Contrato abierto plurianual relativo al Arrendamiento del **"Equipo Firewall/VPN y consola de Administración para expansión de Oficinas Telegráficas de la Red Teldat"**, que celebran por una parte, **Telecomunicaciones de México**, Organismo Descentralizado de la Administración Pública Federal, en lo sucesivo, se denominará **"TELECOMM"** representado legalmente por el **Licenciado Gabriel Salinas Caso**, en su carácter de **Director de Administración Financiera,** asistido por el **Licenciado Roberto Ruiz Dominguez,** Subdirector de Desarrollo de Informática, en su carácter de **administrador y verificador del cumplimiento del contrato** y por otra parte, la empresa **Grupo de Tecnología Cibernética, S.A. de C.V.**, en lo sucesivo, se denominará **"EL ARRENDADOR"** representada en este acto, por la **C. Jennifer Murillo Dominguez**, en su carácter de **Apoderada legal** de acuerdo a las siguientes declaraciones y cláusulas:

## D e c l a r a c i o n e s:

**I.** **"TELECOMM"** declara que:

**I.1** Es un Organismo Descentralizado de la Administración Pública Federal, creado mediante decreto publicado en el Diario Oficial de la Federación el 20 de agosto de 1986 y reformado por diversos publicados en el mismo medio informativo, de fechas 17 de noviembre de 1989, 29 de octubre de 1990, 6 de enero de 1997 y 14 de abril de 2011, con personalidad jurídica y patrimonio propios, cuyo objeto principal es la prestación de los servicios públicos de telégrafos, radiotelegrafía, la comunicación vía satélite y los de telecomunicaciones que expresamente se señalan en el artículo 3° de su decreto de creación, así como los de carácter prioritario que en su caso le encomiende el Ejecutivo Federal.

**I.2** El **Licenciado Gabriel Salinas Caso**, como representante legal y en su carácter de **Director de Administración Financiera**, firma el presente contrato de conformidad con el poder que para tal efecto le fue otorgado mediante testimonio notarial **49,028** de fecha **17 de febrero de 2015**, pasado ante la fe del Notario Público número **221** del Distrito Federal, **Licenciado Francisco Talavera Autrique**, con registro número **42-7-25022015-180235** en el **Registro Público de Organismos Descentralizados (REPODE)**.

**I.3** Para cubrir las erogaciones que se deriven del presente contrato, para el ejercicio fiscal **2015**, **"TELECOMM"**, mediante el oficio número **6110.-0565,** de fecha **28 de mayo de 2015**, signado por el Gerente de Presupuesto, dependiente de la Subdirección de Presupuesto y Contabilidad cuenta con los recursos necesarios autorizados con cargo en la partida presupuestal **32301** para cumplir con las obligaciones derivadas del presente instrumento.

Las obligaciones de este contrato cuyo cumplimiento, se encuentra previsto realizar durante los ejercicios fiscales de **2016, 2017 y 2018** quedarán sujetas, para fines de su ejecución y pago, a la disponibilidad presupuestaria con que cuente **"TELECOMM"**, conforme al Presupuesto de Egresos de la Federación que para los ejercicios fiscales correspondientes apruebe la Cámara de

Diputados del H. Congreso de la Unión, sin que la no realización de la referida condición suspensiva origine responsabilidad para alguna de las partes.

**I.4** La adjudicación del presente contrato se realizó mediante el procedimiento de Licitación Pública Mixta Nacional No. **LA-009KCZ002-N49-2015**, cuyo fallo se llevo a cabo el día **20 de octubre de 2015,** conforme a lo dispuesto en los artículos **25 primer párrafo, 26 fracción I, 26 Bis fracción III, 28 fracción I, 29, 45 y 47** de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, así como en lo dispuesto en el decreto de Presupuesto de Egresos de la Federación para el **ejercicio fiscal de 2015, publicado en el Diario Oficial de la Federación el día 03 de diciembre de 2014.**

**I.5** Que cuenta con el acuerdo con el Director General número **04/2015 DOT** de fecha **12 de mayo de 2015**, a través del cual, el Director General de **"TELECOMM"** autoriza comprometer recursos para llevar a cabo la presente contratación plurianual.

**I.6** Requiere del arrendamiento objeto de este contrato en razón de que no cuenta con los elementos suficientes para realizarlos.

**I.7** Su clave del Registro Federal de Contribuyentes es: **TME-891117-F56.**

**I.8** Que para el ejercicio y cumplimiento de los derechos y obligaciones a su cargo, que se deriven del presente instrumento señala como su domicilio legal el ubicado en: **Eje Central Lázaro Cárdenas número 567, Colonia Narvarte, Delegación Benito Juárez, Código Postal 03020, en México, Distrito Federal.**

**II. "EL ARRENDADOR"** declara que:

**II.1** Es una sociedad legalmente constituida de acuerdo a la legislación de los Estados Unidos Mexicanos, tal como lo acredita con el testimonio de la Escritura Pública número **88,838**, de fecha **17 de abril de 1998,** otorgado ante la fe del Notario Público número **9** del Distrito Federal, **Licenciado José Angel Villalobos Magaña,** debidamente inscrito en el Registro Público de la Propiedad y de Comercio de la Ciudad de **México, Distrito Federal,** bajo el número de Folio Mercantil **234589**, de fecha **04 de mayo de 1998.**

**II.2** Su representante legal es la **C. Jennifer Murillo Dominguez**, en su carácter de Apoderada legal, quien manifiesta que a la fecha no le han sido revocadas o de modo alguno limitadas sus facultades de representación y se identifica con Credencial de Elector con clave de elector [redacted] expedida por el Instituto Nacional Electoral y acredita su personalidad con la exhibición del testimonio del poder notarial número **44,770** de fecha **12 de febrero de 2014**, otorgada ante la fe del Notario Público número **120** del Distrito Federal, **Licenciado Miguel Ángel Espíndola Bustillos.**

**II.3** Entre sus objetivos sociales, se encuentra el arrendamiento de este tipo de equipos al que corresponde el objeto de este contrato.

ELIMINADO: CLAVE DE ELECTOR
FUNDAMENTO: ART. 18, FRACCIÓN II (LFTAIPG)
MOTIVACIÓN: POR SER UN NÚMERO IDENTIFICABLE DE UNA PERSONA FÍSICA.

**II.4** Ha considerado todos los factores que se requieren para la ejecución satisfactoria del arrendamiento contratado, así como las especificaciones contenidas en los anexos indicados en la **cláusula Segunda** de este instrumento.

**II.5** Conoce las disposiciones de tipo legal, administrativo, técnico y financiero que norman la celebración y ejecución del presente contrato y acepta someterse a las mismas sin reserva alguna, disponiendo para ello de los elementos técnicos, humanos, materiales y financieros necesarios para el desarrollo eficaz del arrendamiento objeto del presente instrumento contractual.

**II.6** Manifiesta Bajo protesta de decir verdad, que su representada tiene pleno conocimiento que se encuentra sujeta a la aplicación de la Ley Federal Anticorrupción en Contrataciones Públicas, publicada en el Diario Oficial de la Federación el 11 de julio de 2012, la que conoce en su contenido, aplicación, consecuencias jurídicas y cumple, manifestación que incluye a sus accionistas, socios, asociados, representantes, mandantes o mandatarios, apoderados, comisionistas, agentes, gestores, asociados, consultores, subcontratistas, empleados y cualquier otra persona que con cualquiera otro carácter intervenga en su nombre en las contrataciones públicas, a quienes les ha hecho del conocimiento la existencia de la citada ley, su aplicación y consecuencias jurídicas.

**II.7** Bajo protesta de decir verdad, manifiesta que no se encuentra en ninguno de los supuestos previstos en los artículos 50 y 60, antepenúltimo párrafo, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

**II.8** Para los efectos de lo previsto por el artículo 32-D del Código Fiscal de la Federación, ha presentado a **"TELECOMM"** el documento actualizado expedido por el Servicio de Administración Tributaria (SAT), en el que se emite opinión sobre el cumplimiento de sus obligaciones fiscales, prevista en la regla **2.1.27** de la Resolución Miscelánea Fiscal para el ejercicio fiscal 2015, publicada en el Diario Oficial de la Federación el 30 de diciembre de 2014.

**II.9** Su clave del Registro Federal de Contribuyentes es: **GTC980421R4A**.

**II.10** Para el cumplimiento de las obligaciones y derechos que se desprenden del presente instrumento, bajo protesta de decir verdad, manifiesta que su domicilio es el ubicado en: **Avenida Revolución número 1145, Colonia Merced Gómez, Delegación Benito Juárez, C.P. 03930, México, Distrito Federal**, el cual señala para oír y recibir todo tipo de notificaciones y documentos y que asimismo, lo señala para la práctica de notificaciones, aún las de carácter personal que se deriven de este contrato.

Igualmente **"EL ARRENDADOR"** manifiesta expresamente su aceptación de que dicho domicilio podrá ser verificado en cualquier momento por **"TELECOMM"**; conviniendo que en el caso de que llegaré a cambiar su domicilio, lo notificará a **"TELECOMM"** dentro de los quince días naturales siguientes a aquel en que se produzca dicho cambio.

Hechas las declaraciones que anteceden las partes convienen en obligarse y contratar al tenor de las siguientes:

**C l á u s u l a s:**

**Primera. Objeto.**

**"TELECOMM"** encomienda a **"EL ARRENDADOR"** y éste se obliga a dar a **"TELECOMM"**, en arrendamiento el **"Equipo Firewall/VPN y consola de Administración para expansión de Oficinas Telegráficas de la Red Teldat",** y demás condiciones que al efecto se detallan en los anexos indicados en la **Cláusula Segunda**, los que debidamente rubricados y firmados por las partes forman parte integrante del presente instrumento contractual.

**Segunda. Relación de anexos.**

Son parte integrante de este contrato los **anexos** que a continuación se enumeran:

**I.-** Propuesta Técnica.

**II.-** Propuesta Económica.

Los **anexos** antes descritos debidamente firmados por las partes, quedan integrados al presente contrato.

**Tercera. Importe del contrato.**

**"TELECOMM"** pagará a **"EL ARRENDADOR"** en concepto de contraprestación por la realización de los servicios objeto del presente contrato un **importe máximo** que asciende a la cantidad de **$90'517,241.38 (Noventa millones quinientos diecisiete mil doscientos cuarenta y un pesos 38/100 M.N.),** más la cantidad de **$14'482,758.62 (Catorce millones cuatrocientos ochenta y dos mil setecientos cincuenta y ocho pesos 62/100 M.N.**), por concepto del 16% de Impuesto al Valor Agregado, lo que hace un importe total de **$105'000,000.00 (Ciento cinco millones de pesos 00/100M.N.).**

**"TELECOMM"**, se compromete a ejercer un importe mínimo el cual no podrá ser inferior al 40% del importe máximo del presente contrato, de conformidad con lo establecido en el Articulo 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

El **importe mínimo** de los servicios asciende a la cantidad de **$36'206,896.55 (Treinta y seis millones doscientos seis mil ochocientos noventa y seis pesos 55/100 M.N.**), más la cantidad de **$5'793,103.45 (Cinco millones setecientos noventa y tres mil ciento tres pesos 45/100 M.N.**), por concepto del 16% de Impuesto al Valor Agregado, lo que hace un importe total de **$42'000,000.00 (Cuarenta y dos millones de pesos 00/100 M.N.).**

**Para el ejercicio fiscal 2015**, **"TELECOMM"** pagará a **"EL ARRENDATARIO"** en concepto de contraprestación por la realización del arrendamiento, objeto del presente contrato, un importe máximo que asciende a la cantidad de **$12'500,000.00 (Doce millones quinientos mil pesos 00/100 M.N.),** más la cantidad de **$2'000,000.00 (Dos**

**millones de pesos 00/100 M.N.),** por concepto del16% de Impuesto al Valor Agregado, lo que hace un importe total de **$14'500,000.00 (Catorce millones quinientos mil pesos 00/100 M.N.).**

**"TELECOMM"**, se compromete a ejercer un importe mínimo el cual no podrá ser inferior al 40% del importe máximo del presente convenio, de conformidad con lo establecido en el Artículo 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

El importe mínimo del arrendamiento asciende a la cantidad de **$5'000,000.00** (Cinco millones pesos 00/100 M.N.), más la cantidad de **$800,000.00 (Ochocientos mil pesos 00/100 M.N.),** por concepto del 16% del Impuesto al Valor Agregado, lo que hace un importe total de **$5'800,000.00 (Cinco millones ochocientos mil pesos 00/100 M.N.).**

**Para el ejercicio fiscal 2016**, **"TELECOMM"** pagará a **"EL ARRENDATARIO"** en concepto de contraprestación por la realización del arrendamiento, objeto del presente contrato, un importe máximo que asciende a la cantidad de **$30'172,413.79 (Treinta millones ciento setenta y dos mil cuatrocientos trece pesos 79/100 M.N.),** más la cantidad de **$4'827,586.21 (Cuatro millones ochocientos veintisiete mil quinientos ochenta y seis pesos 21/100 M.N.),** por concepto del16% de Impuesto al Valor Agregado, lo que hace un importe total de **$35'000,000.00 (Treinta y cinco millones de pesos 00/100 M.N.).**

**"TELECOMM"**, se compromete a ejercer un importe mínimo el cual no podrá ser inferior al 40% del importe máximo del presente convenio, de conformidad con lo establecido en el Artículo 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

El importe mínimo del arrendamiento asciende a la cantidad de **$12'068,965.52 (Doce millones sesenta y ocho mil novecientos sesenta y cinco pesos 52/100 M.N.**), más la cantidad de **$1'931,034.48 (Un millón novecientos treinta y un mil treinta y cuatro pesos 48/100 M.N.),** por concepto del 16% del Impuesto al Valor Agregado, lo que hace un importe total de **$14'000,000.00 (Catorce millones de pesos 00/100 M.N.).**

**Para el ejercicio fiscal 2017**, **"TELECOMM"** pagará a **"EL ARRENDATARIO"** en concepto de contraprestación por la realización del arrendamiento, objeto del presente contrato, un importe máximo que asciende a la cantidad de **$30'172,413.79 (Treinta millones ciento setenta y dos mil cuatrocientos trece pesos 79/100 M.N.),** más la cantidad de **$4'827,586.21 (Cuatro millones ochocientos veintisiete mil quinientos ochenta y seis pesos 21/100 M.N.),** por concepto del16% de Impuesto al Valor Agregado, lo que hace un importe total de **$35'000,000.00 (Treinta y cinco millones de pesos 00/100 M.N.).**

**"TELECOMM"**, se compromete a ejercer un importe mínimo el cual no podrá ser inferior al 40% del importe máximo del presente convenio, de conformidad con lo establecido en el artículo 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

El importe mínimo del arrendamiento asciende a la cantidad de **$12'068,965.52** (**Doce millones sesenta y ocho mil novecientos sesenta y cinco pesos 52/100 M.N.**), más la cantidad de **$1'931,034.48 (Un millón novecientos treinta y un mil treinta y cuatro pesos 48/100 M.N.),** por concepto del 16% del Impuesto al Valor Agregado, lo que hace un importe total de **$14'000,000.00 (Catorce millones de pesos 00/100 M.N.).**

**Para el ejercicio fiscal 2018**, **"TELECOMM"** pagará a **"EL ARRENDATARIO"** en concepto de contraprestación por la realización del arrendamiento, objeto del presente contrato, un importe máximo que asciende a la cantidad de **$17,672,413.79 (Diecisiete millones seiscientos setenta y dos mil cuatrocientos trece pesos 79/100 M.N.),** más la cantidad de **$2,827,586.21 (Dos millones ochocientos veintisiete mil quinientos ochenta y seis pesos 21/100 M.N.),** por concepto del16% de Impuesto al Valor Agregado, lo que hace un importe total de **$20,500,000.00 (Veinte millones quinientos mil pesos 00/100 M.N.).**

**"TELECOMM"**, se compromete a ejercer un importe mínimo el cual no podrá ser inferior al 40% del importe máximo del presente convenio, de conformidad con lo establecido en el Artículo 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

El importe mínimo del arrendamiento asciende a la cantidad de **$7'068,965.52 (Siete millones sesenta y ocho mil novecientos sesenta y cinco pesos 52/100 M.N.),** más la cantidad de **$1'131,034.48 (Un millón ciento treinta y un mil treinta y cuatro pesos 48/100 M.N.),** por concepto del 16% de Impuesto al Valor Agregado, lo que hace un importe total de **$8'200,000.00 (Ocho millones doscientos mil pesos 00/100 M.N.).**

El precio unitario de los servicios contratados se detalla en la **Propuesta Económica**, la que debidamente firmada y rubricada por las partes se agrega a este instrumento para formar parte integrante del mismo.

Los precios unitarios del presente contrato, son fijos y no estarán sujetos a fórmula escalatoria alguna durante la vigencia del mismo, por lo que, si **"EL ARRENDADOR"** realiza trabajos por mayor precio unitario del indicado, independientemente de la responsabilidad en que incurra por la ejecución de los trabajos correspondientes, no tendrá derecho a reclamar pago alguno en concepto de ello.

**Cuarta. Forma de pago.**

**"TELECOMM"** pagará a **"EL ARRENDADOR"** el importe pactado en la cláusula que antecede en parcialidades, una vez que se haya suscrito el contrato, concluido el mes de facturación, ya que el arrendamiento se pagará a mes **vencido**, en moneda nacional, dentro del plazo de 20 (veinte) días naturales contados a partir de la entrega y aceptación de la factura correspondiente y demás documentos en que conste la debida entrega de los **bienes** a entera satisfacción de la **Subdirección de Desarrollo de informática,** lo anterior conforme a lo estipulado en el artículo 51 de la ley de Adquisiciones, Arrendamientos y Servicios del sector público.

Dichos pagos se efectuarán a través de transferencia electrónica de fondos vía pago interbancario, en la cuenta bancaria número: [redacted] CLABE: [redacted] Sucursal: número [redacted] Plaza: [redacted] de la institución bancaria: [redacted] Para tal efecto, **"EL ARRENDADOR"** deberá presentar a la firma del presente instrumento, el formato denominado solicitud de pago a través del servicio interbancario debidamente requisitado".

Las partes convienen expresamente que las obligaciones de este contrato, cuyo cumplimiento se encuentra previsto realizar durante los ejercicios fiscales de **2016, 2017 y 2018**, quedarán sujetas para fines de su ejecución y pago a la disponibilidad presupuestaria, con que cuente **"TELECOMM"**, conforme al Presupuesto de Egresos de la Federación que para el ejercicio fiscal correspondiente apruebe la Cámara de Diputados del H. Congreso de la Unión, sin que la no realización de la referida condición suspensiva origine responsabilidad para alguna de las partes.

En caso de incumplimiento en los pagos por parte de **"TELECOMM"**, a solicitud de **"EL ARRENDADOR"**, **"TELECOMM"** deberá pagar gastos financieros, conforme al procedimiento establecido en la Ley de Ingresos de la Federación para el ejercicio fiscal respectivo, como si se tratara del supuesto de prórroga para el pago de créditos fiscales. Dichos gastos se calcularán sobre las cantidades no pagadas y se computarán por días naturales desde que se venció el plazo pactado, hasta que se pongan efectivamente las cantidades a disposición de **"EL ARRENDADOR"**.

Tratándose de pagos en exceso que haya recibido **"EL ARRENDADOR"**, éste deberá de reintegrar las cantidades pagadas en exceso más los intereses correspondientes conforme a *(gastos financieros)* la Ley de Ingresos de la Federación para el Ejercicio **Fiscal 2015.** Los cargos se calcularán sobre las cantidades pagadas en exceso en cada caso y se computarán por días naturales desde la fecha del pago hasta la fecha que se pongan efectivamente las cantidades a disposición del **"TELECOMM"**.

De acuerdo a lo dispuesto en el artículo 95 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, las partes convienen que en el caso de penas convencionales, el pago estará condicionado proporcionalmente, al pago que el proveedor deberá efectuar por concepto de penas convencionales por atraso, en el entendido de que si el contrato es rescindido, no procederá el cobro de dichas penas ni la contabilización de las mismas, al hacer efectiva la garantía de cumplimiento.

**Quinta. Vigencia.**

La prestación del servicio será a partir del día **20 de octubre de 2015** hasta el día **31 de julio de 2018** y el inicio de la operación será a partir de las **00:01 hrs. del día 31 de octubre de 2015 hasta las 24:00 hrs del día 31 de julio de 2018.**

**Sexta. Garantía de cumplimiento de contrato.**

**"EL ARRENDADOR"** se obliga a garantizar el cumplimiento de las obligaciones derivadas del presente contrato, mediante fianza expedida por Institución Afianzadora Mexicana, debidamente autorizada para ello, a favor de **"TELECOMM"**, por un importe

equivalente al 10% del monto máximo total del presente contrato, sin incluir el Impuesto al Valor Agregado, debiendo cubrir el plazo de vigencia del mismo, así como el período de garantía de funcionamiento de los servicios contratados.

**"EL ARRENDADOR"** queda obligado a entregar a **"TELECOMM"**, la fianza en cuestión, dentro de los diez días naturales siguientes a la firma del presente instrumento.

En el supuesto de que el monto de este contrato se incremente, **"EL ARRENDADOR"** se obliga a mantener la fianza en el porcentaje que se menciona en el párrafo primero de la presente cláusula.

La póliza de fianza deberá contener las siguientes declaraciones expresas de la Institución Afianzadora:

1. Que la fianza se otorga para garantizar todas las obligaciones, incluyendo la entrega de los bienes prestación de los servicios, penas convencionales y el período de garantía de funcionamiento, atendiendo además todas las estipulaciones contenidas en el contrato.
2. Que la vigencia de la póliza de fianza será determinada y comprenderá la vigencia del contrato garantizado, así como el plazo máximo de garantía establecido en la cláusula Séptima del presente instrumento contractual, y que en caso de reclamación se deberá realizar dentro de los 180 días naturales siguientes, contados a partir de la terminación de la vigencia pactada del contrato o del período máximo de garantía establecida entre "EL ARRENDADOR" y "TELECOMM", lo anterior **conforme a lo dispuesto en el artículo 174 y 175 de la Ley de Instituciones de Seguros y de Fianzas.**
3. Que la fianza otorgada para garantizar el cumplimiento del referido contrato continuará vigente aún en el caso de que se otorgue prórroga, espera, ampliación al monto o al plazo de ejecución del mismo contrato. En virtud de lo anterior, la afianzadora renuncia expresamente al derecho de manifestar el consentimiento a que se refiere el artículo **179 de la Ley de Instituciones de Seguros y de Fianzas**, por lo que, **"EL ARRENDADOR"**, se obliga a realizar las acciones necesarias a fin de mantener la fianza en el porcentaje que se menciona en el párrafo primero de la presente cláusula.
4. Que acepta expresamente someterse a lo previsto en los artículos **279, 282, 283 y 178** de la Ley de Instituciones de Seguros y de Fianzas.
5. Que permanecerá vigente durante la substanciación de cualquier recurso o juicio que se interponga hasta que se dicte resolución definitiva y firme por autoridad judicial o administrativa, salvo que las partes se otorguen el finiquito.
6. Que para liberar la fianza, será requisito indispensable contar con la constancia de cumplimiento total de las obligaciones contractuales y la manifestación expresa y por escrito de **"TELECOMM"** por medio de la **Subdirección de Recursos Materiales y Servicios Generales.**

7. Que la afianzadora acepta expresamente someterse a los procedimientos establecidos en el artículo **279 Ley de Instituciones de Seguros y de Fianzas**, aún para el caso de que procediera el cobro de intereses con motivo del pago extemporáneo del importe de la póliza de fianza requerida.
8. Que en caso de que exista finiquito y existan saldos a cargo de **"EL ARRENDADOR"** y éste efectúe la totalidad del pago en forma incondicional, **"TELECOMM"** por medio de la **Subdirección de Recursos Materiales y Servicios Generales**, deberá liberar la fianza respectiva que se haya otorgado.
9. Que la fianza garantiza la ejecución total de los servicios objeto del contrato, y en su caso de la entrega de los bienes vinculados al mismo.
10. Que la afianzadora se someterá expresamente a la jurisdicción y competencia de los Tribunales Federales en el Distrito Federal, renunciando al fuero que pudiera corresponderle en razón de su domicilio presente o futuro, o por cualquier otra causa.

**Séptima. Garantía Técnica.**

**"EL ARRENDADOR"** manifiesta que se obliga a cumplir la garantía técnica en los siguientes términos:

**"EL ARRENDADOR"** dará Garantía de la infraestructura instalada durante la vigencia del contrato a partir de la fecha de entrega a entera satisfacción de **"TELECOMM"**.

**"EL ARRENDADOR"** será el único responsable de resolver cualquier condición operativa, ya sea física o lógica (mantenimiento de las plataformas y actualización de las plataformas) relacionada con los equipos ofertados (consolas, firewalls, appliance centrales y remotos) durante la vigencia del contrato.

Asimismo, **"EL ARRENDADOR"** se obliga a proporcionar a **"TELECOMM"** lo siguiente: (se enlistan de manera enunciativa, más no limitativa):

- ✓ Soporte técnico, (soporte del elemento de red, soporte del software del elemento), durante el ciclo de vida de cada uno de los equipos ofertados.
- ✓ Proveer cuantas veces se necesite las refacciones necesarias para las consolas y equipos firewalls appliance centrales y remotos sin costo para **"TELECOMM"**.
- ✓ **Reparación de fallas lógicas y restauración de configuraciones.**
- ✓ **"EL ARRENDADOR"** deberá acudir al sitio cuantas veces sea necesario en caso de necesitar reparación o sustitución de los dispositivos.
- ✓ **"EL ARRENDADOR"** deberá realizar la configuración, traslado y puesta en operación del equipo ofertado reasignado a un sitio por reemplazo, por cambio de domicilio.

**Octava. Administración y verificación del contrato.**

**"TELECOMM"** designa al servidor público y **"EL ARRENDADOR"** nombra al personal a su cargo, para administrar y verificar el debido cumplimiento del presente contrato, a los siguientes:

| Para efectos de la: | Por "TELECOMM": | Por "EL ARRENDADOR": |
|---|---|---|
| Administración y verificación del cumplimiento del contrato. | **Nombre:** Lic. Roberto Ruiz Domínguez.<br>**Cargo:** Subdirector de Desarrollo de Informática.<br>Domicilio: Eje Central Lázaro Cárdenas número 567, piso 9, ala norte, Colonia Narvarte, Delegación Benito Juárez, Código Postal 03020, en México, Distrito Federal.<br>**Teléfono:** 50901100 Extensión 1438<br>**Correo Electrónico:** roberto.ruiz@telecomm.gob.mx | **Nombre:** C. Jennifer Murillo Domínguez.<br>**Cargo:** Representante Legal.<br>**Domicilio:** Avenida Revolución número 1145, Colonia Merced Gómez, Delegación Benito Juárez, C.P. 03930, México, Distrito Federal.<br>**Teléfono:** 52789210.<br>**Correo Electrónico:** jennifer.murillo@tecno.com.mx |

**"TELECOMM"** a través del servidor público designado para administrar y verificar el debido cumplimiento del presente contrato, efectuará sus funciones conforme a los mecanismos, documentos de comprobación y supervisión, tendrá en todo tiempo el derecho de verificar que la ejecución de los servicios objeto del presente contrato, se ajuste a las especificaciones, lugares de realización, programa, fechas y/o plazos establecidos para la prestación de los servicios, términos de referencia y que sean efectivamente prestados, conforme a los requerimientos de cada entregable y la aceptación de los servicios como se especifica en los Anexos precisados en la cláusula Segunda del presente instrumento y dará por escrito a **"EL ARRENDADOR"** las instrucciones que estime pertinentes en relación con dicha ejecución. **"TELECOMM"** podrá realizar la inspección de la cantidad y la calidad de los materiales y accesorios e instrumentos necesarios para la realización del arrendamiento objeto de este contrato que en su caso, deban utilizarse en la ejecución de los servicios objeto de este instrumento.

**"TELECOMM"**, podrá nombrar sustituto del servidor público designado a través de su **Director de Operaciones Telegráficas** y **"EL ARRENDADOR"**, podrá sustituir a la persona nombrada a través de su representante legal, dando aviso a la otra parte por escrito con quince días naturales de anticipación, quienes deberán mantener los registros necesarios de las actividades ejecutadas con motivo de la realización de los servicios objeto del presente contrato.

Asimismo, **"TELECOMM"** y **"EL ARRENDADOR"** designan de su parte a la persona antes indicada para recibir notificaciones relacionadas con el presente contrato.

Cualquier notificación, solicitud o comunicado entre las partes que deba ser entregado o elaborado de acuerdo a lo dispuesto en este contrato y sus anexos, se formulará por escrito, mismos que deberán ser entregados en forma personal al servidor público designado por **"TELECOMM"** o el personal autorizado por **"EL ARRENDADOR"**, en los que deberá estamparse la firma autógrafa y la fecha de recepción de quién reciba la

notificación, solicitud o comunicado, en el caso de preferir la entrega por correo electrónico o fax deberá enviarse al servidor público o a la persona autorizada, según sea el caso, en el entendido de que el receptor deberá acusar de recibido dichos documentos, caso contrario el emisor deberá entregar el comunicado al día siguiente de su transmisión en forma personal y obtendrá el acuse de recibido de la persona designada o autorizada, según sea el caso en horas de oficina en los domicilios que se señalan en este contrato, como corresponda.

**Novena. Responsabilidades de "EL ARRENDADOR".**

Durante la vigencia del presente contrato o hasta que se realicen la totalidad de los servicios objeto del mismo **"EL ARRENDADOR"**, se obliga a:

a) Que la prestación de los servicios objeto del presente contrato, se realice con estricto apego a las especificaciones, lugares de realización, programa, fechas y/o plazos de prestación, términos de referencia y demás condiciones que al efecto se detallan en los anexos que firmados por las partes forman parte integral del mismo.

b) Ejecutar los servicios contratados empleando su máximo esfuerzo, experiencia, organización y personal especializado para que la prestación de dichos servicios sea de la mejor calidad.

c) Entregar a **"TELECOMM"** el (los) reporte(s) y/o la información de los servicios objeto del presente instrumento que hayan sido realizados durante el mes correspondiente.

d) Responder en cualquier caso, de la deficiente calidad de los servicios objeto de este contrato, así como de los defectos y vicios ocultos de los bienes que en su caso utilicen para la realización de los mismos, así como de asumir cualquier responsabilidad en que hubiere incurrido, en los términos señalados en este contrato de conformidad con lo previsto por el segundo párrafo del artículo 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público;

e) Proporcionar a **"TELECOMM"** y/o a las dependencias o entidades que tengan que intervenir, los datos necesarios para la inspección de los servicios objeto del presente contrato.

f) Hacer efectivas en los términos pactados, las garantías establecidas en la cláusula Séptima del presente contrato, dentro de los cinco días naturales siguientes a la fecha en que le comunique la realización del acto o hecho que de lugar a su exigibilidad, incluso durante el plazo máximo de garantía que se haya establecido a partir de que concluya la vigencia del presente contrato y sus prórrogas y/o ampliaciones, en su caso.

En relación con la ejecución de los servicios objeto de este contrato, las partes convienen que **"TELECOMM"** a través del **Licenciado Roberto Ruiz Dominguez, Subdirector de Desarrollo de Informática y/o quien lo sustituya en el cargo**, tendrá la facultad para juzgar acerca de: i) la cantidad y la calidad de los materiales, ii) calidad y cantidad de los accesorios e instrumentos necesarios para realizar el arrendamiento

objeto de este contrato, iii) la mano de obra empleada y iv) El cumplimiento de las especificaciones establecidas en los anexos; y, que de ser el caso rechazará por escrito y con razones técnicamente fundadas los servicios que no estén conforme a lo estipulado en este contrato, notificando a **"EL ARRENDADOR"**, para lo cual el personal autorizado girara instrucciones a efecto de que corrija las fallas de calidad de los servicios objeto del presente contrato o incumplimiento de las especificaciones establecidas en los anexos del mismo, por parte de **"TELECOMM"**.

**"EL ARRENDADOR"** deberá realizar los servicios o reposiciones necesarias, dentro de un plazo que no excederá del establecido en el **anexo I Propuesta Técnica** a partir de que se levante el reporte del incidente, sin que tenga derecho a retribución alguna por concepto de dichos servicios o reposiciones.

Si **"EL ARRENDADOR"** no atendiere los requerimientos de **"TELECOMM"**, éste último podrá elegir libremente entre exigir que se realicen nuevamente los servicios o se sustituyan los materiales o accesorios, conforme a las especificaciones determinadas o encomendar a un tercero la reposición de que se trate con cargo a **"EL ARRENDADOR"**; en su caso, hacer efectiva la garantía de cumplimiento del contrato o ejercitar las acciones correspondientes por daños y perjuicios derivados del incumplimiento de las obligaciones contraídas para la prestación de los servicios contratados.

Si durante la vigencia del contrato o al término de éste existieren responsabilidades a cargo de **"EL ARRENDADOR"**, sus importes se deducirán del saldo a su favor, pero si este último no fuera suficiente, **"TELECOMM"**, en su caso, hará efectiva la garantía de cumplimiento de contrato que al efecto haya presentado **"EL ARRENDADOR"**.

**Décima. Daños y Perjuicios.**

Los daños y perjuicios que se causen a **"TELECOMM"** y/o a terceros con motivo de la prestación de los servicios objeto de este contrato, por negligencia, inobservancia, impericia, dolo o mala fe de **"EL ARRENDADOR"**, o por el mal uso que éste haga de las instalaciones o bienes de **"TELECOMM"** durante la prestación de los referidos servicios, serán de la responsabilidad directa de **"EL ARRENDADOR"** , el cual se obliga a resarcir a **"TELECOMM"** de dichos daños o perjuicios, cubriendo los importes que al efecto se determinen.

Para los efectos de lo establecido en esta cláusula **"EL ARRENDADOR"** , dentro de los diez días naturales siguientes a la fecha de formalización del presente contrato, deberá presentar una póliza de responsabilidad civil general por una suma asegurada equivalente al 10% del importe máximo total del contrato antes de I.V.A., que cubra los riesgos por pérdida, daños y perjuicios o responsabilidad que sufra **"TELECOMM"**, derivados de la prestación de los servicios objeto de este contrato, la cual deberá estar vigente durante el período de vigencia del mismo, así como durante sus prórrogas, esperas o ampliaciones si las hubiere; en la inteligencia de que en caso de que el importe del siniestro sea mayor a la suma asegurada contratada, el excedente será con cargo a **"EL ARRENDADOR"**. La póliza deberá incluir el número de contrato y la cláusula de beneficiario preferente a favor de **"TELECOMM"**.

**Décima Primera. Cesión.**

**"EL ARRENDADOR"** se obliga a no ceder en forma parcial ni total en favor de cualquier persona los derechos y obligaciones derivados del presente contrato, a excepción de los derechos de cobro, en cuyo caso, deberá previamente solicitarlo por escrito a **"TELECOMM"** y contar con el consentimiento expreso de este último.

**Décima Segunda. Impuestos.**

Los impuestos que se generen por la prestación de los servicios objeto del presente contrato, se pagarán y enterarán por quien los cause conforme a la Legislación Fiscal vigente.

**Décima Tercera. Propiedad de la Información.**

La información fuente proporcionada por **"TELECOMM"**, así como la que resulte de la prestación del servicio objeto de este contrato, será en todo momento propiedad exclusiva de **"TELECOMM"**, a excepción de los derechos de autor u otros derechos exclusivos; en razón de lo anterior **"EL ARRENDADOR"** se obliga a guardar total y absoluta reserva de la información que se le proporcione o a la que tenga acceso con motivo de los servicios objeto de este contrato, comprometiéndose a utilizar dicha información exclusivamente para los fines del mismo, por lo que, no podrá divulgarla en provecho propio o de terceros.

**"EL ARRENDADOR"** deberá proporcionar a la Secretaría de la Función Pública y al Órgano Interno de Control en **"TELECOMM"**, la información y/o documentación relacionada con el presente contrato, que en su momento se le requiera con motivo de las auditorias, visitas o inspecciones que se practiquen.

**Décima Cuarta. Lugar de Prestación del Servicio.**

Los servicios objeto de este contrato se prestarán en **los domicilios e inmuebles** especificados en la **Propuesta Técnica** de este contrato, y con estricto apego a las especificaciones, programa, fechas y/o plazos de prestación de los servicios, términos de referencia y demás condiciones descritas en el citado anexo.

**"EL ARRENDADOR"** deberá de entregar un "Plan de Trabajo detallado", incluyendo las actividades a desempeñar para alcanzar los plazos establecidos, considerando los siguientes puntos los cuales son enunciativos más no limitativos:

**"TELECOMM"** requiere que el servicio solicitado inicie su operación de acuerdo como se especifica en la siguiente tabla para los diferentes NODOS, las actividades descritas son enunciativas más no limitativas, **"EL ARRENDADOR"** deberá de dar cumplimiento a los siguientes puntos:

IMPLEMENTACIÓN PARA EQUIPOS CENTRALES
ACTIVIDADES: Instalación, Configuración y pruebas de conectividad.

| EQUIPO | SITIO | FECHA LIMITE DE IMPLEMENTACION |
|---|---|---|
| 2 CONSOLAS DE ADMINISTRACION Y SISTEMAS DE GESTION | TCT Y CTO | 30 OCTUBRE 2015. |
| 10 FIREWALL'S CENTRALES | 7 FIREWALL'S EN CTO | 30 OCTUBRE 2015 |
| | 2 FIREWALL'S EN TCT | 06 NOVIEMBRE 2015 |
| | 1 FIREWALL'S EN TULANCINGO | 13 NOVIEMBRE 2015 |

PROPUESTA EN OPERACIÓN PARA EQUIPOS CENTRALES
ACTIVIDADES: Inicio de operación.

| EQUIPO | SITIO | FECHA LIMITE DE IMPLEMENTACION |
|---|---|---|
| 2 CONSOLAS DE ADMINISTRACION Y SISTEMAS DE GESTION | TCT Y CTO | 31 OCTUBRE 2015. |
| 10 FIREWALL'S CENTRALES | 7 FIREWALL'S EN CTO | 31 OCTUBRE 2015 |
| | 2 FIREWALL'S EN TCT | 07 NOVIEMBRE 2015 |
| | 1 FIREWALL'S EN TULANCINGO | 14 NOVIEMBRE 2015 |

IMPLEMENTACIÓN Y PUESTA EN OPERACIÓN PARA EQUIPOS REMOTOS ACTIVIDADES: Instalación, Configuración y pruebas de conectividad, inicio de operación.

| EQUIPO | SITIO | FECHA LIMITE DE IMPLEMENTACION |
|---|---|---|
| • 32 FIREWALL'S REMOTOS PARA GERENCIAS ESTATALES<br>Y<br>•1,200 FIREWALL'S REMOTOS PARA OFICINAS TELEGRAFICAS | REGION I<br>EdoMex, Guerrero, Hidalgo, Morelos, Puebla, Querétaro, D.F. y Tlaxcala (aproximadamente 266 equipos) | 13 NOVIEMBRE 2015 |
| | REGION II<br>Aguascalientes, Colima, Guanajuato, Jalisco, Michoacán, Nayarit y Zacatecas (aproximadamente 306 equipos) | |
| | REGION III<br>Coahuila, Durango, Nuevo León, San Luis Potosí y Tamaulipas (aproximadamente 196 equipos) | 30 NOVIEMBRE 2015 |
| | REGION IV<br>BCN, BCS, Chihuahua, Sinaloa y Sonora (aproximadamente 192 equipos) | |

| | | |
|---|---|---|
| | REGION V Campeche, Chiapas, Oaxaca, Quintana Roo, Tabasco, Veracruz y Yucatán (aproximadamente 279 equipos) | 31 DICIEMBRE 2015 |
| 400 FIREWALL'S REMOTOS PARA OFICINAS TELEGRAFICAS | DISTRIBUCION A NIVEL NACIONAL | DURANTE LA VIGENCIA DEL CONTRATO A SOLICITUD DE TELECOMM |

**Décima Quinta. Prórrogas.**

Las partes acuerdan que conforme a lo dispuesto en el artículo 91 párrafos segundo y tercero del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, el presente contrato únicamente se podrá prorrogar en caso de presentarse caso fortuito, causa de fuerza mayor, o cuando por alguna causa imputable a **"TELECOMM"** la prestación de los servicios objeto de este contrato no pueda realizarse en la fecha o plazo pactado para ello.

Para los efectos de proceder a la modificación del presente contrato, en vía de prórroga por caso fortuito o causa de fuerza mayor, **"EL ARRENDADOR"** deberá presentar a **"TELECOMM"** la solicitud por escrito, en la que se hará constar el caso concreto acompañándose de los medios de prueba pertinentes; una vez que **"TELECOMM"** reciba la solicitud aludida, se procederá a la revisión de la misma y dentro de un plazo que no exceda de **(3)** tres días hábiles determinará la procedencia o improcedencia de la misma.

En el supuesto de que la solicitud de prórroga, se fundamente en causa imputable a **"TELECOMM"**, no se requerirá la previa solicitud de **"EL ARRENDADOR".**

En cualquiera de los supuestos a que se hace alusión en los párrafos inmediatos anteriores, se deberá formalizar el convenio modificatorio correspondiente, en el que se hará constar la nueva fecha o plazo pactados en vía de prórroga para la prestación de los servicios objeto de este contrato, conviniéndose que en estos mismos supuestos no habrá lugar a la aplicación de penas convencionales por atraso en el cumplimiento de las fechas o plazos pactados originalmente.

**Décima Sexta. Modificaciones al contrato.**

Las modificaciones que por razones fundadas pudieran realizarse al presente contrato, incluidas las adecuaciones por incremento en la cantidad de los servicios objeto del mismo, deberán constar por escrito en términos de lo dispuesto en el artículo 52 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

En el caso de que se incremente la cantidad del arrendamiento objeto de este contrato **"TELECOMM"** notificará a **"EL ARRENDADOR"** dicho incremento en forma desglosada, detallando las especificaciones correspondientes, observándose que el monto total de las modificaciones no rebase, en conjunto, el 20% (veinte por ciento) del monto o cantidad de los conceptos y volúmenes establecidos originalmente en el presente contrato y el precio de los servicios sea igual al pactado originalmente.

En su caso se formalizarán los convenios modificatorios correspondientes, debiendo **"EL ARRENDADOR"** comprometerse expresamente a entregar dentro de los **(10)** diez días naturales siguientes a la formalización del mismo(s), la modificación respectiva de la **garantía de cumplimiento,** así como el endoso de la **póliza de Responsabilidad Civil** presentada, lo cual deberá estipularse en el cuerpo de dicho convenio modificatorio, así como las fechas de la prestación del servicio para las cantidades adicionales.

**Décima Séptima. Pena convencional.**

De conformidad a lo dispuesto en el artículo 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, cuando por causas imputables a **"EL ARRENDADOR"** este no realice los servicios objeto del presente contrato en las fechas y/o plazos pactados que se establecen *ex profeso* en el **anexo I Propuesta Técnica** del presente instrumento, fechas y plazos que se consideran como casos concretos para la aplicación de las penas convencionales, conforme a lo dispuesto en el artículo 96 del Reglamento de la citada ley.

**"TELECOMM"** impondrá a **"EL ARRENDADOR"** una pena convencional consistente en una cantidad igual al **(1) uno al millar** aplicado al valor de los servicios que hayan sido prestados con atraso respecto de las fechas y/o convenidas para ello, sin incluir el importe al valor agregado, por cada día natural de atraso.

Esta pena se estipula, por el simple atraso en el cumplimiento de las fechas o plazos pactados para la prestación de los servicios contratados, no excederá del importe de la garantía a que alude la cláusula **Sexta** de este instrumento, y se determinará en función de los servicios no prestados oportunamente, salvo que por las características de los servicios entregados, éstos no puedan funcionar o ser utilizados por **"TELECOMM"** por estar incompletos, en cuyo caso la pena convencional pactada se aplicará por el total de la garantía correspondiente.

En términos de lo dispuesto en el penúltimo párrafo del artículo 100 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en los casos en que un servicio o parte del mismo no es efectuado y la pena convencional por atraso, rebase el monto de la pena establecida de manera proporcional respecto de la parte no realizada en las fechas pactadas, **"TELECOMM"**, previa notificación al proveedor respectivo, sin rescindir el contrato correspondiente, podrá modificarlo, cancelando los servicios no realizados de que se trate, o bien parte de los mismos, aplicando al proveedor una sanción por cancelación, equivalente a la pena convencional por atraso máxima que correspondería en el caso de que los servicios hubieran sido entregados en fechas posteriores a la pactada para la entrega, siempre y cuando la suma total del monto de las cancelaciones no rebase el **10% (diez por ciento)** del importe total del contrato. En el supuesto de que sea rescindido el contrato, no procederá la contabilización de dicha sanción al hacer efectiva la garantía de cumplimiento.

**Décima Octava. Procedimiento para la aplicación de la pena convencional.**

El área designada por **"TELECOMM"** para los efectos de **administrar y verificar** el presente contrato, con base en los documentos comprobatorios correspondientes, elaborará el o los informes sobre el o los atrasos en que hubiere incurrido **"EL ARRENDADOR"** en la prestación de los servicios contratados, respecto de las fechas o plazos pactados para tal efecto. Una vez determinado el atraso, **dicha área notificará por escrito a "EL ARRENDADOR"** para que en el plazo de (5) cinco días naturales contados a partir de la fecha de tal notificación, manifieste lo que a su derecho convenga.

Si transcurrido el plazo en mención **"EL ARRENDADOR"** no hace manifestación alguna en su defensa, o si después de analizar las razones aducidas por éste, **"TELECOMM"** estima que las mismas no son pertinentes, se procederá a la cuantificación de la pena convencional correspondiente, haciéndolo del conocimiento de **"EL ARRENDADOR"**, para los efectos de su pago, acordándose por las partes que dichas penas podrán hacerse efectivas con cargo al importe de los servicios realizados pendientes de pago, y/o mediante la ejecución de la garantía de cumplimiento otorgada en el mismo; en el entendido de que en el supuesto de que sea rescindido este, no procederá el cobro de dichas penas.

Asimismo, las partes convienen que el pago de los servicios objeto del presente contrato, quedará condicionado proporcionalmente, al pago que **"EL ARRENDADOR"** deba efectuar en concepto de penas convencionales por atraso en las fechas o plazos pactados para la prestación de los servicios objeto de este contrato.

**Décima Novena. Deducciones por cumplimiento parcial o deficiente de los servicios.**

Las partes convienen que si **"EL ARRENDADOR"**, cumple sólo parcialmente los servicios objeto de este contrato o bien se observan deficiencias en la prestación de los mismos, tales circunstancias serán consideradas incumplimientos parciales y **"TELECOMM"** deducirá del pago correspondiente a **"EL ARRENDADOR"** el importe que resulte de calcular la parte proporcional de cada servicio en que se observe tal incumplimiento, asimismo, se conviene que el límite de las deducciones que se apliquen, por cumplimiento parcial o deficiente de los servicios de que se trate, no podrá exceder en su conjunto del 20% del monto total del contrato y en el supuesto de que se exceda ese porcentaje, se procederá a la rescisión de este instrumento contractual.

Las deductivas, se aplicarán en el siguiente caso específico:

Cuando por causas imputables a **"EL ARRENDADOR"** no se proporcione el servicio solicitado, **"TELECOMM"** le impondrá una deductiva equivalente al 2% del importe mensual en la etapa de Operación correspondiente al Ambiente de Producción, por cada décima debajo del Nivel de Servicio solicitado en el Numeral **"11.1.-Niveles de Servicio (SLA)"** de la Propuesta Técnica, para los ambientes productivos (No imputable a fallos provocados por factores externos, no propios a la infraestructura).

**Vigésima. Terminación anticipada.**

**"TELECOMM"** podrá dar por terminado anticipadamente el presente contrato, en cualquier momento sin responsabilidad alguna, por razones de interés general o cuando por causas justificadas, se extinga la necesidad de requerir los servicios originalmente contratados y se demuestre que de continuar con el cumplimiento de las obligaciones pactadas, se ocasionaría algún daño o perjuicio a **"TELECOMM"** o al Estado, o cuando se determine la nulidad total o parcial de los actos que dieron origen al contrato, con motivo de la resolución de una inconformidad emitida por la Secretaría de la Función Pública.

Para efectos de lo anterior, se emitirá un dictamen debidamente fundado y motivado, dando aviso a **"EL ARRENDADOR",** por escrito con quince días naturales de anticipación.

En caso de que **"TELECOMM"** decida terminar anticipadamente el presente contrato, reembolsará a **"EL ARRENDADOR"** los gastos no recuperables en que haya incurrido, siempre que éstos sean razonables, estén debidamente comprobados y se relacionen directamente con este contrato.

**Vigésima Primera. Rescisión administrativa.**

**"TELECOMM"** podrá rescindir administrativamente el presente contrato, sin necesidad de declaración judicial, cuando **"EL ARRENDADOR"** incurra en una o varias de las causas que a continuación se enumeran:

1. Porque no otorgue en tiempo y forma la **fianza de cumplimiento** a que se refiere la **cláusula Sexta** y/o la póliza de responsabilidad civil a que alude la **cláusula Décima** de este instrumento contractual.
2. Si por causa imputable a él, no inicia en la fecha convenida la prestación de los servicios objeto de este contrato o suspenda injustificadamente, de manera total o parcial la ejecución de los mismos.
3. Por prestar los servicios deficientemente o por no apegarse a lo estipulado en el presente contrato y sus anexos o porque sin motivo justificado, no atienda las instrucciones que **"TELECOMM"** le indique en términos de lo establecido en la cláusula Novena de este instrumento contractual.
4. Si no brinda a **"TELECOMM"** y/o a las dependencias que tengan que intervenir, los datos necesarios para la inspección de los servicios objeto del presente contrato.
5. Si se comprueba que la manifestación a que se refiere la declaración II.7, se realizó con falsedad o bien resulta falsa la información proporcionada en su propuesta de servicios.
6. En el caso de que alguna autoridad competente lo declare en concurso mercantil, suspensión de pagos, quiebra, concurso de acreedores o cualquier otra figura análoga, o bien se encuentre en cualquier otra situación que afecte a su patrimonio en forma tal que le impida cumplir con

las obligaciones contraídas en razón de este contrato.

7. Porque transmita, total o parcialmente los derechos y obligaciones derivados de este contrato.

8. Porque incurra en las causales de rescisión previstas en la presente cláusula y en la cláusula Vigésima Tercera de este instrumento contractual.

9. Cuando se agote el monto máximo de aplicación de penas convencionales por atraso, en el cumplimiento de las fechas o plazos pactados exprofeso para la prestación de los servicios objeto de este contrato y persista dicho atraso.

10. Porque incumpla cualquiera de las obligaciones consignadas a su cargo en este contrato, siempre que dicho incumplimiento no se derive del atraso en las fechas pactadas para la ejecución de los servicios objeto de este instrumento; o por el incumplimiento de las disposiciones de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y su Reglamento.

En términos de lo dispuesto por el artículo 81 fracción II, del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en caso de rescisión del presente contrato la aplicación de la garantía de cumplimiento, se hará efectiva por el monto total de la obligación garantizada, salvo que en los contratos se haya estipulado su divisibilidad. En caso que por las características de los servicios prestados, éstos no puedan funcionar o ser utilizados por la dependencia o entidad por estar incompletos, la garantía se hará siempre efectiva por el monto total de la obligación garantizada.

**Vigésima Segunda. Procedimiento de rescisión.**

Si **"TELECOMM"** considera que **"EL ARRENDADOR"** ha incurrido en alguna de las causas de rescisión consignadas en la cláusula que antecede, o en su caso, se hubiere agotado el monto límite de aplicación de penas convencionales, lo comunicará por escrito a éste para que en un término de **5 (cinco)** días hábiles exponga lo que a su derecho convenga respecto del incumplimiento de su obligación y aporte en su caso las pruebas que estime convenientes; si transcurrido el término en mención **"EL ARRENDADOR"** no hace manifestación alguna en su defensa, o si después de analizar las razones aducidas por éste, **"TELECOMM"** estima que las mismas no son pertinentes, en un término de **15 (quince) días naturales dictará** la resolución que en derecho proceda, de conformidad a lo dispuesto en el artículo 54 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

Concluido el procedimiento de rescisión, se formulará el finiquito correspondiente, dentro de los **(20)** veinte días naturales siguientes a la fecha en que se notifique la rescisión, a efecto de hacer constar los pagos que deban efectuarse y demás circunstancias del caso. Al efecto deberá considerarse lo dispuesto en los artículos 99 y en el inciso b) fracción I y en la fracción III del artículo 103 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, ello, sin perjuicio de lo dispuesto del artículo 60 fracción III de la referida Ley.

Si previamente a la determinación de dar por rescindido el presente contrato, se prestaran los servicios conforme al mismo, el procedimiento de rescisión iniciado quedará sin efecto, previa aceptación y verificación de **"TELECOMM"** de que continúa vigente la necesidad de los mismos y que se hayan aplicado en su caso las penas convencionales correspondientes.

En términos de lo dispuesto en los artículos 54 fracción III, segundo párrafo de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 98 tercer párrafo del Reglamento de la propia Ley **"TELECOMM"**, podrá suspender el trámite del procedimiento de rescisión, cuando se hubiere iniciado un procedimiento de conciliación respecto del contrato materia de la rescisión.

En el supuesto de que se determine no dar por rescindido el contrato, **"TELECOMM"** establecerá con **"EL ARRENDADOR"** otro plazo que le permita subsanar el incumplimiento que hubiere motivado el inicio del procedimiento y se deberá ampliar la vigencia de la fianza de garantía.

**Vigésima Tercera. Derechos de propiedad intelectual.**

**"EL ARRENDADOR"** asume cualquier tipo de responsabilidad por las violaciones que en materia de derechos de propiedad intelectual (marcas, patentes y derechos de autor), se ocasionen por la ejecución total o parcial de los servicios descritos en la cláusula Primera de este contrato.

En caso de litigio como consecuencia de lo anterior, **"EL ARRENDADOR"** garantiza la continuidad de los servicios materia del presente contrato, obligándose a subsanar en su totalidad la o las referidas violaciones; en razón de lo anterior, si durante la vigencia de este contrato o con posterioridad a ella, se presentara alguna reclamación a **"TELECOMM"** con ese motivo, **"EL ARRENDADOR"** conviene expresamente en pagar cualquier importe que de ello se derive y sacar en paz y a salvo a **"TELECOMM"** de tales reclamaciones.

En caso de que lo anterior no fuese posible, **"TELECOMM"** podrá rescindir el presente contrato aplicando el procedimiento establecido en la cláusula Segunda del presente instrumento.

**Vigésima Cuarta. Caso fortuito o fuerza mayor.**

Ninguna de las partes en este contrato, será responsable por el retraso en el cumplimiento de sus obligaciones debido a caso fortuito o fuerza mayor.

Se entiende por caso fortuito, a la presentación de un suceso inesperado, sorpresivo, que se produce casual o inopinadamente, o que hubiera sido muy difícil de prever en la medida que no se cuenta con experiencias previas o consistentes de la probabilidad o riesgo de que ocurra un siniestro.

Se entiende por fuerza mayor, la ocurrencia de un suceso inevitable, aunque previsible o relativamente previsible -como un huracán o terremoto- de carácter extraordinario. Consecuentemente, los factores importantes a considerar son la inevitabilidad del hecho dañoso y la consecuente falta de culpa cuando el hecho es ajeno al responsable,

o exterior al vicio o riesgo de la cosa; esto es, lo decisivo consiste en analizar si el daño puede considerarse imprevisible o, pudiendo preverse es inevitable.

En los términos del artículo 55 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, cuando en la prestación del servicio objeto del presente contrato, se presente caso fortuito o de fuerza mayor **"TELECOMM"**, bajo su responsabilidad, podrá suspender la prestación del servicio en cuyo caso únicamente se pagarán aquellos servicios que hubiesen sido efectivamente prestados.

En cualquiera de los casos previstos en el mencionado artículo, en su caso se pactará por las partes el plazo de suspensión, a cuyo término podrá iniciarse el procedimiento de terminación anticipada de este contrato.

Cuando la suspensión obedezca a causas imputables a **"TELECOMM"**, éste pagará a **"EL ARRENDADOR"** los gastos no recuperables por el tiempo que dure la misma, siempre y cuando se compruebe fehacientemente que fueron efectivamente erogados en relación al presente contrato y como consecuencia directa de la suspensión referida; pactándose asimismo que para efectos del pago correspondiente se estará a los plazos que establezca la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

**Vigésima Quinta. Relaciones laborales.**

**"EL ARRENDADOR"** como empresario y patrón del personal que ocupe, con motivo del arrendamiento objeto de este contrato, conviene expresamente en que es el único responsable de las obligaciones laborales y de seguridad social que surjan de las relaciones existentes con el personal, (asesores, factores, agentes, terceros o cualquier otra persona que tenga una relación cualquiera con **("EL ARRENDADOR")**, tales como salarios, indemnizaciones y riesgos profesionales o de cualquier otra obligación o por la prestación de servicios materia de este contrato.

Consecuentemente, en ningún caso y por ningún concepto podrá considerarse a **"TELECOMM"** como patrón directo o sustituto o solidario del personal de **"EL ARRENDADOR"**, por lo que, éste último asume cualquier tipo de responsabilidad con motivo de la realización de los servicios objeto de este contrato que pudiera derivarse de su relación laboral con el personal, asesores, factores, agentes o cualquier otra persona que tenga una relación cualquiera con éste o con un tercero que tenga relación con **"EL ARRENDADOR"** que ejecute los servicios materia de este contrato, relevando de toda responsabilidad obrero-patronal a **"TELECOMM"**.

**"EL ARRENDADOR"** se hace responsable de todas las reclamaciones o demandas individuales o colectivas que en su contra o en contra de **"TELECOMM"**, por cualquier causa pueda promover el personal asesores, factores, agentes o cualquier otra persona que tenga una relación cualquiera con aquél o con un tercero durante y después de concluido el contrato y en su caso las prórrogas del mismo.

**"EL ARRENDADOR"** se obliga a responder de los daños y perjuicios y en su caso efectuar el pago por las sanciones que deriven de la relación laboral antes precisada y que pudieran imponer las autoridades administrativas o judiciales del trabajo a **"TELECOMM"** sacando en paz y a salvo a este último.

**Vigésima Sexta. Confidencialidad.**

**"EL ARRENDADOR"** se compromete a guardar absoluta confidencialidad, sobre los trabajos que resulten del mismo, no pudiendo revelarlos, ya sea en provecho propio o de terceros durante y posterior a la vigencia del servicio o una vez concluido el mismo, en los términos contenidos en el contrato y sus anexos.

**Vigésima Séptima. Ley aplicable.**

Para la interpretación y cumplimiento del presente contrato, las partes se obligan a sujetarse estrictamente para la prestación de los servicios objeto del mismo, a todas y cada una de las cláusulas y anexos que lo integran; a los términos, lineamientos, procedimientos y requisitos que establece la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y su Reglamento; a las disposiciones administrativas aplicables en la materia, así como a lo establecido en la convocatoria del procedimiento de la Licitación Pública Mixta Nacional No. **LA-009KCZ002-N49-2015** y lo establecido en el Acta de Junta de Aclaraciones de fecha 30 de septiembre de 2015.

**Vigésima Octava. Procedimiento de Conciliación.**

Las partes convienen que en caso de desavenencias derivadas del cumplimiento del presente contrato, en cualquier momento durante la ejecución del mismo, podrán iniciar el procedimiento de conciliación, previsto en el Título Sexto, Capítulo Segundo del Procedimiento de Conciliación de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y el Título Sexto, Capítulo Segundo del Procedimiento de Conciliación de su Reglamento.

Cualquiera de las partes presentará ante la Secretaría de la Función Pública o el Órgano Interno de Control de Telecomunicaciones de México, según sea el caso, solicitud de conciliación por escrito con los siguientes requisitos: i) Precisar el nombre, ii) Denominación o razón social de quién o quiénes promuevan, en su caso de su representante legal, iii) Domicilio para recibir notificaciones, iv) Nombre de la persona o personas autorizadas para recibirlas, v) La petición que se formula, vi) Los hechos o razones que dan motivo a la petición, vii) El órgano administrativo a que se dirigen y viii) Lugar y fecha de su emisión, conforme a lo dispuesto en el artículo 128 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y el artículo 15 de la Ley Federal del Procedimiento Administrativo.

El escrito deberá estar firmado por el interesado o su representante legal, a menos que no sepa o no pueda firmar, caso en el cual, se imprimirá su huella digital, deberá adjuntar los documentos que acrediten su personalidad, así como los que en cada caso sean requeridos en los ordenamientos respectivos, refiriendo el objeto, vigencia y monto del contrato y en su caso a los convenios modificatorios, anexando copia de dichos documentos suscritos, en el caso de que el solicitante no cuente con dichos documentos, por no haberse formalizado deberá exhibir copia del fallo correspondiente.

**Vigésima Novena. Jurisdicción.**

Para la interpretación y cumplimiento del presente contrato, en caso de controversia, las partes se someten a la jurisdicción y competencia de los Tribunales Federales en el Distrito Federal, renunciando al que pudiere corresponderles en razón de su domicilio presente o futuro o por cualquier otra causa.

Enteradas las partes del contenido, alcance y fuerza legal del presente contrato, lo firman en tres tantos, en la Ciudad de México, Distrito Federal, a los cuatro días del mes de noviembre de dos mil quince.

**Por "TELECOMM":**

**Lic. Gabriel Salinas Caso.**
Director de Administración Financiera.

**Por "EL ARRENDADOR":**

**C. Jennifer Murillo Domínguez.**
Apoderada legal.
Responsable de la administración y verificación del cumplimiento del presente contrato.

**Por el Área requirente de "TELECOMM":**

**Lic. Roberto Ruiz Domínguez.**
Subdirector de Desarrollo de Informática.
Responsable de la administración y verificación del cumplimiento del presente contrato. Responsable de las especificaciones técnicas de este servicio.

**Por el Área requirente de "TELECOMM":**

**C. Rufino Martínez Becerril.**
Director de Operaciones Telegráficas.
(Área requirente.)

DIRECCIÓN DE ASUNTOS JURÍDICOS
CONTRATO REVISADO
DICTAMEN
8020.-4212
4/DIC/ 2015

Última hoja de firmas del Contrato No. **GJCCCFA/044/2015/GA**

Elaboró: C. Adrián Raúl Fuentes Morando.
Revisó: Lic. Jesús Bringas Vargas.

# Anexo 6

## Propuesta Técnica

**Descripción, Unidad de Presentación y Cantidad de los Bienes Objeto de esta Licitación**

| NOMBRE DEL LICITANTE | REG. FED. DE CAUS | PROCEDIMIENTO |
|---|---|---|
| Grupo de Tecnología Cibernética, S.A. de C.V. | GTC980421 R4A | LA-009KCZ002-N49-2015 |

| PARTIDA | DESCRIPCIÓN DEL SERVICIO | UNIDAD DE MEDIDA |
|---|---|---|
| Única | Arrendamiento de "Equipo Firewall/Vpn y Consola de Administración para Expansión de Oficinas Telegráficas de la Red Teldat" | Servicio |

MÉXICO, D.F., 8 DE OCTUBRE DE 2015
**BAJO PROTESTA DE DECIR VERDAD,**
**GRUPO DE TECNOLOGÍA CIBERNÉTICA, S.A. DE C.V.**

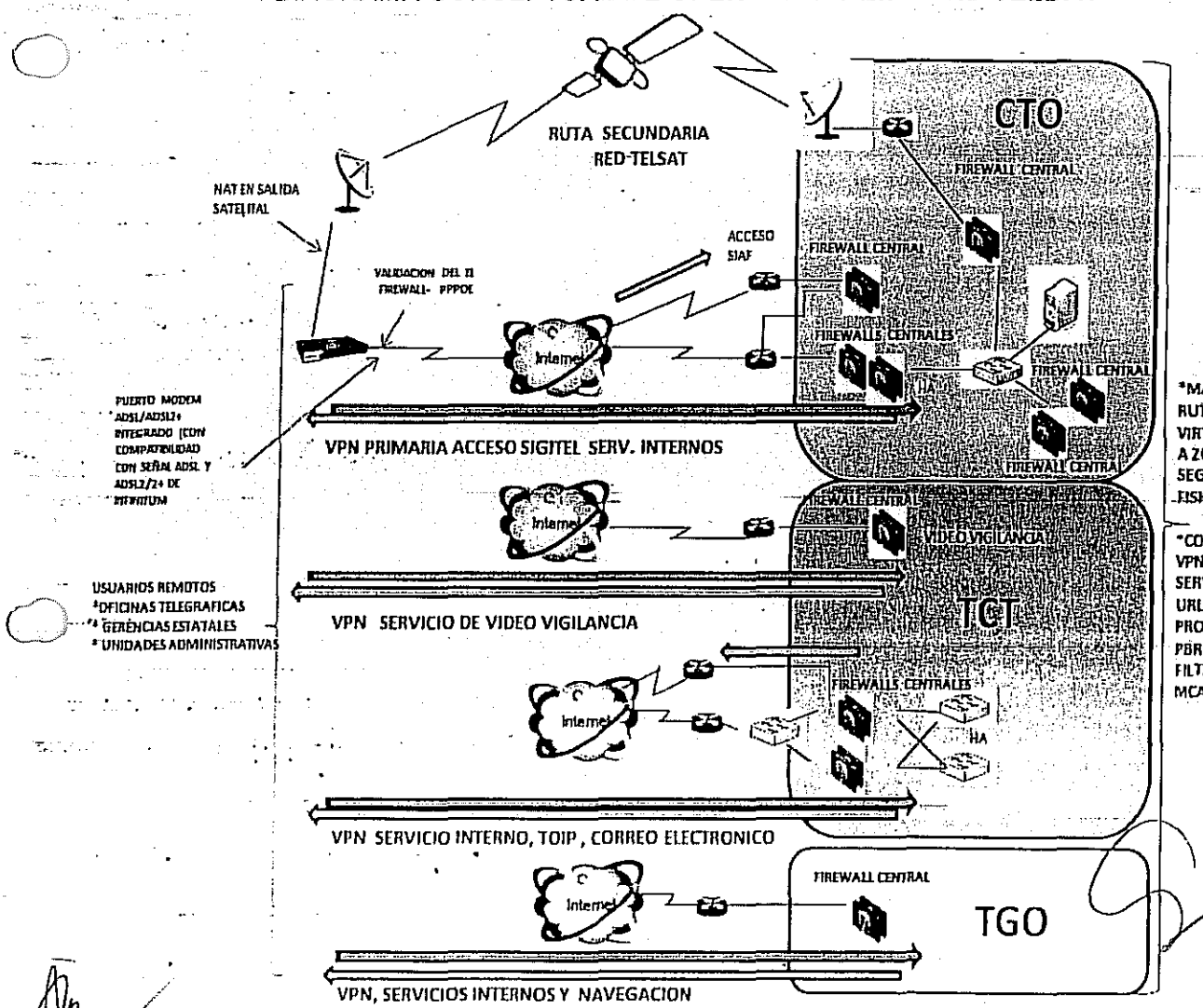
JENNIFER MURILLO DOMINGUEZ
REPRESENTANTE LEGAL

# CONTENIDO

## DESCRIPCIÓN DEL ARRENDAMIENTO

**"GRUPO TECNO"**, entiende y acepta que Telecomunicaciones de México en los sucesivo **"TELECOMM"** requiere contar con un esquema de arrendamiento de equipos firewalls appliance y consolas de administración, que garantice la continuidad de los servicios de la Red Primaria de Comunicaciones "RED TELDAT", para la Red de Oficinas Telegráfica, Gerencias Regionales y Estatales proporcionando el acceso al servicio de datos para aplicaciones de intranet del Servicio de SIGITEL, tales como Giros Telegráficos, Telegramas, Siaf, etc. Así mismo para los servicios de Telefonía IP y Video Vigilancia.

