (s), previa prestación de los servicios en los términos establecidos en el pedido. El plazo señalado no incluye aclaraciones o demoras atribuibles a **"EL PROVEEDOR"** o carencia de documentos comprobatorios para la emisión del pago.

Los Comprobantes Fiscales Digitales deberán cumplir con los requisitos fiscales vigentes, indicando el número de pedido, la descripción completa de los bienes adquiridos, el costo unitario, el desglose del Impuesto al Valor Agregado, el importe total y los datos de **"EL PROVEEDOR"**.

El Titular del Departamento de Control Presupuestal validará los Comprobantes Fiscales Digitales y será el responsable de devolver a **"EL PROVEEDOR"** los comprobantes que tengan errores, deficiencias o falta de requisitos dentro de los dos días hábiles siguientes a la fecha de su recepción, indicando por escrito a **"EL PROVEEDOR"** las deficiencias que deberá corregir.

Las obligaciones fiscales vigentes que resulten con motivo del presente pedido serán cumplidas puntualmente por cada una de **"LAS PARTES"** en lo que les corresponda.

Quinta. - Constancia de cumplimiento.

Una vez cumplidas las obligaciones por parte de **"EL PROVEEDOR"** conforme a las características y especificaciones contratadas, se procederá a extender la constancia de cumplimiento de obligaciones por parte del área requirente para poder efectuarse el último pago.

Sexta. - Finiquito.

"EL PROVEEDOR" otorgará, antes de efectuarse el último pago, el finiquito más amplio que en derecho proceda en el que expresamente manifieste que **"EL INEA"** cumplió con todas y cada una de las obligaciones contraídas, sin reservarse acción ni derecho alguno por ejercitar con posterioridad.

Séptima. - Comprobación, supervisión y verificación.

"EL INEA", por conducto del administrador y supervisor, será el área responsable de verificar, comprobar y supervisar que se cumplan con los derechos y obligaciones establecidas en el presente pedido.

Las funciones como Administrador del pedido son: Es el responsable de interactuar con el supervisor para dar seguimiento y verificar que el servicio cuente con las especificaciones y actividades solicitadas.

Las funciones como Supervisor del pedido son: Es el responsable de interactuar con el administrador y el proveedor para dar seguimiento y verificar que el servicio cumpla con las especificaciones, actividades y entregas puntuales del servicio.

El administrador del pedido será Gustavo Raúl Santillán Velasco, Subdirector de Recursos Tecnológicos y el supervisor del pedido será Roberto Ramírez Guzmán, Jefe del Departamento de Soporte Técnico, Centro de Datos y Comunicaciones, o quién en un futuro les sustituyan.

Octava. - Vigencia.

La vigencia del pedido será de 30 días naturales contados a partir de la firma del mismo.

La vigencia del uso de las licencias será de un año, del 01 de noviembre de 2021 al 31 de octubre de 2022

La entrega del licenciamiento deberá realizarse a más tardar el 29 de octubre de 2021.





Estas vigencias son voluntarias para **"EL INEA"** y forzosas para **"EL PROVEEDOR"**, por lo que el primero podrá dar por terminado anticipadamente el presente pedido cuando concurren razones de interés general, o por causas justificadas se extinga la necesidad del objeto requerido.

Novena. - Defectos y vicios ocultos.

"EL PROVEEDOR" se obliga ante el **"EL INEA"** a responder de los defectos y vicios ocultos en la calidad de los servicios, así como de cualquier responsabilidad en que hubiera incurrido, en los términos señalados en el presente pedido y en la legislación aplicable.

Décima. - Confidencialidad.

"LAS PARTES", acuerdan en tratar como clasificada toda la información intercambiada o acordada con motivo del presente instrumento, excepto aquella que deba considerarse pública según lo dispuesto por los artículos 113 y 116 por la Ley General de Transparencia y Acceso a la Información Pública, los artículos 97, 110 y 113 de la Ley Federal de Transparencia y Acceso a la Información Pública, los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y demás disposiciones aplicables, no se podrá divulgar salvo que sea autorizado por escrito y de forma expresa por el área competente de **"EL INEA"**.

Toda la información impresa, audiovisual, en archivo magnético o que pueda almacenarse por algún otro medio técnico o científico que los adelantos de la ciencia lo permitan, que se proporcionen entre sí **"LAS PARTES"** para el debido cumplimiento del objeto del presente pedido, se considera estrictamente reservada y se prohíbe su divulgación a terceros con cualquier carácter, hasta por el tiempo de doce años, excepto en los casos y condiciones que establezca la ley.

Décima primera. - Suspensión.

"EL INEA" podrá suspender los efectos de este pedido, por razones de austeridad presupuestal o de orden público. En este caso, **"EL INEA"** se compromete a notificar por escrito a **"EL PROVEEDOR"** en el domicilio señalado en su declaración VII, con tres días de anticipación y, por lo tanto, **"EL INEA"** cubrirá el o los pagos por los servicios recibidos, conforme a las características y especificaciones requeridas, procediendo a la suscripción del finiquito correspondiente.

Décima segunda. - Terminación anticipada.

"EL INEA" podrá dar por terminado anticipadamente sin su responsabilidad el presente pedido, cuando por causas justificadas se extinga la necesidad de requerir los servicios recibidos, originalmente contratados, o se determine la nulidad total o parcial de los actos que dieron origen al pedido.

La terminación anticipada del pedido se sustentará mediante dictamen que precise las razones o las causas justificadas que le den origen a la misma en términos del artículo 54 bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y 102 de su Reglamento y demás normatividad aplicable, dando aviso a **"EL PROVEEDOR"** con tres días naturales de anticipación.

Décima tercera. - Rescisión.

"EL INEA" podrá rescindir administrativamente el presente pedido cuando **"EL PROVEEDOR"** incurra en incumplimiento de sus obligaciones, en términos del artículo 54 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, artículo 98 de su Reglamento y las disposiciones de la Ley Federal de Procedimiento Administrativo.

"EL PROVEEDOR" no podrá ceder en forma parcial o total a favor de cualquier otra persona, los derechos y obligaciones que se deriven del presente pedido, en caso que llegase a suceder será causa de rescisión.





Décima cuarta. - Procedimiento de rescisión.

Si se actualiza la hipótesis de incumplimiento mencionada en la cláusula anterior, **"EL INEA"** comunicará por escrito a **"EL PROVEEDOR"** el probable incumplimiento en que haya incurrido, para que en un término de tres días hábiles exponga lo que a su derecho convenga y aporte en su caso, las pruebas que estime pertinentes para desvirtuar el posible incumplimiento.

Transcurrido el término a que se refiere el párrafo anterior, se resolverá considerando los argumentos y pruebas que **"EL PROVEEDOR"** hubiere hecho valer.

La determinación final de dar o no por rescindido el pedido deberá ser fundada y motivada, la cual deberá ser notificada a **"EL PROVEEDOR"** dentro de los quince días hábiles siguientes al término señalado en el párrafo primero de esta cláusula, y cuando se rescinda el pedido se formulará el finiquito correspondiente, a efecto de hacer constar los pagos que deba efectuar **"EL INEA"** por concepto de los servicios recibidos, hasta el momento de la rescisión.

Décima quinta. - Legislación aplicable.

"EL INEA" y **"EL PROVEEDOR"** convienen en someterse a las disposiciones que señala la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, su Reglamento y demás legislación aplicable.

Décima sexta. - Pena convencional.

Se procederá a calcular penas convencionales en apego con lo estipulado por el artículo 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y conforme a lo establecido en el Anexo Único. **"EL INEA"** notificará a **"EL PROVEEDOR"** dicha pena, para que éste realice el pago de la penalización mediante efectivo, cheque de caja o cheque certificado a favor de **"EL INEA"** en el domicilio establecido en la declaración V de **"EL INEA"**.

Así mismo se aplicarán penas deductivas en el caso de cumplimiento deficiente o parcial en la prestación del servicio, de acuerdo a lo estipulado por el artículo 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y conforme a la tabla de deductivas establecidas en el Anexo Único. **"EL INEA"** notificará a **"EL PROVEEDOR"** dicha pena, para que éste realice el pago de la penalización mediante efectivo, cheque certificado o cheque de caja a favor de **"EL INEA"** en el domicilio establecido en la declaración V de **"EL INEA"**.

El cálculo de las penas convencionales y deductivas es responsabilidad del área requirente a través del Administrador y Supervisor del pedido, así como de cualquier incumplimiento y deberá avisar en tiempo y en forma a la Unidad de Administración y Finanzas.

"EL PROVEEDOR" queda obligado ante **"EL INEA"**, de responder por la calidad de los servicios, así como de cualquier otra responsabilidad en que incurra en los términos del presente pedido y su Anexo Único.

Décima séptima. - Garantía de cumplimiento de pedido.

"EL PROVEEDOR", para asegurar el debido cumplimiento de este pedido, se obliga a entregar a **"EL INEA"**, dentro de los diez días naturales siguientes a la fecha de su firma, preferentemente fianza que tendrá carácter de divisible, expedida por compañía legalmente autorizada para ello, a favor de **"EL INEA"**, por un importe equivalente al 10% del monto total del costo del servicio, sin considerar el Impuesto al Valor Agregado.

Para su cancelación, será necesaria la solicitud por escrito de **"EL PROVEEDOR"** y con autorización expresa de **"EL INEA"**.

En el caso de que **"EL INEA"** convenga con **"EL PROVEEDOR"** un incremento en la cantidad de la prestación de los servicios, solicitará a éste la entrega de la modificación respectiva de la garantía de cumplimiento por dicho incremento, lo cual deberá estipularse en el convenio modificatorio respectivo.

Francisco Márquez 160, Col. Condesa, CP. 06140, Alcaldía Cuauhtémoc, CDMX.
Tel: (55) 5241 2700 www.gob.mx/inea





La aplicación de la garantía de cumplimiento se hará efectiva cuando el pedido presente uno de los siguientes casos:

- a) Cuando **"EL PROVEEDOR"** no proporcione los bienes adquiridos, motivo de esta contratación.
- b) Cuando **"EL PROVEEDOR"** no cumpla con alguna de las obligaciones estipuladas en el pedido.

Décima octava. - Caso fortuito o fuerza mayor.

Ninguna de **"LAS PARTES"** será responsable de cualquier retraso o incumplimiento de este pedido que resulte directa o indirectamente de caso fortuito o fuerza mayor, la que de invocarse deberá acreditarse fehacientemente.

Décima novena. - Relación contractual.

La relación existente entre **"EL INEA"** y **"EL PROVEEDOR"** es de carácter estrictamente administrativa, por lo que **"EL PROVEEDOR"** es el único responsable de las obligaciones de carácter civil, laboral y de cualquier otra naturaleza para con las personas con quien se auxilie en el cumplimiento del presente pedido, por lo que expresamente reconoce y acepta lo que dispone el artículo 13 de la Ley Federal del Trabajo, por ser el único y exclusivo patrón de los elementos que comisione, quienes no tienen ni tendrán vínculo laboral de alguna clase con **"EL INEA"** y por lo tanto, en ningún momento se considera a **"EL INEA"** como intermediario.

Por lo anterior **"EL PROVEEDOR"** se obliga a dejar a salvo a **"EL INEA"** de cualquier reclamación o acción instaurada en su contra, o de cualquier juicio o procedimiento que se instaure con motivo del presente pedido, así como a pagar en su caso los daños y perjuicios que se le causen.

Vigésima. - Responsabilidad.

"EL PROVEEDOR" exenta a **"EL INEA"** de toda responsabilidad legal que pudiera surgir, derivada como consecuencia directa o indirecta de la prestación de los servicios.

Vigésima primera. - Datos Personales.

Para efectos de lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y las disposiciones que de ella emanen, **"EL PROVEEDOR"** reconoce y acepta expresamente que la forma y términos en que cualquier información que se considere como datos personales serán protegidos y tratados de conformidad con lo que se establece y se regula en la Ley mencionada y en el "Aviso de Privacidad" correspondiente.

Vigésima segunda. - De la información a los órganos de control.

"EL INEA" y **"EL PROVEEDOR"** se obligan a entregar a la Secretaría de la Función Pública y/o al Órgano Interno de Control en **"EL INEA"**, en el momento que se les requiera, toda la información relacionada con el presente pedido.

Vigésima tercera. - De integridad y combate a la corrupción.

"EL PROVEEDOR" se obliga a que durante la ejecución del pedido ni él ni sus socios, directivos o empleados, por sí o por interpósita persona: a) solicitarán o promoverán la realización, el otorgamiento o la contratación indebidos de los servicios objeto del pedido; b) promoverán ante las personas que detentan la calidad de servidores públicos la gestión, la tramitación o la resolución ilícita de negocios públicos relacionados con la administración del pedido, y, c) ofrecerán, prometerán o darán dinero o cualquier otra dádiva, a los servidores públicos encargados de la administración del pedido.

"EL INEA" y **"EL PROVEEDOR"** acuerdan que durante la vigencia del pedido se comprometen a actuar con estricto apego a las anteriores reglas de conducta para combatir el cohecho, el tráfico de influencia y el uso indebido de atribuciones y facultades.

Francisco Márquez 160, Col. Condesa, CP. 06140, Alcaldía Cuauhtémoc, CDMX.
Tel: (55) 5241 2700 www.gob.mx/inea





Vigésima cuarta. - Patentes, marcas y derechos de autor.

"EL PROVEEDOR" asumirá la responsabilidad total para el caso que se infrinjan patentes o marcas, o violen derechos de autor, tanto en el ámbito nacional como internacional con respecto de la adquisición de los bienes objeto de este pedido, por lo que de presentarse alguna reclamación a **"EL INEA"** con ese motivo, durante la vigencia del pedido o posterior a ella, **"EL PROVEEDOR"** conviene desde ahora en pagar cualquier importe que de ello se derive y sacar a salvo y en paz de tales reclamaciones a **"EL INEA"** a más tardar a los quince días naturales a partir de que sea notificado de ello este último.

Vigésima quinta. - Del combate a las prácticas monopólicas absolutas y relativas.

"EL PROVEEDOR" se obliga a que, durante la vigencia del pedido, se abstendrán de celebrar acuerdos, por sí o a través de interpósita persona, entre sí o con otros agentes económicos, que tengan por finalidad o efecto, en relación con los bienes objeto de este pedido:

- 1) Fijar, elevar, concertar o manipular el precio de dichos bienes;
- 2) Restringir o limitar la prestación de los bienes;
- 3) Dividir, distribuir, asignar o imponer porciones o segmentos del mercado gubernamental;
- 4) Establecer, concertar o coordinar posturas o la abstención en los procedimientos de contratación realizados conforme a lo dispuesto en el pedido, o
- 5) Intercambiar información cuyo propósito o efecto corresponda a los referidos en los numerales anteriores.

"EL PROVEEDOR" se abstendrá de incurrir en prácticas monopólicas relativas, como están definidas en los artículos 54 a 56 de la Ley Federal de Competencia Económica.

Será causa de rescisión del pedido, el que **"EL PROVEEDOR"**, por sí o por interpósita persona, incurra en alguna o algunas de las conductas tipificadas como: a) delito contra la economía pública, conforme a lo dispuesto en el artículo 254 bis del Código Penal Federal; b) prácticas monopólicas absolutas, según lo estatuido en el artículo 53 de la Ley Federal de Competencia Económica; o c) prácticas monopólicas relativas, en términos de los artículos 52 a 56 de esta última ley. Para la actualización de la causal de rescisión será necesario que la conducta típica y antijurídica se haya producido en relación con los servicios que son objeto de este pedido y que la responsabilidad de **"EL PROVEEDOR"** de que se trate, por sí o por interpósita persona, haya sido determinada en resolución firme, dictada por autoridad competente.

Vigésima sexta. - Del procedimiento de conciliación.

En cualquier momento **"EL PROVEEDOR"** y **"EL INEA"** podrán presentar ante la Secretaría de la Función Pública, solicitud de conciliación, por desavenencias derivadas del cumplimiento del pedido, cuyo procedimiento se substanciará conforme a lo dispuesto en el título sexto "De la solución de las controversias", capítulo segundo, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, así como de su reglamento.

En el supuesto de que **"LAS PARTES"** lleguen a un acuerdo durante la conciliación, el convenio respectivo obligará a las mismas, y su cumplimiento podrá ser demandado por la vía judicial; en caso contrario, podrán optar por cualquier vía de solución a su controversia.

Vigésima séptima. - Modificaciones al pedido.

El presente pedido podrá ser modificado o adicionado por voluntad de **"LAS PARTES"**, siempre y cuando medie causa justificada o superviniente. Siempre que el monto total de las modificaciones no rebase en conjunto, el 20% del monto o cantidad de los conceptos y volúmenes establecidos originalmente en el mismo y el precio sea igual al pactado originalmente; así como que se cuente con la disponibilidad presupuestal correspondiente.





Vigésima octava. – Asuntos no previstos.

"LAS PARTES" convienen que en caso de discrepancia entre la convocatoria de Invitación a cuando menos Tres personas Nacional Electrónica IA-011MDA001-E89-2021 y el modelo de pedido, prevalecerá lo establecido en la Convocatoria de Invitación a cuando menos Tres Personas Nacional Electrónica IA-011MDA001-E89-2021.

Vigésima novena. - Cesión de derechos.

"EL PROVEEDOR" no podrá ceder en forma parcial o total a favor de cualquier otra persona, los derechos y obligaciones que se deriven del presente pedido, con excepción de los derechos de cobro, en cuyo caso deberá contar con el consentimiento previo por escrito de **"EL INEA"**, a través de la Unidad de Administración y Finanzas.

Los derechos de cobro, podrán cederse cuando **"EL PROVEEDOR"** opte por adherirse a las cadenas productivas de **"EL INEA"** en la página web <https://cadenasnafin.com.mx>, de conformidad con las disposiciones emitidas por la Secretaría de Hacienda y Crédito Público publicadas en el Diario Oficial de la Federación el 28 de febrero de 2007.

Trigésima. - Ausencia de vicios.

"LAS PARTES" manifiestan que a la firma del presente pedido no media dolo, violencia, mala fe o cualquier otro vicio de consentimiento que pudiera invalidar.

Trigésima primera. - Encabezados y definiciones.

Los encabezados y definiciones señalados en las cláusulas del presente pedido se han utilizado únicamente para una rápida localización e identificación del contenido de la cláusula que se trate, por lo que en ningún momento se entenderá que dichos encabezados y definiciones limitan o alteran el acuerdo de **"LAS PARTES"** contenido en ellas.

Trigésima segunda.- Jurisdicción.

Para la interpretación y cumplimiento de este pedido, **"LAS PARTES"** se someterán expresamente a la jurisdicción y competencia de los tribunales federales con residencia en la Ciudad de México, renunciando a cualquier otro fuero que pudiera corresponderles en razón de sus respectivos domicilios presentes o futuros.

Leído el presente pedido y enteradas **"LAS PARTES"** del valor, alcance y fuerza legal de sus cláusulas, lo firman al calce y al margen, constante de 11 fojas, por duplicado para constancia y validez, en la Ciudad de México, a los veinticinco días del mes de octubre del año dos mil veintiuno, conservando un ejemplar **"EL INEA"** y uno **"EL PROVEEDOR"**.

Por **"EL INEA"**



José Muñoz Gómez
Apoderado Legal

Por **"EL PROVEEDOR"**



Fernando Escobar Olivares
Administrador Único de
"Abasi Sistemas Integrales, S.A. de C.V."





Asistido por

Gustavo Raúl Santillán Velasco
Subdirector de Recursos Tecnológicos y
Administrador del Pedido

El presente instrumento jurídico se firma con fundamento en el numeral 1.6.4, punto 10 del Manual General de Organización del INEA publicado en el D.O.F. de fecha 31 de marzo de 2021.

Roberto Ramírez Guzmán
Jefe del Departamento de Soporte Técnico, Centro
de Datos y Comunicaciones,
Supervisor del Pedido

El presente instrumento jurídico se firma con fundamento en el numeral 1.6.4.3 del Manual General de Organización del INEA publicado en el D.O.F. de fecha 31 de marzo de 2021.

Las firmas que aparecen en esta hoja, forman parte del pedido de prestación de servicios de fecha **25 de octubre de 2021**, celebrado entre este Instituto Nacional para la Educación de los Adultos y **Abasi Sistemas Integrales, S.A. de C.V.**, cuyo objeto es la **"Contratación del licenciamiento de software para el año 2021"**.





EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA



**INSTITUTO
NACIONAL PARA
LA EDUCACIÓN
DE LOS ADULTOS**

ANEXO ÚNICO

**(Anexo Técnico de la
Convocatoria, Propuesta
Técnica y Propuesta
Económica)**





ANEXO 1 (Anexo Técnico)

Contratación del licenciamiento de software para el año 2021

UNIDAD DE ADMINISTRACIÓN Y FINANZAS SUBDIRECCIÓN DE RECURSOS TECNOLÓGICOS			
ÁREA REQUINIENTE	Subdirección de Recursos Tecnológicos		
NOMBRE DEL TITULAR DEL ÁREA REQUINIENTE Y RESPONSABLE DE ADMINISTRAR Y SUPERVISAR EL CUMPLIMIENTO DEL CONTRATO	Gustavo Raúl Santillán Velasco Subdirector de Recursos Tecnológicos Titular del Área Requiriente y Administrador del Contrato. Roberto Ramírez Guzmán Jefe del Departamento de Soporte Técnico, Centro de Datos y Comunicaciones Supervisor del Contrato.		
% PENALIZACIÓN	Con fundamento en lo dispuesto por el artículo 53 de la Ley en la materia y el 95 y 96 de su reglamento, el Instituto aplicará penas convencionales al proveedor del servicio, de la siguiente manera: Pena convencional: se aplicará en el caso de incumplimiento en el tiempo de entrega del licenciamiento, el titular de la Subdirección de Recursos Tecnológicos procederá a calcular la pena convencional al 1% por cada día natural de atraso sobre el costo unitario del licenciamiento no entregado, la que no excederá del monto de la garantía de cumplimiento. Dicha pena tendrá como límite la aplicación de un equivalente al 5% considerando que, el porcentaje de la fianza es del 10% del monto total del contrato y/o pedido antes de	% DE DEDUCCIÓN	Penalización por deductivas: En el caso de que el licenciamiento una vez instalado y en operación deje de funcionar conforme a las características técnicas establecidas en el anexo técnico, el titular de la Subdirección de Recursos Tecnológicos lo notificará al proveedor adjudicado para que, en un término no mayor a 5 días naturales posteriores a la notificación, el licenciamiento funcione conforme a las características técnicas establecidas en el anexo técnico, si el proveedor excede este periodo se obliga a pagar como pena deductiva el equivalente al 1% sobre el costo unitario del licenciamiento notificado por cada día natural de atraso contado a partir de la notificación, dicha pena





	I.V.A., no podrá exceder del monto de la garantía de cumplimiento del contrato y/o pedido, una vez alcanzado el 5% el INEA podrá iniciar el procedimiento de rescisión del instrumento jurídico respectivo y se hará efectiva la garantía de cumplimiento del mismo, el pago de las penalizaciones deberá hacerse a favor del INEA mediante cheque certificado, de caja o dinero en efectivo en el departamento de tesorería. Asimismo, la Subdirección de Recursos Tecnológicos notificará por escrito al proveedor de dicha pena, para que éste realice el pago de la penalización mediante efectivo, cheque de caja o cheque certificado a favor de INEA, se girará copia de este escrito a la Unidad de Administración y Finanzas a fin de que tomen conocimiento de la misma.		tendrá como límite la aplicación de un equivalente al 5% de deductivas considerando que el porcentaje de la fianza es del 10% del monto total del instrumento jurídico, una vez alcanzado el 5% el INEA podrá iniciar el procedimiento de rescisión del instrumento jurídico respectivo y se hará efectiva la garantía de cumplimiento del mismo, el pago de las penalizaciones deberá hacerse a favor del INEA mediante cheque certificado de caja o dinero en efectivo en el departamento de tesorería. Asimismo, la Subdirección de Recursos Tecnológicos notificará por escrito al proveedor de dicha pena, para que éste realice el pago de la penalización mediante efectivo, cheque de caja o cheque certificado a favor de INEA, se girará copia de este escrito a la Unidad de Administración y Finanzas a fin de que tomen conocimiento de la misma.
TIPO DE GARANTÍA	DIVISIBLE ☒	INDIVISIBLE ☐	LÍMITE DE INCUMPLIMIENTO DE LA FIANZA 5 %
OTRAS GARANTÍAS QUE SE DEBERÁN CONSIDERAR, INDICAR EL O LOS TIPOS DE GARANTÍA O	10 % de garantía de cumplimiento	PARTIDA PRESUPUESTAL	32701





RESPONSABILIDAD CIVIL SEÑALANDO VIGENCIA			
PERIODO DE GARANTÍA DEL BIEN O SERVICIO	1 año	PLAZO PARA LA NOTIFICACIÓN Y REPOSICIÓN DEL BIEN O SERVICIO	No aplica
REQUIERE PRUEBAS	No	REQUIERE MUESTRA	No
MÉTODO PARA EJECUTAR LA PRUEBA Y RESULTADO MÍNIMO	No aplica		
PRESENTACIÓN Y CONDICIONES DE LA MUESTRA.	No aplica		
REQUIERE ANTICIPO	No	PORCENTAJE DE ANTICIPO: No aplica	
ORIGEN DE LOS BIENES	No aplica		
NORMAS QUE APLICAN	No aplica		
MÉTODO DE EVALUACIÓN (sólo aplica en Licitación o Invitación)	PUNTOS Y PORCENTAJES	COSTO BENEFICIO	BINARIO X
MODALIDAD DE CONTRATO	ABIERTO ☐	CERRADO ☒	
ES UNA CONTRATACIÓN PLURIANUAL	SI ☐ NO ☒		





VIGENCIA PEDIDO CONTRATO.	DEL Y/O	Vigencia del Contrato y/o Pedido: será de 30 días naturales contados a partir de la firma del mismo. Vigencia del licenciamiento: la vigencia del uso de las licencias será de un año, del 01 de noviembre de 2021 al 31 de octubre de 2022.
LUGAR Y CONDICIONES DE LA PRESTACIÓN DEL SERVICIO.		La entrega del licenciamiento deberá realizarse a más tardar el 29 de octubre de 2021. La aceptación del licenciamiento lo realizará la Subdirección de Recursos Tecnológicos apoyada en el documento o acceso a herramientas de Tecnologías de la Información que respalde el licenciamiento.
MECANISMOS DE COMPROBACIÓN, SUPERVISIÓN Y VERIFICACIÓN DE LO ESTABLECIDO EN PEDIDOS Y/O CONTRATOS		El INEA a través del administrador y supervisor del contrato realizarán la comprobación y verificación en cualquier tiempo y lugar del licenciamiento el cual debe: • Estar operación. • Estar vigente.
ENTREGABLES		Documento o acceso a herramientas de Tecnologías de la Información que respalde el licenciamiento
FORMA Y PLAZO DE PAGO		El pago se realizará a los 20 días naturales posteriores a la entrega de la factura, previa entrega del documento o acceso a herramientas de Tecnologías de la Información que respalde el licenciamiento el cual será validado y aceptado por parte de la Subdirección de Recursos Tecnológicos.
NOMBRE Y CARGO DEL ADMINISTRADOR Y DEL SUPERVISOR DEL INSTRUMENTO JURÍDICO		Gustavo Raúl Santillán Velasco Subdirector de Recursos Tecnológicos Titular del Área Requiriente y Administrador del Contrato Roberto Ramírez Guzmán Jefe del Departamento de Soporte Técnico, Centro de Datos y Comunicaciones Supervisor del Contrato.
FORMA Y TÉRMINOS EN QUE SE REALIZARÁ LA VERIFICACIÓN DE LAS ESPECIFICACIONES Y LA ACEPTACIÓN		La aceptación de los servicios se notificará mediante oficio de liberación para el pago del licenciamiento.

