

٥

Holding Company for water and wastewater  
Kalyobia



الشركة القابضة لمياه الشرب والصرف الصحي

Company for water and wastewater

شركة مياه الشرب والصرف الصحي بالقليوبية

مناقصة ( العامة )

رقم ( ٢ ) لسنة

إسم العملية :- توريد وتركيب منظومة الأمن السيبراني

ثمن الكراسة :- ( ٨٠٠٠٠ جنية ) بخلاف الضرائب والدمغات.

(مظروف / مظروفين)

تاريخ جلسة الفتح الفني :- يوم ( الثلاثاء ) الموافق ١٦ / ٧ / 2024

مقدم العطاء

الإسم :-

العنوان :-

التوقيع :-

رقم الإيصال :-

عند الأمانة

ورقة ٢٦

مسند ثلاث نود ورقة لا غير

رئيس اللجنة

التوقيع / احمد عبدالعقل

عضو فني / سمير مظهر

رئيس قطاع التخطيط والتطوير

الدكتور /

عبدالحميد مهدي

مدير عام المخازن

محاسب /

اسلام السيد ابراهيم

يعتمد،،،،

رئيس مجلس الإدارة والعضو المنتدب

مهندس /

مصطفى مجاهد

تليفاكس ٠١٣٣٢١٤٧٩٧

تليفاكس ٠٢٤٩٨١١٠٦٢

المقر المؤقت للشركة : بنها - محطة المياه المرشحة - شارع الرياح التوفيقي

فرع القناطر الخيرية : محطة مياه القناطر الخيرية الرئيسية - كورنيش النيل



## كراسة الشروط والمواصفات

العملية / توريد وتركيب منظومة الأمن السيبراني

مناقصة (عامة) رقم العملية :-

موعد تقديم العطاءات :- آخر موعد لتقديم العطاءات الساعة الثانية عشر ظهراً الموافق ( / / ٢٠٢٤ ) بمقر الشركة بمدينة بنها .

### الشروط العامة :-

❖ مدة سريان العطاء لاتقل عن ثلاثة أشهر من تاريخ فتح المظاريف الفنية ويجوز للشركة أن تطلب من مقدمي العطاءات مد سريان عطاءهم لمدة أخرى تحددها الشركة ويعتبر تخلف مقدم العطاء عن الرد في المهلة المحددة موافقة وقبولاً منه لمد صلاحية العطاء طبقاً لما حددته إدارة الشركة في كتابها المرسل إلي المورد .

❖ وعلي مقدم العطاء مراعاة الأحكام والقواعد الآتية :-

➤ تقدم العطاءات علي نموذج العطاء والمستندات المرفقة به والتي لا يجوز فصلها عن هذه الشروط والأجزاء الملحقة بها ويتم ملء نموذج العطاء والمستندات وتوضع جميع الأوراق مع هذه المستندات ويوقع عليها مقدم العطاء وتوضع جميع الأوراق مع هذه المستندات داخل مظروف واحد أو مظروفين موضحاً الفني و المالي وموقع من أصحابها ومختوم بخاتم صاحب العطاء وعلي صاحب العطاء مراعاة الآتي :-

### أولاً :-

يشترط أن يقدم مع العطاء تأمين إبتدائي قدره (٤٠٠٠٠٠٠) ( فقط أربعمئة الف جنيها فقط لا غير) وذلك نقداً أو بشيك مقبول الدفع أو بخطاب ضمان بنكي غير مشروع ساري لمدة أربعة أشهر صادراً من أحد البنوك المعتمدة وغير مقترن بأي قيد أو شرط ويوضع التأمين الإبتدائي في المظروف الفني.

### ثانياً :-

١- يؤدي صاحب العطاء المقبول قيمة التأمين النهائي بواقع ٥% من إجمالي قيمة إخطار قبول العطاء وذلك خلال عشرة أيام من تاريخ إخطاره بقبول العطاء وعلي أن يسدد هذا التأمين نقداً أو بشيك مقبول الدفع أو بخطاب ضمان بنكي من أحد البنوك المعتمدة غير مقترن بأي قيد أو شرط ويحتفظ به لمدة عام لدي الشركة لحين إتمام إجراءات التسليم النهائي .

س. م. م. م. م. م.



٢- في حالة عدم سداد التأمين النهائي خلال المدة المحددة يتم مصادرة التأمين الابتدائي مع اتخاذ الإجراءات القانونية تجاه المورد .

ثالثاً :- تقدم العطاءات في مظاروفين مغلقين موقع من أصحابه :-

(أ) ويحتوى المظاروف الفني على :-

١- التأمين الابتدائي المطلوب بالإضافة إلي أي بيانات أو مستندات مطلوب توافرها للتحقق من مطابقة العرض

فنياً و المقدرة المالية لمقدم العطاء بما يتناسب مع طبيعة العملية موضوع التعاقد وهي :-

- صورة السجل التجاري مجدداً وسارياً.

- صورة شهادة القيد بالضريبة العامة علي القيمة المضافة .

- صورة البطاقة الضريبية (تكون مدون آليا) وآخر إقرار ضريبي عن السنة السابقة وعلي أن تكون جميع

البيانات مجددة.

- أصل أية مستندات يري المورد تقديمها وسابقة الأعمال مماثلة أو اوامر توريد معتمدة.

- إرفاق الكتلوجات اللازمة في العرض الفني

٢- جميع الاشتراطات الواردة بكراسة الشروط والمواصفات الخاصة بهذه العملية.

٣- التوقيع علي جميع مستندات العطاء بما في ذلك جداول فئات الأسعار بعد ملئها و ختمها مع توضيح تاريخ

تحريرها.

٤- إرسال العطاء على عنوان شركة مياه الشرب والصرف الصحي بالقليوبية في مظاروفين مغلقين ومختومين

وموضح عليهما إسم وعنوان المورد ورقم وإسم المناقصة مع تحديد نوع المظاروف (الفنى /المالى).

٥- كتابة قيمة العطاء بالأرقام والحروف ويكون سعر الوحدة فى كل بند وحسب ما هو مدون بجدول الفئات دون

التغيير فى الوحدة ولا تقبل العطاءات المكتوبة بالقلم الرصاص ويعول فى كل الأحوال على سعر الوحدة المدون

بالحروف.

٦- عدم الكشط أو المحو فى جدول الفئات وكل تصحيح فى الأسعار وغيرها يجب إعادة كتابة بالأرقام والحروف

معاً والتوقيع بجانبه وختمه بخاتم صاحب العطاء وبغير ذلك لا يعتد بهذا الكشط أو المحو أو التصحيح فى

الأسعار.

٧- يذكر فى العطاء اسم الشخص الذي يمثل المورد وصفته إن كان أصلياً أو وكيلأ.

اسم المورد  
س. م. م. م.



- ٨- الفئات التي يحددها مقدم العطاء في جدول الفئات تشمل و تغطي جميع المصروفات والالتزامات التي يتكبتها بكافة أنواعها بما فيها الضرائب أو الرسوم أو خلافه.
- ٩- يجب أن تكون الأسعار المقدمة من المورد شاملة ضريبة القيمة المضافة وفي حالة عدم النص تعتبر الأسعار شاملة الضريبة مع تقديم ما يثبت القيد بضريبة القيمة المضافة.
- ١٠- وإذا رغب المورد في إبداء أية ملاحظات خاصة بالنواحي الفنية فيتعين عليه إثباتها في كتاب مستقل يتضمنه المظروف الفني ولا يلتفت إلي أي عطاء أو إدعاء من صاحب العطاء بحدوث خطأ في عطاءه إذا قدم بعد فتح المظاريف الفنية كما لا يلتفت إلي التعديل الذي يرد علي العطاء بعد الموعد المحدد بفتح المظاريف الفنية .
- ١١- مدة التوريد والتركيب والتجربة: خلال ستة أشهر من تاريخ إستلام أمر الاسناد .
- ١٢- يجب على المورد تقديم جدول زمني لاعمال التوريد والتركيب والتجربة.
- ١٣- تقديم عرض تقديمي عن تكامل المنظومة المقدمة مع المنظومة الحالية على اسطوانه مدمجة مع العرض الفني على ان يتم إخطار المورد بموعد لشرح ماجاء بالعرض التقديمي وسيتم تحرير محضر إثبات حالة بذلك وفي حالة عدم التقديم يعتبر العرض الفني مرفوض.
- ١٤- يلتزم المورد بجميع الشروط الفنية والماليه وشروط التدريب والتركيب والانتجيشن مع النظام الحالي مع إيضاح كل بند من البنود الفنية في العرض الفني المقدم منه وتفسيره تفسيرا واضحا وفي حاله عدم الالتزام باي شرط من الشروط السابقه الخاصه باي بند يعتبر العرض الفني مرفوض.
- ١٥- يجب تقديم سابقه الاعمال المعتمده للشركه مع الجهات الحكوميه المماثله في تنفيذ مشروعات مماثله صادره من تلك الجهات او شركات قطاع اعمال معتمده من تلك الجهات مع تقديم صوره من أوامر اسناد او العقود
- ١٦- تقديم الهيكل الاداري والتنظيمي للشركه.
- ١٧- يلتزم مقدم العطاء بعمل معاينه على الطبيعه لمواقع التركيب بمعرفته وعلي مسؤولتيه وأيضا أجهزة الحاسبات الرئيسية والسويتشات الحالية الموجودة بمقر الشركه، حتى يتسنى للشركه المورده عمل الربط والتكامل التام بين الاجهزة الحالية والأجهزة التي سيتم توريدها وتركيبها وتشغيلها، وحتى يتلافى المورد أيه سهو أو نسيان في تنفيذ المطلوب بما جاء في كراسه الشروط والمواصفات.

(ب) مظروف مالي ويحتوي على :-

١- قوائم الأسعار.

٢- مدة سريان العرض لا تقل عن ثلاثة أشهر من تاريخ فتح المظاريف الفنية .