### DIAGRAMA CONCEPTUAL DE OPERACIÓN DEL A RED TELDAT



## 1.1. UBICACIÓN FÍSICA DE NODOS CENTRALES

| SITIO | DESCRIPCIÓN |
|---|---|
| TCT | TORRE CENTRAL DE TELECOMUNICACIONES.<br>UBICACIÓN: EJE CENTRAL LÁZARO CARDENAS 567 COL. NARVARTE C.P. 03020 |
| CTO | CENTRO TÉCNICO OPERATIVO.<br>UBICACIÓN: AV. DE LAS TELECOMUNICACIONES S/N COL. LEYES DE REFORMA, IZTAPALAPA, D.F. |
| TGO | CENTRO DE DATOS.<br>UBICACIÓN: CARRETERA MÉXICO-TUXPAN KM 100 COL. LAS CRUCES CÓDIGO POSTAL 43600, TULANCINGO, HGO. |

## 1.2. UBICACIÓN FÍSICA DE NODOS REMOTOS.

"GRUPO TECNO", tuvo en consideración para la presentación de la presente propuesta, que la ubicación física de Nodos Remotos Gerencias Estatales y Oficinas Telegráficas se encuentran listados en el **ANEXO A** de las bases del presente proceso licitatorio y está en el entendido de que; los domicilios pueden cambiar durante la vigencia del contrato y que TELECOMM podrá requerir la apertura de nuevas oficinas telegráficas).

## 2. REQUERIMIENTOS TÉCNICOS

**"GRUPO TECNO"** en caso de resultar adjudicado proveerá a TELECOMM el arrendamiento de equipo contemplado en los siguientes tres niveles de criticidad:

- ✓ "1" CRÍTICO
- ✓ "2" ALTO
- ✓ "3" BAJO

Lo anterior para los equipos:

a) Firewalls Appliances remotos distribuidos a nivel nacional
b) Consolas de Administración y Sistema de Gestión para los equipos Firewalls ubicados en TCT, CTO, TGO

como se especifica en la TABLA 1 del presente documento

"GRUPO TECNO" en caso de resultar adjudicado proveerá una solución integrada en su totalidad por equipos de la misma marca.

Las características de los equipos que integran la solución ofertada por "GRUPO TECNO" se especifican en la TABLA 1, mimos equipos y características que requiere TELECOM, y que forman parte del alcance de la presente propuesta.

Como alcance de la presente propuesta técnica, **"GRUPO TECNO"**, proveerá la migración y puesta en operación del equipo ofertado con objeto de dar continuidad a los servicios actuales así como asegurar la integración con la infraestructura de comunicaciones y seguridad con la que actualmente opera TELECOMM.

## DESCRIPCIÓN DEL EQUIPO SOLICITADO:

### TABLA 1

| NIVEL | EQUIPO | CONSTRUCCION | CANTIDAD | OBSERVACIONES | RESPUESTA |
|---|---|---|---|---|---|
| "1" CRÍTICO | FIREWALL'S CENTRALES | APPLIANCE | 7 | EQUIPO CONCENTRADOR EN LOS SITIOS DE TCT, CTO Y TGO:<br>• 3 Equipos "ACT1" (Appliance Crítico Tipo 1 ) con las siguientes características técnicas mínimas:<br><br>2 Equipos "ACT1" concentradores de VPN's deberán implementarse en HA (HIGH AVAILABILITY) en el sitio TCT y 1 Equipo concentrador de VPN's deberá implementarse en TGO.<br><br>✓ Desempeño de Firewall para tráfico de Internet monitoreado: 40 Gbps<br>✓ Al menos no. de sesiones concurrentes soportadas: 5 millones.<br>✓ Al menos no. de sesiones concurrentes incluidas: 5 millones.<br>✓ Nuevas sesiones/segundo: 220,000<br>✓ Máximo número de usuarios soportados: no restringido. Debe soportar al menos 25,000 usuarios.<br>✓ Al menos 16 puertos Ethernet 10/100/1000 base T.<br>✓ Al menos 16 puertos 1 Gbps SFP.<br>✓ Al menos 4 puertos ópticos 10Gb SFP+ en tecnología SR.<br>✓ Detección de ataques de red<br>✓ Protección a Dos y DDoS Soportando defensa de ataques de la capa de aplicación tales como ataques DNS y HTTP.<br>✓ IPsec VPN site to site tunnels: 15,000<br>✓ Capacidad de administración vía CLI, Web o scripts vía XML-API.<br>✓ Capacidad de integración de identificación de usuarios activos en la red vía Active Directory, Edirectory, Syslog Server o XML-API.<br>✓ Identificación de aplicaciones desconocidas vía TCP o UDP.<br>✓ Editor de nuevas aplicaciones.<br>✓ IPv4/IPv6 VPN<br>✓ Dual stack IPv4/IPv6<br>✓ Redundant VPN Gateway (capacidad de establecimiento de comunicación en una red remota a través de más de 2 VPNs con diferente Gateway.)<br>✓ NAT ( Network Address Translation) Y PAT (port Address Translation)<br>✓ Numero de zonas virtuales de seguridad : 512<br>✓ Numero de ruteadores / firewalls virtuales con funcionalidad capa 3 / PBR : 1000<br>✓ La solución de seguridad deberá tener capacidad de correr | GRUPO DE TECNOLOGÍA CIBERNÉTICA S.A DE C.V OFERTA EQUIPO CONCENTRADOR EN LOS SITIOS DE TCT, CTO Y TGO FORTIGATE 1500D:<br><br>3 Equipos "ACT1" (Appliance Crítico Tipo 1 ) con las siguientes características técnicas:<br><br>2 Equipos "ACT1" concentradores de VPN's deberán implementarse en HA (HIGH AVAILABILITY) en el sitio TCT y 1 Equipo concentrador de VPN's deberá implementarse en TGO.<br><br>✓ Desempeño de Firewall para tráfico de Internet monitoreado: 80 Gbps<br>Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D, Pág. 1, Párrafo 3<br><br>✓ Número de sesiones concurrentes incluidas: 12 millones.<br>Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D Pág. 4, Fila 16<br><br>✓ Nuevas sesiones/segundo: 250,000<br>Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D Pág. 4, Fila 17<br><br>✓ Número de usuarios soportados: Ilimitado<br>Referencia: Capeta: Propuesta Técnica, Numeral 3, Documento: NGFW Solution Brief Pág. , Párrafo 7<br><br>✓ Al menos 16 puertos Ethernet 10/100/1000 base T.<br>✓ Al menos 16 puertos 1 Gbps SFP.<br>✓ Al menos 8 puertos ópticos 10Gb SFP+ en tecnología SR.<br>Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D Pág. 2, Linea 5, 6 y 7<br><br>✓ Detección de ataques de red<br>Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D Pág. 3, Párrafo 5<br><br>✓ Protección a Dos y DDoS Soportando defensa de ataques de la capa de aplicación tales como ataques DNS y HTTP.<br>Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: FortiOS HandbookFirewall for FortiOS 5.0 Pág. 14 Párrafo 4, 82 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | análisis de vulnerabilidades a nivel de red<br>✓ Numero de VLANS: 4096<br>✓ Ruteo OSPF<br>✓ Ruteo estático<br>✓ PBR (Policy Base Routing)<br>✓ Administración local y centralizada mediante la consola de administración, sistema de gestión<br>✓ Soporte de firewall next generation<br>✓ El equipo deberá contar con la capacidad de habilitar las funcionalidades de control de Anti malware en todos los puertos (TCP/IP) incluyendo SSL, descripción (descifrado) de entrada y salida. Para evitar ataques APT's. Ejemplo: Bloqueo de aplicaciones proxy (TOR, ULTRASURF).<br>✓ Incluya la capacidad de detectar y bloquear aplicaciones , trafico malicioso y anomalías de tráfico en protocolos http y https<br>✓ Capacidad de descripción de trafico SSL tanto entrada como de salida.<br>✓ SSL VPN para 10 usuarios para el FW de TCT, Y 10 usuarios para TGO. Esta funcionalidad deberá de estar dentro del mismo Firewall o en su defecto se acepta un equipo externo en donde la funcionalidad de la VPN SSL deberá cumplir al menos :<br>o Acceso a la Intranet desde cualquier dispositivo cliente con acceso a Internet en cualquier parte del mundo, sin instalación de software o controladores en el dispositivo cliente.<br>o Acceso a los servicios y aplicaciones web, sistemas de archivos o únicamente a un archivo, aplicativos y la red de la Intranet de TELECOMM.<br>o Creación de usuarios con perfiles con granularidad de acceso por segmento de red, por host, por aplicativo residente en un elemento de red especifico, por datos o archivos específicos en un servidor, Servicios o aplicaciones web, aplicaciones instaladas localmente de terceros, escritorios remotos, Virtual desktop infraestructures (VDI), escritorios virtuales, sistemas gráficos corriendo en Unix / Linux, legacy systems, con calendarización en horarios y días de acceso.<br>o Creación de perfiles de acceso individuales o de grupo.<br>o Base de datos de usuarios propia.<br>o Compatibilidad con active directory.<br>o Creación de reglas customizadas de validación de elementos de seguridad como puertos o llaves de registro, dirección Mac address, revisión de software con validación de firmas de | Parrafo 1, 100 Párrafo 3.<br><br>✓ IPsec VPN site to site tunnels: 20,000<br>Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D Pág. 4, Linea 20<br><br>✓ Capacidad de administración vía CLI y Web<br>Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: FortiOS Handbook Firewall for FortiOS 5.0 Pág. 86, Párrafo 5<br><br>✓ Capacidad de integración de identificación de usuarios activos en la red vía Active Directory y Syslog Server.<br>Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: FortiOS HandbookFirewall for FortiOS 5.0 Pág. 10, Párrafo 17, Pág.58, Párrafo 3<br><br>✓ Identificación de aplicaciones desconocidas vía TCP/UDP.<br>Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: Referencia: FortiOS HandbookFirewall for FortiOS 5.0 Pág. 97, Párrafo 6.<br><br>✓ Editor de nuevas aplicaciones.<br>Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: FortiOS Handbook Firewall for FortiOS 5.0 Pág. 40, Párrafo 4.<br><br>✓ IPv4/IPv6 VPN<br>Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: FortiOS HandbookFirewall for FortiOS 5.0, Pág. 10 Párrafo 20, Pág. 18 Párrafo 17 y Pág. 20 Párrafo 4<br><br>✓ Dual stack IPv4/IPv6<br>Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: FortiOS Handbook Firewall for FortiOS 5.0 Pág.18, Párrafo 2<br><br>✓ Redundant VPN Gateway (capacidad de establecimiento de comunicación en una red remota a través de más de 2 VPNs con diferente Gateway.)<br>Referencia: Capeta: Propuesta Técnica, Numeral 5, Documento: FortiOS Handbook Version 5.2.3 Pág 1451 Párrafo 12 y Pág. 1588 Párrafo 1.<br><br>✓ NAT ( Network Address Translation) Y PAT (port Address Translation)<br><br>Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: FortiOS Handbook Firewall for FortiOS 5.0 Pág. 20 Párrafo 5 y Pág. 22 Parráfo 1<br>✓ Número de zonas virtuales de seguridad : 8192<br>Referencia: Capeta: Propuesta Técnica, Numeral 5, Documento: |



16445

| | | |
|---|---|---|
| | antivirus, validación de firewall.<br>o Reporteo de accesos y comportamiento. Auditoría sobre la aplicación a la cual se acceso el cliente.<br>o Liberación automática de sesiones inactivas.<br>o Cancelación manual de sesiones establecidas.<br><br>✓ Redundant Power Supply (AC) 100-240 vac | FortiOS Handbook Version 5.2.3 Pág 2108 Párrafo 1 y Pág. 2164 Párrafo 10. Esta referencia con base a la junta de aclaraciones del pasado 30 de septiembre, con referencia a la pregunta 13 de Carvajal Tecnología y Servicios, S.A de C.V Que dice: ¿Es correcto entender que Zonas Virtuales de Seguridad se refiere a segmentos que pueden ser puertos físicos, o bien VLAN que tengan políticas de seguridad?. A lo que TELECOMM respondió SI, es correcto<br>✓ Numero de ruteadores / firewalls virtuales con funcionalidad capa 3 / PBR : 2048<br>Referencia: Capeta: Propuesta Técnica, Numeral 7, Documento: Fortinet About the Maximum Values Table Pág 2 Fila 1 y Pág. 3 Fila 30<br>✓ La solución de seguridad deberá tener capacidad de correr análisis de vulnerabilidades a nivel de red<br>Referencia: Capeta: Propuesta Técnica, Numeral 5, Documento: FortiOS Handbook Version 5.2.3 Pág 114 Párrafo 2<br>✓ Numero de VLANS: 4096<br>Referencia: Capeta: Propuesta Técnica, Numeral 6, Documento: FortiOS Handbook Install and System Administration for FortiOS 5.0 Pág. 113 Párrafo 4<br>✓ Ruteo OSPF<br>Referencia: FortiOS Handbook<br>Firewall for FortiOS.5.0 Pág. 18 Párrafo 7<br>Referencia: Capeta: Propuesta Técnica, Numeral 6, Documento: FortiOS Handbook Install and System Administration for FortiOS 5.0Pág 163 Párrafo 3<br><br>✓ Ruteo estático<br>Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: FortiOS Handbook Firewall for FortiOS 5.0 Pág. 18 Párrafo 4<br>Referencia: Capeta: Propuesta Técnica, Numeral 6, Documento: FortiOS Handbook Install and System Administration for FortiOS 5.0Pág 163 Párrafo 2<br><br>✓ PBR (Policy Base Routing)<br>Referencia: Capeta: Propuesta Técnica, Numeral 6, Documento: FortiOS Handbook Install and System Administration for FortiOS 5.0 Pág 162 Párrafo 4 y 201 Párrafo 4<br><br>✓ Administración local y centralizada mediante la consola de administración, sistema de gestión<br>Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D Pág. 3 Párrafo 7<br><br>✓ Soporte de firewall next generation<br>Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D Pág. 1 Párrafo 2<br><br>✓ El equipo deberá contar con la capacidad de habilitar |

las funcionalidades de control de Anti malware en todos los puertos (TCP/IP) incluyendo SSL, descripción (descifrado) de entrada y salida. Para evitar ataques APT's. Ejemplo: Bloqueo de aplicaciones proxy (TOR, ULTRASURF).

Referencia: Capeta: Propuesta Técnica, Numeral 5, Documento: FortiOS Handbook Version 5.2.3 Pág 986 Párrafo 1, 987 Párrafo 9, 989 Párrafo 4, 993 Párrafo 4, 1872 Párrafo 1

- ✓ Incluya la capacidad de detectar y bloquear aplicaciones , trafico malicioso y anomalías de tráfico en protocolos http y https

Referencia: Capeta: Propuesta Técnica, Numeral 6, Documento: FortiOS Handbook Install and System Administration for FortiOS 5.0. Pág. 124 Párrafo 1 y 231 Párrafo 6

- ✓ Capacidad de descripción de trafico SSL tanto entrada como de salida

Referencia: Capeta: Propuesta Técnica, Numeral 6, Documento: FortiOS Handbook Install and System Administration for FortiOS 5.0. Pág. 132 Párrafo 6

- ✓ SSL VPN para 10,000 usuarios para el FW de TCT, Y 10 usuarios para TGO. Esta funcionalidad deberá de estar dentro del mismo Firewall o en su defecto se acepta un equipo externo en donde la funcionalidad de la VPN SSL deberá cumplir al menos :

Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D Pág. 4, Linea 23

- o Acceso a la Intranet desde cualquier dispositivo cliente con acceso a Internet en cualquier parte del mundo, sin instalación de software o controladores en el dispositivo cliente.

Referencia: Capeta: Propuesta Técnica, Numeral 13, Documento: FortiOS™ Handbook SSL VPN for FortiOS 5.0 Pág 9 Párrafo 2

- o Acceso a los servicios y aplicaciones web, sistemas de archivos o únicamente a un archivo, aplicativos y la red de la Intranet de TELECOMM.

Referencia: Capeta: Propuesta Técnica, Numeral 13, Documento: FortiOS™ Handbook SSL VPN for FortiOS 5.0 Pág 9 Párrafo 3

- o Creación de usuarios con perfiles con granularidad de acceso por segmento de red, por host, por aplicativo residente en un elemento de red especifico, por datos o archivos específicos en un servidor, Servicios o aplicaciones web, aplicaciones instaladas localmente de terceros, escritorios remotos, Virtual desktop

| | |
|---|---|
| | Infraestructures (VDI), escritorios virtuales, sistemas gráficos corriendo en Unix / Linux, legacy systems, con calendarización en horarios y días de acceso.<br>Referencia: Capeta: Propuesta Técnica, Numeral 5, Documento: FortiOS Handbook Version 5.2.3 Pág 424 Párrafo 2, Pág. 427 Párrafo 4, Pág. 477 Párrafos 1 y 3, Pág. 485 Párrafo 3 y Pág.2011 Párrafo 3<br><br>o Creación de perfiles de acceso individuales o de grupo.<br>Referencia: Capeta: Propuesta Técnica, Numeral 5, Documento: FortiOS Handbook Version 5.2.3 Pág 452 Párrafo 1, Pág. 477 Párrafo 1 y Pág. 2016 Párrafo 5<br><br>o Base de datos de usuarios propia.<br>Referencia: Capeta: Propuesta Técnica, Numeral 5, Documento: FortiOS Handbook Version 5.2.3 Pág 891 Linea 7 y 8<br><br>o Compatibilidad con active directory.<br>Referencia: Capeta: Propuesta Técnica, Numeral 5, Documento: FortiOS Handbook Version 5.2.3 Pág 486 Párrafo 4, Pág. 891 Linea 7 y 9, Pág. 2017 Párrafo 2.<br><br>o Creación de reglas customizadas de validación de elementos de seguridad como puertos o llaves de registro, dirección Mac address, revisión de software con validación de firmas de antivirus, validación de firewall.<br>Referencia: Capeta: Propuesta Técnica, Numeral 6, Documento: FortiOS Handbook Install and System Administration for FortiOS 5.0 Pág 89 Párrafo 3, Pág.128 Párrafo 1<br><br>o Reporteo de accesos y comportamiento. Auditoria sobre la aplicación a la cual se acceso el cliente.<br>Referencia: Capeta: Propuesta Técnica, Numeral 6, Documento: FortiOS Handbook Install and System Administration for FortiOS 5.0. Pág. 140 Párrafo 4<br>Referencia: Capeta: Propuesta Técnica, Numeral 8, Documento: FortiAnalyzer Pág 1 Párrafo 1 , 2 Párrafo 7<br><br>o Liberación automática de sesiones inactivas.<br>Referencia: Capeta: Propuesta Técnica, Numeral 6, Documento: FortiOS Handbook Install and System Administration for FortiOS 5.0 Pág. 239 Párrafo 6<br><br>o Cancelación manual de sesiones establecidas.<br>Referencia: Capeta: Propuesta Técnica, Numeral 5, Documento: FortiOS Handbook Version 5.2.3 Pág 2034 Párrafo 3<br><br>✓ Redundant Power Supply (AC) 100-240 vac<br>Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: |

| | |
|---|---|
| | • . 2 Equipos "ACT2" (Appliance Critico Tipo 2 ) con las siguientes caracteristicas técnicas minimas:<br><br>2 Equipos "ACT2" concentradores de VPN's deberán implementarse en HA (HIGH AVAILABILITY) en el SITIO CTO.<br><br>✓ Desempeño de Firewall para tráfico de Internet monitoreado: 40 Gbps<br>✓ Al menos no. de sesiones concurrentes soportadas: 5 millones.<br>✓ Al menos no. de sesiones concurrentes incluidas: 5 millones.<br>✓ Nuevas sesiones/segundo: 220,000<br>✓ Máximo número de usuarios soportados: no restringido<br>✓ Al menos 16 puertos Ethernet 10/100/1000 base T.<br>✓ Al menos 16 puertos 1 Gbps SFP.<br>✓ Al menos 4 puertos ópticos 10Gb SFP+ en tecnología SR.<br>✓ Detección de ataques de red<br>✓ Protección a Dos y DDoS<br>✓ IPsec VPN site to site tunnels: 15,000<br>✓ IPv4/IPv6 VPN<br>✓ Dual stack IPv4/IPv6<br>✓ Redundant VPN Gateway (capacidad de establecimiento de comunicación en una red remota a través de más de 2 VPNs con diferente Gateway.)<br>✓ NAT ( Network Address Translation) Y PAT (port Address Translation)<br>✓ Numero de zonas virtuales de seguridad : 512<br>✓ Numero de ruteadores / firewalls virtuales con funcionalidad capa 3 / PBR : 1000<br>✓ Numero de VLANS: 4096<br>✓ Ruteo OSPF<br>✓ Ruteo estático<br>✓ PBR (Policy Base Routing)<br>✓ Administración local y centralizada mediante la consola de administración, sistema de gestión<br>✓ Soporte de firewall next generation<br>✓ SSL VPN para 300 usuarios en el FW de CTO. Esta funcionalidad deberá de estar dentro del mismo Firewall o en su defecto se acepta un equipo externo en donde la funcionalidad de la VPN SSL deberá cumplir al menos:<br>o Acceso a la intranet desde cualquier dispositivo cliente con acceso a internet en cualquier parte del mundo, sin instalación de software o controladores en el dispositivo cliente.<br>o Acceso a los servicios y aplicaciones web, sistemas de archivos o únicamente a un archivo, aplicativos y la red de la intranet de | Fortigate 1500D Pág 4 Segunda Columna Linea 8 y 13<br>GRUPO DE TECNOLOGÍA CIBERNÉTICA S.A DE C.V OFERTA EQUIPO CONCENTRADOR EN EL SITIO CTO FORTIGATE 1500D:<br><br>2 Equipos "ACT2" (Appliance Critico Tipo 2 ) con las siguientes caracteristicas técnicas minimas:<br><br>2 Equipos "ACT2" concentradores de VPN's deberán implementarse en HA (HIGH AVAILABILITY) en el SITIO CTO.<br><br>☐ Desempeño de Firewall para tráfico de Internet monitoreado: 80 Gbps<br>Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D Pág. 1, Párrafo 3<br><br>☐ Número de sesiones concurrentes soportadas: 12 millones.<br>Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D Pág. 4 Fila 16<br><br>☐ Número de sesiones concurrentes incluidas: 12 millones.<br>Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D Pág. 4 Fila 16<br><br>☐ Nuevas sesiones/segundo: 250,000<br>Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D Pág. 4 Fila 17<br><br>☐ Número de usuarios soportados: Ilimitado<br>Referencia: Capeta: Propuesta Técnica, Numeral 3, Documento: NGFW Solution Brief Pág. 1 Párrafo 7<br><br>☐ Al menos 16 puertos Ethernet 10/100/1000 base T.<br>☐ Al menos 16 puertos 1 Gbps SFP.<br>☐ Al menos 8 puertos ópticos 10Gb SFP+ en tecnología SR.<br>Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D Pág. 2 Linea 5, 6 y 7<br><br>☐ Detección de ataques de red<br>Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D Pág. 3 Parrafo 5<br><br>☐ Protección a Dos y DDoS<br>Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: |

| | | | |
|---|---|---|---|
| | | TELECOMM.<br>o Creación de usuarios con perfiles con granularidad de acceso por segmento de red, por host, por aplicativo residente en un elemento de red especifico, por datos o archivos especificos en un servidor, Servicios o aplicaciones web, aplicaciones instaladas localmente de terceros, escritorios remotos, Virtual desktop infraestructures (VDI), escritorios virtuales, sistemas gráficos corriendo en Unix / Linux, legacy systems, con calendarización en horarios y días de acceso.<br>o Creación de perfiles de acceso individuales o de grupo.<br>o Base de datos de usuarios propia.<br>o Compatibilidad con active directory.<br>o Creación de reglas customizadas de validación de elementos de seguridad como puertos o llaves de registro, dirección Mac address, revisión de software con validación de firmas de antivirus, validación de firewall.<br>o Reporteo de accesos y comportamiento. Auditoria sobre la aplicación a la cual se acceso el cliente.<br>o Liberación automática de sesiones inactivas.<br>o Cancelación manual de sesiones establecidas.<br><br>✓ Redundant Power Supply (AC) 100-240 vac | FortiOS Handbook Firewall for FortiOS 5.0 Pág. 14 Párrafo 4, 82 Parrafo 1, 100 Párrafo 3.<br><br>☐ IPsec VPN site to site tunnels: 20,000<br>Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D Pág. 4 Linea 20<br>☐ IPv4/IPv6 VPN<br>Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: FortiOS Handbook Firewall for FortiOS 5.0 Pág. 10 Párrafo 20, 18 Párrafo 17 y 20 Párrafo 4<br>☐ Dual stack IPv4/IPv6<br>Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: FortiOS Handbook Firewall for FortiOS 5.0 Pág.18 Párrafo 2<br>☐ Redundant VPN Gateway (capacidad de establecimiento de comunicación en una red remota a través de más de 2 VPNs con diferente Gateway.)<br>Referencia: Capeta: Propuesta Técnica, Numeral 5, Documento: FortiOS Handbook Version 5.2.3 Pág 1451 Párrafo 12 y Pág.1588 Párrafo 1.<br>☐ NAT ( Network Address Translation) Y PAT (port Address Translation)<br>Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: FortiOS Handbook Firewall for FortiOS 5.0 Pág. 20 Párrafo 5 y Pág. 22 Parráfo 1<br>☐ Número de zonas virtuales de seguridad : 8192<br>Referencia: Capeta: Propuesta Técnica, Numeral 5, Documento: FortiOS Handbook Version 5.2.3 Pág 2108 Párrafo 1 y Pág. 2164 Párrafo 10. Esta referencia con base a la junta de aclaraciones del pasado 30 de septiembre, con referencia a la pregunta 13 de Carvajal Tecnología y Servicios, S.A de C.V Que dice: ¿Es correcto entender que Zonas Virtuales de Seguridad se refiere a segmentos que pueden ser puertos físicos, o bien VLAN que tengan políticas de seguridad?. A lo que TELECOMM respondió SI, es correcto<br><br>☐ Número de ruteadores / firewalls virtuales con funcionalidad capa 3 / PBR : 2048<br>Referencia: Capeta: Propuesta Técnica, Numeral 7, Documento: Fortinet About the Maximum Values Table Pág 2 Fila 1 y 3 Fila 30<br><br>☐ Numero de VLANS: 4096<br>Referencia: Capeta: Propuesta Técnica, Numeral 6, Documento: FortiOS Handbook Install and System Administration for FortiOS 5.0Pág. 113 Párrafo 4<br>☐ Ruteo OSPF<br>Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: FortiOS Handbook Firewall for FortiOS 5.0 Pág. 18 Párrafo 7<br>Referencia: Capeta: Propuesta Técnica, Numeral 6, Documento: FortiOS Handbook Install and System Administration for FortiOS 5.0Pág 163 Párrafo 3 |

ETUDIO

- ☐ Ruteo estático
  Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: FortiOS Handbook Firewall for FortiOS 5.0 Pág. 18 Párrafo 4
  Referencia: Capeta: Propuesta Técnica, Numeral 6, Documento: FortiOS Handbook Install and System Administration for FortiOS 5.0Pág 163 Párrafo 2

- ☐ PBR (Policy Base Routing)
  Referencia: Capeta: Propuesta Técnica, Numeral 6, Documento: FortiOS Handbook Install and System Administration for FortiOS 5.0 Pág 162 Párrafo 4 y 201 Párrafo 4

- ☐ Administración local y centralizada mediante la consola de administración, sistema de gestión
  Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D Pág. 3 Párrafo 7

- ☐ Soporte de firewall next generation
  Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D Pág. 1 Párrafo 2

- ☐ SSL VPN para 10,000 usuarios para el FW de TCT, Y 10 usuarios para TGO. Esta funcionalidad deberá de estar dentro del mismo Firewall o en su defecto se acepta un equipo externo en donde la funcionalidad de la VPN SSL deberá cumplir al menos :
  Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D Pág. 4 Linea 23

- o Acceso a la intranet desde cualquier dispositivo cliente con acceso a Internet en cualquier parte del mundo, sin instalación de software o controladores en el dispositivo cliente.
  Referencia: Capeta: Propuesta Técnica, Numeral 13, Documento: FortiOS™ Handbook SSL VPN for FortiOS 5.0 Pág 9 Párrafo 2

- o Acceso a los servicios y aplicaciones web, sistemas de archivos o únicamente a un archivo, aplicativos y la red de la Intranet de TELECOMM.
  Referencia: Capeta: Propuesta Técnica, Numeral 13, Documento: FortiOS™ Handbook SSL VPN for FortiOS 5.0 Pág 9 Párrafo 3

- o Creación de usuarios con perfiles con granularidad de acceso por segmento de red, por host, por aplicativo residente en un elemento de red especifico, por datos o archivos específicos en un servidor, Servicios o aplicaciones web, aplicaciones instaladas localmente de terceros, escritorios remotos, Virtual desktop infraestructures (VDI), escritorios virtuales, sistemas gráficos corriendo en Unix / Linux, legacy systems, con calendarización en horarios y días de acceso.

| | | | | | |
|---|---|---|---|---|---|
| | | | | | Referencia: Capeta: Propuesta Técnica, Numeral 5, Documento: FortiOS Handbook Version 5.2.3 Pág 424 Párrafo 2, Pág. 427 Párrafo 4, Pág. 477 Párrafos 1 y 3, Pag. 485 Párrafo 3 y Pág. 2011 Párrafo 3<br><br>o Creación de perfiles de acceso individuales o de grupo.<br>Referencia: Capeta: Propuesta Técnica, Numeral 5, Documento: FortiOS Handbook Version 5.2.3 Pág 452 Párrafo 1, 477 Párrafo 1, 2016 Párrafo 5<br><br>o Base de datos de usuarios propia.<br>Referencia: Capeta: Propuesta Técnica, Numeral 5, Documento: FortiOS Handbook Version 5.2.3 Pág 891 Linea 7 y 8<br><br>o Compatibilidad con active directory.<br>Referencia: Capeta: Propuesta Técnica, Numeral 5, Documento: FortiOS Handbook Version 5.2.3 Pág 486 Párrafo 4, Pág.891 Linea 7 y 9, Pág. 2017 Párrafo 2.<br><br>o Creación de reglas customizadas de validación de elementos de seguridad como puertos o llaves de registro, dirección Mac address, revisión de software con validación de firmas de antivirus, validación de firewall.<br>Referencia: Capeta: Propuesta Técnica, Numeral 6, Documento: FortiOS Handbook Install and System Administration for FortiOS 5.0 Pág 89 Párrafo 3, 128 Párrafo 1<br><br>o Reporteo de accesos y comportamiento. Auditoria sobre la aplicación a la cual se acceso el cliente.<br>Referencia: Capeta: Propuesta Técnica, Numeral 6, Documento: FortiOS Handbook Install and System Administration for FortiOS 5.0. Pág. 140 Párrafo 4<br>Referencia: Capeta: Propuesta Técnica, Numeral 8, Documento: FortiAnalyzer Pág 1 Párrafo 1 , 2 Párrafo 7<br><br>o Liberación automática de sesiones inactivas.<br>Referencia: Capeta: Propuesta Técnica, Numeral 6, Documento: FortiOS Handbook Install and System Administration for FortiOS 5.0 Pág. 239 Párrafo 6<br><br>o Cancelación manual de sesiones establecidas.<br>Referencia: Capeta: Propuesta Técnica, Numeral 5, Documento: FortiOS Handbook Version 5.2.3 Pág 2034 Párrafo 3<br><br>□ Redundant Power Supply (AC) 100-240 vac<br>Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: Fortigate 1500D Pág 4 Segunda Columna Linea 8 y 13 |
| | | | | EN EL SITIO DE CTO : | GRUPO DE TECNOLOGÍA CIBERNÉTICA S.A DE C.V OFERTA EQUIPO CONCENTRADOR EN EL SITIO CTO FORTIGATE 1500D |

| | | |
|---|---|---|
| | • 2 Equipos "ACT3" (Appliance Crítico Tipo 3 ) con las siguientes características técnicas mínimas:<br><br>2 Equipos "ACT3" concentradores de VPN's deberán implementarse en HA (HIGH AVAILABILITY) en el SITIO CTO.<br><br>✓ Desempeño de Firewall para tráfico de Internet monitoreado: 40 Gbps<br>✓ Al menos no. de sesiones concurrentes soportadas: 5 millones.<br>✓ Al menos no. de sesiones concurrentes incluidas: 5 millones.<br>✓ Nuevas sesiones/segundo: 220,000<br>✓ Máximo número de usuarios soportados: no restringido<br>✓ Al menos 16 puertos Ethernet 10/100/1000 base<br>✓ Al menos 16 puertos 1 Gbps SFP.<br>✓ Al menos 4 puertos ópticos 10Gb SFP+ en tecnología SR.<br>✓ Detección de ataques de red<br>✓ Protección a Dos y DDoS<br>✓ IPsec VPN site to site tunnels: 15,000<br>✓ IPv4/IPv6 VPN<br>✓ Dual stack IPv4/IPv6<br>✓ Redundant VPN Gateway (capacidad de establecimiento de comunicación en una red remota a través de más de 2 VPNs con diferente Gateway.)<br>✓ NAT ( Network Address Translation) Y PAT (port Address Translation)<br>✓ Numero de zonas virtuales de seguridad : 512<br>✓ Numero de ruteadores / firewalls virtuales con funcionalidad capa 3 / PBR : 1000<br>✓ Numero de VLANS: 4096<br>✓ Ruteo OSPF<br>✓ Ruteo estático<br>✓ PBR (Policy Base Routing)<br>✓ Administración local y centralizada mediante la consola de administración, sistema de gestión<br>✓ Soporte de firewall next generation<br>✓ Redundant Power Supply (AC) 100-240 vac | 2 Equipos "ACT3" (Appliance Crítico Tipo 3 ) con las siguientes características técnicas mínimas:<br><br>2 Equipos "ACT3" concentradores de VPN's deberán implementarse en HA (HIGH AVAILABILITY) en el SITIO CTO.<br><br>☐ Desempeño de Firewall para tráfico de Internet monitoreado: 80 Gbps<br>Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D Pág. 1 Párrafo 3<br><br>☐ Número de sesiones concurrentes soportadas: 12 millones.<br>Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D Pág. 4 Fila 16<br><br>☐ Número de sesiones concurrentes incluidas: 12 millones.<br><br>Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D Pág. 4 Fila 16<br><br>☐ Nuevas sesiones/segundo: 250,000<br>Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D Pág. 4 Fila 16<br><br>☐ Número de usuarios soportados: ilimitado<br>Referencia: Capeta: Propuesta Técnica, Numeral 3, Documento: NGFW Solution Brief Pág. 1 Párrafo 7<br><br>☐ Al menos 16 puertos Ethernet 10/100/1000 base T.<br>☐ Al menos 16 puertos 1 Gbps SFP.<br>☐ Al menos 8 puertos ópticos 10Gb SFP+ en tecnología SR.<br>Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D Pág. 2 Linea 5, 6 y 7<br><br>☐ Detección de ataques de red<br>Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D Pág. 3, Párrafo 5<br><br>☐ Protección a Dos y DDoS<br>Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: FortiOS Handbook Firewall for FortiOS 5.0 Pág. 14 Párrafo 4, Pág. 82 Parrafo 1 y Pág. 100 Párrafo 3.<br><br>☐ IPsec VPN site to site tunnels: 20,000<br>Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D Pág. 4 Linea 20 |

0000015

| | | | | |
|---|---|---|---|---|
| 9100000 | | | | ☐ IPv4/IPv6 VPN<br>Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: FortiOS Handbook Firewall for FortiOS 5.0 Pág. 10 Párrafo 20, Pág. 18 Párrafo 17 y Pág. 20 Párrafo 4<br><br>☐ Dual stack IPv4/IPv6<br>Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: FortiOS Handbook Firewall for FortiOS 5.0 Pág.18 Párrafo 2<br>☐ Redundant VPN Gateway (capacidad de establecimiento de comunicación en una red remota a través de más de 2 VPNs con diferente Gateway.)<br>Referencia: Capeta: Propuesta Técnica, Numeral 5, Documento: FortiOS Handbook Version 5.2.3 Pág 1451 Párrafo 12 y Pág. 1588 Párrafo 1.<br>☐ NAT ( Network Address Translation) Y PAT (port Address Translation)<br>Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: FortiOS Handbook Firewall for FortiOS 5.0 Pág. 20 Párrafo 5 y Pág. 22 Parráfo 1<br>☐ Número de zonas virtuales de seguridad : 8192<br>Referencia: Capeta: Propuesta Técnica, Numeral 5, Documento: FortiOS Handbook Version 5.2.3 Pág 2108 Párrafo 1 y Pág.2164 Párrafo 10. Esta referencia con base a la junta de aclaraciones del pasado 30 de septiembre, con referencia a la pregunta 13 de Carvajal Tecnología y Servicios, S.A de C.V Que dice: ¿Es correcto entender que Zonas Virtuales de Seguridad se refiere a segmentos que pueden ser puertos físicos, o bien VLAN que tengan políticas de seguridad?. A lo que TELECOMM respondió SI, es correcto<br>☐ Número de ruteadores / firewalls virtuales con funcionalidad capa 3 / PBR : 2048<br>Referencia: Capeta: Propuesta Técnica, Numeral 7, Documento: Fortinet About the Maximum Values Table Pág 2 Fila 1 y Pág. 3 Fila 30<br>☐ Numero de VLANS: 4096<br>Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: FortiOS Handbook Install and System Administration for FortiOS 5.0Pág. 113 Párrafo 4<br><br>☐ Ruteo OSPF<br>Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: FortiOS Handbook Firewall for FortiOS 5.0 Pág. 18 Párrafo 7<br>Referencia: Capeta: Propuesta Técnica, Numeral 6, Documento: FortiOS Handbook Install and System Administration for FortiOS 5.0Pág 163 Párrafo 3<br><br>☐ Ruteo estático<br>Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: FortiOS Handbook Firewall for FortiOS 5.0 Pág. 18 Párrafo 4 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | Referencia: Capeta: Propuesta Técnica, Numeral 6, Documento: FortiOS Handbook Install and System Administration for FortiOS 5.0Pág 163 Párrafo 2<br><br>□ PBR (Policy Base Routing)<br>Referencia: Capeta: Propuesta Técnica, Numeral 6, Documento: FortiOS Handbook Install and System Administration for FortiOS 5.0 Pág 162 Párrafo 4 y Pág. 201 Párrafo 4<br><br>□ Administración local y centralizada mediante la consola de administración, sistema de gestión<br>Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D Pág. 3 Párrafo 7<br><br>□ Soporte de firewall next generation<br>Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: FortiGate 1500D Pág. 1 Párrafo 2<br><br>□ Redundant Power Supply (AC) 100-240 vac<br><br>Referencia: Capeta: Propuesta Técnica, Numeral 2, Documento: Fortigate 1500D Pág 4 Segunda Columna Línea 8 y 13 |
| | | | | EN EL SITIO DE CTO:<br><br>✓ 3 Equipos "ACT4" (Appliance Crítico Tipo 4) con las siguientes características técnicas mínimas.<br>✓ Desempeño de Firewall para tráfico de Internet monitoreado: 5 Gbps<br>✓ IPsec VPN throughput: 5 Gbps<br>✓ IPsec VPN site to site tunnels: 2,000<br>✓ IPsec VPN<br>✓ IPsec NAT Transversal<br>✓ Redundat VPN Gateway<br>✓ Conexiones por segundo 100,000<br>✓ Al menos No. de Sesiones concurrentes : 3 millones<br>✓ Políticas de seguridad: 8,000<br>✓ Usuarios soportados: no restringido<br>✓ Al menos 6 puertos 10/100/1000 base T<br>✓ Al menos 4 puertos 1 Gbps SFP.<br>✓ Al menos 2 puertos ópticos 10Gb SFP+ en tecnología SR.<br>✓ Ruteo OSPF<br>✓ Ruteo estático<br>✓ Número de usuarios: sin restricciones<br>✓ Numero de zonas virtuales de seguridad: 120<br>✓ Numero de ruteadores / firewalls virtuales con funcionalidad capa 3 / PBR : 120 | GRUPO DE TECNOLOGÍA CIBERNÉTICA S.A DE C.V OFERTA EQUIPO CONCENTRADOR EN EL SITIO CTO FORTIGATE 900D:<br><br>✓ 3 Equipos "ACT4" (Appliance Crítico Tipo 4) con las siguientes características técnicas mínimas:<br><br>✓ Desempeño de Firewall para tráfico de Internet monitoreado: 52 Gbps<br>Referencia: Capeta: Propuesta Técnica, Numeral 10, Documento: Fortigate 900D Pág 1 Parráfo 5 y Pág. 4 Línea 12<br><br>✓ IPsec VPN throughput: 25 Gbps<br>Referencia: Capeta: Propuesta Técnica, Numeral 10, Documento: Fortigate 900D Pág 4 Línea 19.<br><br>✓ IPsec VPN site to site tunnels: 2,000<br>Referencia: Capeta: Propuesta Técnica, Numeral 10, Documento: Fortigate 900D Pág 4 Línea 20<br><br>✓ IPsec VPN<br>Referencia: Capeta: Propuesta Técnica, Numeral 10, Documento: Fortigate 900D Pág 4 Línea 20<br><br>✓ IPsec NAT Transversal<br>Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: FortiOS Handbook Firewall for FortiOS 5.0 |

| | |
|---|---|
| ✓ Numero de VLANS: 3,967<br>✓ Administración local y centralizada mediante la consola de administración, sistema de gestión<br>✓ Soporte de firewall next generation<br>Soporte de Redundant Power supply (AC) 100-240 vac | Pág. 20 Párrafo 5, Pág. 26 Párrafo 8 y Pág. 27 Párrafo 3<br><br>✓ Redundat VPN Gateway<br>Referencia: Capeta: Propuesta Técnica, Numeral 5,<br>Documento: FortiOS Handbook Version 5.2.3 Pág 1451 Párrafo 12 y Pág. 1588 Párrafo 1<br><br>✓ Conexiones por segundo 49.5 Millones de paquetes por segundo<br>Referencia: Capeta: Propuesta Técnica, Numeral 10,<br>Documento: Fortigate 900D Pág 4 Linea 15<br><br>✓ Al menos No. de Sesiones concurrentes : 11 millones<br>Referencia: Capeta: Propuesta Técnica, Numeral 10,<br>Documento: Fortigate 900D Pág 4 Linea 16<br><br>✓ Politicas de seguridad: 100,000<br>Referencia: Fortigate 900D Pág 4 Linea 18<br><br>✓ Usuarios soportados: Ilimitado.<br>Referencia: Capeta: Propuesta Técnica, Numeral 3,<br>Documento: NGFW Solution Brief Pág. 1 Párrafo 7.<br><br>✓ Al menos 16 puertos 10/100/1000 base T<br>✓ Al menos 16 puertos 1 Gbps SFP.<br>✓ Al menos 2 puertos ópticos 10Gb SFP+ en tecnología SR.<br>Referencia: Capeta: Propuesta Técnica, Numeral 10,<br>Documento: Fortigate 900D Pág 4 Linea 3, 4 y 5<br><br>✓ Ruteo OSPF<br>Referencia: Capeta: Propuesta Técnica, Numeral 4,<br>Documento: FortiOS Handbook Firewall for FortiOS 5.0 Pág. 18 Párrafo 7<br>Referencia: Capeta: Propuesta Técnica, Numeral 6,<br>Documento: FortiOS Handbook Install and System Administration for FortiOS 5.0Pág 163 Párrafo 3<br><br>✓ Ruteo estático<br>Referencia: Capeta: Propuesta Técnica, Numeral 4,<br>Documento: FortiOS Handbook Firewall for FortiOS 5.0 Pág. 18 Párrafo 4<br>Referencia: Capeta: Propuesta Técnica, Numeral 6,<br>Documento: FortiOS Handbook Install and System Administration for FortiOS 5.0Pág 163 Párrafo 2<br>Referencia: Capeta: Propuesta Técnica, Numeral 3,<br>Documento: NGFW Solution Brief Pág. 1, Párrafo 7<br><br>✓ Numero de zonas virtuales de seguridad: 8192<br>Referencia: Capeta: Propuesta Técnica, Numeral 5, |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | Documento: FortiOS Handbook Version 5.2.3 Pág 2108 Párrafo 1 y 2164 Párrafo 10, Esta referencia con base a la junta de aclaraciones del pasado 30 de septiembre, con referencia a la pregunta 13 de Carvajal Tecnología y Servicios, S.A de C.V Que dice: ¿Es correcto entender que Zonas Virtuales de Seguridad se refiere a segmentos que pueden ser puertos físicos, o bien VLAN que tengan políticas de seguridad?. A lo que TELECOMM respondió SI, es correcto<br>✓ Numero de ruteadores / firewalls virtuales con funcionalidad capa 3 / PBR : 2048<br>Referencia: Capeta: Propuesta Técnica, Numeral 7, Documento: Fortinet About the Maximum Values Table Pág 2 Fila 1 y 3 Fila 30<br>✓ Numero de VLANS: 4096<br>Referencia: Capeta: Propuesta Técnica, Numeral 6, Documento: FortiOS Handbook Install and System Administration for FortiOS 5.0Pág. 113 Párrafo 4<br>✓ Administración local y centralizada mediante la consola de administración, sistema de gestión<br>Referencia: Capeta: Propuesta Técnica, Numeral 10, Documento: FortiGate 900D Pág. 3 Párrafo 7<br>✓ Soporte de firewall next generation<br>Referencia: Capeta: Propuesta Técnica, Numeral 10, Documento: FortiGate 900D Pág. 1 Párrafo 2<br>✓ Soporte de Redundant Power supply (AC) 100-240 vac<br>Referencia: Capeta: Propuesta Técnica, Numeral 10, Documento: FortiGate 900D Pág. 4 Segunda Columna Linea 7 |
| 000019 | CONSOLAS DE ADMINISTRACION Y SISTEMA DE GESTION | APPLIANCE | 3 | El sistema de gestión de la información deberá de contar con las facilidades para configura, recopilar, organizar, analizar y sistema de monitoreo, así mismo deberá proporcionar un análisis de reportero proporciona plantillas de informes predefinidos y diseño de informes profesional para personalizar los informes de estadísticas.<br>La solución de Seguridad deberá soportar la administración de tráfico por usuario, y por grupos de usuarios.<br>La política de administración de tráfico puede definir anchos de banda a un solo usuario o a un grupo de usuarios.<br>La solución de monitoreo deberá proporcionar un Dashboard para detectar rápidamente tráfico anormal (basado en IP, en aplicaciones, en QoS) en toda la red además de contar con un modelo de análisis de tráfico por capas. Además deberá permitir la customización del dashboard.<br>La solución de seguridad deberá tener capacidad de correr análisis de vulnerabilidades a nivel de red. | GRUPO DE TECNOLOGÍA CIBERNÉTICA S.A DE C.V OFERTA FortiManager, junto con la familia FortiAnalyzer un sistema de gestión de la información que cuenta con las facilidades para configurar, recopilar, organizar, analizar y sistema de monitoreo, así mismo deberá proporcionar un análisis de reportero proporciona plantillas de informes predefinidos y diseño de informes profesional para personalizar los informes de estadísticas.<br>La solución de Seguridad deberá soportar la administración de tráfico por usuario, y por grupos de usuarios.<br>La política de administración de tráfico puede definir anchos de banda a un solo usuario o a un grupo de usuarios.<br>La solución de monitoreo deberá proporcionar un Dashboard para detectar rápidamente tráfico anormal (basado en IP, en aplicaciones, en QoS) en toda la red además de contar con un modelo de análisis de tráfico por capas. Además deberá permitir la customización del dashboard.<br>La solución de seguridad deberá tener capacidad de correr análisis de vulnerabilidades a nivel de red<br>Referencia: Capeta: Propuesta Técnica, Numeral 9, Documento: FortiManager pag. 1 Párrafos 1 y 2, 2 Parrafos 1,3 y 5 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | Referencia: Capeta: Propuesta Técnica, Numeral 5, Documento: FortiOS Handbook Version 5.2.3 Pág 908 Párrafos 3 y 4, Pág.63 Párrafo 3 y Pág. 169 Párrafo 7. |
| | | | | EN EL SITIO DE TCT:<br>• Dispositivo 1- Consola de Administración: Con un mínimo de 5,000 dispositivos. Deberá contemplar la opción de monitorear al menos 500 equipos marca JUNIPER modelos SRX110, SRX220, ISG2000, SSG20.<br>• Dispositivo 2- Sistema de Gestión: Capacidad de generar reportes en base a tráfico, aplicaciones y direccionamiento ip.<br>Capacidad de integrar dispositivos de otras marcas para generar reportes en base a logs. | GRUPO DE TECNOLOGÍA CIBERNÉTICA S.A DE C.V OFERTA EN EL SITIO DE TCT:<br>• Dispositivo 1 FORTIMANAGER 3900E - Consola de Administración: Con un mínimo de 5,000 dispositivos. Se contempla la opción de monitorear al menos 500 equipos marca JUNIPER modelos SRX110, SRX220, ISG2000, SSG20.<br>Referencia: Capeta: Propuesta Técnica, Numeral 9, Documento: FortiManager Pág. 1 Párrafo 2, 3 Línea 3<br>Esta referencia con base a la junta de aclaraciones del pasado 30 de septiembre, con referencia a la pregunta 30 de Grupo de Tecnología Cibernética S.A de C.V. que dice; Considerando que el objeto de la licitación es la conexión segura de las gerencias estatales, unidades administrativas, y oficinas telegráficas con los sitio TGT, CTO, y TGO, se entiende que el monitoreo de estos equipos es únicamente de la VPN que se tendrá de los sitios centrales. ¿Es correcta nuestra apreciación?<br>A lo que TELECOMM respondió: SI, Es correcta.<br>• Dispositivo 2 FORTIANALYZER 3900E - Sistema de Gestión: Capacidad de generar reportes en base a tráfico, aplicaciones y direccionamiento ip.<br>Capacidad de integrar dispositivos de otras marcas para generar reportes en base a logs.<br>Referencia: Capeta: Propuesta Técnica, Numeral 8, Documento: FortiAnalyzer Pág 1 Párrafo 1, 2 Párrafo 3 |
| | | | | EN EL SITIO DE CTO:<br>• Dispositivo 3- Consola de Administración: Con licencia incluida para 500 dispositivos y un soporte de hasta 1000 dispositivos. | GRUPO DE TECNOLOGÍA CIBERNÉTICA S.A DE C.V OFERTA EN EL SITIO DE CTO:<br>• Dispositivo 3 FORTIMANAGER 1000D - Consola de Administración: Soporte de hasta 1000 dispositivos.<br>Referencia: Capeta: Propuesta Técnica, Numeral 9, Documento: FortiManager Pág. 3 Línea 3 |
| 020001 | FIREWALL'S REMOTOS PARA GERENCIAS ESTATALES Y UNIDADES ADMINISTRATIVAS. | APPLIANCE | 32 | DISTRIBUIDOS A NIVEL NACIONAL.<br>UBICACIÓN EN LAS CAPITALES DE LOS ESTADOS:<br>✓ 32 Equipos "ACT5" (Appliance Crítico Tipo 5) con las siguientes características técnicas mínimas.<br>✓ Desempeño de Firewall para tráfico de Internet monitoreado: 500 Mbps<br>✓ IPsec VPN throughput: 70 Mbps | GRUPO DE TECNOLOGÍA CIBERNÉTICA S.A DE C.V OFERTA FORTIWIFI -60CX-ADSL-A DISTRIBUIDOS A NIVEL NACIONAL.<br>UBICACIÓN EN LAS CAPITALES DE LOS ESTADOS:<br>✓ 32 Equipos "ACT5" (Appliance Crítico Tipo 5) con las siguientes características técnicas mínimas.<br>✓ Desempeño de Firewall para tráfico de Internet |

| | | | | | |
|---|---|---|---|---|---|
| | | | | ✓ IPsec VPN site to site tunnels: 50<br>✓ IPsec VPN<br>✓ IPsec NAT Transversal<br>✓ Redundat VPN Gateway (capacidad de establecimiento de comunicación a una red remota a través de más de 2 VPN's, con diferente Gateway).<br>✓ Conexiones por segundo de 2,700<br>✓ Al menos No. de Sesiones concurrentes : 200,000<br>✓ Políticas de seguridad: 2,000<br>✓ Usuarios soportados: no restringido<br>✓ **Al menos 8 puertos 10/100/1000 base T, con slots para tarjeta vdsl/adsl2+ wan (anexo A y B) compatible con el servicio de Infinitum de TELMEX, opcional este puerto deberá estar en el mismo equipo appliance o en su defecto se acepta un modem externo ADSL/ADSL2+ compatible con el servicio de Infinitum de TELMEX que solo permita la conexión de la interface externa del firewall basado en MAC address.( El modem deberá de operar en modo transparente "BRIDGE")**<br>✓ **PPPoE (en caso de uso de modem se llevara a cabo la autenticación a través del firewall).**<br>✓ Ruteo OSPF<br>✓ Ruteo estático<br>✓ Número de usuarios: sin restricciones<br>✓ Numero de zonas virtuales de seguridad: 23<br>✓ Numero de ruteadores / firewalls virtuales con funcionalidad capa 3 / PBR : 14<br>✓ Numero de VLANS: 128<br>✓ Administración local y centralizada mediante la consola de administración, sistema de gestión.<br>✓ Soporte de firewall next generation<br>Power Supply (AC)100-240 vac | monitoreado: 1G<br>Referencia: Capeta: Propuesta Técnica, Numeral 11, Documento: FortiWIFI-60C Pág. 4 Línea 16<br><br>✓ IPsec VPN throughput: 70 Mbps<br>Referencia: Capeta: Propuesta Técnica, Numeral 11, Documento: FortiWIFI-60C Pág. 4 Línea 22<br><br>✓ IPsec VPN site to site tunnels: 50<br>Referencia: Capeta: Propuesta Técnica, Numeral 11, Documento: FortiWIFI-60C Pág. 4 Línea 23<br><br>✓ IPsec VPN<br>Referencia: Capeta: Propuesta Técnica, Numeral 11, Documento: FortiWIFI-60C Pág. 4 Línea 22<br><br>✓ IPsec NAT Transversal<br>Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: FortiOS Handbook Firewall for FortiOS 5.0 Pág. 20 Párrafo 5, 26 Párrafo 8 y 27 Párrafo 3<br><br>✓ Redundat VPN Gateway (capacidad de establecimiento de comunicación a una red remota a través de más de 2 VPN's, con diferente Gateway).<br>Referencia: Capeta: Propuesta Técnica, Numeral 5, Documento: FortiOS Handbook Version 5.2.3 Pág 1451 Párrafo 12 y Pág. 1588 Párrafo 1.<br><br>✓ Conexiones por segundo de 1,500,000<br>Referencia: Capeta: Propuesta Técnica, Numeral 11, Documento: FortiWIFI-60C Pág. 4, Línea 18<br><br>✓ Al menos No. de Sesiones concurrentes : 400,000<br>Referencia: Capeta: Propuesta Técnica, Numeral 11, Documento: FortiWIFI-60C Pág. 4 Línea 19<br><br>✓ Políticas de seguridad: 5,000<br>Referencia: Capeta: Propuesta Técnica, Numeral 11, Documento: FortiWIFI-60C Pág. 4 Línea 21<br><br>✓ Usuarios soportados: no restringido<br>Referencia: Capeta: Propuesta Técnica, Numeral 3, Documento: NGFW Solution Brief Pág. 1 Párrafo 7<br><br>✓ **6 puertos 10/100/1000 base T, con slots para tarjeta vdsl/adsl2+ wan (anexo A y B) compatible con el servicio de Infinitum de TELMEX, opcional este puerto deberá estar en el mismo equipo appliance o en su** |

120002

defecto se acepta un modem externo ADSL/ADSL2+ compatible con el servicio de Infinitum de TELMEX que solo permita la conexión de la interface externa del firewall basado en MAC address.( El modem deberá de operar en modo transparente "BRIDGE")

Referencia: Capeta: Propuesta Técnica, Numeral 11, Documento: FortiWIFi-60C Pág. 4 Línea 3-4 y Pág. 5 Línea 7

Esta referencia con base a la junta de aclaraciones del pasado 30 de septiembre, con referencia a la pregunta 31 de Grupo de Tecnología Cibernética S.A de C.V. Que dice: ¿Acepta la convocante una solución que incluya 6 puertos RJ45 10/100/1000 y 4 puertos 10/100? De tal forma que se entreguen 10 puertos RJ45 para las gerencias estatales y unidades administrativas. A lo que TELECOMM respondió: Se acepta su propuesta siempre y cuando como mínimo se entreguen 6 puertos RJ45 10/100/1000 Base T y se complemente a 8 puertos en total con RJ45 10/100 Base T.

- ✓ PPPoE (en caso de uso de modem se llevara a cabo la autenticación a través del firewall).

Referencia: Capeta: Propuesta Técnica, Numeral 5, Documento: FortiOS Handbook Version 5.2.3 Pág 137 Párrafos 1 y 2

- ✓ Ruteo OSPF

Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: FortiOS Handbook Firewall for FortiOS 5.0 Pág. 18 Párrafo 7
Referencia: Capeta: Propuesta Técnica, Numeral 6, Documento: FortiOS Handbook Install and System Administration for FortiOS 5.0Pág 163 Párrafo 3

- ✓ Ruteo estático

Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: FortiOS Handbook Firewall for FortiOS 5.0 Pág. 18 Párrafo 4
Referencia: Capeta: Propuesta Técnica, Numeral 6, Documento: FortiOS Handbook Install and System Administration for FortiOS 5.0Pág 163 Párrafo 2

- ✓ Número de usuarios: sin restricciones

Referencia: Capeta: Propuesta Técnica, Numeral 3, Documento: NGFW Solution Brief Pág. 1 Párrafo 7

- ✓ Numero de zonas virtuales de seguridad: 8192

Referencia: Capeta: Propuesta Técnica, Numeral 5, Documento: FortiOS Handbook Version 5.2.3 Pág 2108 Párrafo 1 y Pág. 2164 Párrafo 10.

| | | | | | |
|---|---|---|---|---|---|
| | | | | | Esta referencia con base a la junta de aclaraciones del pasado 30 de septiembre, con referencia a la pregunta 25 de Carvajal Tecnología y Servicios, S.A de C.V Que dice: ¿Es correcto entender que Zonas Virtuales de Seguridad se refiere a segmentos que pueden ser puertos físicos, o bien VLAN que tengan políticas de seguridad?. A lo que TELECOMM respondió SI, es correcto<br>✓ Numero de ruteadores / firewalls virtuales con funcionalidad capa 3 / PBR : 250<br>Referencia: Capeta: Propuesta Técnica, Numeral 7, Documento: Fortinet About the Maximum Values Table Pág 2 Fila 1 y Pág. 3 Fila 30<br>✓ Numero de VLANS: 4096<br>Referencia: Capeta: Propuesta Técnica, Numeral 6, Documento: FortiOS Handbook Install and System Administration for FortiOS 5.0 Pág. 113 Párrafo 4<br>✓ Administración local y centralizada mediante la consola de administración, sistema de gestión.<br>Referencia: Capeta: Propuesta Técnica, Numeral 11, Documento: FortiWiFi-60C Pág. 3 Párrafo 3<br>✓ Soporte de firewall next generation<br>Referencia: Capeta: Propuesta Técnica, Numeral 11, Documento: FortiWiFi-60C Pág. 3 Párrafo 5<br>- Power Supply (AC)100-240 vac<br>Referencia: Capeta: Propuesta Técnica, Numeral 11, Documento: FortiWiFi-60C Pág. 4 Línea 39 |
| "2"<br>ALTO | FIREWALL'S REMOTOS PARA OFICINAS TELEGRAFICAS. | APPLIANCE | MINIMO DE 1200<br><br>MAXIMO DE 1600 | DISTRIBUIDOS A NIVEL NACIONAL:<br>• Mínimo 1200 a un Máximo de 1600 Equipos "AAT6" (Appliance Alto Tipo 6) y Equipos "ABT7" (Appliance Bajo Tipo 7) con las siguientes características técnicas mínimas.<br>✓ Desempeño de Firewall para tráfico de Internet monitoreado: 290 Mbps<br>✓ IPsec VPN throughput: 70 Mbps<br>✓ IPsec VPN site to site tunnels: 50<br>✓ IPsec VPN<br>✓ IPsec NAT Transversal<br>✓ Redundat VPN Gateway<br>✓ Conexiones por segundo de 1,700<br>✓ Al menos No. Sesiones concurrentes : 100,000<br>✓ Políticas de seguridad: 384<br>✓ Usuarios soportados: sin restricciones<br>✓ Al menos 8 puertos 10/100/1000 base T, con slots para tarjeta vdsl/adsl2+ wan (anexo A y B) compatible con el servicio de Infinitum de TELMEX, opcional este puerto deberá estar en el mismo equipo appliance o en su defecto se acepta un modem externo ADSL/ADSL2+ | GRUPO DE TECNOLOGÍA CIBERNÉTICA S.A DE C.V OFERTA FORTIWIFI -60CX-ADSL-A<br>DISTRIBUIDOS A NIVEL NACIONAL:<br>• Mínimo 1200 a un Máximo de 1600 Equipos "AAT6" (Appliance Alto Tipo 6) y Equipos "ABT7" (Appliance Bajo Tipo 7) con las siguientes características técnicas mínimas:<br>✓ Desempeño de Firewall para tráfico de Internet monitoreado: 1G<br>Referencia: Capeta: Propuesta Técnica, Numeral 11, Documento: FortiWiFi-60C Pág. 4 Línea 16<br>✓ IPsec VPN throughput: 70 Mbps<br>Referencia: Capeta: Propuesta Técnica, Numeral 11, Documento: FortiWiFi-60C Pág. 4 Línea 22<br>✓ IPsec VPN site to site tunnels: 50<br>Referencia: Capeta: Propuesta Técnica, Numeral 11, Documento: FortiWiFi-60C Pág. 4 Línea 23<br>✓ IPsec VPN |

| | | | |
|---|---|---|---|
| | | compatible con el servicio de Infinitum de TELMEX que solo permita la conexión de la interface externa del firewall basado en MAC address. ,( El modem deberá de operar en modo transparente "BRIDGE")<br>✓ PPPoE (en caso de uso de modem se llevara a cabo la autenticación a través del firewall),<br>✓ Ruteo OSPF<br>✓ Ruteo estático<br>✓ Número de usuarios: sin restricciones<br>✓ Numero de zonas virtuales de seguridad: 10<br>✓ Numero de ruteadores / firewalls virtuales con funcionalidad capa 3 / PBR : 3<br>✓ Numero de VLANS: 16<br>✓ Administración local y centralizada mediante la consola de administración, sistema de gestión.<br>✓ Soportar VPNs dinámicas para establecer Túneles de IPSec dinámicos en las oficinas remotas.<br>✓ Soportar configuraciones de políticas de seguridad basados usuario o grupos de usuario, protocolos de capa de aplicación, ubicación, direcciones IP o grupo de direcciones IP y puertos unificados de la web de filtrados de contenido seguro.<br>✓ Soporte de firewall next generation<br>Power supply (AC)100-240 vac | Referencia: Capeta: Propuesta Técnica, Numeral 11, Documento: FortiWIFI-60C Pág. 4 Línea 22<br><br>✓ IPsec NAT Transversal<br>Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: FortiOS Handbook Firewall for FortiOS 5.0 Pág. 20 Párrafo 5, Pág. 26 Párrafo 8 y Pág. 27 Párrafo 3<br><br>✓ Redundat VPN Gateway<br>Referencia: Capeta: Propuesta Técnica, Numeral 5, Documento: FortiOS Handbook Version 5.2.3 Pág 1451 Párrafo 12 y Pág. 1588 Párrafo 1.<br><br>✓ Conexiones por segundo de 1,500,000<br>Referencia: Capeta: Propuesta Técnica, Numeral 11, Documento: : FortiWIFI-60C Pág. 4 Línea 18<br><br>✓ Al menos No. de Sesiones concurrentes : 400,000<br>Referencia: Capeta: Propuesta Técnica, Numeral 11, Documento: FortiWIFI-60C Pág. 4 Línea 19<br><br>✓ Políticas de seguridad: 5,000<br>Referencia: Capeta: Propuesta Técnica, Numeral 11, Documento: FortiWIFI-60C Pág. 4 Línea 21<br><br>✓ Usuarios soportados: no restringido<br>Referencia: Capeta: Propuesta Técnica, Numeral 3, Documento: NGFW Solution Brief Pág. 1 Párrafo 7<br><br>✓ 6 puertos 10/100/1000 base T, con slots para tarjeta vdsl/adsl2+ wan (anexo A y B) compatible con el servicio de Infinitum de TELMEX, opcional este puerto deberá estar en el mismo equipo appliance o en su defecto se acepta un modem externo ADSL/ADSL2+ compatible con el servicio de Infinitum de TELMEX que solo permita la conexión de la interface externa del firewall basado en MAC address.( El modem deberá de operar en modo transparente "BRIDGE")<br>Referencia: Capeta: Propuesta Técnica, Numeral 11, Documento: FortiWIFI-60C Pág. 4 Línea 3-4 y Pág. 5 Línea 7<br>✓ Esta referencia con base a la junta de aclaraciones del pasado 30 de septiembre, con referencia a la pregunta 31 de Grupo de Tecnología Cibernética S.A de C.V. Que dice: ¿Acepta la convocante una solución que incluya 6 puertos RJ45 10/100/1000 y 4 puertos 10/100? De tal forma que se entreguen 10 puertos RJ45 para las |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | gerencias estatales y unidades administrativas. A lo que TELECOMM respondió: Se acepta su propuesta siempre y cuando como mínimo se entreguen 6 puertos RJ45 10/100/1000 Base T y se complemente a 8 puertos en total con RJ45 10/100 Base T.<br>✓ PPPoE (en caso de uso de modem se llevara a cabo la autenticación a través del firewall).<br>Referencia: Capeta: Propuesta Técnica, Numeral 5, Documento: FortiOS Handbook Version 5.2.3 Pág 137 Párrafos 1 y 2<br>✓ Ruteo OSPF<br>Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: FortiOS Handbook Firewall for FortiOS 5.0 Pág. 18 Párrafo 7<br>Referencia: Capeta: Propuesta Técnica, Numeral 6, Documento:FortiOS Handbook Install and System Administration for FortiOS 5.0Pág 163 Párrafo 3<br>✓ Ruteo estático<br>Referencia: Capeta: Propuesta Técnica, Numeral 4, Documento: FortiOS Handbook Firewall for FortiOS 5.0 Pág. 18 Párrafo 4<br>Referencia: Capeta: Propuesta Técnica, Numeral 6, Documento:FortiOS Handbook Install and System Administration for FortiOS 5.0Pág 163 Párrafo 2<br>✓ Número de usuarios: sin restricciones<br>Referencia: Capeta: Propuesta Técnica, Numeral 3, Documento:NGFW Solution Brief Pág. 1 Párrafo 7<br>✓ Numero de zonas virtuales de seguridad: 8192<br>Referencia: Capeta: Propuesta Técnica, Numeral 5, Documento: FortiOS Handbook Version 5.2.3 Pág 2108 Párrafo 1 y Pág 2164 Párrafo 10. Esta referencia con base a la junta de aclaraciones del pasado 30 de septiembre, con referencia a la pregunta 25 de Carvajal Tecnología y Servicios, S.A de C.V Que dice: ¿Es correcto entender que Zonas Virtuales de Seguridad se refiere a segmentos que pueden ser puertos físicos, o bien VLAN que tengan políticas de seguridad?. A lo que TELECOMM respondió Si, es correcto<br>✓ Numero de ruteadores / firewalls virtuales con funcionalidad capa 3 / PBR : 250<br>Referencia: Capeta: Propuesta Técnica, Numeral 7, Documento:Fortinet About the Maximum Values Table Pág 2 Fila 1 y Pág 3 Fila 30 |

000025

| | | | | | |
|---|---|---|---|---|---|
| | | | | | ✓ Numero de VLANS: 4096<br>Referencia: Capeta: Propuesta Técnica, Numeral 6, Documento: FortiOS Handbook Install and System Administration for FortiOS 5.0Pág. 113 Párrafo 4<br><br>✓ Administración local y centralizada mediante la consola de administración, sistema de gestión.<br>Referencia: Capeta: Propuesta Técnica, Numeral 11, Documento:FortiWIFI-60C Pág. 3 Párrafo 3<br><br>✓ Soportar VPNs dinámicas para establecer Túneles de IPSec dinámicos en las oficinas remotas.<br>Referencia: Capeta: Propuesta Técnica, Numeral 5, Documento:: FortiOS Handbook Version 5.2.3 Pág 1451 Párrafo 5<br><br>✓ Soportar configuraciones de políticas de seguridad basados usuario o grupos de usuario, protocolos de capa de aplicación, ubicación, direcciones IP o grupo de direcciones IP y puertos unificados de la web de filtrados de contenido seguro<br>Referencia: Capeta: Propuesta Técnica, Numeral 5, Documento: FortiOS Handbook Version 5.2.3 Pág 808 Párrafos 4 y 5, 63 Párrafo 3, 169 Párrafo 7.<br><br>✓ Soporte de firewall next generation<br>Referencia: Capeta: Propuesta Técnica, Numeral 11, Documento:FortiWIFI-60C Pág. 3 Párrafo 5<br><br>- Power Supply (AC)100-240 vac<br><br>Referencia: Capeta: Propuesta Técnica, Numeral 11, Documento: FortiWIFI-60C Pág. 4 Línea 39 |

## 2.1. FIREWALL´S APPLIANCE CENTRALES (CONCENTRADORES DE "VPN´S), NIVEL "1" (CRÍTICO).

**"GRUPO TECNO"** oferta para los equipos firewall´s el modelo FortiGate 1500D, consolas de administración modelos FortiManager 1000D y FortiManager 3900E y sistema de gestión modelo FortiAnalyzer 3900E de NIVEL "1", solución que cumplirá con los requerimientos de operación y facilidades para reflejar el mismo esquema de operación tal como se muestra en el numeral 1.- DESCRIPCIÓN DEL ARRENDAMIENTO "Diagrama conceptual de operación de la red TELDAT" que se describe en la TABLA 1 incluida en la presente propuesta en el numeral 2 REQUERIMENTOS DE LA PRESENTE PROPUESTA TÉCNICA.

