النهاية : الثانية

أبو أحمد محمد شرارة

mohamed@sharara.org

ابريل 2012

إهداء

إلى مشايخنا الكرام أهل العلم الذين يقفون على الثغور

وطبعاً إلى أمي وأبي رحمهم الله

وزوجتي وأولادي

وإلى الكناس اللي بيقف من الفجر في الشارع في البرد أو الحر حتى لو كان بيحرك التراب من هنا لهنا

المحتويات

شكراً للشباب دول

المراجعة الفنية :

كريم محمد eng-karim-it@hotmail.com

محمود فوزي mahmoudfawzy5@yahoo.co.uk

المراجعة الإملائية :

حاتم أحمد hatem-ahmd@hotmail.com

مقدمة

الحمد لله والصلاة والسلام على رسول الله

أما بعد فمن فضل الله عز وجل أن بدأت سلسلة البداية والنهايات في صنعة الشبكات

فكانت النهاية الأولى : والتي تناولت أساسيات الشبكات و الويندوز إكس بي وسيرفر 2003

ثم النهاية واحدة ونص : وكانت مخصصة لويندوز سفن و2008 سيرفر

والأن اعتقد أنه وقت النهاية الثانية : تي إم جي وأخواتها

تتناول هذه النهاية البقاء على إتصال مع العالم من خلال الإنترنت وتوزيعه والفايروول والبروكسي

ولكن .....

لن نحصر أنفسنا في TMG فقط , بل سنتناول الكثير من البدائل التي يمكنها أن تحل محله وذلك بما يتناسب مع إحتياجات كل منشأة

باختصار : قليل من الثقة منكم بأن هذا العالم به شركات أخرى غير Microsoft

وأكيد أيضا أن بيل جيتس ليس هو الوحيد في عالمنا هذا " اللي دايس في الكمبيوتر"

يتناول الكتاب :-

- معلومات عن الإنترنت من وجهة نظر الـ IT مع حلول التوصيل المختلفة
- حلول متنوعة لتوزيع الإنترنت والفايروول سواء المبنية على الويندوز أو اللينكس
- وفي نهاية الكتاب رأيت أن أستعرض أهم أداتين لمحاولة إجراء تصفح ومحادثة آمنين على الإنترنت مع تجربة للـ Cloud DNS من خلال Open DNS

لم أكن أنتوي ☺ أن تحمل هذه النهاية إسما مختلفاً ولكن منعاً للإلتباس وتطويراً للفكرة فقد رأيت أن يتم إصدار النهايات الجديدة من موسوعة البداية والنهايات في صنعة الشبكات بأسماء تنم عن محتوى كل نهاية على أن تظل هذه النهايات تحت مظلة البداية والنهايات وجزءاً منها لذا فهذا الكتاب سيحمل إسم : تي إم جي وأخواتها مع كونه النهاية الثانية من موسوعة البداية والنهايات في صنعة الشبكات

وإذا شاء الله فستكون النهاية الثالثة أيضا لها إسمها الخاص وهكذا

ومادمنا قد قررنا أن نجعل هذا الكتاب خاص بالإنترنت وتوزيعه والتحكم فيه وقبل أن نبدأ "وندخل في الجد" يجب علينا أن نتحدث قليلا من منطلق ترتيب العمل أو من منطلق تبادل الأفكار أو حتى من منطلق الكلام للكلام

- *لماذا الإنترنت والإتصالات ؟*

نجيب على السؤال بسؤال : *كيف نهضت أمريكا ؟*

طبعا لا يمكننا الإجابة عن هذا السؤال في سطرين أو حتى في كتاب فأسباب نهوض الأمم متعددة ومتشعبة ومتشابكة بالطبع

ولكن سنذكر أحد الأسباب الهامة جدا لنهضة أمريكا : المواصلات !!

لو نتذكر أفلام الهنود الحمر " قبل ماربنا يتوب علينا من مشاهدتها " كان التركيز في أغلب هذه الأفلام يدور حول : خط السكة الحديد

الصراع دائما وأبدا حول : مد خطوط السكك الحديدية

أيضا لا نستطيع أن نتجاهل أحد أهم المشاريع الأميريكية : قناة بناما , ومابذلته أمريكا من محاولات عدة في سبيل إتمام حفر هذه القناة أعجوبة عصرها

وهذا بالفعل ما حدث و تميزت به أمريكا طوال عمرها القصير : خطوط المواصلات القوية جدا والتي تتيح نقل أسرع سواء لخامات أو منتجات أو عمالة أو حتى جيوش

منذ فترة أعددت موضوع حول قناة بناما وذهلت عندما علمت أن هذه القناة كلفتها أمريكا مبلغ 380 مليون دولار " الكلام ده منذ أكثر من 100 سنه " , ولكن يتلاشى الذهول إذا ما تخيلنا حال أمريكا أو نفوذها أو قوتها في حال عدم وجود هذه القناة

- *سؤال : ماهي الخطوة الأولى في فتح الأندلس ؟*

بناء أسطول قوي

- *سؤال كمان : كيف فتح محمد الفاتح القسطنطينية ؟*

حرك الأسطول براً إلى خلف خطوط دفاع العدو " يعني جعل السفن تمشي على الأرض "

وبعد المواصلات Transportations كانت الإتصالات Communications

إحتلت محلها وأخذت منها الأهمية وأصبحت المعلومة وتداولها هي الوسيلة وأحيانا هي الغاية وصار الجميع يركز على كيفية توصيل المعلومة في أسرع وقت وضمان توافرها في أي مكان لمن يحتاجها

وتطورت الأدوات وتغيرت إحتياجاتنا فأصبحت بعض الرفاهيات السابقة ضروريات

يعني من كام سنه كان ممكن يكون لك عنوان بريدي , وجواب يوصل وغيره يضيع

ورقم تليفون أرضي ممكن الناس يتصلوا بيك وترد وأحيانا تكون مش موجود وماتردش

والأن :

- لكل منا إيميل أو أكثر
- وهاتف محمول لا يفارقنا
- وحساب فيس بوك وجوجول بلاس وأحيانا تويتر
- و البعض أيضا يمتلك موقع شخصي ومدونة

المهم أن هذه الأشياء أصبحت من الأساسيات التي لا يمكن " لغالبيتنا " الإستغناء عنها

الدنيا كلها أصبحت تهتم بالـ Communications واحنا كمان ما ينفعش إننا مانهتمش بيه

يعني مكالمة التليفون اللي ممكن ما نكونش موجودين في البيت و مانستقبلهاش , النهارده أصبحت بتطاردنا في الشارع و البيت

الإيميل أصبح شيء مهم جدا جدا وأخذ مكان الفاكس و الجواب العادي , بل أخذ أكثر من كده كمان

من الأشياء المهمة التي أحاول جعل من أعرفهم يعتادوا عليها : كل يوم تفتح الإيميل

حتى لو مش مستني أي ميلات

لازم تعود نفسك على كده

إنك تكون In Touch .... لازم الناس تعرف توصل لك في أي وقت

مش عيب إن الإيميل بوكس في الأول يكون عبارة عن ميلات من مجموعات وكده , لأن ده أسلوب حياة بتتعود عليه وبالتدريج ستعتبر الإيميل هو الوسيلة الأولى بالنسبة لك وده الإنطباع اللي الناس ح يتعاملوا معاك على أساسه وبالتدريج بتعرف أهمية الوقت واللي حواليك بيتأثروا بيك

بالنسبة للـ IT ما ينفعش انك ما تفتحش الأيميل بتاعك الصبح , لأن ممكن يكون في email مهم جدا جدا يغير إتجاهك اليومي

أول خطوات التطوير في أي شركة :إدخال خدمة الإنترنت وضمان إستمراريتها

و أهم خطوات التطوير هي الـ Mail Service مع التركيز على إكساب المستخدم العادي المهارات الأساسية للتعامل مع الإيميل , وتدريجيا تصبح هذه مهارة أساسية لديه وبدلا من إرسال الفاكس أو إنتظاره يتمكن من تداول ما يريد من معلومات في لحظات

لا أستطيع أيضا أن أتصور كيف يمكن لـ IT أن يعيش بدون Smart Phone ويستفيد بإمكانياته لأقصى درجة " أغلب من تعاملت معهم من الـ IT مع إختلاف مستوياتهم كانوا كده للأسف"

والقضية ليست تبادل ملفات بلوتوث ولكن نرجع ونقول : أسلوب حياة

فالموبايل هو إدارة IT ومركز ترفيه مصغر في جيبي بل هو النافذة التي نتعامل بها مع العالم ومع أنفسنا وبخاصة مع ثورة السحاب أو الـ Cloud Computing