[Firma]



[Firma]



DE LOS BIENES O SERVICIOS

DESCRIPCIÓN Y ESPECIFICACIONES DEL SERVICIO DE FORMA DETALLADA

a) Requerimientos funcionales

Licenciamiento que incluya la colección completa de aplicaciones para escritorio y dispositivos móviles de Adobe, desde las más básicas como Photoshop CC hasta herramientas de nueva generación como Adobe XD CC, con acceso a las plantillas incorporadas para poner en marcha proyectos y tutoriales paso a paso para trabajar con las aplicaciones de adobe.

Licenciamiento de antivirus que se utiliza para detectar y eliminar virus y programas que puedan perjudicar un sistema; permite una gestión centralizada a través de una consola que proporcione una visibilidad inmediata y el control de las defensas de seguridad y que unifique el control de todas las herramientas de protección antimalware y antispaam en tiempo real: bloqueo de virus, troyanos, gusanos, adware, spyware y otros programas potencialmente no deseados y ataques selectivos de suplantación de identidad (phishing), seguridad proactiva, advirtiendo a los usuarios sobre sitios web maliciosos, permite el bloqueo o autorización del acceso a sitios web desde la consola.

Licenciamiento de firewall para proteger los equipos conectados en red contra accesos no deseados de intrusos que puedan hacer perder o sustraer información de dichos equipos o denegar servicios que se encuentran disponibles en la red incluye administración y control de los dispositivos de seguridad, de las configuraciones, cambios y respaldos de políticas de todos los equipos, así como poder hacer las actualizaciones necesarias de manera programada y silenciosa; obtener reportes y alarmas de los equipos para poder tomar medidas de control y administración de los recursos.

Licenciamiento de software de escritorio con el cual se puede crear archivos PDF y exportarlos a formato Word, Excel, Power Point, entre otros, con capacidad para editar texto e imágenes directamente en el archivo PDF así como convertir documentos escaneados en archivos PDF editables permitiendo realizar búsquedas en los mismos, también permite la creación, rellenado, firmas y envío de formularios así como la integración con soluciones como Microsoft Office 365.

El licenciamiento contiene un conjunto de aplicaciones de análisis de negocios que permite analizar datos y compartir información ya sea en la nube o localmente. Los paneles ofrecen a los usuarios una vista de 360 grados con sus métricas más importantes en un mismo lugar. La información se actualiza en tiempo real y está disponible para que los usuarios puedan explorar los datos subyacentes del panel mediante herramientas intuitivas que permiten obtener respuestas fácilmente. La creación de un panel es una sencilla operación gracias a los miles de conexiones a conocidas aplicaciones empresariales, que se completan con paneles pregenerados para ayudarle a ponerse en marcha rápidamente. Asimismo, puede acceder datos e informes que se actualizan automáticamente con los cambios que se realizan en los datos.

DESCRIPCIÓN DEL LICENCIAMIENTO

PARTIDA	CONCEPTO	UNIDAD	CANTIDAD
1	Renovación de Creative Cloud licenciamiento por un año.	Licencia	5
2	Renovación de licencia de software antivirus e-Scan Corporate Edition (con soporte para redes híbridas), para Oficinas Centrales, Institutos Estatales, Unidades de	Licencia	11,654





	Operación, Coordinaciones de Zona y Plazas Comunitarias. licenciamiento por un año.		
3	Renovación de licencia por 1 año de Firewall FORTINET modelo FORTIGATE 600C (2 licencias) y FG100D (33 licencias), para Oficinas Centrales, Institutos Estatales y Unidades de Operación. Incluye para los FORTIGATE, servicio de FORTICARE 8x5 y FORTIGUARD UTM que incluye devolución y remplazo por fallas de hardware.	Licencia	35
	Renovación de licencia por 1 año de software para reporte de análisis de seguridad FORTIANALYZER 200F	Licencia	2
	Renovación de licencia por 1 año de software para la administración y control de los dispositivos de seguridad de un FORTIMANAGER modelo 300D la renovación incluye la actualización tecnológica del appliance donde se renueva la licencia del producto.	Licencia	1
4	Renovación de licencia de Acrobat Pro DC por un año.	Licencia	15
5	Renovación de licencia Power BI Pro por un año.	Licencia	40

b) Requerimientos no funcionales

La vigencia del instrumento jurídico será de 30 días naturales, contados a partir de la firma del mismo.

la vigencia del uso de las licencias será de un año, del 01 de noviembre de 2021 al 31 de octubre de 2022.

Se deberá garantizar los licenciamientos comprometiéndose a subsanar cualquier defecto de la elaboración y/o vicios ocultos por un periodo de 1 año (365 días), el esquema de licenciamiento a utilizar será educativo.

Se considera conveniente renovar el licenciamiento ya que se cuenta con infraestructura en operación con el software solicitado, en caso de adquirir otra nueva conllevaría a costos adicionales en: adquisición de hardware, capacitación en el uso del nuevo software, distribución e instalación del nuevo software, periodo de estabilización del software debido a la curva de aprendizaje que conlleva cualquier tecnología, asimismo se cuenta con una plataforma instalada donde reside información, diseño de páginas web, contenidos del portal web, entre otros, que operan con el licenciamiento solicitado por lo cual de adquirir otro software se tendría que realizar migración de aplicativos y de ser el caso reingeniería de plataforma lo cual no permitiría tener disponible de manera continua la información que requieren las áreas usuarias de este licenciamiento.

c) Niveles de servicio.

El licenciamiento solicitado se mantendrá funcionando de forma eficiente para que el personal del Instituto Nacional para la Educación de los Adultos pueda utilizarlo en el momento en que así lo necesiten.

- El tiempo de solución será como máximo de 5 días naturales contados a partir de la notificación por parte de la Subdirección de Recursos Tecnológicos al proveedor adjudicado.
- Si el tiempo de solución excede el tiempo establecido se aplicará la pena deductiva correspondiente.

d) Términos y condiciones de entrega y de aceptación.

2





La aceptación del servicio lo realizará la Subdirección de Recursos Tecnológicos apoyada en el documento o acceso a herramientas de Tecnologías de la Información que respalde el licenciamiento, lo cual quedará documentado en un "Acta de recepción de licenciamiento de software", en la cual se registraran las ligas de acceso al licenciamiento o el documento que acredite el licenciamiento respectivo.

Plazos y forma de pago:

El pago se realizará a los 20 días naturales posteriores a la entrega de la factura, previa entrega del documento o acceso a herramientas de Tecnologías de la Información que respalde el licenciamiento el cual será validado y aceptado por parte de la Subdirección de Recursos Tecnológicos.

e) Escrito de confidencialidad

El licitante en su propuesta técnica deberá entregar un escrito donde manifieste que:

"El proveedor", se obliga a utilizar toda la información que le proporcione "el INEA" únicamente para el cumplimiento del objeto de este contrato y a no reproducirlos ni divulgarlos para otros fines, por ningún medio y bajo ninguna circunstancia, acatando en todo momento, las disposiciones de la ley federal de protección de datos personales en posesión de los particulares.

f) La forma en que se llevará a cabo la supervisión del servicio contratado.

Administración, supervisión y vigilancia.

El administrador del instrumento jurídico será el Titular de la Subdirección de Recursos Tecnológicos y el Supervisor será el Titular del Departamento de Soporte Técnico, Centro de Datos y Comunicaciones.

Funciones del administrador: responsable de interactuar con el supervisor para dar seguimiento y verificar que el servicio cuente con las especificaciones y actividades solicitadas.

Funciones del supervisor: responsable de interactuar con el administrador y el proveedor, para dar seguimiento y verificar que el servicio cumpla con las especificaciones, actividades y entregas puntuales del servicio.

ROBERTO RAMÍREZ GUZMÁN JEFE DEL DEPARTAMENTO DE SOPORTE TÉCNICO, CENTRO DE DATOS Y COMUNICACIONES ELABORACIÓN	GUSTAVO RAÚL SANTILLÁN VELASCO SUBDIRECTOR DE RECURSOS TECNOLÓGICOS AUTORIZACIÓN.
NOMBRE Y FIRMA DEL SERVIDOR PÚBLICO QUE ELABORÓ Y AUTORIZÓ	



X

Ciudad de México, Cuauhtémoc, octubre 18 del 2021

Instituto Nacional para la Educación de los Adultos
Presente

000001

Invitación a cuando menos Tres Personas Nacional Electrónica
No. IA-011MDA001-E89-2021
Relativa a la "Contratación para el licenciamiento de software para el año 2021"

Nombre del licitante: **ABASI Servicios Integrales, S.A. de C.V.**
 email: **fescobar@abasi.com.mx y ggarcia@abasi.com.mx**

Formato A-1
Proposición Técnica

Partida	Concepto	Unidad	Cantidad
1	Renovación de Creative Cloud licenciamiento por un año.	Licencia	5
2	Renovación de licencia de software antivirus e.Scan Corporate Edition (con soporte para redes híbridas), para Oficinas Centrales, Institutos Estatales, Unidades de operación, Coordinaciones de Zona y Plazas Comunitarias. Licenciamiento por un año.	Licencia	11,654
3	Renovación de licencia por 1 año, de firewall FORTINET Modelo FORTIGATE 600C (2 licencias) y FG100D (33 licencias), para oficinas centrales, delegaciones e institutos estatales. Incluir para los FORTIGATE, servicio de FORTICARE 8x5 y FORTIGUARD UTM. Incluye devolución y remplazo por fallas de hardware. Nuestra propuesta incluye la renovación tecnológica a Fortigate 600E (2 licencias) y Fortigate 80F hardware plus (33 licencias) con servicio Forticare 24x7 por un año.	Licencia	35
	Renovación de licencia por 1 año de software para reporte de análisis de seguridad FORTIANALYZER 200F	Licencia	2
	Renovación de licencia por 1 año contado de software para la administración y control de los dispositivos de seguridad de un FORTIMANAGER modelo 300D. La renovación incluye la actualización tecnológica del appliance donde se renueva la licencia del producto. Nuestra propuesta incluye la renovación tecnológica a Fortigate 300F, con Forticare 24x7 por un año.	Licencia	1
4	Renovación de licencia de Acrobat Pro DC por un año	Licencia	15
5	Renovación de licencia PowerBI Pro por un año	Licencia	40

Vigencia de la propuesta desde su presentación y hasta la conclusión del procedimiento.

Atentamente,


Lic. Fernando Escobar Olivares
 Administrador Único

Sucursal Culiacán:
 Av. Insurgentes Sur No. 500 - A
 Col. Centro Sinaloa.
 80129 Culiacán de Rosales
 Tel. (667) 992-3367 y (667) 992-2468

Nayarit No. 85 - 101, Col. Roma Sur
 06760 Cuauhtémoc, Ciudad de México
 RFC ASI0501142C2 www.abasi.com.mx
 Tel. (55) 5219-5702 y (55) 5219-5703

Ciudad de México, Cuauhtémoc, octubre 18 del 2021

Instituto Nacional para la Educación de los Adultos
Presente

000002

Invitación a cuando menos Tres Personas Nacional Electrónica
No. IA-011MDA001-E89-2021
Relativa a la "Contratación para el licenciamiento de software para el año 2021"

Nombre del licitante: **ABASI Servicios Integrales, S.A. de C.V.**
email: **fescobar@abasi.com.mx y ggarcia@abasi.com.mx**

ANEXO TÉCNICO

LICENCIAMIENTO DE SOFTWARE PARA EL AÑO 2021

a) Requerimientos funcionales

Licenciamiento que incluye la colección completa de aplicaciones para escritorio y dispositivos móviles de Adobe, desde las más básicas como Photoshop CC hasta herramientas de nueva generación como Adobe XD CC, con acceso a las plantillas incorporadas para poner en marcha proyectos y tutoriales paso a paso para trabajar con las aplicaciones de adobe.

Licenciamiento de antivirus que se utiliza para detectar y eliminar virus y programas que puedan perjudicar un sistema; permite una gestión centralizada a través de una consola que proporcione una visibilidad inmediata y el control de las defensas de seguridad y que unifique el control de todas las herramientas de protección antimalware y antispam en tiempo real: bloqueo de virus, troyanos, gusanos, adware, spyware y otros programas potencialmente no deseados y ataques selectivos de suplantación de identidad (phishing), seguridad proactiva, advirtiendo a los usuarios sobre sitios web maliciosos, permite el bloqueo o autorización del acceso a sitios web desde la consola.

Licenciamiento de firewall para proteger los equipos conectados en red contra accesos no deseados de intrusos que puedan hacer perder o sustraer información de dichos equipos o denegar servicios que se encuentran disponibles en la red incluye administración y control de los dispositivos de seguridad, de las configuraciones, cambios y respaldos de políticas de todos los equipos, así como poder hacer las actualizaciones necesarias de manera programada y silenciosa; obtener reportes y alarmas de los equipos para poder tomar medidas de control y administración de los recursos.

Licenciamiento de software de escritorio con el cual se puede crear archivos PDF y exportarlos a formato Word, Excel, Power Point, entre otros, con capacidad para editar texto e imágenes directamente en el archivo PDF así como convertir documentos escaneados en archivos PDF editables permitiendo realizar búsquedas en los mismos, también permite la creación, rellenado, firmas y envío de formularios así como la integración con soluciones como Microsoft Office 365.

El licenciamiento contiene un conjunto de aplicaciones de análisis de negocios que permite analizar datos y compartir información ya sea en la nube o localmente. Los paneles ofrecen a los usuarios una vista de 360 grados con sus métricas más importantes en un mismo lugar. La información se actualiza en tiempo real y está disponible para que los usuarios pueden explorar los datos subyacentes del panel mediante herramientas intuitivas que permiten obtener respuestas fácilmente. La creación de un panel es una sencilla operación gracias a los miles de conexiones a conocidas aplicaciones empresariales, que se completan con paneles pregenerados para ayudarle a ponerse en marcha rápidamente. Asimismo, pueden acceder datos e informes que se actualizan automáticamente con los cambios que se realizan en los datos.

Ciudad de México, Cuauhtémoc, octubre 18 del 2021

Instituto Nacional para la Educación de los Adultos
Presente

000003

Invitación a cuando menos Tres Personas Nacional Electrónica
No. IA-011MDA001-E89-2021
Relativa a la "Contratación para el licenciamiento de software para el año 2021"

Nombre del licitante: **ABASI Servicios Integrales, S.A. de C.V.**
 email: **fescobar@abasi.com.mx y ggarcia@abasi.com.mx**

DESCRIPCIÓN DEL LICENCIAMIENTO

Partida	Concepto	Unidad	Cantidad
1	Renovación de Creative Cloud licenciamiento por un año.	Licencia	5
2	Renovación de licencia de software antivirus e.Scan Corporate Edition (con soporte para redes híbridas), para Oficinas Centrales, Institutos Estatales, Unidades de operación, Coordinaciones de Zona y Plazas Comunitarias. Licenciamiento por un año.	Licencia	11,654
3	Renovación de licencia por 1 año, de firewall FORTINET Modelo FORTIGATE 600C (2 licencias) y FG100D (33 licencias), para oficinas centrales, delegaciones e institutos estatales. Incluir para los FORTIGATE, servicio de FORTICARE 8x5 y FORTIGUARD UTM Incluye devolución y remplazo por fallas de hardware. Nuestra propuesta incluye la renovación tecnológica a Fortigate 600E (2 licencias) y Fortigate 80F hardware plus (33 licencias) con servicio Forticare 24x7 por un año.	Licencia	35
	Renovación de licencia por 1 año de software para reporte de análisis de seguridad FORTIANALYZER 200F	Licencia	2
	Renovación de licencia por 1 año contado de software para la administración y control de los dispositivos de seguridad de un FORTIMANAGER modelo 300D. La renovación incluye la actualización tecnológica del appliance donde se renueva la licencia del producto. Nuestra propuesta incluye la renovación tecnológica a Fortigate 300F, con Forticare 24x7 por un año.	Licencia	1
4	Renovación de licencia de Acrobat Pro DC por un año	Licencia	15
5	Renovación de licencia PowerBI Pro por un año	Licencia	40

b) Requerimientos no funcionales

La vigencia del instrumento jurídico será de 30 días naturales, contados a partir de la firma del mismo.

La vigencia del uso de las licencias será de un año, del 01 de noviembre de 2021 al 31 de octubre de 2022.

Se garantizarán los licenciamientos comprometiéndose a subsanar cualquier defecto de la elaboración y/o vicios ocultos por un periodo de 1 año (365 días), el esquema de licenciamiento a utilizar será educativo.

Se considera conveniente renovar el licenciamiento ya que se cuenta con infraestructura en operación con el software solicitado, en caso de adquirir otra nueva conllevaría a costos adicionales en: adquisición de hardware, capacitación en el uso del nuevo software, distribución e instalación del nuevo software, periodo de estabilización del software debido a la curva de aprendizaje que conlleva cualquier tecnología, asimismo se cuenta con una plataforma instalada donde reside información, diseño de páginas web, contenidos del portal web, entre otros, que operan con el licenciamiento solicitado por lo cual de adquirir otro software se tendría que realizar migración de aplicativos y de ser el caso reingeniería de plataforma lo cual no permitiría tener disponible de manera continua la información que requieren las áreas usuarias de este licenciamiento.

c) Niveles de servicio.

Sucursal Culiacán:
 Av. Insurgentes Sur No. 500 - A
 Col. Centro Sinaloa
 80129 Culiacán de Rosales
 Tel. (667) 992-3367 y (667) 992-2468

Nayarit No. 85 - 101, Col. Roma Sur
 06760 Cuauhtémoc, Ciudad de México
 RFC ASI0501142C2 www.abasi.com.mx
 Tel. (55) 5219-5702 y (55) 5219-5703

Ciudad de México, Cuauhtémoc, octubre 18 del 2021

Instituto Nacional para la Educación de los Adultos
Presente

000004

Invitación a cuando menos Tres Personas Nacional Electrónica
No. IA-011MDA001-E89-2021
Relativa a la "Contratación para el licenciamiento de software para el año 2021"

Nombre del licitante: **ABASI Servicios Integrales, S.A. de C.V.**
email: **fescobar@abasi.com.mx y ggarcia@abasi.com.mx**

El licenciamiento solicitado se mantendrá funcionando de forma eficiente para que el personal del Instituto Nacional para la Educación de los Adultos pueda utilizarlo en el momento en que así lo necesiten.

- El tiempo de solución será como máximo de 5 días naturales contados a partir de la notificación por parte de la Subdirección de Recursos Tecnológicos al proveedor adjudicado.
- Si el tiempo de solución excede el tiempo establecido se aplicará la pena deductiva correspondiente.

d) Términos y condiciones de entrega y de aceptación.

La aceptación del servicio lo realizará la Subdirección Técnica apoyada en el documento o acceso a herramientas de Tecnologías de la Información que respalde el licenciamiento, lo cual quedará documentado en un "Acta de recepción de licenciamiento de software", en la cual se registrarán las ligas de acceso al licenciamiento o el documento que acredite el licenciamiento respectivo.

Plazos y forma de pago:

El pago se realizará a los 20 días naturales posteriores a la entrega de la factura, previa entrega del documento o acceso a herramientas de Tecnologías de la Información que respalde el licenciamiento el cual será validado y aceptado por parte de Subdirección de Recursos Tecnológicos.

e) Escrito de confidencialidad

El licitante en su propuesta técnica deberá entregar un escrito donde manifieste que:

"El proveedor", se obliga a utilizar toda la información que le proporcione "el INEA" únicamente para el cumplimiento del objeto de este contrato y a no reproducirlos ni divulgarlos para otros fines, por ningún medio y bajo ninguna circunstancia, acatando en todo momento, las disposiciones de la ley federal de protección de datos personales en posesión de los particulares.

f) La forma en que se llevará a cabo la supervisión del servicio contratado.

Administración, supervisión y vigilancia.

El administrador del instrumento jurídico será el Titular de la Subdirección de Recursos Tecnológicos y el Supervisor será el Titular del Departamento de Soporte Técnico, Centro de Datos y Comunicaciones.

Funciones del administrador: responsable de interactuar con el supervisor para dar seguimiento y verificar que el servicio cuente con las especificaciones y actividades solicitadas.

Funciones del supervisor: responsable de interactuar con el administrador y el proveedor, para dar seguimiento y verificar que el servicio cumpla con las especificaciones, actividades y entregas puntuales del servicio.

Sucursal Culiacán:
Av. Insurgentes Sur No. 500 - A
Col. Centro Sinaloa.
80129 Culiacán de Rosales
Tel. (667) 992-3367 y (667) 992-2468

Nayarit No. 85 - 101, Col. Roma Sur
06760 Cuauhtémoc, Ciudad de México
RFC ASI0501142C2 www.abasi.com.mx
Tel. (55) 5219-5702 y (55) 5219-5703

Ciudad de México, Cuauhtémoc, octubre 18 del 2021

Instituto Nacional para la Educación de los Adultos
Presente

000005

Invitación a cuando menos Tres Personas Nacional Electrónica
No. IA-011MDA001-E89-2021
Relativa a la "Contratación para el licenciamiento de software para el año 2021"

Nombre del licitante: **ABASI Servicios Integrales, S.A. de C.V.**
email: **fescobar@abasi.com.mx y ggarcia@abasi.com.mx**

Escrito de confidencialidad

Fernando Escobar Olivares, en mi carácter de administrador único de la empresa denominada **ABASI Servicios Integrales, S.A. de C.V.**, manifiesto que:

En caso de resultar adjudicados en el presente procedimiento, mi representada se obliga a utilizar toda la información que le proporcione "el INEA" únicamente para el cumplimiento del objeto de este contrato y a no reproducirlos ni divulgarlos para otros fines, por ningún medio y bajo ninguna circunstancia, acatando en todo momento, las disposiciones de la Ley Federal de protección de datos personales en posesión de los particulares.

Atentamente,



Lic. Fernando Escobar Olivares
Administrador Único

Ciudad de México, Cuauhtémoc, octubre 18 del 2021

Instituto Nacional para la Educación de los Adultos
Presente

000006

Invitación a cuando menos Tres Personas Nacional Electrónica
No. IA-011MDA001-E89-2021
Relativa a la "Contratación para el licenciamiento de software para el año 2021"

Nombre del licitante: **ABASI Servicios Integrales, S.A. de C.V.**
email: **fescobar@abasi.com.mx y ggarcia@abasi.com.mx**

Inciso b)
Obligaciones fiscales y laborales

Me refiero al procedimiento de Invitación a cuando menos Tres Personas Nacional Electrónica indicado al rubro en el que mi representada, **ABASI Servicios Integrales, S.A. de C.V.**, participa a través de la proposición que se contiene en el presente sobre.

Sobre el particular, manifiesto que, en caso de resultar adjudicado, me comprometo a cumplir con todas las obligaciones fiscales y laborales conforme a las Leyes correspondientes, así como al cumplimiento de nuestra obligaciones en materia laboral y de prestaciones sociales del 100% del personal que contrate para la prestación de los servicios objeto de la presente convocatoria.

Atentamente,



Lic. Fernando Escobar Olivares
Administrador Único
Sucursal Culiacán:
Av. Insurgentes Sur No. 500 - A
Col. Centro Sinaloa,
80129 Culiacán de Rosales
Tel. (667) 992-3367 y (667) 992-2468
Nayarit No. 85 - 101, Col. Roma Sur
06760 Cuauhtémoc, Ciudad de México
RFC ASI0501142C2 www.abasi.com.mx
Tel. (55) 5219-5702 y (55) 5219-5703


Ciudad de México, Cuauhtémoc, octubre 18 del 2021

Instituto Nacional para la Educación de los Adultos
Presente

000007

Invitación a cuando menos Tres Personas Nacional Electrónica
No. IA-011MDA001-E89-2021
Relativa a la "Contratación para el licenciamiento de software para el año 2021"

Nombre del licitante: **ABASI Servicios Integrales, S.A. de C.V.**
email: **fescobar@abasi.com.mx y ggarcia@abasi.com.mx**

Inciso c)
Formato 3
Garantía contra defectos y/o vicios ocultos

Nombre del licitante: **ABASI Servicios Integrales, S.A. de C.V.**
Email: **fescobar@abasi.com.mx y ggarcia@abasi.com.mx**

Me refiero al procedimiento de Invitación a cuando menos Tres Personas Nacional Electrónica indicada al rubro en el que mi representada, **ABASI Servicios Integrales, S.A. de C.V.**, participa a través de la proposición que se contiene en el presente sobre.

Sobre el particular, manifiesto que, en caso de resultar adjudicado, me comprometo a garantizar los servicios contra defectos y/o vicios ocultos, durante los siguientes 12 (doce) meses, posteriores al servicio.

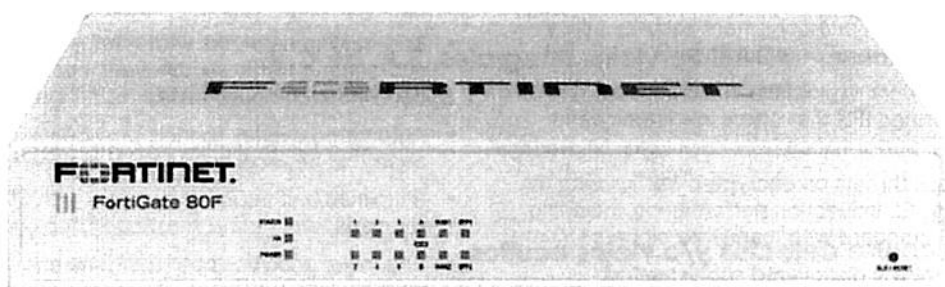
Atentamente,


Lic. Fernando Escobar Olivares
Administrador Único

FortiGate® FortiWiFi 80F Series

FG-80F, FG-80F-POE, FG-80F-Bypass, FG-81F, FG-81F-POE, FWF-81F-2R-POE, and FWF-80F/81F-2R

Next Generation Firewall
Secure SD-WAN



The FortiGate FortiWiFi 80F series provides an application-centric, scalable, and secure SD-WAN solution in a compact, fanless, desktop form factor for enterprise branch offices and mid-sized businesses with integrated WiFi-6 (802.11ax). Protects against cyber threats with system-on-a-chip acceleration and industry-leading secure SD-WAN in a simple, affordable, and easy to deploy solution. Fortinet's Security-Driven Networking approach provides tight integration of the network to the new generation of security.