رئيس العطاء  
سمر صفي



### وعلى مقدم العطاء الإلتزام بما يلي: -

- ❖ لايلتفت إلي أي عطاء أو تعديل يرد بالبرق أو الفاكس أو بأي وسيلة أخرى ما لم يقدم تأييد كتابي بذلك من مقدم العطاء و في حالة وصول العطاء أو التعديل متأخراً وعن الموعد المحدد لفتح المظاريف الفنية وقبل مباشرة لجنة فتح المظاريف لعملها فإنه يؤشر عليه من رئيس اللجنة بساعة و تاريخ وروده و يدرج في العطاءات المتأخرة و يجوز التجاوز علي ذلك التأخير بشرط وروده قبل بدء لجنة فتح المظاريف عملها وفتح المظاريف الفنية وإعداد اللجنة لمحضرها و بموافقة لجنة البت والسلطة المختصة وبشرط أن يكون لصالح الشركة.
- ❖ على أن يتم تسديد التأمين النهائي من موعد أقصاه ( ١٠ أيام) من تاريخ إخطار قبول العطاء.
- ❖ أن يتم تسليم أمر الاسناد بعد سداد التأمين النهائي في مدة لا تزيد عن (١٥ يوم).
- ❖ طريقة السداد : بموجب فاتورة الكترونيه وشهادة ادارية.
- ❖ التنفيذ : بمواقع الشركة المختلفة وفي مواعيد العمل الرسمية للشركة .
- ❖ يقتصر فتح مظاريف العروض المالية علي العروض المقبولة فنياً .
- ❖ يتم التسعير بالدولار الأمريكي وذلك طبقا للمادة رقم ٨/٢٤ من لائحة العقود والمشتريات والتي تنص علي تتولي اللجنة المشكلة لفتح المظاريف تفريغ عطاءات الموردين في قوائم مقارنة ولتوحيد أسس المقارنة يتم تحويل مايرد بعطاء المقاول من أسعار بالعملة الجنبية إلي الجنيه المصري وفقا لمتوسط صرف العملة الأجنبية المعلن عنها من البنك المركزي في اليوم المحدد لفتح المظروف المالي.

### أحكام عامة :-

- ١- يجب علي مقدم العطاء أن يقدم كافة البيانات الخاصة وأن يكون له عنوان معروف ومحل مختار ترسل إليه المكاتبات والإخطارات والاستفسارات وكذلك أرقام الهاتف والفاكس والبريد الإلكتروني.
- ٢- لا يجوز لمقدم العطاء الرجوع فيه او سحبه اثناء سريانه وإلا أصبح التأمين الابتدائي من حق الشركة بدون الحاجة الى إتخاذ أية اجراءات قضائية أو قانونية أو حدوث ضرر لها.
- ٣- لا يجوز للمتعاقد التنازل للغير عن العقد أو التعاقد من الباطن بخصوصه في حالة وفاة المتعاقد أو أحد شركاء المتعاقد الوارد إسمه في السجل التجاري للشركة كشريك جاز للشركة فسخ العقد مع رد التأمين النهائي اذا لم تكن لها أي مطالبات قبل المتعاقد معه أو السماح للورثة بالإستمرار في تنفيذ العقد بشرط أن يعينوا عنهم وكيلًا

سرمهني

إبراهيم السيد



بتوكيل مصدق على التوقيعات فيه أو مطالبة باقي المتعاقدين بالإستمرار في تنفيذه و بموافقة سلطة اعتماد التعاقد .

٤- يحق للشركة تعديل العقد أو أمر التوريد بالزيادة أو النقص في حدود ٢٥% بالنسبة لأي بند بذات الشروط والأسعار دون أن يكون للمورد/المتعاقدين الحق في المطالبة بأى تعويض وذلك خلال فترة سريان العقد

٥- يجوز في حالات الضرورة وبموافقة المورد / المتعاقد تجاوز النسبة الواردة بالفقرة السابقة

٦- و يجوز للسلطة المختصة الموافقة على منح المورد مدد إضافية تضاف إلى مدة تنفيذ العقد طبقاً لدراسة اللجنة المختصة .

٧- و يجوز في حالات الضرورة والإستعجال وبموافقة المورد/المتعاقدين تجاوز النسبة الواردة بالفقرة السابقة بشرط ألا يؤثر ذلك على أولوية المتعاقد في ترتيب العطاءات و وجود الإعتماد المالي اللازم وأن يتم زيادة التعاقد خلال فترة سريان العقد الأصلي .

٨- إذا قدم المتعهد أصنافاً غير مطابقة للعينات أو المواصفات فالشركة الحق في رفض الأصناف كلها أو بعضها دون حاجة الى أية إجراءات قضائية ويخطر المورد فوراً و تحدد له مهلة لإستلامها في حالة رفض الأصناف كلها أو بعضها يخطر المورد فوراً وتحدد له مهلة لإستلامها، ويجوز أن تحصل منه مصاريف تخزين ٢% من قيمة المواد المشونة عن كل أسبوع تأخير أو جزء منه وبحد أقصى ١٠% ويكون للشركة الحق في بيعها على حسابها بعد إخطاره بخطاب موصى عليه، ويُخصم من ثمن البيع ما يكون مستحقاً عليه علاوة ١٠% من قيمتها

#### كمصروفات إدارية

٩- إذا تأخر المورد في توريد كل الكميات المطلوبة او جزء منها يجوز للشركة إعطائه مهلة إضافية لإتمام التوريد او التسليم الابتدائي للأعمال مع توقيع غرامة تأخير عليه وذلك وفقاً للنسب و الأوضاع التالية: -

❖ سيتم توقيع غرامة قدرها ١% عن كل اسبوع تأخير او جزء من إسبوع من إجمالي قيمة الكمية التي يكون المورد قد تأخر في توريدها وبحد أقصى ٨% من قيمة الاصناف المذكورة أو إنهاء التعاقد فيما يخص هذه الاصناف ومصادرة التأمين النهائي بما يوازي ٥% من الاجمالي والحصول على جميع ما تستحق

محمد صديقي

أحمد عبد القادر



الشركة من غرامات دون حاجة الى الالتجاء الى القضاء وإخطار المتعهد بذلك بخطاب موسى عليه ودون الإخلال بحق الشركة في المطالبة بالتعويض و يتم الترسية على العطاء الذي يليه في التقييم مع تحمله فرق التكلفة في الأسعار.

١٠- تظل الأسعار ثابتة طوال مدة التنفيذ.

١١- تسري على هذه المناقصة أحكام لائحة العقود والمشتريات الخاصة بالشركة.

١٢- تلتزم الشركة المورد بتوفير بحد ادنى ثلاث مهندسين طوال مدة التركيب والتسليم مع مراعاة ان يكون اقل خبرة للمهندسين لا تقل عن ٦ سنوات في نفس نوعية المشاريع مع وجود مدير للمشروع خبره لا تقل عن ٥ سنوات في نفس النوع من المشاريع بشكل دائم لمتابعة الاعمال وتسليمها بشكل كامل طوال مدة التنفيذ.

١٣- يجب على الشركة ان تقوم بتوفير مهندس طوال مدة سريان التراخيص بشرط ان يكون بخبره لا تقل عن ٥ سنوات طوال فترة سريان التراخيص وذلك لعدم توقف خدمه ولا يتم نقله الا بموافقه كتابية ويتوجب على الشركة توفير مهندس بديل بنفس الكفاءه وسوف يتم توقيع اتفاقية سرية المعلومات وعدم الافصاح ( NDA ) بالشروط التي سوف يتم الاتفاق عليها.

١٤- تلتزم الشركة الراسي عليها العملية بتجديد التراخيص الخاصة بالمنظومة قبل إنتهائها بشهر على الاقل طبقا للسعر السائد عالميا في حينه على ان تتحمل شركتنا تكاليف تجديد التراخيص طبقا للمطالبة المقدمة الخاصة بالتجديد لمدة مماثلة او ثلاث سنوات طبقا للقيمة المالية المقدمة وسوف يتم تحرير عقد صيانة بالشروط التي سوف يتم الاتفاق عليها بين الطرفين وستكون ملزمه بناء علي اتفاقية سرية المعلومات وعدم الافصاح ( NDA )

١٥- تكون الشركة المورد مسؤوله مسؤوليه كاملة وقانونيه فى حالة توقف التراخيص طوال مدة سريان العقد او خدمه المسؤول عنها.

١٦- تكون الشركة المورد مسؤوله مسؤوليه كاملة وقانونيه عن تأمين البيانات من الاختراق وحماية الانظمه من

الهجمات السيبرانيه داخليا او خارجيا

أحمد عبد العنصر  
م. مصطفى

١٧- في حالة حدوث اعطال حرجه قد تؤدي الى توقف النظام او تخص منظومه الحماية يجب تواجد المهندس المختص حتي بعد إنتهاء مواعيد العمل الرسمية الخاصه بشركه القليوبيه لحين حل المشكله وفي حالة عدم الاستجابه عن طريق وسائل الاتصال المتفق عليها سواء تليفونيا او عن طريق البريد الالكتروني او عن طريق حضور المهندس المختص الى مقر شركة القليوبية في فترة خلال ٢٤ ساعه يتم عمل محضر بعدم الحضور من قبل اداره تكنولوجيا المعلومات ويتم توقيع غرامه ماليه قدرها ١٠ الاف جنيها مصريا عن كل يوم تأخير كشرط جزائي.

١٨- المحافظه علي سلامة البيانات الحاليه واستمرار الاعمال بقدر الإمكان وتحديد مواعيد مسبقه ويتم الموافقه عليها من قبل لجنة الاشراف و إدارة تكنولوجيا المعلومات في حالة التطرق الى اي Downtime أثناء تركيب وتشغيل المنظومه الجديده.