- *ما هو الـ Cloud Computing؟*

بإختصار : أن تكون ملفاتك والجزء الأساسي من نظام تشغيلك و برامجك جزء من الإنترنت يعني بالبلدي أن يكون جهازك مجرد terminal تدخل به على الإنترنت حيث يمكنك منه"على الإنترنت " التعامل على ملفاتك وتحريرها
فالموضوع يعتمد على قيام الشركات بتوفير سيرفرات ضخمه تلبي إحتياجاتنا وهكذا يتم الجزء الأكبر من التشغيل على الإنترنت و يصبح الجهاز الخاص بنا مجرد أداة للوصول إلى نظام التشغيل والملفات وطبعا البرامج

ما يهمنا الآن هو التنبيه على الفكرة الأساسية في الأمر وهي إنك مادمت قادرا على الوصول الى الإنترنت " بإستخدام أي وسيلة " فأنت إذاً في مكتبك أو بصورة " أقسى " فأنت في حياتك

فممارستك للجزء الأكبر من أنشطة حياتك اليومية " سواء عمل أو ترفيه أو التواصل مع بعض أفراد عائلتك " سيتم من خلال الإنترنت

ولهذا فبداية نشاطك اليومي هي : الدخول على الإنترنت , وبعدها كل حاجه تتدبر

و لنتصور الفرق في مرحلة ماقبل الـ Cloud وما بعدها فيمكننا تبسيط الأمر في أننا حاليا نحتاج لتوافر بيئة بشروط معينة لممارسة الكثير من أنشطتنا اليومية

فمثلا إذا رغبت في إجراء بعض التعديلات في Memo وإرسالها للفريق الذي يعمل معي

سنحتاج أولا ملف الـ Memo الأصلي الذي سنجري عليه التعديلات

وسنحتاج برنامج لفتح هذا الملف والتعديل عليه من خلاله " وليكن برنامج MS Office"

وأخيرا سنحتاج عتاد Hardware لتعديل الملف بإستخدام البرنامج

أيضا قد نحتاج لطابعة لطباعة المذكرة بعد تعديلها

ولكن مع الـ Cloud فإن السيناريو مختلف

فالملف ليس مخزنا على جهازك ولكنه في مكان ما على الإنترنت تابع لمزود خدمه

أيضا التعديل لن يتم من خلال برنامج MS Office بل سيتم من خلال أحد البرامج الموجودة أيضا على الإنترنت " وليكن Google Docs"

وبعد إجراء التعديلات نرسله لباقي الفريق من خلال البرنامج سواء للمشاهدة أو لإجراء التعديلات أو إضافة تعليقات

ففي مرحلة ما بعد السحابية Cloud لن نحتاج إلى عتاد معين أو برامج معينة لإتمام المهام ولكن فقط Browser متصل بالإنترنت

لذا فكلما استطعنا التعامل مع البدائل المختلفة للإتصال بمهارة أكثر , كلما أصبحنا أكثر توافقا مع " أبجديات العصر "

سواء كان الإتصال من خلال جهاز المنزل أو الموبايل أو مقهى الإنترنت , المهم أن يتم الإتصال

فالعالم يتجه نحو السحابية من خلال محاور متوازية متسارعة , وكما ذكرت فإن هذا الموضوع سيكون له جزء خاص داخل الكتاب بمشيئة الله عز وجل

- *ياترى ح نلحق؟*

السؤال غامض ولكن ما أعنيه : أننا عندما ننتهي من هذه النهاية" تي إم جي وأخواتها " قد يكون ما يحتويه من معلومات قد عفا عليه الزمن وأصبح وكأنه تأريخ لعصر مضى

معدل التسارع مبهر للغاية وأقف أمامه مذهولا مندهشا

عندما إنتهيت من الجزء الأول تحدثت عن exchange server كمزود للإيميل , والأن فإن خدمة جوجول Google App تتقدم بسرعة رهيبة

و فايرفوكس وكروم Chrome "وليس شروم" يسطيران على جزء كبير من نسبة المتصفحات في مجال كان لوقت قريب حكراً على أنترنت إكسبلورر

عندما كتبت الجزء الأول أستخدمت Office 2003 , الآن أنا أتعامل مع Google Docs لكتابة المسودات ويتم التجهيز والتنسيق على Office

وأعتقد أنه مع التطور السريع جدا فإن خدمة docs والخدمات المماثلة ستجعلنا نستغني تماما عن تثبيت برنامج مثل office على جهازنا

عندما انتهيت من الجزء الأول كنت أتابع الخلاصات Feeds من خلال إضافة Brief التي يتم تثبيتها على Firefox والأن أستخدم Google Reader

عندما إنتهيت من النهاية واحده ونص كنت أتعامل مع لاب توب وجهاز موبايل والأن إنحشر بينهم جهاز Tab أصبحت لا أستغني عنه

- *يبقى من حقي أن أسأل السؤال ده : ياترى ح نلحق ؟*

إن شاء الله ح نلحق

عموما :

إذا كنت قد وصلك معلومات حول : أهمية الـ Communications ومدي تأثيرها

وإذا كنت لاحظت كم مره ذكرت كلمة إنترنت في الصفحات السابقة

فقد إستوعبت ما أريد وممكن نلحق

قبل البدء في هذه النهاية الجديدة أقول :

- **هذا كله مجرد أخذ بالأسباب ويبقى توفيق الله عز وجل لي ولكم , أولا وأخيرا هو الأساس**
- **أكررها مرة ثالثة : ليس المطلوب قراءة مابين السطور , ولكن فقط قراءة السطور بتركيز**
- **بنهاية الكتاب بمشيئة الله أتوقع منك أن تكون قادرا على التعامل مع أي برنامج أو سيرفر أو جهاز يتناول الوظائف ذاتها**
- **إعتدت أن أنشر كتبي في فصول ثم أجمعها وأنقحها ولكن تطويرا للفكرة وإختصاراً للوقت فقد قررت إصدار الكتاب مباشرة وكان من فضل الله أن يسّر لي مجموعة من الشباب تولوا هم المراجعة الفني منها والإملائي مما شجعني على إصدار الكتاب مباشرة فلهم خالص الشكر**
- **يوجد ضعف في تسويق الكتب السابقة لذا فإنني أطلب ممن يقرأ هذه المقدمة أن يجتهد في نشر هذا الكتاب قدر إستطاعته فلربما كان كتابا كهذا سببا في فتح باب رزق لأحد شبابنا الغالي**

نهاية فقد وفقني الله عز وجل في أن يكون هذا الكتاب متميزا لما احتواه من شرح لباقة كاملة متنوعة من برامج الفايروول والبروكسي , فلم أر كتابا يتناول أشهر بدائل توزيع الإنترنت على إختلاف البيئات التي تعمل عليها

لم يكن هذا بإجتهاد مني ولكن كان بتوفيق الله عز وجلّ أما ما كان من أخطاء أو تقصير أو إسهاب في غير محله فهو مني ومن الشيطان الله يحرقه

والله المستعان

سبحانك اللهم وبحمدك , أشهد ألا إله إلا أنت , أستغفرك وأتوب اليك

الفصل الأول : الإنترنت ... إزاي , مين , وبكام ؟؟

الإنترنت ... إزاي , مين , وبكام ؟؟

الحمد لله والصلاة والسلام على رسول الله

دلوقتي عندنا شبكه فيها دومين كونترولر وأجهزه

نبتدي نركز شويه في الخدمات اللي بنقدمها من خلال الشبكه وأهم خدمه ممكن تحتاجها الشبكه (وده من وجهة نظر المستخدمين) هي الإنترنت

ما شاء الله ... أحيانا الواحد بيمر عليه مستخدمين يدولك إحساس إنهم حاجه إلكتروني خالص وطبعا لا تملك معهم إلا نظرة سخريه ولسان حالك يقول : <u>على إيه ما احنا دافنينه سوا</u>

المهم بغض النظر عن الموضوع ده فإنه مما لاشك فيه إننا لازم نوصل خدمة الإنترنت للشبكة وحاليا أعتقد أنه مافيش شبكة من غير : إنترنت

وقبل ما نبتدي نوصل لازم نعرف :

<u>مين (ح نشترك مع مين)</u>

<u>بكام (تكلفة الإشتراك)</u>

<u>وقبلها إزاي (نوع الخدمه)</u>

أحيان كتير جدا بيكون القرار الخاطيء سبب في سلسلة من المواقف الكارثية اللانهائية

يعني مثلا إنك في يوم تتعاقد على توريد جهاز معين (راوتر مثلا) دون دراسة كافية ويكون هذا الجهاز غير متوافق مع ظروف التشغيل عندك ... تخيل كم الشكاوي والمشاكل التي ستواجهها بسبب هذا الجهاز