Security

- Identifies thousands of applications inside network traffic for deep inspection and granular policy enforcement
- Protects against malware, exploits, and malicious websites in both encrypted and non-encrypted traffic
- Prevent and detect against known and unknown attacks using continuous threat intelligence from AI-powered FortiGuard Labs security services

Performance

- Delivers industry's best threat protection performance and ultra-low latency using purpose-built security processor (SPU) technology
- Provides industry-leading performance and protection for SSL encrypted traffic

Certification

- Independently tested and validated for best-in-class security effectiveness and performance
- Received unparalleled third-party certifications from NSS Labs

Networking

- Delivers advanced networking capabilities that seamlessly integrate with advanced layer 7 security and virtual domains (VDOs) to offer extensive deployment flexibility, multi-tenancy and effective utilization of resources
- Delivers high-density, flexible combination of various high-speed interfaces to enable best TCO for customers for data center and WAN deployments

Management

- Includes a management console that is effective, simple to use, and provides comprehensive network automation and visibility
- Provides Zero Touch Integration with Fortinet's Security Fabric's Single Pane of Glass Management
- Predefined compliance checklist analyzes the deployment and highlights best practices to improve overall security posture

Security Fabric

- Enables Fortinet and Fabric-ready partners' products to provide broader visibility, integrated end-to-end detection, threat intelligence sharing, and automated remediation

Firewall	IPS	NGFW	Threat Protection	Interfaces
10 Gbps	1.4 Gbps	1 Gbps	900 Mbps	Multiple GE RJ45 Variants with internal storage WiFi

ABASI
Servicios Integrales S. de C.V.

Horario: No. 83 - 101 Col. Roma México D.F.
Cadastral: C.P. 06700 P.O. Box 30114202
Tel: +52 55 912 4 71 1 - 4 71 1 4 71 1 - 4 71 1 4 71 1

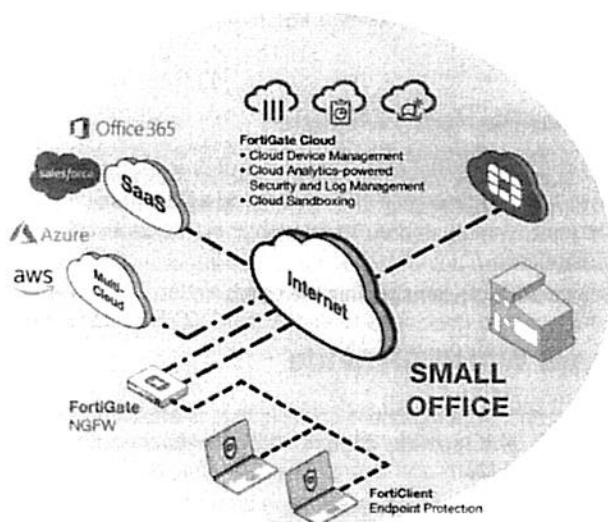
DEPLOYMENT

000009



Next Generation Firewall (NGFW)

- Reduce the complexity and maximize your ROI by integrating threat protection security capabilities into a single high-performance network security appliance, powered by Fortinet's Security Processing Unit (SPU)
- Full visibility into users, devices, and applications across the entire attack surface and consistent security policy enforcement irrespective of asset location
- Protect against network exploitable vulnerabilities with industry-validated IPS that offers low latency and optimized network performance
- Automatically block threats on decrypted traffic using the industry's highest SSL inspection performance, including the latest TLS 1.3 standard with mandated ciphers
- Proactively block newly discovered sophisticated attacks in real-time with AI-powered FortiGuard Labs and advanced threat protection services included in the Fortinet Security Fabric

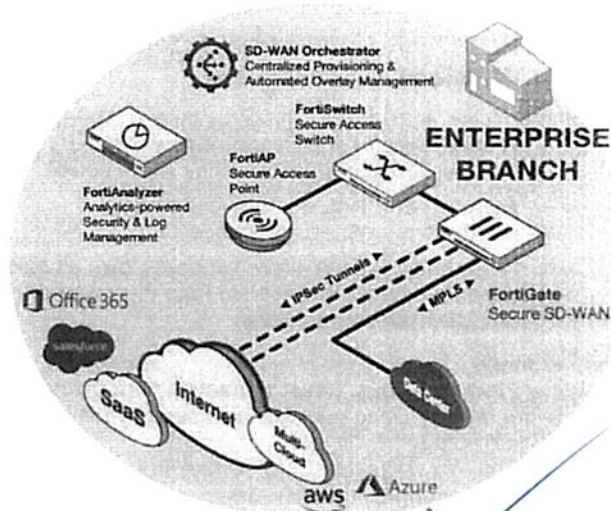


Small Office Deployment
(NGFW)



Secure SD-WAN

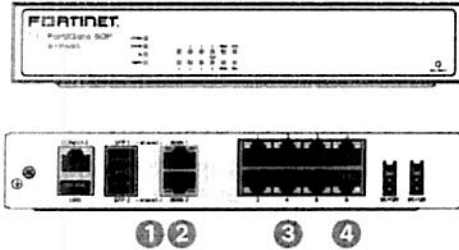
- Consistent business application performance with accurate detection, dynamic WAN path steering on any best-performing WAN transport
- Accelerated multi-cloud access for faster SaaS adoption with cloud-on-ramp
- Self-healing networks with WAN edge high availability, sub-second traffic switchover-based, and real-time bandwidth compute-based traffic steering
- Automated overlay tunnels provides encryption and abstracts physical hybrid WAN making it simple to manage
- Simplified and intuitive workflow with SD-WAN orchestrator for management and zero touch deployment
- Enhanced analytics both real-time and historical provides visibility into network performance and identifies anomalies
- Strong security posture with next generation firewall and real-time threat protection



Enterprise Branch Deployment
(Secure SD-WAN)

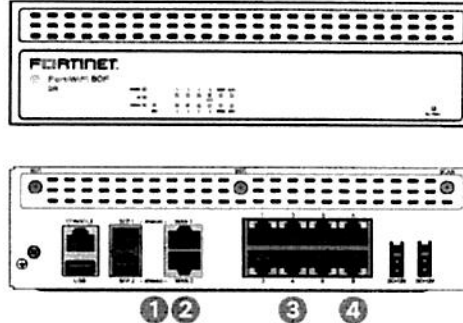
HARDWARE

FortiGate 80F/80F-Bypass/81F, FortiGate 80F/81F-POE



FortiWiFi 80F/81F-2R, FortiWiFi 81F-2R-POE

000010



Interfaces

1. 2x GE RJ45/SFP Shared Media Ports
2. 2x WAN GE RJ45 Ports,
FG80F-Bypass model only: 1x Bypass GE RJ45 Port Pair,
(WAN1 and Port1, default configuration)
3. 6x GE RJ45* Ports
4. 2x GE RJ45* FortiLink Ports

* POE/+ ports for POE Variants

Superior Wireless Coverage

A built-in dual-band, dual-stream access point is integrated on the FortiWiFi 80F-2R series which provides the industry's latest high-speed WiFi-6 (802.11ax) wireless access.

Powered by Purpose-built Secure SD-WAN ASIC SOC4

- Combines a RISC-based CPU with Fortinet's proprietary Security Processing Unit (SPU) content and network processors for unmatched performance
- Delivers industry's fastest application identification and steering for efficient business operations
- Accelerates IPsec VPN performance for best user experience on direct internet access
- Enables best of breed NGFW security and deep SSL inspection with high performance
- Extends security to access layer to enable SD-Branch transformation with accelerated and integrated switch and access point connectivity



Secure Access Layer

FortiLink protocol enables you to converge security and the network access by integrating the FortiSwitch into the FortiGate as a logical extension of the NGFW. These FortiLink enabled ports can be reconfigured as regular ports as needed.

Trusted Platform Module

The FortiGate/FortiWiFi 80F Series features a dedicated module that hardens physical networking appliances by generating, storing, and authenticating cryptographic keys. Hardware-based security mechanisms protect against malicious software and phishing attacks.

Bypass WAN/LAN Mode

The FortiGate-80F-Bypass offers a pair of bypass ports that help organizations avoid network communication interruption due to device faults and improve network reliability.

3G/4G WAN Connectivity

The FortiGate 80F Series includes a 3.0 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.

ABASI
Servicios Integrados S. de C.V.
Nayarit no. 85 - 101 Col. Roma México D.F.
Guatemala C.P. 06700 R.F.C. A308011420
Tel: 55 5210 1377 / 5215 5210 / 5215 5211

FORTINET SECURITY FABRIC

Security Fabric

The industry's highest-performing cybersecurity platform, powered by FortiOS, with a rich ecosystem designed to span the extended digital attack surface, delivering fully automated, self-healing network security.

- **Broad:** Coordinated detection and enforcement across the entire digital attack surface and lifecycle with converged networking and security across edges, clouds, endpoints and users
- **Integrated:** Integrated and unified security, operation, and performance across different technologies, location, deployment options, and the richest Ecosystem
- **Automated:** Context aware, self-healing network & security posture leveraging cloud-scale and advanced AI to automatically deliver near-real-time, user-to-application coordinated protection across the Fabric

The Fabric empowers organizations of any size to secure and simplify their hybrid infrastructure on the journey to digital innovation.



FortiOS™ Operating System

FortiOS, Fortinet's leading operating system enable the convergence of high performing networking and security across the Fortinet Security Fabric delivering consistent and context-aware security posture across network endpoint, and clouds. The organically built best of breed capabilities and unified approach allows organizations to run their businesses without compromising performance or protection, supports seamless scalability, and simplifies innovation consumption.

SERVICES



FortiGuard™ Security Services

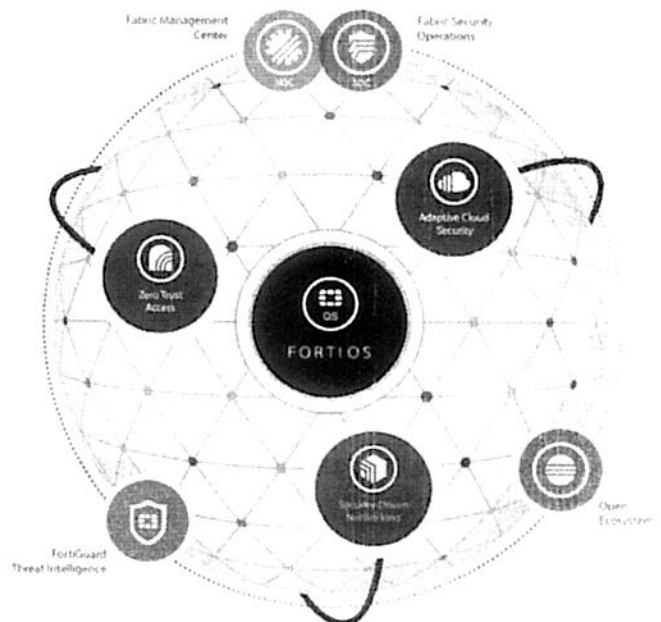
FortiGuard Labs offers real-time intelligence on the threat landscape, delivering comprehensive security updates across the full range of Fortinet's solutions. Comprised of security threat researchers, engineers, and forensic specialists, the team collaborates with the world's leading threat monitoring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



FortiCare™ Services

Fortinet is dedicated to helping our customers succeed, and every year FortiCare services help thousands of organizations get the most from their Fortinet Security Fabric solution. We have more than 1,000 experts to help accelerate technology implementation, provide reliable assistance through advanced support, and offer proactive care to maximize security and performance of Fortinet deployments.

000011



SPECIFICATIONS

000013

	FORTIGATE 80F	FORTIGATE 81F	FORTIGATE 80F-BYPASS	FORTIGATE 80F-POE	FORTIGATE 81F-POE
Dimensions					
Height x Width x Length (inches)	16 x 8.5 x 7.0	16 x 8.5 x 7.0	16 x 8.5 x 7.0	2.4 x 8.5 x 7.0	2.4 x 8.5 x 7.0
Height x Width x Length (mm)	40 x 216 x 178	40 x 216 x 178	40 x 216 x 178	60 x 216 x 178	60 x 216 x 178
Weight	2.4 lbs (1.1 kg)	2.4 lbs (1.1 kg)	2.6 lbs (1.2 kg)	3.1 lbs (1.4 kg)	3.1 lbs (1.4 kg)
Form Factor	Desktop/Wall Mount/Rack Tray				
Operating Environment and Certifications					
Input Rating	12V DC, 3A (dual redundancy optional)				
Power Required (Redundancy Optional)	Powered by up to 2 External DC Power Adapters (1 adapter included), 100-240V AC, 50/60 Hz				
Maximum Current	115VAC/0.4A, 230VAC/0.2A	115VAC/0.4A, 230VAC/0.2A	115VAC/0.4A, 230VAC/0.2A	115VAC/2.2A, 230VAC/1.1A	115VAC/1.2A, 230VAC/0.6A
Total Available PoE Power Budget*	—	—	—	96W	96W
Power Consumption (Average / Maximum)	12.6W / 15.4W	13.5W / 16.5W	12.6W / 15.4W	96W / 118W	20W / 137W
Heat Dissipation	52.55 BTU/h	56.30 BTU/h	52.55 BTU/h	402.26 BTU/h	467.5 BTU/h
Operating Temperature	32-104°F (0-40°C)				
Storage Temperature	31-158°F (-35-70°C)				
Humidity	10-90% non condensing				
Noise Level	Fanless 0 dBA	Fanless 0 dBA	Fanless 0 dBA	31.56 dBA	31.56 dBA
Operating Altitude	Up to 7,400 ft (2,250 m)				
Compliance	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB				
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN				

* Maximum loading on each PoE+ port is 30 W (802.3at).



Mayanit no. 85 - 101 Col. Roma México D.F.
 Cuauhtémoc C.P. 06700 R.F.C. A30901142CC2
 Tel. Fobs 5912-5702 / 5219-5703 www.abasi.com

SPECIFICATIONS

000014

	FORTIWIFI 80F-2R	FORTIWIFI 81F-2R	FORTIWIFI 81F-2R-POE
Hardware Specifications			
GE RJ45/SFP Shared Media Pairs	2	2	2
GE RJ45 Internal Ports	6	6	—
GE RJ45 FortiLink Ports (Default)	2	2	—
GE RJ45 PoE/+ Ports	—	—	6
GE RJ45 PoE/+ FortiLink Ports (Default)	—	—	2
Bypass GE RJ45 Port Pair (WAN1 & Port1, default configuration)	—	—	—
Wireless Interface	Dual WiFi Radio (5 GHz, 2.4 GHz) 802.11a/b/g/n/ac/ax + 1 Scanning Radio		
USB Ports 3.0	1	1	1
Console (RJ45)	1	1	1
Internal Storage	—	1x 128 GB SSD	1x 128 GB SSD
Radio Specifications			
Multiple User (MU) MIMO	2x2		
Maximum Wi-Fi Speeds	574 Mbps @ 2.4 GHz, 1201 Mbps @ 5 GHz		
Maximum Tx Power	23 dBm @ 2.4 GHz, 22 dBm @ 5 GHz		
Antenna Gain	4 SdBi @ 2.4GHz, 5 SdBi @ 5GHz		
System Performance — Enterprise Traffic Mix			
IPS Throughput ²	1.4 Gbps		
NGFW Throughput ^{2, 4}	1 Gbps		
Threat Protection Throughput ^{2, 5}	900 Mbps		
System Performance			
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	10/10/7 Gbps		
Firewall Latency (64 byte UDP packets)	3.23 µs		
Firewall Throughput (Packets Per Second)	10.5 Mpps		
Concurrent Sessions (TCP)	15 Million		
New Sessions/Second (TCP)	45,000		
Firewall Policies	5,000		
IPsec VPN Throughput (512 byte) ¹	6.5 Gbps		
Gateway-to-Gateway IPsec VPN Tunnels	200		
Client-to-Gateway IPsec VPN Tunnels	2,500		
SSL-VPN Throughput	950 Mbps		
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	200		
SSL Inspection Throughput (IPS, avg. HTTPS) ³	715 Mbps		
SSL Inspection CPS (IPS, avg. HTTPS) ³	700		
SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³	100,000		
Application Control Throughput (HTTP 64K) ²	1.8 Gbps		
CAPWAP Throughput (HTTP 64K)	9 Gbps		
Virtual Domains (Default / Maximum)	10 / 10		
Maximum Number of FortiSwitches Supported	16		
Maximum Number of FortiAPs (Total / Tunnel Mode)	96 / 48		
Maximum Number of FortiTokens	500		
High Availability Configurations	Active / Active, Active / Passive, Clustering		

Note: All performance values are "up to" and vary depending on system configuration.

1. IPsec VPN performance test uses AES256-SHA256.

2. IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.

3. SSL inspection performance values use an average of HTTPS sessions of different cipher suites.

4. NGFW performance is measured with Firewall, IPS and Application Control enabled.

5. Threat Protection performance is measured with Firewall, IPS, Application Control, URL filtering, and Malware Protection with sandboxing enabled.

SPECIFICATIONS

000015

	FORTIWIFI 80F-2R	FORTIWIFI 81F-2R	FORTIWIFI 81F-2R-POE
Dimensions			
Height x Width x Length (inches)	2.4 x 8.5 x 7.0	2.4 x 8.5 x 7.0	2.4 x 8.5 x 7.0
Height x Width x Length (mm)	60 x 216 x 178	60 x 216 x 178	60 x 216 x 178
Weight	3.3 lbs (1.5 kg)	3.3 lbs (1.5 kg)	3.3 lbs (1.5 kg)
Form Factor	Desktop/Wall Mount/Rack Tray		
Operating Environment and Certifications			
Input Rating	12V DC, 5A (dual redundancy optional)		
Power Required (Redundancy Optional)	Powered by up to 2 External DC Power Adapters (1 adapter included), 100-240V AC, 50/60 Hz		
Maximum Current	115VAC/0.42A, 230VAC/0.21A	115VAC/0.42A, 230VAC/0.28A	115VAC/0.9A, 230VAC/0.6A
Total Available PoE Power Budget*	—	—	96W
Power Consumption (Average / Maximum)	22.9 W / 27.9 W	24.79 W / 30.29 W	107.4 W / 131.3 W
Heat Dissipation	95.26 BTU/h	103.29 BTU/h	441.4 BTU/h
Operating Temperature	32-104°F (0-40°C)		
Storage Temperature	-31-158°F (-35-70°C)		
Humidity	10-90% non-condensing		
Noise Level	24.14 dBA	24.14 dBA	31.58 dBA
Operating Altitude	Up to 7,400 ft (2,250 m)		
Compliance	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB		
Certifications	ICSA Labs Firewall, IPsec, IPS, Antivirus, SSL VPN		

* Maximum loading on each PoE+ port is 30 W (802.3at)

ORDERING INFORMATION

000016

Product	SKU	Description
FortiGate 80F	FG-80F	8 x GE RJ45 ports, 2 x RJ45/SFP shared media WAN ports.
FortiGate 81F	FG-81F	8 x GE RJ45 ports, 2 x RJ45/SFP shared media WAN ports, 128GB onboard storage
FortiGate 80F-Bypass	FG-80F-Bypass	8 x GE RJ45 ports, 2 x RJ45/SFP shared media WAN ports, may be configured with 1 pair of LAN bypass
FortiGate 80F-POE	FG-80F-POE	8 x GE PoE ports, 2 x RJ45/SFP shared media WAN ports
FortiGate 81F-POE	FG-81F-POE	8 x GE RJ45 PoE ports, 2 x RJ45/SFP shared media WAN ports, 128GB SSD
FortiWiFi 80F-2R	FWF-80F-2R	8 x GE RJ45 ports, 2 x RJ45/SFP shared media WAN ports, dual WiFi radio
FortiWiFi 81F-2R	FWF-81F-2R	8 x GE RJ45 ports, 2 x RJ45/SFP shared media WAN ports, dual WiFi radio, 128GB SSD
FortiWiFi 81F-2R-POE	FWF-81F-2R-POE	8 x GE RJ45 RJ45 PoE ports, 2 x RJ45/SFP shared media WAN ports, dual WiFi radio, 128GB SSD
Accessories	SKU	Description
AC Power Adaptor	SP-FG60E-PDC-5	Pack of 5 AC power adaptors for FG/FWF 60E/61E, 60F/61F, 80E/81E and 80F/81F.
AC Power Adaptor	SP-FWF80F-PDC-5	Pack of 5 AC power adaptors for FWF-80/81F-2R, power cable SP-FG60CPCOR-XX sold separately
AC Power Adaptor	SP-FG80E-POE-PDC	AC power adaptor for FG-60E-POE, FG-80E-POE, FG-81E-POE, FG-80/81F-POE, FWF-81F-2R-POE power cable SP-FG60CPCOR-XX sold separately
Rack Mount Tray	SP-RACKTRAY-02	Rack mount tray for all FortiGate E series and F series desktop models
Wall Mount Kit	SP-FG60F-MOUNT-20	Pack of 20 wall mount kits for FG/FWF-40F series, FG/FWF-60F series, FG-80F, FG-81F and FG-80F-Bypass
Transceivers	SKU	Description
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.

BUNDLES



FortiGuard 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 one of these FortiGuard Bundles.

Bundles	360 Protection	Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiCare	ASE ¹	24x7	24x7	24x7
FortiGuard App Control Service	•	•	•	•
FortiGuard IPS Service	•	•	•	•
FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
FortiGuard Web and Video ² Filtering Service	•	•	•	•
FortiGuard Antispam Service	•	•	•	•
FortiGuard Security Rating Service	•	•	•	•
FortiGuard IoT Detection Service	•	•	•	•
FortiGuard Industrial Service	•	•	•	•
FortiConverter Service	•	•	•	•
SD-WAN Orchestrator Entitlement	•	•	•	•
SD-WAN Cloud Assisted Monitoring	•	•	•	•
SD-WAN Overlay Controller VPN Service	•	•	•	•
Fortinet SOCaaS	•	•	•	•
FortiAnalyzer Cloud	•	•	•	•
FortiManager Cloud	•	•	•	•

1. 24x7 plus Advanced Services Ticket Handling 2. Available when running FortiOS 7.0

FORTINET

www.fortinet.com

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard® are registered trademarks of Fortinet, Inc. and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other names herein may be trademarks of their respective owners. Performance and other metrics contained herein were obtained 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 customer. Fortinet expressly warrants that the identified product will perform according to the performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. Fortinet disclaims all liability with warranty will be limited to performance in the lab under conditions as in Fortinet's internal lab tests. Fortinet disclaims all liability, covenants, representations, and warranties pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer or otherwise remove this publication without notice, and the most current version of this publication shall be applicable.

FORTINET.

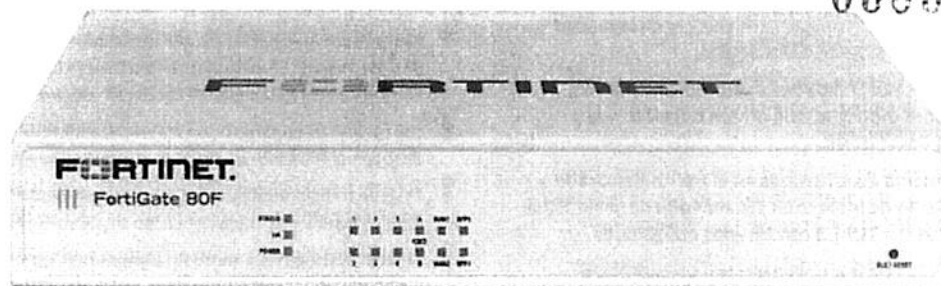
ECIJA DE DATOS

FortiGate® Serie FortiWiFi 80F

FG-80F, FG-80F-POE, FG-80F-Bypass, FG-81F, FG-81F-POE,
FWF-81F-2R-POE y FWF-80F / 81F-2R

Firewall de próxima
generación Secure SD-WAN

000017



La serie FortiGate FortiWiFi 80F proporciona una solución SD-WAN segura, escalable y centrada en la aplicación en un factor de forma de escritorio compacto y sin ventilador para sucursales empresariales y empresas medianas con WiFi-6 integrado (802.11ax). Protege contra las amenazas cibernéticas con la aceleración systemmon-a-chip y SD-WAN segura líder en la industria en una solución simple, asequible y fácil de implementar. El enfoque de redes basadas en la seguridad de Fortinet proporciona una estrecha integración de la red a la nueva generación de seguridad.

Seguridad

- Identifica miles de aplicaciones dentro del tráfico de red para una inspección profunda y aplicación de políticas granulares
- Protege contra malware, exploits y sitios web maliciosos en tráfico cifrado y no cifrado
- Prevenga y detecte ataques conocidos y desconocidos utilizando inteligencia de amenazas continua de los servicios de seguridad de FortiGuard Labs con tecnología de inteligencia artificial

Rendimiento

- Ofrece el mejor rendimiento de protección contra amenazas de la industria y latencia ultrabaja utilizando tecnología de procesador de seguridad (SPU) especialmente diseñada
- Proporciona un rendimiento y una protección líderes en la industria para el tráfico cifrado SSL.