**"GRUPO TECNO"** oferta 10 (diez) appliance´s FIREWALL´S CONCENTRADORES modelo FortiGate 1500D requeridos por TELECOMM que incluyen las facilidades de dividir y desviar diferentes tipos de tráficos por destino y/o fuente de dirección IP (Internet Protocolo) y/o puerto TCP/UDP (Transmission Control Protocolo / User Datagram Protocolo) por cada enlace generado independientemente de su ruta de default original.

## 2.2. CONSOLAS DE ADMINISTRACIÓN Y SISTEMA DE GESTIÓN NIVEL "1" (CRÍTICO).

**"GRUPO TECNO"** oferta 2 (dos) Consolas de Administración modelos FortiManager 1000D y FortiManager 3900E y 1 (un) Sistema de Gestión remota modelo FortiAnalyzer 3900E, que incluye módulos de reporteo y licenciamiento para administrar la cantidad especificada de equipos especicados en la TABLA 1 incluida en la presente propuesta en el numeral 2 REQUERIMENTOS DE LA PRESENTE PROPUESTA TÉCNICA.

## 2.3. FIREWALL´S APPLIANCE REMOTOS (GERENCIAS ESTATALES Y UNIDADES ADMINISTRATIVAS) NIVEL "1" CRITICO.

**"GRUPO TECNO"** como alcance de la presente propuesta oferta 32 (treinta y dos) appliance´s FIREWALL´S remotos modelo FortiWifi -60CX-ADSL-A, requeridos por TELECOMM que incluyen las facilidades de dividir y desviar diferentes tipos de tráficos por destino y/o fuente de dirección IP (Internet Protocolo) y/o puerto TCP/UDP (Transmission Control Protocolo / User Datagram Protocolo) por cada enlace generado independientemente de su ruta de default original, equipos especicados en la TABLA 1 incluida en la presente propuesta en el numeral 2 REQUERIMENTOS DE LA PRESENTE PROPUESTA TÉCNICA.

## 2.4. FIREWALL´S APPLIANCE REMOTOS (OFICINAS TELEGRAFICAS) NIVEL "2" (ALTO) Y NIVEL "3" (BAJO).

"GRUPO TECNO" oferta como minimo 1200 (mil docientos) y hasta un máximo de 1600 (mil seicientos) appliance´s FIREWALL´S remotos modelo FortiWifi -60CX-ADSL-A, requeridos por TELECOMM—los cuales se implementaran a solicitud de TELECOMM de acuerdo a sus necesidades. Equipos especicados en la TABLA 1 incluida en la presente propuesta en el numeral 2 REQUERIMENTOS DE LA PRESENTE PROPUESTA TÉCNICA.

000027

## 3. ALCANCE DEL ARRENDAMIENTO

Como alcance de la presente propuesta **"GRUPO TECNO"**, en caso de resultar adjudicado, será el responsable de la puesta en operación del equipo ofertado, lo que incluye su instalación, configuración, migración e integración con la infraestructura de comunicaciones y seguridad que actualmente operan en TELECOMM.
**"GRUPO TECNO"** en caso de resultar adjudicado, implementará las herramientas de monitoreo necesarias a través del SISTEMA DE GESTIÓN ofertado en la presente propuesta, las cuales permitirán conocer el estado operativo del equipo que integra la solución, así mismo la gestión del servicio se realizará de forma pro-activa respecto a los incidentes que se puedan presentar.

**"GRUPO TECNO"** se encuentra en el entendido de que por razones de seguridad, TELECOMM proporcionará únicamente al LICITANTE QUE RESULTE ADJUDICADO, las configuraciones, políticas, ruteo y parámetros de los equipos que actualmente están operando, con objeto de que este ejecute la migración y puesta en operación del equipo ofertado en su propuesta.

**"GRUPO TECNO"** en caso de resultar adjudicado será responsable de, asegurar la continuidad en la operación de la infraestructura que compone el servicio ofertado en la presente propuesta; esto es, que todas las funcionalidades objeto del contrato se encuentren disponibles en todo momento, conforme a los niveles de servicio ofertados en la sección "11.1 Niveles de Servicio (SLA)" de la presente propuesta técnica.

Con objeto de asegurar el menor tiempo posible en la restauración de los servicios alcance de la presente oferta técnica en caso de desastre/contingencia, **"GRUPO TECNO"** pone a consideración del TELECOMM un plan de continuidad y recuperación (**Ver Carpeta "Documentación Carpeta Técnica" Pestaña "Plan de Continuidad"**) a utilizar en caso de desastre/contingencia, el cual se encuentra acotado a los alcances y componentes relacionados con el arrendamiento y se tomó en cuenta para su construcción las siguientes consideraciones:

### GESTIÓN DEL SERVICIO ADMINISTRADO.

**"GRUPO TECNO"** en caso de resultar adjudicado será el responsable de realizar en su totalidad la gestión del servicio en todos los sitios proporcionados por TELECOMM a través de los siguientes servicios:

- LÍDER DE GESTIÓN.- Será el responsable de planear, organizar, implementar, dirigir y controlar la migración a la infraestructura de los servicios que actualmente proporciona TELECOMM.
- Mesa de ayuda basada en estándares de ITIL y mejores prácticas del mercado.
- Administración de problemas y/o fallas.
- Administración de los niveles de servicio.
- Administración de las plataformas y sus configuraciones.
- Respaldo de configuración de dispositivos ofertados.
- Monitoreo de las plataformas.

000028

## A. SOPORTE A LOS EQUIPOS INCLUIDOS EN EL SERVICIO ADMINISTRADO.

**"GRUPO TECNO"** en caso de resultar adjudicado será responsable de identificar el ciclo de vida de los elementos de red, tanto de hardware como software, para lo cual deberá elaborar un plan de reemplazo en coordinación con personal de TELECOMM.

**"GRUPO TECNO"** en caso de resultar adjudicado será responsable de resolver cualquier condición operativa, ya sea física o lógica (mantenimiento y actualización de las plataformas) relacionada con los equipos (consolas, firewalls appliance centrales y remotos) alcance de la presente oferta técnica sin importar la etapa en la que se encuentre la instrumentación del servicio. Entre las tareas a realizar por parte de **"GRUPO TECNO"** en caso de resultar adjudicado, se enlistan de manera enunciativa, más no limitativa, las siguientes:

- Brindar Soporte técnico, (soporte del elemento de red, soporte del software del elemento) durante el ciclo de vida de cada uno de los dispositivos ofertados
- Proveer las refacciones necesarias para las consolas y equipos firewalls appliance centrales y remotos sin costo para TELECOMM.
- Reparar de fallas lógicas y restauración de configuraciones.
- Acudir y atender en sitio cuantas veces sea necesario, los incidentes que requieran alguna reparación o sustitución de los dispositivos.
- Realizar la configuración, traslado y puesta en operación del equipo ofertado, reasignado a un sitio por reemplazo, por cambio de domicilio y/o por apertura de una nueva oficina telegráfica.

**NOTA: Todo el equipo y componentes ofertados como alcance de la presente oferta técnica serán nuevos.**

- **"GRUPO TECNO"** pone a disposición de TELECOMM los siguientes medios para la atención y soporte:
  - A. vía telefónica: Para el D.F y Área Metropolitana al **5278-9211** y para el resto de la República Mexicana al **01-800-248-0888.**
  - B. vía web: La dirección para e acceso web será definido en coordinación con TELECOMM.
  - C. En sitio: Atención personalizada en sitio para los incidentes relacionados al alcance de la presente propuesta técnica.

## B. ACTUALIZACIONES SOFTWARE

"GRUPO TECNO" en caso de resultar adjudicado, será el responsable de las actualizaciones de versiones de software y/o firmware para consolas y equipos firewall´s appliances centrales y remotos. Y toda actualización de firmware y/o aplicación de parches que proporcione nuevas funcionalidades, será probada en coordinación con personal de TELECOMM, en ambiente controlado previo a su instalación en producción.

"GRUPO TECNO" en caso de resultar adjudicado proveerá acceso a actualizaciones de producto, así como al sitio web del fabricante del hardware y software y también a foros de discusión y a bases de conocimientos del mismo fabricante.

## C. REPORTES Y MONITOREO

El equipo FortiAnalyzer 3900E ofertado dentro del alcance de la presente propuesta técnica, proporcionará la facilidad de generar reportes de desempeño, con la finalidad de realizar análisis proactivos sobre los reportes de alerta que pongan en riesgo la infraestructura ofertada. **"GRUPO TECNO"** en caso de resultar adjudicado, generará y entregará tres tipos de reportes de análisis dentro del módulo de reporteo:

- Análisis de registros (logs) distribuidos.
- Análisis de amenazas.
- Gestión de cumplimiento con normativas de seguridad.

El equipo propuesto FortiManager 1000D y FortiManager 3900E analizará en tiempo real los siguientes puntos:

- Comportamiento de flujos de datos y mejorar los tiempos de respuesta en las sesiones de datos.
- Condiciones de recursos de los componentes de la infraestructura (procesamiento, memoria, ataques de dos, etc.).
- Requerimientos de recursos dinámicos (asignaciones de ancho de banda, priorización de tráfico/aplicaciones/servicios).
- Soportar funcionalidades para realizar distribución de tráfico y perfilamiento de servicio a las aplicaciones.
- Contar con la capacidad de diferenciar aplicaciones en tiempo real y aplicaciones críticas del negocio.

## D. INTEGRACION CON McAfee.

TELECOMM, como parte de sus mecanismos de seguridad en informática cuenta con equipo de filtrado de contenido de páginas web "URL" (Uniform Resource Locator) del fabricante McAfee, el cual está operando mediante la integración del servicio de filtrado de contenido con los actuales equipos firewalls appliance 's centrales. Por lo anterior, **"GRUPO TECNO"** presenta una carta emitida por el fabricante FORTINET INC, la cual manifiesta que los equipos firewall 's appliances ofertados son compatibles con el servicio de filtrado de contenido "URL" mediante el mecanismo de integración PBR (Policy Based Routing) y/o WCCP (Web Cache Control Protocol) para la correcta activación de los servicios que actualmente están operando en sitios centrales (**Ver Carpeta "Documentación Propuesta Técnica", Pestaña "Carta Fabricante Compatibilidad"**).

## E. ADMINISTRACIÓN DE CAMBIOS Y CONFIGURACIÓN.

"GRUPO TECNO" en caso de resultar adjudicado, será responsable de controlar y mantener actualizado el inventario de hardware y software alcance de la presente propuesta de arrendamiento solicitado. De igual forma, realizará las actividades asociadas a la evaluación, selección y adquisición de activos del hardware y software a través de las siguientes actividades:

000030

- Coordinar la entrega, instalación y pruebas minimizando fallas, procurando siempre la continuidad operativa de los equipos ofertados en la presento propuesta técnica.
- En caso de que **"GRUPO TECNO"** resulte adjudicado y derivado de los trabajos de migración de hardware y/o software se requiera hacer cambios, estos serán reportados a TELECOMM con al menos 72 horas de anticipación para efectuar la coordinación correspondiente.
- Cuando TELECOMM solicite cualquier cambio de la infraestructura, será notificado con al menos 72 horas de anticipación a **"GRUPO TECNO"** en caso de que resulte adjudicado.
- En el caso de que TELECOMM requiera activar nuevas facilidades, servicios u oficinas telegráficas durante el período de migración, TELECOMM informará a **"GRUPO TECNO"** en caso de que resulte ganador de estos cambios para que se vean contemplados y reflejados en los equipos ofertados para cuando entren en operación.

## F. TRANSFERENCIA DE CONOCIMIENTOS TECNOLÓGICOS.

**"GRUPO TECNO"**, en caso de resultar adjudicado y con base a la junta de aclaraciones del pasado 30 de septiembre de 2015 en la pregunta 5 de Grupo de Tecnología Cibernética, S.A. de C.V. que dice: Podría la convocante confirmar que la trasferencia de conocimientos se llevará acabo en las oficinas del licitante adjudicado dentro de la ciudad de México y/o Área Metropolitana, así mismo será el licitante adjudicado quien impartirá dicha transferencia y el contenido corresponderá a la implementación del presente proceso licitatorio, sin ser esto una capacitación formal o de certificación.

Respuesta: La transferencia de conocimiento será impartida por personal del fabricante de la marca ofertada y no se requiere certificación, en la CD de México.

Por lo que **"GRUPO TECNO"**, proveerá la transferencia de conocimientos de la nueva tecnología al personal designado por TELECOMM (máximo 10 personas). Tratándose aspectos básicos/ operativos y esquema intermedio/ avanzado para la administración y operación de la solución ofertada.

La transferencia de conocimiento, será impartida por personal del fabricante de la marca de los equipos ofertados en la presente propuesta técnica.

Adicionalmente **GRUPO TECNO** en caso de resultar adjudicado tiene en cuenta que personal de TELECOMM participara durante los trabajos de instalación, migración y puesta en operación del equipo ofertado como parte de la transferencia de conocimientos.

## G. ADMINISTRACIÓN COMPARTIDA

Siendo condición haber concluido la etapa de migración y puesta en operación del equipo ofertado y una vez que se haya concluido la transferencia de conocimientos tecnológicos. "GRUPO TECNO" en caso de resultar adjudicado compartirá la administración con el personal designado por TELECOMM, considerando los siguientes puntos como parte de la administración compartida:

000031

- TELECOMM será el responsable de la configuración especifica del perfil operativo de cada uno de los sitios remotos una vez que **"GRUPO TECNO"** en caso de resultar adjudicado haya realizado durante la etapa de migración de los primeros 100 equipos remotos para Oficinas Telegráficas.
- **"GRUPO TECNO"** en caso de resultar adjudicado será el responsable de la migración y puesta en operación del equipo ofertado del NIVEL "1" (CRITICO) con la finalidad de contar con los servicios activos con los que actualmente opera la Red TELDAT de TELECOMM. Una vez realizado dicha migración TELECOMM será el responsable de llevar a cabo la administración de dichos dispositivos.
- En la implementación y puesta en operación de equipos firewall 's remotos, asignados a Gerencias Estatales y Oficinas Telegráficas, **"GRUPO TECNO"** en caso de resultar adjudicado, facilitará temporalmente el equipo en las instalaciones de TELECOMM, TORRE CENTRAL DE TELECOMUNICACIONES (T.C.T.), EJE CENTRAL LÁZARO CÁRDENAS No 567, COL NARVARTE, B. JUÁREZ, C.P. 03020 1ER PISO ANEXO "B", con la finalidad de que personal de TELECOMM pueda transferir la configuración y parámetros del perfil correspondiente a cada sitio remoto.
- EN LA CONFIGURACIÓN DE POLÍTICAS, RUTEO Y PARÁMETROS. **"GRUPO TECNO"** en caso de resultar adjudicado, se coordinará con personal de TELECOMM para realizar las configuraciones de politicas, ruteo y parámetros para cada uno de los equipos que conforman la plataforma, de acuerdo a las necesidades requeridas por TELECOMM, además de asegurar los niveles de confidencialidad y seguridad que imperan en TELECOMM.
- **GRUPO TECNO** en caso de resultar adjudicado dará solución a problemas sobre nuevas implementaciones y/o modificaciones a las configuraciones de la plataforma instalada, sin costo para TELECOMM durante la vigencia contrato.

## 4. VIGENCIA DEL CONTRATO

**"GRUPO TECNO"** en caso de resultar adjudicado proveerá el arrendamiento alcance de la presente propuesta técnica a partir de la notificación de fallo y hasta el 31 de julio del 2018.

## 5. INICIO DE LA OPERACIÓN DEL ARRENDAMIENTO

GRUPO TECNO en caso de resultar adjudicado proveerá el arrendamiento alcance de la presente propuesta técnica a partir de las 00:00:01 hrs. del día 31 de octubre de 2015 hasta las 24:00:00 hrs., del día 31 de julio del 2018.

"GRUPO TECNO" pone a consideración de TELECOMM un "Plan De Trabajo Detallado" **(Ver Carpeta "Documentación Propuesta Técnica", Pestaña "Plan de Trabajo Detallado")**, el cual incluye las actividades a desempeñar para alcanzar los plazos establecidos y considera entre otros los siguientes puntos:

"GRUPO TECNO" desarrolló el citado "Plan De Trabajo Detallado" considerando que TELECOMM requiere que el arrendamiento solicitado inicie su operación de acuerdo a la especificación de las siguientes tablas para los diferentes NODOS, en el entendido de que las actividades descritas son enunciativas más no limitativas, "GRUPO TECNO" dará cumplimiento a los siguientes puntos:

## ➢ IMPLEMENTACIÓN PARA EQUIPOS CENTRALES

*ACTIVIDADES*: Instalación, Configuración y pruebas de conectividad.

| EQUIPO | SITIO | FECHA LIMITE DE IMPLEMENTACIÓN |
|---|---|---|
| 2 CONSOLAS DE ADMINISTRACIÓN MODELOS FORTIMANAGER 1000D Y FORTIMANAGER 3900E Y 1 SISTEMA DE GESTIÓN REMOTA MODELO FORTIANALYZER 3900E | TCT Y CTO | 30 OCTUBRE 2015 |
| 10 FIREWALL´S CENTRALES. MODELO FORTIGATE 1500D | 7 FIREWALL´S EN CTO | 30 OCTUBRE 2015 |
| | 2 FIREWALL´S EN TCT | 06 NOVIEMBRE 2015 |
| | 1 FIREWALL EN TULANCINGO | 13 NOVIEMBRE 2015 |

## ➢ PUESTA EN OPERACIÓN PARA EQUIPOS CENTRALES

*ACTIVIDADES:* Inicio de operación.

| EQUIPO | SITIO | FECHA DE INICIO DE OPERACIÓN |
|---|---|---|
| 2 CONSOLAS DE ADMINISTRACIÓN MODELOS FORTIMANAGER 1000D Y FORTIMANAGER 3900E Y 1 SISTEMA DE GESTIÓN REMOTA MODELO FORTIANALYZER 3900E | TCT Y CTO | 31 OCTUBRE 2015 |
| 10 FIREWALL´S CENTRALES. MODELO FORTIGATE 1500D | 7 FIREWALL´S EN CTO | 31 OCTUBRE 2015 |
| | 2 FIREWALL´S EN TCT | 07 NOVIEMBRE 2015 |
| | 1 FIREWALL EN TULANCINGO | 14 NOVIEMBRE 2015 |

000033

➢ **IMPLEMENTACIÓN Y PUESTA EN OPERACIÓN PARA EQUIPOS REMOTOS**

*ACTIVIDADES:* Instalación, Configuración y pruebas de conectividad, inicio de operación.

| EQUIPO | SITIO | FECHA LIMITE DE IMPLEMENTACIÓN E INICIO DE OPERACIÓN |
|---|---|---|
| 32 FIRWALL'S REMOTOS PARA GERENCIAS ESTATALES MODELO FORTIWIFI -60CX-ADSL-A<br><br>Y<br><br>1,200 FIREWALL'S REMOTO PARA OFICINAS TELEGRÁFICAS MODELO FORTIWIFI -60CX-ADSL-A | REGION I<br>EdoMex, Guerrero, Hidalgo, Morelos, Puebla, Queretaro, D.F. y Tlaxcala (aproximadamente 266 equipos) | 13 NOVIEMBRE 2015 |
| | REGION II<br>Aguascalientes, Colima, Guanajuato, Jalisco, Michoacan, Nayarit y Zacatecas (aproximadamente 306 equipos) | |
| | REGION III<br>Coahuila, Durango, Nuevo Leon, San Luis Potosi y Tamaulipas (aproximadamente 196 equipos) | 30 NOVIEMBRE 2015 |
| | REGION IV<br>BCN, BCS, Chihuahua, Sinaloa y Sonora (aproximadamente 192 equipos) | |
| | REGION V<br>Campeche,Chiapas, Oaxaca, Quintana Roo, Tabasco, Veracruz y Yucatán (aproximadamente 279 equipos) | 31 DICIEMBRE 2015 |
| 400 FIREWALL'S REMOTOS PARA OFICINAS TELEGRAFICA MODELO FORTIWIFI -60CX-ADSL-A | DISTRIBUCIÓN A NIVEL NACIONAL. | DURANTE LA VIGENCIA DEL CONTRATO A SOLICITUD DE TELECOMM. |

## 6. ASEGURAMIENTO DE LOS EQUIPOS QUE CONFORMAN LA SOLUCIÓN DEL ARRENDAMIENTO SOLICITADO.

"GRUPO TECNO" considera en la presente propuesta que el aseguramiento en el traslado, instalación y puesta en operación de los equipos ofertados; consolas, firewall's, appliances centrales y remotos, que conforman la solución de arrendamiento, estará a su cargo. Para tal efecto, todas las erogaciones y gastos que haga "GRUPO TECNO" en caso de resultar adjudicado por concepto de pagos a su personal, adquisición, transporte e instalación de equipos, amortizaciones, viáticos, soporte, adquisición de materiales, útiles, artículos y uniformes de trabajo de su personal, primas de seguros y deducibles, impuestos y por cualquier otro concepto durante y después de su instalación y puesta en operación; serán a cargo de "GRUPO TECNO", durante la vigencia del contrato.

## 7. INSTALACIÓN, MIGRACIÓN Y PUESTA EN OPERACIÓN DEL EQUIPO OFERTADO.

000034

**"GRUPO TECNO"** considera como alcance de la presente propuesta que será el responsable de la instalación, migración y puesta en operación del equipo ofertado en cada uno de los sitios listados en los numeral 1.1 y 1.2. de la presente propuesta.

- **GRUPO TECNO** entregará los equipos debidamente instalados, probados y funcionando a entera satisfacción de TELECOMM.
- Toda la infraestructura considerada en la presente propuesta ofertada por **"GRUPO TECNO"** será de un mismo fabricante (**Ver Carpeta "Documentación Propuesta Técnica", Pestaña "Carta Infraestructura"**), para el caso del sistema de gestión de seguridad para eventos y flujos de información de tráfico de red, se podrá considerar la integración de una solución de terceros.
- La instalación, migración y puesta en operación del equipo ofertado es responsabilidad de **"GRUPO TECNO"**.
- Durante el periodo de instalación, migración y sustitución de los equipos, **GRUPO TECNO** se compromete a garantizar la operación y los servicios a través de la integración con la infraestructura actual con que cuenta TELECOMM. Así mismo, se incluye en la presente propuesta un plan de retorno en caso de contingencia al momento de la migración y/o implementación **(Ver Carpeta "Documentación Propuesta Técnica", Pestaña "Plan de Retorno")**.
- **GRUPO TECNO** como parte del alance de la presente propuesta considera la instalación y puesta en operación del equipo ofertado, el software y/o firmware requerido:
  - Software/Firmware consola de administración.
  - Software/Firmware de administración de politicas.
  - Software/ Firmware de sistema de gestión de seguridad, eventos y flujos de información de tráfico de red.
  - Licenciamiento.
- **GRUPO TECNO** se compromete a que cualquier cambio durante la ejecución de las instalaciones que se obligue a modificar el proyecto original será solicitado por escrito a TELECOMM, mediante la presentación de un plan de trabajo, mismo que incluirá las especificaciones técnicas replanteadas con las modificaciones propuestas.
- **GRUPO TECNO** asumirá todos los gastos referidos al traslado, aseguramiento, instalación y puesta en operación del equipo ofertado.
- La presente propuesta, considera los herrajes para los dispositivos centrales que se requiere para su instalación en racks.
- En caso de reubicación de equipo objeto de esta licitación atendiendo las necesidades de TELECOMM, "GRUPO TECNO" se compromete a planear éstos en coordinación con personal de TELECOMM, sin que represente algún costo para TELECOMM.
- En caso que TELECOMM requiera aperturar nuevas oficinas telegráficas durante la vigencia, "GRUPO TECNO" se compromete a atender las solicitudes para la activación de nuevos nodos.

8. CONFIDENCIALIDAD

000035

La información y documentación que TELECOMM entregue a **"GRUPO TECNO"** se hace bajo términos de confidencialidad y de reserva, por lo que **"GRUPO TECNO"** está en el entendido de que no podrá divulgar o aprovechar para beneficio o interés propio o de terceros los conocimientos e información propiedad de TELECOMM. Así también **"GRUPO TECNO"** entiende que una vez terminada la vigencia del contrato respectivo o si por algún motivo se cancelara el arrendamiento contratado, quedará obligado a devolver toda la información que se le hubiese proporcionado, prevaleciendo la titularidad de TELECOMM.

De tal forma que **"GRUPO TECNO"** se comprometerá a firmar una carta de confidencialidad con TELECOMM, que proteja el sistema de seguridad que opera en la RTI contra cualquier divulgación de información del sistema, alcanzando la responsabilidad a sus empleados y personal de terceros que participen en este arrendamiento.

## 9. TABLA DE CRITERIO DE EVALUACIÓN

**GRUPO TECNO** presenta la información documental para acreditar el cumplimiento de cada uno de los rubros de la siguiente tabla de puntos y porcentajes:

| **I.- CARACTERISTICA DEL BIEN O BIENES OBJETO DE LA PROPUESTA TÉCNICA.** | | **Puntos del Rubro 20** | **Referencia** |
|---|---|---|---|
| **I.A.- Caracteristicas los bienes objeto de la propuesta técnica.** | | ***Puntos del Subrubro 20*** | |
| **El licitante deberá cumplir con la totalidad de las especificaciones técnicas solicitadas en la TABLA I "DESCRIPCION DEL EQUIPO SOLICITADO" del ANEXO TÉCNICO.**<br>Para cumplir cualquiera de los requisitos de los bienes el Licitante deberá presentar fichas técnicas, manuales o cualquier documento técnico del fabricante acompañado por una carta del fabricante firmada por el representante legal manifestando que dichos documentos están soportados por el fabricante y que los equipos ofertados cumplen con las caracteristicas que se mencionan en la documentación entregada. Para cada especificación técnica del equipo ofertado, se deberá indicar en el documento de referencia, capitulo ó Núm. de página, la referencia deberá estar subrayada.<br><br>Se otorgará 8 puntos al licitante que cumpla en su proposición con la totalidad de las especificaciones técnicas solicitadas. | 8 | 8 | **"GRUPO TECNO"** cumple la totalidad de las especificaciones técnicas deacuerdo a la **TABLA 1** del Numeral **"2 ESPECIFICACIONES TÉCNICAS"** de la presente propuesta técnica.<br><br>Adicionalmente presenta como anexo a ésta propuesta técnica: **"Carta de Documentación y Equipos"** emitida por el fabricante de los equipos ofertados. (Ver Carpeta "Documentación Propuesta Técnica", Pestaña "Carta de Documentación y Equipos") |
| Se otorgará 1 punto al licitante que cumpla en su proposición con el 50% de la totalidad de las especificaciones técnicas solicitadas. | 1 | | |
| Se otorgará 0.5 puntos al licitante que cumpla en su proposición con menos del 50% de la totalidad de las especificaciones técnicas solicitadas. | 0.5 | | |
| El equipo "ACT1, ACT2, ACT3" propuesto deberá de contar con la siguiente cantidad de puertos de forma nativa, sin necesidad de agregar módulos adicionales:<br>Al menos 16 puertos Ethernet 10/100/1000 base T.<br>Al menos 16 puertos 1 Gbps SFP. | 4 | 4 | "GRUPO TECNO" como parte de su propuesta técnica proveerá equipos de firewall para sitios centrales con el siguiente |

| | | | |
|---|---|---|---|
| **Al menos 4 puertos ópticos 10Gb SFP+ en tecnología SR.**<br>Se otorgará 4 puntos al licitante que cumpla de forma nativa con el número de puertos solicitados. | | | número de puertos:<br>✓ 16 puertos Ethernet 10/100/1000 base T.<br>✓ 16 puertos 1 Gbps SFP.<br>✓ 8 puertos ópticos 10Gb SFP+ en tecnología SR.<br><br>Como se describe en la hoja de datos técnicos del equipo, Anexo: "FortiGate-1500D" Página 2, Linea 5,6 y 7. (Ver Carpeta "Propuesta Técnica" Numeral 2 Documento: FortiGate-1500D |
| Se otorgará 0.5 puntos al licitante que no cumpla de forma nativa con el número de puertos solicitados. | 0.5 | | |
| **Los equipos propuestos deberán de contar por lo menos con las siguientes funcionalidades de seguridad, las cuales deberán ser de la misma marca del equipo ofertado:**<br>1. Anti malware<br>2. IPS (Detección de ataques de red y Protección a DoS y DDoS)<br>3. Capacidad de detectar y bloquear aplicaciones, tráfico malicioso y anomalías de tráfico en protocolos http y https.<br>4. Capacidad de descripción de tráfico SSL de entrada y salida.<br>Se otorgará 4 puntos al licitante que cumpla con los cuatro rubros de acuerdo al requerimiento. | 4 | 4 | "GRUPO TECNO" como parte de su propuesta técncia proveerá equios de firewall para sitios centrales con las siguientes funcionalidades de seguridad:<br>1. Anti malware<br>2. IPS (Detección de ataques de red y Protección a DoS y DDoS)<br>3. Capacidad de detectar y bloquear aplicaciones, tráfico malicioso y anomalías de tráfico en protocolos http y https.<br>4. Capacidad de descripción de tráfico SSL de entrada y salida.<br><br>Como se describe en la hoja de datos técnicos del equipo, Anexo: "FortiOS_UTM"<br>Página 4, Columna 1 Filas 21, 24<br>Página 4, Columna 2, fila 1<br>Página 5, Columna 1, Fila 1,3,920 y 23<br><br>(Ver Carpeta "Propuesta Técnica" Numeral 12 Documento: FortiOS_UTM) |
| Se otorgará 1.5 puntos al licitante que cumpla con los rubros 2 y 3 de acuerdo al requerimiento. | 1.5 | | |
| Se otorgará 0.5 puntos al licitante que cumpla con los rubros 1 y 4 de acuerdo al requerimiento. | 0.5 | | |
| **Las consolas de administración propuestas por el licitante deberán presentarse en equipo appliance con dashboard preferentemente en idioma Español.**<br>Se otorgará 4 puntos al licitante que presente en idioma español las consolas de administración. | 4 | 4 | "GRUPO TECNO" como parte de su propuesta técnica oferta consolas de administración con Equipo Appliance con dashboard en idioma español.<br><br>Como se describe en la hoja de datos técnicos del equipo, Anexo: |

| | | | |
|---|---|---|---|
| | | | "FortiOS_UTM" Página 5, Columna 2, Fila 28. (Ver Carpeta "Propuesta Técnica" Numeral 12 Documento: FortiOS_UTM) |
| Se otorgará 0.5 puntos al licitante que presente en idioma inglés las consolas de administración. | 0.5 | | |
| **II.-CAPACIDAD DEL LICITANTE.** | | **Puntos del Rubro 15** | **Referencia** |
| ***II.A.- Capacidad de los Recursos Humanos.*** | | ***Puntos del Subrubro 14.5*** | |
| **El licitante deberá contar con al menos 2 Recursos Humanos certificados con el nivel más alto de Especialista en Seguridad de TI de la marca propuesta y El licitante deberá contar con al menos 2 Recursos Humanos certificados de nivel más alto de Profesional en Seguridad de TI de la marca propuesta para la implementación, administración y soporte en seguridad.**<br><br>Se otorgará 2 puntos al licitante que cumpla con la totalidad de los recursos de este requerimiento. Cada uno de los recursos propuestos deberá presentar sus certificaciones vigentes y carta expedida por el fabricante que avale el nivel más alto de certificación correspondiente. Los recursos propuestos deberán pertenecer a la plantilla de personal de licitante, lo cual se acreditara con el alta ante el Instituto Mexicano del Seguro Social (dicha alta no deberá ser menor a seis meses. | 2 | 2 | "GRUPO TECNO" presenta cuatro certificaciones con el nivel mas alto como especialista de Seguridad de TI de la marca propuesta de los Ingenieros:<br>1) Arturo Zúñiga<br>Certificado: Fortinet Certified Networks Securiy Professional (V4.x)<br>2) Rosarura García Soiano<br>Certificado: Fortinet Certified Networks Securiy<br>3) Jesús Pérez Velasco<br>Certificado: Fortinet Certified Networks Securiy<br>4) Juan Carlos Ramírez Carrasco<br>Certificado: Fortinet Certified Networks Securiy<br><br>Ver copia de las certificaciones en el Anexo "Certificaciones con el Nivel más Alto en Seguridad de TI de la Marca Propuesta"<br><br>Ver también la copia de alta ante el Instituto Mexicano del Seguro Social (fecha mayor a seis meses).<br>Ver Anexo "Copias de Alta Ante el IMSS"<br><br>Así como Anexo "Carta Certificaciones" expedida por el Fabricante |
| Se otorgará 1 punto al licitante que cumpla con al menos 2 Recursos Humanos certificados con el nivel más alto de Especialista en Seguridad de TI y 1 Recursos Humanos certificados de nivel más alto de Profesional en Seguridad de TI de la marca propuesta. Cada uno de los recursos propuestos deberá presentar sus certificaciones vigentes y carta expedida por el fabricante que avale el nivel más alto de certificación correspondiente. Los recursos propuestos deberán pertenecer a la plantilla de personal de licitante, lo cual se | 1 | | |

| | | | |
|---|---|---|---|
| acreditara con el alta ante el Instituto Mexicano del Seguro Social (dicha alta no deberá ser menor a seis meses. | | | |
| Se otorgará 0.5 puntos al licitante que cumpla con al menos 1 Recursos Humanos certificados con el nivel más alto de Especialista en Seguridad de TI y 2 Recursos Humanos certificados de nivel más alto de Profesional en Seguridad de TI de la marca propuesta. Cada uno de los recursos propuestos deberá presentar sus certificaciones vigentes y carta expedida por el fabricante que avale el nivel más alto de certificación correspondiente. Los recursos propuestos deberán pertenecer a la plantilla de personal de licitante, lo cual se acreditara con el alta ante el Instituto Mexicano del Seguro Social (dicha alta no deberá ser menor a seis meses. | 0.5 | | |
| El Licitante deberá acreditar satisfactoriamente la prueba "Prueba para acreditar la capacidad del licitante para firewalls centrales "ACT1" y remotos "AAT6" descritas en el ANEXO "C".<br>Se otorgará 12.5 puntos al licitante que acredite de forma satisfactoria la prueba. | 12.5 | 12.5 | |
| ***II.B.- Participación de discapacitados o empresas que cuenten con trabajadores con discapacidad.*** | | ***Puntaje del Subrubro 0.5*** | |
| **Contar con trabajadores con discapacidad en la plantilla para personas morales y constancia para personas físicas.**<br><br>Se otorgará 0.5 puntos al licitante que cuente con más del 5% de trabajadores discapacitados en su plantilla, deberá presentar el aviso de alta al régimen obligatorio del Instituto Mexicano del Seguro Social, que no sea inferior a seis meses de antigüedad a la presentación de las propuestas de este proceso Licitatorio, así mismo deberá entregar la plantilla de sus trabajadores indicando los trabajadores con discapacidad. | 0.5 | 0.5 | |
| Se otorgará 0.3 puntos al licitante que cuente con 5% de trabajadores discapacitados en su plantilla, deberá presentar el aviso de alta al régimen obligatorio del Instituto Mexicano del Seguro Social, que no sea inferior a seis meses de antigüedad a la presentación de las propuestas de este proceso Licitatorio, así mismo deberá entregar la plantilla de sus trabajadores indicando los trabajadores con discapacidad. | 0.3 | | |
| Se otorgará 0.2 puntos al licitante que cuente con menos de 5% de trabajadores discapacitados en su plantilla, deberá presentar el aviso de alta al régimen obligatorio del Instituto Mexicano del Seguro Social, que no sea inferior a seis meses de antigüedad a la presentación de las propuestas de este proceso Licitatorio, así mismo deberá entregar la plantilla de sus trabajadores indicando los trabajadores con discapacidad. | 0.2 | | |
| **III.- EXPERIENCIA Y ESPECIALIDAD DEL LICITANTE.** | | **Puntaje del Rubro 5** | **Referencia** |
| ***III.A.- Experiencia.*** | | ***Puntaje del Subrubro 2*** | |
| El licitante deberá presentar en hoja membretada, firmada por el cliente al que haya prestado servicios similares, la acreditación.<br>Se otorgará 2 puntos al licitante que cuente con experiencia y capacidad técnica mayor a 3 años en trabajos realizados de caracteristicas, complejidad y magnitud similares a lo solicitado. | 2 | 2 | Ver Carpeta Puntos y Porcentajes |
| Se otorgará 1 punto al licitante que cuente con experiencia y capacidad técnica igual a 3 años en trabajos realizados de caracteristicas, complejidad y magnitud similares a lo solicitado. | 1 | | |
| Se otorgará 0.5 puntos al licitante que cuente con experiencia y capacidad técnica menos a 3 años en trabajos realizados de caracteristicas, complejidad y magnitud similares a lo solicitado. | 0.5 | | |
| ***III.B.-Especialidad.*** | | ***Puntaje del Subrubro 3*** | |
| El licitante deberá presentar copia de contratos y sus anexos correspondientes, los cuales acrediten la experiencia y capacidad técnica en trabajos realizados de caracteristicas, complejidad y magnitud similares al solicitado. Se considerarán como contratos similares todos aquellos incluidos en contratos o pedidos de seguridad, cuyo objeto mencione el aprovisionamiento, implantación y soporte técnico de | 3 | 3 | Ver Carpeta Puntos y Porcentajes |

| | | | |
|---|---|---|---|
| **dispositivos de seguridad (firewalls, consola de administración y gestión).** Se otorgará 3 puntos al licitante que cumpla con más de 3 contratos. | | | |
| Se otorgará 1.5 puntos al licitante que cumpla con 3 contratos. | 1.5 | | |
| Se otorgará 1 puntos al licitante que cumpla con 1 ó 2 contratos. | 1 | | |
| **IV.- CUMPLIMIENTO DE CONTRATOS.** | | **Puntaje del Rubro 10** | **Referencia** |
| **El licitante deberá presentar copia de contratos incluyendo anexos correspondientes, carta o liberación de fianza que avale la terminación satisfactoria del contrato expedida por el cliente al que se le haya prestado servicios similares con una antigüedad de 1 a 10 años. Los contratos deberán acreditar el cumplimiento en trabajos realizados de características, complejidad y magnitud similares al solicitado. Se considerarán como contratos similares todos aquellos incluidos en contratos o pedidos de seguridad, cuyo objeto mencione el aprovisionamiento, implantación y soporte técnico de dispositivos de seguridad (firewalls, consola de administración y gestión).** Se otorgará 10 puntos al licitante que cumpla con más de 5 contratos. | 10 | 10 | Ver Carpeta Puntos y Porcentajes |
| Se otorgará 4 puntos al licitante que cumpla con 5 contratos. | 4 | | |
| Se otorgará 2 puntos al licitante que cumpla con 1 a 4 contratos. | 2 | | |

## 10. SUPERVISIÓN DE LOS TRABAJOS

"GRUPO TECNO" en caso de resultar adjudicado se compromete a contar con todos los recursos necesarios para la brindar las facilidades, las cuales aseguren el funcionamiento de la infraestructura habilitada, como parte del alcance de la presente licitación, y durante el tiempo que contemple el arrendamiento adquirido, así mismo deberá se compromete a poner a disposición en base al requerimiento de TELECOMM ingenieros que cuenten con especialidad certificada por el fabricante para los equipos ofertados para apoyo en sitio en las instalaciones de TCT.

Cada una de las partes designará representantes, "GRUPO TECNO" en caso de resultar adjudicado designará a un Project Manager para la Atención, Seguimiento y Solución de los aspectos Administrativos tales como cumplimiento al Contrato y Aclaración de Facturas; así como para atender las reuniones de supervisión y trabajo a que se convoque por parte de TELECOMM.

Como responsable de vigilar la ejecución del arrendamiento, "GRUPO TECNO" entiende que por parte de TELECOMM se designara al Ing. José Manuel Baños Pérez Gerente de la Red Telegráfica Integrada. Para la supervisión de los trabajos se realizarán reuniones de trabajo en las instalaciones de la Gerencia de Red Telegráfica Integrada primer piso Anexo-TCT, los miércoles de cada mes en el horario de 10:00 hrs. a 12:00 hrs. a partir de la fecha de inicio de contrato, la cual puede variar la fecha y hora dependiendo de las actividades operativas de dicha gerencia. La Gerencia de la Red Telegráfica Integrada realizara la convocatoria vía correo electrónico con una semana de anticipación a los participantes por parte de TELECOMM y "GRUPO TECNO", y se realizarán las minutas correspondientes a cada reunión de trabajo que se lleve a cabo.

Dichos representantes tendrán a su cargo la comunicación regular para todos los efectos del arrendamiento y podrán nombrar sustitutos previo aviso a la otra por escrito y con al menos quince días de anticipación. Ambas partes mantendrán los registros necesarios de las actividades realizadas en cumplimiento del arrendamiento.

000040

**"GRUPO TECNO"** se compromete a entregar reportes de servicio cada vez que se lleve a cabo un servicio. Asimismo, **"GRUPO TECNO"** se compromete durante la vigencia del contrato a entregar una memoria técnica, de los servicios realizados, así como dar sugerencias y propuestas de mejoras al sistema de acuerdo a las mejores prácticas.

**"GRUPO TECNO"** se compromete a mantener los registros necesarios de las actividades realizadas, en cumplimiento del contrato; se manejarán en forma conjunta la bitácora de reportes y **"GRUPO TECNO"** en caso de resultar adjudicado, entregará reportes que contenga lo siguiente:

- Reportes mensuales:
  - Detalle de la utilización actual de la infraestructura de red.
  - Reporte forense, documentando detalladamente cada incidente o problema presentado incluyendo cantidad y tipo de tráfico.
  - Incidentes y problemas ocurridos en el mes.
  - Equipos de sitios más vulnerables en la red.

- Reportes anuales:
  - Inventario de toda la infraestructura de la red de datos instalada.
  - Memoria técnica sobre altas bajas y cambios en la infraestructura de red.

## 11. NIVELES DE SERVICIO

**"GRUPO TECNO"**, cumple con los niveles de servicio que a continuación se indican:

### 11.1. Niveles de Servicio (SLA).

**"GRUPO TECNO"** cumple con procedimientos para otorgar el nivel de servicio medible (SLA-SERVICE-LEVEL AGREEMENT) para los diferentes sitios. Asimismo, **"GRUPO TECNO"** considera y se compromete a que los reportes generados serán atendidos en un tiempo de respuesta para diagnóstico y solución de falla tomando como base el reporte generado por TELECOMM de acuerdo a lo siguiente:

a. NIVEL 1 CRÍTICO: 6 HORAS A PARTIR DE QUE SE LEVANTE EL REPORTE DEL INCIDENTE.
b. NIVEL 2 ALTO: 24 HORAS A PARTIR DE QUE SE LEVANTE EL REPORTE DEL INCIDENTE.
c. NIVEL 3 BAJO: 48 HORAS A PARTIR DE QUE SE LEVANTE EL REPORTE DEL INCIDENTE.

DESCRIPCIÓN DE LOS NIVELES:

NIVEL "1" CRÍTICO:

Equipos que por su operación se consideran de nivel crítico; Consolas, Firewall 's Appliance Centrales de TCT, CTO y TGO., Firewall 's Appliance Remotos de Gerencias Estatales y Unidades Administrativas, para los cuales se requiere una atención no mayor a 6 horas.

000041

**NIVEL "2" ALTO:**

Equipos que por su operación se consideran de nivel alto; Firewalls Appliances Remotos de Oficinas Telegráficas, para los cuales se requiere una atención no mayor a 24 horas. Considerando tiempo de traslado máximo de 3 hrs. desde la capital del estado a sitio remoto.

**NIVEL "3" BAJO:**

Equipos que por su operación se consideran de nivel bajo; Firewalls Appliances Remotos de Oficinas Telegráficas, para los cuales se requiere una atención no mayor a 48 horas. Considerando tiempo de traslado mayor a 3 hrs. desde la capital del estado a sitio remoto.

Para los equipos Firewall 's Appliance Remotos de Gerencias Estatales y Oficinas Telegráficas, en caso de reemplazo del equipo **"GRUPO TECNO"** de entregará en sitio remoto el nuevo equipo para lo cual deberá de cumplir con lo siguiente:

1. Instalar el equipo con la infraestructura del carrier ADSL/TELMEX y de TELECOMM (usuarios).
2. Activar la autenticación PPPoE con el proveedor de servicio de ADSL/TELMEX.
3. Activar la administración a través de INTERNET (para que personal de TELECOMM realice la configuración del perfil en forma remota).

**"GRUPO TECNO"** dará cumplimiento a los siguientes puntos solicitados por TELECOMM:

- ✓ No se deberá de limitar el número de requerimientos para soporte, y/o atención a fallas, no importando las causas que lo provocaron, todo evento requerido será sin costo para TELECOMM durante la vigencia del contrato.
- ✓ En caso de ser necesario retirar algún equipo como consolas, firewall's appliance centrales y/o remotos para su reparación, **"GRUPO TECNO"** considera en su presente propuesta proporcionar un equipo de respaldo con las características iguales en hardware y software, así mismo se compromete a mantener las configuraciones del equipo original y será responsable de la puesta en operación.
- ✓ "GRUPO TECNO" se compromete a reintegrar el equipo reparado al mismo sitio de asignación original.
- ✓ Ante cualquier reporte de falla **"GRUPO TECNO"** proporcionará un número de control para el seguimiento, registrando la fecha y hora del mismo.
- ✓ Las partes y refacciones estarán sujetas al inventario que **"GRUPO TECNO"** considere más adecuado para cumplir con los requerimientos y niveles de servicio establecidos.
- ✓ En caso de sustitución definitiva de equipos, **"GRUPO TECNO"** considera en su presente propuesta que el equipo de sustitución será nuevo, de la misma marca y modelo que integre su propuesta siempre y cuando sea de caracteristicas iguales o superiores al sustituido, debiendo proporcionarse invariablemente dentro de los limites de tiempo anteriormente señalados y la configuración con las mismas caracteristicas en hardware y software al

original; también será responsable de identificar el nuevo equipo y/o componente y será administrado por el sistema de gestión de seguridad. Así mismo, presentará una carta donde constate el cambio, indicando claramente los números de serie y características.

- ✓ El reemplazo de piezas dañadas considerado en la presente propuesta por **"GRUPO TECNO"** será por piezas nuevas de calidad igual, equivalente o mayor a las especificaciones del equipo instalado y de la misma marca del fabricante.
- ✓ **"GRUPO TECNO"** considera que un reporte será considerado como cerrado satisfactoriamente cuando se encuentren reestablecidos los servicios para dicho equipo, dentro de la ventana de tiempo especificada.

## 11.2. CENTRO DE ATENCIÓN

**"GRUPO TECNO"** en caso de resultar adjudicado proporcionará la información relativa a su centro de atención de servicios: procedimiento y escalación (**Ver Carpeta "Documentación de Propuesta Técnica", Pestaña "Procedimiento de Escalación"**) para la atención de fallas que incluya la lista de teléfonos para levantar reportes, así como una lista con los datos (nombre, puesto, teléfono oficina, teléfono móvil, correo electrónico), tiempo establecido para pasar a los niveles de soporte del personal para el escalamiento de fallas, el horario de atención será de 7 x 24 x365, esto es, en caso de interrupción del servicio, este se obliga a efectuar el restablecimiento del servicio de conformidad con el procedimiento de atención, siendo el tiempo máximo estipulado en el nivel de servicio, para diagnóstico y reparación, contado a partir de que TELECOMM levante el reporte del incidente.

El centro de atención o el personal designado por **"GRUPO TECNO"**, llevará el seguimiento de los reportes para solución de fallas y que se mantengan abiertos debido a la severidad de la falla, y notificará cada hora a TELECOMM acerca del estado en que se encuentre dicho reporte hasta la solución del mismo. **"GRUPO TECNO"**, asignará a un ingeniero con el cual se coordinarán todas las acciones relativas a la ejecución de ventanas de mantenimiento programadas, las cuales deberán ser notificados a TELECOMM con 48 hrs. de anticipación con la finalidad de conseguir la autorización para accesar a los sitios de TELECOMM, donde se encuentre el equipo para ejecución de la ventana de mantenimiento correspondiente. **"GRUPO TECNO"** en caso de resultar adjudicado, proporcionará los siguientes medios de atención y soporte:

A. vía telefónica: Para el D.F y Área Metropolitana al 5278-9211 y para el resto de la República Mexicana al **01-800-248-0888.**
B. vía web: La dirección para e acceso web será definido en coordinación con TELECOMM.
C. En sitio: A través de soporte en sitio.

## 12. GARANTÍA TÉCNICA

"GRUPO TECNO" dará Garantía de la infraestructura instalada durante la vigencia del contrato a partir de la fecha de entrega a entera satisfacción de TELECOMM.

"GRUPO TECNO" será el único responsable de resolver cualquier condición operativa, ya sea física o lógica (mantenimiento de las plataformas y actualización de las plataformas) relacionada con los equipos ofertados (consolas, firewalls appliance centrales y remotos) durante la vigencia del

000043

contrato. **"GRUPO TECNO"** proporcionará a TELECOMM, los siguientes servicios (se enlistan de manera enunciativa, más no limitativa):

- Soporte técnico, (soporte del elemento de red, soporte del software del elemento), durante el ciclo de vida de cada uno de los equipos ofertados.
- Proveer cuantas veces se necesite las refacciones necesarias para las consolas y equipos firewalls appliance centrales y remotos sin costo para TELECOMM.
- Reparación de fallas lógicas y restauración de configuraciones.
- **"GRUPO TECNO"** se compromete a acudir al sitio cuantas veces sea necesario en caso de necesitar reparación o sustitución de los dispositivos.
- **"GRUPO TECNO"** realizará la configuración, traslado y puesta en operación del equipo ofertado reasignado a un sitio por reemplazo, por cambio de domicilio y/o por apertura de una nueva oficina telegráfica.
- Todo el equipo y componentes que sean ofertados por **"GRUPO TECNO"** serán nuevos.

000044

## 13. REQUISITOS TÉCNICOS

"GRUPO TECNO" considera la siguiente documentación como parte de los entregables requeridos como a continuación se indica para el arrendamiento solicitado.

| No. | Requisitos Técnicos | Referecia |
|---|---|---|
| 1 | Organigrama de la empresa, así como la Plantilla del personal que participara en la ejecución de las actividades del servicio objeto de la presente Licitación. | Ver Carpeta "Documentación Propuesta Técnica", Pestaña "Organigráma" |
| 2 | Carta emitida por el fabricante, en donde se especifique que TELECOMM tendrá el derecho de uso del licenciamiento para la puesta en operación del equipo ofertado. | Ver Carpeta "Documentación Propuesta Técnica", Pestaña "Carta Fabricante Uso de Licencia" |
| 3 | Plan de trabajo para la instalación, migración y puesta a punto para la solución ofertada. | Ver Carpeta "Documentación Propuesta Técnica", Pestaña "Plan de Trabajo" |
| 4 | Plan de continuidad y recuperación a utilizar en caso de desastre/contingencia, acotado a los alcances y componentes relacionados con el arrendamiento. | Ver Carpeta "Documentación Propuesta Técnica", Pestaña "Plan de Continuidad" |
| 5 | Carta compromiso en donde se especifique que entregará la Memoria Técnica reflejando los aspectos técnicos del servicio proporcionado de acuerdo a las siguientes fechas:<br>29/01/2016<br>16 DICIEMBRE 2016 ( ACTUALIZACIÓN)<br>15 DICIEMBRE 2017 (ACTUALIZACIÓN)<br>31 MAYO 2018 ( ACTUALIZACIÓN) | Ver Carpeta "Documentación Propuesta Técnica", Pestaña "Carta Memoria Técnica" |
| 6 | Carta emitida por el fabricante en donde se indique que los equipos firewall 's appliances ofertados son compatibles con el servicio de filtrado de contenido "URL" mediante el mecanismo de integración PBR (Policy Based Routing) y/o WCCP (Web Cache Control Protocol) para la correcta activación de los servicios que actualmente están operando en sitios centrales. | Ver Carpeta "Documentación Propuesta Técnica", Pestaña "Carta Fabricante Compatibilidad" |
| 7 | Carta original, membretada por el fabricante del(os) equipo(s), en donde se indique que EL LICITANTE cuenta con la capacidad para proporcionar la solución ofertada a nivel implementación, soporte, actualizaciones y servicios administrados y que cuenta con su respaldo para cumplir con los compromisos que llegue a contraer con TELECOMM producto de esta licitación, la carta debe tener fecha de expedición no mayor a tres meses a la publicación de la convocatoria. | Ver Carpeta "Documentación Propuesta Técnica", Pestaña "Carta Fabricante Cumplimiento de Especificaciones Técnicas" |
| 8 | Documento de pruebas realizadas que avalen la capacidad de efectividad del equipo FIREWALL ofertado, dicho documento de referencia deberá ser emitido por algún tercero (NSS Labs, Gartner, | Ver Carpeta "Documentación Propuesta Técnica", Pestaña "Capacidad de Efectividad"<br>Don de se encuentran los documentos:<br>✓ Magic-Quadrant-for-Enterprise- |

| No. | Requisitos Técnicos | Referecia |
|---|---|---|
| | Forrester, Telcordia, etc.) Sobre su efectividad mencionada en las hojas técnicas. | Network-Firewalls<br>✓ Firewall-Comparative-Analysis-Edition-Security-Technical-Brief<br>✓ Next-Generation-Firewall-Comparative-Analysis-SVM |
| 9 | Presentar al menos una de las siguientes certificaciones del equipo ofertado:<br>Certificación ICSA Labs de Firewall<br>Certificación ICSA Labs de IPSec<br>Certificación ICSA Labs de IPS | Ver Carpeta "Documentación Propuesta Técnica", Pestaña "Certificaciones del Equipo"<br>✓ Donde se enceuntran los documentos:<br>FORTINET_FIEWAL_4.2_REPORT<br>✓ FORTINET_iPSec_2.2_Report<br>✓ Fortinet_FG_NIPS_REPORT |
| 10 | Certificación vigente en original (para cotejo) y copia del Proyect Manager (PM) que forman parte de la Plantilla propuesta. | Ver Carpeta "Documentación Propuesta Técnica", Pestaña "Certificación PM" |
| 11 | Carta compromiso en donde se especifique que toda la infraestructura propuesta de equipo FIREWALL será de un mismo fabricante. | Ver Carpeta "Documentación Propuesta Técnica", Pestaña "Carta Infraestructura" |
| 12 | Carta compromiso en donde se especifique durante el periodo de instalación, migración y sustitución de los equipos, EL LICITANTE garantizará la operación y los servicios a través de la integración con la infraestructura actual de comunicaciones y seguridad con que cuenta TELECOMM. | Ver Carpeta "Documentación Propuesta Técnica", Pestaña "Carta Compromiso" |
| 13 | Carta compromiso en donde se especifique realizará la migración y puesta en operación del equipo ofertado para dar continuidad a los servicios actuales e integración con la infraestructura de comunicaciones y seguridad con la que actualmente opera TELECOMM. | Ver Carpeta "Documentación Propuesta Técnica", Pestaña "Carta Continuidad a los Servicios Actuales" |
| 14 | Carta compromiso en donde se especifique que proporcionará e implementar las herramientas de monitoreo necesarias a traves del SISTEMA DE GESTIÓN solicitado, que permitan conocer el estado operativo del equipo que integra la solución, la gestión del servicio deberá ser de forma pro-activa a los incidentes que se puedan presentar. | Ver Carpeta "Documentación Propuesta Técnica", Pestaña "Herramientas de Monitoreo" |
| 15 | Plan de retorno en caso de contingencia al momento de la migración y/o implementación. | Ver Carpeta "Documentación Propuesta Técnica", Pestaña "Plan de Retorno" |
| 16 | Carta compromiso en donde se especifique que:<br>✓ Asumirá todos los gastos referidos al traslado, aseguramiento, instalación y puesta en operación del equipo ofertado.<br>✓ Proporcionará los herrajes para los dispositivos centrales que se requiere para su instalación en racks.<br>✓ En caso de reubicación de equipo objeto de esta licitación atendiendo las necesidades de TELECOMM se realizará sin que represente algún costo para TELECOMM | Ver Carpeta "Documentación Propuesta Técnica", Pestaña "Carta Gastos" |

000046

| No. | Requisitos Técnicos | Referecia |
|---|---|---|
| | ✓ Atenderá las solicitudes de activación de equipo para la apertura de nuevas oficinas telegráficas durante la vigencia del contrato. | |
| 17 | Carta de confidencialidad con TELECOMM, que proteja el sistema de seguridad que opera en la RTI contra cualquier divulgación de información del sistema, alcanzando la responsabilidad a sus empleados y personal de terceros que participen en este arrendamiento. | Ver Carpeta "Documentación Propuesta Técnica", Pestaña "Carta Confidencialdad Propuesta Técnica" |
| 18 | Procedimiento y escalación para la atención de fallas que incluya la lista de teléfonos para levantar reportes así como una lista con los datos (nombre, puesto, teléfono oficina, teléfono móvil, correo electrónico, tiempo establecido para pasar a los niveles de soporte del personal para el escalamiento de fallas el horario de atención será de 7 x 24 x365. | Ver Carpeta "Documentación Propuesta Técnica", Pestaña "Procedimiento de Escalación" |
| 19 | Carta donde proporcione los nombres del Ejecutivo de Cuenta y del Proyect Manager para la atención, seguimiento y solución de los aspectos técnicos y administrativos tales como cumplimiento al contrato y aclaración de facturas; así como para atender las reuniones de supervisión que se convoquen por parte de Telecomm. | Ver Carpeta "Documentación Propuesta Técnica", Pestaña "Ejecutivo de Cuenta y Project Manager" |

## 14. PRUEBA DE CONCEPTO

A fin de acreditar que la proposición **"GRUPO TECNO"** considera la ejecución de la "Prueba para acreditar la capacidad del licitante para firewalls centrales "ACT1" y remotos "AAT5" descrita en el ANEXO "C" de las bases de la presente licitación, con la cual demostrará a la convocante que cuenta con las capacidades técnicas y que la solución ofertada por **"GRUPO TECNO"** en la presente propuesta técnica es capaz de integrarse al esquema actual de TELECOMM.

Los equipos que serán utilizados para la ejecución del protocolo de pruebas se describen en el Anexo "C". y **"GRUPO TECNO"** entiende que las pruebas antes mencionadas forman parte de la evaluación técnica de los licitantes y queda atento a la indicación de la fecha para la realización de las mismas en el acto de presentación de proposiciones.

## 15. DOCUMENTOS DE PRESENTACIÓN OBLIGATORIA QUE AFECTAN LA SOLVENCIA DE LAS PROPOSICIONES

"GRUPO TECNO" tiene por entendido que al igual que todos los licitantes, deberá cumplir con los siguientes requisitos de forma obligatoria toda vez que afectan la solvencia de la proposición.

- ✓ "GRUPO TECNO" cumplirá con los requerimientos solicitados por TELECOMM, en la "Prueba para acreditar la capacidad del licitante para firewalls centrales "ACT1" y remotos "AAT6" - ANEXO "C" con la cual se corroborará que el licitante tenga las capacidades técnicas y que la solución propuesta sea capaz de integrarse al esquema actual de TELECOMM. Los equipos a presentar y el protocolo de pruebas se describen en el Anexo

"C". Las pruebas forman parte de la evaluación técnica de los licitantes y el calendario se formulará de acuerdo a la cantidad de licitantes que hayan presentado proposiciones y este se dará a conocer en el acto de presentación de proposiciones.

- ✓ La información y documentación que TELECOMM entregue a **"GRUPO TECNO"** se hace bajo términos de confidencialidad y de reserva, por lo que no podrá divulgar o aprovechar para beneficio o interés propio o de terceros los conocimientos e información propiedad de TELECOMM. Una vez terminada la vigencia del contrato respectivo o si por algún motivo se cancelara el arrendamiento contratado, **"GRUPO TECNO"** está obligado a devolver toda la información que se le hubiese proporcionado, prevaleciendo la titularidad de TELECOMM.
- ✓ **"GRUPO TECNO"** se compromete a firmar una carta de confidencialidad con TELECOMM, que proteja el sistema de seguridad que opera en la RTI contra cualquier divulgación de información del sistema, alcanzando la responsabilidad a sus empleados y personal de terceros que participen en este arrendamiento.

**"GRUPO TECNO"** pone a disposición de TELECOMM el documento de pruebas realizadas que avalan la capacidad de efectividad del equipo FIREWALL ofertado, dichos documentos de referencia son emitidos por algún tercero (NSS Labs, Gartner, Forrester, Telcordia, etc.) Sobre su efectividad mencionada en las hojas técnicas. Ver Carpeta "Documentación Propuesta Técnica", Pestaña "Capacidad de Efectividad", don de se encuentran los documentos:

- ✓ Magic-Quadrant-for-Enterprise-Network-Firewalls
- ✓ Firewall-Comparative-Analysis-Edition-Security-Technical-Brief
- ✓ Next-Generation-Firewall-Comparative-Analysis-SVM

De la misma Forma **"GRUPO TECNO"** presenta las siguientes certificaciones del equipo ofertado:

- o Certificación ICSA Labs de Firewall
- o Certificación ICSA Labs de IPSec
- o Certificación ICSA Labs de IPS

Ver Carpeta "Documentación Propuesta Técnica", Pestaña "Certificaciones del Equipo", donde se encuentran los documentos:

- ✓ FORTINET_FIEWAL_4.2_REPORT
- ✓ FORTINET_iPSec_2.2_Report
- ✓ Fortinet_FG_NIPS_REPORT

MÉXICO, D.F., 8 DE OCTUBRE DE 2015
BAJO PROTESTA DE DECIR VERDAD,
GRUPO DE TECNOLOGÍA CIBERNÉTICA, S.A. DE C.V.

JENNIFER MURILLO DOMINGUEZ
REPRESENTANTE LEGAL

000048

LICITACIÓN PÚBLICA MIXTA NACIONAL NÚMERO **No. LA-009KCZ002-N49-2015** PARA EL ARRENDAMIENTO DEL "EQUIPO FIREWALL/VPN Y CONSOLA DE ADMINISTRACIÓN PARA EXPANSIÓN DE OFICINAS TELEGRÁFICAS DE LA RED TELDAT."

16487

GRUPOTECNO

# Anexo FortiGate-1500D

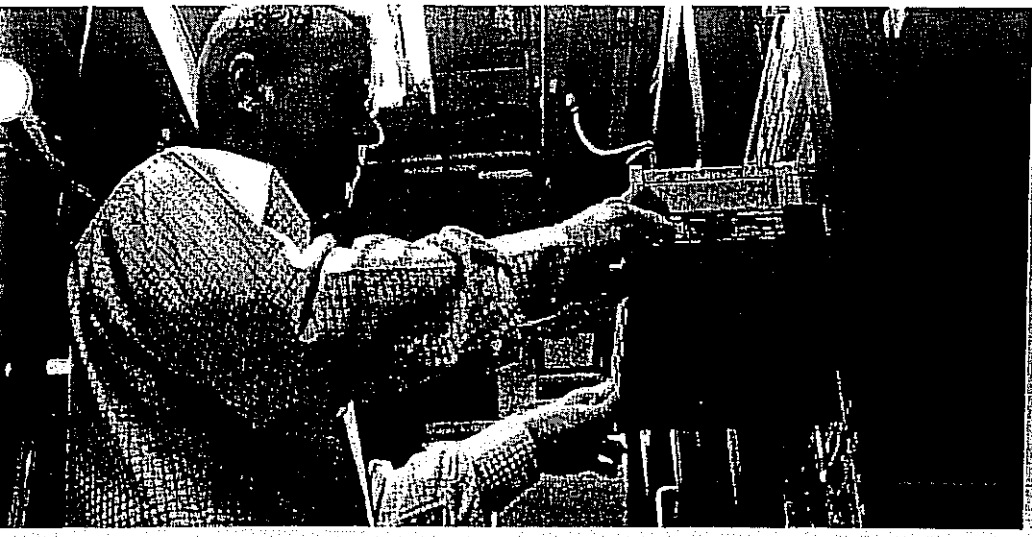
FORTINET

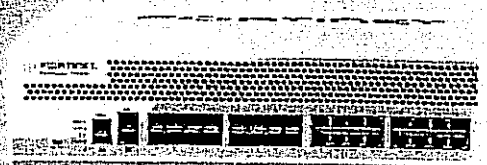
DATA SHEET

16433

FortiGate® 1500D

High Performance Next Generation/ Edge Firewall for the Enterprise





# FortiGate 1500D

FortiGate 1500D and 1500D-DC

Every day you're on the lookout for sophisticated attacks designed to penetrate your organization and steal valuable information. At the same time, you need to increase network speeds and capacities to accommodate the proliferation of consumer-grade applications and devices. To adequately defend against threats across such a broad range of applications and devices — without slowing down your network — you need a high performance next generation/edge firewall (NGFW) appliance for deep inspection, visibility and control.

## Breakthrough Performance

The FortiGate 1500D and 1500D-DC high performance next generation/edge firewalls deliver best-in-class performance with an exceptional 80 Gbps of firewall and 11 Gbps of next generation threat protection. Custom hardware, including the latest FortiASIC™ NP6 processors, and the consolidated security features of the FortiOS™ 5 network security platform make the difference in enabling protection of your applications and network without affecting availability or performance.