وغالبا ما يكون الإعتراف بالقرار الخاطيء أقل البدائل تكلفه لإصلاح هذا الخطأ , ففي مثالنا هذا يكون القرار : إستبدال الراوتر

- *طيب إيه العلاقه بين الإنترنت واللي أنا باقوله ؟*

العلاقه إن قرار مثل توصيل خدمة الإنترنت هو من القرارات التي تتطلب منك دراسة كافيه ومتأنيه

ونصيحه لك : لا تجعل ضغوط إدارة الشركة بالنسبه للوقت وسرعة التنفيذ سبباً في إختصارك لمراحل البحث والدراسه قبل إتخاذ قرارات مصيرية , يعني بالبلدي : نفض وخليك هادي لغاية ما توصل للقرار ساعتها ح تلاقي الإدارة بتشكرك على مجهودك

نرجع لموضوعنا وعلشان نجاوب على الاسئلة الثلاثة (والرابع ح ييجي بعدين) يبقى احنا محتاجين نعرف معلومات عن أنواع الخدمه وبعض المصطلحات المتعلقة بالإنترنت

الدايل اب Dialup

أكيد كلنا عارفين الدايل اب وهو الدخول للإنترنت من خلال خط الهاتف الأرضي عن طريق الإتصال بمزود الخدمه وبعد التأكد يتم فتح session بين الجهاز وبين الـ ISP (مزود خدمة الإنترنت) Internet Service Provider

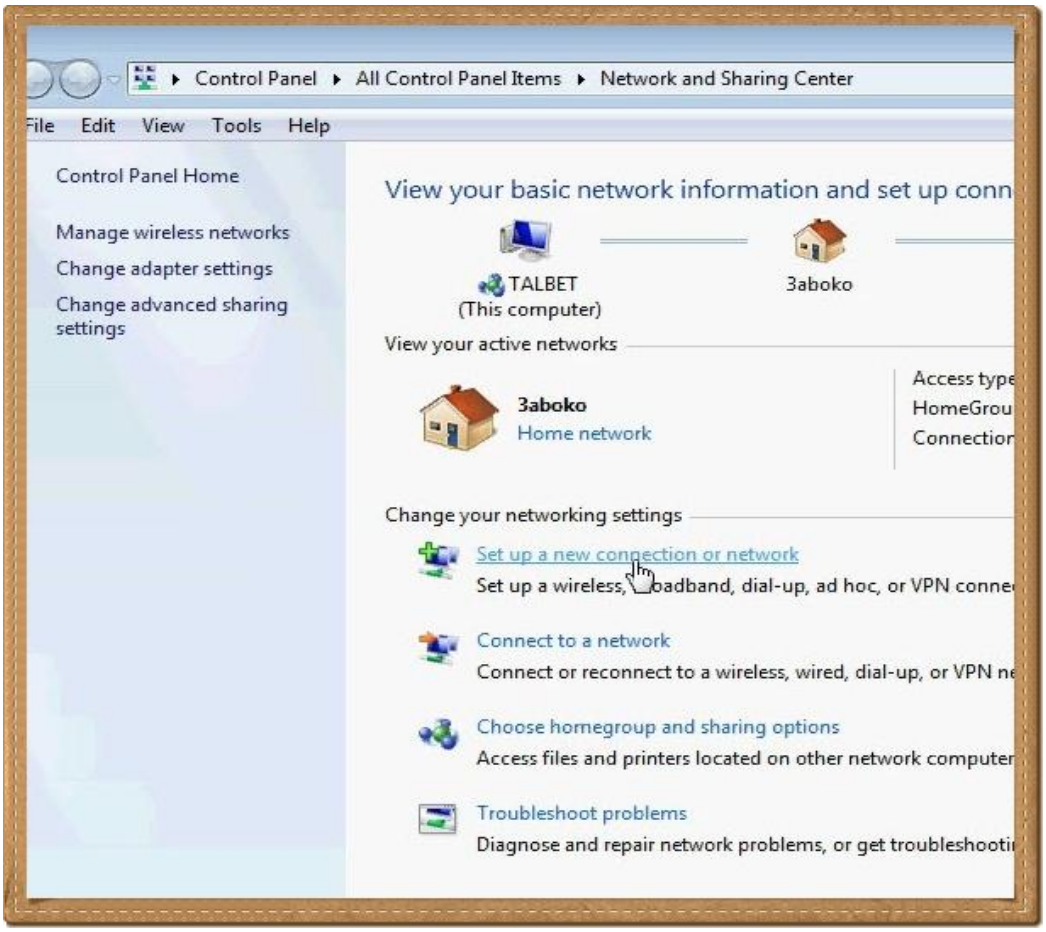
طبعا سرعة الدايل اب لا تتعدى 56kbps وبتكون analog يعني حاجه كده على ما تفرج