Certificación

- Probado y validado de forma independiente para obtener la mejor eficacia y rendimiento de seguridad de su clase
- Recibió certificaciones de terceros incomparables de NSS Labs

Redes

- Ofrece capacidades de red avanzadas que se integran a la perfección con la seguridad avanzada de capa 7 y los dominios virtuales (VDM) para ofrecer una amplia flexibilidad de implementación, tenencia múltiple y utilización eficaz de los recursos.
- Ofrece una combinación flexible y de alta densidad de varias interfaces de alta velocidad para permitir el mejor TCO para los clientes para implementaciones de centros de datos y WAN

Gestión

- Incluye una consola de administración que es efectiva, fácil de usar y proporciona visibilidad y automatización de red integrales
- Proporciona integración Zero Touch con el panel único de administración de vidrio de Security Fabric de Fortinet
- La lista de verificación de cumplimiento predefinida analiza la implementación y destaca las mejores prácticas para mejorar la postura general de seguridad

Tela de seguridad

Habilita los productos de socios preparados para Fortinet y Fabric para proporcionar una visibilidad más amplia, detección integrada de extremo a extremo, intercambio de inteligencia sobre amenazas y reparación automatizada

Cortafuegos	IPS	NGFW	Protección contra amenazas	Interfaces
10 Gbps	1,4 Gbps	1 Gbps	900 Mbps	Múltiples GE RJ45 Variantes con almacenamiento interno Wifi

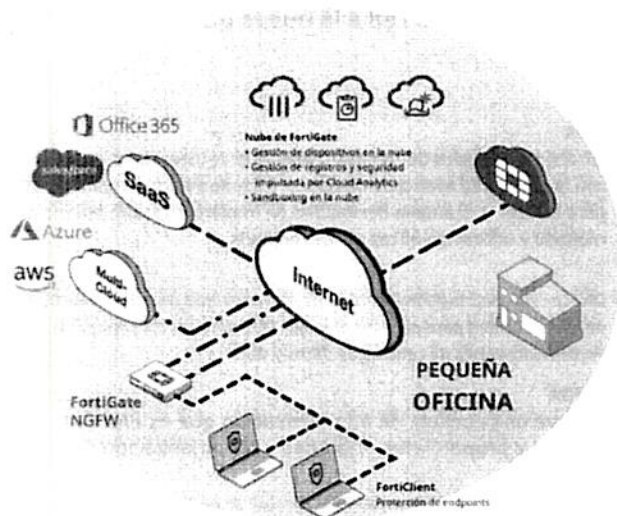
ABASI
Servicios Integrados S.A. de C.V.
Nayarit no. 85 - 101 Col. Roma México D.F.
Cuauhtémoc C.P. 06700 R.F.C. ASIO501142C2
Tel: 5912-5702 / 5219-3703 www.abasi.com.mx

DESPLIEGUE



Próxima generación Cortafuegos (NGFW)

- § Reduzca la complejidad y maximice su ROI integrando las capacidades de seguridad de protección contra amenazas en un solo dispositivo de seguridad de red de alto rendimiento, impulsado por la Unidad de procesamiento de seguridad (SPU) de Fortinet
- § Visibilidad total de los usuarios, dispositivos y aplicaciones en toda la superficie de ataque y aplicación constante de políticas de seguridad independientemente de la ubicación de los activos.
- § Protéjase contra las vulnerabilidades explotables de la red con IPS validado por la industria que ofrece baja latencia y rendimiento de red optimizado
- § Bloquee automáticamente las amenazas en el tráfico descifrado utilizando el rendimiento de inspección SSL más alto de la industria, incluido el último estándar TLS 1.3 con cifrados obligatorios
- § Bloquee de manera proactiva los ataques sofisticados recién descubiertos en tiempo real con los laboratorios FortiGuard con tecnología de inteligencia artificial y los servicios avanzados de protección contra amenazas incluidos en Fortinet Security Fabric



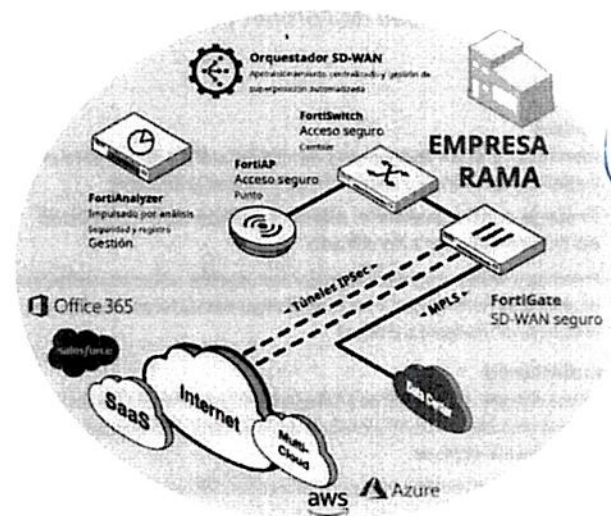
Implementación de pequeñas oficinas
(NGFW)



SD-WAN seguro

000018

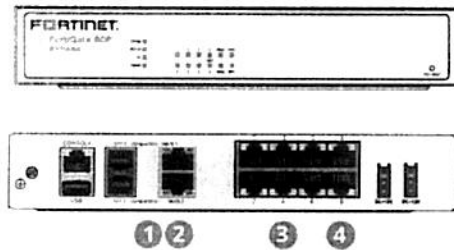
- § Rendimiento constante de las aplicaciones empresariales con detección precisa, direccionamiento dinámico de la ruta WAN en cualquier transporte WAN de mejor rendimiento
- § Acceso acelerado a múltiples nubes para una adopción de SaaS más rápida con nube en rampa
- § Redes de autorreparación con alta disponibilidad de borde WAN, control de tráfico basado en conmutación de tráfico de menos de un segundo y ancho de banda en tiempo real basado en cómputo
- § Los túneles de superposición automatizados proporcionan cifrado y abstraen la WAN híbrida física, lo que facilita su administración.
- § Flujo de trabajo simplificado e intuitivo con SD-WAN orchestrator para la administración y la implementación sin intervención.
- § El análisis mejorado, tanto en tiempo real como histórico, proporciona visibilidad del rendimiento de la red e identifica anomalías.
- § Fuerte postura de seguridad con firewall de próxima generación y protección contra amenazas en tiempo real



Implementación de sucursales empresariales
(SD-WAN seguro)

HARDWARE

FortiGate 80F / 80F-Bypass / 81F, FortiGate 80F / 81F-POE



Interfaces

1. 2x puertos de medios compartidos GE RJ45 / SFP
2. 2 puertos WAN GE RJ45,
Solo modelo FG80F-Bypass: 1x Bypass GE RJ45 Port Pair, (WAN1
y Port1, configuración predeterminada)
3. 6 puertos GE RJ45 *
4. 2 puertos GE RJ45 * FortiLink

* Puertos POE / + para variantes POE

Cobertura inalámbrica superior

En la serie FortiWiFi 80F-2R está integrado un punto de acceso de doble banda y doble flujo integrado que proporciona el acceso inalámbrico WiFi-6 (802.11ax) de alta velocidad más reciente de la industria.

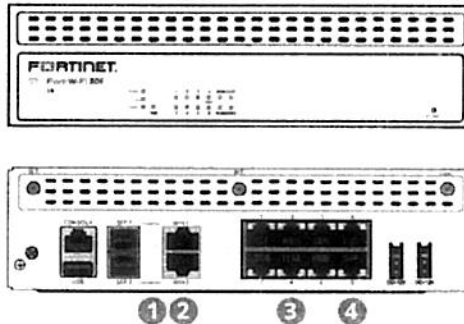
Desarrollado por Secure SD-WAN ASIC SOC4 especialmente diseñado



- § Combina una CPU basada en RISC con la seguridad patentada de Fortinet
Procesadores de red y contenido de la Unidad de procesamiento (SPU) para un rendimiento inigualable
- § Ofrece la identificación y dirección de aplicaciones más rápidas de la industria para operaciones comerciales eficientes
- § Acelera el rendimiento de IPsec VPN para la mejor experiencia de usuario con acceso directo a Internet
- § Permite la mejor seguridad NGFW e inspección SSL profunda con alto rendimiento
- § Extiende la seguridad a la capa de acceso para permitir la transformación SD-Branch con conectividad de punto de acceso y conmutador integrada y acelerada

FortiWiFi 80F / 81F-2R, FortiWiFi 81F-2R-POE

000019



Capa de acceso seguro

El protocolo FortiLink le permite converger la seguridad y el acceso a la red al integrar FortiSwitch en FortiGate como una extensión lógica del NGFW. Estos puertos habilitados para FortiLink se pueden reconfigurar como puertos regulares según sea necesario.

Modulo de plataforma confiable

La serie FortiGate / FortiWiFi 80F cuenta con un módulo dedicado que fortalece los dispositivos de red física al generar, almacenar y autenticar claves criptográficas. Los mecanismos de seguridad basados en hardware protegen contra software malintencionado y ataques de phishing.

Omitir el modo WAN / LAN

El FortiGate-80F-Bypass ofrece un par de puertos de bypass que ayudan a las organizaciones a evitar la interrupción de la comunicación de la red debido a fallas del dispositivo y mejorar la confiabilidad de la red.

Conectividad WAN 3G / 4G

La serie FortiGate 80F incluye un puerto USB 3.0 que le permite conectar un módem USB 3G / 4G de terceros compatible, proporcionando conectividad WAN adicional o un enlace redundante para 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 (tiempo medio entre fallas) superior, lo que minimiza la posibilidad de una interrupción de la red.

TEJIDO DE SEGURIDAD FORTINET

Tela de seguridad

La plataforma de ciberseguridad de mayor rendimiento de la industria, impulsada por FortiOS, con un rico ecosistema diseñado para abarcar la superficie de ataque digital extendida, brindando seguridad de red totalmente automatizada y con recuperación automática.

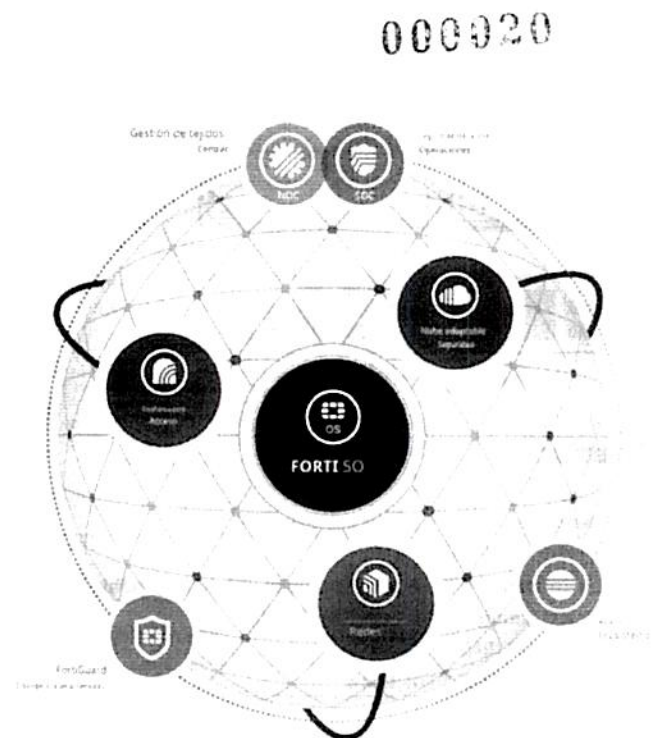
- 5 **Amplio:** Detección y aplicación coordinadas en todo el toda la superficie de ataque digital y el ciclo de vida con redes convergentes y seguridad en los bordes, las nubes, los puntos finales y los usuarios
- 5 **Integrado:** Seguridad, operación y rendimiento integrados y unificados en diferentes tecnologías, ubicación, opciones de implementación y el ecosistema más rico
- 5 **Automatizado:** Posición de seguridad y red auto-reparable y sensible al contexto que aprovecha la escala de la nube y la inteligencia artificial avanzada para brindar automáticamente una protección coordinada de usuario a aplicación casi en tiempo real en toda la tela.

Fabric permite a las organizaciones de cualquier tamaño proteger y simplificar su infraestructura híbrida en el camino hacia la innovación digital.



FortiOS™ Sistema operativo

FortiOS, el sistema operativo líder de Fortinet, permite la convergencia de redes y seguridad de alto rendimiento en Fortinet Security Fabric, lo que brinda una postura de seguridad consistente y sensible al contexto en los puntos finales de la red y las nubes. Las mejores capacidades de su clase construidas orgánicamente y el enfoque unificado permiten a las organizaciones ejecutar sus negocios sin comprometer el rendimiento o la protección, admite una escalabilidad perfecta y simplifica el consumo de innovación.



El lanzamiento de FortiOS 7 expande drásticamente la capacidad de Fortinet Security Fabric para brindar seguridad consistente en modelos de implementación híbrida que consisten en dispositivos, software y As-a-Service con SASE, ZTNA y otras soluciones emergentes de ciberseguridad.

SERVICIOS



FortiGuard™ Servicios de seguridad

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



FortiCare™ Servicios

Fortinet se dedica a ayudar a nuestros clientes a tener éxito, y cada año los servicios de FortiCare ayudan a miles de organizaciones a aprovechar al máximo su solución Fortinet Security Fabric. Contamos con más de 1,000 expertos para ayudar a acelerar la implementación de tecnología, brindar asistencia confiable a través de soporte avanzado y ofrecer atención proactiva para maximizar la seguridad y el rendimiento de las implementaciones de Fortinet.

ESPECIFICACIONES

000021

	FORTIGATE 80F	FORTIGATE 81F	FORTIGATE 80F-BYPASS	FORTIGATE 80F-POE	FORTIGATE 81F-POE
Especificaciones de hardware					
Pares de medios compartidos GE RJ45 / SFP	2	2	2	2	2
Puertos internos GE RJ45	6	6	6	-	-
Puertos GE RJ45 FortiLink	2	2	2	-	-
(predeterminado) Puertos GE RJ45 PoE / +	-	-	-	6	6
Puertos GE RJ45 PoE / + FortiLink (predeterminado)	-	-	-	2	2
Omitir par de puertos GE RJ45 (WAN) y Port1, configuración predeterminada	-	-	SI	-	SI
Interfaz inalámbrica	-	-	-	-	-
Puertos USB 3.0	1	1	1	1	1
Consola (RJ45)	1	1	1	1	1
Almacenamiento interno	-	1 unidad 3.5" SATA / 2TB HDD	-	-	1 unidad 3.5" SATA / 2TB HDD
Rendimiento del sistema: mezcla de tráfico empresarial					
Rendimiento IPS :			1.4 Gbps		
Rendimiento de NGFW :			1 Gbps		
Rendimiento de protección contra amenazas :			900 Mbps		
Rendimiento de sistema					
Rendimiento del cortafuegos (Paquetes UDP de 1518/512/64 bytes)			10/10/7 Gbps		
Latencia del cortafuegos (Paquetes UDP de 64 bytes)			3.23 µs		
Rendimiento del cortafuegos (Paquetes por segundo)			10.5 Mpps		
Sesiones concurrentes (TCP)			1.5 millones		
Nuevas sesiones / Segundas			45,000		
políticas de firewall (TCP)			5,000		
Rendimiento de VPN IPsec (512 bytes) :			6.5 Gbps		
Túneles VPN IPsec de puerta de enlace a puerta de enlace			200		
Túneles VPN IPsec de cliente a puerta de enlace			2500		
Rendimiento SSL-VPN					
Usuarios concurrentes de SSL-VPN (máximo recomendado, modo túnel)			950 Mbps		
			200		
Rendimiento de inspección SSL (IPS, HTTPS promedio) :			715 Mbps		
CPS de inspección SSL (IPS, HTTPS promedio) :			700		
Sesión concurrente de inspección SSL (IPS, HTTPS promedio) :			100,000		
Rendimiento de control de aplicaciones (HTTP 64K) :			1.8 Gbps		
Rendimiento CAPWAP (HTTP 64K)			9 Gbps		
Domínios virtuales (predeterminado / Máximo)			10/10		
Número máximo de					
Compatible con FortiSwitches			-		
Número máximo de FortiAP (modo total / túnel)			96/48		
Número máximo de configuraciones			500		
de alta disponibilidad de FortiTokens			Activo / Activo, Activo / Pasivo, Agrupación		

Nota: Todos los valores de rendimiento son "hasta" y varían según la configuración del sistema.

1. La prueba de rendimiento de IPsec VPN utiliza AES256-SHA256.

2. IPS (Enterprise Mix), Application Control, NGFW y Threat Protection se miden con el registro habilitado.

3. Los valores de rendimiento de la inspección SSL utilizan un promedio de sesiones HTTPS de diferentes conjuntos de cifrado.

4. El rendimiento de NGFW se mide con Firewall, IPS y Application Control habilitados.

5. El rendimiento de Threat Protection se mide con Firewall, IPS, Application Control, filtrado de URL y Malware Protection con sandboxing habilitado.


ABASI
 Servicios Integrados S.A. de C.V.

 Nayarit no. 85 - 101 Col. Torre México D.F.
 C.P. 06700 R.F.C. AS0501142C2
 Tel: 55 5219 4700 - 5219 4701

000022

ESPECIFICACIONES

	FORTIGATE 80F	FORTIGATE 81F	FORTIGATE 80F-BYPASS	FORTIGATE 80F-POE	FORTIGATE 81F-POE
Dimensiones					
Alto x Ancho x Largo (pulgadas)	1,6 x 8,5 x 7,0	1,6 x 8,5 x 7,0	1,6 x 8,5 x 7,0	2,4 x 8,5 x 7,0	2,4 x 8,5 x 7,0
Alto x Ancho x Largo (mm)	40 x 216 x 178	40 x 216 x 178	40 x 216 x 178	60 x 216 x 178	60 x 216 x 178
Peso	2,4 libras (1,1 kg)	2,4 libras (1,1 kg)	2,6 libras (1,2 kg)	3,1 libras (1,4 kg)	3,1 libras (1,4 kg)
Entorno operativo y certificaciones					
Calificación					
de entrada	12V DC, 3A (redundancia dual opcional)				
Energía requerida (Redundancia opcional)	Alimentado por hasta 2 adaptadores de corriente CC externos (1 adaptador incluido). 100-240 V CA, 50/60 Hz				
Corriente máxima	115VAC / 0.4A, 230VAC / 0.2A	115VAC / 0.4A, 230VAC / 0.2A	115VAC / 0.4A, 230VAC / 0.2A	115VAC / 2.2A, 230VAC / 1.1A	115VAC / 1.2A, 230VAC / 0.6A
Presupuesto total de energía PoE disponible *				96W	96W
El consumo de energía (Promedio / Máximo)	12.6 W / 15.4 W	13.5 W / 16.5 W	12.6 W / 15.4 W	96 W / 118 W	20W / 137W
Disipación de calor	52.55 BTU / h	56.30 BTU / h	52.55 BTU / h	402.26 BTU / h	467.5 BTU / h
Temperatura de funcionamiento	32 a 104 ° F (0 a 40 ° C)				
Temperatura de almacenamiento	-31 a 158 ° F (-35 a 70 ° C)				
Humedad	10-90% sin condensación				
Nivel de ruido	50 dBA	50 dBA	50 dBA	31,56 dBA	31,56 dBA
Altitud operativa	Hasta 7,400 pies (2,250 m)				
Cumplimiento	FCC, ICES, CE, RCM, VCCI, BSMI, UL / cUL, CB, ICES				
Certificaciones	Labs: Firewall, IPSec, IPS, Antivirus, SSL-VPN				

* La carga máxima en cada puerto PoE / + es de 30 W (802.3at)

ABASI
Servicios Integrales S.A. de C.V.
Nayabí No. 55 - 101 Col. Roma México D.F.
Código FISCAL C.F. 06700 R.F.C. AS0301143C2
Tel: 578 3912 4700 / 5719 5700 www.abasi.com

ESPECIFICACIONES

000023

	FORTIWIIFI 80F-2R	FORTIWIIFI 81F-2R	FORTIWIIFI 81F-2R-POE
Especificaciones de hardware			
Pares de medios compartidos GE RJ45 / SFP	2	2	2
Puertos internos GE RJ45	6	6	-
Puertos GE RJ45 FortiLink	2	2	-
(predeterminado) Puertos GE RJ45 PoE / +	-	-	6
Puertos GE RJ45 PoE / + FortiLink (predeterminado)	-	-	2
Omitir par de puertos GE RJ45 (WAN1 y Port1, configuración predeterminada)	-	-	-
Interfaz inalámbrica	Radio WiFi dual (5 GHz, 2.4 GHz) 802.11a / b / g / n / ac / ax = 1 radio de exploración		
Puertos USB 3.0	1	1	1
Consola (RJ45)	1	1	1
Almacenamiento interno	-	Unidad SAS 16 TB / 20 GB	Unidad SAS 16 TB / 4 TB
Especificaciones de radio			
Velocidades máximas de Wi-Fi MIMO	2x2		
para múltiples usuarios (MUI)	574 Mbps a 2.4 GHz, 1201 Mbps a 5 GHz		
Potencia máxima de transmisión	23 dBm a 2.4 GHz, 22 dBm a 5 GHz		
Ganancia de la antena	4.5dBi @ 2.4GHz, 5.5dBi @ 5GHz		
Rendimiento del sistema: mezcla de tráfico empresarial			
Rendimiento IPS :	1.4 Gbps		
Rendimiento de NGFW :	1 Gbps		
Rendimiento de protección contra amenazas :	900 Mbps		
Rendimiento de sistema			
Rendimiento del cortafuegos (Paquetes UDP de 1518/512/64 bytes)	10/10/7 Gbps		
Latencia del cortafuegos (paquetes UDP de 64 bytes)	3.23 μs		
Rendimiento del cortafuegos (paquetes por segundo)	10.5 Mpps		
Sesiones simultáneas (TCP)	1.5 millones		
Políticas de firewall de sesiones nuevas / segundas (TCP)	45.000 / 5.000		
Rendimiento de VPN IPsec (512 bytes) :	6,5 Gbps		
Túneles VPN IPsec de puerta de enlace a puerta de enlace	200		
Túneles VPN IPsec de cliente a puerta de enlace	2500		
Rendimiento de VPN SSL	950 Mbps		
Usuarios concurrentes de SSL-VPN (máximo recomendado, modo túnel)	200		
Rendimiento de inspección SSL (IPS, HTTPS promedio) :	715 Mbps		
CPS de inspección SSL (IPS, HTTPS promedio) :	700		
Sesión concurrente de inspección SSL (IPS, HTTPS promedio) :	100.000		
Rendimiento de control de aplicaciones (HTTP 64K) :	1,8 Gbps		
Rendimiento CAPWAP (HTTP 64K) Dominios virtuales (predeterminado / máximo) Número máximo de	9 Gbps / 10/10		
FortiSwitches admitidos	96/48		
Número máximo de FortiAP (modo total / túnel)	500		
Número máximo de configuraciones de alta disponibilidad de FortiTokens	Activo / Activo, Activo / Pasivo, Agrupación		

Nota: Todos los valores de rendimiento son "hasta" y varían según la configuración del sistema.

1. La prueba de rendimiento de IPsec VPN utiliza AES256-SHA256.

2. IPS (Enterprise Mix), Application Control, NGFW y Threat Protection se miden con el registro habilitado.

3. Los valores de rendimiento de la inspección SSL utilizan un promedio de sesiones HTTPS de diferentes conjuntos de cifrado.

4. El rendimiento de NGFW se mide con Firewall, IPS y Application Control habilitados.

5. El rendimiento de Threat Protection se mide con Firewall, IPS, Application Control, filtrado de URL y Malware Protection con sandboxing habilitado.



Novarte no. 85 - 101 Col. Roma México D.F.
Cudaduermoc C.P. 04700 R.F.C. AS0501142C2
Tel. Fax 5912-3702 / 5219-3701 www.abasi.com

ESPECIFICACIONES

000024

	FORTIWIIFI 80F-2R	FORTIWIIFI 81F-2R	FORTIWIIFI 81F-2R-POE
Dimensiones			
Alto x Ancho x Largo (pulgadas)	2.4 x 8.5 x 7.0	2.4 x 8.5 x 7.0	2.4 x 8.5 x 7.0
Alto x Ancho x Largo (mm) Peso	60 x 216 x 178	60 x 216 x 178	60 x 216 x 178
	3.3 libras (1.5 kg)	3.3 libras (1.5 kg)	3.3 libras (1.5 kg)
Entorno operativo y certificaciones			
	12V DC, 5A (redundancia dual opcional)		
Energía requerida (Redundancia opcional)	Alimentado por hasta 2 adaptadores de corriente CC externos (1 adaptador incluido), 100-240 V CA, 50/60 Hz		
Corriente máxima	115VAC / 0.42A, 230VAC / 0.21A	115VAC / 0.42A, 230VAC / 0.28A	115VAC / 0.9A, 230VAC / 0.6A
Presupuesto total de energía PoE disponible *	96W		
El consumo de energía (Promedio / Máximo)	22.9 W / 27.9 W	24.79 W / 30.29 W	107.4 W / 131.3 W
Disipación de calor	95.26 BTU / h	103.29 BTU / h	441.4 BTU / h
Temperatura de funcionamiento	32 a 104 ° F (0 a 40 ° C)		
Temperatura de almacenamiento	31 a 158 ° F (-35 a 70 ° C)		
Humedad	10-90% sin condensación		
Nivel de ruido	24.14 dBA	24.14 dBA	31.50 dBA
Altitud operativa	Hasta 7,400 pies (2,250 m)		
Cumplimiento	FCC, ICES, CE, RCM, VCCI, BSMI, UL / cUL, CB, ICES		
Certificaciones	Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN		

* La carga máxima en cada puerto PoE / + es de 10 W (802.3at).