١٩- لتلزم الشركة المورد بتوصيل كافة الاجهزة المطلوب توصيلها بالشبكة الداخلية والأجهزة والخوادم مع الالتزام بكافة الاعمال المطلوبه لذلك

٢٠- جميع التركيبات لاي مكونات خاصة بالعملية هي مسئولية الشركة المورد وتتم بواسطة المختصين لدينا

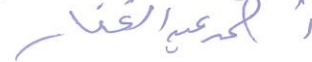
٢١- مسئوليه تركيب وتشغيل الاجهزة تقع على عاتق الشركة المورد بما في ذلك اي اعدادت يتطلبها تشغيل الاجهزة بشكل جيد او تجهيزات لمكان التركيب او كابلات او وصلات

٢٢- مسئولية تركيب وتوافق تلك الاجهزة مع الاجهزة ونظم التشغيل والبرامج الموجودة بالشركة وما يستلزمه ذلك من كروت ترقية او تحديث لبرامج التشغيل مسئوليه الشركه المورد

٢٣- في حالة نقل الخوادم من فرع التجاري بنبها الي الديوان العام بنبها يلتزم المورد بتحمل نفقات اي نقل او تركيب او استبدال او تشغيل في الاجهزه المورد بدون تحمل اي تكلفه اضافيه على الشركه وفي هذه الحاله سيقوم المورد وحده تحت اشراف اداره تكنولوجيا المعلومات بعمل تغليف لجميع الأجهزة التي سيتم نقلها وستكون مسئولية المورد مسئوليه كامله وقانونية مع الاخذ في الاعتبار عمل اي Installation او

Upgrade او Configuration لاي نظام سيتم نقله من مكانه









٢٤- الشركة مسؤولة عن بقاء الاعمال سليمة مدة الضمان فاذا ظهر بها خلل او عيب تقوم باصلاحها على نفقتها

٢٥- العملية غير قابل للتجزئه

٢٦- يجب على مقدم العرض توفير جميع المعدات اللازمة لتثبيت infrastructure cabling system

Patch Panels, Outlets, Ducts, Cables connectors, Cabinets inside the )

( Data center and other infrastructure اللازمة لاستكمال المنظومة

٢٧- يجب أن يكون مقدمو العطاءات مسؤولين عن تركيب جميع ducting system for both Copper

and Fiber داخل مبني الداتا سنتر والمباني الأخرى اذا تم طلبه

٢٨- بعد التشغيل يجب على مقدم العرض تقديم جميع الوثائق الفنية لتثبيت واختبار جميع المكونات المقدمة

Active and passive components.

٢٩- يتم عمل labels لجميع الكابلات من طرفي الكابل وايضا Patch panel

٣٠- يتم عمل fluke test لـ كابلات الـ UTP اذا تم طلبه

٣١- يتم عمل OTDR لـ كابلات الـ Fiber اذا تم طلبه

أحمد عبد الغفار

م. م. م. م. م.



البند الأول :

رقم البند	وصف البند	العدد
١	<b>Internet Firewall ( Perimeter Firewall ) – HQ Firewalls</b> جهاز جدار ناري للمبنى الرئيسي	٢

The proposed Security should support but not be limited to the following specifications:

**General Requirements: | Must be Support the below**

- ✓ The Next-Generation Firewall series is ideal for building security-driven networks at distributed enterprise sites and transforming WAN architecture at any scale.
- ✓ The Next-Generation Firewall has the industry's first integrated SD-WAN enforcement within an NGFW solution and is powered by one OS. automatically controls, verifies, and facilitates user access to applications, delivering consistency with a seamless and optimized user experience.
- ✓ Security-driven networking with FortiOS delivers converged networking and security.
- ✓ FortiOS enables the convergence of high-performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments
- ✓ FortiOS powers all FortiGate deployments whether a physical or virtual device, as a container, or as a cloud service. This universal deployment model enables the consolidation of many technologies and use cases into organically built best-of-breed capabilities, unified operating system, and ultra-scalability. The solution allows organizations to protect all edges, simplify operations, and run their business without compromising performance or protection.
- ✓ FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more. It provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE
- ✓ FortiGuard Labs' suite of AI-powered Security Services—natively integrated with yourNGFW—secures web, content, and devices and protects networks from ransomware and sophisticated cyberattacks
- ✓ Real-time SSL inspection (including TLS 1.3) provides full visibility into users, devices, and applications across the attack surface
- ✓ Fortinet's patented SPU (Security Processing Unit) technology provides industry-leading high-performance protection
- ✓ FortiGate WAN Edge powered by one OS and unified security and management framework and systems transforms and secures WANs

سرمهني

أحمد عبد الغنى



Holding Company for water and wastewater  
Kalyobia



الشركة القابضة لمياه الشرب والصرف الصحي

Company for water and wastewater

شركة مياه الشرب والصرف الصحي بالقليوبية

- ✓ Delivers superior quality of experience and effective security posture for work-from-any where models, SD-Branch, and cloud-first WAN use cases
- ✓ Achieve operational efficiencies at any scale through automation, deep analytics, and self-healing

**Requirements Specs Hardware ,System ,Performance Must be matched with the following specs**

**Hardware Specifications :**

- ✓ GE RJ45 Interfaces: 16
- ✓ GE SFP Slots: 8
- ✓ 10 GE SFP+ / GE SFP Slots: 4
- ✓ 25 GE SFP28 / 10 GE SFP+ Ultra Low Latency Slots : 4
- ✓ 2.5 GE / GE HA Port: 1
- ✓ GE RJ45 Management Ports: 1
- ✓ USB Ports (Client / Server): 2/2
- ✓ RJ45 Console Port : 1
- ✓ Onboard Storage: 2x 480 GB

**System Performance**

- ✓ IPS Throughput : 26 Gbps
- ✓ NGFW Throughput : 22 Gbps
- ✓ Threat Protection Throughput : 20 Gbps
- ✓ IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP) : 164 / 163 / 153 Gbps
- ✓ Firewall Latency (64 byte, UDP) : 3.78 / 2.5  $\mu$ s\*
- ✓ Firewall Throughput (Packet per Second) : 229.5 Mpps
- ✓ Concurrent Sessions (TCP) : 16 Million
- ✓ New Sessions/Second (TCP): 700000
- ✓ Firewall Policies: 10000
- ✓ IPsec VPN Throughput (512 byte) : 55 Gbps
- ✓ Gateway-to-Gateway IPsec VPN Tunnels :2000
- ✓ Client-to-Gateway IPsec VPN Tunnels :50000
- ✓ SSL-VPN Throughput : 10 Gbps
- ✓ Concurrent SSL-VPN Users : (Recommended Maximum, Tunnel Mode) : 10000
- ✓ SSL Inspection Throughput : (IPS, avg. HTTPS) : 16.7 Gbps
- ✓ SSL Inspection CPS (IPS, avg. HTTPS) : 18000
- ✓ SSL Inspection Concurrent Session (IPS, avg. HTTPS) : 1.6 Million
- ✓ Application Control Throughput (HTTP 64K) : 74.8 Gbps
- ✓ CAPWAP Throughput (HTTP 64K) : 70 Gbps
- ✓ Virtual Domains (Default / Maximum) : 10 / 10
- ✓ Number of Switches Supported to manage : 96
- ✓ Number of Aps to manage (Total / Tunnel) : 1024 / 512

سوردي

أحمد عيسى العناني

تليفاكس ٠١٣٣٢١٤٧٩٧

تليفاكس ٠٢٤٩٨١١٠٦٢

المقر المؤقت للشركة : بنها - محطة المياه المرشحة - شارع الرياح التوفيقي  
فرع القناطر الخيرية : محطة مياه القناطر الخيرية الرئيسية - كورنيش النيل



- ✓ High Availability Configurations Active-Active, Active-Passive
- ✓ The Required License: one-year Unified Threat Protection (UTP)
- ✓ Support: FortiCare Premium Support one year
- ✓ Redundant Power Supplies (Hot Swappable)
- ✓ Form Factor Rack Mount, 1 RU
- ✓ Default dual AC PSU for 1+1 Redundancy
- ✓ The system includes everything needed to complete installation
- ✓ Required Transceivers SFP and DAC Cables (Must be the Transceivers & DAC Cables The Same Vendor of Firewall):
  - ❖ FN-CABLE-SFP28-5: 25 GE SFP28 passive direct attach cable 5m with SFP28 slots Quantity 8
  - ❖ FN-TRAN-SFP28-SR : 25GE/10 GE Dual Rate SFP28 transceiver module, short range for systems with SFP28/SFP+ slots Quantity 8
  - ❖ FN-TRAN-SFP+SR: 10 GE SFP+ transceiver module Quantity 8
- ✓ Training:

- ❖ يجب ان يكون العرض الخاص لجهاز الفايروول المقدم شامل التدريب بناء على الشروط الاتية :
- ❖ كورس FortiSwitch & FortiGate Administrator
- ❖ الكورس المقدم لا بد ان يكون معتمد ( Official Course ) بنظام اليوم الكامل من Authorized Training Center وكتابة أسماء مراكز التدريب المعتمدة لهذه الكورسات من الشركات الام
- ❖ يجب أن تكون الكورسات بأحدث إصدار للكورس وتقديم محتوى كل كورس بشكل مفصل ( Course official outlines )
- ❖ عدد المتدربين ٣ أشخاص
- ❖ يجب أن تكون الكورسات مقدمه بناء على التفاصيل في الجدول التالي بناء على أسماء كورسات الشركات المصنعه :

البند	Course Code	Course Description	Number of Days	Attendees number	Training Center Name

إدارة المياه والصرف الصحي

س. م. م. م. م. م.