وعلشان تعمل dialup connection الموضوع بسيط جدا

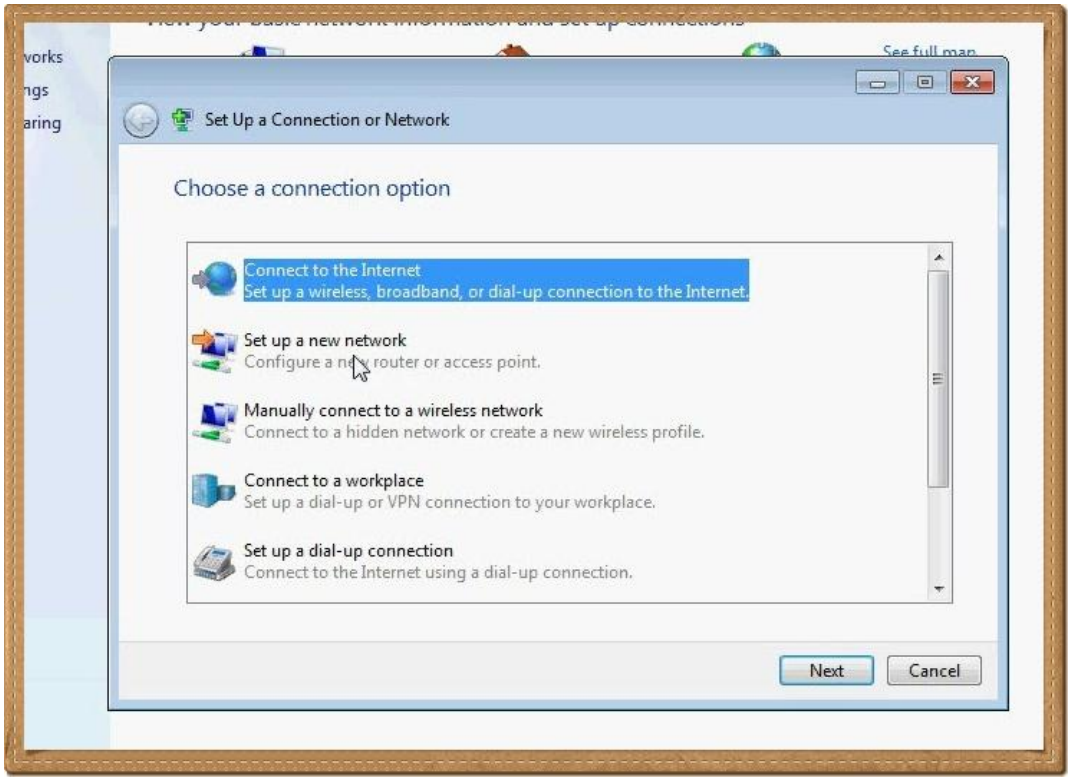
كليك يمين بالماوس على علامة الوايرلس

نختار Open Network and Sharing Center

نختار set up a connection or network

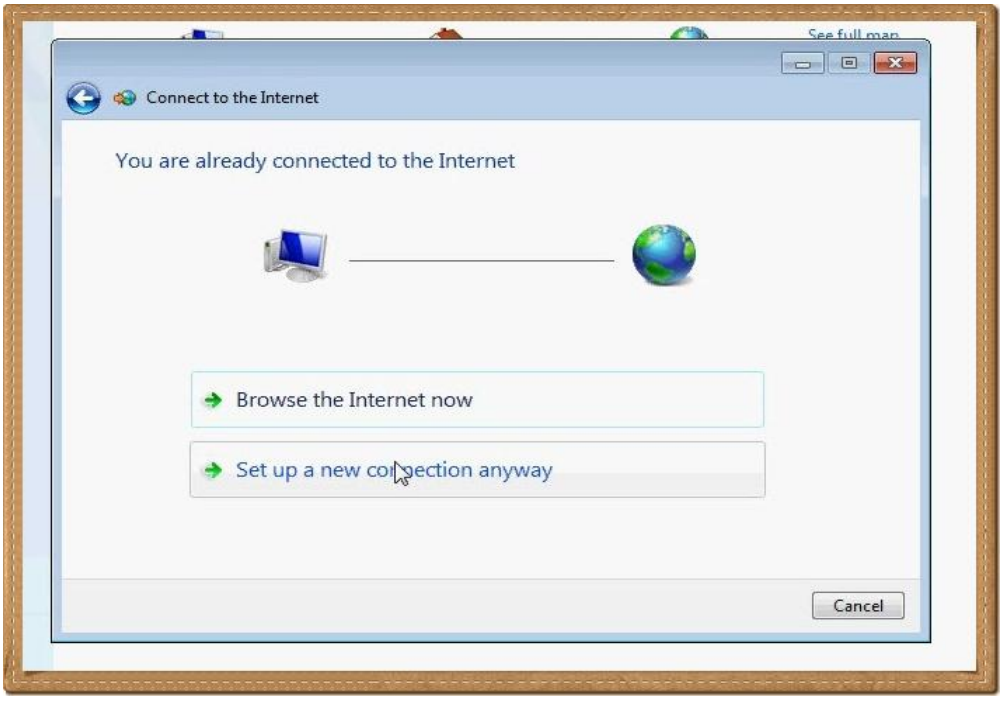


Connect to the Internet

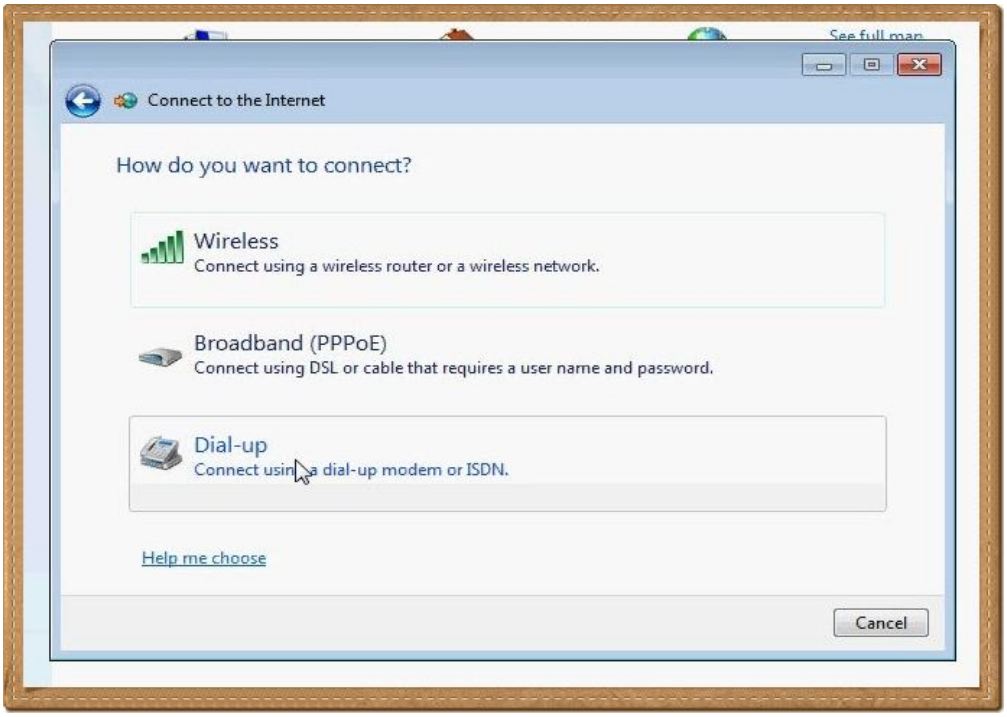


لو عندك إنترنت فعلا على الجهاز ح تلاقي الـ Wizard بيسألك سؤال تأكيد ..

تختار Set up a new connection anyway

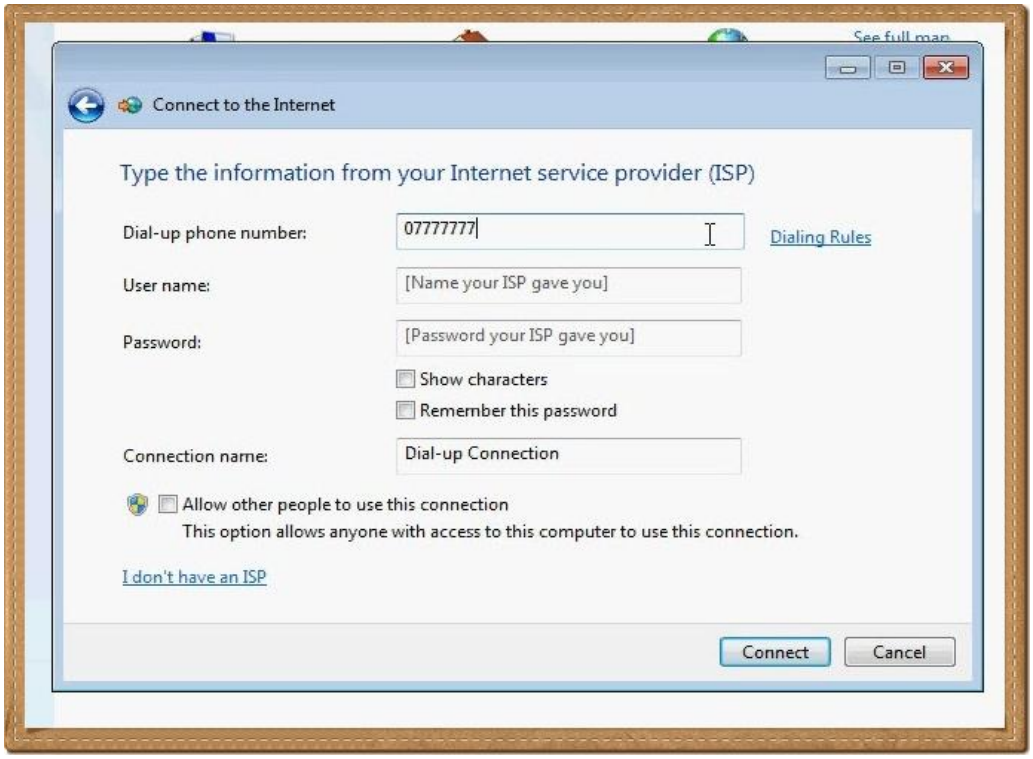


نختار Dial Up



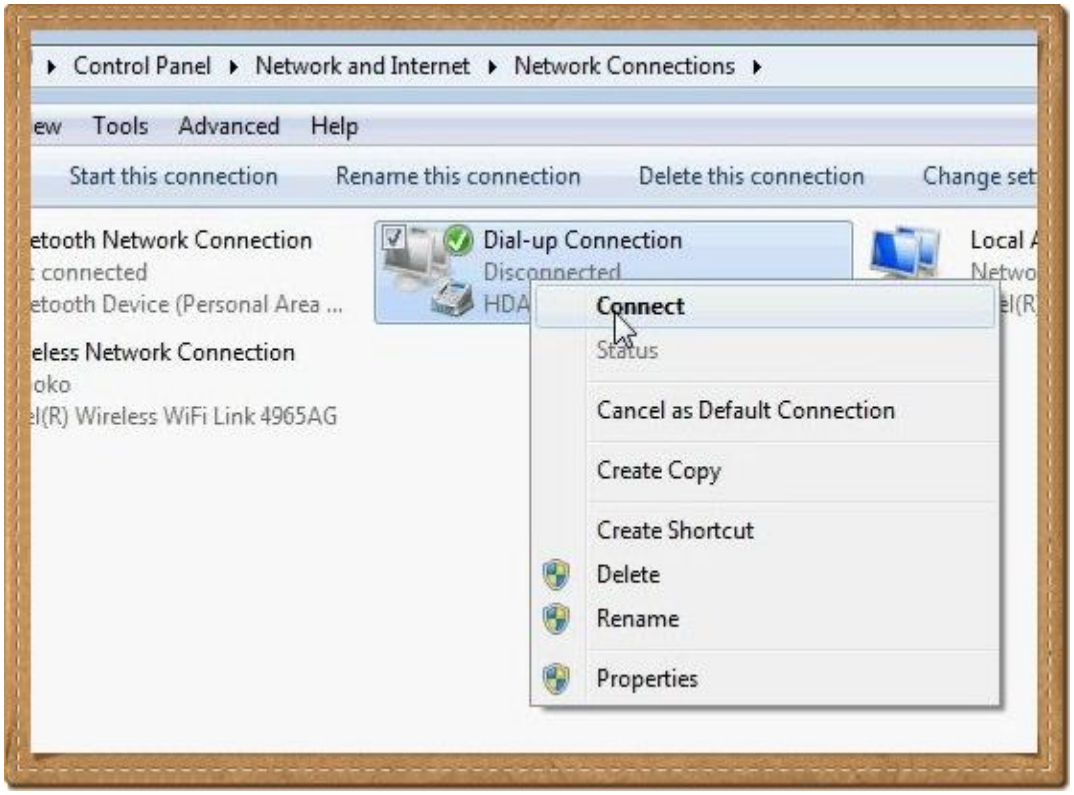
تختلف الإعدادات حسب النظام المطبق في بلدك .. في مصر لا تحتاج لإدخال أي بيانات غير الرقم الخاص بمقدم الخدمة ولا نحتاج لإسم مستخدم أو كلمة سر