ABASI
Servicios Integrales S. de C.V.
Nayarit no. 85 - 101 Col. Roma México D.F.
Código postal: 06700 R.F.C.: AS0301142C2
Tel. Fax: 5512-6102 / 5219-6703 www.abasi.com

000025

INFORMACIÓN SOBRE PEDIDOS

Producto	SKU	Descripción
FortiGate 80F	FG-80F	8 puertos GE RJ45, 2 puertos WAN de medios compartidos RJ45 / SFP
FortiGate 81F	FG-81F	8 puertos GE RJ45, 2 puertos WAN de medios compartidos RJ45 / SFP, almacenamiento integrado de 128 GB
FortiGate 80F-Bypass	Derivación FG-80F	Se pueden configurar 8 puertos GE RJ45, 2 puertos WAN de medios compartidos RJ45 / SFP, con 1 par de derivación LAN / R
FortiGate 80F-POE	FG-80F-POE	puertos GE PoE, 2 puertos WAN de medios compartidos RJ45 / SFP
FortiGate 81F-POE	FG-81F-POE	8 puertos GE RJ45 PoE, 2 puertos WAN de medios compartidos RJ45 / SFP, SSD de 128 GB
FortiWiFi 80F-2R	FWF-80F-2R	8 puertos GE RJ45, 2 puertos WAN de medios compartidos RJ45 / SFP, radio WiFi dual
FortiWiFi 81F-2R	FWF-81F-2R	8 puertos GE RJ45, 2 puertos WAN de medios compartidos RJ45 / SFP, radio WiFi dual, SSD de 128 GB
FortiWiFi 81F-2R-POE	FWF-81F-2R-POE	8 puertos GE RJ45 RJ45 PoE, 2 puertos WAN de medios compartidos RJ45 / SFP, radio WiFi dual, SSD de 128 GB
Accesorios	SKU	Descripción
Adaptador de corriente CA	SP-FG60E-PDC-5	Paquete de 5 adaptadores de corriente CA para FG / FWT 60E / 61E, 60F / 61F, 80E / 81E y 80F / 81F
Adaptador de corriente CA	SP-FWF80F-PDC-5	Paquete de 5 adaptadores de alimentación de CA para FWF 80 / 81F 2R, el cable de alimentación SP-FG60CPCOR-XX se vende por separado
Adaptador de corriente CA	SP-FG80E-POE-PDC	Adaptador de alimentación de CA para FG 60E-POE, FG-80E-POE, FG-81E-POE, FG-80 / 81F-POE, FWF-81F-2R-POE El cable de alimentación SP-FG60CPCOR-XX se vende por separado
Banda de montaje en rack	SP-RACKTRAY-02	Banda de montaje en rack para todos los modelos de escritorio FortiGate serie E y serie F
Kit de montaje en pared	SP-FG60F-MONTAJE-20	Paquete de 20 kits de montaje en pared para las series FG / FWF-40F, FG / FWF-60F, FG-80F, FG-81F y FG-80F-Bypass
Transceptores	SKU	Descripción
1 módulo transceptor GE SFP RJ45 1	FN-TRAN-GE	1 módulo transceptor GE SFP RJ45 para todos los sistemas con ranuras SFP y SFP / SFP *
módulo transceptor GE SFP SX 1	FN-TRAN-SX	módulo transceptor GE SFP SX para todos los sistemas con ranuras SFP y SFP / SFP *
módulo transceptor GE SFP LX	FN-TRAN-LX	transceptor GE SFP LX para todos los sistemas con ranuras SFP y SFP / SFP *

MANOJOS

FortiGuard
Manejo

FortiGuard Labs ofrece una serie de servicios de inteligencia de seguridad para aumentar FortiGate. La plataforma de firewall, usted puede optimizar fácilmente las capacidades de protección de su FortiGate con uno de estos paquetes FortiGuard

manojos	360 Protección	Empresa Protección	Amenaza unificada Protección	Amenaza avanzada Protección
FortiCare	24x7	24x7	24x7	24x7
Servicio de control de aplicaciones de	•	•	•	•
FortiGuard Servicio IPS de FortiGuard	•	•	•	•
FortiGuard Advanced Malware Protection (AMP): antivirus, malware móvil, botnet, CDR, protección contra ataques de virus y servicio en la nube FortiSandbox	•	•	•	•
FortiGuard Web y video, Servicio de filtrado	•	•	•	•
Servicio antispam FortiGuard	•	•	•	•
Servicio de clasificación de seguridad de	•	•	•	•
FortiGuard Servicio de detección de IoT de	•	•	•	•
FortiGuard Servicio Industrial de FortiGuard	•	•	•	•
Servicio de FortiConverter	•	•	•	•
Titularidad de SD-WAN Orchestrator	•	•	•	•
Monitoreo asistido en la nube SD-WAN	•	•	•	•
Controlador de superposición SD-WAN Servicio	•	•	•	•
VPN Fortinet SOCaas	•	•	•	•
FortiAnalyzer Cloud	•	•	•	•
Nube de FortiManager	•	•	•	•

1. 24x7 más gestión de tickets de servicios avanzados

2. Disponible cuando se ejecute FortiGate 7.0

FORTINET

www.fortinet.com

ABASI
 Servicon Integratum S.A de CV

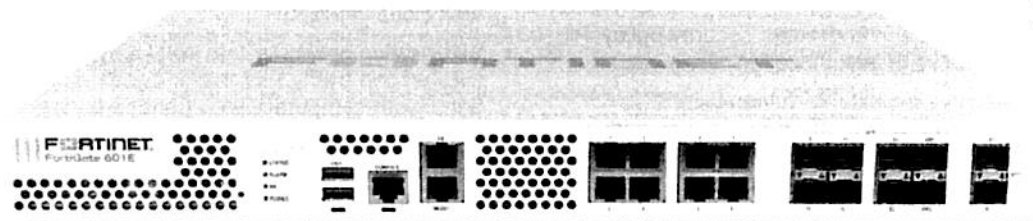
 Noryuri no. 85 - 101 Col. Roma, México D.F.
 Ciudad de México C.F. 06700 R.F.C. ASOS011602
 Tel. Fax 55 12 7102 / 55 19 5795

FortiGate® 600E Series

FG-600E and FG-601E

Next Generation Firewall
Secure SD-WAN
Secure Web Gateway
IPS

000026



The FortiGate 600E series provides an application-centric, scalable, and secure SD-WAN solution with Next Generation Firewall (NGFW) capabilities for mid-sized to large enterprises deployed at the campus or branch level. Protects against cyber threats with system-on-a-chip acceleration and industry-leading secure SD-WAN in a simple, affordable, and easy to deploy solution. Fortinet's Security-Driven Networking approach provides tight integration of the network to the new generation of security.

Security

- Identifies thousands of applications inside network traffic for deep inspection and granular policy enforcement
- Protects against malware, exploits, and malicious websites in both encrypted and non-encrypted traffic
- Prevent and detect against known and unknown attacks using continuous threat intelligence from AI-powered FortiGuard Labs security services

Performance

- Delivers industry's best threat protection performance and ultra-low latency using purpose-built security processor (SPU) technology
- Provides industry-leading performance and protection for SSL encrypted traffic

Certification

- Independently tested and validated for best-in-class security effectiveness and performance
- Received unparalleled third-party certifications from NSS Labs

Networking

- Delivers advanced networking capabilities that seamlessly integrate with advanced layer 7 security and virtual domains (VDMs) to offer extensive deployment flexibility, multi-tenancy and effective utilization of resources
- Delivers high-density, flexible combination of various high-speed interfaces to enable best TCO for customers for data center and WAN deployments

Management

- Includes a management console that is effective, simple to use, and provides comprehensive network automation and visibility
- Provides Zero Touch Integration with Fortinet's Security Fabric's Single Pane of Glass Management
- Predefined compliance checklist analyzes the deployment and highlights best practices to improve overall security posture

Security Fabric

- Enables Fortinet and Fabric-ready partners' products to provide broader visibility, integrated end-to-end detection, threat intelligence sharing, and automated remediation

Firewall	IPS	NGFW	Threat Protection	Interfaces
36 Gbps	10 Gbps	9.5 Gbps	7 Gbps	Multiple GE RJ45, GE SFP, and 10 GE SFP+ Slots

000027

DEPLOYMENT



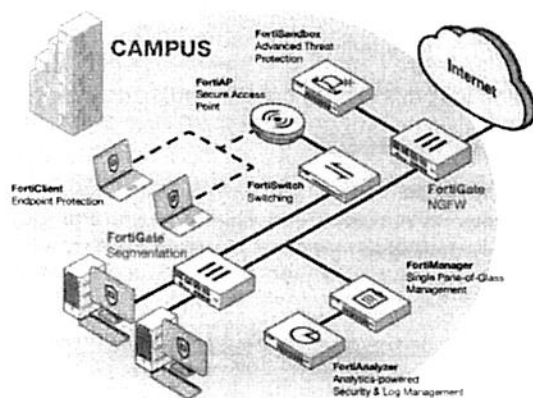
Next Generation Firewall (NGFW)

- Reduce the complexity and maximize your ROI by integrating threat protection security capabilities into a single high-performance network security appliance, powered by Fortinet's Security Processing Unit (SPU)
- Full visibility into users, devices, and applications across the entire attack surface and consistent security policy enforcement irrespective of asset location
- Protect against network exploitable vulnerabilities with industry-validated IPS that offers low latency and optimized network performance
- Automatically block threats on decrypted traffic using the industry's highest SSL inspection performance, including the latest TLS 1.3 standard with mandated ciphers
- Proactively block newly discovered sophisticated attacks in real-time with AI-powered FortiGuard Labs and advanced threat protection services included in the Fortinet Security Fabric



Secure Web Gateway (SWG)

- Secure web access from both internal and external risks, even for encrypted traffic at high performance
- Enhanced user experience with dynamic web and video caching
- Block and control web access based on user or user groups across URLs and domains
- Prevent data loss and discover user activity to known and unknown cloud applications
- Block DNS requests against malicious domains
- Multi-layered advanced protection against zero-day malware threats delivered over the web



Large Campus Network Deployment
(NGFW)



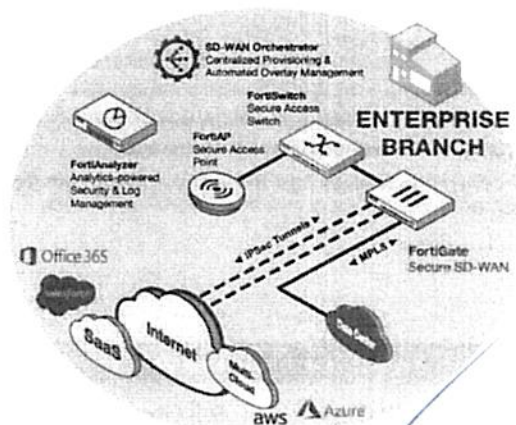
Secure SD-WAN

- Consistent business application performance with accurate detection, dynamic WAN path steering on any best-performing WAN transport
- Accelerated multi-cloud access for faster SaaS adoption with cloud-on-ramp
- Self-healing networks with WAN edge high availability, sub-second traffic switchover-based and real-time bandwidth compute-based traffic steering
- Automated overlay tunnels provides encryption and abstracts physical hybrid WAN making it simple to manage.
- Simplified and intuitive workflow with SD-WAN orchestrator for management and zero touch deployment
- Enhanced analytics both real-time and historical provides visibility into network performance and identifies anomalies
- Strong security posture with next generation firewall and real-time threat protection



IPS

- Purpose-built security processors delivering industry validated IPS performance with high throughput and low latency
- Deploy virtual patches at the network level to protect against network exploitable vulnerabilities and optimize protection time
- Deep packet inspection at wire speeds offers unparalleled threat visibility into network traffic including traffic encrypted with the latest TLS 1.3
- Proactively block newly discovered sophisticated attacks in real-time with advanced threat protection provided by the intelligence services of the Fortinet Security Fabric

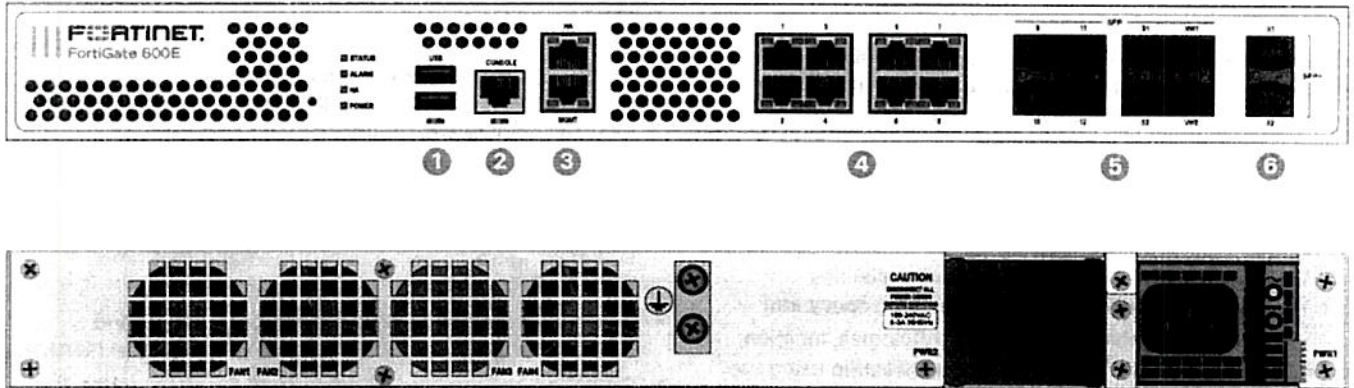


Enterprise Branch Deployment
(Secure SD-WAN)

HARDWARE

000028

FortiGate 600E/601E



Interfaces

1. 1x USB Port
2. 1x Console Port
3. 2x GE RJ45 MGMT/HA Ports
4. 8x GE RJ45 Ports
5. 8x GE SFP Slots
6. 2x 10 GE SFP+ Slots

Hardware Features



Powered by SPU

- Fortinet's 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
- VPN, CAPWAP and IP tunnel acceleration
- Anomaly-based intrusion prevention, checksum offload, and packet defragmentation
- Traffic shaping and priority queuing

Content Processor

Fortinet's ninth generation custom SPU CP9 content processor works outside of the direct flow of traffic and accelerates the inspection.

ABASI
Servicios Integrales S.A. de C.V.
Nayibit no. 83 - 101 Col. Roma México D.F.
Guatemala C.P. 06700 R.F.C. ASI0501142C2
Tel: +52 (55) 519-5193 www.abasi.com

000029

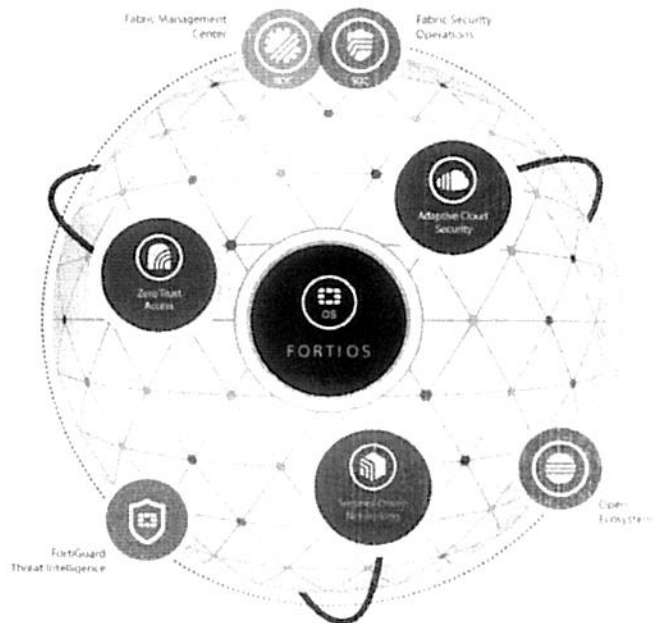
FORTINET SECURITY FABRIC

Security Fabric

The industry's highest-performing cybersecurity platform, powered by FortiOS, with a rich ecosystem designed to span the extended digital attack surface, delivering fully automated, self-healing network security.

- **Broad:** Coordinated detection and enforcement across the entire digital attack surface and lifecycle with converged networking and security across edges, clouds, endpoints, and users
- **Integrated:** Integrated and unified security, operation, and performance across different technologies, location, deployment options, and the richest ecosystem
- **Automated:** Context aware, self-healing network and security posture leveraging cloud-scale and advanced AI to automatically deliver near-real-time, user-to-application coordinated protection across the Fabric

The Fabric empowers organizations of any size to secure and simplify their hybrid infrastructure on the journey to digital innovation.



FortiOS™ Operating System

FortiOS, Fortinet's leading operating system enable the convergence of high performing networking and security across the Fortinet Security Fabric delivering consistent and context-aware security posture across network endpoint, and clouds. The organically built best of breed capabilities and unified approach allows organizations to run their businesses without compromising performance or protection, supports seamless scalability, and simplifies innovation consumption.

The release of FortiOS 7 dramatically expands the Fortinet Security Fabric's ability to deliver consistent security across hybrid deployment models of Hardware, Software, and Software As-a-Service with SASE and ZTNA, among others.

SERVICES



FortiGuard™ Security Services

FortiGuard Labs offer 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 and other network and security vendors, as well as law enforcement agencies.



FortiCare™ Services

Fortinet is dedicated to helping our customers succeed, and every year FortiCare services help thousands of organizations get the most from their Fortinet Security Fabric solution. We have more than 1,000 experts to help accelerate technology implementation, provide reliable assistance through advanced support, and offer proactive care to maximize security and performance of Fortinet deployments.



ABASI
Servicios Integrados S.A. de C.V.
Navya 100, B5 - 101 Col. Roma México D.F.
Cuauhtémoc C.P. 06700 R.F.C. ASIO501142C7
Tel. Fax 5912-1102 / 5219-5703 www.abasi.com.mx

SPECIFICATIONS

000030

	FG-600E	FG-601E
Interfaces and Modules		
Hardware Accelerated 10 GE SFP+ Slots	2	
Hardware Accelerated GE RJ45 interfaces	8	
Hardware Accelerated GE SFP Slots	8	
GE RJ45 Management Ports	2	
USB Ports	2	
RJ45 Console Port	1	
Onboard Storage	0	2 x 240 GB SSD
Included Transceivers		2x SFP (SX 1 GE)
System Performance — Enterprise Traffic Mix		
IPS Throughput ²	10 Gbps	
NGFW Throughput ^{2, 4}	9.5 Gbps	
Threat Protection Throughput ^{2, 5}	7 Gbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	36 / 36 / 27 Gbps	
IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP)	36 / 36 / 27 Gbps	
Firewall Latency (64 byte, UDP)	1.54 µs	
Firewall Throughput (Packet per Second)	40.5 Mpps	
Concurrent Sessions (TCP)	8 Million	
New Sessions/Second (TCP)	450,000	
Firewall Policies	10,000	
IPsec VPN Throughput (512 byte) ¹	20 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	2,000	
Client-to-Gateway IPsec VPN Tunnels	50,000	
SSL-VPN Throughput	7 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	10,000	
SSL Inspection Throughput (IPS, avg. HTTPS) ³	8 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) ³	5,500	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³	800,000	
Application Control Throughput (HTTP 64K) ³	15 Gbps	
CAPWAP Throughput (HTTP 64K)	18 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
Maximum Number of FortiSwitches Supported	96	
Maximum Number of FortiAPs (Total / Tunnel)	1,024 / 512	
Maximum Number of FortiTokens	5,000	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FG-600E	FG-601E
Dimensions and Power		
Height x Width x Length (inches)	17.5 x 17.0 x 15.0	
Height x Width x Length (mm)	44.45 x 432 x 380	
Weight	16.1 lbs (7.3 kg)	16.6 lbs (7.5 kg)
Form Factor	Rack Mount, 1 RU	
Power Source	100-240V, 50/60 Hz	
Power Consumption (Average / Maximum)	129 W / 244 W	
Current (Maximum)	6A@100V	
Heat Dissipation	832 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	10-90% non-condensing	
Noise Level	59 dBA	
Forced Airflow	Side and Front to Back	
Operating Altitude	Up to 9,843 ft (3,000 m)	
Compliance	FCC Part 15 Class A, RCM, 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.

1. IPsec VPN performance test uses AES256-SHA256.

2. IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.

3. SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

4. NGFW performance is measured with Firewall, IPS and Application Control enabled.

5. Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.



ABASI
Servicios Integrales S.A. de C.V.

Mayatl no. 83 - 101 Col. Roma Nueva D.F.
Cuauhtémoc C.P. 06700 R.F.C. AS030114C27
Tel. Fax 5912-5702 / 5219-5701 www.abasi.com.mx

05/18/2018
08:23
10/18/2018

000031

ORDERING INFORMATION

Product	SKU	Description
FortiGate 600E	FG-600E	2× 10 GE SFP+ slots, 10× GE RJ45 ports (including 1x MGMT port, 1x HA port, 8x switch ports), 8x GE SFP slots, SPU NP6 and CP9 hardware accelerated.
FortiGate 601E	FG-601E	2× 10 GE SFP+ slots, 10× GE RJ45 ports (including 1x MGMT port, 1x HA port, 8x switch ports), 8x GE SFP slots, SPU NP6 and CP9 hardware accelerated, 2× 240 GB onboard SSD storage.
Optional Accessories		
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FN-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Long Range	FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver, Extended Range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ RJ45 Transceiver Module	FN-TRAN-SFP+GC	10 GE SFP+ RJ45 transceiver module for systems with 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.
Optional Power Supply	SP-FG300E-PS	AC power supply for FG-300/301E, FG-400/401E, FG-500/501E, FG-600/601E, FAZ-200F/300F/800F and FMG-200F/300F.

BUNDLES



FortiGuard 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 one of these FortiGuard Bundles.

Bundles	360 Protection	Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiCare	ASE ¹	24×7	24×7	24×7
FortiGuard App Control Service	•	•	•	•
FortiGuard IPS Service	•	•	•	•
FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
FortiGuard Web and Video ² Filtering Service	•	•	•	•
FortiGuard Antispam Service	•	•	•	•
FortiGuard Security Rating Service	•	•	•	•
FortiGuard IoT Detection Service	•	•	•	•
FortiGuard Industrial Service	•	•	•	•
FortiConverter Service	•	•	•	•
SD-WAN Orchestrator Entitlement	•	•	•	•
SD-WAN Cloud Assisted Monitoring	•	•	•	•
SD-WAN Overlay Controller VPN Service	•	•	•	•
Fortinet SOCaas	•	•	•	•
FortiAnalyzer Cloud	•	•	•	•
FortiManager Cloud	•	•	•	•

1. 24×7 plus Advanced Services Ticket Handling 2. Available when running FortiOS 7.1

FORTINET

ABASI
Servicios Integrados S.A de C.V.
Noyari no. 85 - 101 Col. Roma México D.F.
Cuidad de México C.P. 06700 R.F.C. AS0601142C7
Tel. Fax 5912-5702 / 5219-5703 www.abasi.com.mx

www.fortinet.com

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other marks contained herein 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 factors 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 or licensee who explicitly states that the defined 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 only, all Fortinet marks will be limited to performance in the same test conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any warranties, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, terminate, or otherwise alter, without notice, the content and/or version of the publication and/or product at any time.

FORTINET.

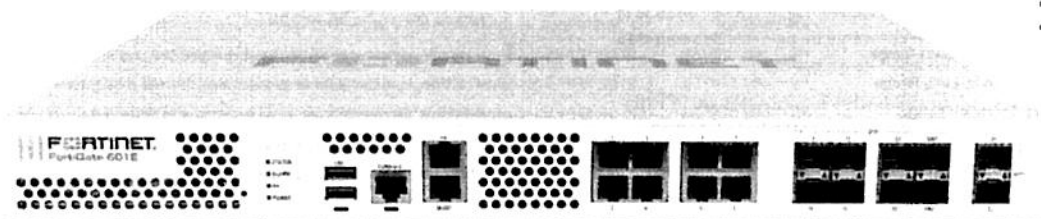
FICHA DE DATOS

FortiGate® Serie 600E

FG-600E y FG-601E

Firewall de próxima
generación Secure SD-WAN
Puerta de enlace web segura
IPS

000032



La serie FortiGate 600E proporciona una solución SD-WAN segura, escalable y centrada en la aplicación con capacidades de firewall de próxima generación (NGFW) para empresas medianas y grandes implementadas a nivel de campus o sucursales. Protege contra las amenazas cibernéticas con aceleración de sistema en un chip y SD-WAN segura líder en la industria en una solución simple, asequible y fácil de implementar. El enfoque de redes basadas en la seguridad de Fortinet proporciona una estrecha integración de la red a la nueva generación de seguridad.

Seguridad

- Identifica miles de aplicaciones dentro del tráfico de red para una inspección profunda y aplicación de políticas granulares
- Protege contra malware, exploits y sitios web maliciosos en tráfico cifrado y no cifrado
- Prevenga y detecte ataques conocidos y desconocidos utilizando inteligencia de amenazas continua de los servicios de seguridad de FortiGuard Labs con tecnología de inteligencia artificial

Rendimiento

- Ofrece el mejor rendimiento de protección contra amenazas de la industria y latencia ultrabaja utilizando tecnología de procesador de seguridad (SPU) especialmente diseñada
- Proporciona un rendimiento y una protección líderes en la industria para el tráfico cifrado SSL.

Certificación

- Probado y validado de forma independiente para obtener la mejor eficacia y rendimiento de seguridad de su clase

Recibió certificaciones de terceros incomparables de NSS Labs

Redes

- Ofrece capacidades de red avanzadas que se integran a la perfección con la seguridad avanzada de capa 7 y los dominios virtuales (VDOM) para ofrecer una amplia flexibilidad de implementación, tenencia múltiple y utilización eficaz de los recursos.

- Ofrece una combinación flexible y de alta densidad de varias interfaces de alta velocidad para permitir el mejor TCO para los clientes para implementaciones de centros de datos y WAN

Gestión

- Incluye una consola de administración que es efectiva, fácil de usar y proporciona visibilidad y automatización de red integrales
- Proporciona integración Zero Touch con el panel único de administración de vidrio de Security Fabric de Fortinet
- La lista de verificación de cumplimiento predefinida analiza la implementación y destaca las mejores prácticas para mejorar la postura general de seguridad

Tela de seguridad

- Habilita los productos de socios preparados para Fortinet y Fabric para proporcionar una visibilidad más amplia, detección integrada de un extremo a otro, intercambio de inteligencia sobre amenazas y reparación automatizada

Cortafuegos	IPS	NGFW	Protección contra amenazas	Interfaces
36 Gbps	10 Gbps	9,5 Gbps	7 Gbps	Múltiples ranuras GE RJ45, GE SFP y 10 GE SFP +

ABASI
Servicios Integrados S.A. de C.V.