## Features & Benefits

- Industry-leading 5x next generation firewall performance and 10x data center firewall
- NSS Labs Recommended NGFW and NGIPS delivers top-rated protection
- Integrated high port density delivers maximum flexibility and scalability
- Intuitive management interface enables broad and deep visibility and control
- Application control plus identity and device-based policy enforcement provides more granular protection

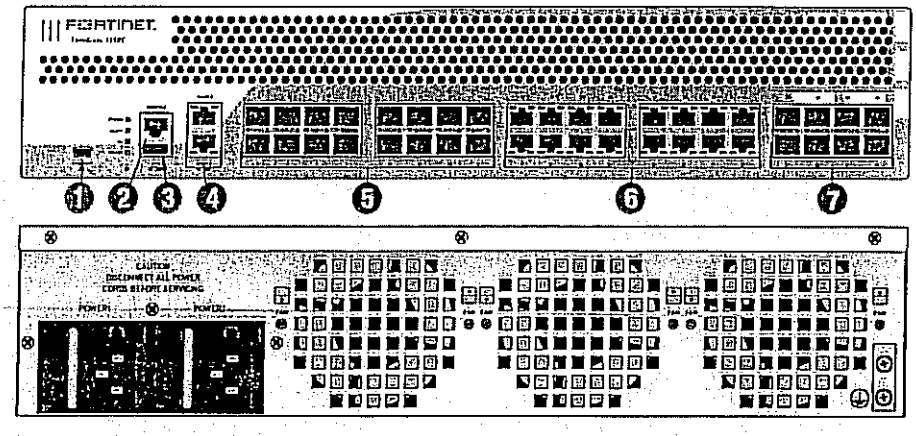
## Highlights

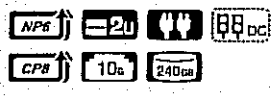
| Firewall Performance | IPS Performance | Interfaces |
|---|---|---|
| 80 Gbps | 11 Gbps | Multiple 10 GE SFP+, GE SFP and GE RJ45 |

16489

# HARDWARE

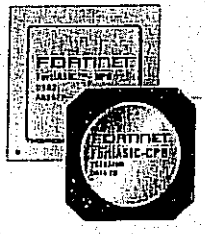
## FortiGate 1500D and 1500D-DC




### Interfaces

1. USB Management Port
2. Console Port
3. USB Port
4. 2x GE RJ45 Management Ports
5. 16x GE SFP Slots
6. 16x GE RJ45 Ports
7. 8x 10 GE SFP+ Slots




### Powered by FortiASICs

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

### Network Processor

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

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

### Content Processor

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

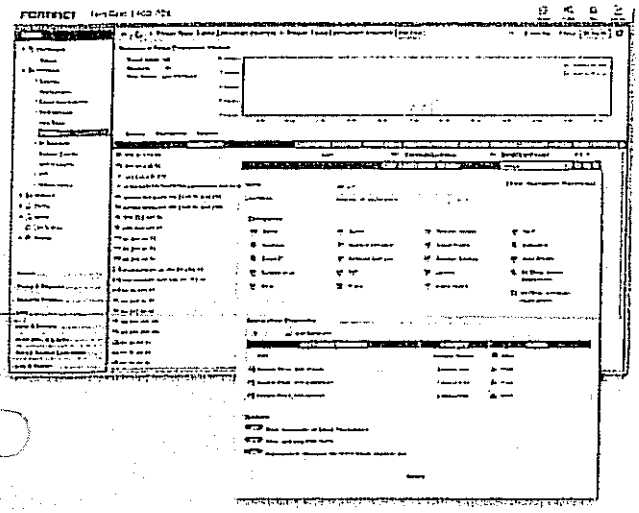
- Signature-based content inspection acceleration
- Encryption and decryption offloading

### 10 GE Connectivity

High speed connectivity is essential for network security segmentation at the core of data networks. The FortiGate 1500D and FG-1500D-DC provide high 10 GE port densities, simplifying network designs without relying on additional devices to bridge desired connectivity.

16490

# SOFTWARE



FortiOS Managment UI — FortiView and Application Control Panel

## FortiOS

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

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

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

# SERVICES

## FortiGuard™ Security Services

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

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

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

## FortiCare™ Support Services

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

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

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

16491

# SPECIFICATIONS

| FortiGate 1500D / 1500D-DC | |
|---|---|
| **Hardware Specifications** | |
| Hardware Accelerated 10 GE SFP+ Slots | 8 |
| Hardware Accelerated GE SFP Slots | 16 |
| Hardware Accelerated GE RJ45 Ports | 16 |
| GE RJ45 Management / HA Ports | 2 |
| USB Ports (Client / Server) | 1 / 1 |
| Console Port | 1 |
| Onboard Storage | 240 GB |
| Included Transceivers | 2x SFP+ (SR 10GE) |
| **System Performance** | |
| IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP) | 80 / 80 / 55 Gbps |
| IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP) | 80 / 80 / 55 Gbps |
| Firewall Latency (64 byte, UDP) | 3 µs |
| Firewall Throughput (Packet per Second) | 82.5 Mpps |
| Concurrent Sessions (TCP) | 12 Mi |
| New Sessions/Second (TCP) | 250,000 |
| Firewall Policies | 100,000 |
| IPsec VPN Throughput (512 byte) | 50 Gbps |
| Gateway-to-Gateway IPsec VPN Tunnels | 20,000 |
| Client-to-Gateway IPsec VPN Tunnels | 50,000 |
| SSL-VPN Throughput | 4 Gbps |
| Concurrent SSL-VPN Users (Recommended Maximum) | 10,000 |
| IPS Throughput | 11 Gbps |
| Antivirus Throughput | 4.3 Gbps |
| CAPWAP Clear-text Throughput (HTTP) | 12.30 Gbps |
| Virtual Domains (Default / Maximum) | 10 / 250 |
| Maximum Number of FortiAPs (Total / Tunnel) | 4,096 / 1,024 |
| Maximum Number of FortiTokens | 5,000 |
| Maximum Number of Registered Endpoints | 8,000 |
| High Availability Configurations | Active-Active, Active-Passive, Clustering |

| FortiGate 1500D / 1500D-DC | |
|---|---|
| **Dimensions** | |
| Height x Width x Length (inches) | 3.5 x 17.24 x 21.81 |
| Height x Width x Length (mm) | 89 x 438 x 554 |
| Weight | 32.50 lbs (14.70 kg) |
| Form Factor | Rack Mount, 2 RU |
| **Power** | |
| AC Power Supply | 100–240V AC, 47–63 Hz |
| DC Power Supply (FG-1500D-DC) | 40.5–57V DC |
| Maximum Current | 110V / 8A, 220V / 4A |
| Power Consumption (Average / Maximum) | 338 / 406 W |
| Heat Dissipation | 1,385 BTU/h |
| Redundant Power Supplies | Yes, Hot swappable |
| **Environment** | |
| Operating Temperature | 32–104°F (0–40°C) |
| Storage Temperature | -31–158°F (-35–70°C) |
| Humidity | 15–90% non-condensing |
| Operating Altitude | Up to 7,400 ft (2,250 m) |
| **Compliance** | |
| | FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB |
| **Certifications** | |
| | ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN |

Note: All performance values are "up to" and vary depending on system configuration. Antivirus performance is measured using 44 Kbyte HTTP files. IPS performance is measured using 1 Mbyte HTTP files. IPsec VPN performance is based on 512 byte UDP packets using AES-256+SHA1. Antivirus Throughput is measured in proxy mode.

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

# ORDER INFORMATION

| Product | SKU | Description |
|---|---|---|
| FortiGate 1500D | FG-1500D | 8x 10 GE SFP+ slots, 16x GE SFP slots, 16x GE RJ45 ports (including 16x ports, 2x management/HA ports), FortiASIC NP6 and CP8 hardware accelerated, 240 GB SSD onboard storage, dual AC power supplies. |
| FortiGate 1500D-DC | FG-1500D-DC | 8x 10 GE SFP+ slots, 16x GE SFP slots, 16x GE RJ45 ports (including 16x ports, 2x management/HA ports), FortiASIC NP6 and CP8 hardware accelerated, 240 GB SSD onboard storage, dual DC power supplies. |
| **Optional Accessories** | | |
| 1 GE SFP LX transceiver module | FG-TRAN-LX | 1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots. |
| 1 GE SFP RJ45 transceiver module | FG-TRAN-GC | 1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots. |
| 1 GE SFP SX transceiver module | FG-TRAN-SX | 1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots. |
| 10 GE SFP+ transceiver module, short range | FG-TRAN-SFP+SR | 10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots. |
| 10 GE SFP+ transceiver module, long range | FG-TRAN-SFP+LR | 10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots. |
| 10 GE SFP+ active direct attach cable, 10m / 32.8 ft | SP-CABLE-ADASFP+ | 10 GE SFP+ active direct attach cable, 10m / 32.8 ft for all systems with SFP+ and SFP/SFP+ slots. |
| Rack mount sliding rails | SP-FG3040B-RAIL | Rack mount sliding rails for FG-1000C/-DC, FG-1500D, FG-3040B/-DC, FG-3140B/-DC, FG-3240C/-DC, 3700D and 3950B/-DC |
| AC power supply | SP-FG1240B-PS | AC power supply for FG-1240B, FG-1500D, FG-3040B and FG-3140B |
| DC power supply | SP-FG1500D-DC-PS | DC power supply for FG-1500D-DC |

FORTINET

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

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

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

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

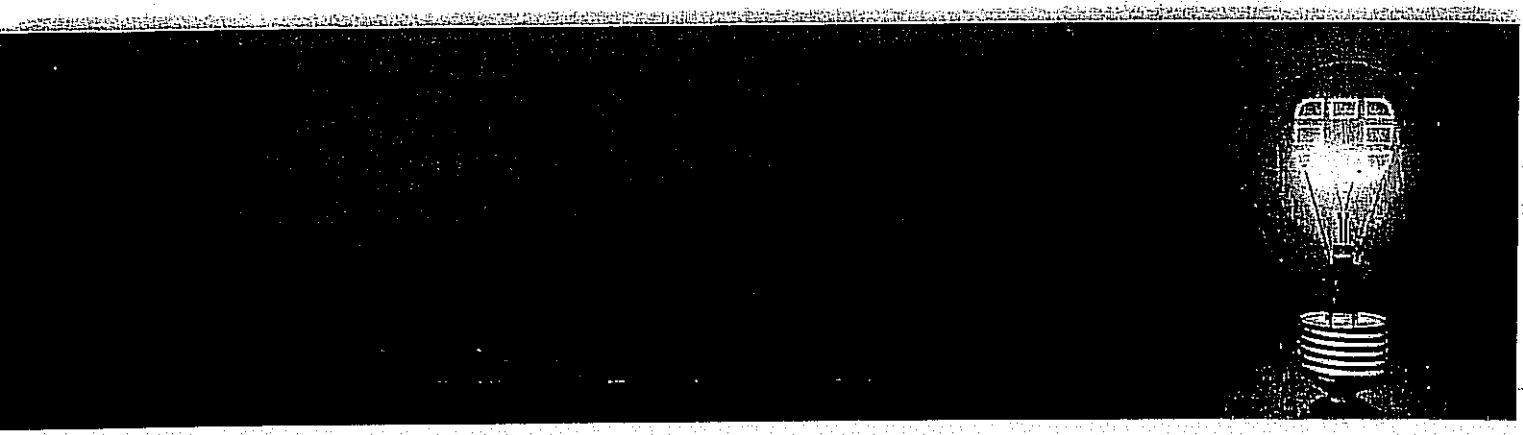
LICITACIÓN PÚBLICA MIXTA NACIONAL NÚMERO **No. LA-009KCZ002-N49-2015** PARA EL ARRENDAMIENTO DEL "EQUIPO FIREWALL/VPN Y CONSOLA DE ADMINISTRACIÓN PARA EXPANSIÓN DE OFICINAS TELEGRÁFICAS DE LA RED TELDAT."

GRUPOTECNO

# Anexo NGFW_Solution_Brief

FORTINET

Solution Brief



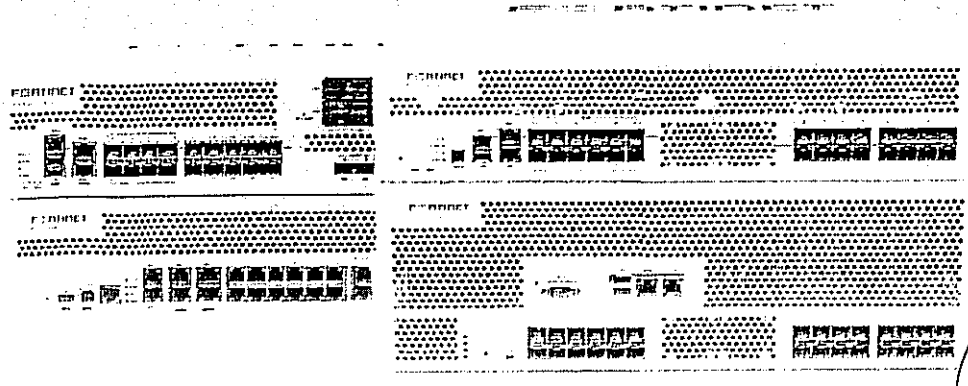
# The World's Most Intelligent and Powerful NGFW

## Introduction

The continuous evolution of your enterprise network requires an advanced firewall solution that is capable of delivering a range of attributes: exceptional performance and scalability, protection against sophisticated threats, future-ready functionality that protects your investment, and consolidation and integration of technologies, simplified policy creation and enforcement.

In addition, as the behavior of the applications, users, and devices accessing your network changes over time, you need a solution that can continue to deliver unmatched visibility and control. Perhaps most importantly, you also need a focused set of security technologies that can help you defeat today's targeted attacks that intend to compromise your network.

Fortinet FortiGate appliances, the most intelligent and powerful next-generation firewalls, deliver the protection and performance your enterprise network needs.



## FortiGate NGFW Benefits

- **Eliminates blind spots:** Consolidated security architecture closes gaps in policy enforcement caused by stand-alone devices and consoles, improves protection, increases performance, and decreases latency.
- **Innovative protection from advanced threats:** Client reputation and cloud-based antimalware deliver additional layers of protection to detect and block compromised systems and malicious content
- **Reduced complexity and decreased costs:** "Single Pane of Glass Management" manages all security functions through one console, enabling existing IT resources to become more effective.
- **Simplified Licensing:** Comprehensive, unlimited user licensing eliminates need to purchase additional modules or count users, increasing ease of deployment and maintenance

LICITACIÓN PÚBLICA MIXTA NACIONAL NÚMERO **No. LA-009KCZ002-N49-2015** PARA EL ARRENDAMIENTO DEL "EQUIPO FIREWALL/VPN Y CONSOLA DE ADMINISTRACIÓN PARA EXPANSIÓN DE OFICINAS TELEGRÁFICAS DE LA RED TELDAT."

GRUPOTECNO

# Anexo FortiOS Handbook Firewall for FortiOS 5.0

16495

FORTINET®

# FortiOS Handbook
## Firewall for FortiOS 5.0

This section is for showing you where you need to input your information and let you know what format the interface expects to get that information

Building firewall objects and policies is similar to a cookbook in that it will refer to a number of common tasks that you will likely perform to get the full functionality out of your FortiGate firewall. Because of the way that firewall are designed, performing many of the tasks requires that firewall components be set up in a number of different sections of the interface and be configured to work together to achieve the desired result. This section will bring those components all together as a straight forward series of instructions.

Multicast forwarding is a reference guide including the concepts and examples that are involved in the use of multicast addressing and policy forwarding as it is used in the FortiGate firewall.

## FortiGate Firewall Components

The FortiGate firewall is made up of a number of different components that are used to build an impressive list of features that have flexibility of scope and granularity of control that provide protection that is beyond that provided by the basic firewalls of the past.

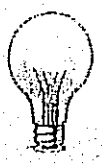
Some of the components that FortiOS uses to build features are:

- Interfaces
- VLANs
- Soft Switches
- Zones
- Predefined Addresses
- IP address based
- FODN based
- Geography based
- Access Schedules
- Authentication
- Local User based
- Authentication Server based (Active Directory, Radius, LDAP)
- Device Based
- Configureable Services
- IPv4 and IPv6 protocol support

The features of FortiOS include but are not limited to:

- Unified Threat Management (UTM)
- Predefined firewall addresses (this includes IPv4 and IPv6, IP pools, wildcard addresses and netmasks, and geography-based addresses)
- Monitoring traffic
- Traffic shaping and per-IP traffic shaping (advanced)
- Firewall schedules
- Services (such as AOL, DHCP and FTP)
- Logging traffic
- Quality of Service (QoS)
- Identity-based policies
- Endpoint security

the rules set for new connections. Predetermined rules are used in the same way as a stateless firewall but they can now work with the additional criteria of the state of the connection to the firewall.



Best PracticesTip for improving performance:

Blocking the packets in a denied session can take more cpu processing resources than passing the traffic through. By putting denied sessions in the session table, they can be kept track of in the same way that allowed session are so that the FortiGate unit does not have to redetermine whether or not to deny all of the packets of a session individually. If the session is denied all packets of that session are also denied.

In order to configure this you will need to use 2 CLI commands

```
config system setting
    set ses-denied-traffic enable
    set block-session-timer <integer 1 - 300> (this determines in seconds
      how long, in seconds, the session is kept in the table)
end
```

## Application Layer Firewalls

Application layer filtering is yet another approach and as the name implies it works primarily on the Application Layer of the OSI Model.

Application Layer Firewalls actually, for lack of a better term, understand certain applications and protocols. Examples would be FTP, DNS and HTTP. This form of filtration is able to check to see if the packets are actually behaving incorrectly or if the packets have been incorrectly formatted for the protocol that is indicated. This process also allows for the use of deep packet inspection and the sharing of functionality with Intrusion Prevention Systems (IPS).

Application-layer firewalls work on the application level of the TCP/IP stack (i.e., all browser traffic, or all telnet or ftp traffic), and may intercept all packets traveling to or from an application. They block other packets (usually dropping them without acknowledgment to the sender). Application firewalls work much like a packet filter but application filters apply filtering rules (allow/block) on a per process basis instead of filtering connections on a per port basis.

On inspecting all packets for improper content, firewalls can restrict or prevent outright the spread of networked computer worms and trojans. The additional inspection criteria can add extra latency to the forwarding of packets to their destination.

## Proxy Servers

A proxy server is an appliance or application that acts as an intermediary for communicating between computers. A computer has a request for information. The packets are sent to the designated resource but before they can get there they are blocked by the proxy server saying that it will take the request and pass it on. The Proxy Server processes the request and if it is valid it passes onto the designated computer. The designated computer gets the packet and processes the request, sending the answer back to the proxy server. The proxy server sends the information back to the originating computer. It's all a little like a situation with two people who refuse to talk directly with each other using someone else to take messages back and forth.

## IPv6 in FortiOS

From an administrative point of view IPv6 works almost the same as IPv4 in FortiOS. The primary difference is the use IPv6 format for addresses. There is also no need for NAT if the FortiGate firewall is the interface between IPv6 networks. If the subnets attached to the FortiGate firewall are IPv6 and IPv4 NAT can be configured between the 2 different formats. This will involve either configuring a dual stack routing or IPv4 tunnelling configuration. The reason for this is simple. NAT was developed primarily for the purpose of extending the number of usable IPv4 addresses. IPv6's addressing allows for enough available addresses so the NAT is no longer necessary.

When configuring IPv6 in FortiOS, you can create a dual stack route or IPv4-IPv6 tunnel. A dual stack routing configuration implements dual IP layers, supporting both IPv4 and IPv6, in both hosts and routers. An IPv4-IPv6 tunnel is essentially similar, creating a tunnel that encapsulates IPv6 packets within IPv4 headers that carry these IPv6 packets over IPv4 tunnels. The FortiGate unit can also be easily integrated into an IPv6 network. Connecting the FortiGate unit to an IPv6 network is exactly the same as connecting it to an IPv4 network, the only difference is that you are using IPv6 addresses.

By default the IPv6 settings are not displayed in the Web-based Manager. It is just a matter of enabling the display of these feature to use them through the web interface. To enable them just go to System > Admin > Settings and select IPv6 Support on GUI. Once enabled, you will be able to use IPv6 addresses as well as the IPv4 addressing for the following FortiGate firewall features:

- Static routing
- Policy Routing
- Packet and network sniffing
- Dynamic routing (RIPv6, BGP4+, and OSPFv3)
- IPSec VPN
- DNS
- DHCP
- SSL-VPN
- Network interface addressing
- UTM protection
- Routing access lists and prefix lists
- NAT/Route and Transparent mode
- NAT 64 and NAT 66
- IPv6 tunnel over IPv4 and IPv4 tunnel over IPv6
- Logging and reporting
- Security policies
- SNMP
- Authentication
- Virtual IPs and groups
- IPv6 over SCTP
- IPv6-specific troubleshooting, such as ping6

## Dual Stack routing configuration

Dual stack routing implements dual IP layers in hosts and routers, supporting both IPv6 and IPv4. A dual stack architecture supports both IPv4 and IPv6 traffic and routes the appropriate

| | |
|---|---|
| Host to Host | Dual Stack capable hosts that are interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves. In this case, the tunnel spans the entire path taken by the IPv6 packets. |
| Network Device to Host | Dual Stack capable network devices can tunnel IPv6 packets to their final destination IPv6 or IPv4 host. This tunnel spans only the last segment of the path taken by the IPv6 packets. |

Regardless of whether the tunnel starts at a host or a network device, the node that does the encapsulation needs to maintain soft state information, such as the maximum transmission unit (MTU), about each tunnel in order to process the IPv6 packets.

### Tunnelling IPv6 through IPSec VPN

A variation on the tunnelling IPv6 through IPv4 is using an IPSec VPN tunnel between to FortiGate devices. FortiOS supports IPv6 over IPSec. In this sort of scenario, 2 networks using IPv6 behind FortiGate units are separated by the Internet, which uses IPv4. An IPSec VPN tunnel is created between the 2 FortiGate units and a tunnel is created over the IPv4 based Internet but the traffic in the tunnel is IPv6. This has the additional advantage of make the traffic secure as well.

## NAT

### What is NAT?

NAT or Network Address Translation is the process that enables a single device such as a router or firewall to act as an agent between the Internet or Public Network and a local or private network. This "agent", in real time, translates the source IP address of a device on one network interface, usually the Internal, to a different IP address as it leaves another interface, usually the interface connected to the ISP and the Internet. This enables a single public address to represent a significantly larger number of private addresses.

### The Origins of NAT

In order to understand NAT it helps to know why it was created. At one time, every computer that was part of a network had to have it's own addresses so that the other computers could talk to it. There were a few protocols in use at the time, some of which were only for use on a single network, but of those that were routable, the one that had become the standard for the Internet was IP (Internet Protocol) version 4.

When IP version 4 addressing was created nobody had any idea how many addresses would be needed. The total address range was based on the concept of 2 to the 32nd power, which works out to be 4 294 967 296 potential addresses. Once you eliminate some of those for reserved addresses, broadcast addresses, network addresses, multicasting, etc., you end up with a workable scope of about 3.2 million addressees. This was thought to be more than enough at the time. The designers were not expecting the explosion of personal computing, the World Wide Web or smart phones. As of the beginning of 2012, some estimate the number of computers in the world in the neighborhood of 1 billion, and most of those computer users are going to want to be on the Internet or Search the World Wide Web. In short, we ran out of addresses.

This problem of an address shortage was realized before we actually ran out, and in the mid 1990s 2 technical papers called RFCs numbered 1631 (http://www.ietf.org/rfc/rfc1631.txt) and 1918 (http://tools.ietf.org/html/rfc1918), proposed components of a method that would be used

### Overloading

This is a form of Dynamic NAT that maps multiple private IP address to a single Public IP address but differentiates them by using a different port assignment. This is probably the most widely used version of NAT. This is also referred to as PAT (Port Address Translation) or Masquerading.

An example would be if you had a single IP address assigned to you by your ISP but had 50 or 60 computers on your local network.

Say the internal address of the interface connected to the ISP was 256.16.32.65 (again an impossible address) with 256.16.32.64 being the remote gateway. If you are using this form of NAT any time one of your computers accesses the Internet it will be seen from the Internet as 256.16.32.65. If you wish to test this go to 2 different computers and verify that they each have a different private IP address then go to a site that tells you your IP address such as www.ipchicken.com. You will see that the site gives the same result of 256.16.32.65, if it existed, as the public address for both computers.

As mentioned before this is sometimes called Port Address Translation because network device uses TCP ports to determine which internal IP address is associated with each session through the network device. For example, if you have a network with internal addresses ranging from 192.168.1.1 to 192.168.1.255 and you have 5 computers all trying to connect to a web site which is normally listening on port 80 all of them will appear to the remote web site to have the IP address of 256.16.32.65 but they will each have a different sending TCP port, with the port numbers being somewhere between 1 and 65 535, although the port numbers between 1 to 1024 are usually reserved or already in use. So it could be something like the following:

```
192.168.1.10    256.16.32.65:   port 486
192.168.1.23    256.16.32.65:   port 2409
192.168.1.56    256.16.32.65:   port 53763
192.168.1.109   256.16.32.65:   port 5548
192.168.1.201   256.16.32.65:   port 4396
```

And the remote web server would send the responding traffic back based on those port numbers so the network device would be able to sort through the incoming traffic and pass it on to the correct computer.

### Overlapping

Because everybody is using the relative same small selection of Private IP addresses it is inevitable that there will be two networks that share the same network range that will need to talk with each other. This happens most often over Virtual Private Networks or when one organization ends up merging with another. This is a case where a private IP address may be translated into a different private IP address so there are no issues with conflict of addresses or confusion in terms of routing.

An example of this would be when you have a Main office that is using an IP range of 172.16.0.1 to 172.20.255.255 connecting through a VPN to a recently acquired branch office that is already running with an IP range of 172.17.1.1 to 172.17.255.255. Both of these ranges are perfectly valid but because the Branch office range is included in the Main Office range any time the system from the Main office try to connect to an address in the Branch Office the routing the system will not send the packet to the default gateway because according to the routing table the address is in its own subnet.

The plan here would be to NAT in both directions so that traffic from neither side of the firewall would be in conflict and they would be able to route the traffic. Everything coming from the Branch Office could be assigned an address in the 192.168.1.1 to 192.168.1.255 range and everything from the Main office going to the Branch Office could be assigned to an address in the 192.168.10.1 to 192.168.10.255 range.

to be the maintaining of the existing address scheme of the internal network despite changes outside of it. Imagine that you have an internal network of 2000 IP addresses and one day the company changes its ISP and thus the addresses assigned to it. Even if most of the addressing is handled by DHCP, changing the address scheme is going to have an impact on operations.

Addressing stability can be achieved by:

- Keeping the same provider - this would depend on the reason for the change. If the cost of this provider has become too expensive this is unlikely. If the ISP is out of business it becomes impossible.
- Transfer the addresses from the old provider to the new one - There is little motivation for an ISP to do you a favor for not doing business with them.
- Get your own autonomous system number - this can be too expensive for smaller organizations.
- NAT - this is the only one on the list that is in the control of IT.

There are differences between NAT66 and IPv4 NAT. Because there is no shortage of addresses most organizations will be given a /48 network that can be translated into another /48 network. This allows for a one to one translation, no need for port forwarding. This is a good thing because port forwarding is more complicated in IPv6. In fact, NAT66 will actually just be the rewriting of the prefix on the address.

Example:

If your current IPv6 address is

```
2001:db8:cafe::/48
```

you could change it to

```
2001:db8:fea7::/48
```

There is an exception to the one to one translation. NAT66 cannot translate internal networks that contain 0xffff in bits 49 through 63 - this is due to the way checksums are calculated in TCP/IP: they use the one's-complement representation of numbers which assigns the value zero to both 0x0000 and 0xffff.

## How Packets are handled by FortiOS

To give you idea of what happens to a packet as it makes its way through the FortiGate unit here is a brief overview. This particular trip of the packet is starting on the Internet side of the FortiGate firewall and ends with the packet exiting to the Internal network. An outbound trip would be similar. At any point in the path if the packet is going through what would be considered a filtering process and if fails the filter check the packet is dropped and does not continue any further down the path.

This information is covered in more detail in other in the Troubleshooting chapter of the FortiOS Handbook in the Life of a Packet section.

The incoming packet arrives at the external interface. This process of entering the device is referred to as ***ingress***.

Step #1 - Ingress

1. Denial of Service Sensor
2. IP integrity header checking
3. IPSec connection check
4. Destination NAT
5. Routing

Step #2 - Stateful Inspection Engine

1. Session Helpers
2. Management Traffic
3. SSL VPN
4. User Authentication
5. Traffic Shaping
6. Session Tracking
7. Policy lookup

Step #3 - UTM scanning process

1. Flow-based Inspection Engine
2. IPS
3. Application Control
4. Data Leak Prevention
5. Email Filter
6. Web Filter
7. Anti-virus
8. Proxy-based Inspection Engine
9. VoIP Inspection
10. Data Leak Prevention
11. Email Filter
12. Web Filter
13. Anti-virus
14. ICAP

Step #4 - Egress

1. IPSec
2. Source NAT
3. Routing

## FortiGate Modes

The FortiGate unit has a choice of modes that it can be used in, either NAT/Route mode or Transparent mode. The FortiGate unit is able to operate as a firewall in both modes, but some of its features are limited in Transparent mode. It is always best to choose which mode you are going to be using at the beginning of the set up. Once you start configuring the device, if you want to change the mode you are going to lose all configuration settings in the change process.

### NAT/Route Mode

NAT/Route mode is the most commonly used mode by a significant margin and is thus the default setting on the device. As the name implies the function of NAT is commonly used in this mode and is easily configured but there is no requirement to use NAT. The FortiGate unit performs network address translation before IP packets are sent to the destination network.

everyone a large number of the more commonly used services started using a standardized list of ports. For instance, though it is not required, by default, most web servers listen for HTTP requests on port 80 and by default, web browsers will send HTTP traffic to port 80. If you wish to use another port such as 8080 you would put ":8080" at the end of the URL to indicate that you want the browser to use 8080 instead of the default port.

**Example:**

Default URL for HTTP traffic when the web server is listening on the standard HTTP port:

http://fortinet.com

URL to the same address when the web server is listening for HTTP traffic on port 8080

http://fortinet.com:8080

Services represent typical traffic types and application packets that pass through the FortiGate unit. Firewall services define one or more protocols and port numbers associated with each service. Security policies use service definitions to match session types. You can organize related services into service groups to simplify your security policy list.

Many well-known traffic types have been predefined on the FortiGate unit. If there is a service that does not appear on the list you can create a service or edit an existing one. You need to know the ports, IP addresses or protocols of that particular service or application uses, to create a service.

Best Practices

While you can edit a predefined service it is best to leave those ones alone and create a new service and name it something similar such as the same service name with a descriptive identifier appended.

Based on the previous example, instead of the name "HTTP" you could name the service "HTTP8080" or use the application that is using that port, "HTTP-Application".

## Categories

In order to make sorting through the services easier there is a field to categorize the services. The services can be sorted into the following groups:

- Uncategorized
- General
- Web Access
- File Access
- Email
- Network Services
- Authentication
- Remote Access
- Tunnelling
- VoIP, Messaging and Other Applications

## Creating an address for the subnet

In the same way that the VIP was created to identify and direct incoming traffic an address should be created to identify the addresses of computer that will be in the Conference room. This included computers on the LAN as well as the Teleconferencing equipment.

Go to *Firewall Objects -> Address -> Addresses*

*Create New*

Fill out the fields with the following information:

| | |
|---|---|
| **Category** | Address |
| **Name** | Port7_subnet |
| **Type** | Subnet |
| **Subnet/IP Range** | 192.168.7.0/255.255.255.0 |
| **Interface** | port7 |
| **Show in address list** | checked |

## Configuring the services

### Services already created:

The following are standard services that have already been created by default:

| | |
|---|---|
| **HTTP** | TCP 80 |
| **SNMP** | TCP 161-162/UDP 161-162 |
| **LDAP** | TCP 389 |
| **HTTPS** | TCP 443 |
| **SYSLOG** | UDP 514 |

### Existing Services to be edited:

There are a few services that have already been created for you, but they need to be expanded to accommodate the list of protocols listed for this scenario.

**The default h323 contains:**

- TCP 1503
- UDP 1719
- TCP 1720

**We need to add:**

- TCP1719

**The default SIP contains:**

Here is an example of an interface policy,

```
config firewall interface-policy
 edit 1
     set status enable
     set interface "port14"
     set srcaddr "all"
     set dstaddr "all"
     set service "ALL"
     set application-list-status disable
     set ips-sensor-status enable
     set ips-sensor "default"
     set av-profile-status disable
     set webfilter-profile-status disable
     set spamfilter-profile-status disable
     set dlp-sensor-status disable
     set label "Port 14 Interface Policy"
  next
end
```

## DoS Protection

Denial of Service (DoS) policies are primarily used to apply DoS anomaly checks to network traffic based on the FortiGate interface it is entering as well as the source and destination addresses. DoS checks are a traffic anomaly detection feature to identify network traffic that does not fit known or common traffic patterns and behavior. A common example of anomalous traffic is the denial of service attack. A denial of service occurs when an attacking system starts an abnormally large number of sessions with a target system. The large number of sessions slows down or disables the target system, so that legitimate users can no longer use it.

DoS policies are similar to firewall policies except that instead of defining the way traffic is allowed to flow, they keep track of certain traffic patterns and attributes and will stop traffic displaying those attributes. Further, DoS policies affect only incoming traffic on a single interface. You can further limit a DoS policy by source address, destination address, and service.

DoS configurations have been changed a couple of times in the past. In FortiOS 4.0, DoS protection is moved to the interface policy, so when it is enabled, it is the first thing checked when a packet enters FortiGate. Because of this early detection, DoS policies are a very efficient defence that uses few resources. Denial of service attacks, for example, are detected and its packets dropped before requiring security policy look-ups, antivirus scans, and other protective but resource-intensive operations.

A DoS policy examines network traffic arriving at an interface for anomalous patterns usually indicating an attack. This does not mean that all anomalies experience by the firewall are the result of an intentional attack.

Because an improperly configured DoS anomaly check can interfere with network traffic, no DoS checks are preconfigured on a factory default FortiGate unit. You must create your own

To enable One-Arm IDS, the user should first enable sniff-mode on the interface.

```
config system interface
  edit port2
    set ips-sniffer-mode enable
  next
end
```

Once sniff-mode is turned on, both incoming and outgoing packets will be dropped after IPS inspections. The port can be connected to a hub or a switch's SPAN port. Any packet picked up by the interface will still follow the interface policy so different IPS and DoS anomaly checks can be applied.

## IPv6 IPS

IPv6 IPS signature scan can be enabled by interface policy. The user can create an normal IPS sensor and assign it to the IPv6 interface policy.

```
config firewall interface-policy6
    edit 1
      set interface "port1"
      set srcaddr6 "all"
      set dstaddr6 "all"
      set service6 "ANY"
      set ips-sensor-status enable
      set ips-sensor "all_default"
    next
end
```

## Traffic Destined to the FortiGate unit

IPS enabled in firewall policies can only inspect the traffic pass through FortiGate unit, not the traffic destined to FortiGate unit. Enabling IPS in interface-policy allows IPS to pick up any packet on the interface so it is able to inspect attacks targeting FGT.

## Dropped, Flooded, Broadcast, Multicast and L2 packets

In many evaluation or certification tests, FortiGate firewall is often required to log any packets dropped by the firewall. In most of cases, these packets are of invalid headers so firewall just drops them silently. It is natural to forward all these packets to IPS first so FortiGate firewall is able to generate logs for invalid packets.

Flooded, broadcast and multicast traffics do not reach any of services in the forwarding path. They can be inspected by the interface policy as long as they match the addresses defined. Potentially, L2 packets can also be sent to IPS for inspection through interface-policy, but it is not enabled in FortiOS 4.0.

## GUI and CLI

Now in FortiGate, there are two places that IPS can be enabled, in a firewall policy and in an interface policy. In the firewall policy implementation, IPS sensor can be configured in both CLI and GUI. When adding an IPS sensor to an interface policy it must be done through the CLI. There is no GUI input window for the "Interface Policy". There is however, a DoS Policy section in the GUI.

security and possibly succeed. FortiGate security recognizes a wide variety of evasion techniques and normalizes data traffic before inspecting it.

### Packet fragmentation

Information sent across local networks and the Internet is encapsulated in packets. There is a maximum allowable size for packets and this maximum size varies depending on network configuration and equipment limitations. If a packet arrives at a switch or gateway and it is too large, the data it carries is divided among two or more smaller packets before being forwarded. This is called fragmentation.

When fragmented packets arrive at their destination, they are reassembled and read. If the fragments do not arrive together, they must be held until all of the fragments arrive. Reassembly of a packet requires all of the fragments.

The FortiGate unit automatically reassembles fragmented packets before processing them because fragmented packets can evade security measures. Both IP packets and TCP packets are reassembled by the IPS engine before examination.

For example, you have configured the FortiGate unit to block access to the example.org web site. Any checks for example.com will fail if a fragmented packet arrives and one fragment contains `http://www.exa` while the other contains `mple.com/`. Viruses and malware can be fragmented and avoid detection in the same way. The FortiGate unit will reassemble fragmented packets before examining network data to ensure that inadvertent or deliberate packet fragmentation does not hide threats in network traffic.

### Non-standard ports

Most traffic is sent on a standard port based on the traffic type. The FortiGate unit recognizes most traffic by packet content rather than the TCP/UDP port and uses the proper IPS signatures to examine it. Protocols recognized regardless of port include DHCP, DNP3, FTP, HTTP, IMAP, MS RPC, NNTP, POP3, RSTP, SIP, SMTP, and SSL, as well as the supported IM/P2P application protocols.

In this way, the FortiGate unit will recognize HTTP traffic being sent on port 25 as HTTP rather than SMTP, for example. Because the protocol is correctly identified, the FortiGate unit will examine the traffic for any enabled HTTP signatures.

### Negotiation codes

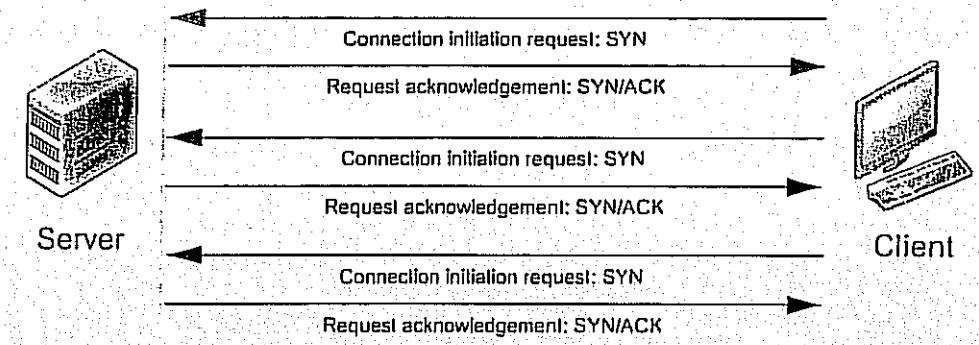
Telnet and FTP servers and clients support the use of negotiation information to allow the server to report what features it supports. This information has been used to exploit vulnerable servers. To avoid this problem, the FortiGate unit removes negotiation codes before IPS inspection.

### HTTP URL obfuscation

Attackers encode HTML links using various formats to evade detection and bypass security measures. For example, the URL www.example.com/cgi.bin could be encoded in a number of ways to avoid detection but still work properly, and be interpreted the same, in a web browser.

The FortiGate prevents the obfuscation by converting the URL to ASCII before inspection.

Figure 3: A single client launches a SYN flood attack

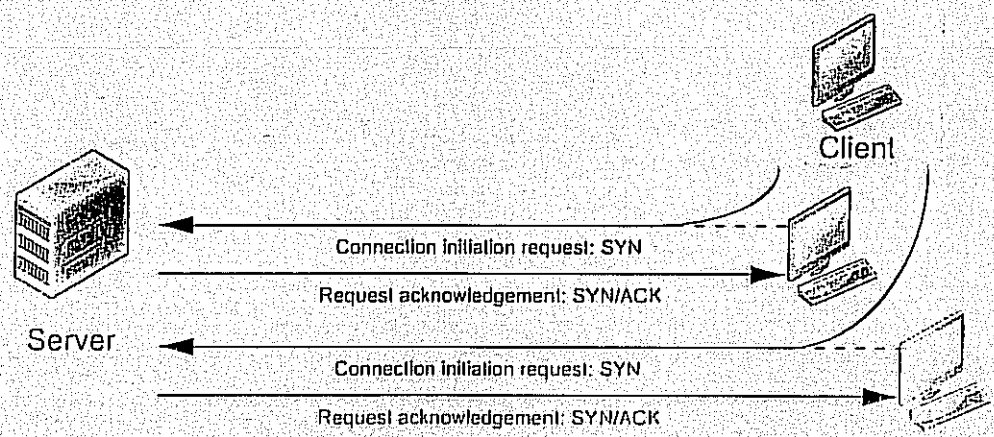



SYN floods are seldom launched from a single address so limiting the number of connection attempts from a single IP address is not usually effective.

## SYN spoofing

With a flood of SYN packets coming from a single attacker, you can limit the number of connection attempts from the source IP address or block the attacker entirely. To prevent this simple defense from working, or to disguise the source of the attack, the attacker may spoof the source address and use a number of IP addresses to give the appearance of a distributed denial of service (DDoS) attack. When the server receives the spoofed SYN packets, the SYN+ACK replies will go to the spoofed source IP addresses which will either be invalid, or the system receiving the reply will not know what to do with it.

Figure 4: A client launches a SYN spoof attack




## DDoS SYN flood

The most severe form of SYN attack is the distributed SYN flood, one variety of distributed denial of service attack (DDoS). Like the SYN flood, the target receives a flood of SYN packets and the ACK+SYN replies are never answered. The attack is distributed across multiple sources sending SYN packets in a coordinated attack.

LICITACIÓN PÚBLICA MIXTA NACIONAL NÚMERO **No. LA-009KCZ002-N49-2015** PARA EL ARRENDAMIENTO DEL "EQUIPO FIREWALL/VPN Y CONSOLA DE ADMINISTRACIÓN PARA EXPANSIÓN DE OFICINAS TELEGRÁFICAS DE LA RED TELDAT."

GRUPOTECNO

# Anexo FortiOS Handbook Version 5.2.3

16510

FORTINET.

*High Performance Network Security*

# FortiOS™ Handbook

**VERSION 5.2.3**

16511

# Top Features

This chapter introduces the following top features of FortiOS 5.2:

- Unified Policy Management
- FortiView Dashboards
- SSL Inspection
- Web Filtering
- Application Control
- IPsec VPN Creation Wizard
- Captive Portal
- FortiAP Management
- Flow-based Antivirus
- FortiExtender Support
- Using a Virtual WAN Link for Redundant Internet Connections
- Internet Key Exchange (IKE)
- SSL VPN Creation
- On-Net Status for FortiClient Devices

## Unified Policy Management

The different creation pages in the web-based manager for policy types and subtypes (user-identity, device identity, and VPN) have been merged into a single main policy creation page. New fields have been added for **Source User(s)** and **Source Device Type** that remove the need for multiple authentication rules in a single policy. This allows for greater control and customization of policies, as a combination of these source types can be used in a single policy rather than having to pick one type.

For more information, see Unified Policy Management on page 94.

## FortiView Dashboards

The FortiView dashboards integrate real time and historical dashboards into a single view that displays the top 100 sessions on a FortiGate unit. The different dashboards show information on the following:

- Sources
- Applications
- Cloud applications
- Destinations
- Web sites
- Threats
- All sessions

For more information, see "Usability Enhancements" on page 83.

16512

### Support for Non-HTTP WAN Optimization and Explicit Proxy Traffic

IPS is now supported for both non-HTTP WAN optimization traffic and explicit proxy traffic.

## Vulnerability Scanning Visibility

The options to configure vulnerability scanning either in the web-based manager or the CLI are also only available in NAT/Route mode.

Vulnerability scanning options in the web-based manager are now hidden by default. To enable vulnerability scanning, go to **System > Config > Features**, select **Show More**, turn on **Vulnerability Scan**, and select **Apply**.

Vulnerability scanning is also hidden by default for FortiClient profiles until being enabled in the CLI. To enable scanning, enter the following commands:

```
config endpoint-control profile
  edit <profile-name>
    config forticlient-winmac-settings
      set forticlient-vuln-scan {enable | disable}
      set forticlient-vuln-scan-schedule {daily | weekly | monthly}
      set forticlient-vuln-scan-on-registration {enable | disable}
      set forticlient-ui-options {av | wf | af | vpn | vs}
    end
end
```

## Removed IM Proxy Options from the CLI

The proxy options related to instant messaging (IM) functions and attributes have been removed from the CLI in FortiOS 5.2. This includes the following commands:

- `config imp2p`
- `get imp2p`
- The DLP sensor options for AIM, ICQ, MSN, and Yahoo protocols.
- The AntiVirus profile option `config im`.
- The AntiVirus quarantine options for IM.
- The Application Control profile options for IM.
- The firewall profile protocol options for IM.

## Client Reputation

The 5.0 feature client reputation has been renamed Threat Weight in FortiOS 5.2 and has been moved from Security Profiles to **Log & Report > Log Config > Threat Weight**. It can now be configured in the CLI using the command `config log threat-weight`.

# High Availability

New high availability features include:

- DHCP and PPPOE Support for Active-Passive Mode
- VRRP Support
- Trigger Failover
- Synchronizing a GTP Tunnel over Physical Ports
- IPv6 Management Interface Gateway

## DHCP and PPPOE Support for Active-Passive Mode

High Availability is now supported in Active-Passive mode when there are interfaces working in DHCP client or PPPOE client mode.

## VRRP Support

Additional features have been added to support Virtual Router Redundancy Protocol (VRRP).

### VRRP Groups

A VRRP group includes all the relevant VRRP IDs and tracks the VRRP status in order to force the status of all group members if a VRRP domain is changed from master to backup.

VRRP groups are configured through the CLI. The VRRP group ID can be between 1 and 65535.

**Syntax**

```
config system interface
  edit <port>
    config vrrp
      edit <id>
        set vrgrp <id>
      end
  end
```

A VRRP column has also been added to the interfaces list in the web-based manager that will show the VRRP ID, group, and status. This list can be found at **System > Network > Interfaces**.

### Using a Second Destination IP (VRDST)

VRRP can now be configured with second destination IP (VRDST) for monitoring. When two IPs are used, VRRP failure will only be reported if both monitored IPs are down. A second VRDST can be configured using the CLI.

**Syntax**

```
config system interface
  edit <interface>
    config vrrp
      edit <id>
```

16514

| | |
|---|---|
| | Configure the unit to act as a wireless network controller, managing the wireless Access Point (AP) functionality of FortiWiFi and FortiAP units. |
| **WiFi Controller** | On certain FortiGate models, this menu is called **WiFi & Switch Controller** and has additional features allowing for FortiSwitch units to be managed by the FortiGate. |
| **Log & Report** | Configure logging and alert email as well as reports. View log messages and reports. |
| **Current VDOM** | This menu only appears when VDOMs are enabled on the unit and is used to switch between VDOMs. |

## Dashboards

The various dashboard menus provides a way to access information about network activity and events, as well as configure basic system settings.

There are two main dashboards: the Status Dashboard and the FortiView Dashboards.

### Status Dashboard

The **Status Dashboard** can be found by going to **System > Dashboard > Status.** The dashboard consists of a number of widgets, each displaying a different set of information. A number of pre-configured widgets are available which can be customized to meet your needs.

To choose which widgets will be shown, select **Widget** and select the widget you wish to view, which will add it to the dashboard. Widgets can be rearranged in the **Status Dashboard** for easier access and viewing. You can also change the display from two columns to one by selecting the **Dashboard** button, selecting **Edit Dashboard** and choosing the one column display from the options.

### Custom Dashboards

You can create custom dashboards that will be added to the menu under the default **Status Dashboard**. You can add, remove, or rename a dashboard, regardless of whether it is default. You can also reset the Dashboard menu to its default settings by selecting **Reset Dashboards.**

If VDOMs are enabled, only the dashboards within Global are available for configuration.

To add a dashboard

1. Go to System > Dashboard > Status.
2. Select Dashboard, located at the top left of the page.
3. Select Add Dashboard.

That information identifies the user and user group, which is then matched using a security policy. See SSO using RADIUS accounting records on page 568.

### FortiGuard Web Filter override authentication

Optionally, users can be allowed the privilege of overriding FortiGuard Web Filtering to view blocked web sites. Depending on the override settings, the override can apply to the user who requested it, the entire user group to which the user belongs, or all users who share the same web filter profile. As with other FortiGate features, access to FortiGuard overrides is controlled through user groups. Firewall and Directory Services user groups are eligible for the override privilege. For more information about web filtering and overrides, see the UTM chapter of this FortiOS Handbook.

## VPN authentication

Authentication involves authenticating the user. In IPsec VPNs authenticating the user is optional, but authentication of the peer device is required.

This section includes:

- Authenticating IPsec VPN peers (devices)
- Authenticating IPsec VPN users
- Authenticating SSL VPN users
- Authenticating PPTP and L2TP VPN users

### Authenticating IPsec VPN peers (devices)

A VPN tunnel has one end on a local trusted network, and the other end is at a remote location. The remote peer (device) must be authenticated to be able to trust the VPN tunnel. Without that authentication, it is possible for a malicious hacker to masquerade as a valid VPN tunnel device and gain access to the trusted local network.

The three ways to authenticate VPN peers are with a preshared key, RSA X.509 certificate, or a specific peer ID value.

The simplest way for IPsec VPN peers to authenticate each other is through the use of a preshared key, also called a shared secret. The preshared key is a text string used to encrypt the data exchanges that establish the VPN tunnel. The preshared key must be six or more characters. The VPN tunnel cannot be established if the two peers do not use the same key. The disadvantage of preshared key authentication is that it can be difficult to securely distribute and update the preshared keys.

RSA X.509 certificates are a better way for VPN peers to authenticate each other. Each peer offers a certificate signed by a Certificate Authority (CA) which the other peer can validate with the appropriate CA root certificate. For more information about certificates, see Certificate-based authentication on page 500.

You can supplement either preshared key or certificate authentication by requiring the other peer to provide a specific peer ID value. The peer ID is a text string configured on the peer device. On a FortiGate peer or FortiClient Endpoint Security peer, the peer ID provided to the remote peer is called the Local ID.

### Authenticating IPsec VPN users

An IPsec VPN can be configured to accept connections from multiple dynamically addressed peers. You would do this to enable employees to connect to the corporate network while traveling or from home. On a FortiGate unit, you create this configuration by setting the Remote Gateway to Dialup User.

## FortiGate administrator's view of authentication

Authentication is based on user groups. The FortiGate administrator configures authentication for security policies and VPN tunnels by specifying the user groups whose members can use the resource. Some planning is required to determine how many different user groups need to be created. Individual user accounts can belong to multiple groups, making allocation of user privileges very flexible.

A member of a user group can be:

- a user whose username and password are stored on the FortiGate unit
- a user whose name is stored on the FortiGate unit and whose password is stored on a remote or external authentication server
- a remote or external authentication server with a database that contains the username and password of each person who is permitted access

The general process of setting up authentication is as follows:

1. If remote or external authentication is needed, configure the required servers.
2. Configure local and peer (PKI) user identities. For each local user, you can choose whether the FortiGate unit or a remote authentication server verifies the password. Peer members can be included in user groups for use in security policies.
3. Create user groups.
4. Add local/peer user members to each user group as appropriate. You can also add an authentication server to a user group. In this case, all users in the server's database can authenticate. You can only configure peer user groups through the CLI.
5. Configure security policies and VPN tunnels that require authenticated access.

For authentication troubleshooting, see the specific chapter for the topic or for general issues see Troubleshooting on page 594.

## General authentication settings

Go to **User & Device > Authentication > Settings** to configure authentication timeout, protocol support, and authentication certificates.

When user authentication is enabled within a security policy, the authentication challenge is normally issued for any of the four protocols (depending on the connection protocol):

- HTTP (can also be set to redirect to HTTPS)
- HTTPS
- FTP
- Telnet

The selections made in the **Protocol Support** list of **Authentication Settings** control which protocols support the authentication challenge. Users must connect with a supported protocol first so they can subsequently connect with other protocols. If HTTPS is selected as a method of protocol support, it allows the user to authenticate with a customized Local certificate.

When you enable user authentication within a security policy, the security policy user will be challenged to authenticate. For user ID and password authentication, users must provide their user names and passwords. For certificate authentication (HTTPS or HTTP redirected to HTTPS only), you can install customized certificates on

16517

# Users and user groups

FortiGate authentication controls system access by user group. By assigning individual users to the appropriate user groups you can control each user's access to network resources. The members of user groups are user accounts, of which there are several types. Local users and peer users are defined on the FortiGate unit. User accounts can also be defined on remote authentication servers.

This section describes how to configure local users and peer users and then how to configure user groups. For information about configuration of authentication servers see Authentication servers on page 429.

This section contains the following topics:

- Users
- User groups

## Users

A user is a user account consisting of username, password, and in some cases other information, configured on the FortiGate unit or on an external authentication server. Users can access resources that require authentication only if they are members of an allowed user group. There are several different types of user accounts with slightly different methods of authentication:

| User type | Authentication |
|---|---|
| **Local user** | The username and password must match a user account stored on the FortiGate unit. Authentication by FortiGate security policy. |
| **Remote user** | The username must match a user account stored on the FortiGate unit and the username and password must match a user account stored on the remote authentication server. FortiOS supports LDAP, RADIUS, and TACACS+ servers. |
| **Authentication server user** | A FortiGate user group can include user accounts or groups that exist on a remote authentication server. |
| **FSSO user** | With Fortinet Single Sign On (FSSO), users on a Microsoft Windows or Novell network can use their network authentication to access resources through the FortiGate unit. Access is controlled through FSSO user groups which contain Windows or Novell user groups as their members. |
| **PKI or Peer user** | A Public Key Infrastructure (PKI) or peer user is a digital certificate holder who authenticates using a client certificate. No password is required, unless two-factor authentication is enabled. |
| **IM Users** | IM users are not authenticated. The FortiGate unit can allow or block each IM user name from accessing the IM protocols. A global policy for each IM protocol governs access to these protocols by unknown users. |
| **Guest Users** | Guest user accounts are temporary. The account expires after a selected period of time. |

# Configuring authenticated access

When you have configured authentication servers, users, and user groups, you are ready to configure security policies and certain types of VPNs to require user authentication.

This section describes:

- Authentication timeout
- Password policy
- Authentication protocols
- Authentication in Captive Portals
- Authentication in security policies
- VPN authentication

## Authentication timeout

An important feature of the security provided by authentication is that it is temporary—a user must re-authenticate after logging out. Also if a user is logged on and authenticated for an extended period of time, it is a good policy to have them re-authenticate at set periods. This ensures a user's session is cannot be spoofed and used maliciously for extended periods of time — re-authentication will cut any spoof attempts short. Shorter timeout values are more secure.

### Security authentication timeout

You set the security user authentication timeout to control how long an authenticated connection can be idle before the user must authenticate again. The maximum timeout is 480 minutes (8 hours).

**To set the security authentication timeout - web-based manager:**

1. Go to **User & Device > Authentication > Settings**.
2. Enter the **Authentication Timeout** value in minutes.
   The default authentication timeout is 5 minutes.
3. Select **Apply**.

### SSL VPN authentication timeout

You set the SSL VPN user authentication timeout (**Idle Timeout**) to control how long an authenticated connection can be idle before the user must authenticate again. The maximum timeout is 28 800 seconds. The default timeout is 300 seconds.

**To set the SSL VPN authentication timeout - web-based manager:**

1. Go to **VPN > SSL > Interface**.
2. Make sure that Idle Timeout is enabled and enter the **Idle Timeout** value (seconds).
3. Select **OK**.

## Enabling security logging

There are two types of logging that relate to authentication — event logging, and security logging.

When enabled, event logging records system events such as configuration changes, and authentication. To configure event logging, go to **Log&Report > Log Config > Log Settings** and enable **Event Logging**. Select the events you want to log, such as **User activity event**.

When enabled, security logging will log UTM and security policy traffic.

You must enable logging within a security policy, as well as the options that are applied to a security policy, such as UTM features. Event logs are enabled within the Event Log page.

For more information on logging, see the FortiOS Log and Reporting guide.

For more information on specific types of log messages, see the FortiOS Log Message Reference.

You need to set the logging severity level to **Notification** when configuring a logging location to record traffic log messages.

**To enable logging within an existing security policy - web-based manager:**

1. Go to **Policy > Policy**.
2. Expand to reveal the policy list of a policy.
3. Select the security policy you want to enable logging on and then select **Edit**.
4. To log all general firewall traffic, select the check box beside **Log Allowed Traffic**.
5. On the security policy's page, select the check box beside **UTM**.
6. In **UTM Security Profiles**, select enable the UTM profiles that you want applied to the policy, then select the profile or sensor from the drop-down list as well.
7. Select **OK**.

## Identity-based policy

An identity-based policy (IBP) performs user authentication in addition to the normal security policy duties. If the user does not authenticate, access to network resources is refused. This enforces Role Based Access Control (RBAC) to your organization's network and resources.

Identity-based policies also support Single Sign-On operation. The user groups selected in the policy are of the Fortinet Single Sign-On (FSSO) type.

User authentication can occur through any of the following supported protocols, including: HTTP, HTTPS, FTP, and Telnet. The authentication style depends on which of these protocols is included in the selected security services group and which of those enabled protocols the network user applies to trigger the authentication challenge.

For username and password-based authentication (HTTP, FTP, and Telnet) the FortiGate unit prompts network users to enter their username, password, and token code if two-factor authentication is selected for that user account. For certificate-based authentication, including HTTPS or HTTP redirected to HTTPS only, see Certificate authentication on page 487.

With identity-based policies, the FortiGate unit allows traffic that matches the source and destination addresses, device types, and so on. This means specific security policies must be placed **before** more general ones to be effective.

When the identity-based policy has been configured, the option to customize authentication messages is available. This allows you to change the text, style, layout, and graphics of the replacement messages associated with this firewall policy. When enabled, customizing these messages follows the same method as changing the disclaimer. See Disclaimer on page 484.

Types of authentication also available in identity-based policies are

- NTLM authentication
- Certificate authentication

## NTLM authentication

NT LAN Manager (NTLM) protocol can be used as a fallback for authentication when the Active Directory (AD) domain controller is unreachable. NTLM uses the web browser to send and receive authentication information. See "NTLM" and "FSSO NTLM authentication support".

### To enable NTLM

1. Edit the policy in the CLI to enable NTLM. For example, if the policy ID is 4:
2. Go to **Policy & Objects > Policy > IPv4** and note the ID number of your FSSO policy.
3. The policy must have an FSSO user group as **Source User(s)**. There must be at least one FSSO Collector agent configured on the FortiGate unit.

```
config firewall policy
  edit 4
    set ntlm enable
  end
```

## NTLM guest access

Guest profile access may be granted to users who fail NTLM authentication, such as visitors who have no user credentials on the network. To allow guest user access, edit the FSSO security policy in the CLI, like this:

```
config firewall policy
  edit 4
    set ntlm enable
    set ntlm-guest enable
  end
```

## NTLM enabled browsers - CLI

User agent strings for NTLM enabled browsers allow the inspection of initial HTTP-User-Agent values, so that non-supported browsers are able to go straight to guest access without needlessly prompting the user for credentials that will fail. `ntlm-guest` must be enabled to use this option.

```
config firewall policy
  edit 4
    set ntlm enable
    set ntlm-guest enable
    set ntlm-enabled-browsers <user_agent_string>
  next
  end
```

16521

- Zones
- Predefined addresses
  - IP address-based
  - FQDN-based
  - Geography-based
- Access schedules
- Authentication
  - Local user-based
  - Authentication server-based (Active Directory, RADIUS, LDAP)
  - Device-based
- Configurable services
- IPv4 and IPv6 protocol support

The features of FortiOS include but are not limited to:

- Security profiles, sometimes referred to as Unified Threat Management (UTM) or Next Generation Firewall (NGFW)
- Predefined firewall addresses (this includes IPv4 and IPv6, IP pools, wildcard addresses and netmasks, and geography-based addresses)
- Monitoring traffic
- Traffic shaping and per-IP traffic shaping (advanced)
- Firewall schedules
- Services (such as AOL, DHCP and FTP)
- Logging traffic
- Quality of Service (QoS)
- Identity-based policies
- Endpoint security

The "Firewall concepts" expand on what each of the features does and how they relate to the administration of the FortiGate firewall. The section will also try to explain some of the common firewall concepts that will be touched on in the implementing of these features.

"Building firewall objects and policies" shows how to perform specific tasks with the FortiGate firewall.

## How does a FortiGate protect your network?

The FortiGate firewall protects your network by taking the various components and using them together to build a kind of wall or access control point so anyone that is not supposed to be on your network is prevented from accessing your network in any way other than those approved by you. It also protects your network from itself by keeping things that shouldn't happen from happening and optimizing the flow of traffic so the network is protected from traffic congestion that would otherwise impede traffic flow.

Most people have at one time or another played with a child's toy system made up of interlocking blocks. The blocks come in different shapes and sizes so you can build structures to suit your needs. The components of the FortiGate firewall are similar. You are not forced to use all of the blocks all of the time. You mix and match them to get the results that you are looking for. You can build a very basic structure, where its only function is to direct traffic in and out to the correct subnets. You can build a fortress that only allows specific traffic to or from specific hosts at specific times of day and only when credentials that have been pre-approved have been provided. You can also add in that all of the traffic is encrypted, so that even when the traffic is out on the Internet it is private

- The FortiGate unit uses a Management IP address for the purposes of Administration.
- Still able to use NAT to a degree, but the configuration is less straightforward

In Transparent mode, you can also perform NAT by creating a security policy or policies that translates the source addresses of packets passing through the FortiGate unit as well as virtual IP addresses and/or IP pools.

## Quality of Service

The Quality of Service (QoS) feature allows the management of the level of service and preference given to the various types and sources of traffic going through the firewall so that the traffic that is important to the services and functions connecting through the firewall gets the treatment required to ensure the level of quality that is required. QoS can be helpful for organizations that are trying to manage their voice and streaming multi-media traffic, which can rapidly consume bandwidth. Both voice and streaming multi-media are sensitive to latency. FortiGate units support QoS using traffic policing, traffic shaping, and queuing.

### Traffic policing

Packets are dropped that do not conform to bandwidth limitations

### Traffic shaping

Assigning minimum levels of bandwidth to be allocated to specific traffic flows to guarantee levels of service or assigning maximum levels of bandwidth to be allocated to specific traffic flows so that they do not impede other flows of traffic.

This helps to ensure that the traffic may consume bandwidth at least at the guaranteed rate by assigning a greater priority queue if the guarantee is not being met. Traffic shaping also ensures that the traffic cannot consume bandwidth greater than the maximum at any given instant in time. Flows that are greater than the maximum rate are subject to traffic policing.

### Queuing

Assigning differing levels of priority to different traffic flows so that traffic flows that are adversely effected by latency are prevented from being effected by traffic flows that are not subject to the effects of latency. All traffic in a higher priority traffic queue must be completely transmitted before traffic in lower priority queues will be transmitted.

An example of where you would want to use something like this is if you had competing traffic flows of Voice over IP traffic and email traffic. The VoIP traffic is highly susceptible to latency issues. If you have a delay of a few seconds it is quickly noticeable when it is occurring. Email on the other hand can have a time delay of much longer and it is highly unlikely that it will be noticed at all.

By default, the priority given to any traffic is high, so if you want to give one type of traffic priority over all other traffic you will need to lower the priority of all of the other traffic.

## Interfaces and zones

A Firewall is a gateway device that may be the nexus point for more than 2 networks. The interface that the traffic is coming in on and should be going out on is a fundamental concern for the purposes of routing as well as

# Network defense

This section describes in general terms the means by which attackers can attempt to compromise your network and steps you can take to protect it. The goal of an attack can be as complex as gaining access to your network and the privileged information it contains, or as simple as preventing customers from accessing your web server. Even allowing a virus onto your network can cause damage, so you need to protect against viruses and malware even if they are not specifically targeted at your network.

The following topics are included in this section:

- Monitoring
- Blocking external probes
- Defending against DoS attacks

## Monitoring

Monitoring, in the form of logging, alert email, and SNMP, does not directly protect your network. But monitoring allows you to review the progress of an attack, whether afterwards or while in progress. How the attack unfolds may reveal weaknesses in your preparations. The packet archive and sniffer policy logs can reveal more details about the attack. Depending on the detail in your logs, you may be able to determine the attackers location and identity.

While log information is valuable, you must balance the log information with the resources required to collect and store it.

## Blocking external probes

Protection against attacks is important, but attackers often use vulnerabilities and network tools to gather information about your network to plan an attack. It is often easier to prevent an attacker from learning important details about your network than to defend against an attack designed to exploit your particular network.

Attacks are often tailored to the hardware or operating system of the target, so reconnaissance is often the first step. The IP addresses of the hosts, the open ports, and the operating systems the hosts are running is invaluable information to an attacker. Probing your network can be as simple as an attacker performing an address sweep or port scan to a more involved operation like sending TCP packets with invalid combinations of flags to see how your firewall reacts.

### Address sweeps

An address sweep is a basic network scanning technique to determine which addresses in an address range have active hosts. A typical address sweep involves sending an ICMP ECHO request (a ping) to each address in an address range to attempt to get a response. A response signifies that there is a host at this address that responded to the ping. It then becomes a target for more detailed and potentially invasive attacks.

Address sweeps do not always reveal all the hosts in an address range because some systems may be configured to ignore ECHO requests and not respond, and some firewalls and gateways may be configured to prevent ECHO requests from being transmitted to the destination network. Despite this shortcoming, Address sweeps are still used because they are simple to perform with software tools that automate the process.

Use the `icmp_sweep` anomaly in a DoS policy to protect against address sweeps.

There are a number of IPS signatures to detect the use of ICMP probes that can gather information about your network. These signatures include `AddressMask`, `Traceroute`, `ICMP.Invalid.Packet.Size`, and `ICMP.Oversized.Packet`. Include ICMP protocol signatures in your IPS sensors to protect against these probes/attacks.

### Port scans

Potential attackers may run a port scan on one or more of your hosts. This involves trying to establish a communication session to each port on a host. If the connection is successful, a service may be available that the attacker can exploit.

Use the DoS anomaly check for `tcp_port_scan` to limit the number of sessions (complete and incomplete) from a single source IP address to the configured threshold. If the number of sessions exceed the threshold, the configured action is taken.

Use the DoS anomaly check for `udp_scan` to limit UDP sessions in the same way.

### Probes using IP traffic options

Every TCP packet has space reserved for eight flags or control bits. They are used for communicating various control messages. Although space in the packet is reserved for all eight, there are various combinations of flags that should never happen in normal network operation. For example, the SYN flag, used to initiate a session, and the FIN flag, used to end a session, should never be set in the same packet.

Attackers may create packets with these invalid combinations to test how a host will react. Various operating systems and hardware react in different ways, giving a potential attackers clues about the components of your network.

The IPS signature `TCP.Bad.Flags` detects these invalid combinations. The default action is pass though you can override the default and set it to **Block** in your IPS sensor.

### Configure packet replay and TCP sequence checking

The anti-replay CLI command allows you to set the level of checking for packet replay and TCP sequence checking (or TCP Sequence (SYN) number checking). All TCP packets contain a Sequence Number (SYN) and an Acknowledgement Number (ACK). The TCP protocol uses these numbers for error free end-to-end communications. TCP sequence checking can also be used to validate individual packets.

FortiGate units use TCP sequence checking to make sure that a packet is part of a TCP session. By default, if a packet is received with sequence numbers that fall out of the expected range, the FortiGate unit drops the packet. This is normally a desired behavior, since it means that the packet is invalid. But in some cases you may want to configure different levels of anti-replay checking if some of your network equipment uses non-RFC methods when sending packets.

Configure the anti-replay CLI command:

```
config system global
  set anti-replay {disable | loose | strict}
end
```

You can set anti-replay protection to the following settings:

- `disable` — No anti-replay protection.
- `loose` — Perform packet sequence checking and ICMP anti-replay checking with the following criteria:
- The SYN, FIN, and RST bit can not appear in the same packet.

When fragmented packets arrive at their destination, they are reassembled and read. If the fragments do not arrive together, they must be held until all of the fragments arrive. Reassembly of a packet requires all of the fragments.

The FortiGate unit automatically reassembles fragmented packets before processing them because fragmented packets can evade security measures. Both IP packets and TCP packets are reassembled by the IPS engine before examination.

For example, you have configured the FortiGate unit to block access to the example.org web site. Any checks for example.com will fail if a fragmented packet arrives and one fragment contains `http://www.exa` while the other contains `mple.com/`. Viruses and malware can be fragmented and avoid detection in the same way. The FortiGate unit will reassemble fragmented packets before examining network data to ensure that inadvertent or deliberate packet fragmentation does not hide threats in network traffic.