ندخل رقم مزود الخدمة



ثم Connect

طبعا للإتصال بعد كده , كليك يمين على Dial up Connection



ثم Connect

وبكده يكون الإتصال مع الإنترنت بطريقة الـ dial up , طبعا الطريقة دي بطيييييييئه ولكن أحيانا بتكون هي الحل الوحيد للدخول على الإنترنت

ونصيحه ليك كـ IT إهتم دائما بتعريف كارت الفاكس ولو أمكن إنك تكون مجرب dialup connection على الأجهزة المهمة اللي عندك في الشركه واللي بيحتاج عمل مستخدميها الإتصال بالإنترنت (زي الـ Top managers) لإن في حالة الطوارىء (حصل down لخط الإنترنت وشبكة الموبايل واقعه) ممكن ألا يكون أمامك إلا الـ dialup تدخل بيه المستخدم على الإنترنت

لكن خد بالك من معلومه مهمه جدا :

الدايل اب أحيانا ما ينفعش من خط داخل على سنترال , يعني إيه ؟

يعني لو إنت عايز تدخل على الإنترنت دايل اب غالبا مش ح ينفع إنك تسحب خط من الخطوط اللي على سنترال الشركه وأول ما تيجي الحرارة تعمل دايل لإن كارت الفاكس Fax modem مش ح يعرف يتعامل ساعتها مع الخط والحل إنك بتعمل الدايل اب من الخط مباشرة من غير ما يمر على أي سنترال.

الـ ISDN

كان سابق عصره وأوانه لفتره من الزمن وهو إختصار لـ

Integrated Services Digital Network

وبالـ ISDN إبتدينا اللعب مع السلك النحاس

- *يعني إيه ؟*

الفكره قامت على إن الأسلاك النحاس لها قدرة كبيره جدا على نقل البيانات وإن الحزم الخاصة بنقل الصوت لا تستهلك إلا حيزاً ضئيلاً من هذه القدرة فقامت الفكرة على الإستفادة من إمكانيات هذه الأسلاك عن طريق تحويل البيانات من أحادية analog إلى رقمية digital مما يتيح نقل البيانات مثل الإنترنت جنبا إلى جنب مع خدمة الصوت , وده بيتيح لي إني أنقل بيانات بسرعه تصل إلى 128 Kbps لو ح نستخدمها إنترنت فقط أو نقسم الخط إلى قناتين (أو خطين) كل خط بيكون سرعته 64 Kbps تقدر تستخدم كل واحد فيهم على حده للدخول على الإنترنت أو تدخل على الإنترنت من قناة وتخلي القناة الثانيه للإتصالات التليفونيه .

مش مطلوب منك إلا 3 أشياء :

1- تحويل الخط لخاصية ISDN

2- بعد تحويل الخط يتم توصيل جهاز ISDN Modem بالخط و يقوم هذا الجهاز بتقسيم الخط الداخل عليه إلى قناتين و خلاص على كده

3- الإشتراك في الخدمه مع ISP

عن نفسي إشتغلت على الخدمة دي بسرعة 128 وكانت فعلا ممتازه وكان عيبها الرئيسي التكلفه

لكن كان زمان لإن النهارده ظهرت تقنيات تانيه في موضوع الإنترنت وكانت سبب في إن الـ ISDN يفقد بريقه

بالمناسبه دي صورة مودم ال ISDN

الـ DSL

من الطبيعي بعد أن تحدثنا عن ISDN نتحدث عن DSL إختصار لـ

Digital Subscriber Line

وهي المنافس الأحدث للـ ISDN والسبب في إزاحته عن عرش السرعه الذي لم يستمر عليه طويلا وتقوم فكرتها على إستخدام خطوط الهاتف من خلال نقل إشارة البيانات جنبا إلى جنب مع إشارة الهاتف من خلال سنترال خدمة الهاتف الذي يتصل بدوره بخدمة الإنترنت من خلال ISP

وبصفه عامه فان تكنولوجيا الـ DSL تم تطويرها في أكثر من إتجاه وأصبحت لها حلول كثيره جداً جداً وعلشان نريح نفسنا ح نتكلم على 3 فئات فقط وهما اللي ح يساعدونا في اختيار البدائل بعد كده :

ADSL

VDSL

MSDSL

الـ ADSL

هي خدمة قائمة على تكنولوجيا DSL , حرف الـ A فيها إختصار لكلمة Asymmetric ويتم فيها نقل الإشارتين معاً من السنترال و عند العميل يتم تقسيم الخط من خلال splitter يتم توصيله من ناحية بخط الهاتف القادم من السنترال ويخرج لنا من الناحية الأخرى خطين :

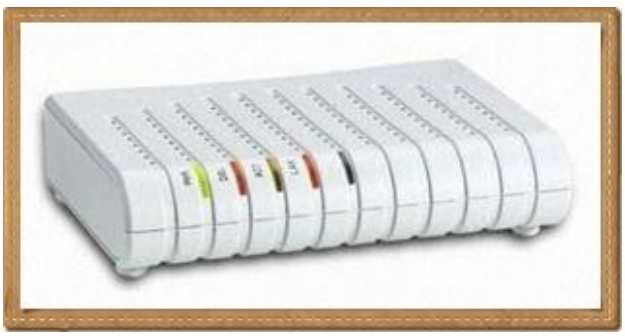
يتم توصيل الأول بالهاتف لإستخدامه في إجراء المكالمات

ويتم توصيل الخط الآخر بـ ADSL router لإستخدامه لتوزيع خدمة الإنترنت

طبعا مافيش حد منا لم يتعامل مع الـ ADSL وفقط أنبه لثلاث نقاط :-

- إن الكونيكشن بتاع ADSL بيكون شيرد Shared وليس Dedicated فما تحلمش إنك تستفيد بكامل السرعة اللي إنت متعاقد عليها
- سرعة الكونيكشن بتكون متقسمه بين الداونلوود والأبلوود بنسبة واحد إلى أربعة , يعني لو إنت واخد سرعة واحد ميجا يبقى سرعة الداونلوود 1 ميجا وسرعة الأبلوود ربع ميجا , لو إنت بتربط شبكة VPN أو مثلا موصل كاميرات مراقبة على الخط بتطلب من الشركة المزودة إنها ترفع لك سرعة الأبلوود وغالبا بيتم الأمر بدون مشاكل
- السرعة اللي بتاخدها من ISP بتكون محسوبة بالبت bit وليست بالبايت Byte بينما أغلب البرامج بتحسب السرعة بالبايت وليس بالبت علشان كده لما تكون واخد سرعة 512 Kb/s وتلاقي الداونلوود سرعته 50 KB/s إعرف إن الإتنين حاجه واحده وإنك مستخدم سرعة الخط بالكامل " لاحظ الفرق بين حرف b وحرف B فالأول يرمز للبت والآخر يرمز للبايت

VDSL



إختصارا لـ Very high bit rate DSL وهو كما يتضح من إسمه خاص بالسرعات العالية

ويسمح لسرعة Download قصوى 52 Mbit/s وسرعة Upload قصوى 16 Mbit/s

MSDSL

إختصاراً لـ Multi rate symmetric DSL وهو يتيح أن يكون الربط One to One و سرعة أبلوود مساوية لسرعة الداونلوود بحد أقصى 2 Mbit/s

أفضل إستخدام للـ MSDSL هو الربط بين شبكتين نظرا للإستغلال الأمثل لكونه وان تو وان .. بالمناسبه أنا اشتغلت بيه من حوالي عشر سنوات كحل ربط وليس لتوصيل خدمة إنترنت ☺

E1

وسيلة جيدة للإتصال بالإنترنت , والجودة ليست مجرد السرعة المرتفعة ولكن كونها Dedicated فهي عبارة عن خط مؤجر بين العميل و مزود الخدمة " إن شئنا الدقة فهي بين العميل و السنترال " وهي ذات سرعات تتراوح بين واحد ونصف إلى اثنين ميجا بت ..