تليفاكس ٠١٣٣٢١٤٧٩٧  
تليفاكس ٠٢٤٩٨١١٠٦٢

المقر المؤقت للشركة : بنها - محطة المياه المرشحة - شارع الرياح التوفيقي  
فرع القناطر الخيرية : محطة مياه القناطر الخيرية الرئيسية - كورنيش النيل



## البند الثاني :

رقم البند	وصف البند	العدد
٢	<b>Branches Firewalls</b> جهاز جدار ناري للأفرع	١٣

The proposed Security should support but not limited to the following specifications:

**General Requirements: | Must be Support the below**

- ✓ The Next-Generation Firewall series is ideal for building security-driven networks at distributed enterprise sites and transforming WAN architecture at any scale.
- ✓ The Next-Generation Firewall has the industry's first integrated SD-WAN enforcement within an NGFW solution and is powered by one OS. automatically controls, verifies, and facilitates user access to applications, delivering consistency with a seamless and optimized user experience.
- ✓ Security-driven networking with FortiOS delivers converged networking and security.
- ✓ FortiOS enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments
- ✓ FortiOS powers all FortiGate deployments whether a physical or virtual device, as a container, or as a cloud service. This universal deployment model enables the consolidation of many technologies and use cases into organically built best-of-breed capabilities, unified operating system, and ultra-scalability. The solution allows organizations to protect all edges, simplify operations, and run their business without compromising performance or protection.
- ✓ FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more. It provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE
- ✓ FortiGuard Labs' suite of AI-powered Security Services—natively integrated with your NGFW—secures web, content, and devices and protects networks from ransomware and sophisticated cyberattacks
- ✓ Real-time SSL inspection (including TLS 1.3) provides full visibility into users, devices, and applications across the attack surface
- ✓ Fortinet's patented SPU (Security Processing Unit) technology provides industry-leading high-performance protection
- ✓ FortiGate WAN Edge powered by one OS and unified security and management framework and systems transforms and secures WANs

سمر مصطفى



- ✓ Delivers superior quality of experience and effective security posture for work-from-any where models, SD-Branch, and cloud-first WAN use cases
- ✓ Achieve operational efficiencies at any scale through automation, deep analytics, and self-healing

### Requirements Specs Hardware, System, Performance Must be matched with the following specs

#### Hardware Specifications :

- ✓ Hardware Based
- ✓ 1x USB Port
- ✓ 1x Console Port
- ✓ 1x GE RJ45 WAN Port
- ✓ 1x GE RJ45 Forti Link Port
- ✓ 3x GE RJ45 Ethernet Ports

#### System Performance

- ✓ IPS Throughput : 1 Gbps
- ✓ NGFW Throughput : 800 Mbps
- ✓ Threat Protection Throughput : 600 Mbps
- ✓ Firewall Throughput (1518 / 512 / 64 byte UDP packets) : 5 / 5 / 5 Gbps
- ✓ Firewall Latency (64 byte UDP packets) : 2.97  $\mu$ s
- ✓ Firewall Throughput (Packets Per Second) : 7.5 Mpps
- ✓ Concurrent Sessions (TCP) : 700 000
- ✓ New Sessions/Second (TCP) : 35 000
- ✓ Firewall Policies : 5000
- ✓ IPsec VPN Throughput (512 byte) : 4.4 Gbps
- ✓ Gateway-to-Gateway IPsec VPN Tunnels : 200
- ✓ Client-to-Gateway IPsec VPN Tunnels : 250
- ✓ SSL-VPN Throughput : 490 Mbps
- ✓ Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode) : 200
- ✓ SSL Inspection Throughput (IPS, avg. HTTPS) : 310 Mbps
- ✓ SSL Inspection CPS (IPS, avg. HTTPS) : 320
- ✓ SSL Inspection Concurrent Session (IPS, avg. HTTPS) : 55000
- ✓ Application Control Throughput (HTTP 64K) : 990 Mbps
- ✓ CAPWAP Throughput (HTTP 64K) : 3.5 Gbps
- ✓ Virtual Domains (Default / Maximum) : 10 / 10
- ✓ Number of FortiSwitches Supported to manage: 8
- ✓ Number of FortiAPs Supported to manage (Total / Tunnel Mode) : 16 / 8
- ✓ Number of FortiTokens : 500
- ✓ High Availability Configurations Active-Active, Active-Passive, Clustering

سوردي  
المقر المؤقت للشركة



- ✓ The Required License: one-year Unified Threat Protection (UTP)
- ✓ Support: FortiCare Premium Support one year
- ✓ The system include everything needed to complete installation
- ✓ Training:

- ❖ يجب ان يكون العرض الخاص لجهاز الفايروول المقدم شامل التدريب بناء على الشروط الاتية :
- ❖ كورس FortiEDR & FortiManager Administrator
- ❖ الكورس المقدم لابد ان يكون معتمد ( Official Course ) بنظام اليوم الكامل من Authorized Training Center وكتابة أسماء مراكز التدريب المعتمدة لهذه الكورسات من الشركات الام
- ❖ يجب أن تكون الكورسات بأحدث إصدار للكورس وتقديم محتوى كل كورس بشكل مفصل ( Course official outlines )
- ❖ عدد المتدربين ٣ أشخاص
- ❖ يجب أن تكون الكورسات مقدمه بناء على التفاصيل في الجدول التالي بناء على اسماء كورسات الشركات المصنعه :

البند	Course Code	Course Description	Number of Days	Attendees number	Training Center Name

إلى مدير القنصل

مكرم حسن

البند الثالث :

رقم البند	وصف البند	العدد
٣	Sandboxing جهاز ساندبوكس	١

The proposed Sandbox should support but not limited to the following specifications:

**General Requirements: | Must be Support the below**

- ✓ The Sandbox is the most flexible threat-analysis appliance available as it offers various deployment options for unique configurations and requirements. Organizations can choose to combine these options.
- ✓ The Sandbox is a high-performance security solution that utilizes AI/machine learning technology to identify and isolate advanced threats in real-time.
- ✓ The Sandbox inspects files, websites, URLs and network traffic for malicious activity, including zero-day threats, and uses sandboxing technology to analyze suspicious files in a secure virtual environment
- ✓ The Sandbox supports multiple operating systems and file types, and provides reporting capabilities for quick threat identification and response. Suitable for organizations of any size and can be deployed on-premises, in the cloud, or as a hosted service, and integrates natively with 11 Security Fabric products and other tools to evaluate suspicious content
- ✓ Real Time VERDICTS Prevent delays and unknown files from entering the network with real-time analysis and filtering
- ✓ Integration at every stage Extend zero-day threat protection to NGFWs and other major areas of your infrastructure
- ✓ Accelerated Threat Investigation Speed investigation with built-in MITRE ATT&CK® matrix to identify a variety of malware
- ✓ Performance Optimization With twice the VM capacity and file processing capabilities, and the highest detection accuracy, and best-breed throughput, while offering flexible and cost-effective deployment solutions.
- ✓ The Sandbox natively integrates with FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy, FortiClient (ATP agent) , Fabric-Ready Partner solutions, and via JSON API or ICAP with third party security vendors. The integration provides suspicious content submission, timely remediation, and reporting capabilities.
- ✓ NetShare Scan : The Sandbox facilitates scanning of file repositories via CIFs, NFS, AWS S3 Buckets, and Azure Blob. This feature allows system admin and web hosting to sanitize any file sharing. It is the ideal option for enhancing an existing multi-vendor threat protection approach.

أحمد عبد الفتاح  
مدير عمليات





- ✓ HA-Cluster : The Sandbox natively supports clustering to expand the throughput capacity of up to 99 worker nodes. The HA feature provides redundancy for uninterrupted critical operation
- ✓ Platform as a Service (PaaS) Hosted Sandbox services offer the same Fortinet Security Fabric integration as the Sandbox appliances. The Sandbox (PaaS) can easily scale to facilitate current and future business needs without big upfront investments, offering lower operational costs. Fortinet maintains, updates, and operates the platform on your behalf.
- ✓ Real Time Anti-Phishing The Sandbox provides protection against zero-day phishing. The URLs extracted from emails and embedded from documents are processed in the FortiGuard cloud. The web pages are downloaded in real-time and analyze using patented technologies to determine any phishing signs

**Requirements Specs Hardware, System, Performance Must be matched with the following specs**

**Hardware and System Specifications:**

- ✓ Must be H/W Appliance 1RU Appliance
- ✓ Network Interfaces: 4x GE RJ45 ports
- ✓ Storage Capacity: 1x 960 GB
- ✓ Trusted Platform Module (TPM) : YES
- ✓ Effective Sandboxing Throughput4 (Files/Hr) : 10,000
- ✓ Static Analysis Throughput7 (Files/Hr) :20,000
- ✓ Dynamic Analysis Throughput8 (Files/Hr ) : 500
- ✓ FortiMail Throughput9 (Emails/Hr) : 100,000
- ✓ MTA Adapter Throughput (Emails/Hr) : 10,000
- ✓ Sniffer Mode Throughput (Gbps) : 0.5
- ✓ Number of Users : 1400

**Systems Integration Support**

- ✓ File and URL submission by Security Fabric devices
  - Integrated mode with FortiGate. HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM, and their equivalent SSL-encrypted versions
  - Integrated mode with FortiMail. SMTP, POP3, IMAP
  - Integrated mode with FortiClient EMS. HTTP, FTP, SMB
  - Integrated mode with FortiWeb. HTTP
  - Integrated mode with FortiEDR
- ✓ Sniffer mode. HTTP, FTP, POP3, IMAP, SMTP, SMB
- ✓ Proxy inspection via ICAP
- ✓ MTA/BCC mode via SMTP
- ✓ NetShare Scan mode via CIFs, NFS, AWS S3, and Azure Blob

محمد حسن  
محمد عبد الغفار



- ✓ JSON API to automate the process of uploading samples and downloading actionable malware indicators to remediate
- ✓ Dynamic Threat Intelligence DB update of malicious file checksum and URL
- ✓ Remote and secured logging with FortiAnalyzer, FortiSIEM, CEF servers and syslog servers