### Non-standard ports

Most traffic is sent on a standard port based on the traffic type. The FortiGate unit recognizes most traffic by packet content rather than the TCP/UDP port and uses the proper IPS signatures to examine it. Protocols recognized regardless of port include DHCP, DNP3, FTP, HTTP, IMAP, MS RPC, NNTP, POP3, RSTP, SIP, SMTP, and SSL, as well as the supported IM/P2P application protocols.

In this way, the FortiGate unit will recognize HTTP traffic being sent on port 25 as HTTP rather than SMTP, for example. Because the protocol is correctly identified, the FortiGate unit will examine the traffic for any enabled HTTP signatures.

### Negotiation codes

Telnet and FTP servers and clients support the use of negotiation information to allow the server to report what features it supports. This information has been used to exploit vulnerable servers. To avoid this problem, the FortiGate unit removes negotiation codes before IPS inspection.

### HTTP URL obfuscation

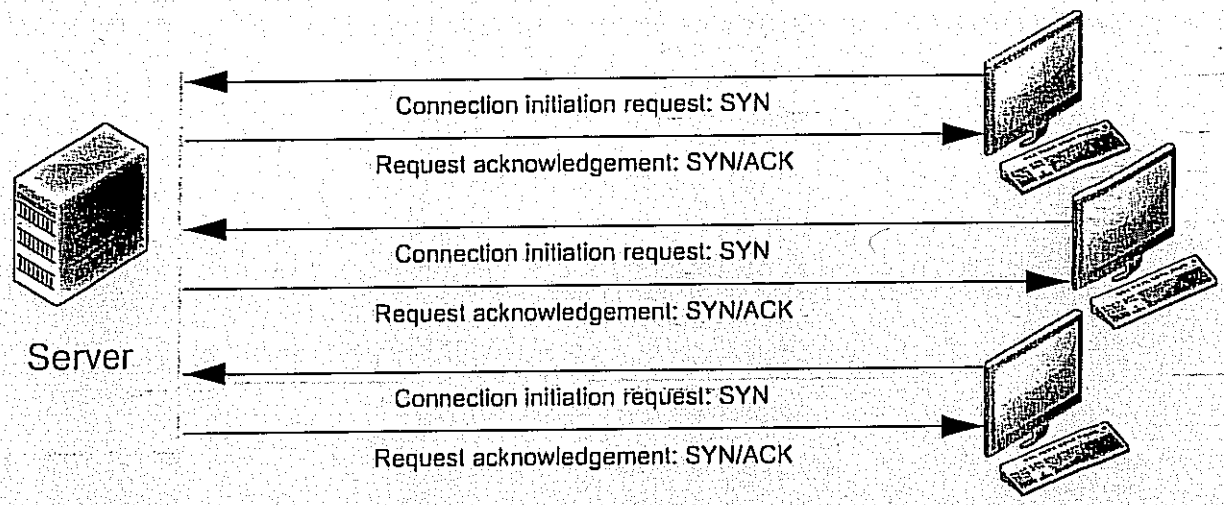
Attackers encode HTML links using various formats to evade detection and bypass security measures. For example, the URL www.example.com/cgi.bin could be encoded in a number of ways to avoid detection but still work properly, and be interpreted the same, in a web browser.

The FortiGate prevents the obfuscation by converting the URL to ASCII before inspection.

HTTP URL obfuscation types

| Encoding type | Example |
|---|---|
| No encoding | http://www.example.com/cgi.bin/ |
| Decimal encoding | http://www.example.com/cgi.bin/ |
| URL encoding | http://www.example.com/%43%47%49%2E%42%49%4E%2F |

**Multiple attackers launch a distributed SYN flood**




The distributed SYN flood is more difficult to defend against because multiple clients are capable of creating a larger volume of SYN packets than a single client. Even if the server can cope, the volume of traffic may overwhelm a point in the network upstream of the targeted server. The only defence against this is more bandwidth to prevent any choke-points.

## Configuring the SYN threshold to prevent SYN floods

The preferred primary defence against any type of SYN flood is the DoS anomaly check for `tcp_syn_flood` threshold. The threshold value sets an upper limit on the number of new incomplete TCP connections allowed per second. If the number of incomplete connections exceeds the threshold value, and the action is set to **Pass**, the FortiGate unit will allow the SYN packets that exceed the threshold. If the action is set to **Block**, the FortiGate unit will block the SYN packets that exceed the threshold, but it will allow SYN packets from clients that send another SYN packet.

The tools attackers use to generate network traffic will not send a second SYN packet when a SYN+ACK response is not received from the server. These tools will not "retry." Legitimate clients will retry when no response is received, and these retries are allowed even if they exceed the threshold with the action set to **Block**.

## SYN proxy

FortiGate units with network acceleration hardware, whether built-in or installed in the form of an add-on module, offer a third action for the `tcp_syn_flood` threshold. Instead of **Block** and **Pass**, you can choose to **Proxy** the incomplete connections that exceed the threshold value.

When the `tcp_syn_flood` threshold action is set to **Proxy**, incomplete TCP connections are allowed as normal as long as the configured threshold is not exceeded. If the threshold is exceeded, the FortiGate unit will intercept incoming SYN packets from clients and respond with a SYN+ACK packet. If the FortiGate unit receives an ACK response as expected, it will "replay" this exchange to the server to establish a communication session between the client and the server, and allow the communication to proceed.

## Other flood types

UDP and ICMP packets can also be used for DoS attacks, though they are less common. TCP SYN packets are so effective because the target receives them and maintains a session table entry for each until they time out.

16527

# Chapter 14 - IPsec VPN

This FortiOS Handbook chapter contains the following sections:

IPsec VPN concepts explains the basic concepts that you need to understand about virtual private networks (VPNs).

IPsec VPN overview provides a brief overview of IPsec technology and includes general information about how to configure IPsec VPNs using this guide.

IPsec VPN in the web-based manager describes the IPsec VPN menu of the web-based manager interface.

Gateway-to-gateway configurations explains how to set up a basic gateway-to-gateway (site-to-site) IPsec VPN. In a gateway-to-gateway configuration, two FortiGate units create a VPN tunnel between two separate private networks.

Hub-and-spoke configurations describes how to set up hub-and-spoke IPsec VPNs. In a hub-and-spoke configuration, connections to a number of remote peers and/or clients radiate from a single, central FortiGate hub.

Dynamic DNS configuration describes how to configure a site-to-site VPN, in which one FortiGate unit has a static IP address and the other FortiGate unit has a dynamic IP address and a domain name.

FortiClient dialup-client configurations guides you through configuring a FortiClient dialup-client IPsec VPN. In a FortiClient dialup-client configuration, the FortiGate unit acts as a dialup server and VPN client functionality is provided by the FortiClient Endpoint Security application installed on a remote host.

FortiGate dialup-client configurations explains how to set up a FortiGate dialup-client IPsec VPN. In a FortiGate dialup-client configuration, a FortiGate unit with a static IP address acts as a dialup server and a FortiGate unit with a dynamic IP address initiates a VPN tunnel with the FortiGate dialup server.

Supporting IKE Mode config clients explains how to set up a FortiGate unit as either an IKE Mode Config server or client. IKE Mode Config is an alternative to DHCP over IPsec.

Internet-browsing configuration explains how to support secure web browsing performed by dialup VPN clients, and hosts behind a remote VPN peer. Remote users can access the private network behind the local FortiGate unit and browse the Internet securely. All traffic generated remotely is subject to the security policy that controls traffic on the private network behind the local FortiGate unit.

Redundant VPN configurations discusses the options for supporting redundant and partially redundant tunnels in an IPsec VPN configuration. A FortiGate unit can be configured to support redundant tunnels to the same remote peer if the FortiGate unit has more than one interface to the Internet.

Transparent mode VPNs describes two FortiGate units that create a VPN tunnel between two separate private networks transparently. In transparent mode, all FortiGate unit interfaces except the management interface are invisible at the network layer.

IPv6 IPsec VPNs describes FortiGate unit VPN capabilities for networks based on IPv6 addressing. This includes IPv4-over-IPv6 and IPv6-over-IPv4 tunnelling configurations. IPv6 IPsec VPNs are available in FortiOS 3.0 MR6 and later.

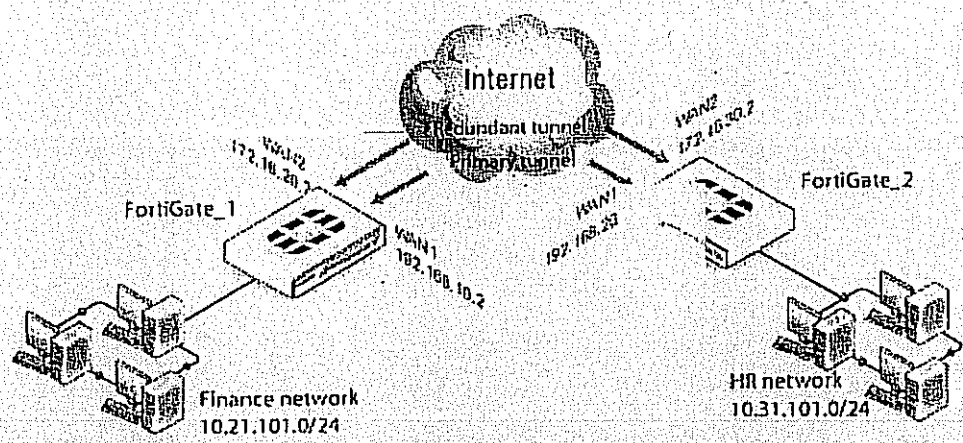
L2TP and IPsec (Microsoft VPN) explains how to support Microsoft Windows native VPN clients.

## Redundant route-based VPN configuration example

This example demonstrates a fully redundant site-to-site VPN configuration using route-based VPNs. At each site, the FortiGate unit has two interfaces connected to the Internet through different ISPs. This means that there are four possible paths for communication between the two units. In this example, these paths, listed in descending priority, are:

- FortiGate_1 WAN 1 to FortiGate_2 WAN 1
- FortiGate_1 WAN 1 to FortiGate_2 WAN 2
- FortiGate_1 WAN 2 to FortiGate_2 WAN 1
- FortiGate_1 WAN 2 to FortiGate_2 WAN 2

### Example redundant route-based VPN configuration




For each path, VPN configuration, security policies and routing are defined. By specifying a different routing distance for each path, the paths are prioritized. A VPN tunnel is established on each path, but only the highest priority one is used. If the highest priority path goes down, the traffic is automatically routed over the next highest priority path. You could use dynamic routing, but to keep this example simple, static routing is used.

## Configuring FortiGate_1

When configuring FortiGate_1, you must:

- Configure the interfaces involved in the VPN.
- Define the Phase 1 configuration for each of the four possible paths, creating a virtual IPsec interface for each one.
- Define the Phase 2 configuration for each of the four possible paths.
- Configure routes for the four IPsec interfaces, assigning the appropriate priorities.
- Configure incoming and outgoing security policies between the internal interface and each of the virtual IPsec interfaces.

### To configure the network interfaces

1. Go to System > Network > Interfaces.
2. Select the Internal interface and select Edit.

# AntiVirus

This section describes how to configure the antivirus options. From an antivirus profile you can configure the FortiGate unit to apply antivirus protection to HTTP, FTP, IMAP, POP3, SMTP, and NNTP sessions. If your FortiGate unit supports SSL content scanning and inspection, you can also configure antivirus protection for HTTPS, IMAPS, POP3S, SMTPS, and FTPS sessions.

In many cases you can just customize the default antivirus profile and apply it to the security policy that accepts the traffic to be virus scanned. You can also create custom antivirus profiles if want to apply different types of virus protection to different traffic.

The following topics are included in this section:

- Antivirus concepts
- Enabling AntiVirus scanning
- Testing your antivirus configuration
- Example Scenerios

## Antivirus concepts

The word "antivirus" refers to a group of features that are designed to prevent unwanted and potentially malicious files from entering your network. These features all work in different ways, which include checking for a file size, name, or type, or for the presence of a virus or grayware signature.

The antivirus scanning routines your FortiGate unit uses are designed to share access to the network traffic. This way, each individual feature does not have to examine the network traffic as a separate operation, and the overhead is reduced significantly. For example, if you enable file filtering and virus scanning, the resources used to complete these tasks are only slightly greater than enabling virus scanning alone. Two features do not require twice the resources.

Antivirus scanning examines files for viruses, worms, trojans, and other malware. The antivirus scan engine has a database of virus signatures it uses to identify infections. If the scanner finds a signature in a file, it determines that the file is infected and takes the appropriate action.

### Malware Threats

### Viruses

Viruses are self replicating code that install copies of themselves into other programs, data files for boot sectors of storage devices. Virus can often carry a "payload" which performs some undesirable function. These functions can include but are not limited to:

- Stealing drive-space
- Stealing cpu cycles
- Accessing private information
- Corrupting data

## SSL VPN modes of operation

When a remote client connects to the FortiGate unit, the FortiGate unit authenticates the user based on username, password, and authentication domain. A successful login determines the access rights of remote users according to user group. The user group settings specify whether the connection will operate in web-only mode or tunnel mode.

### Web-only mode

Web-only mode provides remote users with a fast and efficient way to access server applications from any thin client computer equipped with a web browser. Web-only mode offers true clientless network access using any web browser that has built-in SSL encryption and the Sun Java runtime environment.

Support for SSL VPN web-only mode is built into FortiOS. The feature comprises of an SSL daemon running on the FortiGate unit, and a web portal, which provides users with access to network services and resources including HTTP/HTTPS, Telnet, FTP, SMB/CIFS, VNC, RDP, and SSH.

In web-only mode, the FortiGate unit acts as a secure HTTP/HTTPS gateway and authenticates remote users as members of a user group. After successful authentication, the FortiGate unit redirects the web browser to the web portal home page and the user can access the server applications behind the FortiGate unit.

When the FortiGate unit provides services in web-only mode, a secure connection between the remote client and the FortiGate unit is established through the SSL VPN security in the FortiGate unit and the SSL security in the web browser. After the connection has been established, the FortiGate unit provides access to selected services and network resources through a web portal.

FortiGate SSL VPN web portals have a 1- or 2-column page layout and portal functionality is provided through small applets called widgets. Widget windows can be moved or minimized. The controls within each widget depend on its function. There are predefined web portals and the administrator can create additional portals.

Configuring the FortiGate unit involves selecting the appropriate web portal configuration in the user group settings. These configuration settings determine which server applications can be accessed. SSL encryption is used to ensure traffic confidentiality.

The following table lists the operating systems and web browsers supported by SSL VPN web-only mode.

**VPN Web-only Mode, supported operating systems and web browsers**

| Operating System | Web Browser |
|---|---|
| Microsoft Windows 7 32-bit SP1 | • Microsoft Internet Explorer versions 8, 9, 10 and 11<br>• Mozilla Firefox version 26 |
| Microsoft Windows 7 64-bit SP1 | • Microsoft Internet Explorer versions 8, 9, 10 and 11<br>• Mozilla Firefox version 26 |
| Linux CentOS version 5.6 and Ubuntu version 12.0.4 | • Mozilla Firefox version 5.6 |

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

# Basic configuration

Configuring SSL VPN involves a number of configurations within FortiOS that you need to complete to make it all come together. This chapter describes the components required, and how and where to configure them to set up the FortiGate unit as an SSL VPN server. The configurations and steps are high level, to show you the procedures needed, and where to locate the options in FortiOS. For real-world examples, see Setup examples on page 2053.

There are three or four key steps to configuring an SSL VPN tunnel. The first three in the points below are mandatory, while the others are optional. This chapter outlines these key steps as well as additional configurations for tighter security and monitoring.

The key steps are:

- Create user accounts and user groups for the remote clients.
  (Basic configuration on page 2016)
- Create a web portal to define user access to network resources.
  (Basic configuration on page 2016)
- Configure the security policies.
  (Basic configuration on page 2016)
- For tunnel-mode operation, add routing to ensure that client tunnel-mode packets reach the SSL VPN interface.
  (Basic configuration on page 2016)
- Setup logging of SSL VPN activities.
  (Basic configuration on page 2016)

This section contains the following information:



## User accounts and groups

The first step for an SSL VPN tunnel is to add the users and user groups that will access the tunnel. You may already have users defined for other authentication-based security policies.

The user group is associated with the web portal that the user sees after logging in. You can use one policy for multiple groups, or multiple policies to handle differences between the groups such as access to different services, or different schedules.

To create a user account:

- In the web-based manager, go to **User & Device > User > User Definition**, and select **Create New**.
- In the CLI, use the commands in `config user local`.

All users accessing the SSL tunnel must be in a firewall user group. User names can be up to 64 characters long.

To create user groups:

- In the web-based manager, go to **User & Device > User > User Groups** and select **Create New**.
- In the CLI, use the commands in `config user group`.

## Authentication

Remote users must be authenticated before they can request services and/or access network resources through the web portal. The authentication process can use a password defined on the FortiGate unit or optionally use established external authentication mechanisms such as RADIUS or LDAP.

To authenticate users, you can use a plain text password on the local FortiGate unit, forward authentication requests to an external RADIUS, LDAP or TACACS+ server, or utilize PKI certificates.

For information about how to create RADIUS, LDAP, TACACS+ or PKI user accounts and certificates, see the Authentication Guide.

FortiOS supports LDAP password renewal notification and updates through SSL VPN. Configuration is enabled using the CLI commands:

```
config user ldap
    edit <username>
        set server <domain>
        set password-expiry-warning enable
        set password-renewal enable
end
```

For more information, see the Authentication Guide.

## MAC host check

When a remote client attempts to log in to the portal, you can have the FortiGate unit check against the client's MAC address to ensure that only a specific computer or device is connecting to the tunnel. This can ensure better security should a password be compromised.

MAC addresses can be tied to specific portals and can be either the entire MAC address or a subset of the address. MAC host checking is configured in the CLI using the following commands:

```
conf vpn ssl web portal
  edit portal
    set mac-addr-check enable
    set mac-addr-action allow
      config mac-addr-check-rule
        edit "rule1"
          set mac-addr-list 01:01:01:01:01:01 08:00:27:d4:06:5d
          set mac-addr-mask 48
      end
  end
```

### Setting the idle timeout setting

The idle timeout setting controls how long the connection can remain idle before the system forces the remote user to log in again. For security, keep the default value of 5000 seconds or less. Set the timeout value to 0 to disable idle timeouts.

**To set the idle timeout - web-based manager:**

1. Go to **VPN > SSL > Settings** and enable **Idle Logout**.
2. In the **Inactive For** field, enter the timeout value.
   The valid range is from 10 to 28800 seconds.
3. Select **Apply**.

**To set the idle timeout - CLI:**

```
config vpn ssl settings
   set idle-timeout <seconds_int>
end
```

### SSL-VPN logs

Logging is available for SSL VPN traffic so you can monitor users connected to the FortiGate unit and their activity. For more information on configuring logs on the FortiGate unit, see the Logging and Reporting Guide.

**To enable logging of SSL VPN events - web-based manager:**

1. Go to **Log & Report > Log Config > Log Settings**.
2. Enable **Event Logging**, and select **VPN activity event**.
3. Select **Apply**.

To view the SSL VPN log data, in the web-based manager, go to **Log & Report** and select either the **Event Log** or **Traffic Log**.

In event log entries, look for the sub-types "sslvpn-session" and "sslvpn-user".

For information about how to interpret log messages, see the FortiGate Log Message Reference.

### Monitoring active SSL VPN sessions

You can go to **User & Device > Monitor** to view a list of active SSL VPN sessions. The list displays the user name of the remote user, the IP address of the remote client, and the time the connection was made. You can also see which services are being provided, and delete an active web session from the FortiGate unit.

**To monitor SSL VPNs - web-based manager:**

To view the list of active SSL VPN sessions, go to **VPN > Monitor > SSL-VPN Monitor**.

When a tunnel-mode user is connected, the **Description** field displays the IP address that the FortiGate unit assigned to the remote host.

If required, you can end a session/connection by selecting its checkbox and then clicking the **Delete** icon.

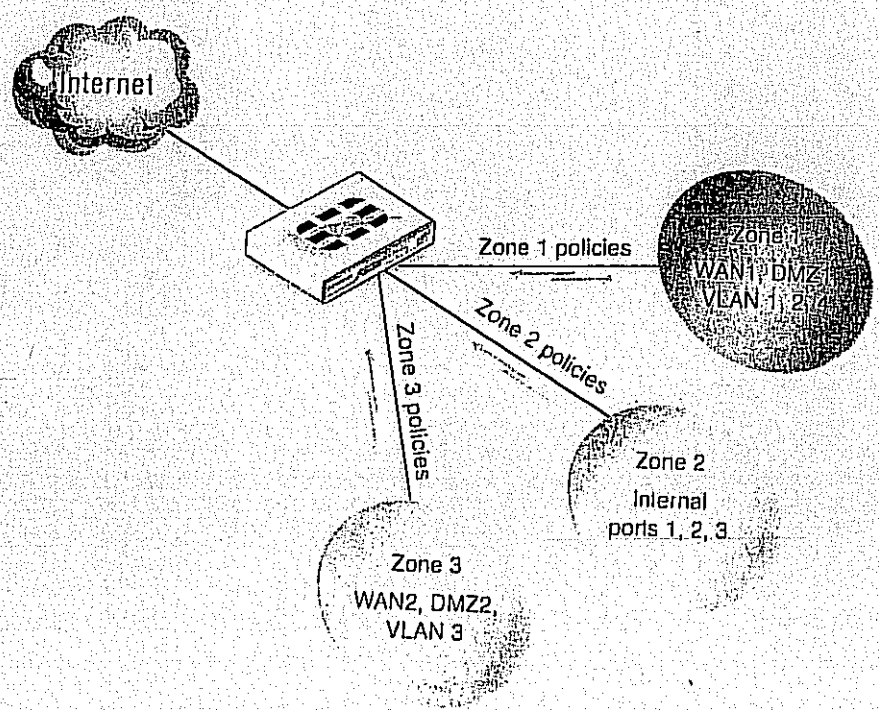
```
    edit VLAN_1
      set interface internal
      set type vlan
      set vlanid 100
      set ip 10.13.101.101/24
      set allowaccess https ssh
    next
end
```

## Zones

Zones are a group of one or more FortiGate interfaces, both physical and virtual, that you can apply security policies to control inbound and outbound traffic. Grouping interfaces and VLAN subinterfaces into zones simplifies the creation of security policies where a number of network segments can use the same policy settings and protection profiles. When you add a zone, you select the names of the interfaces and VLAN subinterfaces to add to the zone. Each interface still has its own address and routing is still done between interfaces, that is, routing is not affected by zones. Security policies can also be created to control the flow of intra-zone traffic.

For example, in the illustration below, the network includes three separate groups of users representing different entities on the company network. While each group has its own set of port and VLANs, in each area they can all use the same security policy and protection profiles to access the Internet. Rather than the administrator making nine separate security policies, he can add the required interfaces to a zone, and create three policies, making administration simpler.

**Network zones**




You can configure policies for connections to and from a zone, but not between interfaces in a zone. Using the above example, you can create a security policy to go between zone 1 and zone 3, but not between WAN2 and WAN1, or WAN1 and DMZ1.

This example explains how to set up a zone to include the Internal interface and a VLAN.

- Packets going through the FortiGate unit in transparent mode more than once
- More than one forwarding domain (such as incoming on one forwarding domain and outgoing on another)
- IPS and AV enabled.

Now IPS and AV is applied the first time packets go through the FortiGate unit, but not on subsequent passes. Only applying IPS and AV to this first pass fixes the network layer-2 related connection issues.

### NetBIOS

Computers running Microsoft Windows operating systems that are connected through a network rely on a WINS server to resolve host names to IP addresses. The hosts communicate with the WINS server by using the NetBIOS protocol.

To support this type of network, you need to enable the forwarding of NetBIOS requests to a WINS server. The following example will forward NetBIOS requests on the internal interface for the WINS server located at an IP address of 192.168.111.222.

```
config system interface
  edit internal
    set netbios_forward enable
    set wins-ip 192.168.111.222
end
```

These commands apply only in NAT mode. If VDOMs are enabled, these commands are per VDOM. You must set them for each VDOM that has the problem.

### STP forwarding

The FortiGate unit does not participate in the Spanning Tree Protocol (STP). STP is an IEEE 802.1 protocol that ensures there are no layer-2 loops on the network. Loops are created when there is more than one route for traffic to take and that traffic is broadcast back to the original switch. This loop floods the network with traffic, reducing available bandwidth to nothing.

If you use your FortiGate unit in a network topology that relies on STP for network loop protection, you need to make changes to your FortiGate configuration. Otherwise, STP recognizes your FortiGate unit as a blocked link and forwards the data to another path. By default, your FortiGate unit blocks STP as well as other non-IP protocol traffic.

Using the CLI, you can enable forwarding of STP and other layer-2 protocols through the interface. In this example, layer-2 forwarding is enabled on the external interface:

```
config system interface
  edit external
    set l2forward enable
    set stpforward enable
end
```

By substituting different commands for `stpforward enable`, you can also allow layer-2 protocols such as IPX, PPTP or L2TP to be used on the network.

### Too many VLAN interfaces

Any virtual domain can have a maximum of 255 interfaces in transparent mode. This includes VLANs, other virtual interfaces, and physical interfaces. NAT mode supports from 255 to 8192 depending on the FortiGate model. This total number of interfaces includes VLANs, other virtual interfaces, and physical interfaces.

LICITACIÓN PÚBLICA MIXTA NACIONAL NÚMERO **No. LA-009KCZ002-N49-2015** PARA EL ARRENDAMIENTO DEL "EQUIPO FIREWALL/VPN Y CONSOLA DE ADMINISTRACIÓN PARA EXPANSIÓN DE OFICINAS TELEGRÁFICAS DE LA RED TELDAT."

16536

GRUPOTECNO

# Anexo FortiOS Handbook Install and System Administration for FortiOS 5.0

FORTINET®

16537

# FortiOS™ Handbook
## Install and System Administration for FortiOS 5.0

- Web filtering within an HA cluster impacts performance.
- Always review the DNS settings to ensure the servers are fast.
- Content blocking may cause performance overhead.
- Local URL filters are faster than FortiGuard web filters, because the filter list is local and the FortiGate unit does not need to go out to the Internet to get the information from a FortiGuard web server.

## Antispam

- If possible use, a FortiMail unit. The antispam engines are more robust.
- Use fast DNS servers.
- Use specific security profiles for the rule that will use antispam.
- DNS checks may cause false positive with HELO DNS lookup.
- Content analysis (banned words) may impose performance overhead.

## Security

- Use NTP to synchronize time on the FortiGate and the core network systems, such as email servers, web servers, and logging services.
- Enable log rules to match corporate policy. For example, log administration authentication events and access to systems from untrusted interfaces.
- Minimize adhoc changes to live systems, if possible, to minimize interruptions to the network. When not possible, create backup configurations and implement sound audit systems using FortiAnalyzer and FortiManager.
- If you only need to allow access to a system on a specific port, limit the access by creating the strictest rule possible.

| | |
|---|---|
| Interface | Displayed when *Type* is set to *VLAN*.<br>Select the name of the physical interface to which to add a VLAN interface. Once created, the VLAN interface is listed below its physical interface in the Interface list.<br>You cannot change the physical interface of a VLAN interface except when adding a new VLAN interface. |
| VLAN ID | Displayed when *Type* is set to *VLAN*.<br>Enter the VLAN ID. You cannot change the *VLAN ID* except when adding a new VLAN interface.<br>The VLAN ID can be any number between 1 and 4094 and must match the VLAN ID added by the IEEE 802.1Q-compliant router or switch connected to the VLAN subinterface. |
| Virtual Domain | Select the virtual domain to add the interface to.<br>Admin accounts with super_admin profile can change the *Virtual Domain*. |
| Physical Interface Members | This section has two different forms depending on the interface type:<br>• **Software switch interface** - this section is a display-only field showing the interfaces that belong to the software switch virtual interface.<br>• **802.3ad aggregate or Redundant interface** - this section includes available interface and selected interface lists to enable adding or removing interfaces from the interface. For more information, see Redundant interfaces.<br>Select interfaces from this *Available Interfaces* list and select the right arrow to add an interface to the *Selected Interface* list. |
| Addressing mode | Select the addressing mode for the interface.<br>• Select *Manual* and add an *IP/Netmask* for the interface. If IPv6 configuration is enabled you can add both a IPv4 and an IPv6 IP address.<br>• Select *DHCP* to get the interface IP address and other network settings from a DHCP server. For more information, see DHCP addressing mode on an interface.<br>• Select *PPPoE* to get the interface IP address and other network settings from a PPPoE server. For more information, see PPPoE addressing mode on an interface.<br>• Select *One-Arm Sniffer* to enable the interface as a means to detect possible traffic threats. This option is available on physical ports not configured for the primary Internet connection. For more information see One-armed sniffer.<br>• Select *Dedicate to FortiAP/FortiSwitch* to have a FortiAP unit or FortiSwitch unit connect exclusively to the interface. This option is only available when editing a physical interface, and it has a static IP address. When you enter the IP address, the FortiGate unit automatically creates a DHCP server using the subnet entered. This option is not available on the ADSL interface.<br>The FortiSwitch option is currently only available on the FortiGate-100D. |

16540

Interfaces, especially the public-facing ports can be potentially accessed by those who you may not want access to the FortiGate unit. When setting up the FortiGate unit, you can set the type of protocol an administrator must use to access the FortiGate unit. The options include:

- HTTPS
- HTTP
- SSH
- TELNET
- SNMP
- PING
- FortiManager Access (FMG-Access
- FortiClient Access (FCT-Access)

You can select as many, or as few, even none, that are accessible by an administrator.

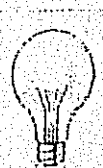
This example adds an IPv4 address 172.20.120.100 to the WAN1 interface as well as the administrative access to HTTPS and SSH. As a good practice, set the administrative access when you are setting the IP address for the port.

**To add an IP address on the WAN1 interface - web-based manager**

1. Go to *System* > *Network* > *Interface*.
2. Select the WAN1 interface row and select *Edit*.
3. Select the *Addressing Mode* of *Manual*.
4. Enter the IP address for the port of 172.20.120.100/24.
5. For *Administrative Access*, select *HTTPS* and *SSH*.
6. Select *OK*.

**To create IP address on the WAN1 interface - CLI**

```
config system interface
  edit wan1
    set ip 172.20.120.100/24
    set allowaccess https ssh
end
```



When adding to, or removing a protocol, you must type the entire list again. For example, if you have an access list of HTTPS and SSH, and you want to add PING, typing:

```
set allowaccess ping
```

...only PING will be set. In this case, you must type...

```
set allowaccess https ssh ping
```

## Wireless

A wireless interface is similar to a physical interface only it does not include a physical connection. The FortiWiFi units enables you to add multiple wireless-interfaces that can be available at the same time (the FortiWiFi-30B can only have one wireless interface). On FortiWiFi units, you can configure the device to be either an access point, or a wireless client. As an access point, the FortiWiFi unit can have up to four separate SSIDs, each on their own subnet for wireless access. In client mode, the FortiWiFi only has one SSID, and is used as a receiver, to enable remote users to connect to the existing network using wireless protocols.

FortiGate unit interfaces cannot have overlapping IP addresses, the IP addresses of all interfaces must be on different subnets. This rule applies to both physical interfaces and to virtual interfaces such as VLAN subinterfaces. Each VLAN subinterface must be configured with its own IP address and netmask. This rule helps prevent a broadcast storm or other similar network problems.

Any FortiGate unit, with or without VDOMs enabled, can have a maximum of 255 interfaces in Transparent operating mode. In NAT/Route operating mode, the number can range from 255 to 8192 interfaces per VDOM, depending on the FortiGate model. These numbers include VLANs, other virtual interfaces, and physical interfaces. To have more than 255 interfaces configured in Transparent operating mode, you need to configure multiple VDOMs with many interfaces on each VDOM.

This example shows how to add a VLAN, vlan_accounting on the FortiGate unit internal interface with an IP address of 10.13.101.101.

**To add a VLAN - web-based manager**

1. Go to *System* > *Network* > *Interface* and select *Create New*.

   The *Type* is by default set to VLAN.
2. Enter a name for the VLAN to `vlan_accounting`.
3. Select the *Internal* interface.
4. Enter the *VLAN ID*.

   The VLAN ID is a number between 1 and 4094 that allow groups of IP addresses with the same VLAN ID to be associated together.
5. Select the *Addressing Mode* of *Manual*.
6. Enter the IP address for the port of 10.13.101.101/24.
7. Set the *Administrative Access* to *HTTPS* and *SSH*.
8. Select *OK*.

**To add a VLAN - CLI**

```
config system interface
  edit VLAN_1
    set interface internal
    set type vlan
    set vlanid 100
    set ip 10.13.101.101/24
    set allowaccess https ssh
  next
end
```

## Zones

Zones are a group of one or more FortiGate interfaces, both physical and virtual, that you can apply security policies to control inbound and outbound traffic. Grouping interfaces and VLAN subinterfaces into zones simplifies the creation of security policies where a number of network segments can use the same policy settings and protection profiles. When you add a zone, you select the names of the interfaces and VLAN subinterfaces to add to the zone. Each interface still has its own address and routing is still done between interfaces, that is, routing is not affected by zones. Security policies can also be created to control the flow of intra-zone traffic.

For example, in the illustration below, the network includes three separate groups of users representing different entities on the company network. While each group has its own set of

FortiGate unit whether it is running in either NAT mode or transparent mode. The FortiManager unit provides remote management of a FortiGate unit over TCP port 541. 16542

If you have not already done so, register the FortiGate unit by visiting http://support.fortinet.com and select *Product Registration*. By registering your Fortinet unit, you will receive updates to threat detection and prevention databases (Antivirus, Intrusion Detection, etc.) and will also ensure your access to technical support.

You must enable the FortiGate management option so the FortiGate unit can accept management updates to firmware, antivirus signatures, and IPS signatures.

**To configure the FortiGate unit - web-based manager**

1. Log in to the FortiGate unit.
2. Go to *System* > *Admin* > *Settings*.
3. Enter the *IP address* for the FortiManager unit.
4. Select *Send Request*.

The FortiManager ID now appears in the Trusted FortiManager table.

As an additional security measure, you can also select *Registration Password* and enter a password to connect to the FortiManager.

**To configure the FortiGate unit - CLI**

```
config system central-management
    set fmg <ip_address>
end
```

To use the registration password enter:

```
execute central-mgmt register-device
    <fmg-serial-no><fmg-register-password><fgt-usrname><fgt-password>
```

### Configuring an SSL connection

An SSL connection can be configured between the two devices and an encryption level selected. Use the following CLI commands in the FortiGate CLI to configure the connection:

```
config system central-management
    set status enable
    set enc-algorithm {default | high | low}
end
```

The default encryption automatically sets high and medium encryption algorithms. Algorithms used for high, medium, and low follows openssl definitions:

- *High* - Key lengths larger than 128 bits, and some cipher suites with 128-bit keys.
  Algorithms are: DHE-RSA-AES256-SHA:AES256-SHA: EDH-RSA-DES-CBC3-SHA: DES-CBC3-SHA:DES-CBC3-MD5:DHE-RSA-AES128-SHA:AES128-SHA
- *Medium* - Key strengths of 128 bit encryption.
  Algorithms are: RC4-SHA:RC4-MD5:RC4-MD
- *Low* - Key strengths of 64 or 56 bit encryption algorithms but excluding export cipher suites
  Algorithms are: EDH-RSA-DES-CBC-SHA; DES-CBC-SHA; DES-CBC-MD5.

## FortiManager configuration

Once the connection between the FortiGate unit and the FortiManager unit has been configured, you can add the FortiGate to the Device Manager in the FortiManager unit's

Further options are available when enabled to configure log file sizes, and uploading/backup events.

As well, note that the write speeds of hard disks compared to the logging of ongoing traffic may cause the dropping such, it is recommended that traffic logging be sent to a FortiAnalyzer or other device meant to handle large volumes of data.

## Syslog server

An industry standard for collecting log messages, for off-site storage. In the web-based manager, you are able to send logs to a single syslog server, however in the CLI you can configure up to three syslog servers where you can also use multiple configuration options. For example, send traffic logs to one server, antivirus logs to another. The FortiGate unit sends Syslog traffic over UIDP port 514. Note that if a secure tunnel is configured for communication to a FortiAnalyzer unit, then Syslog traffic will be sent over an IPSec connection, using UPD 500/4500, protocol IP/50.

To configure a Syslog server in the web-based manager, go to *Log & Report* > *Log Config* > *Log Settings*. In the CLI use the commands:

```
config log syslogd setting
  set status enable
end
```

Further options are available when enabled to configure a different port, facility and server IP address.

For Syslog traffic, you can identify a specific port/IP address for logging traffic. Configuration of these services is performed in the CLI, using the command `set source-ip`. When configured, this becomes the dedicated port to send this traffic over.

For example, to set the source IP of a Syslog server to be on the DMZ1 port with an IP of 192.168.4.5, the commands are:

```
config log syslogd setting
  set status enable
  set source-ip 192.168.4.5
end
```

## FortiAnalyzer

The FortiAnalyzer family of logging, analyzing, and reporting appliances securely aggregate log data from Fortinet devices and other syslog-compatible devices. Using a comprehensive suite of easily-customized reports, users can filter and review records, including traffic, event, virus, attack, Web content, and email data, mining the data to determine your security stance and assure regulatory compliance. FortiAnalyzer also provides advanced security management functions such as quarantined file archiving, event correlation, vulnerability assessments, traffic analysis, and archiving of email, Web access, instant messaging and file transfer content.

The FortiGate unit sends log messages over UDP port 514 or OFTP (TCP 514). If a secure connection has been configured, log traffic is sent over UDP port 500/4500, Protocol IP/50. For more information on configuring a secure connection see "Sending logs using a secure connection" on page 141.

For FortiAnalyzer traffic, you can identify a specific port/IP address for logging traffic. Configuration of these services is performed in the CLI, using the command set `source-ip`. When configured, this becomes the dedicated port to send this traffic over.

3. Select *Create New* to add a VLAN subinterface.
4. Enter the following:

16544

| | |
|---|---|
| VLAN Name | VLAN_100 |
| Type | VLAN |
| Interface | internal |
| VLAN ID | 100 |
| Addressing Mod | Manual |
| IP/Netmask | 172.100.1.1/255.255.255.0 |
| Administrative Access | HTTPS, PING, TELNET |

5. Select *OK*.

To view the new VLAN subinterface, select the expand arrow next to the parent physical interface (the internal interface). This will expand the display to show all VLAN subinterfaces on this physical interface. If there is no expand arrow displayed, there are no subinterfaces configured on that physical interface.

For each VLAN, the list displays the name of the VLAN, and, depending on column settings, its IP address, the Administrative access you selected for it, the VLAN ID number, and which VDOM it belongs to if VDOMs are enabled.

**To add a VLAN subinterface in NAT mode - CLI**

```
config system interface
  edit VLAN_100
    set interface internal
    set type vlan
    set vlanid 100
    set ip 172.100.1.1 255.255.255.0
    set allowaccess https ping telnet
end
```

## Configuring security policies and routing

Once you have created a VLAN subinterface on the FortiGate unit, you need to configure security policies and routing for that VLAN. Without these, the FortiGate unit will not pass VLAN traffic to its intended destination. Security policies direct traffic through the FortiGate unit between interfaces. Routing directs traffic across the network.

### Configuring security policies

Security policies permit communication between the FortiGate unit's network interfaces based on source and destination IP addresses. Interfaces that communicate with the VLAN interface need security policies to permit traffic to pass between them and the VLAN interface.

Each VLAN needs a security policy for each of the following connections the VLAN will be using:

- from this VLAN to an external network
- from an external network to this VLAN
- from this VLAN to another VLAN in the same virtual domain on the FortiGate unit
- from another VLAN to this VLAN in the same virtual domain on the FortiGate unit.

The packets on each VLAN are subject to antivirus scans and other UTM measures as they pass through the FortiGate unit.

### Configuring routing

As a minimum, you need to configure a default static route to a gateway with access to an external network for outbound packets. In more complex cases, you will have to configure different static or dynamic routes based on packet source and destination addresses.

As with firewalls, you need to configure routes for VLAN traffic. VLANs need routing and a gateway configured to send and receive packets outside their local subnet just as physical interfaces do. The type of routing you configure, static or dynamic, will depend on the routing used by the subnet and interfaces you are connecting to. Dynamic routing can be routing information protocol (RIP), border gateway protocol (BGP), open shortest path first (OSPF), or multicast.

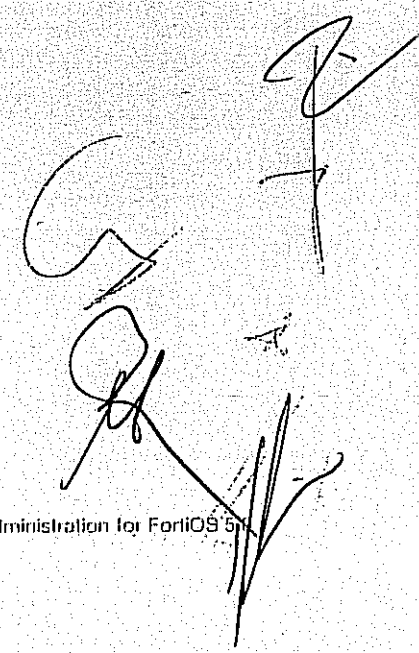
If you enable SSH, PING, Telnet, HTTPS and HTTP on the VLAN, you can use those protocols to troubleshoot your routing and test that it is properly configured. Enabling logging on the interfaces and using CLI diagnose commands such as `diagnose sniff packet <interface_name>` can also help locate any possible configuration or hardware issues.

## Example VLAN configuration in NAT mode

In this example two different internal VLAN networks share one interface on the FortiGate unit, and share the connection to the Internet. This example shows that two networks can have separate traffic streams while sharing a single interface. This configuration could apply to two departments in a single company, or to different companies.

There are two different internal network VLANs in this example. VLAN_100 is on the 10.1.1.0/255.255.255.0 subnet, and VLAN_200 is on the 10.1.2.0/255.255.255.0 subnet. These VLANs are connected to the VLAN switch, such as a Cisco 2950 Catalyst switch.

The FortiGate internal interface connects to the VLAN switch through an 802.1Q trunk. The internal interface has an IP address of 192.168.110.126 and is configured with two VLAN subinterfaces (VLAN_100 and VLAN_200). The external interface has an IP address of 172.16.21.2 and connects to the Internet. The external interface has no VLAN subinterfaces.



### Security policies

When creating security policies, you need to configure duplicate policies to ensure that after traffic fails over WAN1, regular traffic will be allowed to pass through WAN2 as it did with WAN1. This ensures that fail-over will occur with minimal affect to users. For more information on creating security policies see the *Firewall* Guide.

## Load sharing

Load sharing enables you to use both connections to the internet at the same time, but do not provide fail over support: When configuring for load sharing, you need to ensure routing is configured for both external ports, for example, WAN1 and WAN2, have static routes with the same distance and priority.

Further configuration can be done using Equal Cost Multiple Path (ECMP). For more information on ECMP and load sharing, see the *Advanced Routing* Guide.

## Link redundancy and load sharing

In this scenario, both links are available to distribute Internet traffic over both links. Should one of the interfaces fail, the FortiGate unit will continue to send traffic over the other active interface. Configuration is similar to the Redundant interfaces configuration, with the main difference being that the configured routes should have equal distance settings.

This means both routes will remain active in the routing table. To make one interface the preferred interface, use a default policy route to indicate the interface that is preferred for accessing the Internet. If traffic matches the security policy, the policy overrides all entries in the routing table, including connected routes. You may need to add a specific policy routes that override these default policy routes.

To redirect traffic over the secondary interface, create policy routes to direct some traffic onto it rather than the primary interface. When adding the policy route, only define the outgoing interface and leave the gateway blank. This ensures that the policy route will not be active when the link is down.

# Single firewall vs. multiple virtual domains

A typical FortiGate setup, with a small to mid-range appliance, enables you to include a number of subnets on your network using the available ports and switch interfaces. This can potentially provide a means of having three or more mini networks for the various groups in a company. Within this infrastructure, multiple network administrators have access to the FortiGate to maintain security policies.

However, the FortiGate unit may not have enough interfaces to match the number of departments in the organization. If the FortiGate unit it running in transparent mode however, there is only one interface, and multiple network branches through the FortiGate are not possible.

A FortiGate unit with Virtual Domains (VDOMs) enabled, provides a means to provide the same functionality in transparent mode as a FortiGate in NAT mode. VDOMs are a method of dividing a FortiGate unit into two or more virtual units that function as multiple independent units. VDOMs can provide separate security policies and, in NAT mode, completely separate configurations for routing and VPN services for each connected network. For administration, an administrator can be assigned to each VDOM, minimizing the possibility of error or fouling network communications.

To disable ping administrative access - CLI

```
config system interface
  edit external
    set allowaccess https
end
```

## Opening TCP 113

Although seemingly contrary to conventional wisdom of closing ports from hackers, this port, which is used for ident requests, should be opened.

Port 113 initially was used as an authentication port, and later defined as an identification port (see RFC 1413). Some servers may still use this port to help in identifying users or other servers and establish a connection. Because port 113 receives a lot of unsolicited traffic, many routers, including on the FortiGate unit, close this port.

The issue arises in that unsolicited requests are stopped by the FortiGate unit, which will send a response saying that the port is closed. In doing so, it also lets the requesting server know there is a device at the given address, and thus announcing its presence. By enabling traffic on port 113, requests will travel to this port, and will most likely, be ignored and never responded to.

By default, the ident port is closed. To open it, use the following CLI commands:

```
config system interface
  edit <port_name>
    set ident_accept enable
end
```

You could also further use port forwarding to send the traffic to a non-existent IP address and thus never have a response packet sent.

## Obfuscate HTTP responses

The FortiGate unit can obfuscate the HTTP responses from the FortiGate admin GUI and SSL-VPN servers. By default this option is not enabled. To obfuscate HTTP headers, use the following CLI command:

```
config system global
  set http-obfucate {none | header-only | modified | no-error}
end
```

Where:

`none` — do not hide the FortiGate web server identity.

`header-only` — hides the HTTP server banner.

`modified` — provides modified error responses.

`no-error` — suppresses error responses.

After the PPTP establishing a TCP connection with the PPTP server, the client sends a start control connection request message to establish a control connection. The server replies with a start control connection reply message. The client then sends a request to establish a call and sends an outgoing call request message. FortiOS assigns a Call ID (bytes 12-13 of the control message) that is unique to each PPTP tunnel. The server replies with an outgoing call reply message that carries its own Call ID in bytes 12-13 and the client's call ID in bytes 14-15. The pptp session helper parses the control connection messages for the Call ID to identify the call to which a specific PPP packet belongs. The session helper also identifies an outgoing call request message using the control message type field (bytes 8-9) with the value 7. When the session helper receives this message, it parses the control message for the call ID field (bytes 12-13). FortiOS translates the call ID so that it is unique across multiple calls from the same translated client IP. After receiving outgoing call response message, the session helper holds this message and opens a port that accepts GRE traffic that the PPTP server sends. An outgoing call request message contains the following parts:

- The protocol used for the outgoing call request message (usually GRE)
- Source IP address (PPTP server IP)
- Destination IP address (translated client IP)
- Destination port number (translated client call ID)

The session helper identifies an outgoing call reply message using the control message type field (bytes 8-9) with the value 8. The session helper parses these control messages for the call ID field (bytes 12-13) and the client's call ID (bytes 14-15). The session helper then uses the client's call ID value to find the mapping created for the other direction, and then opens a pinhole to accept the GRE traffic that the client sends.

An outgoing call reply message contains the following parts:

- Protocol used for the outgoing call reply message (usually GRE)
- Source IP address (PPTP client IP)
- Destination IP address (PPTP server IP)
- Destination port number (PPTP server Call ID)

Each port that the session opens creates a session for data traffic arriving in that direction. The session helper opens the following two data sessions for each tunnel:

- Traffic from the PPTP client to the server, using the server's call ID as the destination port
- Traffic from the PPTP server to the client, using the client's translated call ID as the destination port

The default timeout value of the control connection is 30 minutes. The session helper closes the pinhole when the data session exceeds the timeout value or is idle for an extended period.

## Remote shell session helper (rsh)

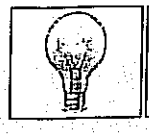
Using the remote shell program (RSH), authenticated users can run shell commands on remote hosts. RSH sessions most often use TCP port 514. To accept RSH sessions you must add a security policy with service set to any or to the RSH pre-defined service (which listens on TCP port number 514).

FortiOS automatically invokes the rsh session helper to process all RSH sessions on TCP port 514. The rsh session helper opens ports required for the RSH service to operate through a FortiGate unit running NAT or transparent and supports port translation of RSH traffic.

GRUPOTECNO

# Anexo Fortinet About the Maximum Values Table

# About the Maximum Values Table



The values in this table are the hard-coded maximum values. As such, they may not be practical limits for every situation and are not a promise of performance.

All objects in the maximum values table have either a global limit, which applies to the entire FortiGate configuration, or a VDOM limit, which applies only to a single VDOM. For objects that have only a VDOM limit, the global limit is the VDOM limit multiplied by the number of VDOMs for that unit. For example, the FortiGate60C can have 10 VDOMs and has a VDOM limit of 32 DHCP servers. This means that the global limit is 320.

By default, most FortiGate models support a maximum of 10 VDOMs in any combination of NAT/Route and Transparent operating modes. For FortiGate models 3000 and higher, a license key can be purchased to increase the maximum number.

The Maximum Values Table contains the values for FortiOS 5.2.4. For more information, see the Change Log.

If you wish to find out the complete maximum values for your FortiGate unit, use the following CLI command:

```
print tablesize
```

| LEGEND | |
|---|---|
| Black cells | Objects with global limits. |
| Gray cells | Objects with VDOM limits. |
| 0 | Objects with no hard limit, such as objects limited by system memory. |
| INT | Objects that are limited by the number of available interfaces. This number includes both physical and virtual interfaces. |
| - | Unsupported features. |
| * | An exception is listed at the bottom of this field for the limit. |

Models: Toggle All

| | | | |
|---|---|---|---|
| FortiGate VM (Evaluation Version) | FortiGate 200B series | FortiGate 800C & 900D | FortiGate 3600C |
| | | | FortiGate 3810A |
| FortiGate/FortiWiFi 20 series | FortiGate 200D series | FortiGate VM04 | FortiGate 3810D |
| FortiGate/FortiWiFi 30 series | FortiGate 300C, 300D, 310B-DC, 311B, 400D & 500D | FortiGate 1000C, 1240B, & 1500D | FortiGate 3000D, 3100D, 3700D, 3950B, 3951B, & VM08 |

16551

series

☐ FortiGate/FortiWiFi 30 series

☐ FortiGate/FortiWiFi 40C

☑ FortiGate/FortiWiFi 60 series (including FortiGate Rugged)

☐ FortiGate/FortiWiFi 70D & 90 series

☐ FortiGate/FortiWiFi 80 series

☐ FortiGate 100 series (including FortiGate Rugged)

☐ FortiGate VM00

series

☐ FortiGate 300C, 300D, 310B-DC, 311B, 400D & 500D

☐ FortiGate 310B

☐ FortiGate VM01

☐ FortiGate 600C & 600D

☐ FortiGate 620B-DC

☐ FortiGate 620B & 621B

☐ FortiGate VM02

VM04

☑ FortiGate 1000C, 1240B, & 1500D

☐ FortiGate 1000D

☐ FortiGate 1200D

☐ FortiGate 3016B

☐ FortiGate 3040B & 3140B

☐ FortiGate 3240C

☐ FortiGate 3810D

☐ FortiGate 3000D, 3100D, 3700D, 3950B, 3951B, & VM08

☐ FortiGate VM & VM64

☐ FortiGate 5001 series

☐ FortiGate 5101C & FortiController 5902D

☐ FortiSwitch 5203B

| OBJECT | | 60 series | 800C & 900D | 1000C, 1240B & 1500D |
|---|---|---|---|---|
| **SYSTEM** | | | | |
| Access profiles | | 8 | 16 | 64 |
| Admin accounts | | 300 | 300 | 300 |
| ARP | Proxy | 200 | 200 | 200 |
| | Table size | 2000 | 10240 | 16834 |
| Certificates | Local | 200 | 500 | 1000 |
| | CA | 200 | 200 | 500 |
| | CRL | 200 | 200 | 200 |
| Concurrent explicit proxy users | | 1000* | 16000 | 15000* |
| DHCP | Address ranges per server | 3 | 3 | 3 |
| | Exclude ranges per server | 4 | 16 | 16 |
| | Reserved addresses | 200 | 200 | 5000 |
| | Servers | 32 | 256 | 1024 |
| | | INT | INT | INT |
| Interfaces (VLAN + physical) | | 256 | 8192 | 8192 |
| | Transparent mode | 254 | 254 | 254 |
| | | 20 | 20 | 20 |
| IPv6 prefix lists per interface | | 32 | 32 | 32 |
| IPv6 tunnels | | 4 | 4 | 4 |
| MAC address table size | | 200 | 200 | 2000 |

| | | | | |
|---|---|---|---|---|
| | Hosts per community | 16 | 16 | 16 |
| | Users | 32 | 32 | 32 |
| VDOM links | | INT | INT | INT |
| WiFi MAC address list entries | | 0 | 0 | 0 |
| Zones | | 20 | 100 | 500 |
| **ROUTER** | | | | |
| Access lists | Entries | 32 | 100 | 100 |
| | Rules per entry | 128 | 256 | 512 |
| Authentication paths | | 0 | 0 | 0 |
| BGP | Aggregate addresses | 0 | 0 | 0 |
| | Confederation peers | 0 | 0 | 0 |
| | Neighbors | 1000 | 1000 | 5000 |
| | Networks | 0 | 0 | 0 |
| | Redistribution tables | 100 | 100 | 100 |
| | Routes | 0 | 0 | 0 |
| Community lists | | 64 | 512 | 2048 |
| Keychain | Entries | 16 | 16 | 100 |
| | Rules per entry | 20 | 20 | 20 |
| OSPF | Areas | 0 | 0 | 0 |
| | Area ranges | 0 | 0 | 0 |
| | Distribute lists | 10 | 10 | 10 |
| | Filter lists | 0 | 0 | 0 |
| | Interfaces | 0 | 0 | 0 |
| | Neighbours | 10 | 10 | 10 |
| | Networks | 0 | 0 | 0 |
| | Passive interfaces | 0 | 0 | 0 |
| | Redistribution tables | 100 | 100 | 100 |
| | Summary addresses | 25 | 25 | 25 |
| | Virtual links | 0 | 0 | 0 |
| Policy routes | | 250 | 512 | 2048 |
| Prefix lists | Entries | 32 | 100 | 100 |
| | Rules per entry | 64 | 64 | 64 |
| RIP | Distances | 100 | 100 | 100 |
| | Distribute lists | 100 | 100 | 100 |
| | Interfaces | 32 | 32 | 32 |
| | Neighbours | 100 | 100 | 100 |
| | Networks | 100 | 100 | 100 |
| | Offset lists | 32 | 32 | 32 |
| | Passive interfaces | 256 | 300 | 300 |
| | Redistribution tables | 100 | 100 | 100 |

| | | | | |
|---|---|---|---|---|
| Route | Maps | 100 | 100 | 100 |
| | Rules per map | 20 | 20 | 20 |
| Static routes | | 100 | 10000 | 10000 |
| Static routes (IPv6) | | 8 | 500 | 500 |
| **FIREWALL & FIREWALL OBJECTS** | | | | |
| Addresses | Addresses | 5000 | 10000 | 40000 |
| | Addresses per group | 300 | 300 | 1500 |
| | Address groups | 2500 | 2500 | 20000 |
| Central NAT table entries | | 256 | 1024 | 10000 |
| DNS translations | | 32 | 512 | 1024 |
| IP addresses per FQDN list | | 32 | 32 | 32 |
| IP pools | | 512 | 1024 | 2048 |
| IPv6 | Addresses | 5000 | 10000 | 40000 |
| | Address groups | 2500 | 8192 | 8192 |
| | Policies | 5000 | 10000 | 100000 |
| Multicast | Addresses | 512 | 1024 | 4096 |
| | Policies | 32 | 128 | 256 |
| NAT46 Policies | | 5000 | 10000 | 100000 |
| NAT64 Policies | | 5000 | 10000 | 100000 |
| Policies | Policies | 5000 | 10000 | 100000 |
| | Users/devices /groups per identity-based policy | 100 | 500 | 800 |
| Profile groups | | 32 | 500 | 20000 |
| Protocol options profiles | | 32 | 500 | 500 |
| Schedules | One-time | 256 | 256 | 256 |
| | Recurring | 256 | 256 | 256 |
| Services | Categories | 200 | 500 | 5000 |
| | Groups | 500 | 500 | 500 |
| | Members per group | 300 | 300 | 300 |
| | Services | 1024 | 1024 | 4096 |
| SSL/SSH/deep inspection options | | 32 | 500 | 500 |
| Traffic shaping | Per IP traffic shapers | 32 | 500 | 500 |
| | Traffic shapers | 32 | 500 | 500 |
| Virtual IPs | Groups | 500 | 500 | 500 |
| | IPv6 groups | 500 | 500 | 500 |
| | IPv6 virtual-IP mapping | 512 | 16384 | 32768 |
| | Load balancing monitors | 256 | 256 | 512 |
| | Load balancing virtual servers | 128 | 512 | 2048 |

| | | | | |
|---|---|---|---|---|
| | Members per group | 500 | 500 | 1024 |
| | NAT46 groups | 500 | 500 | 500 |
| | NAT46 virtual IP mapping | 512 | 16384 | 32768 |
| | NAT64 groups | 500 | 500 | 500 |
| | NAT64 virtual IP mapping | 512 | 16384 | 32768 |
| | Real servers per virtual server | 4 | 8 | 32 |
| | Virtual IP mapping (excluding load balance virtual servers) | 512 | 16384 | 32768 |
| **SECURITY PROFILES** | | | | |
| AntiVirus | Content Type | 10 | 1000 | 2000 |
| | Profiles | 32 | 500 | 500 |
| Application control sensors | | 32 | 64 | 1000 |
| Data leak prevention | Entries per file pattern | 20000 | 50000 | 250000 |
| | File patterns | 200 | 1000 | 5000 |
| | Filters per sensor | 100 | 2000 | 10000 |
| | Fingerprint sensitivity levels | 128 | 128 | 128 |
| | Sensors | 32 | 64 | 1000 |
| Intrusion prevention system | Custom signatures | 256 | 256 | 256 |
| | Sensors | 32 | 64 | 1000 |
| Vulnerability scan assets | | 200 | 2000 | 65535 |
| Spam filter | Banned word entries per list | 20000 | 50000 | 250000 |
| | Banned words lists | 10 | 1000 | 2000 |
| | Black/white list entries | 40000 | 100000 | 500000 |
| | Black/white lists | 20 | 2000 | 4000 |
| | DNS-based blackhole list entries | 20000 | 50000 | 250000 |
| | DNS-based blackhole lists | 10 | 1000 | 2000 |
| | MIME header list entries | 20000 | 50000 | 250000 |
| | >MIME header lists | 10 | 1000 | 2000 |
| | Profiles | 32 | 500 | 500 |
| | Trusted IP addresses list entries | 20000 | 50000 | 250000 |
| | Trusted IP addresses lists | 10 | 1000 | 2000 |

| | | | | |
|---|---|---|---|---|
| | Content block entries per list | 20000 | 50000 | 250000 |
| | Content block lists | 10 | 10 | 2000 |
| | Exempt word entries per list | 20000 | 50000 | 250000 |
| | Exempt word lists | 10 | 1000 | 2000 |
| | FortiGuard local categories | 52 | 52 | 52 |
| Web filter | FortiGuard local ratings | 2000 | 12000 | 12000 |
| | FortiGuard warnings | 50 | 400 | 400 |
| | Overrides | 50 | 400 | 400 |
| | Profile keyword matches | 64 | 64 | 64 |
| | Profiles | 32 | 20000 | 20000 |
| | URL Filters | 10 | 32 | 1000 |
| | URL filter entries | 20000 | 50000 | 250000 |

## VPN

| | | | | |
|---|---|---|---|---|
| | Concentrators | 500 | 500 | 500 |
| | Manual key configurations | 50 | 2000 | 2000 |
| | Phase 1 (Interface mode) | INT | INT | INT |
| IPsec | Phase 1 (Policy mode) | 200 | 2000 | 20000 |
| | Phase 2 (Interface mode) | INT | INT | INT |
| | Phase 2 (Policy mode) | 200 | 2000 | 20000 |
| | Tunnels per concentrator | 100 | 300 | 300 |
| | Bookmarks per portal | 256 | 256 | 256 |
| SSL | Bookmarks per user | 128 | 128 | 128 |
| | Portals | 10 | 50 | 256 |

## USER & DEVICE

| | | | |
|---|---|---|---|
| AD groups | 256 | 1024 | 8192 |
| Devices | 400 | 4000 | 16000 |
| Endpoint control profiles | 32 | 32 | 32 |
| FortiTokens | 100 | 1000 | 5000 |
| FSSO polling entries | 5 | 20 | 100 |
| FSSO servers | 5 | 5 | 5 |
| Guest users | 500 | 500 | 1024 |
| LDAP servers | 10 | 10 | 10 |
| Local users | 500 | 1000 | 5000 |

| | | | | |
|---|---|---|---|---|
| Members per user group | | 350 | 350 | 350 |
| Peers | | 500 | 1000 | 5000 |
| RADIUS | Accounting servers per RADIUS server | 4 | 4 | 4 |
| | Servers | 10 | 10 | 10 |
| TACACS+ servers | | 10 | 10 | 10 |
| User groups | | 100 | 500 | 800 |
| **WAN OPTIMIZATION & CACHE** | | | | |
| Authentication groups | | 16 | 64 | 128 |
| Peers | | 32 | 128 | 256 |
| Profiles | | 32 | 128 | 256 |
| SSL servers | | 32 | 128 | 256 |
| **WIRELESS CONTROLLER** | | | | |
| Custom AP profiles | | 128 | 128 | 128 |
| Custom AP profile MAC deny list entries | | 256 | 256 | 256 |
| Managed FortiAPs (Total / Tunnel Mode) | | 10 / 5 | 1024 / 512 | 4069 / 1024 |
| SSIDs | | 32 | 256 | 1024 |
| SSID lists per FortiAP | | 16 | 16 | 16 |
| WIDS profiles | | 256 | 256 | 256 |
| **LOG & REPORT** | | | | |
| Custom log fields per policy | | 5 | 5 | 5 |
| Reports | Body items per layout | 256 | 256 | 256 |
| | Charts | 256 | 256 | 320 |
| | Datasets | 256 | 256 | 320 |
| | Fields-per-datasets | 32 | 32 | 32 |
| | Footers per page per layout | 2 | 2 | 2 |
| | Headers per page per layout | 2 | 2 | 2 |
| | Layouts | 16 | 16 | 32 |
| | Mapping per chart | 8 | 8 | 8 |
| | Styles | 128 | 128 | 256 |
| | Summaries | 16 | 16 | 32 |
| | Themes | 8 | 8 | 16 |
| Threat Weight | Application-control settings | 32 | 32 | 32 |
| | Geolocation-based settings | 10 | 10 | 10 |
| | Web-based settings | 96 | 96 | 96 |

* Exception: FortiGate 60C-SFP has a concurrrent explicit proxy users limit of 500.

* Exception: the following models have a concurrrent explicit proxy users limit of 500: FortiGate 90D, FortiGate 92D, and FortiWiFi 92D.

* Exception: FortiGate 1240B and FortiGate 1500D have a concurrent explicit proxy users limit of 16000.

| CHANGE LOG | |
|---|---|
| Sept 25, 2015 | Initial release. |

LICITACIÓN PÚBLICA MIXTA NACIONAL NÚMERO **No. LA-009KCZ002-N49-2015** PARA EL ARRENDAMIENTO DEL "EQUIPO FIREWALL/VPN Y CONSOLA DE ADMINISTRACIÓN PARA EXPANSIÓN DE OFICINAS TELEGRÁFICAS DE LA RED TELDAT."

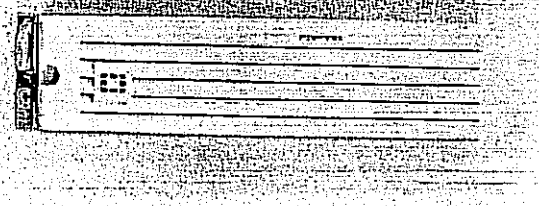
GRUPOTECNO

# Anexo FortiAnalyzer

FORTINET.