E1 عبارة عن معيار Standard أوروبي يقابله معيار أمريكي T1 ... يعني إيه ؟

يعني لو مزود الخدمة قال لك أنا عندي حل لتوصيل الإنترنت و الحل ده مطايق للمعيار T1 يبقى في نفس الوقت الحل ده تقدر تقول لأصحابك وانت بتترسم عليهم : عندنا في الشركة موصلين الإنترنت بخط E1 ☺

أتمنى أن تكون فكرة : يعني إيه معيار وصلت لكم

لا نستطيع بصفة عامة أن نتحدث عن حدود قصوى نهائية لسرعات التوصيل , بمعنى أن الحد الأقصى للسرعات يتغير بتطور التكنولوجيا وبالتالي فإنه لايوجد حد أقصى نهائي

GPRS

إختصار لـ General Packet Radio Services وهي تكنولوجيا تتعلق بنقل الباكيت من خلال شبكة الموبايل . من خلالها تستطيع دخول الإنترنت من خلال الموبايل وكذلك إرسال وإستقبال رسائل المالتيميدا

سرعتها كحد أقصى 115 كيلو بت ... عندينا في العالم الثالث السرعة مش ح تزيد عن 40 كيلو ... يعني باختصار ما تنفش في حاجه

عموما الـ GPRS يطلق عليها الجيل إتنين ونص 2.5 G

EDGE

إختصار لـ Enhanced Data for Global Evolution وهي تكنولوجيا نقل بيانات من خلال شبكة الموبايل .

سرعتها كحد أقصى 473 كيلو بت ... ولكنها في المتوسط لا تبلغ إلا 135 كيلو

يطلق عليها الجيل ثلاثة إلا ربع ☺ 2.75 G

3G

الجيل الثالث ...لا يطلق المصطلح على تكنولوجيا محددة بل يعبر عن أكثر من تكنولوجيا تضمن توصيل البيانات وتبادلها بسرعات عالية

يعني باختصار 3G مش معيار محدد ولكن هناك عدة معايير تندرج تحته . مثل :

UMTS المستخدم في أوروبا واليابان و CDMA2000 بتاع أمريكا وكوريا

HSPA

إختصار لـ High Speed Packet Access وهي الجيل التالي أو الترقية لشبكات UMTS وتصل فيها سرعة الداونلوود الى 7.2 Mbps وهي المستخدمة في خدمات الإنترنت عبر الموبايل حاليا في أغلب دول العالم

تنقسم الـ HSPA إلى قسمين :

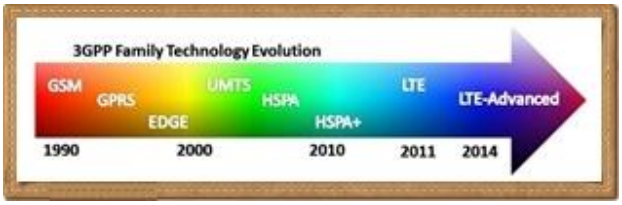
HSDPA وهي الخاصة بالـ Downlink

HSUPA وهي الخاصة بالـ Uplink

علشان كده لما تلاقي إعلان بيتكلم عن HSDPA ما تستغربش

LTE

ياناس يا عسل الجيل الرابع وصل



Long Term Evolution وهو بإختصار الجيل الرابع " في ناس بيعتبروه الجيل قبل الرابع "

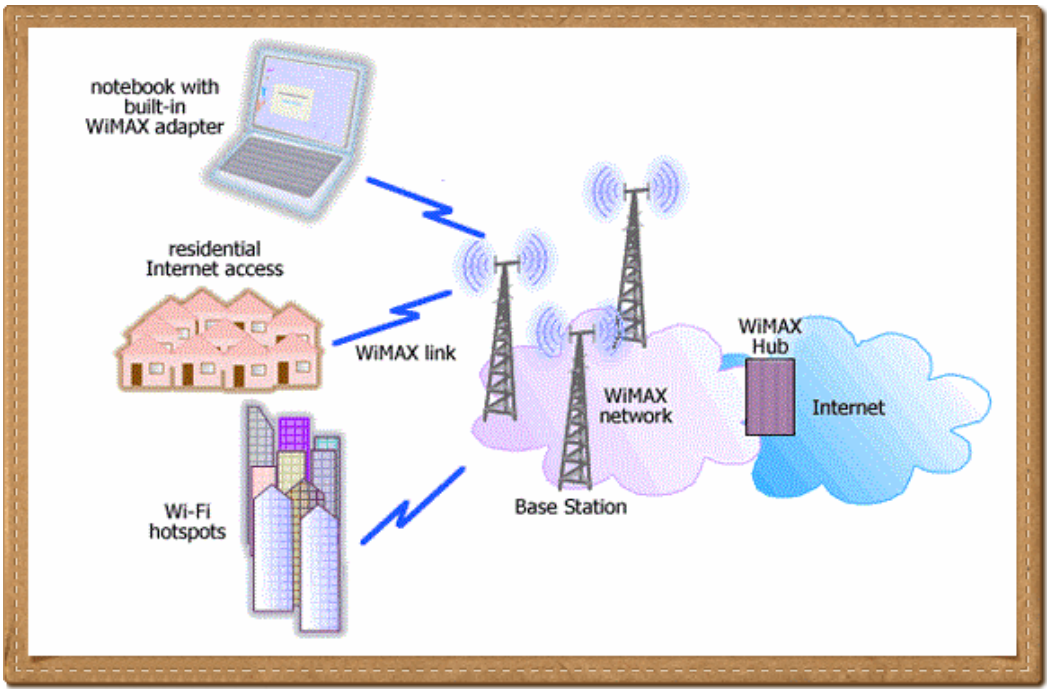
السرعة بتوصل في الداونلوود 300 ميجا .. أيوه 300 ميجا

مصطلح LTE ح تلاحظوه في الفترة القادمة على أجهزة الموبايل و مودمات الإنترنت

المعيار يطبق حاليا بالفعل و الخدمات أصبحت تقدمها شركات عالمية مثل Verizon و AT&T

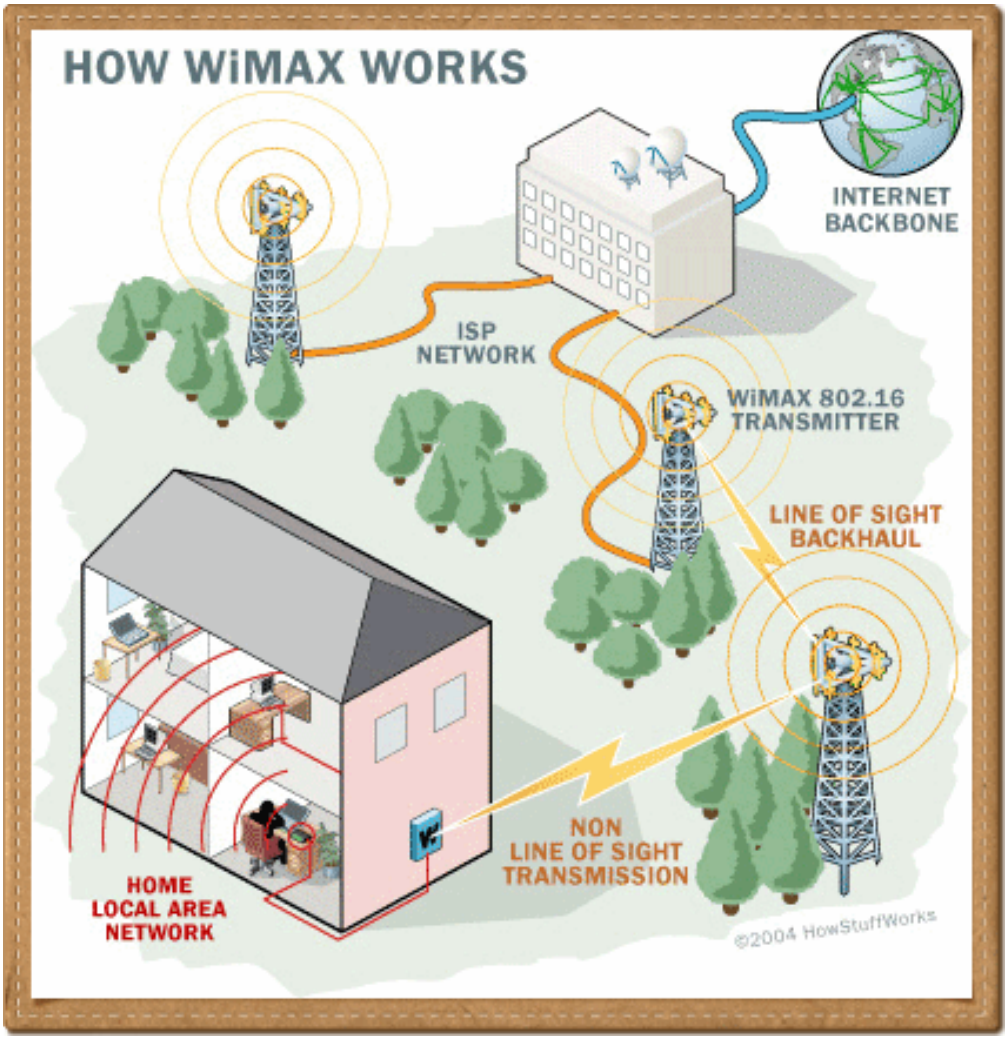
WiMax

الواي ماكس هو التطور الطبيعي للحاجة الساقعه .. قصدي التطور الطبيعي للواي فاي



الواي ماكس بيصل لسرعة 1 جيجا بت وهو جزء من نظام الجيل الرابع ..