#### Advanced Threat Protection:

- ✓ Inline blocking to detect and protect against Zero-day Malware including ransomware
- ✓ Real-time identification of Zero-day Phishing sites including spam and malware-hosted sites
- ✓ AI-powered static code analysis identifying possible threats within non-running code
- ✓ Deep learning powered VM-Less emulation of Windows executable codes (PEXBox)
- ✓ Network threat detection in sniffer mode. Identify botnet activities and network attacks, malicious URL visits
- ✓ Sandbox Community Cloud for shared analysis within the worldwide community of deployments

#### Monitoring and Report

- ✓ Configuration via GUI and CLI
- ✓ Multiple administrator accounts supporting full or view only access
- ✓ Radius authentication for administrators
- ✓ Single Sign-On via SAML
- ✓ Cluster management page for administering the HA and cluster nodes
- ✓ Centralized search page allowing administrators to build customized search conditions
- ✓ Upload any license from a single convenient page
- ✓ Self-Check widget for configurations, connectivity, and services
- ✓ VM status monitoring
- ✓ Automatic engine and signature updates
- ✓ Automatic check for new VM image availability
- ✓ System health check alerting system
- ✓ NTP via FortiGuard support
- ✓ Backup, restore, and revision of system configuration
- ✓ Consolidated CLI for troubleshooting
- ✓ Option to auto-submit suspicious files to cloud service for manual analysis and signature creation
- ✓ Option on NetShare scan mode to prioritize and forward files to a third-party scanning for further scanning

#### Sandboxing (Dynamic AI Scan) Support

- ✓ AI-powered behavioral analysis constantly learning new malware and ransomware techniques
- ✓ Concurrent Sandbox instances
- ✓ OS type supported: Windows 11/10/8.1/7, macOS, Linux, Android, and ICS systems
- ✓ Customizable VMs for Windows and Linux OS

*Handwritten signature*

*Handwritten signature*



- ✓ Configurable internet browser supporting Internet Explorer, Microsoft Edge, Google Chrome, and Mozilla Firefox
- ✓ Sandbox interactive mode
- ✓ Video-recording of malware interaction
- ✓ Anti-evasion detection techniques:
  - API Obfuscation
  - Bare-metal Detection
  - Command and Control
  - Direct System Calls
  - Execution Delay
  - Memory Only Payload
  - Process Hollowing/Injection
  - Runtime Encryption/Packing
  - System Fingerprinting
  - Time Bomb
  - User Files Check
  - User Interaction Check
  - VM/Sandbox Detection
- ✓ Callback detection. Malicious URL visit, botnet C&C communication, and attacker traffic from activated malware
- ✓ Downloadable captured packets, tracer logs, and screenshots
- ✓ User-defined extension

#### File Types Support:

- Windows Executables: .bat, .cab, .cmd, .dll, .exe, .js, .msi, .ps1, .vbs, wsf
- Microsoft Office: .doc, .docm, .docx, .dot, .dotm, .dotx, .iqy, .one, .pot, .potm, .potx, .ppt, .pptm, .pptx, .ppam, .pps, .ppsm, .ppsx, .pub, .rtf, .sldm, .sldx, .xlam, .xls, .xlsb, .xlt, .xlsm, .xlsx, .xlt, .xltm, .xltx
- Document/Email files: .eml, .pdf, .rl
- Android files: .apk
- Linux files: .elf
- MacOS files: .app, .dmg, Mach-O
- Web files: .htm, html, .lnk, WEblink
- Compress files: .7z, .ace, .arj, .bz2, .gz, .iso, .jar, .kgb, .lzh, .rar, .swf, .tar, .tgz, .upx, .xz, .z, .zip

#### Sandboxing HW , License and Support:

- ✓ Sandboxing Appliance - 4 GE RJ45, 1 Win11, 1 Win10, 1 Office21. Upgradable to max 14 VMs.
- ✓ License and support :
  - Expands licensed VM capacity by 2. Includes 1 Win11 and 1 Win10 licenses. Quantity 1
  - Sandbox Threat Intelligence (Antivirus, IPS, Web Filtering, File Query, Industrial Security, SandBox Engine) Quantity 1

محمد مصطفى  
مدير العمليات

٠١٣٣٢١٤٧٩٧ تليفاكس  
٠٢٤٩٨١١٠٦٢ تليفاكس

المقر المؤقت للشركة : بنها - محطة المياه المرشحة - شارع الرياح التوفيقي  
فرع القناطر الخيرية : محطة مياه القناطر الخيرية الرئيسية - كورنيش النيل



- FSA-UPG-OFFICE2021-1 :Expands FSA (Appliance/VM) licenses of Microsoft Office 2021 Quantity 1
- The license must include features to detect in real-time, signs of Phishing, SPAM or Malicious content in a website Quantity 1
- One year Premium Support
- The system include everything needed to complete installation

## ✓ Training:

- ❖ يجب ان يكون العرض الخاص لجهاز Sandbox المقدم شامل التدريب بناء على الشروط الاتية :
- ❖ كورس FortiSandbox
- ❖ الكورس المقدم لايد ان يكون معتمد ( Official Course ) بنظام اليوم الكامل من Authorized Training Center وكتابة أسماء مراكز التدريب المعتمدة لهذه الكورسات من الشركات الام
- ❖ يجب أن تكون الكورسات بأحدث إصدار للكورس وتقديم محتوى كل كورس بشكل مفصل ( Course official outlines )
- ❖ عدد المتدربين ٣ أشخاص
- ❖ يجب أن تكون الكورسات مقدمه بناء على التفاصيل في الجدول التالي بناء على اسماء كورسات الشركات المصنعه :

البند	Course Code	Course Description	Number of Days	Attendees number	Training Center Name

أحمد عبد العنانه  
م. مصطفى

البند الرابع :

رقم البند	وصف البند	العدد
٤	<b>Network Access Control (NAC SOLUTION)</b> جهاز تحكم لوصول الشبكة	١

The proposed Network Access Control (NAC SOLUTION) should support but not limited to the following specifications:

**General Requirements: | Must be Support the below**

- ✓ Network access control solution that enhances the Security Fabric with visibility, control, and automated response for everything that connects to the network. NAC SOLUTION provides protection against IoT threats, extends control to third-party devices, and orchestrates automatic responses to a wide range of networking events.
- ✓ The NAC Solution provides detailed profiling of even headless devices on your network using multiple information and behavior sources to accurately identify what is on your network.
- ✓ Implement micro-segmentation policies and change configurations on switches and wireless products. Extend the reach of the Security Fabric in heterogeneous environments.
- ✓ React to events in your network in seconds to contain threats before they spread. NAC SOLUTION offers a broad and customizable set of automation policies that can instantly trigger configuration changes when the targeted behavior is observed.
- ✓ Scan the network for detection and classification of devices via agent or agentless (automated)
- ✓ Create an inventory of all devices on the network
- ✓ Assess risk of every endpoint on the network
- ✓ Centralize architecture for easier deployment and management
- ✓ Provide extensive support for third-party network devices to ensure effectiveness with existing network infrastructure
- ✓ Automate onboarding process for a large number of endpoints, users, and guests
- ✓ Enforce dynamic network access control and enable network segmentation
- ✓ Reduce containment time from days to seconds
- ✓ Provide event reporting to SIEM with detailed contextual data to reduce investigation time
- ✓ Ensuring the integrity of devices before they connect to the network minimizes risk and the possible spread of malware. NAC SOLUTION validates a device's configuration as it attempts to join the network. If the configuration is found to be non-compliant, the device can be handled appropriately such as by an

محمد مصطفى

د. محمد عبد العطار



isolated or limited access VLAN that has no access to corporate resources as a threat, NAC SOLUTION triggers an automated response to contain the endpoint in real-time.

- ✓ The solution's capability now extends beyond automated onboarding of new endpoints; it incorporates real-time threat intelligence and continuous risk assessment of devices, leveraging machine learning and AI technologies from FortiGuard Services. Given the rising prominence of BYOD (Bring Your Own Device) and IoT (Internet of Things) and continuous monitoring and immediate remediation of non-compliant devices have become even more crucial.
- ✓ Continues to be a cutting-edge network access control solution, enabling organizations to enforce network access policies and assure adherence to security protocols in light of increasingly sophisticated threats. It provides a comprehensive snapshot of all devices and users on the network, facilitating granular control of access based on user roles, device types, network locations, and now the behavioral patterns of devices and users.
- ✓ Granular Visibility Across the Network for Every Device and User : NAC SOLUTION leverages AI and machine learning to provide detailed profiling of devices, including headless devices and IoT assets on your network. This profiling incorporates multiple information sources, behavior patterns, and real-time threat intelligence to accurately identify and assess what is on your network.
- ✓ NAC SOLUTION will monitor the network on an ongoing basis, evaluating endpoints to ensure they conform to their profile. NAC SOLUTION will rescan devices to ensure MAC-address spoofing does not bypass your network access security. Additionally, NAC SOLUTION can watch for anomalies in traffic patterns. This passive anomaly detection works in conjunction with FortiGate appliances. Once a compromised or vulnerable endpoint is detected
- ✓ Seamless Integration and Control Across Diverse Environments: With the power of micro-segmentation and Zero Trust policies, NAC SOLUTION allows for configuration changes on switches and wireless products from an extended range of vendors. It amplifies the reach of the Security Fabric across multi-cloud, hybrid IT, and heterogeneous environments, implementing "never trust, always verify" principles.
- ✓ Automated Response: NAC SOLUTION reacts to network events in real-time to contain threats before they spread, utilizing a broad and customizable set of automation policies. Leveraging AI, these policies can instantly trigger configuration changes and remediation actions when targeted behavior or anomalies are observed, aligning with the Zero Trust model's dynamic and proactive approach.
- ✓ Network Security and Intelligent Segmentation: After successful classification of devices and user identification, NAC SOLUTION now integrates advanced segmentation techniques to ensure only authorized users and devices have access to requisite resources, thus preventing unauthorized intrusion. Through its progressive role-based network access control, NAC SOLUTION allows for strategic network segmentation by logically grouping similar data and applications, limiting access to a particular set of users or devices. This strategy effectively confines a compromised device, thereby inhibiting its ability to traverse the network and inflict damage on other resources. NAC SOLUTION not only fortifies the protection of sensitive data and vital assets but also ensures adherence to internal, industrial, and government regulations and mandates

إ. محمد عبدالقنا  
م. مصطفى



- ✓ Device Integrity Verification and Malware Prevention: NAC SOLUTION emphasizes on the importance of device integrity prior to network connection, significantly reducing the risk and potential spread of malicious software. As a device attempts to join the network, NAC SOLUTION assesses its configuration for compliance. Any non-compliant configuration is promptly managed; for instance, the device may be allocated to an isolated or restricted access VLAN, devoid of any access to corporate resources. This feature has become increasingly relevant with the rise of IoT devices and remote work trends, ensuring a secure and controlled network environment.
- ✓ Security Fabric Integrations: The NAC Solutions must integrate with multiple Fortinet products such as FortiGate, FortiSIEM, FortiAnalyzer, FortiEDR . The Security Rules are triggered by syslog/SNMP messages from the other Fortinet products.