DATA SHEET

FortiAnalyzer
Centralized logging, analytics and reporting



# FortiAnalyzer

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

## Centralized logging, analytics and reporting

### Comprehensive Visualization of Your Network

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

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

### Key Features & Benefits

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

## Fortinet's Versatile Management Solution

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

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

Key tenets of Fortinet's management versatility:

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

16560

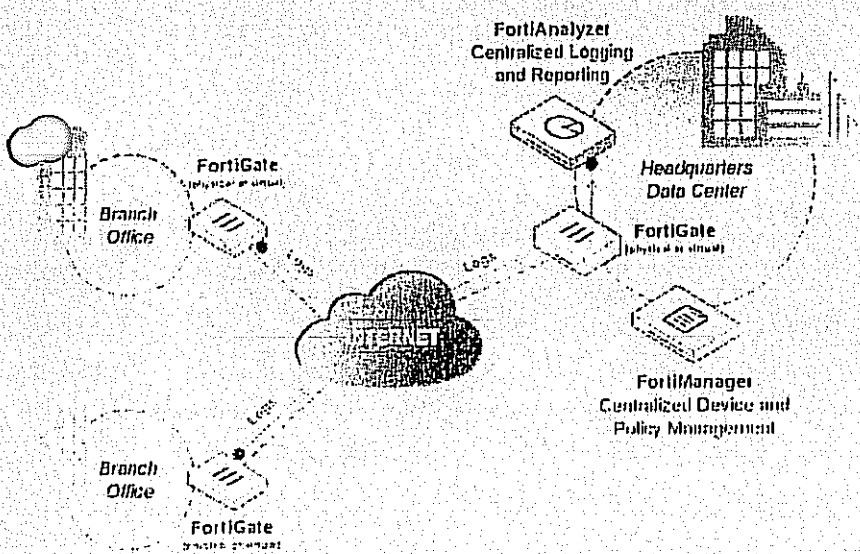
# HIGHLIGHTS

## Reporting and Visualization Tools

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

## JSON and XML (Web Services) APIs

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




## Log Viewer

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

## Event Management

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

## Better with FortiManager

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

## DLP Archiving

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

## FortiAnalyzer Supported Devices

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

16561

# SPECIFICATIONS

| | FORTIANALYZER 200D | FORTIANALYZER 300D | FORTIANALYZER 1000D | FORTIANALYZER 2000E |
|---|---|---|---|---|
| **Capacity and Performance** | | | | |
| GB/Day of Logs | 5 | 15 | 75 | 200 |
| Sustained Log Rate (Standalone Mode) | 120 | 200 | 350 | 1,500 |
| Peak Log Rate (Standalone Mode)* | 350 | 625 | 1,000 | 5,000 |
| Devices/VDOMs/ADOMs (Maximum) | 150 | 175 | 2,000 | 2,000 |
| **Hardware Specifications** | | | | |
| Form Factor | 1 RU Rackmount | 1 RU Rackmount | 2 RU Rackmount | 2 RU Rackmount |
| Total Interfaces | 4x GE | 4x GE | 6x GE, 2x GE SFP | 6x GE |
| Storage Capacity | 1 TB (1x 1 TB) | 4 TB (2x 2 TB) | 8 TB (4x 2 TB) | 4 TB (2x 2 TB – 12 TB maximum) |
| Removable Hard Drives | No | No | Yes | Yes |
| RAID Levels Supported | None | RAID 0/1 | RAID 0/1/5/10 | RAID 0/1/5/10/50 |
| Default RAID Level | – | 1 | 10 | 10 |
| Redundant Hot Swap Power Supplies | No | No | Yes | Yes |
| **Dimensions** | | | | |
| Height x Width x Length (inches) | 1.8 x 17.1 x 13.9 | 1.7 x 17.1 x 14.3 | 3.5 x 17.2 x 14.5 | 3.4 x 17.4 x 26.8 |
| Height x Width x Length (cm) | 4.5 x 43.3 x 35.2 | 4.4 x 43.5 x 36.4 | 9 x 43.8 x 36.8 | 8.6 x 44.3 x 68.1 |
| Weight | 13.4 lbs (6.1 kg) | 15.9 lbs (7.2 kg) | 30.6 lbs (13.9 kg) | 63 lbs (28.6 kg) |
| **Environment** | | | | |
| AC Power Supply | 100–240V AC, 50–60 Hz, 6 Amp Max. | 100–240V AC, 50–60 Hz, 4 Amp Max. | 100–240V AC, 50–60 Hz, 5 Amp Max. | 100–240V AC, 50–60 Hz, 9 Amp Max. |
| Power Consumption (Average) | 60 W | 162 W | 133 W | 200 W |
| Heat Dissipation | 205 BTU/h | 666 BTU/h | 546 BTU/h | 519 BTU/h |
| Operating Temperature | 32–104°F (0–40°C) | 50–95°F (10–35°C) | 32–104°F (0–40°C) | 50–95°F (10–35°C) |
| Storage Temperature | -13–158°F (-35–70°C) | -40–158°F (-40–70°C) | -13–158°F (-25–70°C) | -40–149°F (-40–65°C) |
| Humidity | 5–95% non-condensing | 8–90% non-condensing | 5–95% non-condensing | 5–95% non-condensing |
| Operating Altitude | Up to 7,400 ft (2,250 m) | Up to 7,400 ft (2,250 m) | Up to 7,400 ft (2,250 m) | Up to 7,400 ft (2,250 m) |
| **Compliance** | | | | |
| Safety Certifications | FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB | FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB | FCC Part 15 Class A, C-Tick, VCCI, CE, BSMI, UL/cUL, CB | FCC Part 15 Class A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST |

| | FORTIANALYZER 3000E | FORTIANALYZER 3500E | FORTIANALYZER 3900E |
|---|---|---|---|
| **Capacity and Performance** | | | |
| GB/Day of Logs | 800 | 3,000 | 4,000 |
| Sustained Log Rate (Standalone Mode) | 15,000 | 36,000 | 48,000 |
| Peak Log Rate (Standalone Mode)* | 50,000 | 60,000 | 75,000 |
| Devices/VDOMs/ADOMs (Maximum) | 4,000 | 4,000 | 4,000 |
| **Hardware Specifications** | | | |
| Form Factor | 2 RU Rackmount | 4 RU Rackmount | 2 RU Rackmount |
| Total Interfaces | 4x GE, 2x GE SFP | 2x GE, 2x GE SFP | 2x GE, 2x GE SFP+ |
| Storage Capacity | 16 TB (8x 2 TB) | 24 TB (12x 2 TB – 48 TB maximum) | 15 TB SSD (15x 1 TB SSD) |
| Removable Hard Drives | Yes | Yes | Yes |
| RAID Storage Management | RAID 0/1/5/6/10/50/60 | RAID 0/1/5/6/10/50/60 | RAID 0/1/5/6/10/50/60 |
| Default RAID Level | 10 | 10 | 10 |
| Redundant Hot Swap Power Supplies | Yes | Yes | Yes |
| **Dimensions** | | | |
| Height x Width x Length (inches) | 3.4 x 19 x 29.7 | 6.9 x 19.1 x 27.2 | 3.5 x 17.2 x 26.9 |
| Height x Width x Length (cm) | 8.7 x 48.2 x 75.5 | 17.5 x 48.5 x 69.0 | 8.9 x 43.7 x 68.4 |
| Weight | 71.5 lbs (32.5 kg) | 77 lbs (34.9 kg) | 52 lbs (23.6 kg) |
| **Environment** | | | |
| AC Power Supply | 100–240V AC, 50–60 Hz, 10 Amp Maximum | 100–240V AC, 50–60 Hz, 11.5 Amp Maximum | 100–240V AC, 50–60 Hz, 11.5 Amp Maximum |
| Power Consumption (Average) | 375.8 W | 465 W for 12 HDD | 470 W for 15 HDD |
| Heat Dissipation | 1947 BTU/h | 1904 BTU/h | 1637 BTU/h |
| Operating Temperature | 50–95°F (10–35°C) | 32–104°F (0–40°C) | 50–95°F (10–35°C) |
| Storage Temperature | -40–149°F (-40–65°C) | -13–158°F (-25–70°C) | -40–60°C (-40–140°F) |
| Humidity | 20–90% non-condensing | 10–90% non-condensing | 5–95% non-condensing |
| Operating Altitude | Up to 7,400 ft (2,250 m) | Up to 7,400 ft (2,250 m) | Up to 7,400 ft (2,250 m) |
| **Compliance** | | | |
| Safety Certifications | FCC Part 15 Class A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST | FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB | FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB |

* [illegible] can be [illegible]

16562

# SPECIFICATIONS

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

** Unlimited GB/Day when deployed in collector mode

# ORDER INFORMATION

| Product | SKU | Description |
|---|---|---|
| FortiAnalyzer 200D | FAZ-200D | Centralized log and analysis appliance — 4x GE RJ45, 1 TB storage, up to 5 GB/Day of logs. |
| FortiAnalyzer 300D | FAZ-300D | Centralized log and analysis appliance — 4x GE RJ45, 4 TB storage, up to 15 GB/Day of logs. |
| FortiAnalyzer 1000D | FAZ-1000D | Centralized log and analysis appliance — 6x GE RJ45, 2x SFP slots, 8 TB storage, up to 75 GB/Day of Logs. |
| FortiAnalyzer 2000B | FAZ-2000B-E03S | Centralized log and analysis appliance — 6x GE RJ45, 12 TB storage, dual power supplies, up to 200 GB/Day of Logs. |
| FortiAnalyzer 3000E | FAZ-3000E | Centralized log and analysis appliance — 4x GE RJ45, 2x GE SFP slots, 16 TB storage, dual power supplies, up to 800 GB/Day of Logs. |
| FortiAnalyzer 3500E | FAZ-3500E-E02S | Centralized log and analysis appliance — 2x GE RJ45, 2x GE SFP slots, 48 TB storage, dual power supplies, up to 3,000 GB/Day of Logs. |
| FortiAnalyzer 3900E | FAZ-3900E | Centralized log and analysis appliance — 2x GE RJ45, 2x 10 GE SFP+ slots, flash-based 15 TB SSD storage, dual power supplies, up to 4,000 GB/Day of Logs. |
| FortiAnalyzer VM Base | FAZ-VM-Base | Base license for stackable FortiAnalyzer-VM; 1 GB/Day of Logs and 200 GB storage capacity. Unlimited GB/Day when used in collector mode only. Designed for AWS, VMware vSphere, Xen, KVM and Hyper-V platforms. |
| FortiAnalyzer VM GB1 | FAZ-VM-GB1 | Upgrade license for adding 1 GB/Day of Logs and 200 GB storage capacity. |
| FortiAnalyzer VM GB5 | FAZ-VM-GB5 | Upgrade license for adding 5 GB/Day of Logs and 1 TB storage capacity. |
| FortiAnalyzer VM GB25 | FAZ-VM-GB25 | Upgrade license for adding 25 GB/Day of Logs and 8 TB storage capacity. |
| FortiAnalyzer VM GB100 | FAZ-VM-GB100 | Upgrade license for adding 100 GB/Day of Logs and 16 TB storage capacity. |

FORTINET

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

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

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

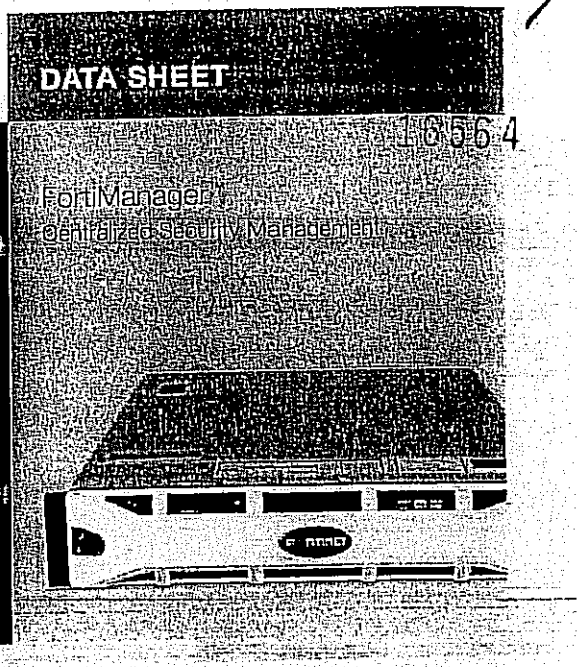
LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480

GRUPOTECNO

# Anexo FortiManager

FORTINET

DATA SHEET




# FortiManager

FortiManager 200D, 300D, 1000D, 3900E, 4000E and Virtual Appliances

## Centralized Security Management

### Take Control of Your Security Infrastructure

The FortiManager family delivers the versatility you need to effectively manage your Fortinet-based security infrastructure. FortiManager drastically reduces management costs, simplifies configuration, and accelerates deployment cycles, whether you are deploying new devices, installing security policies, or Virdistributing updates.

FortiManager also provides crucial timesaving features like device auto-discovery, group management, global policies, auditing facilities, and the ability to manage complex VPN environments. FortiManager, coupled with the FortiAnalyzer™ family of centralized logging and reporting appliances, provides a comprehensive and powerful centralized management solution for your organization.

## Key Features & Benefits

| | |
|---|---|
| Integrated FortiAnalyzer Logging | This allows for a tighter integration and correlation of events and policies. A consolidated platform allows customers to more easily deploy Fortinet management products. |
| Hierarchical Objects Database | Facilitates reuse of common configurations across the organization in both local and global ADOM levels. |
| Automated Device Provisioning/ Centralized Policy Configuration | Reduces cost of deploying new FortiGate or FortiClient installations and maintains policies across all managed assets. |
| Role-Based Administration | Enables distributed administration, an important requirement for larger organizations. |
| Policy/Device Auditing | Allows you to prove compliance, and track any deviations from the required security policy. |
| In-View Policy Object Editing | Faster rulebase editing without opening new windows or changing context. |
| Device Profiles | Aids in mass provisioning of managed devices. |

## Fortinet's Versatile Management Solution

Networks are constantly evolving due to threats, organizational growth or new regulatory/business requirements. Traditional management products focus on mitigating company-wide threats through firewall policies, firmware updates and keeping content security current.

FortiManager offers enterprise class features to contain these threats, but also provides flexibility to evolve along with your ever-changing network. In addition to being able to manage hundreds or even thousands of FortiGate devices, FortiManager now includes basic FortiAnalyzer logging and reporting functions for administrators who prefer a consolidated management platform.

Key tenets of Fortinet's management versatility:

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

16565

# HIGHLIGHTS

## Administrative Domains (ADOMs) and Global Policy

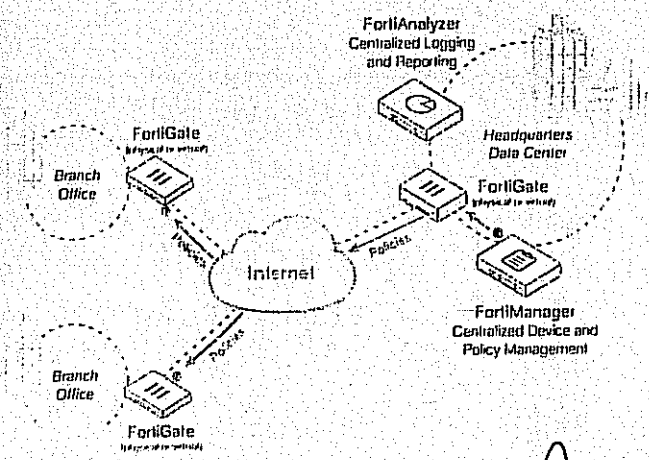
Enables a primary administrator to create groups of devices for other administrators to monitor and manage:

- Administrators can manage devices in their geographic location or business division
- Multiple FortiGate virtual domains (VDOMs) can be divided among multiple ADOMs
- Granular permissions allow assigning ADOMs and policies to particular users
- Administrators can only access devices or VDOMs assigned to them
- Create device configuration templates to quickly configure a new Fortinet appliance
- Within each ADOM, there is a common database of objects shared by all devices and policy packages allowing users to reuse similar configurations among a group of managed assets
- Global Policy capabilities are available on all FortiManager hardware models and virtual machines

## Fortinet Developer Network (FNDN)

Access tools, sample code, documentation and interact with the Fortinet developer community by subscribing to the Fortinet Developer Network.

Note: With the purchase of a FortiManager 1000 series or above, customers receive a complimentary 90 day trial access to FNDN.




## JSON and XML (Web Services) APIs

- JSON API — Allows MSSPs/large enterprises to create customized, branded web portals for policy and object administration
- XML API — Enables administrators to automate common tasks such as provisioning new FortiGates and configuring existing devices

## Locally Hosted Security Content

Hosting security content locally allows the administrator greater control over security content updates and provides improved response time for rating databases. Includes support for:

- Antivirus definition updates
- Intrusion Prevention updates
- Vulnerability and Compliance Management updates
- Web Filtering (select systems)
- Antispam (select systems)

## Command and Control

- Manage devices and endpoint agents individually or as logical groups
- Update device firmware
- Discover new devices automatically
- Create, deploy, and monitor virtual private networks
- Delegate control to other users with distributed administration features
- Audit configuration changes to ensure compliance

## Monitor, Analyze and Report

- Access vital security and network statistics
- Real-time monitoring and integrated basic reporting provide visibility into network and user activity
- For more powerful analytics, combine with a FortiAnalyzer appliance for additional data mining and graphical reporting capabilities

## FortiManager Supported Devices

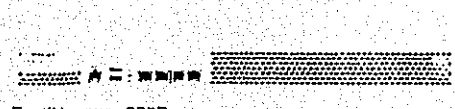
- FortiGate and FortiCarrier Consolidated Security Appliances
- FortiAP Wireless Access Points
- FortiMail Messaging Security Systems
- FortiWeb Web Application Security
- FortiAnalyzer Reporting and Analysis Appliances
- FortiSwitch Switching Platforms
- FortiSandbox Advanced Threat Protection Appliances

# SPECIFICATIONS

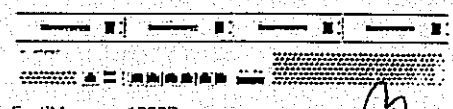
| FORTIMANAGER APPLIANCES | FORTIMANAGER 200D | FORTIMANAGER 300D | FORTIMANAGER 1000D | FORTIMANAGER 3900E | FORTIMANAGER 3000E |
|---|---|---|---|---|---|
| **Capacity and Performance** | | | | | |
| Devices/VDOMs (Maximum)[1] | 30 | 300 | 1,000 | 10,000 | 4,000 |
| GB/Day of Logs | 2 | 2 | 2 | 10 | 10 |
| **Hardware Specifications** | | | | | |
| Hardware Form Factor | 1 RU Rackmount | 1 RU Rackmount | 2 RU Rackmount | 2 RU Rackmount | 2 RU Rackmount |
| Total Interfaces | 4x GE | 4x GE | 6x GE, 2x GE SFP | 2x GE, 2x GE SFP+ | 4x GE, 2x GE SFP |
| Console Port | RJ45 | RJ45 | RJ45 | DB-9 | DB-9 |
| LCD Display | No | No | No | Yes | Yes |
| Storage Capacity | 1 TB (1x 1 TB) | 4 TB (2x 2 TB) | 8 TB (4x 2 TB) | 15 TB SSD (15x 1 TB SSD) | 16 TB (8x 2 TB) |
| Removable Hard Drives | No | No | Yes | Yes | Yes |
| RAID Levels Supported | None | RAID 0/1 | RAID 0/1/5/10 | RAID 0/1/5/6/10/50/60 | RAID 0/1/5/6/10/50/60 |
| High Availability Support | Yes | Yes | Yes | Yes | Yes |
| Redundant Hot Swap Power Supplies | No | No | Yes | Yes | Yes |
| **Dimensions** | | | | | |
| Height x Width x Length (inches) | 1.8 x 17.1 x 13.9 | 1.7 x 17.1 x 14.3 | 3.5 x 17.1 x 14.5 | 3.5 x 17.2 x 26.9 | 3.4 x 19 x 29.7 |
| Height x Width x Length (cm) | 4.5 x 43.4 x 35.2 | 4.4 x 43.4 x 36.4 | 9 x 43.4 x 36.8 | 8.9 x 43.7 x 68.4 | 8.7 x 48.2 x 75.5 |
| Weight | 13.4 lbs (6.1 kg) | 15.9 lbs (7.2 kg) | 30.6 lbs (13.9 kg) | 52 lbs (23.6 kg) | 71.5 lbs (32.5 Kg) |
| **Environment** | | | | | |
| AC Power Supply | 100–240V AC, 50–60 Hz, 6 Amp Maximum | 100–240V AC, 50–60 Hz, 4.0 Amp Maximum | 100–240V AC, 50–60 Hz, 5 Amp Maximum | 100–240V AC, 50–60 Hz, 10 Amp Maximum | 100–240V AC, 50–60 Hz, 10 Amp Maximum |
| Power Consumption (Average / Maximum) | 60 W / 72 W | 162 W / 172 W | 133 W / 160 W | 391 W / 470 W | 376 W / 561 W |
| Heat Dissipation | 205 BTU/h | 666 BTU/h | 546 BTU/h | 1637 BTU/h | 1947 BTU/h |
| Operating Temperature | 32–104°F (0–40°C) | 50–95°F (10–35°C) | 32–104°F (0–40°C) | 50–95°F (10–35°C) | 50–95°F (10-35°C) |
| Storage Temperature | -13–158°F (-25–70°C) | -40–158°F (-40–70°C) | -13–158°F (-25–70°C) | -40–140°F (-40–60°C) | -40–149°F (-40–65°C) |
| Humidity | 5–95% non-condensing | 8–90% non-condensing | 5–95% non-condensing | 5–95% (non-condensing) | 20–90% non-condensing |
| Operating Altitude | Up to 7,400 ft (2,250 m) | Up to 7,400 ft (2,250 m) | Up to 7,400 ft (2,250 m) | Up to 7,400 ft (2,250 m) | Up to 7,400 ft (2,250 m) |
| **Compliance** | | | | | |
| Safety Certifications | FCC Class A Part 15, UL/CB/cUL, C-Tick, VCCI, CE | FCC Class A Part 15, UL/CB/cUL, C-Tick, VCCI, CE | FCC Class A Part 15, C-Tick, VCCI, CE, BSMI, UL/CB/cUL | FCC Part 15 Class A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST | FCC Part 15 Class A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST |

| FORTIMANAGER VIRTUAL APPLIANCES | FMG-VM-BASE | FMG-VM-10-UG | FMG-VM-100-UG | FMG-VM-1000-UG | FMG-VM-5000-UG | FMG-VM-U-UG |
|---|---|---|---|---|---|---|
| **Capacity** | | | | | | |
| Devices/VDOMs (Maximum)[1] | 10 | +10 | +100 | +1,000 | +5,000 | Unlimited[2] |
| Storage Capacity[3] | 100 GB | 200 GB | 1 TB | 4 TB | 8 TB | 16 TB |
| GB/Day of Logs[3] | 1 | 2 | 5 | 10 | 25 | 50 |
| **Virtual Machine** | | | | | | |
| Hypervisor Support | VMware ESX/ESXi 4.0/4.1/5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2 / 2012, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS) | | | | | |
| vCPU Support (Minimum / Maximum) | 1 / Unlimited | | | | | |
| Network Interface Support (Minimum / Maximum) | 1 / 4 | | | | | |
| Storage Support (Minimum / Maximum) | 80 GB / 16 TB | | | | | |
| Memory Support (Minimum / Maximum) | 1 GB / 4 GB for 32-bit and 2 GB / Unlimited for 64-bit | | | | | |
| High Availability Support | Yes | | | | | |

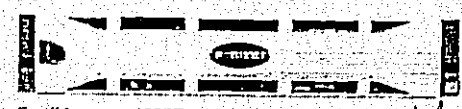
1. One Virtual Domain (VDOM) counting as 1 device or when device counts as one (1) managed network device
2. Limited in software to 10,000 devices/VDOMs
3. Storage Capacity and GB/Day of Logs are not enforced. These values represent the maximum available with technical support



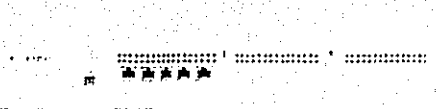
FortiManager 200D



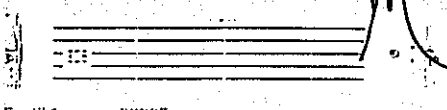
FortiManager 1000D



FortiManager 4000E



FortiManager 300D



FortiManager 3900E

FortiManager Virtual Appliance

16567

# FEATURES

| | LOCALLY HOSTED SECURITY CONTENT | | | | | MISCELLANEOUS FEATURES | | |
|---|---|---|---|---|---|---|---|---|
| | AntiVirus | Intrusion Prevention | Vulnerability Management | Web Filtering | Antispam Databases | Shelf Manager | VM Activation/ Closed Network Mode | Global Policies |
| FortiManager 200D | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| FortiManager 300D | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| FortiManager 1000D | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| FortiManager 3900E | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| FortiManager 4000E | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| FortiManager VM Base | Yes | Yes | Yes | No | No | No | Yes | Yes |
| FortiManager VM Base + FMG-VM-10-UG | Yes | Yes | Yes | No | No | No | Yes | Yes |
| FortiManager VM Base + FMG-VM-100-UG | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| FortiManager VM Base + FMG-VM-1000-UG | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| FortiManager VM Base + FMG-VM-5000-UG | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| FortiManager VM Base + FMG-VM-U-UG | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

# ORDER INFORMATION

| ADDITIONAL FORTIMANAGER ITEMS | |
|---|---|
| SKU | Description |
| FMG-200D | Centralized management, log and analysis appliance — 4x GE RJ45, 1 TB storage, manages up to 30 Fortinet network devices/administrative domains, up to 2 GB/day of logs. |
| FMG-300D | Centralized management, log and analysis appliance — 4x GE RJ45, 4 TB storage, manages up to 300 Fortinet devices/administrative domains, up to 2 GB/day of logs. |
| FMG-1000D | Centralized management, log and analysis appliance — 6x GE RJ45, 2x SFP slots, 8 TB storage, manages up to 1,000 Fortinet devices/administrative domains, up to 2 GB/day of logs. |
| FMG-3900E | Centralized management, log and analysis appliance — 2x GE RJ45, 2x 10 GE SFP+ slots, flash-based 15 TB SSD storage, dual power supplies, manages up to 10,000 Fortinet devices/ administrative domains, up to 10 GB/day of Llogs. |
| FMG-4000E | Centralized management, log and analysis appliance — 4x GE RJ45, 2x GE SFP slots, 16 TB storage, dual power supplies, manages up to 4,000 Fortinet devices/administrative domains, up to 10 GB/day of logs. |

| ADDITIONAL FORTIMANAGER ITEMS | |
|---|---|
| SKU | Description |
| FC-10-FNDN1-139-01-12 | 1 Year Subscription for 1-User to Fortinet Developer Network |
| FC-10-FNDN2-139-02-12 | 1 Year Subscription for Unlimited Users to Fortinet Developer Network |

| FORTIMANAGER VIRTUAL APPLIANCES | | |
|---|---|---|
| SKU | Licensed Network Devices (Maximum) | Description |
| Built-In Evaluation | 10 | Built-in 15-day EVAL license, no activation required. |
| Evaluation (60-days) | 10,000 | EVAL license. License and activation required. |
| FMG-VM-Base | 10 | Base license for stackable FortiManager VM. Manages up to 10 FortiGate devices/Administrative Domains, 1 GB/day of logs and 100 GB device quota. Designed for AWS, VMware vSphere and Microsoft Hyper-V platforms. |
| FMG-VM-10-UG | +10 | Upgrade license for adding 10 FortiGate devices/Administrative Domains; allows for total of 2 GB/day of logs and 200 GB device quota. |
| FMG-VM-100-UG | +100 | Upgrade license for adding 100 FortiGate devices/Administrative Domains; allows for total of 5 GB/day of logs and 1 TB device quota. |
| FMG-VM-1000-UG | +1,000 | Upgrade license for adding 1,000 FortiGate devices/Administrative Domains; allows for total of 10 GB/day of logs and 4 TB device quota. |
| FMG-VM-5000-UG | +5,000 | Upgrade license for adding 5,000 FortiGate devices/Administrative Domains; allows for total of 25 GB/day of logs and 8 TB device quota. |
| FMG-VM-U-UG | Unrestricted | Upgrade license for adding unlimited FortiGate devices/Administrative Domains; allows for total of 50 GB/day of logs and 16 TB device quota. |

* Unlimited when CPU, Memory and Hard Disk are to the operating system limit of 4 GB (32-bit) / Unlimited (64-bit)
Limited to software to 10,000 devices/ADOMs

FORTINET

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

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

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

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

LICITACIÓN PÚBLICA MIXTA NACIONAL NÚMERO **No. LA-009KCZ002-N49-2015** PARA EL ARRENDAMIENTO DEL "EQUIPO FIREWALL/VPN Y CONSOLA DE ADMINISTRACIÓN PARA EXPANSIÓN DE OFICINAS TELEGRÁFICAS DE LA RED TELDAT."

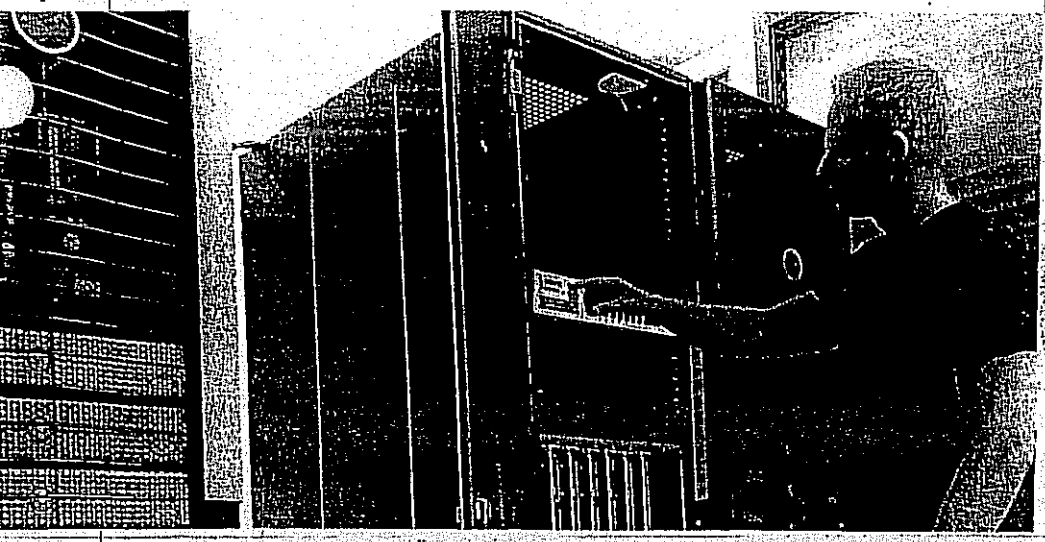
16568

GRUPOTECNO

# Anexo FortiGate-900D

FORTINET

DATA SHEET



FortiGate® 900D

High Performance Enterprise Firewall for Large Branch Offices

16569

# FortiGate 900D

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

## 5 Times Next Generation Firewall Performance

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

## Deeper Visibility and Top-rated Security

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

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

## Highlights

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

## Features & Benefits

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

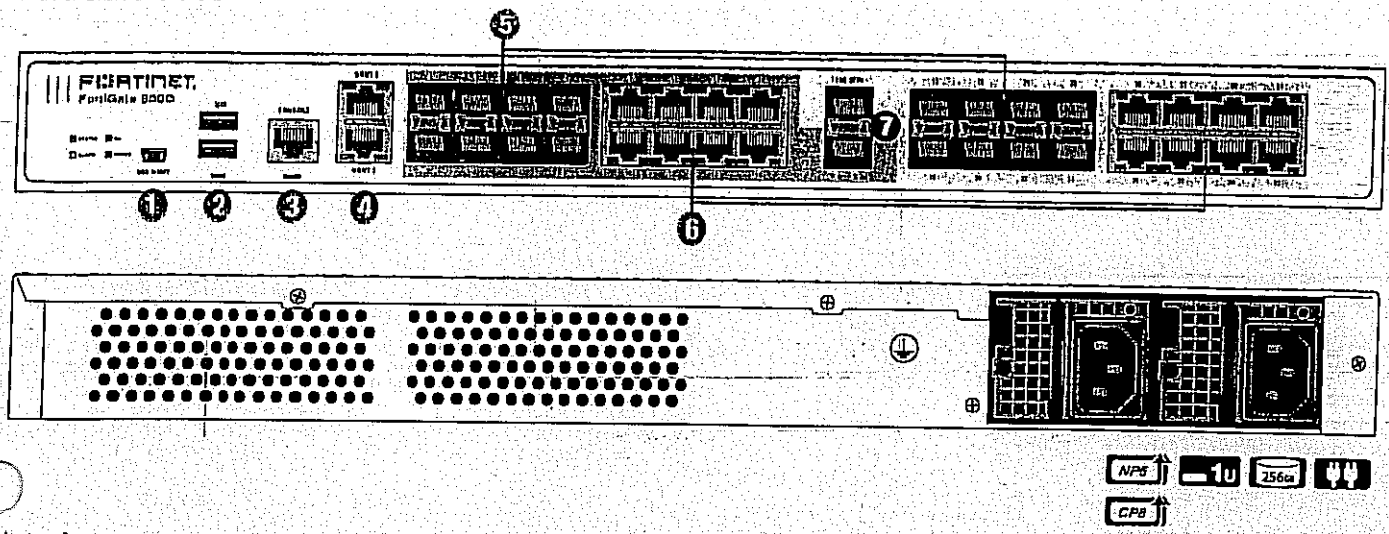
NSS labs NSS labs NSS labs

NSS labs NSS labs

# HARDWARE

16570

## FortiGate 900D




NP6 1U 256GB CP8

### Interfaces

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


## Powered by FortiASICs

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

## Network Processor

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

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

## Content Processor

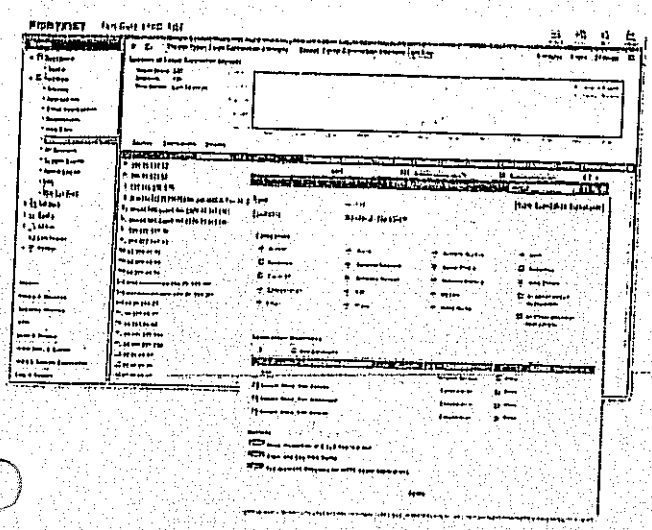
The FortiASIC CP8 content processor works outside of the direct flow of traffic, providing high-speed cryptography and content inspection services including:

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

## 10 GE Connectivity

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

SOFTWARE



FortiOS Managment UI — FortiView and Application Control Panel

## FortiOS

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

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

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

# SERVICES

## FortiGuard™ Security Services

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

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

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

## FortiCare™ Support Services

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

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

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

# SPECIFICATIONS

16572

| FORTIGATE 9000 | |
|---|---|
| **Interfaces and Modules** | |
| Hardware Accelerated 10 GE SFP+ Slots | 2 |
| Hardware Accelerated GE SFP Slots | 16 |
| Hardware Accelerated GE RJ45 Ports | 16 |
| GE RJ45 Management / HA Ports | 2 |
| USB Ports (Client / Server) | 1 / 2 |
| Console Port | 1 |
| Onboard Storage | 256 GB |
| Included Transceivers | 0 |
| **System Performance and Capacity** | |
| IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP) | 52 / 52 / 33 Gbps |
| IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP) | 52 / 52 / 33 Gbps |
| Firewall Latency (64 byte, UDP) | 3 µs |
| Firewall Throughput (Packet per Second) | 49.5 Mpps |
| Concurrent Sessions (TCP) | 11 Million |
| New Sessions/Second (TCP) | 280,000 |
| Firewall Policies | 100,000 |
| IPsec VPN Throughput (512 byte) | 25 Gbps |
| Gateway-to-Gateway IPsec VPN Tunnels | 2,000 |
| Client-to-Gateway IPsec VPN Tunnels | 10,000 |
| SSL-VPN Throughput | 3.6 Gbps |
| Concurrent SSL-VPN Users (Recommended Maximum) | 10,000 |
| IPS Throughput | 8 Gbps |
| Antivirus Throughput | 3.5 Gbps |
| CAPWAP Clear-text Throughput (HTTP) | 8 Gbps |
| Virtual Domains (Default / Maximum) | 10 / 10 |
| Maximum Number of FortiAPs (Total / Tunnel) | 1024 / 512 |
| Maximum Number of FortiTokens | 1,000 |
| Maximum Number of Registered Endpoints | 2,000 |
| High Availability Configurations | Active-Active, Active-Passive, Clustering |

| FORTIGATE 9000 | |
|---|---|
| **Dimensions and Power** | |
| Height x Width x Length (inches) | 1.74 x 17.22 x 18.24 |
| Height x Width x Length (mm) | 44.2 x 437.5 x 463.2 |
| Weight | 20.24 lbs (9.18 kg) |
| Form Factor | 1 RU |
| AC Power Supply | 100–240V AC, 60–50 Hz, 300 W Redundant |
| Power Consumption (Average / Maximum) | 135 W / 187.2 W |
| Current (Maximum) | 100V/5A, 240V/3A |
| Heat Dissipation | 638.75 BTU/h |
| Redundant Power Supplies | Yes |
| **Operating Environment and Certifications** | |
| Operating Temperature | 32–104°F (0–40°C) |
| Storage Temperature | -31–158°F (-35–70°C) |
| Humidity | 20–90% non-condensing |
| Operating Altitude | Up to 7,400 ft (2,250 m) |
| Compliance | FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB |
| Certifications | ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN |

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

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

# ORDER INFORMATION

| Product | SKU | Description |
|---|---|---|
| FortiGate 9000 | FG-9000 | 2x 10 GE SFP+ slots, 16x GE SFP slots, 16x GE RJ45 ports, 2x GE RJ45 Management ports, FortiASIC NP6 and CP8 hardware accelerated, 1x 256 GB SSD onboard storage, dual AC power supplies |
| **Optional Accessories/Spares** | **SKU** | **Description** |
| 1 GE SFP LX Transceiver Module | FG-TRAN-LX | 1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots |
| 1 GE SFP RJ45 Transceiver Module | FG-TRAN-GC | 1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots |
| 1 GE SFP SX Transceiver Module | FG-TRAN-SX | 1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots |
| 10 GE SFP+ Transceiver Module, Short Range | FG-TRAN-SFP+SR | 10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots |
| 10 GE SFP+ Transceiver Module, Long Range | FG-TRAN-SFP+LR | 10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots |
| 10 GE SFP+ Active Direct Attach Cable, 10m / 32.8 ft | SP-CABLE-ADASFP+ | 10 GE SFP+ active direct attach cable, 10m / 32.8 ft for all systems with SFP+ and SFP/SFP+ slots |
| AC Power Supply | SP-FXX1000D | AC power supply for FG-9000, FG-10000 and FXX-10000 |

FORTINET

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

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

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

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

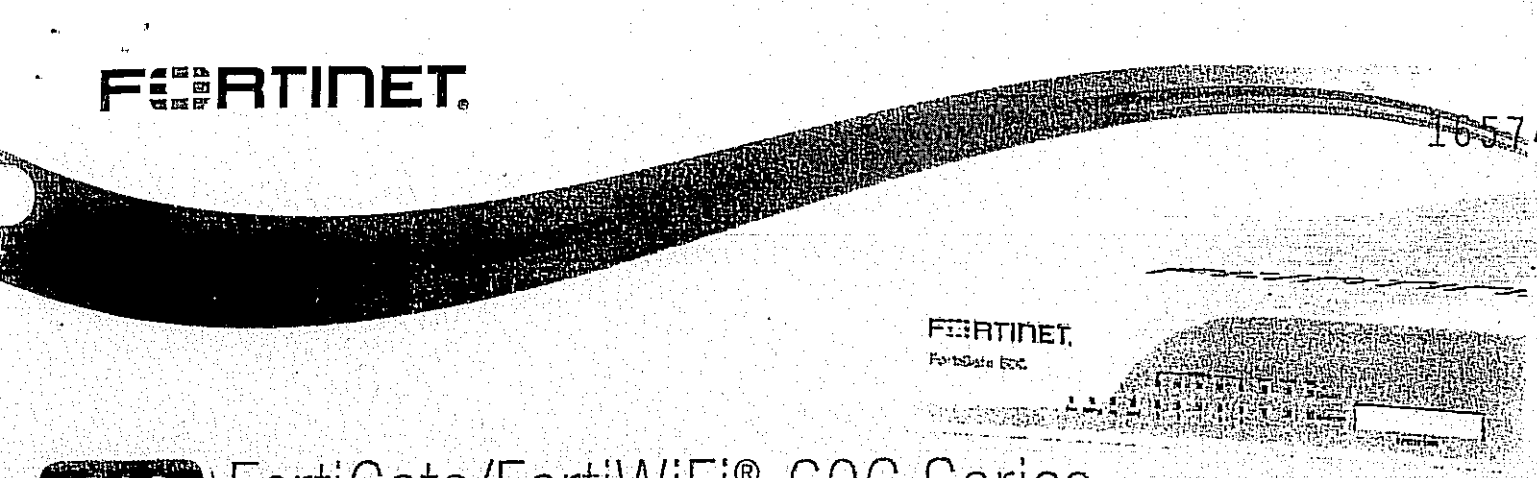
GRUPOTECNO

# Anexo FortiGate-60C

00135

FORTINET

16574




# FortiGate/FortiWiFi®-60C Series

## Integrated Threat Management for Small Networks

The FortiGate/FortiWiFi-60C Series are compact, all-in-one security appliances that deliver Fortinet's Connected UTM. Ideal for small business, remote, customer premise equipment (CPE) and retail networks, these appliances offer the network security, connectivity and performance you need at a single low per-device price..

**Advanced Protection and Wireless Connectivity**

You get advanced threat protection, including firewall, application control, advanced threat protection, IPS, VPN, and web filtering, all from one device that's easy to deploy and manage. With our FortiGuard® security subscription services you'll have automated protection against today's sophisticated threats.

Reduce the need for additional wireless access points by integrating a high-bandwidth "fat-client" into your FortiGate with the FortiWiFi-60C. It's also a great option to secure mobile devices in BYOD environments with automatic device identification and customizable access and security policies.

VDOMs on the FortiGate/FortiWiFi-60C, let you segment networks to enable guest and employee access, or protect things like cardholder data. You get the flexibility to match your business needs and meet compliance standards like PCI and HIPAA.

**All-in-one High Performance Network Security**

Built on the foundation of the FortiASIC System on a Chip (SoC) and FortiOS 5, the FortiGate-60C series provides an integrated set of essential security technologies to protect all of your applications and data. You get the industry's best firewall plus the latest in Advanced Threat Protection, Intrusion Protection, Web-filtering and many new features like Sandboxing, Feature Select Options for simplifying configurations and deployments, and Contextual Visibility for enhanced reporting and management.

### *Enterprise-Class Protection that's Easy to Deploy and Manage*

- 1 Gbps throughput performance ensures your network security won't be a bottleneck
- Integrated switch and options for PoE simplify your network infrastructure
- Up to 2x WAN, 5x LAN and 1x DMZ interface ports (24x Power Over Ethernet ports on POE model)
- Runs on FortiOS 5 – the most powerful security operating system in the world delivers more protection for fighting advanced threats, more control to simplify configurations and deployments, and more contextual visibility for enhanced reporting and management

ICSA labs

ICSA labs ICSA labs

ICSA labs ICSA labs

## Key Features & Benefits

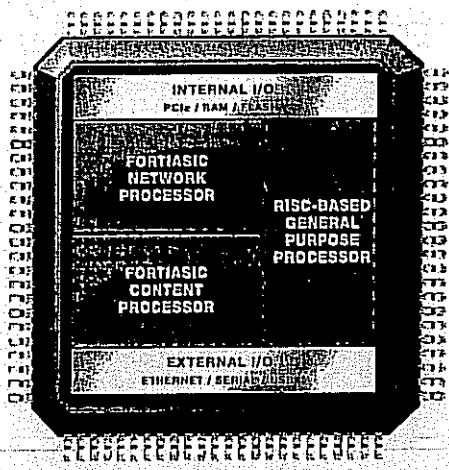
| | |
|---|---|
| Unified Security | Multi-threat protection from a single device increases security and lowers costs |
| Simplified Licensing | Unlimited user licensing and comprehensive features |
| Multi-Port Interfaces | Multiple network interfaces and optional wireless connectivity enable data segmentation for compliance and flexible deployment |

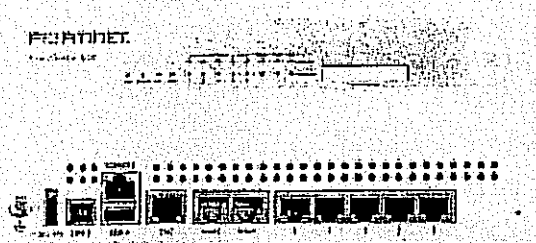
16575

## The Fortinet FS1 System-on-a-Chip

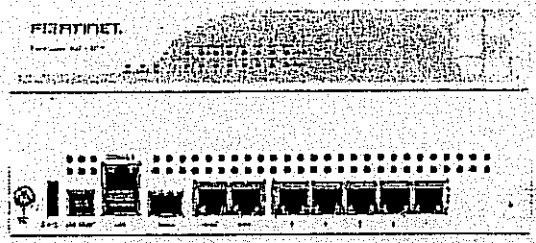
The FortiGate/FortiWiFi-60C series represent a new generation of desktop network security appliances from Fortinet, and include the first Fortinet System-on-a-chip (SoC), the FS1. Integrating FortiASIC acceleration logic together with a RISC-based main processor and other system components, the FS1 SoC simplifies appliance design and enables breakthrough performance for smaller networks.

The FS1 and resulting FortiGate/FortiWiFi-60C series appliances allow large distributed enterprises to provide integrated, multi-threat protection across all points on their network without sacrificing performance.

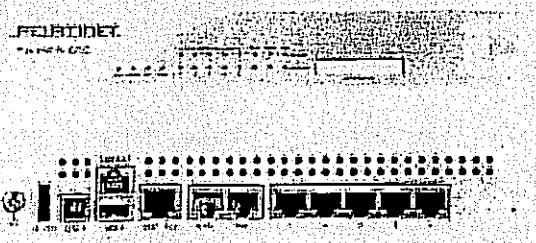


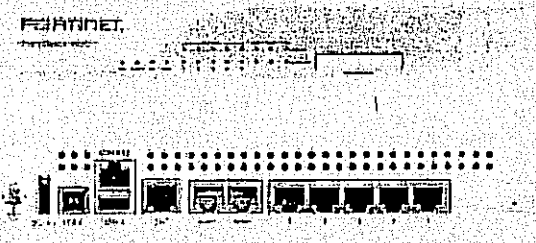
FortiGate-60C



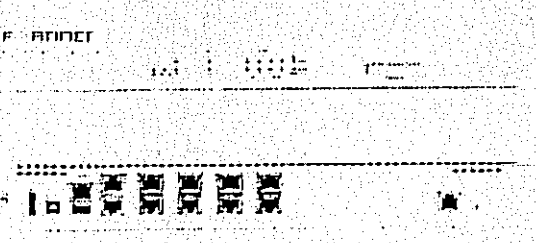
FortiGate-60C-SFP



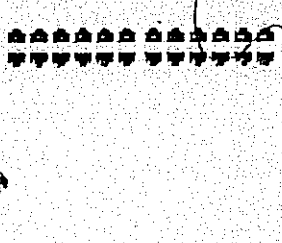
FortiWiFi-60C
(Wireless antennas not shown)



FortiWiFi-60CM
(Wireless antennas not shown)



FortiWiFi-60CX-ADSL-A
(Wireless antennas not shown)



FortiGate-60C-POE

16576

## Complete and Real-time Security

Fortinet designed FortiOS to deliver the advanced protection and performance that standalone products simply cannot match. The integrated technologies work together as a system to provide better visibility and mitigation of the latest network and application threats, stopping attacks before damage can occur. FortiGuard Subscription Services provide automated, real-time, up-to-date protection against security threats.

## Industry Validation

The FortiGate family of physical and virtual appliances has earned more certifications than any other vendor by consistently meeting rigorous third-party standards. Our industry-leading technology provides you with air-tight security.

## Unique Visibility and Control

FortiOS gives you greater visibility and more consistent, granular control over users, devices, applications and data. Dashboard widgets allow administrators to quickly view and understand real-time network activities and threat situations while reputation-based analysis quickly identifies potentially compromised systems.

## Ease of Use

FortiOS lowers costs and reduces IT staff workloads. Physical or virtual FortiGate appliances give you the flexibility to match your security to your environment while enforcing a uniform security policy. Single pane of glass management and centralized analysis ensure consistent policy creation and enforcement while minimizing deployment and configuration challenges.

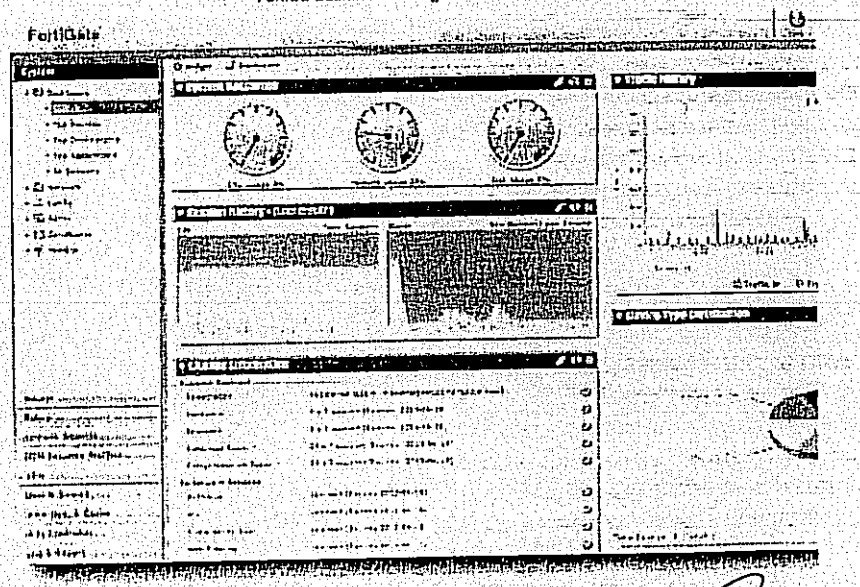
## PCI Compliance Out-of-the-Box

Fortinet simplifies your network security assessment-ready PCI compliance without sacrificing performance. Retail, health care, and other affected industries can ease the process of PCI DSS assessment-readiness with an ISO security framework and unified threat management approach.

## World-Class Technical Support and Documentation

Fortinet FortiCare support offerings provide comprehensive global support for all Fortinet products and services. You can rest assured your Fortinet security products are performing optimally and protecting your users, applications, and data around the clock.

*FortiOS Dashboard - Single Pane of Glass Management*



## *FortiOS - The World's Most Advanced Security Operating System*

- Client reputation measurements to identify compromised systems in real time
- On-device behavior-based heuristic engine for protection against advanced threats
- Cloud-based threat protection with operating system sandbox
- Mobile device identification that lets you apply specific access policies to smartphones and tablets
- Next-Generation Firewall functions, including Application Control and IPS
- Data Loss Prevention to protect critical information
- Web filtering to prevent access to malicious or inappropriate web sites
- Web-based GUI, 'single pane of glass' management console and on-board reporting for unmatched visibility and control

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

# SPECIFICATIONS

16577

| | FortiGate 50E | FortiGate 51E | FortiWiFi 50E-2R | FortiGate 50E-2R | FortiWiFi 50E | FortiWiFi 50E-2R | FortiWiFi 50E-2R-2DSL-A |
|---|---|---|---|---|---|---|---|
| **Hardware Specifications** | | | | | | | |
| 10/100/1000 WAN Interfaces (RJ45) | 2 | 2 | 1 | 2 | 2 | 2 | |
| 10/100/1000 Switch Interfaces (RJ45) | 5 | 5 | - | 5 | 5 | 4 | |
| GbE SFP WAN Interfaces | - | 1 | - | - | - | - | |
| 10/100/1000 PDE+ / POE Switch Interfaces (RJ45) | - | - | 4 / 20 | - | - | - | |
| 10/100 Switch Interfaces (RJ45) | - | - | - | - | - | 4 | |
| 10/100/1000 DMZ Interfaces (RJ45) | 1 | - | - | 1 | 1 | - | |
| ADSL2+ Annex A and M Interface | - | - | - | - | - | 1 | |
| Wireless Interface | - | - | - | 802.11 a/b/g/n | 802.11 a/b/g/n | 802.11 a/b/g/n | |
| Modem Port | - | - | - | - | 1 | - | |
| Management Console Interface (RJ45) | 1 | | | | | | |
| USB Interfaces (Client / Server) | 1 / 1 | 1 / 1 | 1 / 0 | 1 / 1 | 1 / 1 | 1 / 1 | |
| ExpressCard Slot | 1 | - | - | 1 | 1 | 1 | |
| **System Performance** | | | | | | | |
| Firewall Throughput (1518 / 512 / 64 byte UDP packets) | 1 / 1 / 1 Gbps | | | | | | |
| Firewall Latency (64 byte UDP packets) | 4 µs | | | | | | |
| Firewall Throughput (Packets Per Second) | 1.5 Mpps | | | | | | |
| Concurrent Sessions (TCP) | 400,000 | | | | | | |
| New Sessions/Sec (TCP) | 3,000 | | | | | | |
| Firewall Policies | 5,000 | | | | | | |
| IPSec VPN Throughput (512 byte packets) | 70 Mbps | | | | | | |
| Gateway-to-Gateway IPSec VPN Tunnels | 50 | | | | | | |
| Client-to-Gateway IPSec VPN Tunnels | 500 | | | | | | |
| SSL-VPN Throughput | 19 Mbps | | | | | | |
| Concurrent SSL-VPN Users (Recommended Max) | 100 | | | | | | |
| IPS Throughput | 135 Mbps | | | | | | |
| Antivirus Throughput (Proxy Based / Flow Based) | 20 / 40 Mbps | | | | | | |
| Virtual Domains (Default / Max) | 10 / 10 | | | | | | |
| Max Number of FortiAPs (Total / Tunnel Mode) | 10 / 5 | | | | | | |
| Max Number of FortiTokens | 100 | | | | | | |
| Max Number of Registered FortiClients | 200 | | | | | | |
| High Availability Configurations | Active / Active, Active / Passive, Clustering | | | | | | |
| Unlimited User Licenses | Yes | | | | | | |
| **Dimensions** | | | | | | | |
| Height x Width x Length (in) | 1.50 x 8.50 x 5.83 in (38 x 216 x 148 mm) | 1.50 x 8.50 x 5.91 in (38 x 216 x 15 mm) | 1.75 x 17.32 x 12.28 in (44 x 440 x 312 mm) | 1.50 x 8.50 x 6.18 in (38 x 216 x 15 mm) | 1.50 x 8.50 x 6.18 in (38 x 216 x 15 mm) | 1.75 x 13.56 x 8.27 in (44 x 344 x 210 mm) | |
| Weight | 1.9 lbs (0.9 kg) | 1.9 lbs (0.9 kg) | 10.2 lbs (4.7 kg) | 1.9 lbs (0.9 kg) | 1.9 lbs (0.9 kg) | 1.9 lbs (0.9 kg) | |
| **Environment** | | | | | | | |
| Power Required | 100-240 VAC, 50-60 Hz | | | | | | |
| Power Consumption (Avg / Max) | 11 / 13 W | 11 / 13 W | 263 / 310 W | 11 / 13 W | 11 / 13 W | 11 / 13 W | |
| PoE Power Budget | - | - | 185 W | - | - | - | |
| Heat Dissipation | 49 BTU/h | 49 BTU/h | 1058 BTU/h | 49 BTU/h | 49 BTU/h | 49 BTU/h | |
| Operating Temperature | 32 - 104 °F (0 - 40 °C) | | | | | | |
| Storage Temperature | -31 - 158 °F (-35 - 70 °C) | | | | | | |
| Humidity | 20 to 90% non-condensing | | | | | | |
| **Compliance** | FCC Part 15 Class B, C-Tick, VCCI, CE, UL/cUL, CB | | | | | | |
| **Certifications** | ICSA Labs: Firewall, IPSec, IPv6 | | | | | | |

# ORDER INFORMATION

16578

| SKU | Description |
|---|---|
| FG-60C | 8 x GE RJ45 ports (including 2 x WAN ports,1 x DMZ port, 5 x switch ports), ExpressCard slot |
| FG-60C-SFP | 7 x GE RJ45 ports (including 1 x WAN ports,1 x DMZ port, 5 x switch ports), 1 x GE SFP Slot |
| FG-60C-POE | 25 x GE RJ45 Ports (including 1 x Management port, 20 x PoE ports, 4 x PoE+ ports) |
| FWF-60C | 8 x GE RJ45 ports (including 2 x WAN ports,1 x DMZ port, 5 x switch ports), Wireless (802.11a/b/g/n), ExpressCard slot |
| FWF-60CM | 8 x GE RJ45 ports (including 2 x WAN ports,1 x DMZ port, 5 x switch ports), Wireless (802.11a/b/g/n), ExpressCard slot, analog V.90 modem |
| FWF-60CX-ADSL-A | 6 x GE RJ45 ports (including 2 x WAN ports, 4 x switch ports), 4 x FE switch ports, Wireless (802.11a/b/g/n), ADSL2+ Annex A interface, ExpressCard slot |

# FORTIWIFI-60C SERIES SKU SUFFIX

| Region/Country | International | Korea | Japan | Configurable |
|---|---|---|---|---|
| SKU Suffix | -I | -K | -J | No Suffix |
| Frequency Range (GHz) | 2.400 - 2.483<br>5.100 - 5.250 | 2.400 - 2.483<br>5.150 - 5.250<br>5.725 - 5.825 | 2.400 - 2.483<br>5.150 - 5.250<br>5.250 - 5.350*<br>5.470 - 5.725* | 2.400 - 2.483<br>5.150 - 5.250<br>5.725 - 5.850 |

* Requires FortiOS 4.3.10 or later with DFS feature enabled


GLOBAL HEADQUARTERS
Fortinet Inc.
1090 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE
300 Beach Road #20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

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





FST-PROD-DS-FWF60C

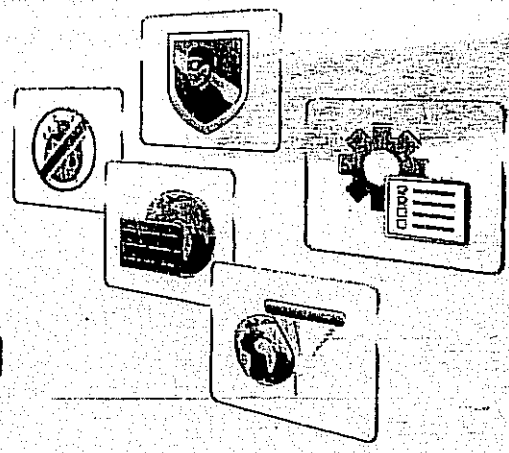
LICITACIÓN PÚBLICA MIXTA NACIONAL NÚMERO **No. LA-009KCZ002-N49-2015** PARA EL ARRENDAMIENTO DEL "EQUIPO FIREWALL/VPN Y CONSOLA DE ADMINISTRACIÓN PARA EXPANSIÓN DE OFICINAS TELEGRÁFICAS DE LA RED TELDAT."

GRUPOTECNO

# Anexo FortiOS_UTM

FORTINET

16530



# FortiOS® 5.2 Network Security Operating System

## For Unified Threat Management

FortiOS is a security-hardened, purpose-built Operating System that is the foundation of all FortiGate® network security platforms from our entry-level devices to our most powerful carrier-grade models. FortiOS 5.2 includes over 150 standard features, and many new enhancements that help fight advanced threats, simplify FortiGate installations and expand threat reporting and management.

*Rich feature set for protecting your applications, data and users.*

- Enterprise-grade security for any sized organization
- Easy to deploy and manage
- Outstanding manageability with consolidated security and access control setup
- Strong and flexible user and device management with multiple authentication options.

### Robust Complete Network Security

No matter how large or small your organization is, you face numerous challenges as your network environment, usage patterns and security threats evolve. FortiOS gives you the latest in all-in-one network security protection that's easy to deploy and manage. Besides the industry's best firewall, intrusion protection and VPN you get Advanced Threat Protection that fights against advanced persistent threats (ATPs) and additional features like email filtering, data-loss prevention and vulnerability scanning - a complete Unified Threat Management (UTM) solution for your business.

### Flexible Architecture that Adapts with Your Needs

Whether you need a simple firewall or a complete UTM installation, FortiOS gives you the flexibility to easily configure the options you need for your environment. From a "single pane of glass" you can set up, manage, and get detailed reporting on your network and security threats, all within minutes.

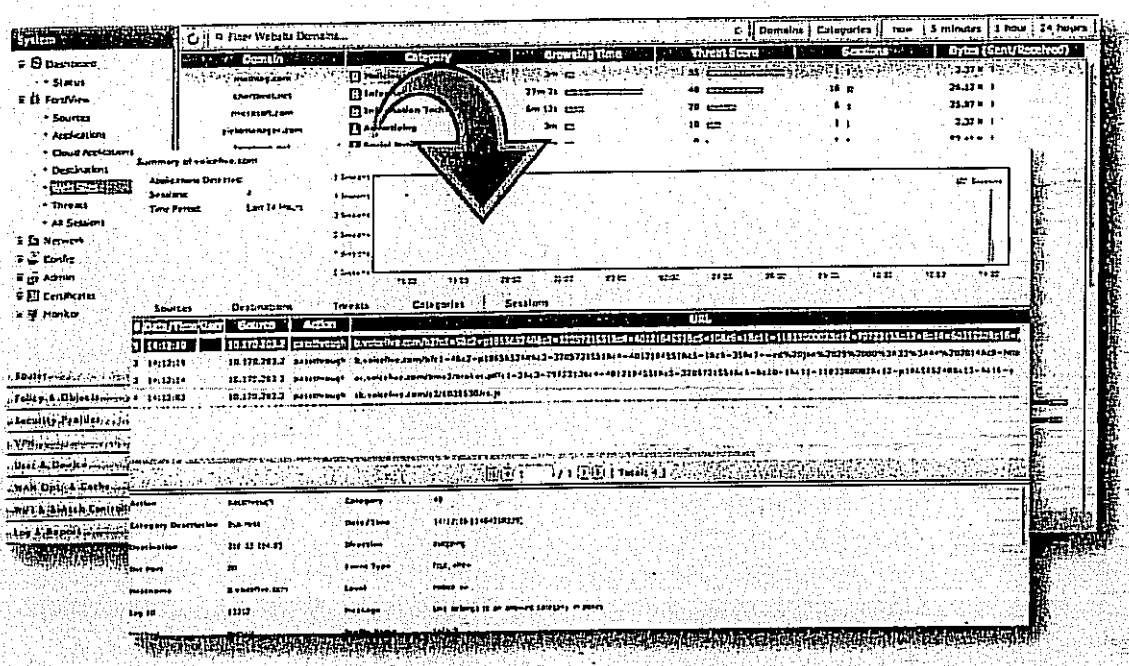
### Key Features & Benefits

| | |
|---|---|
| Unified Threat Management | Comprehensive network security protection with advanced threat protection, email filtering, data-loss prevention and vulnerability scanning. |
| Intuitive and Customizable | Easy to configure and manage with the flexibility to choose the security and UTM options you need. |
| Advanced Network Segmentation | Support for multiple zones and VDOMs to meet your data protection and compliance requirements. |

ICSA labs ICSA labs ICSA labs

ICSA labs ICSA labs

000142



*FortiOS web-based GUI — FortiView on-demand query tool*

## Complete Security

Fortinet designed and built FortiOS 5.2 to deliver the advanced protection and performance that standalone products simply can't match. The services work together as a system to provide better visibility and mitigation of the latest network and application threats, stopping attacks before damage can occur.

## Unique Visibility and Control

Advanced security features such as flow-based inspection and integrated wireless controller capability allow you to monitor and protect your wired and wireless networks from endpoints to the core, and from remote offices to headquarters. FortiOS allows greater traffic visibility and more consistent, granular control over users, applications and sensitive data.

## Easier to Manage

FortiOS 5.2 lowers costs and reduces IT staff workloads. Physical or virtual FortiGate appliances give you the flexibility to match your security to your environment while enforcing a uniform security policy. Single pane of glass management and centralized analysis ensure consistent policy creation and enforcement while minimizing deployment and configuration challenges.

## Securing Mobile Devices

FortiOS 5.2 helps secure mobile device and BYOD environments (including iOS®, Android® and Windows® clients) by identifying devices and applying specific access policies as well as security profiles, according to the device type or device group, location, and usage.

## Client Reputation

Signature-based security alone is not enough anymore; it is now critical to understand how devices on your network are behaving. FortiView with threat score provides a cumulative security ranking of each client device on your network based on a range of behaviors. It provides specific, actionable information that helps identify compromised systems and potential zero-day attacks in real time.

## Smart Policies

FortiOS 5.2 enables intelligent, automatic adjustment of role-based policies for users and guests based on location, data, and application profile. Enhanced reporting and analysis provides deeper insights into the behavior of your network, users, devices, applications and threats.

# HIGHLIGHTS

## Extensive Network Support

FortiOS supports numerous network design requirements and interoperates with other networking devices. This includes support for a wealth of routing, multicasting and network resiliency protocols. Administrators can also configure interfaces for VLANs, VLAN trunks, port aggregation and one-armed sniffer mode.

It also offers robust high-availability and clustering options, including advanced sub-second failover, virtual clusters and much more.

## Unified Access Security

OS empowers organizations to apply consistent olicies across various types of networks, simplifying policy enforcement in today's complex environments. Its wireless controller features extend the same protection to wireless networks while endpoint control capabilities provision and enforce security for mobile users even when they are away from the office.

## Device ID and User ID Access Control

FortiOS supports both local and remote authentication services such as LDAP, Radius and TACACS+ to identify users and apply access policies and security profiles accordingly. It simplifies identity-based implementations and also provides a seamless user authorization experience with various single sign-on capabilities. FortiOS can capture terminal service user or wireless login credentials, among others, and intelligently apply policies and profiles without additional user input.

As device types continue to evolve, you'll be ready with device access control. You can apply security policies based on the type of device such as computers, tablets or phones and apply different policies depending if the devices are company or privately owned.

## Sophisticated Application Control

Identifying applications and providing relevant enforcement is essential in the current Web 2.0 and cloud environments. FortiOS offers gradual controls and can identify over 3,000 applications, even those on encrypted channels. It also offers mitigation against sophisticated botnet activities that easily evade traditional firewalls.

## Physical and Virtual Segmentation

From simple small wired networks to the complex multi-tenant managed datacenter environments, FortiOS supports everything you need to set up and manage your network traffic. You can configure physical network segmentation using the LAN ports built-in to every FortiGate, or you can provide virtual segmentation using virtual LANs (VLANs).

## Powerful & Scalable Management

FortiManager makes it easy to provision and manage thousands of FortiGate devices in a distributed organization. Using standardized setup profiles, you get the ability to configure a standard set of policy and provisioning workflows to meet your business needs or compliance standards. Detailed configuration audit trails are supported and can reside externally on secured storage with FortiAnalyzer.

FortiOS also integrates well with third-party solutions such as Network Management Systems and SIEMs through Fortinet's technology alliances.