تغطيته بتصل حتى 50 كيلومتر علشان كده شركات الإتصالات إعتمدت على WiMax في نقل الداتا في الجيل الرابع علشان تساعد إنها تستغل التكلفة المنخفضة وفي نفس الوقت تقدر تصل بالسرعة إلى واحد جيجا بت



Internet Satellite

الإنترنت عن طريق الستالايت ...

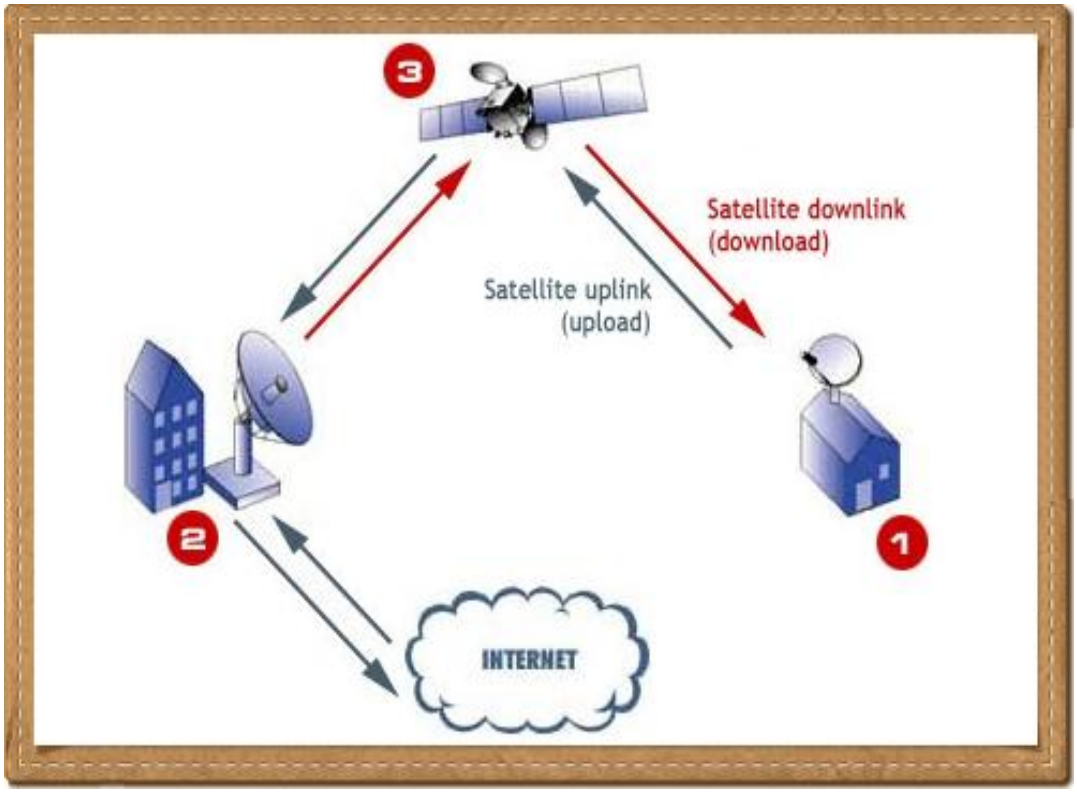
بهدوء ومن غير توتر .. الإنترنت كونكشن بيكون عبارة عن اتجاهين Upload و Download تمام كده ؟

الفكرة باختصار إن الكونيكشن بيتم من خلال الستاليت .. يعني حزمة البيانات بيتم إرسالها من القمر الصناعي إلى ريسيفر عند العميل ومن الريسيفر بيتم تحويل البيانات إلى أجهزة العميل

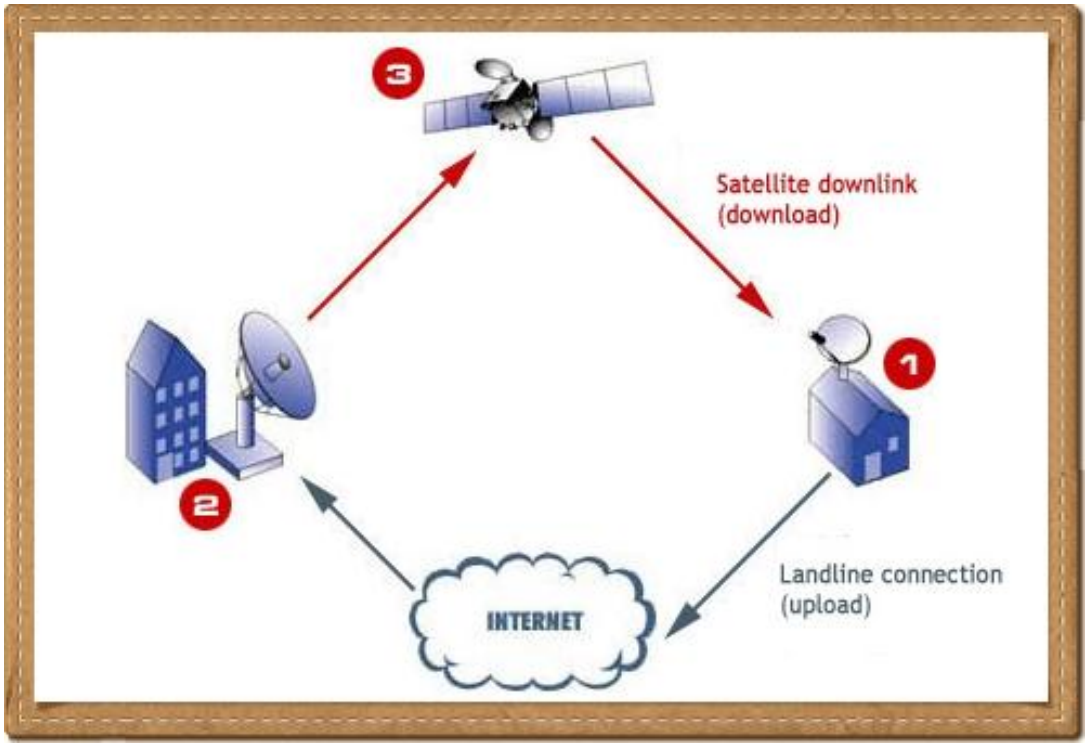
ده بالنسبة للداونلوود

أما بالنسبة للأبلوود فهناك طريقتين :

أن يتم الأبلوود أيضا عن طريق الستالايت أي يكون الإتصال 2 way



أن يتم الأبلوود عن طريق آخر كإستخدام Dialup Connection أو GPRS



الإنترنت من خلال الستالايت أحيانا بيكون هو الحل الوحيد المتاح أمامك

فمثلا لو الموقع في الصحراء بدون أي تغطية أو في منصة بترول في محيط حينها سيكون الحل الوحيد هو إنترنت الستالايت 2 Way Connection

من الممكن أن تكون شركتك في منطقة لا يوجد بها خدمة إنترنت إلا بسرعة محدودة "مثلا Dialup" ويحتاج العمل لسرعة إنترنت عالية حينها سيكون الحل أن تخصص الدايل اب للأبلوود ويكون الداونلوود من خلال الستالايت

الخلاصة :

- كل ما سبق من معلومات الغرض منها كسر الحاجز فقط بينك وبين المعلومة
- بتقدم التكنولوجيا ستظهر أنواع ومصطلحات جديدة وتنقرض أخرى
- تقدم الشركات حلول متعددة قد تتكون من أكثر من نظام أو معيار .. وقد تكون عبارة عن تكنولوجيا مستحدثه ... أو معيار موجود بالفعل ولكن أدخل عليه تطوير معين أو تعديل معين