Nayarit no. 85 - 101 Col. Roma México D.F.
Cuauhtémoc C.P. 06700 R.F.C. ASI0301142C2
Tel. Fijo 5912-5702 / 5219-5703 www.abasi.com.mx

DESPLIEGUE

000033



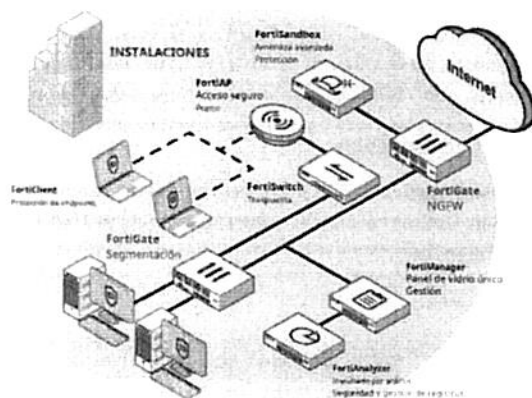
Próxima generación Cortafuegos (NGFW)

- Reduzca la complejidad y maximice su ROI integrando las capacidades de seguridad de protección contra amenazas en un solo dispositivo de seguridad de red de alto rendimiento, impulsado por la Unidad de procesamiento de seguridad (SPU) de Fortinet
- Visibilidad total de los usuarios, dispositivos y aplicaciones en toda la superficie de ataque y aplicación constante de políticas de seguridad independientemente de la ubicación de los activos.
- Protéjase contra las vulnerabilidades explotables de la red con IPS validado por la industria que ofrece baja latencia y rendimiento de red optimizado
- Bloquee automáticamente las amenazas en el tráfico descifrado utilizando el rendimiento de inspección SSL más alto de la industria, incluido el último estándar TLS 1.3 con cifrados obligatorios
- Bloquee de manera proactiva los ataques sofisticados recién descubiertos en tiempo real con los laboratorios FortiGuard con tecnología de inteligencia artificial y los servicios avanzados de protección contra amenazas incluidos en Fortinet Security Fabric



Puerta de enlace web segura (SWG)

- Asegure el acceso a la web frente a riesgos internos y externos, incluso para tráfico cifrado de alto rendimiento
- Experiencia de usuario mejorada con almacenamiento en caché web y de video dinámico
- Bloquear y controlar el acceso web en función de usuarios o grupos de usuarios en URL y dominios
- Evite la pérdida de datos y descubra la actividad del usuario en aplicaciones en la nube conocidas y desconocidas
- Bloquear solicitudes de DNS contra dominios maliciosos
- Protección avanzada de varias capas contra las amenazas de malware de día cero entregadas a través de la web



Implementación de red de campus grande
(NGFW)



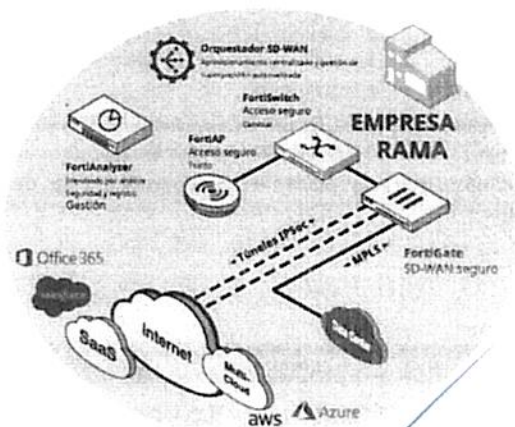
SD-WAN seguro

- Rendimiento constante de las aplicaciones empresariales con detección precisa, direccionamiento dinámico de la ruta WAN en cualquier transporte WAN de mejor rendimiento
- Acceso acelerado a múltiples nubes para una adopción de SaaS más rápida con nube en rampa
- Redes de recuperación automática con alta disponibilidad de borde WAN, dirección de tráfico basada en cómputo de ancho de banda en tiempo real y basada en conmutación de tráfico inferior a un segundo
- Los túneles de superposición automatizados proporcionan cifrado y abstraen la WAN híbrida física, lo que facilita su administración.
- Flujo de trabajo simplificado e intuitivo con SD-WAN orchestrator para la administración y la implementación sin intervención.
- El análisis mejorado, tanto en tiempo real como histórico, proporciona visibilidad del rendimiento de la red e identifica anomalías.
- Fuerte postura de seguridad con firewall de próxima generación y protección contra amenazas en tiempo real



IPS

- Procesadores de seguridad especialmente diseñados que ofrecen un rendimiento IPS validado por la industria con alto rendimiento y baja latencia
- Implemente parches virtuales a nivel de red para proteger contra vulnerabilidades explotables de la red y optimizar el tiempo de protección de la red.
- La inspección profunda de paquetes a velocidades de cable ofrece una visibilidad incomparable de las amenazas en el tráfico de la red, incluido el tráfico cifrado con el último TLS 1.3.
- Bloquee de forma proactiva los ataques sofisticados recién descubiertos en tiempo real con la protección avanzada contra amenazas proporcionada por los servicios de inteligencia de Fortinet Security Fabric

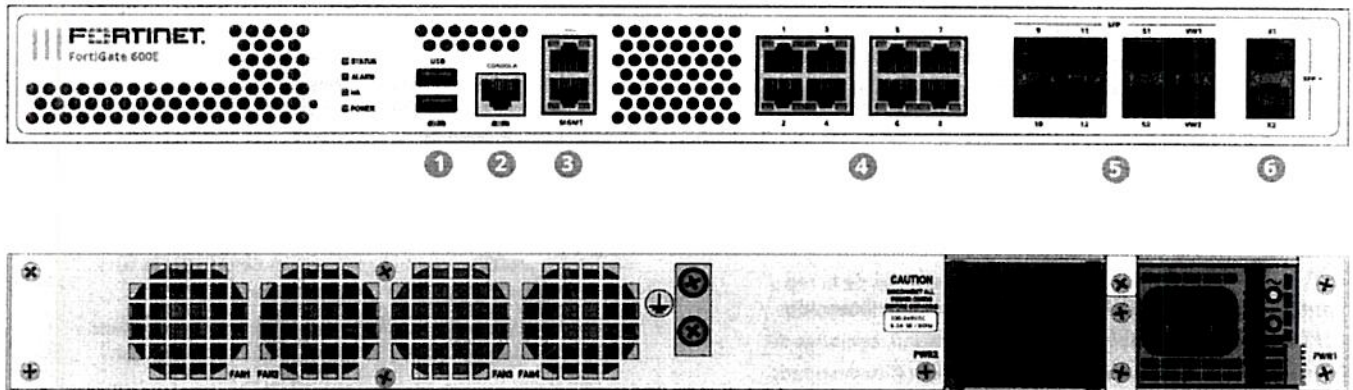


Implementación de sucursales empresariales
(SD-WAN seguro)

HARDWARE

FortiGate 600E / 601E

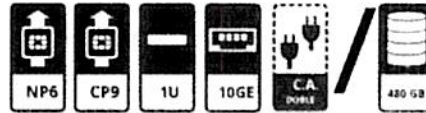
000034



Interfaces

1. 1x puerto USB
2. 1x puerto de consola
3. 2 puertos GE RJ45 MGMT / HA
4. 8 puertos GE RJ45
5. 8X Ranuras GE SFP
6. 2X 10 ranuras GE SFP +

Funciones de hardware



Desarrollado por SPU

- § Los procesadores SPU personalizados de Fortinet brindan 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 porque dependen de CPU de uso general, lo que genera una brecha de rendimiento peligrosa.
- § Los procesadores SPU proporcionan el rendimiento necesario para bloquear las amenazas emergentes, cumplir con rigurosas certificaciones de terceros y garantizar que su solución de seguridad de red no se convierta en un cuello de botella en la 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 superior del firewall para tráfico IPv4 / IPv6, SCTP y multidifusión con latencia ultrabaja
- § Aceleración de túneles VPN, CAPWAP e IP
- § Prevención de intrusiones basadas en anomalías, descarga de suma de comprobación y desfragmentación de paquetes
- § Conformación del tráfico y colas de prioridad

Procesador de contenido

El procesador de contenido SPU CP9 personalizado de novena generación de Fortinet funciona fuera del flujo directo de tráfico y acelera la inspección.

TEJIDO DE SEGURIDAD FORTINET

Tela de seguridad

La plataforma de ciberseguridad de mayor rendimiento de la industria, impulsada por FortiOS, con un rico ecosistema diseñado para abarcar la superficie de ataque digital extendida, brindando seguridad de red totalmente automatizada y con recuperación automática.

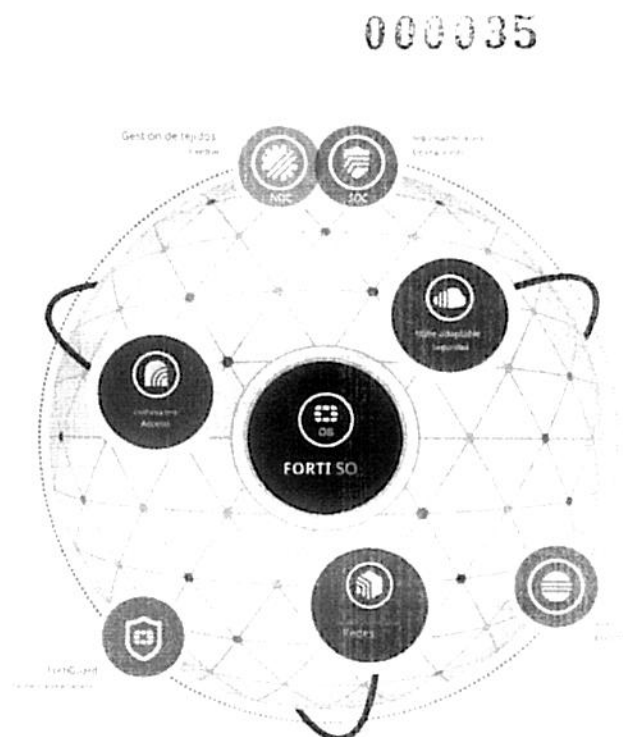
- § **Amplio:** Detección y aplicación coordinadas en todo el toda la superficie de ataque digital y el ciclo de vida con redes convergentes y seguridad en los bordes, las nubes, los puntos finales y los usuarios.
- § **Integrado:** Seguridad, operación y rendimiento integrados y unificados en diferentes tecnologías, ubicación, opciones de implementación y el ecosistema más rico
- § **Automatizado:** Red consciente del contexto, autorreparable y postura de seguridad que aprovecha la escala de la nube y la inteligencia artificial avanzada para brindar automáticamente una protección coordinada entre el usuario y la aplicación casi en tiempo real en toda la tela.

Fabric permite a las organizaciones de cualquier tamaño proteger y simplificar su infraestructura híbrida en el camino hacia la innovación digital.



FortiOS™ Sistema operativo

FortiOS, el sistema operativo líder de Fortinet, permite la convergencia de redes y seguridad de alto rendimiento en Fortinet Security Fabric, lo que brinda una postura de seguridad consistente y sensible al contexto en los puntos finales de la red y las nubes. Las mejores capacidades de su clase construidas orgánicamente y el enfoque unificado permiten a las organizaciones ejecutar sus negocios sin comprometer el rendimiento o la protección, admite una escalabilidad perfecta y simplifica el consumo de innovación.



SERVICIOS



FortiGuard™ Servicios de seguridad

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



FortiCare™ Servicios

Fortinet se dedica a ayudar a nuestros clientes a tener éxito, y cada año los servicios de FortiCare ayudan a miles de organizaciones a aprovechar al máximo su solución Fortinet Security Fabric. Contamos con más de 1,000 expertos para ayudar a acelerar la implementación de tecnología, brindar asistencia confiable a través de soporte avanzado y ofrecer atención proactiva para maximizar la seguridad y el rendimiento de las implementaciones de Fortinet.

ESPECIFICACIONES

000036

	FG-600E	FG-601E
Interfaces y módulos		
Ranuras 10 GE SFP + aceleradas por hardware	2	
Interfaces GE RJ45 aceleradas por hardware	8	
Ranuras SFP de GE aceleradas por hardware	8	
Puertos de administración RJ45 de GE	2	
Puertos USB	2	
Puerto de consola RJ45	1	
Almacenamiento a bordo	0	2 unidades M2 de 240 GB
Transceptores incluidos	2x SFP (SX 1 GE)	
Rendimiento del sistema: rendimiento de IPS de mezcla de		
tráfico empresarial	10 Gbps	
Rendimiento de NGFW	9.5 Gbps	
Rendimiento de protección contra amenazas	7 Gbps	
Rendimiento y capacidad del sistema		
Rendimiento del cortafuegos IPv4 (1518/512/64 bytes, UDP)	36/36/27 Gbps	
Rendimiento del cortafuegos IPv6 (1518/512/64 bytes, UDP)	36/36/27 Gbps	
Latencia del cortafuegos (64 bytes, UDP)	1.54 µs	
Rendimiento del cortafuegos (paquete por segundo)	40.5 Mpps	
Sesiones simultáneas (TCP)	8 millones	
Políticas de firewall de sesiones nuevas / segundas (TCP)	450,000 / 10,000	
Rendimiento de VPN IPsec (512 bytes)	20 Gbps	
Túneles VPN IPsec de puerta de enlace a puerta de enlace	2,000	
Túneles VPN IPsec de cliente a puerta de enlace	50,000	
Rendimiento de VPN SSL	7 Gbps	
Usuarios concurrentes de SSL-VPN (máximo recomendado, modo túnel)	10,000	
Rendimiento de inspección SSL (IPS, HTTPS promedio)	8 Gbps	
CPS de inspección SSL (IPS, HTTPS promedio)	5,500	
Sesión concurrente de inspección SSL (IPS, HTTPS promedio)	800,000	
Rendimiento de control de aplicaciones (HTTP 64K)	15 Gbps	
Rendimiento CAPWAP (HTTP 64K) Dominios virtuales (predeterminado / máximo)	18 Gbps / 10/10	
Número máximo de FortiSwitches admitidos	96	
Número máximo de FortiAP (total / túnel)	1,024 / 512	
Número máximo de configuraciones de alta disponibilidad de FortiTokens	5,000	
	Activo activo, activo-pasivo, agrupación	

	FG-600E	FG-601E
Dimensiones y potencia		
Alto x Ancho x Largo (pulgadas)	1.75 x 17.0 x 15.0	
Alto x Ancho x Largo (mm) Peso	44.45 x 432 x 380	
	16.1 libras (7.3 kg) 16.6 libras (7.5 kg)	
Factor de forma	Montaje en bastidor 1	
Fuente de alimentación	9U 100-240 V, 50/60 Hz	
El consumo de energía (Promedio / Máximo)	129 W / 244 W	
Corriente (máxima)	6A a 100 V	
Disipación de calor	532 BTU / h	
Fuentes de alimentación redundantes intercambiables en caliente	Opcional	
Entorno operativo y certificaciones		
Temperatura operativa	32 a 104 °F (0 a 40 °C)	
Temperatura de almacenamiento	31 a 158 °F (-35 a 70 °C)	
Humedad	10-90% sin condensación	
Nivel de ruido	59 dBA	
Flujo de aire forzado	Lateral y un aspirante hacia	
Altitud operativa	hasta hasta 9,843 pies (3,000 m)	
Cumplimiento	FCC Parte 15 Clase A, RCM, VCCI, CE, UL / cUL, CB	
Certificaciones	Laboratorios ILSA: Firewall, IPsec, IPS, Antivirus, SSL VPN, USGv6 / IPv6	

Nota: Todos los valores de rendimiento son "hasta" y varían según la configuración del sistema.

1. La prueba de rendimiento de IPsec VPN utiliza AES256-SHA256.

2. IPS (Enterprise Mix), Application Control, NGFW y Threat Protection se miden con el registro habilitado.

3. Los valores de rendimiento de la inspección SSL utilizan un promedio de sesiones HTTPS de diferentes conjuntos de cifrado.

4. El rendimiento de NGFW se mide con Firewall, IPS y Application Control habilitados.

5. El rendimiento de Threat Protection se mide con Firewall, IPS, Application Control y Malware Protection habilitados.



Nayarit no. 85 - 101 Col. Roma México D.F.
Cuculméc C.P. 04700 R.F.C. AS0501147C2
Tel. Fax 5912-5702 / 5219-5793 www.abasi.com.mx

000036
000 000
100 000 000

000037

INFORMACIÓN SOBRE PEDIDOS

Producto	SKU	Descripción
FortiGate 600E	FG-600E	2 ranuras 10 GE SFP + 10 puertos GE RJ45 (incluido 1 puerto MGMT, 1 puerto HA, 8 puertos de conmutador), 8 ranuras GE SFP, SPU NP6 y CP9 acelerado por hardware
FortiGate 601E	FG-601E	2 ranuras 10 GE SFP + 10 puertos GE RJ45 (incluido 1 puerto MGMT, 1 puerto HA, 8 puertos de conmutador), 8 ranuras GE SFP, SPU NP6 y CP9 acelerado por hardware, 2 unidades de almacenamiento SSD integrado de 240 GB
Accesorios Opcionales		
1 módulo transceptor GE SFP LX	FN-TRAN-LX	1 módulo transceptor GE SFP LX para todos los sistemas con ranuras SFP y SFP / SFP +
1 módulo transceptor GE SFP RJ45 1	FN-TRAN-GC	1 módulo transceptor GE SFP RJ45 para todos los sistemas con ranuras SFP y SFP / SFP + 1
módulo transceptor GE SFP SX	FN-TRAN-SX	módulo transceptor GE SFP SX para todos los sistemas con ranuras SFP y SFP / SFP +
Módulo transceptor 10 GE SFP +, módulo transceptor	FN-TRAN-SFP + SR	Módulo transceptor 10 GE SFP +, corto alcance para todos los sistemas con ranuras SFP + y SFP / SFP +
10 GE SFP + de corto alcance, transceptor 10 GE SFP +	FN-TRAN-SFP + LR	Módulo transceptor 10 GE SFP +, largo alcance para todos los sistemas con ranuras SFP + y SFP / SFP +
de largo alcance, módulo transceptor 10 GE SFP +	FN-TRAN-SFP + ER	Módulo transceptor 10 GE SFP +, rango extendido para todos los sistemas con ranuras SFP + y SFP / SFP +
RJ45 de rango extendido	FN-TRAN-SFP + GC	Módulo transceptor 10 GE SFP + RJ45 para sistemas con ranuras SFP +
Cable de conexión directa activo SFP + 10 GE, 10 m / 32.8 pies	SP-CABLE-ADASFP +	Cable de conexión directa activo 10 GE SFP +, 10 m / 32.8 pies para todos los sistemas con ranuras SFP + y SFP / SFP +
Fuente de alimentación opcional	SP-FG300E-PS	Fuente de alimentación CA para FG-300 / 301E, FG-400 / 401E, FG-500 / 501E, FG-600 / 601E, FAZ-200F / 300F / 600F y FMG-200F / 300F

MANOJOS

FortiGuard
Manajo

FortiGuard Labs ofrece una serie de servicios de inteligencia de seguridad para aumentar FortiGate plataforma de firewall. Usted puede optimizar fácilmente las capacidades de protección de su FortiGate con uno de estos paquetes FortiGuard.

manojos	360 Protección	Empresa Protección	Amenaza unificada Protección	Amenaza avanzada Protección
FortiCare		24x7	24x7	24x7
Servicio de control de aplicaciones de	+	+	+	+
FortiGuard Servicio IPS de FortiGuard	+	+	+	+
FortiGuard Advanced Malware Protection (AMP): antivirus, malware móvil, botnet, CDR, protección contra ataques de virus y servicio en la nube FortiSandbox	+	+	+	+
FortiGuard Web y video: Servicio de filtrado	+	+	+	+
Servicio antispam FortiGuard	+	+	+	+
Servicio de clasificación de seguridad de	+	+	+	+
FortiGuard Servicio de detección de IoT de	+	+	+	+
FortiGuard Servicio Industrial de FortiGuard	+	+	+	+
Servicio de FortiConverter	+	+	+	+
Titularidad de SD-WAN Orchestrator	+	+	+	+
Monitoreo asistido en la nube SD-WAN	+	+	+	+
Controlador de superposición SD-WAN Servicio	+	+	+	+
VPN Fortinet SOCAas	+	+	+	+
FortiAnalyzer Cloud	+	+	+	+
Nube de FortiManager	+	+	+	+

1. 24x7 más gestión de tickets de servicios avanzados

2. Disponible cuando se solicita FortiOS 7.0

FORTINET

ABASI
Servicios Integrados S. de C.V.Nayarit no. 85 - 101 Col. Roma México D.F.
Guadalupe C.P. 06700 México A.S. 50114702
Tel. Pbx 5912-5702 / 5219-5703 www.abasi.com

www.fortinet.com

FortiManager

Available in:



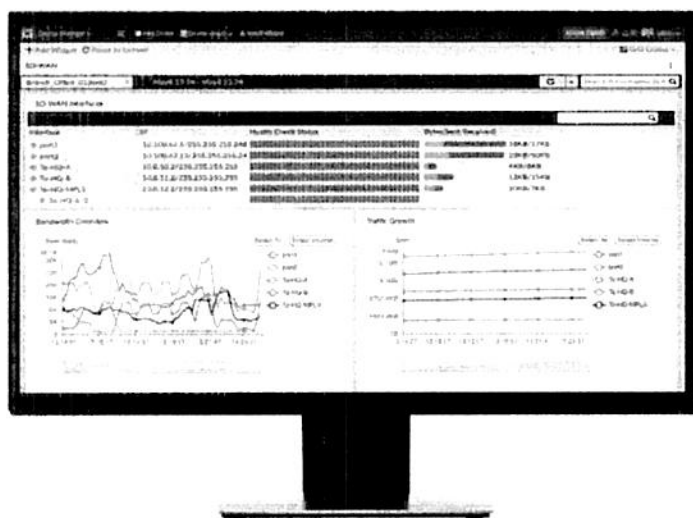
FortiManager

FortiManager

FortiManager

FortiManager provides Automation-Driven Centralized Management of your Fortinet devices from a single console for full administration and visibility of your network devices through streamlined provisioning and innovative automation tools.

Integrated with Fortinet's Security Fabric, the advanced security architecture and FortiManager's Automation Driven Network Operations capabilities provide a solid foundation to secure and optimize your network security.



Single-Pane Management streamlines centralized policy and object management, automatic revision history and control, and enhanced RBAC features for script management and IPS management with role separation.

Security Fabric Automation simplifies the ZTP deployment process for SD-Branch (FortiGates and access devices) with powerful templates that directly utilize meta-variables for scalable provisioning to thousands of sites.

NOC Cloud Services offers the FortiManager platform as a service with new management extensions that can be pulled and installed from the cloud.

000038

Key Features

- Centrally manage thousands of FortiGates, policies and objects as well as FortiSwitches, FortiAP, and FortiExtender. Provide signature updates to FortiGate, FortiMail, FortiSandbox, and FortiClient
- Centralized distribution of security content and signatures through the use of the built-in FortiGuard module
- Use templates for firmware upgrades and zero-touch provisioning for Secure SD-WAN, setting up IPSec VPN, static route, and FortiExtender for fast and easy configuration
- Reduce complexity and costs by leveraging automated REST API, scripts, connectors, and automation stitches
- Automate workflows and configurations for Fortinet firewalls, switches, and wireless infrastructure
- Separate customer data and manage domains leveraging ADOMs to be compliant and operationally effective
- High Availability to automate backups for up to five nodes with streamlined software and security updates for all managed devices



ABASI
Servicios Integrados S.A. de C.V.

Nayarit no. 85 - 101 Col. Roma México D.F.
Cuidatémoc C.P. 06700 R.F.C. AS05011720
Tel. Fax 5912-5702 / 5219-5703

FEATURE HIGHLIGHTS

000039

Single Pane Management

FortiManager's Single Pane Management provides centralized management and provisioning strategy built around Fortinet's Security Fabric that tightly integrates an organization's network infrastructure and security architecture to apply access control, segmentation and consistent protection of devices, applications and users.

Device Configuration and Provisioning

FortiManager expands the network administrator's capabilities with a rich set of tools to centrally manage up to 100,000 devices including FortiGates, FortiExtender, FortiSwitch, FortiAPs, SD-WAN and more.

Collectively configure device settings and use new enhanced CLI templates with variables, and provisioning templates to assign firmware and policy packages from a single console, including policy and object revision history for auditing.

FortiManager includes extended SSL and Certificate support for enhanced ssl-ssh-profile configuration, as well as Restricted IPS Admin Profiles to support customers who are transitioning and upgrading from dedicated IPS solutions to Fortinet products.

Automated device configuration backups and revision control make daily administrative tasks easy, with change tracking in the enhanced Event Log view for review of configuration and change detail for auditing & compliance.

FortiManager also now enables Admins to configure and assign custom commands on FortiSwitch and configure MCLAG from the FortiSwitch Manager.

Multi-Tenancy and Role-Based Administration

FortiManager provides granular device and role-based administration for clear visibility of every device and user on the network, facilitating zero-trust, multi-tenancy deployments for large enterprises and a hierarchical objects database for re-use of common configurations to serve multiple customers.

ADOMs (administrative domains) are used to manage independent security environments, each with its own security policies and configuration database. The intuitive GUI makes it easy for Admins to view, create, clone, and manage ADOMs, define global Objects, Policies and Security Profiles across ADOMs, with Health Check to ensure ADOMs are in sync.

FortiManager's zero-touch deployment utilizes templates to provision devices for quick mass deployments, and supports firmware version enforcement for defining firmware requirements for installs and upgrades.

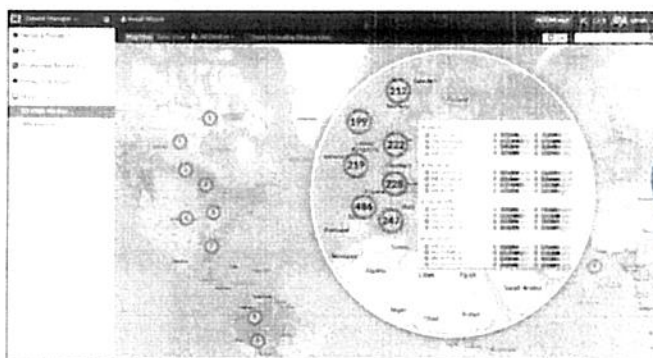
FortiManager's new IPS admin is a restricted user role for performing only IPS related object configuration and installations. Admin users can also be assigned per-admin UI background themes, for unique visual associations.

Security Policy and Objects Management

FortiManager's Policy & Objects views enable Admins to centrally manage and configure device policies, including updating network settings, antivirus definitions, intrusion protection signatures, access rules, and software updates.

The global policy feature allows MSSP and PaaS providers to apply ADOM level header/footer policies for updating all policy packages or select packages. Policy and Objects views now include a revision history, providing an account of admins who have made changes, change date, summary, and a mandatory change notes field to capture change reason.

The per-policy lock feature allows admins to control the policy change by implicitly locking a policy rule when a policy is changed. Admins can also group commonly used policies in a policy block and insert in different Policy Packages.



Secure SD-WAN

FortiManager offers powerful SD-WAN management capabilities using intuitive workflows and simplified provisioning at scale. Leverage application centric SD-WAN business policies to fine-tune traffic steering decisions based on performance SLA targets for each WAN provider.

Admins can use the SD-WAN monitoring dashboard to keep an eye on application performance and bandwidth utilization per WAN link, and integrate FortiAnalyzer for enhanced analytics views and SD-WAN assessment reports.



Horizonte no. 83 - 101 Col. Roma México D.F.
Código Postal: 06700 R.F.C. AS0501142C2
Tel: +52 (55) 5219-5701 - www.abasi.com

FEATURE HIGHLIGHTS

Manage and Monitor with Deep Visibility

FortiManager's Device Manager provides full visibility, access and management of Fortinet managed devices, interfaces, scripts, templates, automation, monitors, users, settings, and more. Install, edit and delete policies, monitor the health of FortiGate devices through the customizable dashboards and widgets to see resource usage, network status of DHCP, IPsec and SSL VPN, routing, traffic shapers, and more. Easily navigate the hierarchical tree with categories for Managed Devices, Logging Devices, Unauthorized Devices, and customize to display as a table, folder, or a map view.

Use Fabric View to check Security Fabric Ratings and configurations of FortiGate devices or groups. Access vital security and network statistics, as well as real-time monitoring and topology information to provide visibility into network and user activity. Add a FortiAnalyzer appliance or VM for powerful analytics and enhanced Fabric view with asset and identity info, additional data mining, statistical analysis, and graphical reporting capabilities.

FortiManager High Availability (HA)

FortiManager high availability (HA) provides enhanced reliability, data protection, redundancy, and operational performance to ensure agreed uptimes and availability. In the event that the operating FortiManager unit fails, a backup FortiManager (one primary and up to four secondary) unit can take the place of the failed unit, making sure that companies have seamless access to their devices and business-critical network operations.

The FortiManager HA Cluster Wizard now also supports defining a hostname for each cluster member, exposing the session-pick option from GUI, as well as the option to dedicate an interface for management of the individual cluster member.

000040

Security Fabric Automation

Network and Security Operations Visibility (NOC/SOC)

FortiManager supports NOC-SOC workflows to assist network teams in maintaining optimal performance. Automated data exchanges between security (SOC) workflows and operational (NOC) workflows, create a single, complete workflow that not only saves time, but also provides the capacity to complete additional incident response activities.

Integration with FortiAnalyzer magnifies visibility with advanced data visualization and analytics helping analysts quickly connect-the-dots, identify threats, and simplify the expeditious configuration and security of managed devices.



Automation and Connectors

Utilize Automation and Orchestration and optimize with FortiManager through querying of FortiGates and the Fortinet Security Fabric via application programming interfaces (APIs) to actively collect and share network information and broaden end-to-end visibility and response.