### Requirements Specs Hardware, System ,Performance Must be matched with the following specs

#### Hardware and System Specifications:

- ✓ Must be H/W Appliance 1RU Appliance
- ✓ CPU: 24 Core, 2.65GHz
- ✓ Memory: 32GB DDR4 memory
- ✓ Hard Disk: 2x 960GB SSDs
- ✓ Network Interfaces: 1x GbE RJ45 and 4x 10GbE SFP+ ( must be SFP+ MM transceivers included)
- ✓ RAID Configuration: Software RAID1
- ✓ Power Supply: Hot Plug, 1+1 Redundant PSU
- ✓ Cooling: 5x system fans
- ✓ Deployment: Single site Deployment

#### NAC Solution Integrations :

Extensive integration with desktop security software, directories, network infrastructure, and third-party security systems provides unparalleled visibility and control across the network environment.

- ✓ The NAC Solution integrates examples:
  - **Network Infrastructure:** Fortinet, Adtran, Aerohive, AlaxaIA Networks, Alcatel-Lucent, Allied Telesis, Alteon, APC, Apple, APRESIA Systems, Avaya, Brocade/Foundry Networks/Ruckus, Cisco/Meraki, D-Link, Extreme/Enterasys/Siemens, H3C, HP/Colubris/3Com/Aruba, Intel, Juniper, NEC, Riverbed/Xirrus, and SonicWall
  - **Security Infrastructure:** CheckPoint, Cisco/SourceFire, PaloAlto , Cyphort, FireEye, Juniper/ Netscreen, Qualys, Sonicwall, Tenable
  - **Authentication and Directory Services:** RADIUS — Cisco ACS, Free RADIUS, Microsoft IAS, LDAP — Google SSO, Microsoft Active Directory, OpenLDAP
  - **Operating Systems:** Android, Apple MAC OSX and iOS, Linux, Microsoft Windows

المهندس محمد العبد  
محمد مصطفى



- **Endpoint Security Applications:** FortiEDR , Authentium, Avast, AVG, Avira, Blink, Bullguard, CA, ClamAV, Dr. Web, Enigma, ESET, F-Prot, F-Secure, G Data, Intego, Javacool, Lavasoft, Lightspeed, McAfee, Microsoft, MicroWorld, Norman, Norton, Panda, PC Tools, Rising, Softwin, Sophos, Spyware Bot, Sunbelt, Symantec, Trend Micro, Vexira, Webroot SpySweeper, Zone Alarm
- **Mobile Device Management:** AirWatch, Google GSuite, MaaS360, Microsoft InTune, Mobile Iron, XenMobile, JAMF, Nozomi Networks

### NAC Solution License and Support:

The proposed NAC Solution Must be providing the following features: -

- ✓ Hardware and software Support Duration: one year support
- ✓ License Duration: one year
- ✓ The system includes everything needed to complete installation
- ✓ Number of Concurrent Endpoints: 500 Endpoints
- ✓ The license must be providing the ultimate in visibility, control and response.
- ✓ The license offers real-time endpoint visibility, comprehensive access control, and automated threat response and delivers contextual information with triaged alerts.
- ✓ The license level is appropriate for organizations that want complete endpoint visibility, a flexible NAC solution with granular controls, as well as accurate event triage and real-time automated threat response.
- ✓ The license must be providing the following features: -
  - Event Correlation
  - Extensible Actions & Audit Trail
  - Alert Criticality & Routing
  - Guided Triage Workflows
- ✓ Training:

- ❖ يجب ان يكون العرض الخاص بال NAC المقدم شامل التدريب بناء على الشروط الاتية :
- ❖ كورس FortiNAC
- ❖ الكورس المقدم لابد ان يكون معتمد ( Official Course ) بنظام اليوم الكامل من Authorized Training Center وكتابة أسماء مراكز التدريب المعتمدة لهذه الكورسات من الشركات الام
- ❖ يجب أن تكون الكورسات بأحدث إصدار للكورس وتقديم محتوى كل كورس بشكل مفصل ( Course official outlines )
- ❖ عدد المتدربين ٣ أشخاص
- ❖ يجب أن تكون الكورسات مقدمه بناء على التفاصيل في الجدول التالي بناء على اسماء كورسات الشركات المصنعه :

البند	Course Code	Course Description	Number of Days	Attendees number	Training Center Name

د. محمد الخنار

تليفاكس ٠١٣٣٢١٤٧٩٧  
تليفاكس ٠٢٤٩٨١١٠٦٢

المقر المؤقت للشركة : بنها - محطة المياه المرشحة - شارع الرياح التوفيقي  
فرع القناطر الخيرية : محطة مياه القناطر الخيرية الرئيسية - كورنيش النيل



البند الخامس :

رقم البند	وصف البند	العدد
٥	Data Center Firewall جهاز جدار ناري للداتا سنتر	١

The Data Center Firewall solution should support but not limited to the following specifications:

**General Requirements: | Must be Support the below**

- ✓ Identifies the applications traversing your network irrespective of port, protocol, evasive techniques, or encryption (TLS/SSL). In addition, it automatically discovers and controls new applications
- ✓ Uses the application, not the port, as the basis for all your safe enablement policy decisions: allow, deny, schedule, inspect, and apply traffic-shaping.
- ✓ Offers the ability to create custom App-ID™ tags for proprietary applications or request App-ID development for new applications.
- ✓ Embeds machine learning (ML) in the core of the firewall to provide inline signatureless attack prevention for file-based attacks while identifying and immediately stopping never-before-seen phishing attempts.
- ✓ based ML processes to push zero-delay signatures and instructions back to the NGFW
- ✓ Identifies all payload data within the application (e.g., files and data patterns) to block malicious files and thwart data exfiltration attempts.
- ✓ Creates standard and customized application usage reports, including software-as-a-service (SaaS) reports that provide insight into all sanctioned and unsanctioned SaaS traffic on your network.
- ✓ Enables safe migration of legacy Layer 4 rule sets to App-ID-based rules with built-in Policy Optimizer, giving you a rule set that is more secure and easier to manage
- ✓ Enables visibility, security policies, reporting, and forensics based on users and groups—not just IP addresses.
- ✓ Easily integrates with a wide range of repositories to leverage user information: wireless LAN controllers, VPNs, directory servers, SIEMs, proxies, and more.
- ✓ Allows you to define Dynamic User Groups (DUGs) on the firewall to take time-bound security actions without waiting for changes to be applied to user directories.
- ✓ Applies consistent policies irrespective of users' locations (office, home, travel, etc.) and devices (iOS and Android® mobile devices, macOS®, Windows®, Linux desktops, laptops; Citrix and Microsoft VDI and Terminal Servers).
- ✓ Prevents corporate credentials from leaking to third-party websites and prevents reuse of stolen

سرموصفي

أحمد عبدالغندر



credentials by enabling multi-factor authentication (MFA) at the network layer for any application without any application changes.

- ✓ Provides dynamic security actions based on user behavior to restrict suspicious or malicious users.
- ✓ Consistently authenticates and authorizes your users, regardless of location and where user identity stores live, to quickly move towards a Zero Trust security posture with Cloud Identity Engine—an entirely new cloud-based architecture for identity-based security
- ✓ Inspects and applies policy to TLS/SSL-encrypted traffic, both inbound and outbound, including for traffic that uses TLS 1.3 and HTTP/2.
- ✓ Offers rich visibility into TLS traffic, such as amount of encrypted traffic, TLS/SSL versions, cipher suites, and more, without decrypting.
- ✓ Enables control over use of legacy TLS protocols, insecure ciphers, and misconfigured certificates to mitigate risks.
- ✓ Facilitates easy deployment of decryption and lets you use built-in logs to troubleshoot issues, such as applications with pinned certificates.
- ✓ Lets you enable or disable decryption flexibly based on URL category and source and destination zone, address, user, user group, device, and port, for privacy and regulatory compliance purposes.
- ✓ Allows you to create a copy of decrypted traffic from the firewall (i.e., decryption mirroring) and send it to traffic collection tools for forensics, historical purposes, or data loss prevention (DLP).
- ✓ Allows you to intelligently forward all traffic (decrypted TLS, non-decrypted TLS, and non-TLS) to third-party security tools with Network Packet Broker and optimize your network performance and reduce operating expenses.
- ✓ Routing
  - OSPFv2/v3 with graceful restart, BGP with graceful restart, RIP, static routing
  - Policy-based forwarding
  - (PPPoE) and DHCP supported for dynamic address assignment
  - Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3
  - Bidirectional Forwarding Detection (BFD)
- ✓ IPsec VPN
  - Key exchange: manual key, IKEv1, and IKEv2 (pre-shared key, certificate-based authentication)
  - Encryption: 3DES, AES (128-bit, 192-bit, 256-bit)
  - Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512
- ✓ VLANs
  - 802.1Q VLAN tags per device/per interface: 4,094/4,094
  - Aggregate interfaces (802.3ad), LACP
- ✓ Network Address Translation
  - NAT modes (IPv4): static IP, dynamic IP, dynamic IP and port (port address translation)
  - NAT64, NPTv6
  - Additional NAT features: dynamic IP reservation, tunable dynamic IP and port oversubscription
- ✓ High Availability