## *FortiGate® - High performance Network Security Platform*

- **ASIC-Powered Performance**
  FortiGate purpose-built hardware delivers unmatched price/performance for the most demanding networking environments. FortiASIC processors ensure that your network security solution does not become a network bottleneck.
- **High speed and Flexible Connectivity**
  The FortiGate product family offer a variety of interfaces for today's network, ranging from integrated WAN interfaces, 3G/4G USB wireless broadband support to high speed 40G interfaces for data centers.
- **Broad Product Offerings**
  The FortiGate product family scales from desktop units for remote branch offices, mid-range for small and medium enterprises to high-end platforms for service providers and data centers

# FEATURE SUMMARY

16583

## Network Services and Support

- Built-in DHCP, NTP, DNS Server and DNS proxy (available on most models)
- FortiGuard NTP, DDNS and DNS service
- Interface modes: sniffer, port aggregated, loopback, VLANs (802.1Q and Trunking), virtual hardware, software and VLAN switches (available on most models)
- Static and policy routing
- Hybrid WAN support: load balancing and redundancy with link health check on monitoring using TWAMP
- Support USB 3G/4G Wireless WAN modems
- Dynamic routing protocols:
  - RIPv1 and v2, OSPF v2 and v3, ISIS, BGP4
- Multicast traffic: sparse and dense mode, PIM support
- Content routing: WCCP and ICAP
- Traffic shaping and QoS per policy or applications: shared policy shaping, per-IP shaping, maximum & guaranteed bandwidth, maximum concurrent connections per IP, traffic prioritization, Type of Service (TOS) and Differentiated Services (DiffServ) support
- IPv6 Support: Management over IPv6, IPv6 routing protocols, IPv6 tunneling, firewall and [illegible] for IPv6 traffic, NAT46, NAT64, IPv6 IPSEC VPN

## vWAN Optimization, Web Cache and Explicit Proxy^

- Inline and out-of-path WAN optimization topology, peer to peer and remote client support
- Transparent Mode option: keeps the original source address of the packets, so servers appear to receive traffic directly from clients.
- WAN optimization techniques: protocol optimization and byte caching
- WAN Optimization protocols supported: CIFS, FTP, HTTP(S), MAPI, TCP
- Secure Tunneling option: use AES-128bit-CBC SSL to encrypt the traffic in the WAN optimization tunnel.
- Tunnel sharing option: multiple WAN optimization sessions share the same tunnel.
- Web caching: object caching that accelerates web applications and web servers by reducing bandwidth usage, server load, and perceived latency. Supports caching of HTTP 1.0 and HTTP 1.1 web sites.
- SSL Offloading with Web caching:
  - Full mode: performs both decryption and encryption of the HTTPS traffic.
  - Half mode: only performs one encryption or decryption action.
- Option to exempt certain web sites from web caching with URL patterns.
- Support advanced web caching configurations and options:
  - Always-revalidate, Max-cache-object-size, negative response duration, fresh factor, Max/Min/Default-TTL, proxy FQDN, Max-HTTP-request/message length, ignore options, cache expired objects, revalidated pragma-no-cache
- Explicit web & FTP proxy: FTP, HTTP, and HTTPS proxying on one or more interfaces
- Proxy auto-config (PAC): provide automatic proxy configurations for explicit web proxy [illegible]rs.
- [illegible]y chaining: web proxy forwarding to redirect web proxy sessions to other proxy servers.
- Web proxy forwarding server monitoring and health checking
- IP reflect capability
- Load balancing for forward proxy and proxy chaining
- Explicit web proxy authentication: IP-Based authentication and per session authentication
- WAN optimization and web cache monitor

## User & Device Identity Control

- Local user database & remote user authentication service support: LDAP, Radius and TACACS+, 2-factor authentication
- Single-sign-on: Windows AD, Novell eDirectory, FortiClient, Citrix and Terminal Server Agent, Radius (accounting message), POP3/POP3S, user access (802.1x, captive portal) authentication
- PKI and certificates: X.509 certificates, SCEP support, Certificate Signing Request (CSR) creation, auto-renewal of certificates before expiry, OCSP support
- Device identification: device and OS fingerprinting, automatic classification, inventory management
- User and device-based policies

## Integrated Token Server

- Integrated token server that provisions and manages physical, SMS and Soft One Time Password (OTP) tokens

## Firewall

- Operating modes: NAT/route and transparent (bridge)
- Schedules: one-time, recurring
- Session helpers & ALGs: dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS (Oracle)
- VoIP traffic support: SIP/H.323 /SCCP NAT traversal, RTP pin holing
- Protocol type support: SCTP, TCP, UDP, ICMP, IP
- Section or global policy management view
- Policy objects: predefined, customs, object grouping, tagging and coloring
- Address objects: subnet, IP, IP range, GeoIP (Geography), FQDN
- NAT configuration: per policy based and central NAT Table
- NAT support: NAT64, NAT46, static NAT, dynamic NAT, PAT, Full Cone NAT, STUN

## VPN

IPSEC VPN:
- Remote peer support: IPSEC-compliant dialup clients, peers with static IP/dynamic DNS
- Authentication method: certificate, pre-shared key
- IPSEC Phase 1 mode: aggressive and main (ID protection) mode
- Peer acceptance options: any ID, specific ID, ID in dialup user group
- supports IKEv1, IKEv2 (RFC 4306)
- IKE mode configuration support (as server or client), DHCP over IPSEC
- Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128, AES192, AES256
- Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512
- Phase 1/Phase 2 Diffie-Hellman Group support: 1, 2, 5, 14
- XAuth support as client or server mode
- XAuth for dialup users: Server type option (PAP, CHAP, Auto), NAT Traversal option
- Configurable IKE encryption key expiry, NAT traversal keepalive frequency
- Dead peer detection
- Replay detection
- Autokey keep-alive for Phase 2 SA

- IPSEC Configuration Wizard for termination with popular 3rd party devices
- IPSEC VPN deployment modes: gateway-to-gateway, hub-and-spoke, full mesh, redundant-tunnel, VPN termination in transparent mode,
- IPSEC VPN Configuration options: route-based or policy-based
- Customizable SSL VPN portal: color themes, layout, bookmarks, connection tools, client download
- SSL VPN realm support: allows multiple custom SSL VPN logins associated with user groups (URL paths, design)
- Single-sign-on bookmarks: reuse previous login or predefined credentials to access resources
- Personal bookmarks management: allow administrators to view and maintain remote client bookmarks
- SSL portal concurrent users limiting
- One time login per user options: prevents concurrent logins using same username
- SSL VPN web mode: for thin remote clients equipped with a web browser only and support web application such as:
  - HTTP/HTTPS Proxy, FTP, Telnet, SMB/CIFS, SSH, VNC, RDP, Citrix
- SSL VPN tunnel mode: for remote computers that run a variety of client and server applications. SSL VPN client supports MAC OSX, Linux, Windows Vista and with 64-bit Windows operating systems
- SSL VPN port forwarding mode: uses a Java Applet that listens on local ports on the user's computer. When it receives data from a client application, the port forward module encrypts and sends the data to the SSL VPN device, which then forwards the traffic to the application server.
- Host integrity checking and OS check (for windows terminals only) prior to SSL tunnel mode connections
- MAC host check per portal
- Cache cleaning option just before the SSL-VPN session ends
- Virtual desktop option to isolates the SSL VPN session from the client computer's desktop environment
- VPN monitoring: view and manage current IPSEC and SSL VPN connections in details
- Other VPN support: L2TP client (on selected models) and server mode, L2TP over IPSEC, PPTP, GRE over IPSEC

# FEATURE SUMMARY

## SSL Inspection

Inspect SSL Encrypted traffic option for IPS, application control, antivirus, web filtering and DLP

## IPS

IPS engine: 7,000+ up-to-date signatures, protocol anomaly detection, rate-based detection, custom signatures, manual, automatic pull or push signature update, threat encyclopedia integration

IPS Actions: default, monitor, block, reset, or quarantine (attackers IP, attackers IP and Victim IP, incoming interface) with expiry time

Filter Based Selection: severity, target, OS, application and/or protocol

Packet logging option

IP(s) exemption from specified IPS signatures

IPv4 and IPv6 Rate based DOS protection (Available on most Models) with threshold settings against TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/SCTP/ICMP session flooding (source/destination)

IDS sniffer mode

Active bypass with bypass interfaces (selected models) and FortiBridge

## Application Control

Detects over 3,000 applications in 18 Categories:
Botnet, Collaboration, Email, File Sharing, Game, General Interest, Network Service, P2P, Proxy, Remote Access, Social Media, Storage Backup, Update, Video/Audio, VoIP, Industrial, Special, Web (Others)

Custom application signature support

Supports detection for traffic using SPDY protocol

Deep Application visibility: login names, files/video activities and information

Filter based selection: by category, popularity, technology, risk, vendor and/or protocol

Actions: block, reset session, monitor only, application control traffic shaping

SSH Inspection

## Anti-Malware / Advanced Threat Protection

Botnet server IP blocking with global IP reputation database

Antivirus database type selection (on selected models)

Flow-based Antivirus: protocols supported - HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, SMB, ICQ, YM, NNTP

Proxy-based Antivirus:
- Protocol Support: HTTP/HTTPS, STMP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, ICQ, YM, NNTP
- External cloud-based file analysis (OS sandbox) support
- File submission blacklisting and whitelisting
- File quarantine (local storage required)
- Heuristic scanning option

## Web Filtering

Web filtering inspection mode support: proxy-based, flow-based and DNS

Manually defined web filtering based on URL, web content & MIME header

Dynamic web filtering with cloud-based realtime categorization database: over 250 Million URLs rated into 78 categories, in 70 languages

Safe Search enforcement: transparently inserts Safe Search parameter to queries. Supports Google, Yahoo!, Bing & Yandex, delinable YouTube Education Filter

Additional features offered by proxy-based web filtering:
- Filter Java Applet, ActiveX and/or cookie
- Block HTTP Post
- Log search keywords
- Rate images by URL
- Block HTTP redirects by rating
- Exempt scanning encrypted connections on certain categories for privacy
- Web Browsing quota by categories

Web filtering local categories & category rating override

Web filtering profile override: allows administrator to temporarily assign different profiles to user/user group/IP

Restrict access to Google Corporate Accounts only

Proxy avoidance prevention: proxy site category blocking, rule, URL, by domain & IP address, block redirects from cache & translation sites, proxy avoidance application blocking (application control), proxy behavior blocking (IPS)

## Data Leak Prevention (DLP)

Web filtering inspection mode support: proxy-based, flow-based and DNS

DLP message filter:
- Protocol supported: HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP
- Actions: log only, block, quarantine user/IP/interface
- Predefined filter: credit card number, Social Security ID

DLP File Filter:
- Protocol Supported: HTTP-POST, HTTP=-GET,SMTP, POP3, IMAP, MAPI, FTP, NNTP
- Filter options: size, file type, watermark, content, if encrypted

DLP watermarking: allows filter files that pass through the FortiGate unit and contain a corporate identifier (a text string) and a sensitivity level (Critical, Private, and Warning) hidden in a watermark. Support Windows and Linux free watermarking tools.

DLP fingerprinting: generates a checksum fingerprint from intercepted files and compare it to those in the fingerprint database.

DLP archiving: records full content in email, FTP, IM, NNTP, and web traffic

## Endpoint Control

Manages network devices via client software:
- Posture checking: enforce client software installation and desired settings
- Client configuration provisioning: push and update client configurations such as VPN and web filtering settings accordingly to device type/group and/or user/usergroup
- "Off-net" security enforcement: detects when not protected by security gateway, activates provisioning security settings
- allows client activities logging implementation

Client software support: Windows, OS X, iOS, Android

## Vulnerability Scanning

Network Vulnerability Scan: protect network assets (servers and workstations) by scanning them for security weaknesses.
- On-demand or scheduled
- Scan Modes: Quick, standard or Full
- authenticated scanning

Vulnerability Result: detailed scan results are logged with direct reference on threat encyclopedia

## Wireless and Switch Controller

Manages and provisions settings for local and remote Thin Access points or switches (selected models)

Set up access and authentication methods for SSIDs and VLANs, supports integrated or external captive portal, 802.1x, preshared keys

WiFi Security: Rogue AP suppression, wireless IDS

Wireless topology support: Fast roaming, AP load balancing, Wireless Mesh and bridging

## High Availability

High availability modes: active-passive, active-active, virtual clusters, VRRP, FG-5000 series clustering

Redundant heartbeat interfaces

HA reserved management interface

Failover:
- Port, local & remote link monitoring
- stateful failover
- subsecond failover
- Failure detection notification

Deployment Options:
- HA with link aggregation
- Full mesh HA
- Geographically dispersed HA

Standalone session synchronization

## Administration, Monitoring & Diagnostics

Management Access: HTTPS via web browser, SSH, telnet, console

Web UI administration language support: English, Spanish, French, Portuguese, Japanese, Simplified Chinese, Traditional Chinese, Korean

Central management support: FortiManager, FortiCloud hosted service, web service APIs

Systems Integration: SNMP, sFlow, Netflow, syslog, alliance partnerships

Rapid deployment: install wizards, USB auto-install, local and remote script execution

Dynamic, real-time dashboard status & drill-in monitoring widgets

# FEATURE SUMMARY

16585

| Log & Reporting |
|---|
| Logging facilities support: local memory & storage (if available), multiple syslog servers, multiple FortiAnalyzers, WebTrends servers, FortiCloud hosted service |
| Reliable logging using TCP option (RFC 3195) |
| Encrypted logging & log integrity with FortiAnalyzer |
| Scheduled batch log uploading |
| Detailed traffic logs: Forwarded, violated sessions, local traffic, invalid packets |
| Comprehensive event logs: systems & administrators activity audits, routing & networking, VPN, user authentications, WiFi related events |
| Brief traffic log format option |
| IP and service port name resolution option |

NOTE: Feature set based on FortiOS V5.2.1+, some features or certification may not apply to all models. ^ Local storage required.

# ADDITIONAL REFERENCES

| Resource | URL |
|---|---|
| The FortiOS Handbook - The Complete Guide | http://docs.fortinet.com/fgt.html |
| Fortinet Knowledge Base | http://kb.fortinet.com/ |
| Datasheets & Matrix | http://www.fortinet.com/resource_center/datasheets.html |
| Other Solution Page | http://www.fortinet.com/solutions/unified_threat_management.html |


GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE
300 Beach Road #20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

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




FCS-FTIA-DS1-15-1113

LICITACIÓN PÚBLICA MIXTA NACIONAL NÚMERO **No. LA-009KCZ002-N49-2015** PARA EL ARRENDAMIENTO DEL "EQUIPO FIREWALL/VPN Y CONSOLA DE ADMINISTRACIÓN PARA EXPANSIÓN DE OFICINAS TELEGRÁFICAS DE LA RED TELDAT."

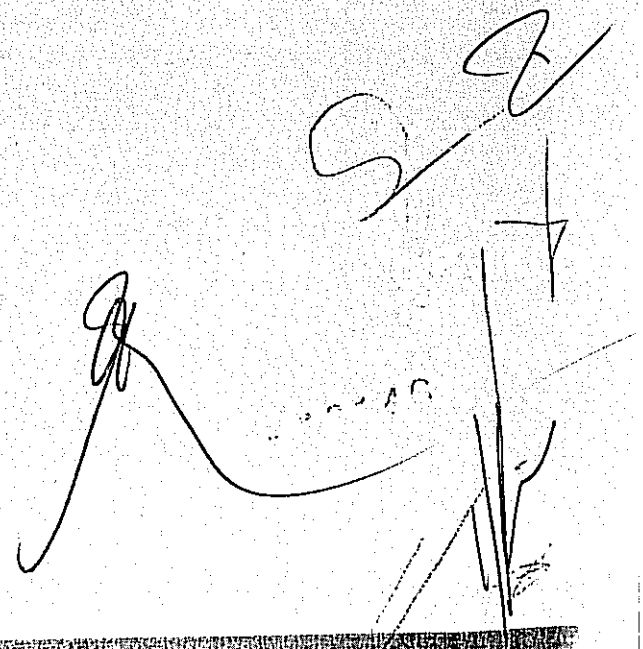
GRUPOTECNO

# Anexo FortiOS™ Handbook SSL VPN

## for FortiOS 5.0

FORTINET

# FortiOS™ Handbook
## SSL VPN for FortiOS 5.0



# SSL VPN modes of operation

When a remote client connects to the FortiGate unit, the FortiGate unit authenticates the user based on user name, password, and authentication domain. A successful login determines the access rights of remote users according to user group. The user group settings specify whether the connection will operate in web-only mode or tunnel mode.

## Web-only mode

Web-only mode provides remote users with a fast and efficient way to access server applications from any thin client computer equipped with a web browser. Web-only mode offers true clientless network access using any web browser that has built-in SSL encryption and the Sun Java runtime environment.

Support for SSL VPN web-only mode is built into the FortiOS operating system. The feature comprises of an SSL daemon running on the FortiGate unit, and a web portal, which provides users with access to network services and resources including HTTP/HTTPS, telnet, FTP, SMB/CIFS, VNC, RDP and SSH.

In web-only mode, the FortiGate unit acts as a secure HTTP/HTTPS gateway and authenticates remote users as members of a user group. After successful authentication, the FortiGate unit redirects the web browser to the web portal home page and the user can access the server applications behind the FortiGate unit.

When the FortiGate unit provides services in web-only mode, a secure connection between the remote client and the FortiGate unit is established through the SSL VPN security in the FortiGate unit and the SSL security in the web browser. After the connection has been established, the FortiGate unit provides access to selected services and network resources through a web portal.

FortiGate SSL VPN web portals have a 1- or 2-column page layout and portal functionality is provided through small applets called widgets. Widget windows can be moved or minimized. The controls within each widget depend on its function. There are predefined web portals and the administrator can create additional portals.

Configuring the FortiGate unit involves selecting the appropriate web portal configuration in the user group settings. These configuration settings determine which server applications can be accessed. SSL encryption is used to ensure traffic confidentiality.

For information about client operating system and browser requirements, see the Release Notes for your FortiGate firmware.

## Tunnel mode

Tunnel mode offers remote users the freedom to connect to the internal network using the traditional means of web-based access from laptop computers, as well as from airport kiosks, hotel business centers, and Internet cafés. If the applications on the client computers used by your user community vary greatly, you can deploy a dedicated SSL VPN client to any remote client through its web browser. The SSL VPN client encrypts all traffic from the remote client computer and sends it to the FortiGate unit through an SSL VPN tunnel over the HTTPS link between the web browser and the FortiGate unit. Another option is split tunneling, which ensures that only the traffic for the private network is sent to the SSL VPN gateway. Internet traffic is sent through the usual unencrypted route. This conserves bandwidth and alleviates bottlenecks.

In tunnel mode, remote clients connect to the FortiGate unit and the web portal login page using Microsoft Internet Explorer, Firefox, Chrome, Mac OS, or Linux. The FortiGate unit acts as a secure HTTP/HTTPS gateway and authenticates remote users as members of a user group. After successful authentication, the FortiGate unit redirects the web browser to the web portal

FORTINET

16589

# *Carta derecho de uso de licencia*

Fecha: 10/08/2015

TELECOMUNICACIONES DE MÉXICO
DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS
SUBDIRECCIÓN DE RECURSOS MATERIALES Y SERVICIOS GENERALES
GERENCIA DE ADQUISICIONES
P R E S E N T E

Referente a la licitación No. LA-009KCZ002-N49-2015, manifiesto que TELECOMM tendrá derecho de uso sobre las licencias de los equipos Fortinet Inc., para la puesta en operación de los equipos de esta Marca, ofertados por el licitante Grupo de Tecnología Cibernética, S.A. de C.V., y descritos en el Plan de Trabajo con sus respectivos números de serie.

Sin otro particular, quedo de usted.

Atentamente,

Manuel Acosta
VP Fortinet Mexico
Representante Legal

000021

## "Carta Compromiso que Especifica que GRUPO TECNO Entregará la Memoria Técnica Reflejando los Aspectos Técnicos del Servicio Proporcionado"

MEXICO, D.F. A 8 DE OCTUBRE DE 2015

TELECOMUNICACIONES DE MÉXICO

DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS

SUBDIRECCIÓN DE RECURSOS MATERIALES Y SERVICIOS GENERALES

GERENCIA DE ADQUISICIONES

PRESENTE

**JENNIFER MURILLO DOMÍNGUEZ,** EN MI CARÁCTER DE REPRESENTANTE LEGAL DE LA EMPRESA **GRUPO DE TECNOLOGÍA CIBERNÉTICA S.A. DE C.V., MANIFIESTO BAJO PROTESTA DE DECIR VERDAD,** MANIFIESTO NUESTRO COMPROMISO PARA LA ENTREGA DE LAS CORRESPONDIENTES MEMORIAS TÉCNICAS REFLEJANDO LOS ASPECTOS TÉCNICOS DEL SERVICIO PROPORCIONADO DE ACUERDO A LAS SIGUIENTES FECHAS:

| FECHAS COMPROMISO |
|---|
| 29-ENERO 2016 |
| 16 DICIEMBRE 2016 (ACTUALIZACIÓN) |
| 15 DICIEMBRE 2017 (ACTUALIZACIÓN) |
| 31 MAYO 2018 (ACTUALIZACIÓN) |

ATENTAMENTE

MÉXICO, D.F., 08 DE OCTUBRE DE 2015
BAJO PROTESTA DE DECIR VERDAD,
GRUPO DE TECNOLOGÍA CIBERNÉTICA, S.A. DE C.V.

JENNIFER MURILLO DOMÍNGUEZ
REPRESENTANTE LEGAL

000028

FORTINET

16591

*Carta de Compatibilidad con el Servicio de Filtrado de Contenido*

Fecha: 10/08/2015

TELECOMUNICACIONES DE MEXICO
DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS
SUBDIRECCIÓN DE RECURSOS MATERIALES Y SERVICIOS GENERALES
GERENCIA DE ADQUISICIONES
P R E S E N T E

Referente a la licitación No. LA-009KCZ002-N49-2015, manifiesto que los equipos firewall's appliances ofertados por el licitante Grupo de Tecnología Cibernética, S.A. de C.V. son compatibles con el servicio de filtrado de contenido "URL" mediante el mecanismo de integración PBR (Policy Based Routing), para la correcta activación de los servicios que actualmente están operando en sitios centrales.

Sin otro particular, quedo de usted.

Atentamente,

PA

Manuel Acosta
VP Fortinet Mexico
Representante Legal

000039

FORTINET

16592

Fecha: 10/08/2015

TELECOMUNICACIONES DE MÉXICO
DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS
SUBDIRECCIÓN DE RECURSOS MATERIALES Y SERVICIOS GENERALES
GERENCIA DE ADQUISICIONES
P R E S E N T E

Referente a la licitación No. LA-009KCZ002-N49-2015 Para el arrendamiento del "EQUIPO FIREWALL/VPN Y CONSOLA DE ADMINISTRACIÓN PARA EXPANSIÓN DE OFICINAS TELEGRÁFICAS DE LA RED TELDAT", manifiesto que EL LICITANTE **Grupo de Tecnología Cibernética S.A de C.V**, es distribuidor autorizado de Fortinet Inc. y está debidamente autorizado para suministrar los servicios solicitados en la presente licitación.

**Grupo de Tecnología Cibernética S.A. de C.V.,** cuenta con la capacidad para proporcionar la solución ofertada a nivel de implementación, soporte, actualizaciones y servicios. Fortinet Inc. garantiza el abastecimiento suficiente del equipamiento propuesto para el cumplimiento de las obligaciones pactadas producto de la presente licitación, respaldando la proposición del LICITANTE **Grupo de Tecnología Cibernética S.A. de C.V.** en los términos establecidos en la presente convocatoria, así como el debido cumplimiento en la entrega de los servicios durante la vigencia del contrato.

Sin otro particular, quedo de usted.

Atentamente,

PA

Manuel Acosta
VP Fortinet Mexico
Representante Legal

000032

FORTINET

16593

# *Carta del Mismo Fabricante*

Fecha: 10/08/2015

**TELECOMUNICACIONES DE MÉXICO**
**DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS**
**SUBDIRECCIÓN DE RECURSOS MATERIALES Y SERVICIOS GENERALES**
**GERENCIA DE ADQUISICIONES**
**P R E S E N T E**

Referente a la licitación No. LA-009KCZ002-N49-2015, manifiesto que toda la infraestructura de equipo firewall, propuesta por el licitante Grupo de Tecnología Cibernética, S.A. de C.V., es de un mismo fabricante.

Sin otro particular, quedo de usted.

Atentamente,

PA

Manuel Acosta
VP Fortinet Mexico
Representante Legal

00013

GRUPOTECNO

**LICITACIÓN PÚBLICA MIXTA NACIONAL NÚMERO No. LA-009KCZ002-N49-2015 PARA EL ARRENDAMIENTO DEL "EQUIPO FIREWALL/VPN Y CONSOLA DE ADMINISTRACIÓN PARA EXPANSIÓN DE OFICINAS TELEGRÁFICAS DE LA RED TELDAT."**

16594

## "Carta donde se manifiesta que los equipos serán de un mismo fabricante"

MEXICO, D.F. A 8 DE OCTUBRE DE 2015

TELECOMUNICACIONES DE MÉXICO

DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS

SUBDIRECCIÓN DE RECURSOS MATERIALES Y SERVICIOS GENERALES

GERENCIA DE ADQUISICIONES

P R E S E N T E

JENNIFER MURILLO DOMÍNGUEZ, EN MI CARÁCTER DE REPRESENTANTE LEGAL DE LA EMPRESA GRUPO DE TECNOLOGÍA CIBERNÉTICA S.A. DE C.V., MANIFIESTO BAJO PROTESTA DE DECIR VERDAD, QUE TODA LA INFRAESTRUCTURA PROPUESTA DE EQUIPO FIREWALL SERÁ DE UN MISMO FABRICANTE.

A T E N T A M E N T E

MÉXICO, D.F., 08 DE OCTUBRE DE 2015
BAJO PROTESTA DE DECIR VERDAD,
GRUPO DE TECNOLOGÍA CIBERNÉTICA, S.A. DE C.V.

JENNIFER MURILLO DOMÍNGUEZ
REPRESENTANTE LEGAL

000140

GRUPOTECNO

16595

MÉXICO, D.F. A 8 DE OCTUBRE DE 2015

TELECOMUNICACIONES DE MÉXICO
DIREECCIÓN DE ADMINISTRACIÓN Y FINANZAS
SUBDIRECCIÓN DE RECURSOS MATERIALES Y SERVICIOS GENERALES
GERENCIA DE ADQUISICIONES

PRESENTE

CONVOCATORIA A LA LICITACIÓN PÚBLICA MIXTA NACIONAL No. LA-009KCZ002-N49-2015, PARA EL ARRENDAMIENTO DEL "EQUIPO FIREWALL/VPN Y CONSOLA DE ADMINISTRACIÓN PARA EXPANSIÓN DE OFICINAS TELEGRÁFICAS DE LA RED TELDAT."

JENNIFER MURILLO DOMÍNGUEZ , EN MI CARÁCTER DE REPRESENTANTE LEGAL DE LA EMPRESA GRUPO DE TECNOLOGÍA CIBERNÉTICA, S.A. DE C.V., MANIFIESTO QUE DURANTE EL PERIODO DE INSTALACIÓN, MIGRACIÓN Y SUSTITUCIÓN DE LOS EQUIPOS, SE GARANTIZA LA OPERACIÓN Y LOS SERVICIOS A TRAVÉS DE LA INTEGRACIÓN CON LA INFRAESTRUCTURA ACTUAL DE COMUNICACIONES Y SEGURIDAD CON QUE CUENTA TELECOMM.

MÉXICO, D.F. A 8 DE OCTUBRE DE 2015
GRUPO DE TECNOLOGÍA CIBERNÉTICA S.A. DE C.V.

JENNIFER MURILLO DOMÍNGUEZ
REPRESENTANTE LEGAL

000142

MÉXICO, D.F. A 8 DE OCTUBRE DE 2015

TELECOMUNICACIONES DE MÉXICO
DIREECCIÓN DE ADMINISTRACIÓN Y FINANZAS
SUBDIRECCIÓN DE RECURSOS MATERIALES Y SERVICIOS GENERALES
GERENCIA DE ADQUISICIONES

PRESENTE

CONVOCATORIA A LA LICITACIÓN PÚBLICA MIXTA NACIONAL No. LA-009KCZ002-N49-2015, PARA EL ARRENDAMIENTO DEL "EQUIPO FIREWALL/VPN Y CONSOLA DE ADMINISTRACIÓN PARA EXPANSIÓN DE OFICINAS TELEGRÁFICAS DE LA RED TELDAT."

JENNIFER MURILLO DOMÍNGUEZ , EN MI CARÁCTER DE REPRESENTANTE LEGAL DE LA EMPRESA GRUPO DE TECNOLOGÍA CIBERNÉTICA, S.A. DE C.V., MANIFIESTO QUE MI REPRESENTADA SE COMPROMETE A REALIZAR LA MIGRACIÓN Y PUESTA EN OPERACIÓN DEL EQUIPO OFERTADO PARA DAR CONTINUIDAD A LOS SERVICIOS ACTUALES E INTEGRACIÓN CON LA INFRAESTRUCTURA DE COMUNICACIONES Y SEGURIDAD CON LA QUE ACTUALMENTE OPERA TELECOMM.

MÉXICO, D.F. A 8 DE OCTUBRE DE 2015
GRUPO DE TECNOLOGÍA CIBERNÉTICA S.A. DE C.V.

JENNIFER MURILLO DOMÍNGUEZ
REPRESENTANTE LEGAL

000145

GRUPOTECNO

16597

MÉXICO, D.F. A 8 DE OCTUBRE DE 2015

TELECOMUNICACIONES DE MÉXICO
DIREECCIÓN DE ADMINISTRACIÓN Y FINANZAS
SUBDIRECCIÓN DE RECURSOS MATERIALES Y SERVICIOS GENERALES
GERENCIA DE ADQUISICIONES

PRESENTE

CONVOCATORIA A LA LICITACIÓN PÚBLICA MIXTA NACIONAL No. LA-009KCZ002-N49-2015, PARA EL ARRENDAMIENTO DEL "EQUIPO FIREWALL/VPN Y CONSOLA DE ADMINISTRACIÓN PARA EXPANSIÓN DE OFICINAS TELEGRÁFICAS DE LA RED TELDAT."

JENNIFER MURILLO DOMÍNGUEZ , EN MI CARÁCTER DE REPRESENTANTE LEGAL DE LA EMPRESA GRUPO DE TECNOLOGÍA CIBERNÉTICA, S.A. DE C.V., MANIFIESTO QUE MI REPRESENTADA SE COMPROMETE A PROPORCIONAR E IMPLEMENTAR LAS HERRAMIENTAS DE MONITOREO NECESARIAS A TRAVES DEL SISTEMA DE GESTIÓN SOLICITADO, QUE PERMITAN CONOCER EL ESTADO OPERATIVO DEL EQUIPO QUE INTEGRA LA SOLUCIÓN, LA GESTIÓN DEL SERVICIO SERÁ DE FORMA PRO-ACTIVA A LOS INCIDENTES QUE SE PUEDAN PRESENTAR.

MÉXICO, D.F. A 8 DE OCTUBRE DE 2015
GRUPO DE TECNOLOGÍA CIBERNÉTICA S.A. DE C.V.

JENNIFER MURILLO DOMÍNGUEZ
REPRESENTANTE LEGAL

000147

GRUPOTECNO

16598

**MÉXICO, D.F. A 8 DE OCTUBRE DE 2015**

TELECOMUNICACIONES DE MÉXICO
DIREECCIÓN DE ADMINISTRACIÓN Y FINANZAS
SUBDIRECCIÓN DE RECURSOS MATERIALES Y SERVICIOS GENERALES
GERENCIA DE ADQUISICIONES

PRESENTE

CONVOCATORIA A LA LICITACIÓN PÚBLICA MIXTA NACIONAL No. LA-009KCZ002-N49-2015, PARA EL ARRENDAMIENTO DEL "EQUIPO FIREWALL/VPN Y CONSOLA DE ADMINISTRACIÓN PARA EXPANSIÓN DE OFICINAS TELEGRÁFICAS DE LA RED TELDAT."

JENNIFER MURILLO DOMÍNGUEZ , EN MI CARÁCTER DE REPRESENTANTE LEGAL DE LA EMPRESA GRUPO DE TECNOLOGÍA CIBERNÉTICA, S.A. DE C.V., MANIFIESTO QUE MI REPRESENTADA SE COMPROMETE A:

- ASUMIR TODOS LOS GASTOS REFERIDOS AL TRASLADO, ASEGURAMIENTO, INSTALACIÓN Y PUESTA EN OPERACIÓN DEL EQUIPO OFERTADO.
- PROPORCIONAR LOS HERRAJES PARA LOS DISPOSITIVOS CENTRALES QUE SE REQUIERE PARA SU INSTALACIÓN EN RACKS.
- EN CASO DE REUBICACIÓN DE EQUIPO OBJETO DE ESTA LICITACIÓN ATENDIENDO LAS NECESIDADES DE TELECOMM SE REALIZARÁ SIN QUE REPRESENTE ALGÚN COSTO PARA TELECOMM
- ATENDER LAS SOLICITUDES DE ACTIVACIÓN DE EQUIPO PARA LA APERTURA DE NUEVAS OFICINAS TELEGRÁFICAS DURANTE LA VIGENCIA DEL CONTRATO.

MÉXICO, D.F. A 8 DE OCTUBRE DE 2015
GRUPO DE TECNOLOGÍA CIBERNÉTICA S.A. DE C.V.

JENNIFER MURILLO DOMÍNGUEZ
REPRESENTANTE LEGAL

# CARTA COMPROMISO CONTINUIDAD EN LA OPERACIÓN

MÉXICO, D.F. A 8 DE OCTUBRE DE 2015

TELECOMUNICACIONES DE MÉXICO
DIREECCIÓN DE ADMINISTRACIÓN Y FINANZAS
SUBDIRECCIÓN DE RECURSOS MATERIALES Y SERVICIOS GENERALES
GERENCIA DE ADQUISICIONES

PRESENTE

CONVOCATORIA A LA LICITACIÓN PÚBLICA MIXTA NACIONAL No. LA-009KCZ002-N49-2015, PARA EL ARRENDAMIENTO DEL "EQUIPO FIREWALL/VPN Y CONSOLA DE ADMINISTRACIÓN PARA EXPANSIÓN DE OFICINAS TELEGRÁFICAS DE LA RED TELDAT."

JENNIFER MURILLO DOMÍNGUEZ, EN MI CARÁCTER DE REPRESENTANTE LEGAL DE LA EMPRESA GRUPO DE TECNOLOGÍA CIBERNÉTICA, S.A. DE C.V., MANIFIESTO A NOMBRE DE MI REPRESENTADA QUE SE GARANTIZA LA CONTINUIDAD EN LA OPERACIÓN DE LA INFRAESTRUCTURA QUE COMPONE EL SERVICIO OFERTADO, ESTO ES, QUE TODAS LAS FUNCIONALIDADES OBJETO DEL CONTRATO SE ENCUENTREN DISPONIBLES EN TODO MOMENTO, CONFORME A LOS NIVELES DE SERVICIO REQUERIDOS. SE PROPORCIONARÁ UN PLAN DE CONTINUIDAD Y RECUPERACIÓN A UTILIZAR EN CASO DE DESASTRE/CONTINGENCIA, ACOTADO A LOS ALCANCES Y COMPONENTES RELACIONADOS CON EL ARRENDAMIENTO.

MÉXICO, D.F. A 8 DE OCTUBRE DE 2015
GRUPO DE TECNOLOGÍA CIBERNÉTICA S.A. DE C.V.

JENNIFER MURILLO DOMÍNGUEZ
REPRESENTANTE LEGAL

PROYECTO:

"EQUIPO FIREWALL/VPN Y CONSOLA DE ADMINISTRACIÓN PARA EXPANSIÓN DE OFICINAS TELEGRÁFICAS DE LA RED TELDAT."

DOCUMENTO:

# PLAN DE CONTINUIDAD Y RECUPERACIÓN EN CASO DE DESASTRE / CONTINGENCIA

08 de Octubre de 2015

Control de cambios

| Versión | Fecha | Autor | Cambio | Aprueba |
|---|---|---|---|---|
| 1.0 | 29 septiembre 2015 | Grupo Tecno | Versión inicial | Carlos Doce |

000174

## Contenido



000175

# Resumen ejecutivo

En el presente documento se describe el plan de continuidad y recuperación ante desastres a utilizar en caso de desastre/contingencia, dicho plan queda acotado a los alcances y componentes relacionados con el arrendamiento.

A continuación se resume cada uno de los apartados del documento:

1. **Resumen ejecutivo:** este apartado.
2. **Alcance:** descripción del alcance que abarca el presente plan.
3. **Escenarios de fallo:** descripción de los distintos escaneos de fallo/desastre/contingencia contemplados en el presente documento.
4. **Planes de recuperación:** descripción de tareas a realizar ante cada escenario de fallo.

# Alcance

El alcance del presente plan se limita a los componentes de la solución ofertada para implementar VPN entre las oficinas centrales de Telecomm y las oficinas repartidas por todo el territorio Mexicano. Esta solución se basa en:

- Consolas de administración
  - Fortimanager
  - Fortianalyzer
  - Fortimanager
- Firewalls centrales
- Firewalls estatales y de oficinas telegráficas

**Limitaciones:**

El presente plan se ha escrito en base a la información disponible en las bases públicas de la convocatoria de arrendamiento de equipo firewall, y como tal, debe considerarse un borrador que se ampliará y concretará en fase de proyecto a partir del estudio *Business*

000176

*Impact Analysis* donde se estudiará el Tiempo de Recuperación Objetivo (RTO) y el Punto de Recuperación Objetivo (RPO) para los procesos afectados por la tecnología de firewalls.

Adicionalmente, durante la fase de proyecto, se definirá y ejecutará un plan de pruebas de este plan de contingencia para verificar su efectividad y medir los tiempos que se tarda en ejecutarlo.

## Escenarios de fallo

- Fallo software: al realizar un cambio en la versión del sistema operativo (actualización de firmware) o al aplicar un cambio de configuración (creación, modificación o eliminación de rutas, objetos, políticas, etc.) el equipo se desconfigura total o parcialmente impidiendo su uso normal.
- Fallo de hardware: debido a un fallo hardware el equipo deja de funcionar de forma parcial o totalmente impidiendo su uso normal. También se incluyen en este apartado fallos software que dejan al equipo inutilizable si no es con una intervención física.

## Planes de recuperación

GRUPO TECNO, antes de aplicar cualquier actualización de firmware y/o cambio en la configuración, tiene como procedimiento habitual realizar una copia completa de la configuración y tener descargada la última versión de firmware utilizada, así como la configuración de plantillas de reportes de forma individual. Adicionalmente, tenemos preparado un servidor TFTP y los comandos necesarios en caso de tener que realizar un formateo u otra acción de bajo nivel.

A continuación describimos los planes de recuperación organizados en base a los escenarios de fallo (fallo software o fallo hardware).

### Fallo software

Los fallos software se dividen en dos grupos, los debidos a un error humano al configurar el equipo (p.ej. ruta o política) y los atribuidos a un error del sistema como una actualización corrupta. Se describen estos escenarios en función del tipo de equipo.

000172

Consolas de administración y/o firewalls centrales

- Recuperación del último cambio: deshaciendo el último cambio es posible volver al estado normal de funcionamiento.

  a. En algunos casos este cambio se puede deshacer manualmente y/o regresando a un checkpoint/configuración anterior.

  b. En otros casos puede ser necesario restaurar la última configuración respaldada con funcionamiento correcto del dispositivo.

- Recuperación tras actualización fallida:

  a. Si es posible acceder a la interfaz gráfica y/o consola, cargar el firmware y configuración anterior.

  b. Si no es posible acceder al equipo, acceder mediante el puerto de consola y cargar el firmware y configuración anterior de un servidor TFTP.

Firewalls estatales y/u oficinas telegráficas

- Recuperación del último cambio: deshaciendo el último cambio es posible volver al estado normal de funcionamiento.

  a. En algunos casos este cambio se puede deshacer manualmente y/o regresando a un checkpoint/configuración anterior.

  b. En otros casos puede ser necesario restaurar la última configuración respaldada con funcionamiento correcto del dispositivo.

- Recuperación tras actualización fallida:

  a. Si es posible acceder a la interfaz gráfica y/o consola, cargar el firmware y configuración anterior.

  b. Si no es posible acceder al equipo, acceder mediante el puerto de consola y cargar el firmware y configuración anterior de un servidor TFTP.

  c. Si no es posible acceder al equipo mediante ningún mecanismo de administración remota, tratar el caso como un fallo hardware, ver .

000178

## Fallo hardware

En este apartado se incluyen fallos

### Consolas de administración y/o firewalls centrales

- Diagnosticar el fallo hardware y verificar que se requiere la sustitución de piezas o del equipo completo.
- Según el tipo de fallo:
  - Si es posible (p. Ej. Sistemas en alta disponibilidad (HA) o un único disco con fallo en sistema RAID 1, 5 o 6) seguir trabajando en modo degradado.
  - Si no es posible seguir trabajando en modo degradado:
    - Enviar de forma urgente un equipo idéntico pre-configurado.
    - Al llegar y conectar el equipo a sitio, restaurar último firmware y configuración.
    - De forma temporal:
      - Si falla una consola Fortimanager: es posible gestionar la administración de sistemas desde la otra consola Fortimanager.
      - Si falla la consola Fortianalyzer: es posible recibir eventos y generar informes desde una de las consolas Fortimanager.
      - Si fallan los firewalls centrales: es posible terminar las VPN en otro firewall y desviar el tráfico con rutas hasta su destino. La viabilidad de esta configuración se tiene que estudiar en fase de proyecto ya que depende de varios factores.
- Solicitar al fabricante las piezas o equipo en situación de fallo.
- Al recibir las piezas nuevas o nuevo equipo, aplicar último firmware y configuración en uso y sustituir las antiguas por el nuevo equipo.
- Formatear discos y configuración del equipo antiguo en situación de fallo.
- Enviar al fabricante el material en situación de fallo.

000170

Firewalls estatales y/u oficinas telegráficas

- Diagnosticar el fallo hardware y verificar que se requiere la sustitución de piezas o del equipo completo.
- Según el tipo de fallo:
  - Si es posible, seguir trabajando en modo degradado.
  - Si no es posible seguir trabajando en modo degradado:
    - Enviar de forma urgente un equipo idéntico pre-configurado.
    - Al llegar y conectar el equipo a sitio, restaurar último firmware y configuración.
- Solicitar al fabricante las piezas o equipo en situación de fallo.
- Al recibir las piezas nuevas o nuevo equipo, aplicar último firmware y configuración en uso y sustituir las antiguas por el nuevo equipo.
- Formatear discos y configuración del equipo antiguo en situación de fallo.
- Enviar al fabricante el material en situación de fallo.

ATENTAMENTE

MÉXICO, D.F., 08 DE OCTUBRE DE 2015
BAJO PROTESTA DE DECIR VERDAD,
GRUPO DE TECNOLOGÍA CIBERNÉTICA, S.A. DE C.V.

JENNIFER MURILLO DOMÍNGUEZ
REPRESENTANTE LEGAL

000160

## PROYECTO:

## "EQUIPO FIREWALL/VPN Y CONSOLA DE ADMINISTRACIÓN PARA EXPANSIÓN DE OFICINAS TELEGRÁFICAS DE LA RED TELDAT."

## DOCUMENTO:

# PLAN DE RETORNO EN CASO DE CONTINGENCIA AL MOMENTO DE LA MIGRACIÓN Y/O IMPLEMENTACIÓN

08 de Octubre de 2015

### Control de cambios

| Versión | Fecha | Autor | Cambio | Aprueba |
|---|---|---|---|---|
| 1.0 | 01 sepliembre 2015 | Grupo Tecno | Versión inicial | Carlos Doce |

000150

## Contenido



00015

# Resumen ejecutivo

En el presente documento se describe el plan de retorno (en inglés rollback) a utilizar en caso de fallo y/o situación de contingencia en caso de fallo en una migración, actualización o cambio de configuración o versiones de firmware, dicho plan queda acotado a los alcances y componentes relacionados con el arrendamiento.

A continuación se resume cada uno de los apartados del documento:

1. **Resumen ejecutivo:** este apartado.
2. **Alcance:** descripción del alcance que abarca el presente plan.
3. **Escenarios de fallo:** descripción de los distintos escenarios de fallo/ /contingencia contemplados en el presente documento.
4. **Planes de retorno:** descripción de tareas a realizar ante situación de fallo.

# Alcance

El alcance del presente plan se limita a los componentes de la solución ofertada para implementar VPN entre las oficinas centrales de Telecomm y las oficinas repartidas por todo el territorio Mexicano. Esta solución se basa en:

- Consolas de administración
  - Fortimanager
  - Fortianalyzer
- Firewalls centrales
- Firewalls estatales y de oficinas telegráficas

**Limitaciones:**

El presente plan se ha escrito en base a la información disponible en las bases públicas de la convocatoria de arrendamiento de equipo firewall, y como tal, debe considerarse un borrador que se ampliará y concretará en fase de proyecto en función de las necesidades y requerimientos específicos de Telecomm.

000152

Adicionalmente, durante la fase de proyecto, se definirá y ejecutará un plan de pruebas de este plan de retorno para verificar su efectividad y medir los tiempos que se tarda en ejecutarlo.

## Escenarios de fallo

Fallo software: al realizar un cambio en la versión del sistema operativo (actualización de firmware) o al aplicar un cambio de configuración (creación, modificación o eliminación de rutas, objetos, políticas, etc.) el equipo se desconfigura total o parcialmente impidiendo su uso normal.

## Planes de retorno

GRUPO TECNO, antes de aplicar cualquier actualización de firmware y/o cambio en la configuración, tenemos como procedimiento habitual realizar una copia completa de la configuración y tener descargada la última versión de firmware utilizada, así como la configuración de plantillas de reportes de forma individual. Adicionalmente, tenemos preparado un servidor TFTP y los comandos necesarios en caso de tener que realizar un formateo u otra acción de bajo nivel.

A continuación describimos los planes de retorno organizados en base a los equipos que pueden fallar.

### Fallo software

Los fallos software se dividen en dos grupos, los debidos a un error humano al configurar el equipo (p.ej. ruta o política) y los atribuidos a un error del sistema como una actualización corrupta.

### Consolas de administración

- Recuperación del último cambio: deshaciendo el último cambio es posible volver al estado normal de funcionamiento.
  a. En algunos casos este cambio se puede deshacer manualmente y/o regresando a un checkpoint/configuración anterior.
  b. En otros casos puede ser necesario restaurar la última configuración respaldada con funcionamiento correcto del dispositivo.

1. Ir a *System Settings* > *General* > *Dashboard*.

00015

2. En el widget *System Information* > *System Configuration*, seleccionar Restore.
3. Seleccionar el fichero de configuración anterior funcional para subirlo, este puede estar en la computadora local y/o en una memoria USB conectada al Fortimanager/Fortianalyzer.
4. Introducir la ruta y el nombre del fichero de configuración o seleccionar *Browse* para localizar el fichero.
5. Introducir una contraseña si el fichero estaba cifrado.
6. Seleccionar *Restore*.

- Recuperación tras actualización fallida:
  a. Si es posible acceder a la interfaz gráfica y/o consola, cargar el firmware y configuración anterior. Para ello acceder a la interfaz gráfica basada en Web como usuario administrador y:
     1. Ir a *System Settings* > *General* > *Dashboard*.
     2. En el widget *System Information* > *Firmware Version*, seleccionar *Update*.
     3. Introducir la ruta y el nombre del fichero de firmware o seleccionar *Browse* para localizar el fichero.
     4. Seleccionar *OK*.
     5. La unidad Fortimanager/Fortianalyzer subirá la imagen de firmware, actualizará a la versión de firmware, reiniciará y mostrará el login de Fortigate. Este proceso puede tardar varios minutos.
     6. Posteriormente verificar que la configuración del equipo es la correcta, si no es el caso, restaurar la configuración.

  b. Si no es posible acceder al equipo, acceder mediante el puerto de consola y cargar el firmware y configuración anterior de un servidor TFTP.
     1. Verificar que el servidor de TFTP se está ejecutando en el equipo local.
     2. Copiar el nuevo firmware al directorio raiz del servidor TFTP.
     3. Acceder por linea de comandos (CLI).

000154

4. Verificar que la unidad Fortimanager/Fortianalyzer puede conectar al servidor TFTP. Para ello pueden usar el siguiente comando. Suponiendo que la dirección IP del servidor TFTP es 192.168.1.100:

   execute ping 192.168.1.100

5. Introducir el siguiente comando para copiar la imagen del firmware del servidor TFTP a la unidad Fortigate:

   execute restore image tftp <filename> <tftp_ipv4>

   Donde <name_str> es el nombre de la imagen del firmware y <tftp_ip4> es la dirección IP del servidor TFTP. Por ejemplo, si el nombre de la imagen de firmware is image.out y la dirección IP del servidor TFTP es 192.168.1.100, introducir:

   execute restore image tftp image.out 192.168.1.100

6. La unidad Fortimanager/Fortianalyzer responderá con el siguiente mensaje:

   This operation will replace the current firmware version!
   Do you want to continue? (y/n)

7. Escribir y.
8. La unidad Fortimanager/Fortianalyzer subirá la imagen de firmware, actualizará a la versión de firmware, reiniciará y mostrará el login de Fortimanager/Fortianalyzer. Este proceso puede tardar varios minutos.
9. Posteriormente verificar que la configuración del equipo es la correcta, si no es el caso, restaurar la configuración.
10. Acceder a la consola (CLI).
11. Finalmente, verificar que el sistema funciona correctamente. Para ello escribir:

    get system status

## Firewalls centrales, firewalls estatales y/u oficinas telegráficas

- Recuperación del último cambio: deshaciendo el último cambio es posible volver al estado normal de funcionamiento.
  a. En algunos casos este cambio se puede deshacer manualmente y de esta manera regresar a una configuración anterior.

000156

b. En otros casos puede ser necesario restaurar la última configuración respaldada con funcionamiento correcto del dispositivo. Para ello hay dos formas, el primer método desde la consola del propio firewall, el segundo desde la consola de Fortimanager.

i. Método 1, acceder a la interfaz gráfica basada en Web del dispositivo con fallo y:

1. Ir a *System* > *Dashboard* > *Status*.
2. En el widget *System Information*, seleccionar *Restore* para la *System Configuration*.
3. Seleccionar el fichero de configuración anterior funcional para subirlo, este puede estar en la computadora local y/o en una memoria USB conectada al Fortimanager. También es posible restaurar la configuración desde la consola de Fortimanager.
4. Introducir la ruta y el nombre del fichero de configuración o seleccionar *Browse* para localizar el fichero.
5. Introducir una contraseña si el fichero estaba cifrado.
6. Seleccionar *Restore*.

ii. Método 2, acceder a la interfaz gráfica basada en Web de Fortimanager y:

1. Ir a *Device manager* seleccionar el ADOM correcto bajo *Devices & Groups* seleccionar el dispositivo en situación de fallo.
2. En el panel de la derecha dentro del Widget *Configuration and Instalation status* seleccionar *Revision history*.
3. En la nueva pantalla que aparece seleccionar la versión de configuración con funcionamiento correcto, habitualmente debe ser la última que aparece.
4. Seleccionar la opción *Install* y esperar algunos minutos a que instale la nueva configuración e reinicie el equipo.

- Recuperación tras actualización fallida:

a. Si es posible acceder a la interfaz gráfica y/o consola, cargar el firmware y configuración anterior. Para ello acceder a la interfaz gráfica basada en Web como usuario administrador y:

1. Ir a *System* > *Dashboard* > *Status*.

000156

2. En el widget *System Information* > *Firmware Version*, seleccionar *Update*.
3. Introducir la ruta y el nombre del fichero de firmware o seleccionar *Browse* para localizar el fichero.
4. Seleccionar *OK*.
5. La unidad FortiGate subirá la imagen de firmware, actualizará a la versión de firmware, reiniciará y mostrará el login de Fortigate. Este proceso puede tardar varios minutos.
6. Posteriormente verificar que la configuración del equipo es la correcta, si no es el caso, restaurar la configuración.
7. Finalmente, actualizar firmas de antivirus, IPS y control de aplicaciones. Para ello acceder a System > Config > Fortiguard y seleccionar en la sección "AV & IPS Download options" el botón que dice "Update now", esperar dos minutos y recargar para verificar que ya está actualizado.

b. Si no es posible acceder al equipo, acceder mediante el puerto de consola y cargar el firmware y configuración anterior de un servidor TFTP.

1. Verificar que el servidor de TFTP se está ejecutando en el equipo local.
2. Copiar el nuevo firmware al directorio raíz del servidor TFTP.
3. Acceder por línea de comandos (CLI).
4. Verificar que la unidad FortiGate puede conectar al servidor TFTP. Para ello pueden usar el siguiente comando. Suponiendo que la dirección IP del servidor TFTP es 192.168.1.100:

   execute ping 192.168.1.100

5. Introducir el siguiente comando para copiar la imagen del firmware del servidor TFTP a la unidad Fortigate:
   execute restore image tftp <filename> <tftp_ipv4>
   Donde <name_str> es el nombre de la imagen del firmware y <tftp_ip4> es la dirección IP del servidor TFTP. Por ejemplo, si el nombre de la imagen de firmware is image.out y la dirección IP del servidor TFTP es 192.168.1.100, introducir:
   execute restore image tftp image.out 192.168.1.100
6. La unidad Fortigate responderá con el siguiente mensaje:
   This operation will replace the current firmware version!
   Do you want to continue? (y/n)

7. Escribir y.
8. La unidad FortiGate subirá la imagen de firmware, actualizará a la versión de firmware, reiniciará y mostrará el login de Fortigate. Este proceso puede tardar varios minutos.
9. Posteriormente verificar que la configuración del equipo es la correcta, si no es el caso, restaurar la configuración.
10. Acceder a la consola (CLI).
11. Finalmente, actualizar firmas de antivirus, IPS y control de aplicaciones. Para ello escribir:

    execute update-now

c. Si no es posible acceder al equipo mediante ningún mecanismo de administración remota, tratar el caso como un fallo hardware, ver el manual "Telecomm - Fortinet - Plan de Continuidad y Recuperación 20150929 v1.0".

ATENTAMENTE

MÉXICO, D.F., 08 DE OCTUBRE DE 2015
BAJO PROTESTA DE DECIR VERDAD,
GRUPO DE TECNOLOGÍA CIBERNÉTICA, S.A. DE C.V.

JENNIFER MURILLO DOMÍNGUEZ
REPRESENTANTE LEGAL

# PROYECTO:

# "EQUIPO FIREWALL/VPN Y CONSOLA DE ADMINISTRACIÓN PARA EXPANSIÓN DE OFICINAS TELEGRÁFICAS DE LA RED TELDAT."

# DOCUMENTO:

# PROCEDIMIENTO Y ESCALACIÓN PARA LA ATENCIÓN DE FALLAS

08 de Octubre de 2015

Control de cambios

| Versión | Fecha | Autor | Cambio | Aprueba |
|---|---|---|---|---|
| 1.0 | 29 septiembre 2015 | Grupo Tecno | Versión inicial | Daniel Fernandez |

| Propietario | | | |
|---|---|---|---|
| Nombre | Área/Depto. | Teléfono | Correo Electrónico |
| Daniel Eduardo Fernández Mejia | Gerente de Mesa de Ayuda y NOC. | 5278 9210 ext. 1507 | daniel.fernandez@tecno.com.mx |

## Contenido

# PROCEDIMIENTO Y ESCALACIÓN PARA LA ATENCIÓN DE FALLAS

## 1. Definición de Mesa de Ayuda.

De acuerdo con la Biblioteca de Infraestructuras de Tecnologías de la Información (ITIL® por sus siglas en inglés), dentro de la gestión del servicio, la Mesa de Ayuda proveerá a TELECOMM y al personal que así lo designe, un solo punto de contacto para reportar fallas o realizar solicitudes específicas.

Adicionalmente brindará seguimiento a los reportes recibidos, supervisando al personal, o fabricante asignado para la resolución de la petición; proporcionará información estadística sobre la operación o continuidad del servicio.

Grupo Tecno pondrá a su disposición una Mesa de ayuda alienada las mejores prácticas ITIL®, los procesos que ofrece dentro del servicio que brindaremos a su organización son:

- Gestión de Accesos.
- Gestión de Incidentes.
- Gestión de Solicitudes.

A través de estos procesos, se garantizará el acceso al servicio solo al personal autorizado, y a través de la gestión de incidentes, se garantizará la atención de las fallas que usted o su personal reporte a la Mesa de Ayuda de Grupo Tecno.

## 2. Gestión de accesos, incidentes y solicitudes.

La gestión de accesos agilizará la atención a los usuarios autorizados por TELECOMM para reportar incidentes, asegura también que sólo el personal registrado previamente tenga acceso a la información.

El proceso de gestión de incidentes tiene por objeto restaurar el servicio lo más pronto posible y minimizar el impacto al negocio. Es importante mencionar que el soporte de Grupo Tecno está enfocado a restaurar el servicio, aplicando los workarounds o soluciones que el especialista aplique con base en su conocimiento o documentados en la base de conocimientos.

Por su parte la gestión de solicitudes, tiene por objeto atender de manera rápida solicitudes pre aprobadas, las cuales no afectan de ninguna manera la continuidad del negocio.

000165

**2.1 Contacto.**

Para reportar un incidente o solicitud, TELECOMM deberá contactar a la mesa de ayuda de Grupo Tecno a través de alguno de los siguientes medios:

1. Vía telefónica: Para el D.F y Área Metropolitana al **5278 9211** y para el resto de la República Mexicana al **01 800 248 0888**

2. Vía WEB: Será definido en coordinación con TELECOMM

3. Vía correo electrónico: servicedesk@tecno.com.mx

Cuando una petición es atendida por cualquiera de estos medios, la mesa de ayuda generará un número de caso o ticket, mismo que le será proporcionado a TELECOMM, y será enviado por correo electrónico a la dirección del personal que levante el incidente y se pondrá en copia al personal que el TELECOMM defina, esto servirá para validar el tiempo desde la generación del ticket hasta su solución, dicho número servirá como referencia para solicitar actualizaciones, estatus o avance del caso.

**2.2 Prioridad.**

A cualquier ticket correspondiente a un incidente o solicitud, se le asigna un nivel de prioridad, la cual dependerá de la afectación que el servicio este presentando. La definición de la prioridad está definida conforme a los SLA´s (Niveles de Servicio) expresados en el presente proceso licitatorio:

| | |
|---|---|
| 1<br>Crítico | Equipos que por su operación se consideran de nivel crítico; Consolas, Firewall 's Appliance Centrales de TCT, CTO y TGO., Firewall 's Appliance Remotos de Gerencias Estatales y Unidades Administrativas, |
| 2<br>Alto | Equipos que por su operación se consideran de nivel alto; Firewalls Appliances Remotos de Oficinas Telegráficas. |
| 3<br>Bajo | Equipos que por su operación se consideran de nivel bajo; Firewalls Appliances Remotos de Oficinas Telegráficas, para los cuales se requiere una atención no mayor a 48 horas. Considerando tiempo de traslado mayor a 3 hrs. desde la capital del estado a sitio remoto. |

### 2.3 Niveles de servicio.

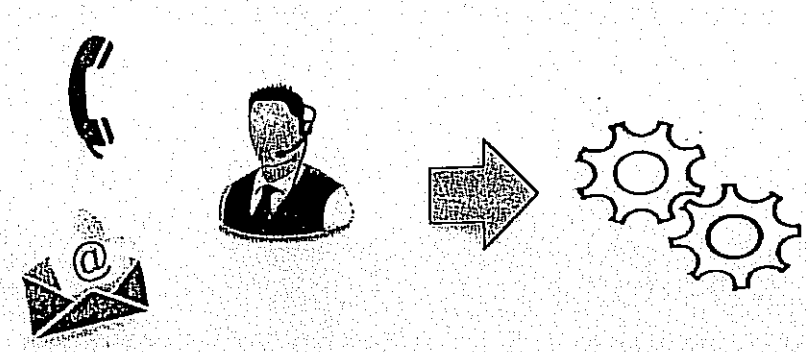
Los niveles de servicio a cubrir son de acuerdo a la prioridad son:

| | | |
|---|---|---|
| 1<br>Crítico | 1 hora. | No mayor a 6 horas. |
| 2<br>Alto | 1 hora. | No mayor a 24 horas.<br>*Considerando tiempo de traslado máximo de 3 hrs. desde la capital del estado a sitio remoto.* |
| 3<br>Bajo | 1 hora. | No mayor a 48 horas.<br>*Considerando tiempo de traslado mayor a 3 hrs. desde la capital del estado a sitio remoto.* |

La atención se brindará en un esquema 7x24x365.

### 2.4 Flujo de atención a tickets.

Una vez que se ha asignado un número de ticket y se ha establecido el nivel de prioridad, la atención de los mismos será canalizada al personal de ingeniería de Grupo Tecno y/o al soporte del fabricante y la mesa de ayuda de Grupo Tecno, vigilará que la atención se de en tiempo y forma.



Registro y asignación de prioridad

Soporte técnico

**2.5 Requisitos para el registro y atención de incidentes y solicitudes.**

Para poder dar una atención rápida a un incidente o solicitud reportados a la mesa de ayuda, es necesario que TELECOMM tome en cuenta los siguientes puntos:

El usuario que llame deberá proporcionar nombre completo, cargo, correo electrónico y/o algún otro medio de contacto para poder ser localizarlo.

Deberá proporcionar el número de serie y modelo del equipo que presente fallas.

Proporcionar a la mesa de ayuda una descripción detallada de la falla o de la solicitud, de ser posible proporcionar logs, fotografías, códigos de error, etc.

Conservar el número de ticket proporcionado por la mesa de ayuda para el seguimiento del caso.

Estar disponible ante cualquier solicitud por parte del grupo de soporte, incluyendo sesiones remotas o acceso a las instalaciones.

Se notificará vía correo electrónica una vez que el incidente haya sido resuelto, en este correo se incluirá una descripción de cómo fue resuelto, el diagnóstico y recomendaciones para evitar que el incidente se repita.

3. Escalación

La escalación sirve cuando el servicio brindado no está cumpliendo las expectativas de cliente, no se ha cumplido con los niveles de servicio o bien un nivel superior dentro del organigrama debe estar enterado de la situación.

### 3.1 Directorio de escalación.

| | |
|---|---|
| N4 – Dirección de Servicios Profesionales Sergio Navarro Barrientos<br>Tel. 5278 9210 ext. 1500 | Se involucra cuando no hay una solución satisfactoria sobre todo en un caso considerado como crítico o prioridad 1. Si el manejo del incidente no es el adecuado |
| N3 – Gerencia de Entrega de Servicios<br>Mauricio Sáenz Amezcua<br>Tel. 5278 9210 ext. 1400 | Se escala a la gerencia cuando los SLA's están por vencerse y el incidente continua sin solucionarse. Se involucra desde el principio cuando el caso reportado tiene un impacto |
| N2 – Service Delivery Manager<br>Abraham Espinosa Carbajal.<br>Tel. 5278 9210 ext. 3102 | Aunque es un segundo nivel de escalación se encuentra involucrado desde que el caso es generado. Se accede a él cuando el servicio ofertado ha tenido desviaciones o no cumple con las expectativas del cliente. |
| N1 – Gerencia de Mesa de Ayuda.<br>Daniel Eduardo Fernández Mejía<br>Tel. 5278 9210 ext. 1507 | Se realiza la escalación cuando el operador de mesa de ayuda no brinda un trato adecuado al usuario o bien no ha dado un seguimiento puntual al caso. |

ATENTAMENTE

MÉXICO, D.F., 08 DE OCTUBRE DE 2015
BAJO PROTESTA DE DECIR VERDAD,
GRUPO DE TECNOLOGÍA CIBERNÉTICA, S.A. DE C.V.

JENNIFER MURILLO DOMÍNGUEZ
REPRESENTANTE LEGAL

GRUPOTECNO

16625

I.B

MÉXICO, D.F. A 8 DE OCTUBRE DE 2015

TELECOMUNICACIONES DE MÉXICO
DIREECCIÓN DE ADMINISTRACIÓN Y FINANZAS
SUBDIRECCIÓN DE RECURSOS MATERIALES Y SERVICIOS GENERALES
GERENCIA DE ADQUISICIONES

PRESENTE

CONVOCATORIA A LA LICITACIÓN PÚBLICA MIXTA NACIONAL No. LA-009KCZ002-N49-2015, PARA EL ARRENDAMIENTO DEL "EQUIPO FIREWALL/VPN Y CONSOLA DE ADMINISTRACIÓN PARA EXPANSIÓN DE OFICINAS TELEGRÁFICAS DE LA RED TELDAT".

JENNIFER MURILLO DOMÍNGUEZ EN MI CARÁCTER DE REPRESENTANTE LEGAL DE LA EMPRESA GRUPO DE TECNOLOGÍA CIBERNÉTICA S.A. DE C.V., MANIFIESTO QUE PARA DAR CUMPLIMIENTO AL PUNTO DE REFERENCIA EL EQUIPO "ACT1, ACT2, ACT3" PROPUESTO CUENTA CON LA SIGUIENTE CANTIDAD DE PUERTOS DE FORMA NATIVA, SIN NECESIDAD DE AGREGAR MÓDULOS ADICIONALES:

AL MENOS 16 PUERTOS ETHERNET 10/100/1000 BASE T.
AL MENOS 16 PUERTOS 1 GBPS SFP.
AL MENOS 8 PUERTOS ÓPTICOS 10GB SFP+ EN TECNOLOGÍA SR.

MÉXICO, D.F. A 8 DE OCTUBRE DE 2015
GRUPO DE TECNOLOGÍA CIBERNÉTICA S.A. DE C.V.

JENNIFER MURILLO DOMÍNGUEZ
REPRESENTANTE LEGAL

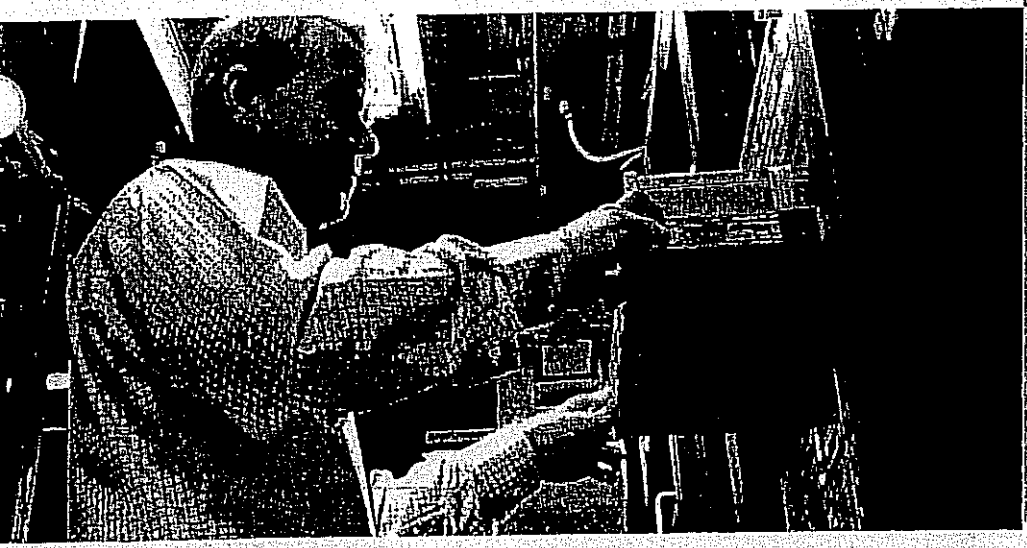
FORTINET

DATA SHEET

16626

FortiGate® 1500D

High Performance Next Generation/ Edge Firewall for the Enterprise



# FortiGate 1500D

FortiGate 1500D and 1500D-DC

Every day you're on the lookout for sophisticated attacks designed to penetrate your organization and steal valuable information. At the same time, you need to increase network speeds and capacities to accommodate the proliferation of consumer-grade applications and devices. To adequately defend against threats across such a broad range of applications and devices — without slowing down your network — you need a high performance next generation/edge firewall (NGFW) appliance for deep inspection, visibility and control.

## Breakthrough Performance

The FortiGate 1500D and 1500D-DC high performance next generation/edge firewalls deliver best-in-class performance with an exceptional 80 Gbps of firewall and 11 Gbps of next generation threat protection. Custom hardware, including the latest FortiASIC™ NP6 processors, and the consolidated security features of the FortiOS™ 5 network security platform make the difference in enabling protection of your applications and network without affecting availability or performance.

## Features & Benefits

- Industry-leading 5x next generation firewall performance and 10x data center firewall
- NSS Labs Recommended NGFW and NGIPS delivers top-rated protection
- Integrated high port density delivers maximum flexibility and scalability
- Intuitive management interface enables broad and deep visibility and control
- Application control plus identity and device-based policy enforcement provides more granular protection

## Highlights

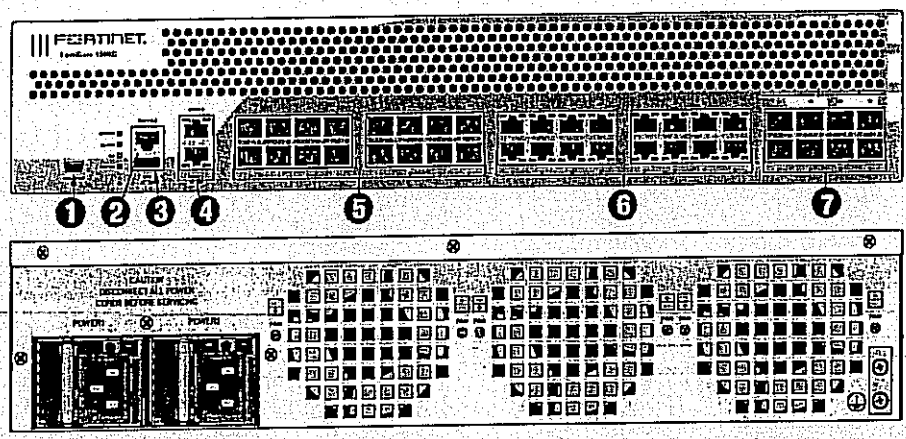
| Firewall Performance | IPS Performance | Interfaces |
|---|---|---|
| 80 Gbps | 11 Gbps | Multiple 10 GE SPF+, GE SFP and GE RJ45 |

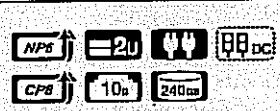
000008

16627

# HARDWARE

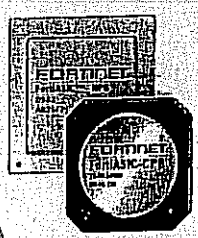
## FortiGate 1500D and 1500D-DC




### Interfaces

1. USB Management Port
2. Console Port
3. USB Port
4. 2x GE RJ45 Management Ports
5. 16x GE SFP Slots
6. 16x GE RJ45 Ports
7. 8x 10 GE SFP+ Slots



### Powered by FortiASICs

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

### Network Processor

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

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

### Content Processor

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

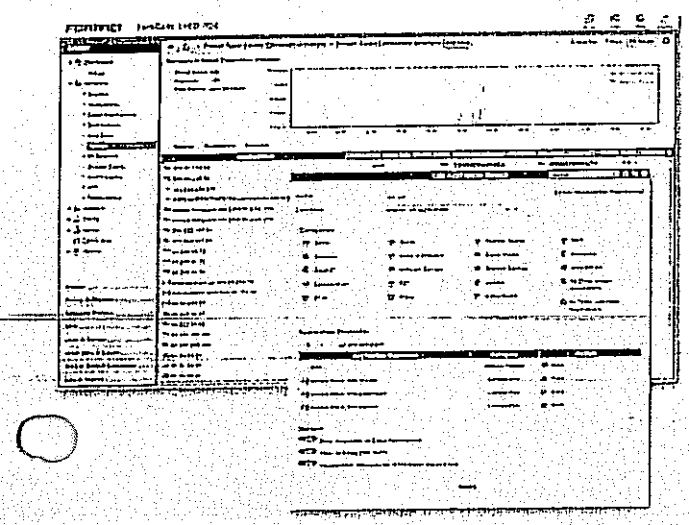
- Signature-based content inspection acceleration
- Encryption and decryption offloading

### 10 GE Connectivity

High speed connectivity is essential for network security segmentation at the core of data networks. The FortiGate 1500D and FG-1500D-DC provide high 10 GE port density, simplifying network designs without relying on additional devices to bridge desired connectivity.