FortiManager reduces complexity and cost by leveraging REST API, scripts, connectors, and FortiGate automation stitches to automate time-intensive processes and accelerate workflows for offloading NOC-SOC, reducing administrative tasks, and addressing talent shortages. Admins can automate common tasks such as provisioning of FortiGates and configuring new or existing devices.

Join Fortinet Developer Network (FNDN) for exclusive access to articles, how-to content for automation and customization, community-built tools, scripts, and sample code.

000041

FEATURE HIGHLIGHTS

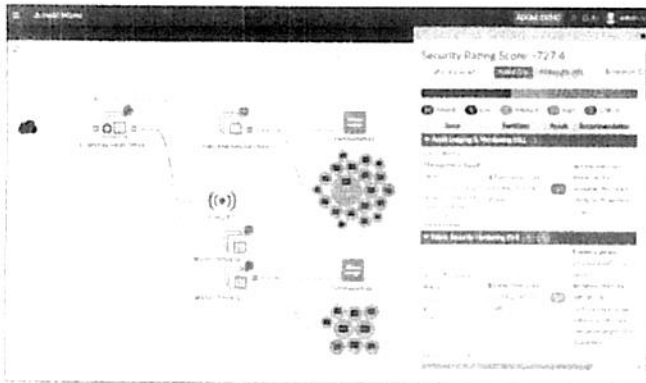
NOC Cloud Services

Management Extensions

FortiManager's Management Extensions pane allows rapid expansion of the Single Pane to manage more Security Fabric products. The built-in engine runs containerized management extension applications (MEAs), pulled from FortiGuard.

FortiManager's management extensions include modules for the following:

- SD-WAN Orchestrator for all configuration, management, and monitoring of FortiGates on your SD-WAN network
- FortiPortal for cloud-based security and log management, allowing Managed Security Service Providers to delegate controlled access to device configuration and analytics
- FortiWLM to monitor, operate, and administer wireless networks on FortiGates that are managed by FortiManager
- FortiSigConverter to convert Snort network intrusion detection and intrusion prevention system rules to Fortinet supported IPS signatures directly into FortiManager
- FortiAuthenticator for identity and access management, allowing admins to provide access to protected network assets, and track user activity and compliance with security policies
- FortiSOAR – Full Security Orchestration, Automation and Response features with a subscription to FortiSOAR



Dynamic Cloud Security

Fortinet Cloud Security and Management Solutions offers customers a PaaS based delivery option for central management of FortiGate devices from a cloud-based FortiManager.

FortiManager Cloud provides an automation-driven and single pane-of-glass management capability that is easy-to-implement, easy-to-manage, flexible, and scalable for an organization's business growth.

Use the single Sign-on Portal to manage Fortinet NGFW and SD-WAN. The built-in cloud-init service allows Administrators to easily customize a prepared image of a virtual installation for KVM, AZURE, and AWS. FortiManager's cloud-based network management helps customers streamline FortiGate provisioning with automation-enabled management of Fortinet devices.

With the FortiCloud Premium subscription, customers can easily enable the FortiManager Cloud service with the 360 Protection bundle or by purchasing it a-la-carte, providing access to manage a range of Fortinet solutions and services for simplified network and security management. Customers and partners can easily access their FortiManager Cloud from their FortiCloud Single-Sign-On Portal.

Security Fabric and Third Party Integration

FortiManager integrates with ITSM to seamlessly mitigate security incidents and events, apply configuration changes, and update policies. Integration with FortiAnalyzer provides in-depth discovery, analysis, prioritization, and reporting of network security events.

Use fabric connectors to facilitate connections with third-party vendors like vCenter, pxGrid, Clearpass, OCI, ESXi, AWS, and others to share and exchange data.

FortiManager's workflow for audit and compliance enables review, approval, and auditing policy changes including automating processes for policy compliance, policy lifecycle management, and enforced workflow to reduce risk.

VIRTUAL OFFERINGS

FortiManager VM

FortiManager Virtual Machines are a virtual version of the hardware appliance and are designed to run on many virtualization platforms, offering all the latest features of the FortiManager appliance. They allow organizations to centrally manage any number of Fortinet Network Security Fabric devices and scale from several to thousands, supporting centralized management, best practices compliance, and automated workflows to deliver superior protection against threats. FortiManager VMs are available in both a subscription and perpetual offering.

FortiManager VM-S

The new FortiManager VM Subscription license model consolidates the VM product SKU and the FortiCare Support SKU into one single SKU to simplify the product purchase, upgrade, and renewal.

000113

The FortiManager S-Series SKUs come in stackable subscriptions to manage 10, 100, and 1,000 devices/ vdoms so that multiple units of this SKU can be purchased at a time to increase the number of devices/ vdoms as needed. This SKU can also be purchased together with other FMG VM-S SKUs to expand the total number of devices/ vdoms.

FortiManager VM

Fortinet offers the FortiManager VM in a stackable license model. This software-based version of the FortiManager hardware appliance is designed to run on many virtualization platforms which allows you to expand your virtual solution as your environment expands. The FortiManager virtual appliance family minimizes the effort required to monitor and maintain your network and offers all the features of the FortiManager hardware appliance.

SPECIFICATIONS

FORTIMANAGER VIRTUAL APPLIANCES	FMG-VM-10-UG	FMG-VM-100-UG	FMG-VM-1000-UG	FMG-VM-5000-UG
Capacity				
Devices/VDOMs (Maximum) ^{1,2}	10 *	100 *	1,000 *	5,000 *
Storage Capacity	200 GB	1 TB	4 TB	8 TB
GB/Day of Logs ²	2	5	10	25
Chassis Management	✓	✓	✓	✓
Virtual Machine				
Hypervisor Support	Up-to-date hypervisor support can be found in the release notes for each FortiManager version. Visit https://docs.fortinet.com/product/fortimanager/ and find the Release information at the bottom section. Go to "Product Integration and Support" → "FortiManager [version] support" → "Virtualization"			
vCPU Support (Minimum / Maximum)	4 / Unlimited			
Network Interface Support (Min / Max) *	1 / 4			
Storage Support (Minimum / Maximum)	100 GB / 16 TB			
Memory Support (Minimum / Maximum)	8 GB / Unlimited for 64-bit			
High Availability Support	Yes			

1 Each Virtual Domain (VDM) operating on a physical or virtual device counts as one (1) licensed network device.

2 Storage Capacity and GB/Day of Logs are not stackable. These values represent the maximum available with purchased license.

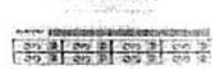
3 *Indicates Device Add-On License available.

4 VM supports up to 12 vNIC interfaces/ports. Applicable to 6.4.3+. Actual consumable numbers vary depending on cloud platforms.

ABASI
Servicios Integrados S.A. de C.V.
Hoytall no. 86 - 101 Col. Roma México D.F.
Código Postal: 06700 P.C. A30501142C2
Tel. Fax 5912-5702 / 5219-3703 www.abasi.com

SPECIFICATIONS

000043



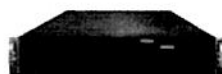
FORTIMANAGER APPLIANCES	FMG-200G	FMG-300F	FMG-400G
Capacity and Performance			
Devices/VDOMs (Maximum) ¹	30	100	150
Sustained Log Rates	50	50	50
GB/Day	2	2	2
Hardware Specifications			
Storage Capacity	8 TB (2 x 4 TB)	16 TB (4 x 4 TB)	32 TB (8 x 4 TB)
Usable Storage (after RAID)	4 TB	8 TB	24 TB
RAID Levels Supported	RAID 0/1	RAID 0/1s/5.5s/10	RAID 0/1s/5.5s/6.6s/10/50/60
Default RAID Level	1	10	50
Hardware Form Factor	1 RU Rackmount	1 RU Rackmount	2 RU Rackmount
Total Interfaces	4xRJ45 GE	4 x GE RJ45, 2 x SFP	4 x GE RJ45, 2 x SFP
Console Port	RJ45	RJ45	RJ45
Removable Hard Drives	No		
Redundant Hot Swap Power Supplies	No		
Chassis Management			
Dimensions			
Height x Width x Length (inches)	17.3 x 17.24 x 16.38	17.5 x 17.44 x 22.16	3.5 x 17.5 x 22.2
Height x Width x Length (cm)	4.4 x 43.8 x 41.6	4.4 x 44.3 x 56.3	8.9 x 44.5 x 56.5
Weight	22.5 lbs (10.2 kg)	28.6 lbs (13.0 kg)	35.27 lbs (16 kg)
Environment			
AC Power Supply	100-240V 50-60 Hz	100-240V AC, 50-60 Hz	100-240V AC, 50-60 Hz
Power Consumption (Average / Maximum)	90W / 99 W	108W / 186 W	140 / 182 W
Heat Dissipation	337.8 BTU/h	634 BTU/h	621 BTU/h
Operating Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Storage Temperature	-13-167°F (-25-75°C)	-31-158°F (-35-70°C)	-4-167°F (-20-75°C)
Humidity	20 to 90% non-condensing	20 to 90% non-condensing	5-95% non-condensing
Operating Altitude	Up to 7,400 ft (2,250 m)	Up to 7,400 ft (2,250 m)	Up to 7,400 ft (2,250 m)
Compliance			
Safety Certifications	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB

¹ Each Virtual Domain (VDOM) operating on a physical or virtual device counts as one (1) licensed network device.
² Optional Policies and high availability support available on all models.
³ Optional redundant AC power supply, not included.

ABASI
 Network Integration Sdn Bhd
 No. 11, Jln. 88, 101, C-1, Bangi, Selangor D.F.
 43000 Kajang, Malaysia
 Tel: +603-8921 1111 Fax: +603-8921 1112
 Email: info@abasi.com.my www.abasi.com.my

SPECIFICATIONS

000044



FORTIMANAGER APPLIANCES	FMG-1000F	FMG-2000E	FMG-3000G
Capacity and Performance			
Devices/VDOMs (Maximum) ^{1,4}	1000	1,200	4,000+
Sustained Log Rates	50	50	150
GB/Day	2	2	10
Hardware Specifications			
Storage Capacity	32 TB (8 × 4TB)	36 TB (12 × 3 TB)	64 TB (16 × 4TB)
Usable Storage (after RAID)	24 TB	30 TB	56 TB
RAID Levels Supported	RAID 0/1, 5, 6, 10/50/60	RAID 0/1, 5, 6, 10/50/60	RAID 0/1, 5, 6, 10/50/60
Default RAID Level	50	50	50
Hardware Form Factor	2 RU Rackmount	2 RU Rackmount	3 RU Rackmount
Total Interfaces	2 × RJ45 10G ports, 2 × SFP+ ports	4 × GE, 2 × 10 GE SFP+	2 × GbE RJ45 ports, 2 × 25GbE SFP28
Console Port	DB-9	DB-9	DB-9
Removable Hard Drives	✓	✓	✓
Redundant Hot Swap Power Supplies	✓	✓	✓
Chassis Management	✓	✓	✓
Dimensions			
Height x Width x Length (inches)	3.5 × 17.2 × 25.6	3.5 × 17.2 × 25.6	5.2 × 17.2 × 25.5
Height x Width x Length (cm)	8.9 × 43.7 × 65.0	8.9 × 43.7 × 64.8	13.2 × 44.0 × 65.0
Weight	34 lbs (15.42 kg)	58 lbs (26.3 kg)	65.5 lbs (30.15 kg)
Environment			
AC Power Supply	100-240V AC, 50-60 Hz	100-240V AC, 50-60 Hz	100-127V~/10A, 200-240V~/5A Hz
Power Consumption (Average / Maximum)	192.5W/275 W	293.8W/354 W	449W/541 W
Heat Dissipation	920 BTU/h	1209 BTU/h	1846.5 BTU/h
Operating Temperature	50-95°F (10-35°C)	50-95°F (10-35°C)	32-104°F (0-40°C)
Storage Temperature	-40-140°F (-40-60°C)	-40-158°F (-40-70°C)	-40-167°F (-20-75°C)
Humidity	8-90% non-condensing	8-90% non-condensing	5-95% non-condensing
Operating Altitude	Up to 7,400 ft (2,250 m)	Up to 7,400 ft (2,250 m)	Up to 7,400 ft (2,250 m)
Compliance			
Safety Certifications	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST

¹ Each Virtual Domain (VDOM) operating on a physical or virtual device counts as one (1) licensed network device.

Global Policies and high availability support available on all models.

⁴ + Indicates Device Add-On License available



ABASI
Sociedad Anónima S.A. de C.V.

Nayarit no. 85-101 C.A. P.O. Box 14200 D.F.
Cuahuatmuc C.P. 06700 R.F.C. ASI0301142C2
Tel. Fax 5712-5702 / 5219-1703 - www.abasi.com.mx

ORDER INFORMATION

000045

PRODUCT	SKU	DESCRIPTION
FortiManager	FMG-200G	Centralized management appliance — 4xRJ45 GE, 8 TB storage, up to 30x Fortinet devices/virtual domains
	FMG-300F	Centralized management appliance — 4x GE RJ45, 2xSFP, 16 TB storage, up to 100x Fortinet devices/virtual domains
	FMG-400G	Centralized management appliance — 4 x GE RJ45, 2 x SFP, 32 TB storage, up to 150x Fortinet devices/Virtual Domains
	FMG-1000F	Centralized management appliance — 2x RJ45 10G, 2x SFP+ slots, 32 TB storage, up to 1000x Fortinet devices/virtual domains
	FMG-2000E	Centralized management appliance — 4x GE RJ45, 2x 10 GE SFP+ slots, 36 TB storage, dual power supplies, manages up to 1,200 Fortinet devices/virtual domains
	FMG-3000G	Centralized management appliance — 2 x GbE RJ45 ports, 2x 25GbE SFP28, 64 TB storage, dual power supplies, manages up to 4,000 Fortinet devices/virtual domains
FortiManager-VM Subscription License with Support and BPS	FC1-10-FMGVS-448-01-DD	Subscription license for 10 devices/vdms managed by FortiManager VM S-series 24x7 FortiCare support plus FortiCare Best Practice services included
	FC2-10-FMGVS-448-01-DD	Subscription license for 100 devices/vdms managed by FortiManager VM S-series 24x7 FortiCare support plus FortiCare Best Practice services included
	FC3-10-FMGVS-448-01-DD	Subscription license for 1000 devices/vdms managed by FortiManager VM S-series 24x7 FortiCare support plus FortiCare Best Practice services included
FortiManager-VM	FMG-VM-10-UG	Upgrade license for adding 10 Fortinet devices/Virtual Domains; allows for total of 2 GB/Day of Logs and 200 GB storage capacity
	FMG-VM-100-UG	Upgrade license for adding 100 Fortinet devices/Virtual Domains; allows for total of 5 GB/Day of Logs and 1 TB storage capacity
	FMG-VM-1000-UG	Upgrade license for adding 1,000 Fortinet devices/Virtual Domains; allows for total of 10 GB/Day of Logs and 4 TB storage capacity
	FMG-VM-5000-UG	Upgrade license for adding 5,000 Fortinet devices/Virtual Domains; allows for total of 25 GB/Day of Logs and 8 TB storage capacity
FortiManager-Cloud*	FC-10-[FortiGate Model Code]-179-02-DD	Cloud-based Central Management & Orchestration Service for FortiGate
	FC-10-[FortiGate Model Code]-841-02-DD	360 Protection (FMG/FAZ Cloud, FortiCloud SOCaaS, IPS, AMP, App Ctrl, Web & Video Filtering, AS, Security Rating, IoT Detection, Industrial Security, SD-WAN Orchestrator, SD-WAN Cloud Monitoring, FortiConverter Svc, and ASE FortiCare)
	FC-10-[FortiGate VM Model Code]-842-02-DD	360 Protection (FMG/FAZ Cloud, FortiCloud SOCaaS, IPS, AMP, App Ctrl, Web & Video Filtering, AS, Security Rating, IoT Detection, Industrial Security, SD-WAN Orchestrator, SD-WAN Cloud Monitoring, FortiConverter Svc, and ASE FortiCare)
	FC1-10-MVCLD-227-01-DD	Subscription for 10 devices/vdms managed by FortiManager Cloud. 24x7 FortiCare support included
	FC2-10-MVCLD-227-01-DD	Subscription for 100 devices/vdms managed by FortiManager Cloud. 24x7 FortiCare contract is included
	FC3-10-MVCLD-227-01-DD	Subscription for 1000 devices/vdms managed by FortiManager Cloud. 24x7 FortiCare support included
Hardware Bundle	FMG-[Hardware Model]-BDL-447-DD	Hardware plus 24x7 FortiCare and FortiCare BPS.
FortiManager Device Upgrade License	FMG-DEV-100-UG	FortiManager device upgrade license for adding 100 Fortinet devices/vdms (3000 series and above - hardware only)

* Requires FortiCloud Premium Account license

NOTE

For hardware models, the default number of ADOMs can be found in the Release Notes on docs.fortinet.com
 For FortiManager VM Subscription licenses 5 ADOMs are included. Additional ADOMs can be purchased.



FORTINET.

www.fortinet.com

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet, FortiGate, FortiCare and FortiGuard, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names hereof may also be registered and/or common law trademarks of Fortinet. All other marks are trademarks or registered trademarks of their respective owners. Performance and other metrics contained herein were obtained in internal lab tests, under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other factors 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 into a binding written contract, signed by Fortinet's General Counsel, with a customer. Fortinet is not responsible for the performance of the certified product, all performance is based on certain expressly identified performance metrics and, in any event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute certainty, all performance will be limited to performance in the same test conditions as in Fortinet's internal lab tests. Fortinet disclaims all liability, warranties, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, replace, or remove any information published without notice, and the most current version of the publication shall be applicable.

FORTINET

FICHA DE DATOS

FortiManager

Disponible en:



Físicos



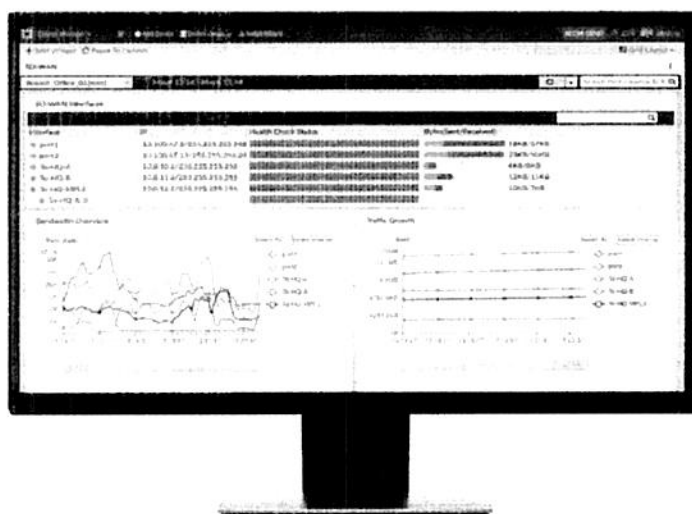
Virtual
Máquina



Nube
(PaaS)

FortiManager proporciona administración centralizada impulsada por la automatización de sus dispositivos Fortinet desde una única consola para una administración y visibilidad completas de sus dispositivos de red a través de un aprovisionamiento optimizado y herramientas de automatización innovadoras.

Integrada con el Security Fabric de Fortinet, la arquitectura de seguridad avanzada y las capacidades de operaciones de red impulsadas por la automatización de FortiManager proporcionan una base sólida para proteger y optimizar la seguridad de su red.



Gestión de un solo panel agiliza la gestión centralizada de políticas y objetos, el historial y el control de revisiones automáticos, y las funciones RBAC mejoradas para la gestión de scripts y la gestión de IPS con separación de funciones.

Automatización de Security Fabric simplifica el proceso de implementación de ZTP para SD-Branch (FortiGate y dispositivos de acceso) con potentes plantillas que utilizan directamente metavariables para el aprovisionamiento escalable a miles de sitios.

Servicios en la nube NOC ofrece la plataforma FortiManager como servicio con nuevas extensiones de administración que se pueden extraer e instalar desde la nube.

000046

Características clave

- **Gestione miles de forma centralizada** de FortiGates, políticas y objetos, así como FortiSwitches, FortiAP y FortiExtender. Proveer actualizaciones de firmas para FortiGate, FortiMail, FortiSandbox y FortiClient
- **Distribución centralizada de** firmas y contenido de seguridad mediante el uso del módulo FortiGuard integrado
- **Utilice plantillas para actualizaciones de** firmware y aprovisionamiento sin intervención para Secure SD-WAN, configurando IPSec VPN, ruta estática y FortiExtender para una configuración rápida y fácil
- **Reduzca la complejidad y los costos** aprovechando la automatización API REST, scripts, conectores y puntadas de automatización
- **Automatice los flujos de trabajo y** configuraciones para firewalls, conmutadores e infraestructura inalámbrica de Fortinet
- **Separar los datos del cliente y** administrar dominios aprovechando las ADOM para que sean compatibles y operativamente eficaces
- **Alta disponibilidad para automatizar** copias de seguridad de hasta cinco nodos con software optimizado y actualizaciones de seguridad para todos los dispositivos administrados



ABASI
Servicios Integrados S.A de C.V.

Nayarit no. 85 - 101 Col. Roma México D.F.
Código postal: 06700 R.F.C. A30501142C7
Tel. Fax 5712-5702 / 5219-5703 - www.abasi.com

CARACTERÍSTICAS DESTACADAS

Gestión de panel único

La gestión de panel único de FortiManager proporciona una gestión centralizada y una estrategia de aprovisionamiento basada en el Security Fabric de Fortinet que integra estrechamente la infraestructura de red y la arquitectura de seguridad de una organización para aplicar control de acceso, segmentación y protección constante de dispositivos, aplicaciones y usuarios.

Configuración y aprovisionamiento de dispositivos

FortiManager amplía las capacidades del administrador de red con un amplio conjunto de herramientas para administrar de forma centralizada hasta 100.000 dispositivos, incluidos FortiGate, FortiExtender, FortiSwitch, FortiAPs, SD-WAN y más.

Configure colectivamente la configuración del dispositivo y utilice nuevas plantillas de CLI mejoradas con variables y plantillas de aprovisionamiento para asignar paquetes de firmware y políticas desde una sola consola, incluido el historial de revisión de políticas y objetos para la auditoría.

FortiManager incluye soporte extendido de SSL y certificados para una configuración mejorada del perfil ssl-ssh, así como perfiles de administración de IPS restringidos para ayudar a los clientes que están en transición y actualización de soluciones IPS dedicadas a productos Fortinet.

Las copias de seguridad automatizadas de la configuración del dispositivo y el control de revisiones facilitan las tareas administrativas diarias, con el seguimiento de cambios en la vista mejorada del Registro de eventos para revisar la configuración y los detalles de los cambios para auditoría y cumplimiento.

FortiManager ahora también permite a los administradores configurar y asignar comandos personalizados en FortiSwitch y configurar MCLAG desde FortiSwitch Manager.

Administración multiempresa y basada en roles

FortiManager proporciona administración granular basada en funciones y dispositivos para una visibilidad clara de cada dispositivo y usuario en la red, lo que facilita implementaciones multi-tenencia de confianza cero para grandes empresas y una base de datos de objetos jerárquicos para la reutilización de configuraciones comunes para servir a múltiples clientes.

Los ADOM (dominios administrativos) se utilizan para gestionar entornos de seguridad independientes, cada uno con sus propias políticas de seguridad y base de datos de configuración. La GUI intuitiva facilita a los administradores ver, crear, clonar y administrar ADOM, definir objetos globales, políticas y perfiles de seguridad en ADOM, con Health Check para garantizar que los ADOM estén sincronizados.

La implementación sin intervención de FortiManager utiliza plantillas para aprovisionar dispositivos para implementaciones masivas rápidas y admite la aplicación de la versión de firmware para definir los requisitos de firmware para instalaciones y actualizaciones.

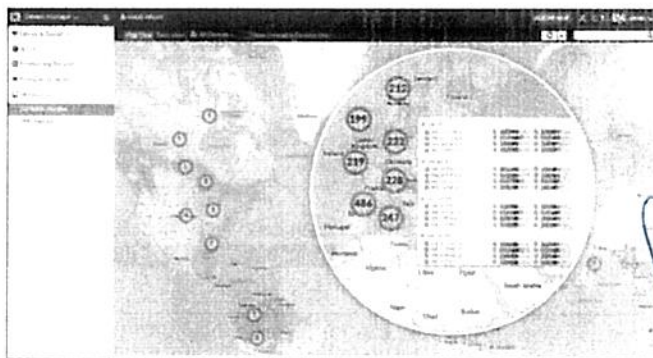
El nuevo administrador de IPS de FortiManager es un rol de usuario restringido para realizar solo configuraciones e instalaciones de objetos relacionados con IPS. A los usuarios administradores también se les pueden asignar temas de fondo de la interfaz de usuario por administrador, para asociaciones visuales únicas.

Política de seguridad y gestión de objetos

Las vistas de políticas y objetos de FortiManager permiten a los administradores administrar y configurar de forma centralizada las políticas de los dispositivos, incluida la actualización de la configuración de red, las definiciones de antivirus, las firmas de protección contra intrusiones, las reglas de acceso y las actualizaciones de software.

La función de política global permite a los proveedores de MSSP y PaaS aplicar políticas de encabezado / pie de página de nivel ADOM para actualizar todos los paquetes de políticas o paquetes seleccionados. Las vistas de políticas y objetos ahora incluyen un historial de revisión, que proporciona una cuenta de administradores que han realizado cambios, fecha de cambio, resumen y un campo de notas de cambio obligatorio para capturar el motivo del cambio.

La función de bloqueo por política permite a los administradores controlar el cambio de política bloqueando implícitamente una regla de política cuando se cambia una política. Los administradores también pueden agrupar las políticas de uso común en un bloque de políticas e insertarlas en diferentes paquetes de políticas.



SD-WAN seguro

FortiManager ofrece potentes capacidades de administración de SD-WAN mediante flujos de trabajo intuitivos y aprovisionamiento simplificado a escala. Aproveche las políticas comerciales de SD-WAN centradas en las aplicaciones para ajustar las decisiones de dirección del tráfico en función de los objetivos de SLA de rendimiento para cada proveedor de WAN.

Los administradores pueden usar el panel de control de SD-WAN para vigilar el rendimiento de la aplicación y la utilización del ancho de banda por enlace WAN, e integrar FortiAnalyzer para obtener vistas analíticas mejoradas e informes de evaluación de SD-WAN.

CARACTERÍSTICAS DESTACADAS

Administrar y monitorear con visibilidad profunda

El Administrador de dispositivos de FortiManager brinda visibilidad, acceso y administración completos de los dispositivos administrados de Fortinet, interfaces, scripts, plantillas, automatización, monitores, usuarios, configuraciones y más. Instale, edite y elimine políticas, controle el estado de los dispositivos FortiGate a través de los paneles y widgets personalizables para ver el uso de recursos, el estado de la red de DHCP, IPsec y SSL VPN, enrutamiento, modeladores de tráfico y más. Navegue fácilmente por el árbol jerárquico con categorías para dispositivos administrados, dispositivos de registro, dispositivos no autorizados y personalice los para que se muestren como una tabla, carpeta o vista de mapa.