أحمد عبد الفتاح / محمد حسن



- Modes: active/active, active/passive, HA clustering
- Failure detection: path monitoring, interface monitoring
- ✓ Mobile Network Infrastructure\*
  - 5G Security
  - 5G MEC (multi-access edge computing) Security
  - GTP Security
  - SCTP Security

**Requirements Specs Hardware, System, Performance Must be matched with the following specs**

**Data Center Firewall Hardware and System Specifications:**

- ✓ Must be H/W Appliance
- ✓ CPU: 24 cores
- ✓ Storage Capacity: 480 GB SSD
- ✓ Network Interfaces:
  - 1G/10G SFP/SFP+ : 12
  - 25G SFP28 : 4
  - 40G/100G QSFP+/QSFP28 : 4
- ✓ Management Interfaces:
  - Out-of-band management 1G SFP : 1
  - High availability 1G SFP : 2
  - High availability 40G QSFP+ : 1
  - Console port RJ-45 : 1
- ✓ Max BTU/hr : 1638
- ✓ Power Supplies (Base/Max) : 1:1 fully redundant (2/2)
- ✓ AC Power Supply Output : 1,200 watts/power supply
- ✓ Mean Time Between Failure (MTBF) : 22 years
- ✓ Required Transceivers SFP and DAC Cables (Must be the Transceivers & DAC Cables The Same Vendor of Firewall):
  - 100 Gb transceiver module MM Quantity 2
  - 40 Gb QSFP+ transceiver module MM Quantity 10
  - 25 Gb SFP28 transceiver module MM Quantity 8

**Data Center Firewall Performance Specifications:**

- ✓ Firewall throughput (HTTP/appmix) : 46.2/39.0 Gbps
- ✓ Threat Prevention throughput (HTTP/appmix): 22.5/24.8 Gbps
- ✓ IPsec VPN throughput: 21 Gbps
- ✓ Max sessions: 5M
- ✓ New sessions per second: 295,000

رئيس الشركة  
محمد مصطفى



- ✓ Virtual systems (base/max): 10/20

### Data Center Firewall License and Support:

The proposed Data Center Firewall Solution Must be providing the following features: -

- ✓ Advanced Threat Prevention: Stop known exploits, malware, malicious URLs, spyware, and com-mand and control with prevention of web-based Cobalt Strike
- ✓ Hardware and software Support Duration: one year support
- ✓ License Duration: one year
- ✓ The system include everything needed to complete installation
- ✓ Training:

❖ يجب ان يكون العرض الخاص لجهاز الفايروول المقدم شامل التدريب بناء على الشروط الاتية :

❖ كورس ( Network Security Engineer covers how to (design, deploy, operate, manage, and troubleshoot

❖ الكورس المقدم لابد ان يكون معتمد ( Official Course ) بنظام اليوم الكامل من Authorized Training Center وكتابة أسماء مراكز التدريب المعتمدة لهذه الكورسات من الشركات الام

❖ يجب أن تكون الكورسات بأحدث إصدار للكورس وتقديم محتوى كل كورس بشكل مفصل ( Course official outlines )

❖ عدد المتدربين ٣ أشخاص

❖ يجب أن تكون الكورسات مقدمه بناء على التفاصيل في الجدول التالي بناء على اسماء كورسات الشركات المصنعه :

البند	Course Code	Course Description	Number of Days	Attendees number	Training Center Name

أحمد العبد  
م. مصطفى

البند السادس :

رقم البند	وصف البند	العدد
٦	WAF جهاز جدار ناري للمتصفح والتطبيقات	١

The WAF solution should support but not limited to the following specifications:

General Requirements and system features: | Must be Support the below

- ✓ (WAF) that protects web applications and APIs from attacks that target known and unknown exploits and helps maintain compliance with regulations.
- ✓ Using machine learning to model each application, WAF defends applications from known vulnerabilities and from zero-day threats. High performance physical appliances on-site—from small businesses to service providers, carriers, and large enterprises
- ✓ OWASP Top 10 risks to web applications: There are various ways to exploit vulnerable applications. At the core, a WAAP solution must compensate for these risks (such as SQL injections, XSS, broken access control, denial-of-service) including anomaly detection and zero-day protection.
- ✓ Bot management: Machine learning and behavioral analysis to distinguish bots from human users, and good from bad bots
- ✓ Real-time monitoring: Ensure the solution offers real-time monitoring capabilities to detect and respond to threats as they occur
- ✓ API Protection : Protect your APIs from malicious actors by automatically enforcing positive and negative security policies. Seamlessly integrate API security into your CI/CD pipeline.
- ✓ Application Protection : Multi layer protection against the OWASP Top 10 application attacks including machine learning to defend against known and unknown attacks.
- ✓ Bot Mitigation : Protect websites, mobile applications, and APIs from automated attacks with advanced bot mitigation that accurately differentiates between good bot traffic and malicious bots. The WAF Bot Mitigation provides the visibility and control you need without slowing down your users with unnecessary captchas or challenges.
- ✓ Machine Learning Improves Detection and Drives Operational Efficiency : multi-layer approach provides two key benefits: superior threat detection and improved operational efficiency and ability to detect anomalous behavior relative to the specific application being protected enables the solution to block unknown, never-before-seen exploits, providing your best protection against zero-day attacks targeting your application and machine learning relieves you of time-consuming tasks such as remediating false

محمد مصطفى  
أحمد عبد العنار



positives or manually tuning WAF rules and continually updates the model as your application evolves, so there is no need to manually update rules every time you update your application.

- ✓ Comprehensive Web Application Security : Using an advanced multi-layered and correlated approach, WAF provides complete security for your web-based applications from the OWASP Top 10 and many other threats. NGWAF first layer of defense uses traditional WAF detection engines (e.g. attack signatures, IP address reputation, protocol validation, and more) to identify and block malicious traffic, powered by intelligence from Fortinet's industry leading security research. WAF provide machine learning detection engine then examines traffic that passes this first layer, using a continuously updated model of your application to identify malicious anomalies and block them as well.
- ✓ AI-based Threat Analytics Help Zoom In on the Most Important Threats : Without better tools, security teams risk becoming overwhelmed by the volume of events, with many of those events turning out to be of low value when seen in isolation—or even worse, turning out to be false positives after further investigation. This alert fatigue can result in critical security events being missed or overlooked. WAF Provide Threat Analytics uses machine learning algorithms to identify attack patterns across your entire application attack surface and aggregate them into comprehensible security incidents. The solution separates significant threats from informational alerts and false positives by identifying patterns and assigning a severity to help your security team focus on the threats that matter. Investigating security alerts requires context and the ability to connect the dots across multiple events over time. WAF Provide Threat Analytics removes the complexity that comes from manually evaluating alerts by evaluating thousands of alerts and grouping those alerts into incidents based on the patterns identified. With this streamlined view, SOC analysts can focus their efforts on the important threats.
- ✓ Bot Mitigation : protects against automated bots, webs scrapers, crawlers, data harvesting, credential stuffing and other automated attacks to protect your web assets, mobile APIs, applications, users and sensitive data. Combining machine learning with policies such as threshold-based detection, Bot deception and Biometrics based detection with superior good bot identification, WAF is able to block malicious bot attacks while reducing friction on legitimate users. With advanced tracking techniques WAF can differentiate between humans, automated requests and repeat offenders, track behavior over time to better identify humans from bots and enforce CAPTCHA challenges when required. Together with graphical analysis dashboard organizations can quickly identify attacks and differentiate from good bots and legitimate users.
- ✓ Deep Integration into the Fortinet Security Fabric and Third-Party Scanners : As the threat landscape evolves, many new threats require a multi-pronged approach for protecting web-based applications. Advanced Persistent Threats that target users can take many different forms than traditional single-vector attack types and can evade protections offered only by a single device. The proposed WAF must be support integration with FortiGate and FortiSandbox extend basic WAF protections through synchronization and sharing of threat information to both deeply scan suspicious files and share infected internal sources.
- ✓ The proposed WAF must be support integration with leading third-party vulnerability scanners including Acunetix, HP WebInspect, IBM AppScan, Qualys, ImmuniWeb and WhiteHat to provide dynamic virtual

محمد مصطفى  
1 محمد عبد الفتاح



patches to security issues in application environments. Vulnerabilities found by the scanner are quickly and automatically turned into security rules to protect the application until developers can address them in the application code.

- ✓ Web Application Security : Block known and zero-day threats to applications without blocking legitimate users.
- ✓ Solving the Challenge of False Threat Detections: False positive threat detections can be very disruptive and force many administrators to loosen security rules on their web application firewalls to the point where many often become a monitoring tool rather than a trusted threat avoidance platform. The installation of a WAF may take only minutes, however fine-tuning can take days, or even weeks. Even after setup, a WAF can require regular checkups and tweaks as applications and the environment change.