16628

# SOFTWARE



FortiOS Managment UI — FortiView and Application Control Panel

## FortiOS

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

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

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

# SERVICES

## FortiGuard™ Security Services

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

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

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

## FortiCare™ Support Services

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

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

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

000010

# SPECIFICATIONS

| | FortiGate 1500D and 1500D-DC |
|---|---|
| **Hardware Specifications** | |
| Hardware Accelerated 10 GE SFP+ Slots | 8 |
| Hardware Accelerated GE SFP Slots | 16 |
| Hardware Accelerated GE RJ45 Ports | 16 |
| GE RJ45 Management / HA Ports | 2 |
| USB Ports (Client / Server) | 1 / 1 |
| Console Port | 1 |
| Onboard Storage | 240 GB |
| Included Transceivers | 2x SFP+ (SR 10GE) |
| **System Performance** | |
| IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP) | 80 / 80 / 55 Gbps |
| IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP) | 80 / 80 / 55 Gbps |
| Firewall Latency (64 byte, UDP) | 3 µs |
| Firewall Throughput (Packet per Second) | 82.5 Mpps |
| Concurrent Sessions (TCP) | 12 Mi |
| New Sessions/Second (TCP) | 250,000 |
| Firewall Policies | 100,000 |
| IPsec VPN Throughput (512 byte) | 50 Gbps |
| Gateway-to-Gateway IPsec VPN Tunnels | 20,000 |
| Client-to-Gateway IPsec VPN Tunnels | 50,000 |
| SSL-VPN Throughput | 4 Gbps |
| Concurrent SSL-VPN Users (Recommended Maximum) | 10,000 |
| IPS Throughput | 11 Gbps |
| Antivirus Throughput | 4.3 Gbps |
| CAPWAP Clear-text Throughput (HTTP) | 12.30 Gbps |
| Virtual Domains (Default / Maximum) | 10 / 250 |
| Maximum Number of FortiAPs (Total / Tunnel) | 4,096 / 1,024 |
| Maximum Number of FortiTokens | 5,000 |
| Maximum Number of Registered Endpoints | 8,000 |
| High Availability Configurations | Active-Active, Active-Passive, Clustering |

| | FortiGate 1500D and 1500D-DC |
|---|---|
| **Dimensions** | |
| Height x Width x Length (inches) | 3.5 x 17.24 x 21.81 |
| Height x Width x Length (mm) | 89 x 438 x 554 |
| Weight | 32.50 lbs (14.70 kg) |
| Form Factor | Rack Mount, 2 RU |
| **Power** | |
| AC Power Supply | 100–240V AC, 47–63 Hz |
| DC Power Supply (FG-1500D-DC) | 40.5–57V DC |
| Maximum Current | 110V / 8A, 220V / 4A |
| Power Consumption (Average / Maximum) | 338 / 406 W |
| Heat Dissipation | 1,385 BTU/h |
| Redundant Power Supplies | Yes, Hot swappable |
| **Environment** | |
| Operating Temperature | 32–104°F (0–40°C) |
| Storage Temperature | -31–158°F (-35–70°C) |
| Humidity | 15–90% non-condensing |
| Operating Altitude | Up to 7,400 ft (2,250 m) |
| **Compliance** | |
| | FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB |
| **Certifications** | |
| | ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN |

Note: All performance values are "up to" and vary depending on system configuration. Antivirus performance is measured using 44 Kbyte HTTP files. IPS performance is measured using 1 Mbyte HTTP files. IPsec VPN performance is based on 512 byte UDP packets using AES-256+SHA1. Antivirus Throughput is measured in proxy mode.

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

# ORDER INFORMATION

| Product | SKU | Description |
|---|---|---|
| FortiGate 1500D | FG-1500D | 8x 10 GE SFP+ slots, 16x GE SFP slots, 16x GE RJ45 ports (including 16x ports, 2x management/HA ports), FortiASIC NP6 and CP8 hardware accelerated, 240 GB SSD onboard storage, dual AC power supplies. |
| FortiGate 1500D-DC | FG-1500D-DC | 8x 10 GE SFP+ slots, 16x GE SFP slots, 16x GE RJ45 ports (including 16x ports, 2x management/HA ports), FortiASIC NP6 and CP8 hardware accelerated, 240 GB SSD onboard storage, dual DC power supplies |
| **Optional Accessories** | | |
| 1 GE SFP LX transceiver module | FG-TRAN-LX | 1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots. |
| 1 GE SFP RJ45 transceiver module | FG-TRAN-GC | 1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots. |
| 1 GE SFP SX transceiver module | FG-TRAN-SX | 1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots. |
| 10 GE SFP+ transceiver module, short range | FG-TRAN-SFP+SR | 10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots |
| 10 GE SFP+ transceiver module, long range | FG-TRAN-SFP+LR | 10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots |
| 10 GE SFP+ active direct attach cable, 10m / 32.8 ft | SP-CABLE-ADASFP+ | 10 GE SFP+ active direct attach cable, 10m / 32.8 ft for all systems with SFP+ and SFP/SFP+ slots |
| Rack mount sliding rails | SP-FG3040B-RAIL | Rack mount sliding rails for FG-1000C/-DC, FG-1500D, FG-3040B/-DC, FG-3140B/-DC, FG-3240C/-DC, 3700D and 3950B/-DC |
| AC power supply | SP-FG1240B-PS | AC power supply for FG-1240B, FG-1500D, FG-3040B and FG-3140B |
| DC power supply | SP-FG1500D-DC-PS | DC power supply for FG-1500D-DC |

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

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

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

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

GRUPOTECNO

16630

I.C.

MÉXICO, D.F. A 8 DE OCTUBRE DE 2015

TELECOMUNICACIONES DE MÉXICO
DIREECCIÓN DE ADMINISTRACIÓN Y FINANZAS
SUBDIRECCIÓN DE RECURSOS MATERIALES Y SERVICIOS GENERALES
GERENCIA DE ADQUISICIONES

PRESENTE

CONVOCATORIA A LA LICITACIÓN PÚBLICA MIXTA NACIONAL No. LA-009KCZ002-N49-2015, PARA EL ARRENDAMIENTO DEL "EQUIPO FIREWALL/VPN Y CONSOLA DE ADMINISTRACIÓN PARA EXPANSIÓN DE OFICINAS TELEGRÁFICAS DE LA RED TELDAT".

JENNIFER MURILLO DOMÍNGUEZ EN MI CARÁCTER DE REPRESENTANTE LEGAL DE LA EMPRESA GRUPO DE TECNOLOGÍA CIBERNÉTICA S.A. DE C.V., MANIFIESTO QUE PARA DAR CUMPLIMIENTO AL PUNTO DE REFERENCIA LOS EQUIPOS PROPUESTOS CUENTAN CON LAS SIGUIENTES FUNCIONALIDADES DE SEGURIDAD, LAS CUALES SON DE LA MISMA MARCA DEL EQUIPO OFERTADO:

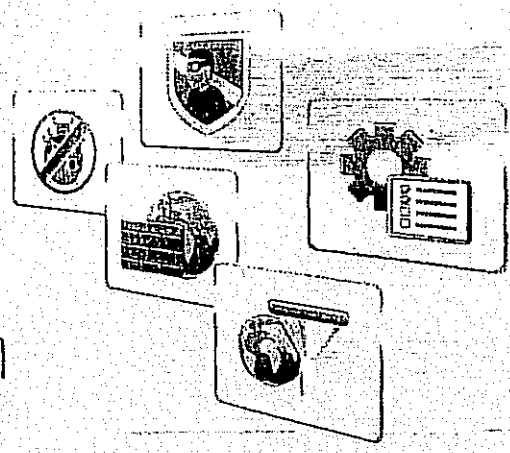
1. ANTI MALWARE
2. IPS (DETECCIÓN DE ATAQUES DE RED Y PROTECCIÓN A DOS Y DDOS)
3. CAPACIDAD DE DETECTAR Y BLOQUEAR APLICACIONES, TRÁFICO MALICIOSO Y ANOMALÍAS DE TRÁFICO EN PROTOCOLOS HTTP Y HTTPS.
4. CAPACIDAD DE DESCRIPCIÓN DE TRÁFICO SSL DE ENTRADA Y SALIDA.

MÉXICO, D.F. A 8 DE OCTUBRE DE 2015
GRUPO DE TECNOLOGÍA CIBERNÉTICA S.A. DE C.V.

JENNIFER MURILLO DOMÍNGUEZ
REPRESENTANTE LEGAL

0000

FORTINET



# FortiOS® 5.2 Network Security Operating System

## For Unified Threat Management

FortiOS is a security-hardened, purpose-built Operating System that is the foundation of all FortiGate® network security platforms from our entry-level devices to our most powerful carrier-grade models. FortiOS 5.2 includes over 150 standard features, and many new enhancements that help fight advanced threats, simplify FortiGate installations and expand threat reporting and management.

*Rich feature set for protecting your applications, data and users.*

- Enterprise grade security for any sized organization
- Easy to deploy and manage
- Outstanding manageability with consolidated security and access control setup
- Strong and flexible user and device management with multiple authentication options

### Robust Complete Network Security

No matter how large or small your organization is, you face numerous challenges as your network environment, usage patterns and security threats evolve. FortiOS gives you the latest in all-in-one network security protection that's easy to deploy and manage. Besides the industry's best firewall, intrusion protection and VPN you get Advanced Threat Protection that fights against advanced persistent threats (ATPs) and additional features like email filtering, data-loss prevention and vulnerability scanning - a complete Unified Threat Management (UTM) solution for your business.

### Flexible Architecture that Adapts with Your Needs

Whether you need a simple firewall or a complete UTM installation, FortiOS gives you the flexibility to easily configure the options you need for your environment. From a "single pane of glass" you can set up, manage, and get detailed reporting on your network and security threats, all within minutes.

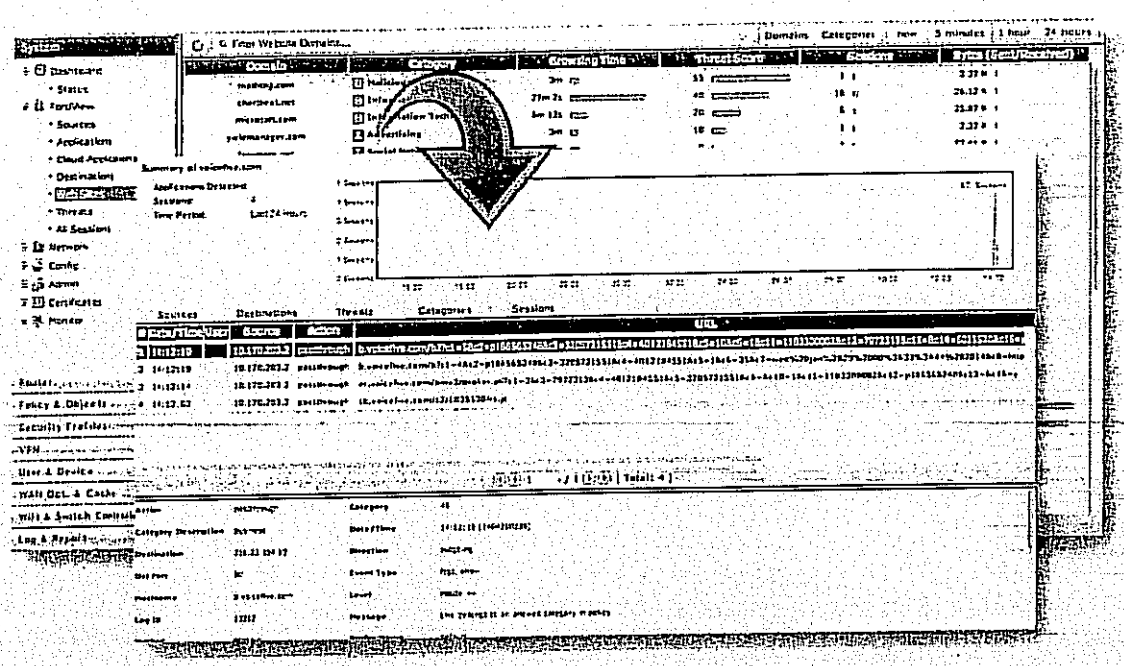
### Key Features & Benefits

| | |
|---|---|
| Unified Threat Management | Comprehensive network security protection with advanced threat protection, email filtering, data-loss prevention and vulnerability scanning. |
| Intuitive and Customizable | Easy to configure and manage with the flexibility to choose the security and UTM options you need. |
| Advanced Network Segmentation | Support for multiple zones and VDOMs to meet your data protection and compliance requirements. |

ICSA labs ICSA labs ICSA labs

ICSA labs ICSA labs

000014



*FortiOS web-based GUI — FortiView on-demand query tool*

## Complete Security

Fortinet designed and built FortiOS 5.2 to deliver the advanced protection and performance that standalone products simply can't match. The services work together as a system to provide better visibility and mitigation of the latest network and application threats, stopping attacks before damage can occur.

## Unique Visibility and Control

Advanced security features such as flow-based inspection and integrated wireless controller capability allow you to monitor and protect your wired and wireless networks from endpoints to the core, and from remote offices to headquarters. FortiOS allows greater traffic visibility and more consistent, granular control over users, applications and sensitive data.

## Easier to Manage

FortiOS 5.2 lowers costs and reduces IT staff workloads. Physical or virtual FortiGate appliances give you the flexibility to match your security to your environment while enforcing a uniform security policy. Single pane of glass management and centralized analysis ensure consistent policy creation and enforcement while minimizing deployment and configuration challenges.

## Securing Mobile Devices

FortiOS 5.2 helps secure mobile device and BYOD environments (including iOS®, Android® and Windows® clients) by identifying devices and applying specific access policies as well as security profiles, according to the device type or device group, location, and usage.

## Client Reputation

Signature-based security alone is not enough anymore; it is now critical to understand how devices on your network are behaving. FortiView with threat score provides a cumulative security ranking of each client device on your network based on a range of behaviors. It provides specific, actionable information that helps identify compromised systems and potential zero-day attacks in real time.

## Smart Policies

FortiOS 5.2 enables intelligent, automatic adjustment of role-based policies for users and guests based on location, data, and application profile. Enhanced reporting and analysis provides deeper insights into the behavior of your network, users, devices, applications and threats.

000015

## Extensive Network Support

FortiOS supports numerous network design requirements and interoperates with other networking devices. This includes support for a wealth of routing, multicasting and network resiliency protocols. Administrators can also configure interfaces for VLANs, VLAN trunks, port aggregation and one-armed sniffer mode.

It also offers robust high-availability and clustering options, including advanced sub-second failover, virtual clusters and much more.

## Unified Access Security

FortiOS empowers organizations to apply consistent ...cies across various types of networks, simplifying policy enforcement in today's complex environments. Its wireless controller features extend the same protection to wireless networks while endpoint control capabilities provision and enforce security for mobile users even when they are away from the office.

## Device ID and User ID Access Control

FortiOS supports both local and remote authentication services such as LDAP, Radius and TACACS+ to identify users and apply access policies and security profiles accordingly. It simplifies identity-based implementations and also provides a seamless user authorization experience with various single sign-on capabilities. FortiOS can capture terminal service user or wireless login credentials, among others, and intelligently apply policies and profiles without additional user input.

...levice types continue to evolve, you'll be ready with ...evice access control. You can apply security policies based on the type of device such as computers, tablets or phones and apply different policies depending if the devices are company or privately owned.

## Sophisticated Application Control

Identifying applications and providing relevant enforcement is essential in the current Web 2.0 and cloud environments. FortiOS offers gradual controls and can identify over 3,000 applications, even those on encrypted channels. It also offers mitigation against sophisticated botnet activities that easily evade traditional firewalls.

## Physical and Virtual Segmentation

From simple small wired networks to the complex multi-tenant managed datacenter environments, FortiOS supports everything you need to set up and manage your network traffic. You can configure physical network segmentation using the LAN ports built-in to every FortiGate, or you can provide virtual segmentation using virtual LANs (VLANs).

## Powerful & Scalable Management

FortiManager makes it easy to provision and manage thousands of FortiGate devices in a distributed organization. Using standardized setup profiles, you get the ability to configure a standard set of policy and provisioning workflows to meet your business needs or compliance standards. Detailed configuration audit trails are supported and can reside externally on secured storage with FortiAnalyzer.

FortiOS also integrates well with third-party solutions such as Network Management Systems and SIEMs through Fortinet's technology alliances.

*FortiGate® - High performance Network Security Platform*

- **ASIC-Powered Performance**
  FortiGate purpose-built hardware delivers unmatched price/performance for the most demanding networking environments. FortiASIC processors ensure that your network security solution does not become a network bottleneck.
- **High speed and Flexible Connectivity**
  The FortiGate product family offer a variety of interfaces for today's network, ranging from integrated WAN interfaces, 3G/4G USB wireless broadband support to high speed 40G interfaces for data centers.
- **Broad Product Offerings**
  The FortiGate product family scales from desktop units for remote branch offices, mid-range for small and medium enterprises to high-end platforms for service providers and data centers

000016

# FEATURE SUMMARY

16634

## Network Services and Support

- Built-in DHCP, NTP, DNS Server and DNS proxy (available on most models)
- FortiGuard NTP, DDNS and DNS service
- Interface modes: sniffer, port aggregated, loopback, VLANs (802.1Q and Trunking), virtual hardware, software and VLAN switches (available on most models)
- Static and policy routing
- Hybrid WAN support: load balancing and redundancy with link health check on monitoring using TWAMP
- Support USB 3G/4G Wireless WAN modems
- Dynamic routing protocols:
  - RIPv1 and v2, OSPF v2 and v3, ISIS, BGP4
- Multicast traffic: sparse and dense mode, PIM support
- Content routing: WCCP and ICAP
- Traffic shaping and QoS per policy or applications: shared policy shaping, per-IP shaping, maximum & guaranteed bandwidth, maximum concurrent connections per IP, traffic prioritization, Type of Service (TOS) and Differentiated Services (DiffServ) support
- IPv6 Support: Management over IPv6, IPv6 routing protocols, IPv6 tunnelling, firewall and UTM for IPv6 traffic, NAT46, NAT64, IPv6 IPSEC VPN

## WAN Optimization, Web Cache and Explicit Proxy^

- Single and out-of-path WAN optimization topology, peer to peer and remote client support
- Transparent Mode option: keeps the original source address of the packets, so servers appear to receive traffic directly from clients.
- WAN optimization techniques: protocol optimization and byte caching
- WAN Optimization protocols supported: CIFS, FTP, HTTP(S), MAPI, TCP
- Secure Tunneling option: use AES-128bit-CBC SSL to encrypt the traffic in the WAN optimization tunnel.
- Tunnel sharing option: multiple WAN optimization sessions share the same tunnel.
- Web caching: object caching that accelerates web applications and web servers by reducing bandwidth usage, server load, and perceived latency. Supports caching of HTTP 1.0 and HTTP 1.1 web sites.
- SSL Offloading with Web caching:
  - Full mode: performs both decryption and encryption of the HTTPS traffic.
  - Half mode: only performs one encryption or decryption action.
- Option to exempt certain web sites from web caching with URL patterns.
- Support advanced web caching configurations and options:
  - Always revalidate, Max cache object size, negative response duration, fresh factor, Max/Min/Default-TTL, proxy-FQDN, Max HTTP request/message length, ignore options, cache expired objects, revalidate pragma-no-cache
- Explicit web & FTP proxy: FTP, HTTP, and HTTPS proxying on one or more interfaces
- Proxy auto-config (PAC): provide automatic proxy configurations for explicit web proxy users.
- Proxy chaining: web proxy forwarding to redirect web proxy sessions to other proxy servers.
- Web proxy forwarding server monitoring and health checking
- IP reflect capability
- Load balancing for forward proxy and proxy chaining
- Explicit web proxy authentication: IP-Based authentication and per session authentication
- WAN optimization and web cache monitor

## User-&-Device Identity Control

- Local user database & remote user authentication service support: LDAP, Radius and TACACS+, 2-factor authentication
- Single-sign-on: Windows AD, Novell eDirectory, FortiClient, Citrix and Terminal Server Agent, Radius (accounting message), POP3/POP3S, user access (802.1x, captive portal) authentication
- PKI and certificates: X.509 certificates, SCEP support, Certificate Signing Request (CSR) creation, auto-renewal of certificates before expiry, OCSP support
- Device identification: device and OS fingerprinting, automatic classification, inventory management
- User and device-based policies

## Integrated Token Server

- Integrated token-server that provisions and manages Physical, SMS and Soft One Time Password (OTP) tokens

## Firewall

- Operating modes: NAT/route and transparent (bridge)
- Schedules: one-time, recurring
- Session helpers & ALGs: dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS (Oracle)
- VoIP traffic support: SIP/H.323 /SCCP NAT traversal, RTP pin holing
- Protocol type support: SCTP, TCP, UDP, ICMP, IP
- Section or global policy management view
- Policy objects: predefined, customs, object grouping, tagging and coloring
- Address objects: subnet, IP, IP range, GeoIP (Geography), FQDN
- NAT configuration: per policy based and central NAT Table
- NAT support: NAT64, NAT46, static NAT, dynamic NAT, PAT, Full Cone NAT, STUN

## VPN

IPSEC VPN:
- Remote peer support: IPSEC-compliant dialup clients, peers with static IP/dynamic DNS
- Authentication method: certificate, pre-shared key
- IPSEC Phase 1 mode: aggressive and main (ID protection) mode
- Peer acceptance options: any ID, specific ID, ID in dialup user group
- supports IKEv1, IKEv2 (RFC 4306)
- IKE mode configuration support (as server or client), DHCP over IPSEC
- Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128, AES192, AES256
- Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512
- Phase 1/Phase 2 Diffie-Hellman Group support: 1, 2, 5, 14
- XAuth support as client or server mode
- XAuth for dialup users: Server type option (PAP, CHAP, Auto), NAT Traversal option
- Configurable IKE encryption key expiry, NAT traversal keepalive frequency
- Dead peer detection
- Replay detection
- Autokey keep-alive for Phase 2 SA

- IPSEC Configuration Wizard for termination with popular 3rd party devices
- IPSEC VPN deployment modes: gateway-to-gateway, hub-and-spoke, full mesh, redundant-tunnel, VPN termination in transparent mode,
- IPSEC VPN Configuration options: route-based or policy-based
- Customizable SSL VPN portal: color themes, layout, bookmarks, connection tools, client download
- SSL VPN realm support: allows multiple custom SSL VPN logins associated with user groups (URL paths, design)
- Single-sign-on bookmarks: reuse previous login or predefined credentials to access resources
- Personal bookmarks management: allow administrators to view and maintain remote client bookmarks
- SSL portal concurrent users limiting
- One time login per user options: prevents concurrent logins using same username
- SSL VPN web mode: for thin remote clients equipped with a web browser only and support web application such as:
  - HTTP/HTTPS Proxy, FTP, Telnet, SMB/CIFS, SSH, VNC, RDP, Citrix
- SSL VPN tunnel mode: for remote computers that run a variety of client and server applications, SSL VPN client supports MAC OSX, Linux, Windows Vista and with 64-bit Windows operating systems
- SSL VPN port forwarding mode: uses a Java Applet that listens on local ports on the user's computer. When it receives data from a client application, the port forward module encrypts and sends the data to the SSL VPN device, which then forwards the traffic to the application server.
- Host integrity checking and OS check (for windows terminals only) prior to SSL tunnel mode connections
- MAC host check per portal
- Cache cleaning option just before the SSL VPN session ends
- Virtual desktop option to isolates the SSL VPN session from the client computer's desktop environment
- VPN monitoring: view and manage current IPSEC and SSL VPN connections in details
- Other VPN support: L2TP client (on selected models) and server mode, L2TP over IPSEC, PPTP, GRE over IPSEC

000013

# FEATURE SUMMARY

16635

### SSL Inspection

Inspect SSL Encrypted traffic option for IPS, application control, antivirus, web filtering and DLP

### IPS

IPS engine: 7,000+ up-to-date signatures, protocol anomaly detection, rate-based detection, custom signatures, manual, automatic pull or push signature update, threat encyclopedia integration

IPS Actions: default, monitor, block, reset, or quarantine (attackers IP, attackers IP and Victim IP, incoming interface) with expiry time

Filter Based Selection: severity, target, OS, application and/or protocol

Packet logging option

IP(s) exemption from specified IPS signatures

IPv4 and IPv6 Rate based DOS protection (Available on most Models) with threshold settings against TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/SCTP/ICMP session flooding (source/destination)

IDS sniffer mode

Active bypass with bypass interfaces (selected models) and FortiBridge

### Application Control

Detects over 3,000 applications in 18 Categories:
Botnet, Collaboration, Email, File Sharing, Game, General Interest, Network Service, P2P, Proxy, Remote Access, Social Media, Storage Backup, Update, Video/Audio, VoIP, Industrial, Special, Web (Others)

Custom application signature support

Supports detection for traffic using SPDY protocol

Deep Application visibility: login names, files/video activities and information

Filter based selection: by category, popularity, technology, risk, vendor and/or protocol

Actions: block, reset session, monitor only, application control traffic shaping

SSH Inspection

### Anti-Malware / Advanced Threat Protection

Botnet server IP blocking with global IP reputation database

Antivirus database type selection (on selected models)

Flow-based Antivirus: protocols supported - HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, SMB, ICQ, YM, NNTP

Proxy-based Antivirus:
- Protocol Support: HTTP/HTTPS, STMP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, ICQ, YM, NNTP
- External cloud-based file analysis (OS sandbox) support
- File submission blacklisting and whitelisting
- File quarantine (local storage required)
- Heuristic scanning option

### Web Filtering

Web filtering inspection mode support: proxy-based, flow-based and DNS

Manually defined web filtering based on URL, web content & MIME header

Dynamic web filtering with cloud-based realtime categorization database: over 250 Million URLs rated into 78 categories, in 70 languages

Safe Search enforcement: transparently inserts Safe Search parameter to queries. Supports Google, Yahoo!, Bing & Yandex, definable YouTube Education Filter

Additional features offered by proxy-based web filtering:
- Filter Java Applet, ActiveX and/or cookie
- Block HTTP Post
- Log search keywords
- Rate images by URL
- Block HTTP redirects by rating
- Exempt scanning encrypted connections on certain categories for privacy
- Web Browsing quota by categories

Web filtering local categories & category rating override

Web filtering profile override: allows administrator to temporarily assign different profiles to user/user group/IP

Restrict access to Google Corporate Accounts only

Proxy avoidance prevention: proxy site category blocking, rate URLs by domain & IP address, block redirects from cache & translation sites, proxy avoidance application blocking (application control), proxy behavior blocking (IPS)

### Data Leak Prevention (DLP)

Web filtering inspection mode support: proxy-based, flow-based and DNS

DLP message filter:
- Protocol supported: HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP
- Actions: log only, block, quarantine user/IP/interface
- Predefined filter: credit card number, Social Security ID

DLP File Filter:
- Protocol Supported: HTTP-POST, HTTP=-GET,SMTP, POP3, IMAP, MAPI, FTP, NNTP
- Filter options: size, file type, watermark, content, if encrypted

DLP watermarking: allows filter files that pass through the FortiGate unit and contain a corporate identifier (a text string) and a sensitivity level (Critical, Private, and Warning) hidden in a watermark. Support Windows and Linux free watermarking tools.

DLP fingerprinting: generates a checksum fingerprint from intercepted files and compare it to those in the fingerprint database.

DLP archiving: records full content in email, FTP, IM, NNTP, and web traffic

### Endpoint Control

Manages network devices via client software:
- Posture checking: enforce client software installation and desired settings
- Client configuration provisioning: push and update client configurations such as VPN and web filtering settings accordingly to device type/group and/or user/usergroup
- "Off-net" security enforcement: detects when not protected by security gateway, activates provisioning security settings
- allows client activities logging implementation

Client software support: Windows, OS X, IOS, Android

### Vulnerability Scanning

Network Vulnerability Scan: protect network assets (servers and workstations) by scanning them for security weaknesses.
- On-demand or scheduled
- Scan Modes: Quick, standard or Full
- authenticated scanning

Vulnerability Result: detailed scan results are logged with direct reference on threat encyclopedia

### Wireless and Switch Controller

Manages and provisions settings for local and remote Thin Access points or switches (selected models)

Set up access and authentication methods for SSIDs and VLANs, supports integrated or external captive portal, 802.1x, preshared keys

WiFi Security: Rogue AP suppression, wireless IDS

Wireless topology support: Fast roaming, AP load balancing, Wireless Mesh and bridging

### High Availability

High availability modes: active-passive, active-active, virtual clusters, VRRP, FG-5000 series clustering

Redundant heartbeat interfaces

HA reserved management interface

Failover:
- Port, local & remote link monitoring
- stateful failover
- subsecond failover
- Failure detection notification

Deployment Options:
- HA with link aggregation
- Full mesh HA
- Geographically dispersed HA

Standalone session synchronization

### Administration, Monitoring & Diagnostics

Management Access: HTTPS via web browser, SSH, telnet, console

Web UI administration language support: English, Spanish, French, Portuguese, Japanese, Simplified Chinese, Traditional Chinese, Korean

Central management support: FortiManager, FortiCloud hosted service, web service APIs

Systems integration: SNMP, sFlow, NetFlow, syslog, alliance partnerships

Rapid deployment: install wizards, USB auto-install, local and remote script execution

Dynamic, real-time dashboard status & drill-in monitoring widgets

000018

# FEATURE SUMMARY

16636

| Log & Reporting |
|---|
| Logging facilities support: local memory & storage (if available), multiple syslog servers, multiple FortiAnalyzers, WebTrends servers, FortiCloud hosted service |
| Reliable logging using TCP option (RFC 3195) |
| Encrypted logging & log integrity with FortiAnalyzer |
| Scheduled batch log uploading |
| Detailed traffic logs: Forwarded, violated sessions, local traffic, invalid packets |
| Comprehensive event logs: systems & administrators activity audits, routing & networking, VPN, user authentications, WiFi related events |
| Brief traffic log format option |
| IP and service port name resolution option |

NOTE: Feature set based on FortiOS V5.2.1+, some features or certification may not apply to all models. ^ Local storage required.

# ADDITIONAL REFERENCES

| Resource | URL |
|---|---|
| The FortiOS Handbook - The Complete Guide | http://docs.fortinet.com/fgt.html |
| Fortinet Knowledge Base | http://kb.fortinet.com/ |
| Product Datasheets & Matrix | http://www.fortinet.com/resource_center/datasheets.html |
| UTM Solution Page | http://www.fortinet.com/solutions/unified_threat_management.html |


GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE
300 Beach Road #20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

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

I.D.

MÉXICO, D.F. A 8 DE OCTUBRE DE 2015

TELECOMUNICACIONES DE MÉXICO
DIREECCIÓN DE ADMINISTRACIÓN Y FINANZAS
SUBDIRECCIÓN DE RECURSOS MATERIALES Y SERVICIOS GENERALES
GERENCIA DE ADQUISICIONES

PRESENTE

CONVOCATORIA A LA LICITACIÓN PÚBLICA MIXTA NACIONAL No. LA-009KCZ002-N49-2015, PARA EL ARRENDAMIENTO DEL "EQUIPO FIREWALL/VPN Y CONSOLA DE ADMINISTRACIÓN PARA EXPANSIÓN DE OFICINAS TELEGRÁFICAS DE LA RED TELDAT".

JENNIFER MURILLO DOMÍNGUEZ EN MI CARÁCTER DE REPRESENTANTE LEGAL DE LA EMPRESA GRUPO DE TECNOLOGÍA CIBERNÉTICA S.A. DE C.V., MANIFIESTO QUE PARA DAR CUMPLIMIENTO AL PUNTO DE REFERENCIA LAS LAS CONSOLAS DE ADMINISTRACIÓN PROPUESTAS SE PRESENTAN EN EQUIPO APPLIANCE CON DASHBOARD EN IDIOMA ESPAÑOL.

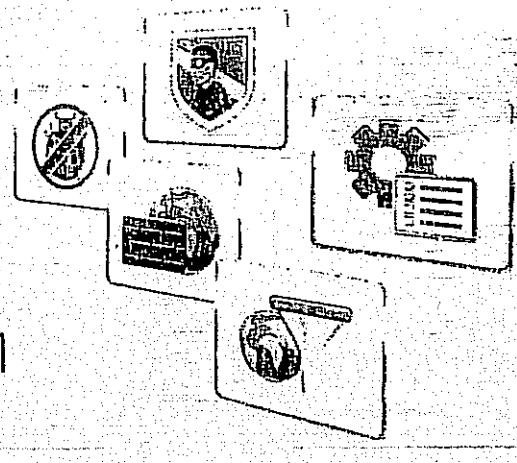
MÉXICO, D.F. A 8 DE OCTUBRE DE 2015
GRUPO DE TECNOLOGÍA CIBERNÉTICA S.A. DE C.V.

JENNIFER MURILLO DOMÍNGUEZ
REPRESENTANTE LEGAL

00002

FORTINET.

16638



# FortiOS® 5.2 Network Security Operating System

## For Unified Threat Management

FortiOS is a security-hardened, purpose-built Operating System that is the foundation of all FortiGate® network security platforms from our entry-level devices to our most powerful carrier-grade models. FortiOS 5.2 includes over 150 standard features, and many new enhancements that help fight advanced threats, simplify FortiGate installations and expand threat reporting and management.

### Robust Complete Network Security

No matter how large or small your organization is, you face numerous challenges as your network environment, usage patterns and security threats evolve. FortiOS gives you the latest in all-in-one network security protection that's easy to deploy and manage. Besides the industry's best firewall, intrusion protection and VPN you get Advanced Threat Protection that fights against advanced persistent threats (ATPs) and additional features like email filtering, data-loss prevention and vulnerability scanning - a complete Unified Threat Management (UTM) solution for your business.

### Flexible Architecture that Adapts with Your Needs

Whether you need a simple firewall or a complete UTM installation, FortiOS gives you the flexibility to easily configure the options you need for your environment. From a "single pane of glass" you can set up, manage, and get detailed reporting on your network and security threats, all within minutes.

*Rich feature set for protecting your applications, data and users.*

- Enterprise grade security for any sized organization
- Easy to deploy and manage
- Outstanding manageability with consolidated security and access control setup
- Strong and flexible user and device management with multiple authentication options.

### Key Features & Benefits

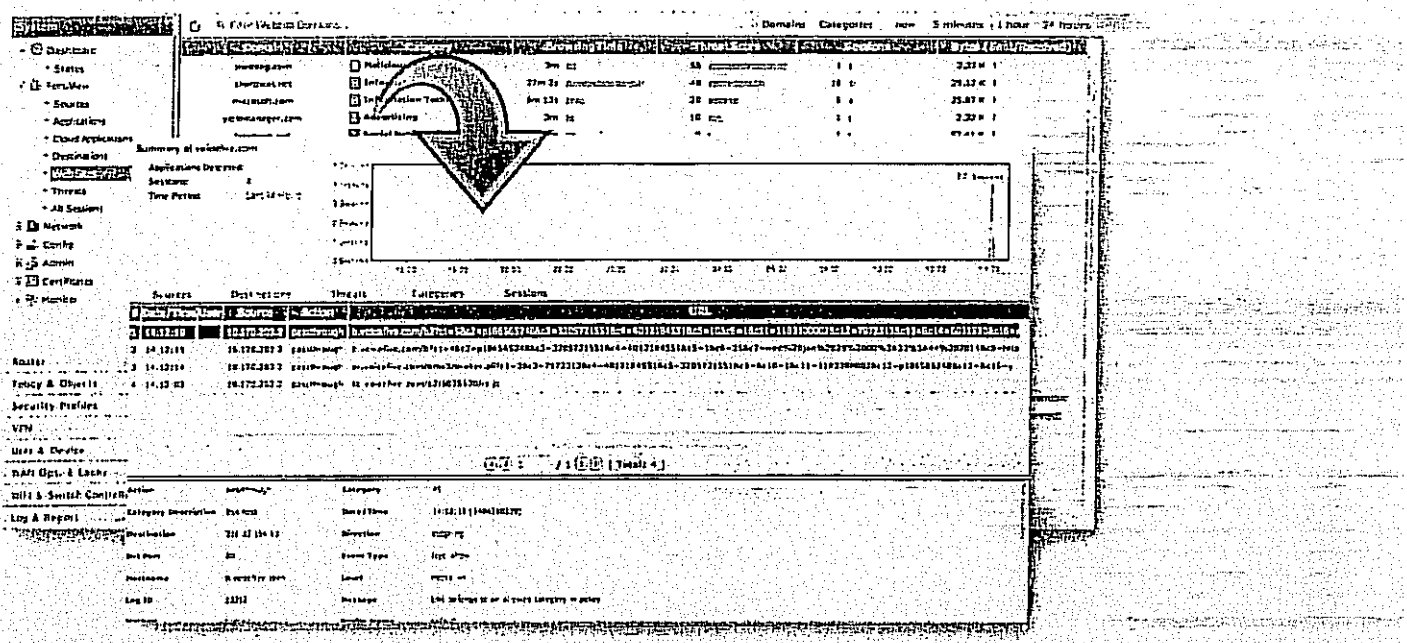
| | |
|---|---|
| Unified Threat Management | Comprehensive network security protection with advanced threat protection, email filtering, data-loss prevention and vulnerability scanning. |
| Intuitive and Customizable | Easy to configure and manage with the flexibility to choose the security and UTM options you need. |
| Advanced Network Segmentation | Support for multiple zones and VDOMs to meet your data protection and compliance requirements. |

ICSA labs ICSA labs ICSA labs

ICSA labs ICSA labs

00002

16639



*FortiOS web-based GUI — FortiView on-demand query tool*

## Complete Security

Fortinet designed and built FortiOS 5.2 to deliver the advanced protection and performance that standalone products simply can't match. The services work together as a system to provide better visibility and mitigation of the latest network and application threats, stopping attacks before damage can occur.

## Unique Visibility and Control

Advanced security features such as flow-based inspection and integrated wireless controller capability allow you to monitor and protect your wired and wireless networks from endpoints to the core, and from remote offices to headquarters. FortiOS allows greater traffic visibility and more consistent, granular control over users, applications and sensitive data.

## Easier to Manage

FortiOS 5.2 lowers costs and reduces IT staff workloads. Physical or virtual FortiGate appliances give you the flexibility to match your security to your environment while enforcing a uniform security policy. Single pane of glass management and centralized analysis ensure consistent policy creation and enforcement while minimizing deployment and configuration challenges.

## Securing Mobile Devices

FortiOS 5.2 helps secure mobile device and BYOD environments (including iOS®, Android® and Windows® clients) by identifying devices and applying specific access policies as well as security profiles, according to the device type or device group, location, and usage.

## Client Reputation

Signature-based security alone is not enough anymore; it is now critical to understand how devices on your network are behaving. FortiView with threat score provides a cumulative security ranking of each client device on your network based on a range of behaviors. It provides specific, actionable information that helps identify compromised systems and potential zero-day attacks in real time.

## Smart Policies

FortiOS 5.2 enables intelligent, automatic adjustment of role-based policies for users and guests based on location, data, and application profile. Enhanced reporting and analysis provides deeper insights into the behavior of your network, users, devices, applications and threats.

16640

## Extensive Network Support

FortiOS supports numerous network design requirements and interoperates with other networking devices. This includes support for a wealth of routing, multicasting and network resiliency protocols. Administrators can also configure interfaces for VLANs, VLAN trunks, port aggregation and one-armed sniffer mode.

It also offers robust high-availability and clustering options, including advanced sub-second failover, virtual clusters and much more.

## Unified Access Security

FortiOS empowers organizations to apply consistent policies across various types of networks, simplifying policy enforcement in today's complex environments. Its wireless controller features extend the same protection to wireless networks while endpoint control capabilities provision and enforce security for mobile users even when they are away from the office.

## Device ID and User ID Access Control

FortiOS supports both local and remote authentication services such as LDAP, Radius and TACACS+ to identify users and apply access policies and security profiles accordingly. It simplifies identity-based implementations and also provides a seamless user authorization experience with various single sign-on capabilities. FortiOS can capture terminal service user or wireless login credentials, among others, and intelligently apply policies and profiles without additional user input.

As device types continue to evolve, you'll be ready with device access control. You can apply security policies based on the type of device such as computers, tablets or phones and apply different policies depending if the devices are company or privately owned.

## Sophisticated Application Control

Identifying applications and providing relevant enforcement is essential in the current Web 2.0 and cloud environments. FortiOS offers gradual controls and can identify over 3,000 applications, even those on encrypted channels. It also offers mitigation against sophisticated botnet activities that easily evade traditional firewalls.

## Physical and Virtual Segmentation

From simple small wired networks to the complex multi-tenant managed datacenter environments, FortiOS supports everything you need to set up and manage your network traffic. You can configure physical network segmentation using the LAN ports built-in to every FortiGate, or you can provide virtual segmentation using virtual LANs (VLANs).

## Powerful & Scalable Management

FortiManager makes it easy to provision and manage thousands of FortiGate devices in a distributed organization. Using standardized setup profiles, you get the ability to configure a standard set of policy and provisioning workflows to meet your business needs or compliance standards. Detailed configuration audit trails are supported and can reside externally on secured storage with FortiAnalyzer.

FortiOS also integrates well with third-party solutions such as Network Management Systems and SIEMs through Fortinet's technology alliances.

## *FortiGate® - High performance Network Security Platform*

- **ASIC-Powered Performance**
  FortiGate purpose-built hardware delivers unmatched price/performance for the most demanding networking environments. FortiASIC processors ensure that your network security solution does not become a network bottleneck.
- **High speed and Flexible Connectivity**
  The FortiGate product family offer a variety of interfaces for today's network, ranging from integrated WAN interfaces, 3G/4G USB wireless broadband support to high speed 40G interfaces for data centers.
- **Broad Product Offerings**
  The FortiGate product family scales from desktop units for remote branch offices, mid-range for small and medium enterprises to high-end platforms for service providers and data centers

00002

# FEATURE SUMMARY

## Network Services and Support

- Built-in DHCP, NTP, DNS Server and DNS proxy (available on most models)
- FortiGuard NTP, DDNS and DNS service
- Interface modes: sniffer, port aggregated, loopback, VLANs (802.1Q and Trunking), virtual hardware, software and VLAN switches (available on most models)
- Static and policy routing
- Hybrid WAN support: load balancing and redundancy with link health check on monitoring using TWAMP
- Support USB 3G/4G Wireless WAN modems
- Dynamic routing protocols:
  - RIPv1 and v2, OSPF v2 and v3, ISIS, BGP4
- Multicast traffic: sparse and dense mode, PIM support
- Content routing: WCCP and ICAP
- Traffic shaping and QoS per policy or applications: shared policy shaping, per-IP shaping, maximum & guaranteed bandwidth, maximum concurrent connections per IP, traffic prioritization, Type of Service (TOS) and Differentiated Services (DiffServ) support
- IPv6 Support: Management over IPv6, IPv6 routing protocols, IPv6 tunnelling, firewall and UTM for IPv6 traffic, NAT46, NAT64, IPv6 IPSEC VPN

## WAN Optimization, Web Cache and Explicit Proxy^

- ...e and out-of-path WAN optimization topology, peer to peer and remote client support
- ...nsparent Mode option: keeps the original source address of the packets, so servers appear to receive traffic directly from clients.
- WAN optimization techniques: protocol optimization and byte caching
- WAN Optimization protocols supported: CIFS, FTP, HTTP(S), MAPI, TCP
- Secure Tunneling option: use AES-128bit-CBC SSL to encrypt the traffic in the WAN optimization tunnel.
- Tunnel sharing option: multiple WAN optimization sessions share the same tunnel.
- Web caching: object caching that accelerates web applications and web servers by reducing bandwidth usage, server load, and perceived latency. Supports caching of HTTP 1.0 and HTTP 1.1 web sites.
- SSL Offloading with Web caching:
  - Full mode: performs both decryption and encryption of the HTTPS traffic.
  - Half mode: only performs one encryption or decryption action.
- Option to exempt certain web sites from web caching with URL patterns.
- Support advanced web caching configurations and options:
  - Always revalidate, Max cache object size, negative response duration, fresh factor, Max/Min/Default TTL, proxy FQDN, Max HTTP request/message length, ignore options, cache expired objects, revalidated pragma-no-cache
- Explicit web & FTP proxy: FTP, HTTP, and HTTPS proxying on one or more interfaces
- Proxy auto-config (PAC): provide automatic proxy configurations for explicit web proxy users.
- Proxy chaining: web proxy forwarding to redirect web proxy sessions to other proxy servers.
- ...proxy forwarding server monitoring and health checking
- IP reflect capability
- Load balancing for forward proxy and proxy chaining
- Explicit web proxy authentication: IP-Based authentication and per session authentication
- WAN optimization and web cache monitor

## User & Device Identity Control

- Local user database & remote user authentication service support: LDAP, Radius and TACACS+, 2-factor authentication
- Single-sign-on: Windows AD, Novell eDirectory, FortiClient, Citrix and Terminal Server Agent, Radius (accounting message), POP3/POP3S, user access (802.1x, captive portal) authentication
- PKI and certificates: X.509 certificates, SCEP support, Certificate Signing Request (CSR) creation, auto-renewal of certificates before expiry, OCSP support
- Device identification: device and OS fingerprinting, automatic classification, inventory management
- User and device-based policies

## Integrated Token Server

- Integrated token server that provisions and manages physical, SMS and Soft One Time Password (OTP) Tokens

## Firewall

- Operating modes: NAT/route and transparent (bridge)
- Schedules: one-time, recurring
- Session helpers & ALGs: dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS (Oracle)
- VoIP traffic support: SIP/H.323 /SCCP NAT traversal, RTP pin holing
- Protocol type support: SCTP, TCP, UDP, ICMP, IP
- Section or global policy management view
- Policy objects: predefined, customs, object grouping, tagging and coloring
- Address objects: subnet, IP, IP range, GeoIP (Geography), FQDN
- NAT configuration: per policy based and central NAT Table
- NAT support: NAT64, NAT46, static NAT, dynamic NAT, PAT, Full Cone NAT, STUN

## VPN

IPSEC VPN:
- Remote peer support: IPSEC-compliant dialup clients, peers with static IP/dynamic DNS
- Authentication method: certificate, pre-shared key
- IPSEC Phase_1 mode: aggressive and main (ID protection) mode
- Peer acceptance options: any ID, specific ID, ID in dialup user group
- supports IKEv1, IKEv2 (RFC 4306)
- IKE mode configuration support (as server or client), DHCP over IPSEC
- Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128, AES192, AES256
- Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512
- Phase 1/Phase 2 Diffie-Hellman Group support: 1, 2, 5, 14
- XAuth support as client or server mode
- XAuth for dialup users: Server type option (PAP, CHAP, Auto), NAT Traversal option
- Configurable IKE encryption key expiry, NAT traversal keepalive frequency
- Dead peer detection
- Replay detection
- Autokey keep-alive for Phase 2 SA

- IPSEC Configuration Wizard for termination with popular 3rd party devices
- IPSEC VPN deployment modes: gateway-to-gateway, hub-and-spoke, full mesh, redundant-tunnel, VPN termination in transparent mode,
- IPSEC VPN Configuration options: route-based or policy-based
- Customizable SSL VPN portal: color themes, layout, bookmarks, connection tools, client download
- SSL VPN realm support: allows multiple custom SSL VPN logins associated with user groups (URL paths, design)
- Single-sign-on bookmarks: reuse previous login or predefined credentials to access resources
- Personal bookmarks management: allow administrators to view and maintain remote client bookmarks
- SSL portal concurrent users limiting
- One time login per user options: prevents concurrent logins using same username
- SSL VPN web mode: for thin remote clients equipped with a web browser only and support web application such as:
  - HTTP/HTTPS Proxy, FTP, Telnet, SMB/CIFS, SSH, VNC, RDP, Citrix
- SSL VPN tunnel mode: for remote computers that run a variety of client and server applications, SSL VPN client supports MAC OSX, Linux, Windows Vista and with 64-bit Windows operating systems
- SSL VPN port forwarding mode: uses a Java Applet that listens on local ports on the user's computer. When it receives data from a client application, the port forward module encrypts and sends the data to the SSL VPN device, which then forwards the traffic to the application server.
- Host integrity checking and OS check (for windows terminals only) prior to SSL tunnel mode connections
- MAC host check per portal
- Cache cleaning option just before the SSL VPN session ends
- Virtual desktop option to isolates the SSL-VPN session from the client computer's desktop environment
- VPN monitoring: view and manage current IPSEC and SSL VPN connections in details
- Other VPN support: L2TP client (on selected models) and server mode, L2TP over IPSEC, PPTP, GRE over IPEC

000025

# FEATURE SUMMARY

## SSL Inspection

Inspect SSL Encrypted traffic option for IPS, application control, antivirus, web filtering and DLP

## IPS

IPS engine: 7,000+ up-to-date signatures, protocol anomaly detection, rate-based detection, custom signatures, manual, automatic pull or push signature update, threat encyclopedia integration

IPS Actions: default, monitor, block, reset, or quarantine (attackers IP, attackers IP and Victim IP, incoming interface) with expiry time

Filter Based Selection: severity, target, OS, application and/or protocol

Packet logging option

IP(s) exemption from specified IPS signatures

IPv4 and IPv6 Rate based DOS protection (Available on most Models) with threshold settings against TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/SCTP/ICMP session flooding (source/destination)

IDS sniffer mode

Active bypass with bypass interfaces (selected models) and FortiBridge

## Application Control

cts over 3,000 applications in 18 Categories:
t, Collaboration, Email, File Sharing, Game, General Interest, Network Service, P2P, Proxy, Remote Access, Social Media, Storage Backup, Update, Video/Audio, VoIP, Industrial, Special, Web (Others)

Custom application signature support

Supports detection for traffic using SPDY protocol

Deep Application visibility: login names, files/video activities and information

Filter based selection: by category, popularity, technology, risk, vendor and/or protocol

Actions: block, reset session, monitor only, application control traffic shaping

SSH Inspection

## Anti-Malware / Advanced Threat Protection

Botnet server IP blocking with global IP reputation database

Antivirus database type selection (on selected models)

Flow-based Antivirus: protocols supported - HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, SMB, ICQ, YM, NNTP

Proxy-based Antivirus:
- Protocol Support: HTTP/HTTPS, STMP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, ICQ, YM, NNTP
- External cloud-based file analysis (OS sandbox) support
- File submission blacklisting and whitelisting
- File quarantine (local storage required)
- Heuristic scanning option

## Web Filtering

iltering inspection mode support: proxy-based, flow-based and DNS

Manually defined web filtering based on URL, web content & MIME header

Dynamic web filtering with cloud-based realtime categorization database: over 250 Million URLs rated into 78 categories, in 70 languages

Safe Search enforcement: transparently inserts Safe Search parameter to queries. Supports Google, Yahoo!, Bing & Yandex, definable YouTube Education Filter

Additional features offered by proxy-based web filtering:
- Filter Java Applet, ActiveX and/or cookie
- Block HTTP Post
- Log search keywords
- Rate images by URL
- Block HTTP redirects by rating
- Exempt scanning encrypted connections on certain categories for privacy
- Web Browsing quota by categories

Web filtering local categories & category rating override

Web filtering profile override: allows administrator to temporarily assign different profiles to user/user group/IP

Restrict access to Google Corporate Accounts only

Proxy avoidance prevention: proxy site category blocking, rate URLs by domain & IP address, block redirects from cache & translation sites, proxy avoidance application blocking (application control), proxy behavior blocking (IPS)

## Data Leak Prevention (DLP)

Web filtering inspection mode support: proxy-based, flow-based and DNS

DLP message filter:
- Protocol supported: HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP
- Actions: log only, block, quarantine user/IP/interface
- Predefined filter: credit card number, Social Security ID

DLP File Filter:
- Protocol Supported: HTTP-POST, HTTP=-GET,SMTP, POP3, IMAP, MAPI, FTP, NNTP
- Filter options: size, file type, watermark, content, if encrypted

DLP watermarking: allows filter files that pass through the FortiGate unit and contain a corporate identifier (a text string) and a sensitivity level (Critical, Private, and Warning) hidden in a watermark. Support Windows and Linux free watermarking tools.

DLP fingerprinting: generates a checksum fingerprint from intercepted files and compare it to those in the fingerprint database.

DLP archiving: records full content in email, FTP, IM, NNTP, and web traffic

## Endpoint Control

Manages network devices via client software:
- Posture checking: enforce client software installation and desired settings
- Client configuration provisioning: push and update client configurations such as VPN and web filtering settings accordingly to device type/group and/or user/usergroup
- "Off-net" security enforcement: detects when not protected by security gateway, activates provisioning security settings
- allows client activities logging implementation

Client software support: Windows, OS X, IOS, Android

## Vulnerability Scanning

Network Vulnerability Scan: protect network assets (servers and workstations) by scanning them for security weaknesses.
- On-demand or scheduled
- Scan Modes: Quick, standard or Full
- authenticated scanning

Vulnerability Result: detailed scan results are logged with direct reference on threat encyclopedia

## Wireless and Switch Controller

Manages and provisions settings for local and remote Thin Access points or switches (selected models)

Set up access and authentication methods for SSIDs and VLANs, supports integrated or external captive portal, 802.1x, preshared keys

WiFi Security: Rogue AP suppression, wireless IDS

Wireless topology support: Fast roaming, AP load balancing, Wireless Mesh and bridging

## High Availability

High availability modes: active-passive, active-active, virtual clusters, VRRP, FG-5000 series clustering

Redundant heartbeat interfaces

HA reserved management interface

Failover:
- Port, local & remote link monitoring
- stateful failover
- subsecond failover
- Failure detection notification

Deployment Options:
- HA with link aggregation
- Full mesh HA
- Geographically dispersed HA

Standalone session synchronization

## Administration, Monitoring & Diagnostics

Management Access: HTTPS via web browser, SSH, telnet, console

Web UI administration language support: English, Spanish, French, Portuguese, Japanese, Simplified Chinese, Traditional Chinese, Korean

Central management support: FortiManager, FortiCloud hosted service, web service APIs

Systems Integration: SNMP, sFlow, Netflow, syslog, alliance partnerships

Rapid deployment: install wizards, USB auto-install, local and remote script execution

Dynamic, real-time dashboard status & drill-in monitoring widgets

# FEATURE SUMMARY

16643

| Log & Reporting |
|---|
| Logging facilities support: local memory & storage (if available), multiple syslog servers, multiple FortiAnalyzers, WebTrends servers, FortiCloud hosted service |
| Reliable logging using TCP option (RFC 3195) |
| Encrypted logging & log integrity with FortiAnalyzer |
| Scheduled batch log uploading |
| Detailed traffic logs: Forwarded, violated sessions, local traffic, invalid packets |
| Comprehensive event logs: systems & administrators activity audits, routing & networking, VPN, user authentications, WiFi related events |
| Brief traffic log format option |
| IP and service port name resolution option |

NOTE: Feature set based on FortiOS V5.2.1+, some features or certification may not apply to all models. ^ Local storage required.

# ADDITIONAL REFERENCES

| Resource | URL |
|---|---|
| The FortiOS Handbook - The Complete Guide | http://docs.fortinet.com/fgt.html |
| Fortinet Knowledge Base | http://kb.fortinet.com/ |
| Product Datasheets & Matrix | http://www.fortinet.com/resource_center/datasheets.html |
| UTM Solution Page | http://www.fortinet.com/solutions/unified_threat_management.html |


GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE
300 Beach Road #20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

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

# ANEXO 2

## LUGAR Y CONDICIONES DE ENTREGA

MÉXICO, D.F. A 8 DE OCTUBRE DE 2015

TELECOMUNICACIONES DE MÉXICO
DIREECCIÓN DE ADMINISTRACIÓN Y FINANZAS
SUBDIRECCIÓN DE RECURSOS MATERIALES Y SERVICIOS GENERALES
GERENCIA DE ADQUISICIONES

PRESENTE

JENNIFER MURILLO DOMÍNGUEZ, EN MI CARÁCTER DE REPRESENTANTE LEGAL DE LA EMPRESA GRUPO DE TECNOLOGÍA CIBERNÉTICA MANIFIESTO LO SIGUIENTE:

LA PRESTACIÓN DEL SERVICIO OBJETO DE ESTA LICITACIÓN SERÁ PROPORCIONADO EN LAS SIGUIENTES UBICACIONES:

SE ENTREGARÁ EN NUESTRA PROPUESTA TÉCNICA EL "PLAN DE TRABAJO DETALLADO", INCLUYENDO LAS ACTIVIDADES A DESEMPEÑAR PARA ALCANZAR LOS PLAZOS ESTABLECIDOS, CONSIDERANDO LOS SIGUIENTES PUNTOS LOS CUALES SON ENUNCIATIVOS MÁS NO LIMITATIVOS:

TELECOMM REQUIERE QUE EL ARRENDAMIENTO SOLICITADO INICIE SU OPERACIÓN DE ACUERDO COMO SE ESPECIFICA EN LA SIGUIENTE TABLA PARA LOS DIFERENTES NODOS, LAS ACTIVIDADES DESCRITAS SON ENUNCIATIVAS MÁS NO LIMITATIVAS, GRUPO TECNO DARÁ CUMPLIMIENTO A LOS SIGUIENTES PUNTOS:

- *IMPLEMENTACIÓN PARA EQUIPOS CENTRALES*
  *ACTIVIDADES*: INSTALACIÓN, CONFIGURACIÓN Y PRUEBAS DE CONECTIVIDAD.

| *EQUIPO* | *SITIO* | *FECHA LIMITE DE IMPLEMENTACIÓN* |
|---|---|---|
| 2 CONSOLAS DE ADMINISTRACIÓN Y SISTEMA DE GESTIÓN. | TCT Y CTO | 30 OCTUBRE 2015 |
| 10 FIREWALL'S CENTRALES. | 7 FIREWALL'S EN CTO | 30 OCTUBRE 2015 |
| | 2 FIREWALL'S EN TCT | 06 NOVIEMBRE 2015 |
| | 1 FIREWALL EN TULANCINGO | 13 NOVIEMBRE 2015 |

- ***PUESTA EN OPERACIÓN PARA EQUIPOS CENTRALES***
  ***ACTIVIDADES*: INICIO DE OPERACIÓN.**

| *EQUIPO* | *SITIO* | *FECHA DE INICIO DE OPERACIÓN* |
|---|---|---|
| 2 CONSOLAS DE ADMINISTRACION Y SISTEMA DE GESTION | TCT Y CTO | 31 OCTUBRE 2015 |
| 10 FIREWALL´S CENTRALES | 7 FIREWALL´S EN CTO | 31 OCTUBRE 2015 |
| | 2 FIREWALL´S EN TCT | 07 NOVIEMBRE 2015 |
| | 1 FIREWALL EN TULANCINGO | 14 NOVIEMBRE 2015 |

- ***IMPLEMENTACIÓN Y PUESTA EN OPERACIÓN PARA EQUIPOS REMOTOS***
  ***ACTIVIDADES*: INSTALACIÓN, CONFIGURACIÓN Y PRUEBAS DE CONECTIVIDAD, INICIO DE OPERACIÓN.**

| *EQUIPO* | *SITIO* | *FECHA LIMITE DE IMPLEMENTACIÓN E INICIO DE OPERACIÓN* |
|---|---|---|
| • 32 FIRWALL´S REMOTOS PARA GERENCIAS ESTATALES<br>Y<br>• 1,200 FIREWALL´S REMOTO PARA OFICINAS TELEGRÁFICAS. | REGION I<br>EDOMEX, GUERRERO, HIDALGO, MORELOS, PUEBLA, QUERETARO, D.F. Y TLAXCALA (APROXIMADAMENTE 266 EQUIPOS) | 13 NOVIEMBRE 2015 |
| | REGION II<br>AGUASCALIENTES, COLIMA, GUANAJUATO, JALISCO, MICHOACAN, NAYARIT Y ZACATECAS (APROXIMADAMENTE 306 EQUIPOS) | |
| | REGION III<br>COAHUILA, DURANGO, NUEVO LEON, SAN LUIS POTOSI Y TAMAULIPAS (APROXIMADAMENTE 196 EQUIPOS) | 30 NOVIEMBRE 2015 |
| | REGION IV<br>BCN, BCS, CHIHUAHUA, SINALOA Y SONORA (APROXIMADAMENTE 192 EQUIPOS) | |
| | REGION V<br>CAMPECHE,CHIAPAS, | 31 DICIEMBRE 2015 |

| | | |
|---|---|---|
| | OAXACA, QUINTANA ROO, TABASCO, VERACRUZ Y YUCATÁN (APROXIMADAMENTE 279 EQUIPOS) | |
| 400 FIREWALL´S REMOTOS PARA OFICINAS TELEGRAFICA | DISTRIBUCIÓN A NIVEL NACIONAL. | DURANTE LA VIGENCIA DEL CONTRATO A SOLICITUD DE TELECOMM. |

MÉXICO, D.F. A 8 DE OCTUBRE DE 2015
GRUPO DE TECNOLOGÍA CIBERNÉTICA S.A. DE C.V.

JENNIFER MURILLO DOMÍNGUEZ
REPRESENTANTE LEGAL

**Por el Área requirente de "TELECOMM":**

**Lic. Roberto Ruiz Dominguez.**
Subdirector de Desarrollo de Informática.
Responsable de la administración y verificación del cumplimiento del presente contrato. Responsable de las especificaciones técnicas de este servicio.

**Por "EL ARRENDADOR":**

**C. Jennifer Murillo Dominguez.**
Apoderada legal.
Responsable de la administración y verificación del cumplimiento del presente contrato.

**Por el Área requirente de "TELECOMM":**

C. Rufino Martínez Becerril.
Director de Operaciones Telegráficas.
(Área requirente.)

ANEXO 7

## PROPUESTA ECONÓMICA

MÉXICO, D.F. A 8 DE OCTUBRE DE 2015

TELECOMUNICACIONES DE MÉXICO
DIREECCIÓN DE ADMINISTRACIÓN Y FINANZAS
SUBDIRECCIÓN DE RECURSOS MATERIALES Y SERVICIOS GENERALES
GERENCIA DE ADQUISICIONES

DESCRIPCIÓN, UNIDAD DE PRESENTACIÓN Y CANTIDAD DE LOS BIENES OBJETO DE ESTA LICITACIÓN

NOMBRE DEL LICITANTE: GRUPO DE TECNOLOGÍA CIBERNÉTICA, S.A. DE C.V.
REGISTRO FEDERAL DE CONTRIBUYENTES: GTC-980421-R4A
HOJA NUM:1.
DIRECCIÓN:
CALLE Y NÚMERO: AV. REVOLUCIÓN NO. 1145
COLONIA: MERCED GÓMEZ
DELEGACIÓN O MUNICIPIO: BENITO JUÁREZ
ENTIDAD FEDERATIVA: DISTRITO FEDERAL
CÓDIGO POSTAL: 03930
TELÉFONO: (55) 52789210
FECHA: MÉXICO, D.F. A 8 DE OCTUBRE DE 2015

| "EQUIPO FIREWALL/VPN Y CONSOLA DE ADMINISTRACIN PARA EXPANSION DE OFICINAS TELEGRÁFIGAS DE LA RED TELDAT". | | | | | PRECIO UNITARIO MENSUAL | PRECIO MENSUAL POR EL TOTAL DE LOS ELEMENTOS |
|---|---|---|---|---|---|---|
| NIVEL | EQUIPO | HARDWARE | CANTIDAD / SITIO | | | |
| "1" CRITICO | FIREWALL'S CENTRALES | APPLIANCE | 7 | 2 FW en HA / TCT | 30,484.03 | 60,968.06 |
| | | | | 1 FW TGO | 30,484.03 | 30,484.03 |
| | | | | 2 FW en HA / CTO | 30,484.03 | 60,968.06 |
| | | | | 2 FW en HA / CTO | 30,484.03 | 60,968.06 |
| | | | 3 | 3 FW CTO | 14,162.80 | 42,488.41 |
| | CONSOLAS DE ADMINISTRACIÓN, | APPLIANCE o SERVIDOR | 2 | TCT | 100,126.41 | 100,126.41 |
| | | | | CTO | 100,126.41 | 100,126.41 |
| | SISTEMA DE GESTION | APPLIANCE o SERVIDOR | 1 | TCT | 154,989.85 | 154,989.85 |
| | FIREWALL'S REMOTOS PARA | APPLIANCE | 32 | ESTADOS | 979.36 | 31,339.62 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | GERENCIAS ESTATALES Y UNIDADES ADMINISTRATIVAS. | | | | | |
| "2" ALTO | FIREWALL'S / REMOTOS PARA OFICINAS TELEGRAFICAS. | APPLIANCE | MINIMO DE 1200 | A NIVEL NACIONAL | 1,001.18 | 1,201,410.79 |
| "3" BAJO | | | MAXIMO DE 1600 | | 1,001.18 | 1,601,881.06 |
| | MONTO MINIMO | SUB TOTAL | | | | 1,843,869.73 |
| | | I.V.A. | | | | 295,019.16 |
| | | TOTAL | | | | 2,138,888.89 |
| | MONTO MAXIMO | SUB TOTAL | | | | 2,244,340.00 |
| | | I.V.A. | | | | 359,094.40 |
| | | TOTAL | | | | 2,603,434.39 |

| "EQUIPO FIREWALL/VPN Y CONSOLA DE ADMINISTRACION PARA EXPANSION DE OFICINAS TELEGRÁFICAS DE LA RED TELDAT." | | | | | |
|---|---|---|---|---|---|
| | EJERCICIOS FISCALES | | | | |
| | 2015 | 2016 | 2017 | 2018 | TOTAL M.N. (36 MESES) |
| MONTO MINIMO | 4,277,777.78 | 25,666,666.66 | 25,666,666.66 | 21,388,888.89 | 76,999,999.99 |
| MONTO MAXIMO | 5,206,868.79 | 31,241,212.74 | 31,241,212.74 | 26,034,343.95 | 93,723,638.21 |

- Los precios del arrendamiento permanecerán fijos e incondicionados durante la vigencia de la propuesta y el contrato.
- Los precios expresados son exclusivamente en moneda nacional, a dos decimales de acuerdo con la Ley monetaria en vigor.
- Se cotiza el 100% del volumen requerido de la partida única a licitar.
- Se cotiza por precio unitario
- Se desglosa IVA

Nota: Esta proposición tendrá una vigencia obligatoria hasta la entrega total del servicio

MÉXICO, D.F. A 8 DE OCTUBRE DE 2015
GRUPO DE TECNOLOGÍA CIBERNÉTICA S.A. DE C.V.

JENNIFER MURILLO DOMÍNGUEZ
REPRESENTANTE LEGAL

FIRMAS A LA VUELTA

16643

**Por el Área requirente de "TELECOMM":**

**Lic. Roberto Ruiz Dominguez.**
Subdirector de Desarrollo de Informática.
Responsable de la administración y verificación del cumplimiento del presente contrato. Responsable de las especificaciones técnicas de este servicio.

**Por "EL ARRENDADOR":**

**C. Jennifer Murillo Dominguez.**
Apoderada legal.
Responsable de la administración y verificación del cumplimiento del presente contrato.

**Por el Área requirente de "TELECOMM":**

**C. Rufino Martínez Becerril.**
Director de Operaciones Telegráficas.
(Área requirente.)