Use Fabric View para verificar las clasificaciones de Security Fabric y las configuraciones de los dispositivos o grupos de FortiGate. Acceda a estadísticas vitales de red y seguridad, así como a información de topología y supervisión en tiempo real para proporcionar visibilidad de la red y la actividad de los usuarios. Agregue un dispositivo FortiAnalyzer o VM para obtener análisis potentes y una vista de Fabric mejorada con información de activos e identidad, minería de datos adicional, análisis estadístico y capacidades de informes gráficos.

Alta disponibilidad de FortiManager (HA)

La alta disponibilidad (HA) de FortiManager proporciona mayor confiabilidad, protección de datos, redundancia y rendimiento operativo para garantizar tiempos de actividad y disponibilidad acordados. En caso de que falle la unidad FortiManager operativa, una unidad FortiManager de respaldo (una primaria y hasta cuatro secundarias) puede reemplazar a la unidad fallada, asegurándose de que las empresas tengan acceso sin problemas a sus dispositivos y operaciones de red críticas para el negocio.

FortiManager HA Cluster Wizard ahora también admite la definición de un nombre de host para cada miembro del clúster, exponiendo la opción de selección de sesión de la GUI, así como la opción de dedicar una interfaz para la administración del miembro individual del clúster.

Automatización de Security Fabric

Visibilidad de operaciones de red y seguridad (NOC / SOC)

FortiManager admite los flujos de trabajo NOC-SOC para ayudar a los equipos de la red a mantener un rendimiento óptimo. Los intercambios de datos automatizados entre los flujos de trabajo de seguridad (SOC) y los flujos de trabajo operativos (NOC) crean un flujo de trabajo único y completo que no solo ahorra tiempo, sino que también brinda la capacidad de completar actividades adicionales de respuesta a incidentes.

La integración con FortiAnalyzer aumenta la visibilidad con análisis y visualización de datos avanzados que ayudan a los analistas a conectar rápidamente los puntos, identificar amenazas y simplificar la configuración y la seguridad rápidas de los dispositivos administrados.



Automatización y conectores

Utilice Automatización y Orquestación y optimice con FortiManager a través de consultas de FortiGates y Fortinet Security Fabric a través de interfaces de programación de aplicaciones (API) para recopilar y compartir activamente información de red y ampliar la visibilidad y respuesta de un extremo a otro.

FortiManager reduce la complejidad y el costo al aprovechar la API REST, los scripts, los conectores y los puntos de automatización de FortiGate para automatizar los procesos que requieren mucho tiempo y acelerar los flujos de trabajo para descargar NOC-SOC, reducir las tareas administrativas y abordar la escasez de talento. Los administradores pueden automatizar tareas comunes como el aprovisionamiento de FortiGates y la configuración de dispositivos nuevos o existentes.

Únase a Fortinet Developer Network (FNDN) para obtener acceso exclusivo a artículos, contenido instructivo para automatización y personalización, herramientas creadas por la comunidad, scripts y código de muestra.

000049

CARACTERÍSTICAS DESTACADAS

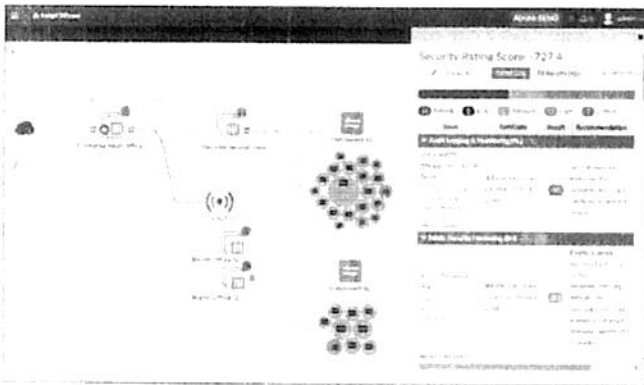
Servicios en la nube NOC

Extensiones de administración

El panel de extensiones de administración de FortiManager permite una rápida expansión del panel único para administrar más productos de Security Fabric. El motor integrado ejecuta aplicaciones de extensión de administración en contenedores (MEA), extraídas de FortiGuard.

Las extensiones de administración de FortiManager incluyen módulos para lo siguiente:

- § SD-WAN Orchestrator para toda la configuración, administración y monitoreo de FortiGates en su red SD-WAN
- § FortiPortal para la seguridad basada en la nube y la gestión de registros, lo que permite a los proveedores de servicios de seguridad gestionados delegar el acceso controlado a la configuración y el análisis del dispositivo.
- § FortiWLM para monitorear, operar y administrar redes inalámbricas en FortiGates que son administradas por FortiManager
- § FortiSigConverter para convertir las reglas del sistema de prevención de intrusiones y detección de intrusiones en la red Snort en firmas IPS compatibles con Fortinet directamente en FortiManager
- § FortiAuthenticator para la gestión de identidades y accesos, que permite a los administradores proporcionar acceso a activos de red protegidos y realizar un seguimiento de la actividad del usuario y el cumplimiento de las políticas de seguridad.
- § FortiSOAR: funciones de respuesta, automatización y orquestación de seguridad total con una suscripción a FortiSOAR



Seguridad dinámica en la nube

Las soluciones de administración y seguridad en la nube de Fortinet ofrecen a los clientes una opción de entrega basada en PaaS para la administración centralizada de dispositivos FortiGate desde un FortiManager basado en la nube.

FortiManager Cloud proporciona una capacidad de administración de panel único y basada en la automatización que es fácil de implementar, fácil de administrar, flexible y escalable para el crecimiento comercial de una organización.

Utilice el portal de inicio de sesión único para administrar Fortinet NGFW y SD-WAN. El servicio de inicio en la nube integrado permite a los administradores personalizar fácilmente una imagen preparada de una instalación virtual para KVM, AZURE y AWS. La administración de red basada en la nube de FortiManager ayuda a los clientes a optimizar el aprovisionamiento de FortiGate con la administración habilitada para la automatización de los dispositivos Fortinet.

Con la suscripción a FortiCloud Premium, los clientes pueden habilitar fácilmente el servicio FortiManager Cloud con el paquete de protección 360 o comprándolo a la carta, brindando acceso para administrar una gama de soluciones y servicios de Fortinet para una gestión simplificada de la red y la seguridad. Los clientes y socios pueden acceder fácilmente a su FortiManager Cloud desde su portal de inicio de sesión único de FortiCloud.

Security Fabric e integración de terceros

FortiManager se integra con ITSM para mitigar sin problemas los incidentes y eventos de seguridad, aplicar cambios de configuración y actualizar políticas. La integración con FortiAnalyzer proporciona descubrimiento, análisis, priorización e informes en profundidad de eventos de seguridad de la red.

Utilice conectores de estructura para facilitar las conexiones con proveedores de terceros como vCenter, pxGrid, Clearpass, OCI, ESXi, AWS y otros para compartir e intercambiar datos.

El flujo de trabajo de FortiManager para auditoría y cumplimiento permite revisar, aprobar y auditar cambios en las políticas, incluida la automatización de procesos para el cumplimiento de políticas, la gestión del ciclo de vida de las políticas y el flujo de trabajo forzado para reducir el riesgo.

000050

OFERTAS VIRTUALES

FortiManager VM

Las máquinas virtuales FortiManager son una versión virtual del dispositivo de hardware y están diseñadas para ejecutarse en muchas plataformas de virtualización, ofreciendo todas las funciones más recientes del dispositivo FortiManager. Permiten a las organizaciones administrar de manera centralizada cualquier cantidad de dispositivos Fortinet Network Security Fabric y escalar de varios a miles, lo que respalda la administración centralizada, el cumplimiento de las mejores prácticas y los flujos de trabajo automatizados para brindar una protección superior contra las amenazas. Las máquinas virtuales de FortiManager están disponibles tanto en suscripción como en oferta perpetua.

FortiManager VM-S

El nuevo modelo de licencia de suscripción de FortiManager VM consolida la SKU del producto VM y la SKU de soporte de FortiCare en una única SKU para simplificar la compra, actualización y renovación del producto.

Los SKU de FortiManager S-Series vienen en suscripciones apilables para administrar 10, 100 y 1,000 dispositivos / vdoms, de modo que se puedan comprar varias unidades de este SKU a la vez para aumentar la cantidad de dispositivos / vdom según sea necesario. Este SKU también se puede comprar junto con otros SKU de FMG VM-S para expandir el número total de dispositivos / vdom.

FortiManager VM

Fortinet ofrece FortiManager VM en un modelo de licencia apilable. Esta versión basada en software del dispositivo de hardware FortiManager está diseñada para ejecutarse en muchas plataformas de virtualización, lo que le permite expandir su solución virtual a medida que se expande su entorno. La familia de dispositivos virtuales FortiManager minimiza el esfuerzo requerido para monitorear y mantener su red y ofrece todas las características del dispositivo de hardware FortiManager.

ESPECIFICACIONES

APARATOS VIRTUALES FORTIMANAGER	FMG-VM-10-UG	FMG-VM-100-UG	FMG-VM-1000-UG	FMG-VM-5000-UG
Capacidad				
Dispositivos / VDOM (máximo)	10 *	100 *	1000 *	5000 *
Capacidad de almacenamiento	200 GB	1 TB	4 TB	8 TB
GB / día de registros	2	5	10	25
Gestión de chasis	✓	✓	✓	✓
Máquina virtual				
Soporte de hipervisor	Se puede encontrar soporte de hipervisor actualizado en las notas de la versión para cada versión de FortiManager. Visite https://docs.fortinet.com/product/fortimanager/ y busque la información de la versión en la sección inferior. Vaya a "Soporte e integración de productos" -> "Soporte de [versión] de FortiManager" -> "Virtualización".			
Compatibilidad con vCPU (mínimo / máximo)	4 / Ilimitado			
Soporte de interfaz de red (mín. / Máx.)	1/4			
Soporte de almacenamiento (mínimo / máximo)	100 GB / 16 TB			
Soporte de memoria (mínimo / máximo)	8 GB / Ilimitado para 64 bits			
Soporte de alta disponibilidad	Sí			

* Cada dominio virtual (VDOM) que opera en un dispositivo físico o virtual cuenta como un (1) dispositivo de red con licencia.

2. La capacidad de almacenamiento y los GB / día de registros no se pueden apilar. Estos valores representan el máximo disponible con la licencia comprada. 3. * Indica que

4. * y dispone de una licencia complementaria de dispositivo.

5. VM admite hasta 12 interfaces / puertos vNIC. Aplicable a 6.4.3+. La cantidad real de consumibles varía según las plataformas en la nube.

ABASI
Servicios Integrados S.A. de C.V.
Norell no. 85 - 101 Col. Roma México D.F.
Cucunhémoc C.P. 04700 R.F.C. AS0501142C2
Tel. Fax 5912-5702 / 8219-6703 www.abasi.com

ESPECIFICACIONES

000051

ELECTRODOMÉSTICOS FORTIMANAGER			
	FMG-200G	FMG-300F	FMG-400G
Dispositivo de capacidad y			
rendimiento / VDOM (máximo)	30	100	150
Tasa de registro por segundo	50	50	50
GB / día	2	2	2
Especificaciones de hardware			
Capacidad de almacenamiento	8 TB (2 x 4 TB)	16 TB (4 x 4 TB)	32 TB (8 x 4 TB)
Almacenamiento utilizable (después de)	4 TB	8 TB	24 TB
RAID Nivel de RAID admitidos	RAID 0/1	RAID 0/1/5/5L/10	RAID 0/1/5/5L/6/6L/10/50/60
Nivel RAID predefinido	1	10	50
Tipo de forma del hardware	Montaje en rack de 1 RU	Montaje en rack de 1 RU	Montaje en rack de 1 RU
Interfaces totales	4xRJ45 GE	4 x GE RJ45, 2 x SFP	4 x GE RJ45, 2 x SFP
Forma de conexión	RJ45	RJ45	RJ45
Discos duros extraíbles	No		
Unidad de fuentes de alimentación de	No		
Interfaz en caliente redundante			
Dimensiones			
Alto x Ancho x Largo (pulgadas)	1,73 x 17,24 x 16,38	1,75 x 17,44 x 22,16	3,5 x 17,5 x 22,2
Alto x Ancho x Largo (cm) Peso	4,4 x 43,8 x 41,6 22,5 libras (10,2 kg)	4,4 x 44,3 x 56,3 28,6 libras (13,0 kg)	8,8 x 44,5 x 56,5 35,27 libras (16 kg)
Medio ambiente			
Temperatura de funcionamiento de CA	100-240 V 50-60 Hz	100-240 V CA, 50-60 Hz	100-240 V CA, 50-60 Hz
Consumo de energía (promedio / máximo)	90,1 W / 99 W	108 W / 186 W	140/182 W
Disipación de calor	337,8 BTU / h	634 BTU / h	621 BTU / h
Temperatura de funcionamiento	32 a 104 ° F (0 a 40 ° C)	32 a 104 ° F (0 a 40 ° C)	32 a 104 ° F (0 a 40 ° C)
Temperatura de almacenamiento	-13-167 ° F (-25-75 ° C)	-31-158 ° F (-35-70 ° C)	-4-167 ° F (-20-75 ° C)
Humedad	20 a 90% sin condensación	20 a 90% sin condensación	5-95% sin condensación
Altitud operativa	Hasta 7.400 pies (2.250 m)	Hasta 7.400 pies (2.250 m)	Hasta 7.400 pies (2.250 m)
Cumplimiento			
Certificaciones de seguridad	FCC Parte 15 Clase A, RCM, VCCI, CE, UL / cUL, CB	FCC Parte 15 Clase A, RCM, VCCI, CE, BSMI, KC, UL / cUL, CB, GOST	FCC Parte 15 Clase A, RCM, VCCI, CE, UL / cUL, CB

El término "virtual VDOM" que opera en un dispositivo físico o virtual cuenta como un (1) dispositivo de red con licencia. Políticas de licencia y soporte de alta disponibilidad disponibles en todos los modelos.

La licencia de alta disponibilidad (HA) redundante opcional no incluye.



ESPECIFICACIONES

000052



ELECTRODOMÉSTICOS FORTIMANAGER	FMG-1000F	FMG-2000E	FMG-3000G
Dispositivos de capacidad y			
rendimiento / VDOM (máximo)	1000	1200	4000*
Tasa de registro sostenida	50	50	150
GB / día	2	2	10
Especificaciones de hardware			
Capacidad de almacenamiento	32 TB (8 de 4 TB)	36 TB (12 x 3 TB)	64 TB (16 x 4 TB)
Almacenamiento utilizable (después de RAID)	24 TB	30 TB	56 TB
RAID Niveles de RAID admitidos	RAID 0 / 1, 1s / 5, 5s / 6, 6s / 10/50/60	RAID 0 / 1, 1s / 5, 5s / 6, 6s / 10/50/60	RAID 0 / 1, 1s / 5, 5s / 6, 6s / 10/50/60
Nivel RAID predefinido	50	50	50
Factor de forma del hardware	Montaje en bastidor de 2 U	Montaje en bastidor de 2 U	Montaje en rack de 3 U
Interfaces totales	2 puertos RJ45 10G, 2 puertos SFP *	4x GE, 2x 10 GE SFP *	2 puertos RJ45 fast, 2 puertos SFP26 de 25 GbE
Puerto de consola	DB-9	DB-9	DB-9
Discos duros extraíbles	☒	☒	☒
Gestión de chasis de fuentes de alimentación de	☒	☒	☒
Modo de operación en caliente redundantes	☒	☒	☒
Dimensiones			
Alto x Ancho x Largo (pulgadas)	3,5 x 17,2 x 25,6	3,5 x 17,2 x 25,6	5,2 x 17,2 x 25,5
Alto x Ancho x Largo (cm) Peso	8,9 x 43,7 x 65,0 34 libras (15,42 kg)	8,9 x 43,7 x 64,8 58 libras (26,3 kg)	13,2 x 44,0 x 65,0 65,5 libras (30,15 kg)
Medio ambiente			
Fuente de alimentación por CA	100-240 V CA, 50-60 Hz	100-240 V CA, 50-60 Hz	100-127 V ~ 110 A 200-240 V ~ 15 A Hz
Consumo de energía (promedio / máximo)	192,5 W / 275 W	293,8 W / 354 W	449 W / 541 W
Disipación de calor	920 BTU / h	1209 BTU / h	1646,5 BTU / h
Temperatura de funcionamiento	50 a 95 ° F (10 a 35 ° C)	50 a 95 ° F (10 a 35 ° C)	32 a 104 ° F (0 a 40 ° C)
Temperatura de almacenamiento	-40 a 140 ° F (-40 a 60 ° C)	-40 a 158 ° F (-40 a 70 ° C)	-40 a 167 ° F (-20 a 75 ° C)
Humedad	8-90% sin condensación	8-90% sin condensación	5-95% sin condensación
Altitud operativa	Hasta 7.400 pies (2.250 m)	Hasta 7.400 pies (2.250 m)	Hasta 7.400 pies (2.250 m)
Cumplimiento			
Certificaciones de seguridad	FCC Parte 15 Clase A, RCM, VCCI, CE, UL / cUL, CB	FCC Parte 15 Clase A, RCM, VCCI, CE, UL / cUL, CB	FCC Parte 15 Clase A, RCM, VCCI, CE, IEC, KC, UL / cUL, CB, GSMT

* Cada dominio virtual (VDOM) que opera en un dispositivo físico o virtual cuenta como un (1) dispositivo de red con licencia. Políticas globales y soporte de alta disponibilidad disponible en todos los modelos.

* El número de puertos de consola depende del tipo de montaje en rack o bastidor.

ABASI
Servicios Integrados S.A. de C.V.
Núñez no. 83 - 101 Col. Roma México D.F.
Cuidad de México C.P. 06700 R.F.C. AS0601142C2
Tel: Fax 52-5702 / 5219-5703 www.abasi.com

INFORMACIÓN DEL PEDIDO

000053

PRODUCTO	SKU	DESCRIPCIÓN
FortiManager	FMG-200G	Dispositivo de administración centralizada: 4x RJ45 GE, almacenamiento de 8 TB, hasta 30 dispositivos Fortinet / dominios virtuales
	FMG-300G	Dispositivo de administración centralizada: 4x RJ45, 2x SFP, almacenamiento de 16 TB, hasta 100 dispositivos Fortinet / dominios virtuales
	FMG-400G	Dispositivo de administración centralizada: 4 x GE RJ45, 2 x SFP, almacenamiento de 32 TB, hasta 150 dispositivos Fortinet / dominios virtuales
	FMG-1000G	Dispositivo de administración centralizada: 2x RJ45 10G, 2x ranuras SFP + almacenamiento de 32 TB, hasta 1000x dispositivos Fortinet / dominios virtuales
	FMG-2000E	Dispositivo de administración centralizada: 4 puertos GE RJ45, 2 ranuras 10 GE SFP + almacenamiento de 36 TB, fuentes de alimentación dual y administra hasta 1200 dispositivos Fortinet / dominios virtuales
	FMG-3000G	Dispositivo de gestión centralizada: 2 puertos RJ45 GbE, 2x SFP28 de 25 GbE, almacenamiento de 64 TB, fuentes de alimentación dual, gestiona hasta 4.000 dispositivos Fortinet / dominios virtuales
FortiManager-VM Licencia de suscripción con soporte y BPS	FC1-10 FMGVS-448-01-DD	Licencia de suscripción para 10 dispositivos / vdoms administrados por FortiManager VM S-series. Soporte de FortiCare 24x7 más servicios de mejores prácticas de FortiCare incluidos.
	FC2-10 FMGVS-448-01-DD	Licencia de suscripción para 100 dispositivos / vdoms administrados por FortiManager VM S-series. Soporte de FortiCare 24x7 más servicios de mejores prácticas de FortiCare incluidos.
	FC3-10 FMGVS-448-01-DD	Licencia de suscripción para 1.000 dispositivos / vdoms administrados por FortiManager VM S-series. Soporte de FortiCare 24x7 más servicios de mejores prácticas de FortiCare incluidos.
FortiManager-VM	FMG-VM-10-UG	Actualizar la licencia para agregar 10 dispositivos Fortinet / dominios virtuales, permite un total de 2 GE / día de registros y 200 GB de capacidad de almacenamiento
	FMG-VM-100-UG	Actualizar la licencia para agregar 100 dispositivos Fortinet / dominios virtuales, permite un total de 5 GB / día de registros y una capacidad de almacenamiento de 1 TB
	FMG-VM-1000-UG	Actualizar la licencia para agregar 1.000 dispositivos Fortinet / Dominios virtuales, permite un total de 10 GB / día de registros y una capacidad de almacenamiento de 4 TB
	FMG-VM-5000-UG	Actualizar la licencia para agregar 5.000 dispositivos Fortinet / dominios virtuales, permite un total de 25 GB / día de registros y 8 TB de capacidad de almacenamiento
FortiManager-Cloud *	FC-10 [Código de modelo de FortiGate]-179-02-DD	Servicio de Orquestación y Gestión Central basado en la Nube para FortiGate
	FC-10 [Código de modelo de FortiGate]-841-02-DD	Protección 360 (FMG / FAZ Cloud, FortiCloud SOCAas, IPS, AMP, App Ctrl, Filtrado de video y web, AS, Clasificación de seguridad, Detección de IoT, Seguridad industrial, SD-WAN Orchestrator, SD-WAN Cloud Monitoring, FortiConverter Svc y ASE FortiCare)
	FC-10 [Código de modelo FortiGate VM]-842-02-DD	Protección 360 (FMG / FAZ Cloud, FortiCloud SOCAas, IPS, AMP, App Ctrl, Filtrado de video y web, AS, Clasificación de seguridad, Detección de IoT, Seguridad industrial, SD-WAN Orchestrator, SD-WAN Cloud Monitoring, FortiConverter Svc y ASE FortiCare).
	FC1-10 MVCLD-227-01-DD	Suscripción para 10 dispositivos / vdoms administrados por FortiManager Cloud. Soporte FortiCare 24x7 incluido. Suscripción
	FC2-10 MVCLD-227-01-DD	para 100 dispositivos / vdoms administrados por FortiManager Cloud. Se incluye contrato FortiCare 24x7.
	FC3-10 MVCLD-227-01-DD	Suscripción para 1000 dispositivos / vdoms administrados por FortiManager Cloud. Soporte FortiCare 24x7
Paquete de hardware	FMG (Modelo de hardware) BDL-447-DD	Incluido Hardware más FortiCare y FortiCare BPS 24x7.
Dispositivo FortiManager Actualizar licencia	FMG DEV-100-UG	Licencia de actualización de dispositivo FortiManager para agregar 100 dispositivos Fortinet / vdoms (serie 3000 y superior, solo hardware).

* Incluye licencia de cuenta FortiCloud Premium

El número de módulos de software, el número predeterminado de ADDM se puede encontrar en las Notas de la versión en docs.oracle.com/Para.
 Para la configuración de PatchManager, VM, reemplazar \$ADDM se pueden añadir x ADDM adicionales.

**FORTINET**

~~www.fortinet.com~~

Ciudad de México, Cuauhtémoc, octubre 18 del 2021

Instituto Nacional para la Educación de los Adultos
Presente

Invitación a cuando menos Tres Personas Nacional Electrónica
No. IA-011MDA001-E89-2021
Relativa a la "Contratación para el licenciamiento de software para el año 2021"

Nombre del licitante: **ABASI Servicios Integrales, S.A. de C.V.**
 email: **fescobar@abasi.com.mx y ggarcia@abasi.com.mx**

Formato A-2
Proposición Económica

Partida	Concepto	Unidad	Cantidad	Precio Unitario	Precio Total
1	Renovación de Creative Cloud licenciamiento por un año.	Licencia	5	\$0.00	\$0.00
2	Renovación de licencia de software antivirus e.Scan Corporate Edition (con soporte para redes híbridas), para Oficinas Centrales, Institutos Estatales, Unidades de operación, Coordinaciones de Zona y Plazas Comunitarias. Licenciamiento por un año.	Licencia	11,654	\$58.50	\$681,759.00
3	Renovación de licencia por 1 año, de firewall FORTINET Modelo FORTIGATE 600C (2 licencias) y FG100D (33 licencias), para oficinas centrales, delegaciones e institutos estatales. Incluir para los FORTIGATE, servicio de FORTICARE 8x5 y FORTIGUARD UTM. Incluye devolución y remplazo por fallas de hardware. Nuestra propuesta incluye la renovación tecnológica a Fortigate 600E (2 licencias) y Fortigate 80F hardware plus (33 licencias) con servicio Forticare 24x7 por un año.	Licencia	35	\$56,000.00	\$1'960,000.00
	Renovación de licencia por 1 año de software para reporte de análisis de seguridad FORTIANALYZER 200F	Licencia	2	\$95,698.00	\$191,396.00
	Renovación de licencia por 1 año contado de software para la administración y control de los dispositivos de seguridad de un FORTIMANAGER modelo 300D. La renovación incluye la actualización tecnológica del appliance donde se renueva la licencia del producto. Nuestra propuesta incluye la renovación tecnológica a Fortigate 300F, con Forticare 24x7 por un año.	Licencia	1	\$134,376.00	\$134,376.00
4	Renovación de licencia de Acrobat Pro DC por un año	Licencia	15	\$0.00	\$0.00
5	Renovación de licencia PowerBI Pro por un año	Licencia	40	\$960.00	\$38,400.00
Nuestra oferta asciende a \$3'486,879.96 (Tres Millones Cuatrocientos Ochenta y Seis Mil Ochocientos Setenta y Nueve Pesos 96/100 M.N.) Incluyendo el Impuesto al Valor Agregado				Sub Total	\$3'005,931.00
				I.V.A. 16%	\$480,948.96
				Total	\$3'486,879.96

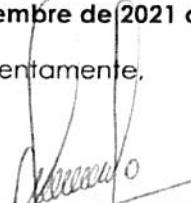
Moneda: **Pesos Mexicanos.**

Vigencia de la propuesta: **Desde su presentación y hasta la conclusión del procedimiento.**

Vigencia del contrato o pedido: **Será de 30 días naturales contados a partir de la firma del mismo.**

Vigencia del licenciamiento: **Un año, del 01 de noviembre de 2021 al 31 de octubre del 2022**

Atentamente,


Lic. Fernando Escobar Olivares
 Administrador Único

Sucursal Culiacán:
 Av. Insurgentes Sur No. 500 - A
 Col. Centro Sinaloa.
 80129 Culiacán de Rosales
 Tel. (667) 992-3367 y (667) 992-2468

Hoja 1 de 1

Nayarit No. 85 - 101, Col. Roma Sur
 06760 Cuauhtémoc, Ciudad de México
 RFC ASIO501142C2 www.abasi.com.mx
 Tel. (55) 5219-5702 y (55) 5219-5703