### Requirements Specs Hardware, System ,Performance Must be matched with the following specs

#### Web Application Firewall Capabilities: | Must be Support the below Security Features

##### Security Services:

- Malware detection
- Virtual patching
- Protocol validation
- Brute force protection
- Cookie signing and encryption
- Threat scoring and weighting
- Syntax-based SQLi and XSS detection
- HTTP Header Security
- Custom error message and error code handling
- Operating system intrusion signatures
- Known threat and zero-day attack protection
- L4 Stateful Network Firewall
- DoS prevention
- Advanced correlation protection using multiple security elements
- Data leak prevention
- Web Defacement Protection

##### Application Attack Protection:

- OWASP Top 10
- Cross Site Scripting
- SQL Injection
- Cross Site Request Forgery
- Session Hijacking
- Built-in Vulnerability Scanner

محمد مصطفى  
أحمد عبد الفتاح



- Third-party scanner integration (virtual patching)
- File upload scanning with AV and sandbox

**Application Delivery:**

- Layer 7 server load balancing
- URL Rewriting
- Content Routing
- HTTPS/SSL Offloading
- HTTP Compression
- Caching

**Authentication:**

- Active and passive authentication
- Site Publishing and SSO
- RSA Access for 2-factor authentication
- LDAP, RADIUS, and SAML support
- SSL client certificate support
- CAPTCHA and Real Browser Enforcement (RBE)

**API Protection**

- Machine Learning based API Discovery and Protection
- XML and JSON protocol conformance
- CI/CD integration
- Schema verification
- API Gateway
- Web services signatures

**Bot Mitigation**

- Machine Learning based Bot
- Mitigation
- Biometrics Based Detection
- Threshold Based Detection
- Bot Deception
- Know Bots

**Management and Reporting**

- Web user interface
- Command line interface
- graphical analysis and reporting tools
- Central management for multiple web devices
- Active/Active HA Clustering

محمد عبد الفتاح  
مدير عمليات



١٢٧

Holding Company for water and wastewater  
Kalyobia



الشركة القابضة لمياه الشرب والصرف الصحي

Company for water and wastewater

شركة مياه الشرب والصرف الصحي بالقليوبية

- REST API
- Centralized logging and reporting
- User/device tracking
- Real-time dashboards
- Bot dashboard
- OWASP Top 10 attack categorization
- Geo IP Analytics
- SNMP, Syslog and Email Logging/Monitoring
- Administrative Domains with full RBAC

#### Web Security

- AI-based Machine Learning
- Automatic profiling (white list)
- Web server and application signatures (black list)
- IP address reputation
- IP address geolocation
- HTTP RFC compliance
- Native support for HTTP/2
- WebSocket protection and signature enforcement
- Man in the Browser (MiTB) protection

#### Deployment Options

- Reverse Proxy
- Inline Transparent
- True Transparent Proxy
- Offline Sniffing
- WCCP

#### Hardware and System Specifications: | Must be matched with the following specs |

- ✓ Must be H/W Appliance
- ✓ 10/100/1000 Interfaces (RJ-45 ports) : 4 GE RJ45 ,
- ✓ SFP Interfaces : 4 SFP GE ( must be SFP MM transceivers included)
- ✓ SSL/TLS Processing : Hardware
- ✓ USB Interfaces : 2
- ✓ Storage : 480 GB SSD
- ✓ Form Factor : 1U
- ✓ Power Supply : Dual PSU
- ✓ System Performance Throughput : 1 Gbps
- ✓ Latency : <5ms
- ✓ High Availability : Active/Passive, Active/Active Clustering

سور محمد  
عبد الفتاح

تليفاكس ٠١٣٣٢١٤٧٩٧  
تليفاكس ٠٢٤٩٨١١٠٦٢

المقر المؤقت للشركة : بنها - محطة المياه المرشحة - شارع الرياح التوفيقي  
فرع القناطر الخيرية : محطة مياه القناطر الخيرية الرئيسية - كورنيش النيل



- ✓ Application Licenses : Unlimited
- ✓ Administrative Domains : 32
- ✓ Forced Airflow : Front to Back
- ✓ Safety Certifications : FCC Class A Part 15, RCM, VCCI, CE, UL/CB/cUL
- ✓ Warranty and support : FortiCare Premium Support one year
- ✓ The Required License : one year Advanced Bundle License
- ✓ NOTE : the system include everything needed to complete installation
- ✓ Training:

- ❖ يجب ان يكون العرض الخاص بال WAF المقدم شامل التدريب بناء على الشروط الاتية :
- ❖ كورس FortiWeb Administrator
- ❖ الكورس المقدم لابد ان يكون معتمد ( Official Course ) بنظام اليوم الكامل من Authorized Training Center وكتابة أسماء مراكز التدريب المعتمدة لهذه الكورسات من الشركات الام
- ❖ يجب أن تكون الكورسات بأحدث إصدار للكورس وتقديم محتوى كل كورس بشكل مفصل ( Course official outlines )
- ❖ عدد المتدربين ٣ أشخاص
- ❖ يجب أن تكون الكورسات مقدمه بناء على التفاصيل في الجدول التالي بناء على أسماء كورسات الشركات المصنعه :

البند	Course Code	Course Description	Number of Days	Attendees number	Training Center Name

زاد عبد القادر  
مدير مبيعات



## البند السابع :

رقم البند	وصف البند	
V	Accessories	مستلزمات تشغيل
N	Description	QYT
1	Dell Host Bus Adapter (HBA) 16Gb/s Dual Port (DP) Fiber Channel (FC) For Dell R720	6
2	Network Card dual Port 10G SFP+ with transceivers For Dell R720	5
3	Network Card dual Port 10G SFP+ with transceivers For Dell R730	1
4	D4-2SFXL-3200 D4 3.2TB SAS FAST VP 25X2.5 SSD for Unity XT 380 480 Hard Disk	15
5	Dell 8TB 7.2K RPM SAS 12Gbps 512e 3.5in For IDPA 4400 WE need to check with DELL EMC	8
6	Rack 42U 800*1200	1
7	Windows Server 2022 Standard - 16 Core License Pack Part Number: DG7GMGF0D5RK	15
8	40GE QSFP+ Passive Direct Attach Cable, 5m for Systems with QSFP+ slots , Part Number : SP-CABLE-FS-QSFP+5	10
9	100 GE QSFP28 breakout to 4x 25 GE SFP28 passive direct attach cable, 3m , Part Number : FN-CABLE-QSFP28-4SFP28-3	8
10	10 GE SFP+ passive direct attach cable, 5m for systems with SFP+ and SFP/SFP+ slots. Part Number : FN-CABLE-SFP+5	20
11	100GE QSFP28 Passive Direct Attach Cable, 5 m for Systems with QSFP28 slots Part Number : FN-CABLE-QSFP28-5	12
12	Supply and install Video wall system include 4 Screens 49 Inch Panel Bezel to Panel Bezel: Maximum 1.25 mm (B/R) Vendor List: LG or Samsung ❖ The System must include all accessories required to installation	1

أ.ع. عبد الفتاح  
م.ع. محمد رمضان

تليفاكس ٠١٣٣٢١٤٧٩٧  
تليفاكس ٠٢٤٩٨١١٠٦٢

المقر المؤقت للشركة : بنها - محطة المياه المرشحة - شارع الرياح التوفيقي  
فرع القناطر الخيرية : محطة مياه القناطر الخيرية الرئيسية - كورنيش النيل

### جدول الكميات والفئات

م	بيان الاعمال والمواصفة	العدد	سعر الوحدة	الإجمالي
البند الأول	جهاز جدار ناري للمبني الرئيسي	٢		
البند الثاني	جهاز جدار ناري للأفرع	١٣		
البند الثالث	جهاز ساندبوكس	١		
البند الرابع	جهاز تحكم لوصول الشبكة	١		
البند الخامس	جهاز جدار ناري للداتا سنتر	١		
البند السادس	جهاز جدار ناري للمتنصفح والتطبيقات	١		
البند السابع	كارت فايبر شانيل بسرعة ١٦ جيجا ثنائي المنفذ Dell720	٦		
	كارت شبكة بسرعة ١٠ جيجا ثنائي المنفذ Dell 720	٥		
	كارت شبكة بسرعة ١٠ جيجا ثنائي المنفذ Dell730	١		
	هارد ديسك بمساحة ٣,٢ تيرا بايت Unity 380 XT	١٥		
	هارد ديسك بمساحة ٨ تيرا بايت لوحدة lpd4_4400	٨		
	راك 42U 800*1200	١		
	نظام تشغيل Windows server 2022	١٥		
	كابل فايبر بسرعة ٤٠ جيجا بطول ٥ امتار	١٠		
	كابل فايبر بسرعة ١٠٠ جيجا بطول ٣ امتار 4*1	٨		
	كابل فايبر بسرعة ١٠ جيجا بطول ٥ امتار	٢٠		
كابل فايبر بسرعة ١٠٠ جيجا بطول ٥ امتار	١٢			
شاشات حائط لمراقبة منظومة الأمن السيبراني	١			

❖ **ملاحظة:** يتم التسعير بالدولار الأمريكي وذلك طبقاً للمادة رقم ٨/٢٤ من لائحة العقود والمشتريات والتي تنص علي تتولي اللجنة المشكلة لفتح المظاريف تفرغ عطاءات الموردين في قوائم مقارنة ولتوحيد أسس المقارنة يتم تحويل مايرد بعباء المقاول من أسعار بالعملة الجنية إلي الجنيه المصري وفقاً لمتوسط صرف العملة الأجنبية المعلن عنها من البنك المركزي في اليوم المحدد لفتح المظروف المالي. للاستفسار يرجى الإرسال على فاكس الشركة (٠١٣٠٣١٨٨١٢٢) أو المراسلة بالبريد أو البريد الإلكتروني

(sale7.it@qlbww.com.eg / medhat.it@qlbww.com.eg / alshaimaa.it@qlbww.com.eg / it@qlbww.com.eg)

محمد مصطفى  
أحمد عبد العظمى

تليفاكس ٠١٣٣٢١٤٧٩٧  
تليفاكس ٠٢٤٩٨١١٠٦٢

المقر المؤقت للشركة : بنها - محطة المياه المرشحة - شارع الرياح التوفيقي  
فرع القناطر الخيرية : محطة مياه القناطر الخيرية الرئيسية - كورنيش النيل