فقد تجد مثلا عرض فني يصلك لحل باسم IMM .. تقعد تدور على IMM ماتلاقيهاش ولا حتى في طبق اليوم

مش عايزك ترتبك أو تنبهر

لو دققت في العرض ح تعرف حقيقة الحل إيه من غير الماكياج ولو مش موجودة في العرض ممكن تجيب مندوب الشركة وماتسيبوش إلا لما تعرف الحقيقة وإيه المعيار أو التكنولوجيا

وساعتها قد تفاجأ بأن IMM اختصار لكلمة Internet Metwaly Ma7asalsh

متولي ده ممكن يكون إسم الشركة أو إسم صاحب الشركة أو المندوب اللي جاب لك العرض

نيجي للمهم : إنت IT في شركة ومطلوب منك تدخل الإنترنت في الشركة لازم ساعتها قبل أخذ القرار تجيب على أسئلة مثل :

- ماهي التكلفة التي ستتحملها سواء قيمة معدات أو مصاريف شهرية أو سنوية
- مامدى احتياجك لخدمات الإنترنت من حيث السرعة أو جودة الخدمة والـ Uptime
- حالة البنية الأساسية سواء في شركتك أو السنترال الحكومي أو الكابلات وصناديق التوصيل وما هي الخدمات الممكن تشغيلها من خلال هذه البنية

إجابتك على الأسئلة دي بتساعدك في إتخاذ القرار المناسب أو عرض الصورة بأمانة على متخذ القرار

أحيانا نقع في خطأ شائع في مجال الأي تي وهو : إختيار الحل الأعلى تكلفة أو جودة

- *إختيار الحل الأعلى تكلفة أو جودة خطأ ؟*

أيوه خطأ

- *فهمني !!!*

تخيل إنك عايز تأجر عربية تنقل بيها بضاعه وزنها ثلاث أطنان ... ووجدت في السوق عربيتان واحده حمولة أربعة أطنان والأخرى عشرة أطنان ح تأجر أي واحده منهم ؟؟

- *مش محتاجه فكاكه ولا ذكاء خارق لإنك بديهي ح تختار العربية ذات الحمولة أربعة أطنان*

طيب لو قلتلك ان العربية ذات الحمولة الأكبر أعلى في التكلفة هل ح تغير قرارك ؟

- *قشطه يا مان ... طيب بالنسبة للجوده ؟*

الجوده لا يفترض بها أن تكون في أعلى درجاتها ولكن يجب أن تكون :

- مناسبة لإحتياجات
- لا تقل عن القيمة المدفوعة

يعني مش شرط إني أحصل على أعلى جوده إذا لم أكن محتاج لها أو لم أدفع مقابلها ولكن الشرط أن أحصل على الجودة التي أريدها والتي تعادل ما دفعته

فإذا ذهبت لشراء موبايل من نوعية رخيصة فلا يصح أن تطالب البائع بأن تكون جودته مماثلة لأفخم الأنواع ولكن في المقابل فإنه من غير المقبول أن يعطيك البائع جهاز لا يعمل أو مكسور ويتعلل بإنخفاض السعر

أتمنى أن تكون الصورة قد وضحت قليلا وتكون عرفت الإنترنت :

ح تجيبه من مين

ونوعه ح يكون ايه

وح يكلفك كام

وهنا يظهر السؤال الرابع : جبنا الانترنت , ح نوزعه ونديره ونتحكم فيه إزاي ؟

اللهم إني أعوذ بك أن أشرك بك شيء أعلمه

وأستغفرك لما لا أعلمه

والله المستعان

سبحانك اللهم وبحمدك , أشهد ألا إله إلا أنت , أستغفرك وأتوب اليك

الفصل الثاني : قبل ماتتورط في القضية

قبل ماتتورط في القضية

—

الحمد لله والصلاة والسلام على رسول الله

نبدأ بسم الله العليم البصير في شرح توزيع الإنترنت وكيف سيتم وبدائله

في الفصل السابق إطلعنا على بدائل خدمة الإنترنت ونعتبر نفسنا وصلنا الخدمة حتى دخل الشركة والآن سنتناول كيفية توزيع هذه الخدمة على المستخدمين

وعلشان نبدأ في توزيع الخدمة ونختار البديل الصح لازم نتعرف على أهم مصطلحين بيقابلونا أثناء تعاملنا في توزيع الإنترنت

البروكسي Proxy

الجيت واي Gateway

الفايروول Firewall

يو تي إم UTM

و باختصار

وكمان لازم نعرف الكتاب ح يتناول إيه وماهي النقاط العامة التي يجب أن نتفق عليها

البروكسي سيرفر Proxy Server

البروكسي يطلق على جهاز سيرفر يقوم بمهام متعلقة بخدمة الإنترنت مثل :

- توزيع طلبات المستخدمين من المواقع المطلوب زيارتها وإعادة توزيعها إلى الجهات المطلوبة
- إتاحة التخفي للمستخدم بحيث يتم تضليل المتلصصين وإيهامهم أن المستخدم يقوم بزيارة مواقع وهمية غير المواقع الفعلية
- زيادة سرعة التصفح من خلال تحويل طلبات الزيارة عن طريق سيرفرات ذات إمكانيات أعلى
- فلترة محتويات التصفح
- التلصص على المواقع التي يتم زيارتها و معرفة سلوك المستخدمين

وظائف البروكسي كثيرة جدا و لا مجال هنا لحصرها ولكن فقط ننبه لإن :

- البروكسي قد يكون خارج الشركة أو داخلها
- قد يكون حكوميا أو مناهضا للحكومة
- قد يكون عدوا وقد يكون صديقا

نراجع معلومة بسيطة : السيرفر يقصد به جهاز خادم يخدم الشبكة من خلال قيامه بتقديم خدمة Service معينة مثل توزيع الإنترنت أو إدارة الطباعة أو حفظ الملفات أو إدارة الأكتيف دايركتوري

ولا يشترط أن يكون السيرفر جهاز كمبيوتر بمواصفات عاليه جدا ولكن يجب أن تكون المواصفات محققة لإحتياجات الخدمة

كما لا يفترض أن يكون متخصصا لخدمه معينه بمفردها بل من الممكن أن يكون نفس الجهاز مخصصا لتقديم خدمتين أو أكثر معا بالطبع شريطة عدم التعارض بين الخدمات المقدمه فمثلا يمكن تقديم خدمة مشاركة الطباعة sharing printer و الحفظ الإحتياطي backup على نفس الجهاز حينها سيكون هذا الجهاز برينت سيرفر وباك اب سيرفر

الجيت واي Gateway

هما كلمتين : الجيت واي سيرفر Gateway Server يقوم بجزء من وظائف البروكسي مثل إتاحة الولوج إلى مواقع الإنترنت

وهنا يظهر مصطلح آخر وهو Default Gateway وهو الأيبي الذي يستخدمه جهاز المستخدم للوصول إلى الإنترنت وهو بالطبع رقم سيرفر جيتواي وبروكسي يتم من خلاله تحويل الطلبات من المستخدم إلى الإنترنت وكده ☺

الفايروول Firewall

كلنا عارفينه ولكن ما يمنعش إننا نقول إنه بمثابة حائط قوي ذكي يمنع الأشرار اللى في الخارج إنهم يؤذوا الطيبين اللى في الداخل

ذكي لإنه ما بيمنعش مرور الترافيك تماماً ولكنه يتحكم فيه ويحدد الصالح من الطالح والمرغوب من الممنوع فيسمح للصالح ويمنع الطالح

يو تي إم UTM

هو الكلام اللي فوق ده مع بعض , يعني بإختصار مع زيادة التهديدات اللي بتتعرض لها الشبكة ظهرت حاجه لحل يجمع كل وسائل الحماية الممكنة مثل :

فايروول

أنتي فايروس

Antimalware

Intrusion Detect

وتم إطلاق إسم Unified Threat Management **وإختصاره** UTM

الموضوع به جزء تجاري كالعادة وبالتدريج ستجد أن مصطلح UTM **سينتشر ويبقى موضة ومطلوب في كل الشركات وإستثمارات جديده والبيزنس يمشي**

عموما اللي عايز تفاصيل أكثر عن الـ UTM **ممكن تزوروا الموقع الخفيف ده**

unifiedthreatmanagement.com

عن نفسي لا أهتم بالمصطلحات مادامت لا تقدم معيارا ملموساً فما يهمني هو وجود معيار محدد لتطبيقة ورفع كفاءة العمل فعليا

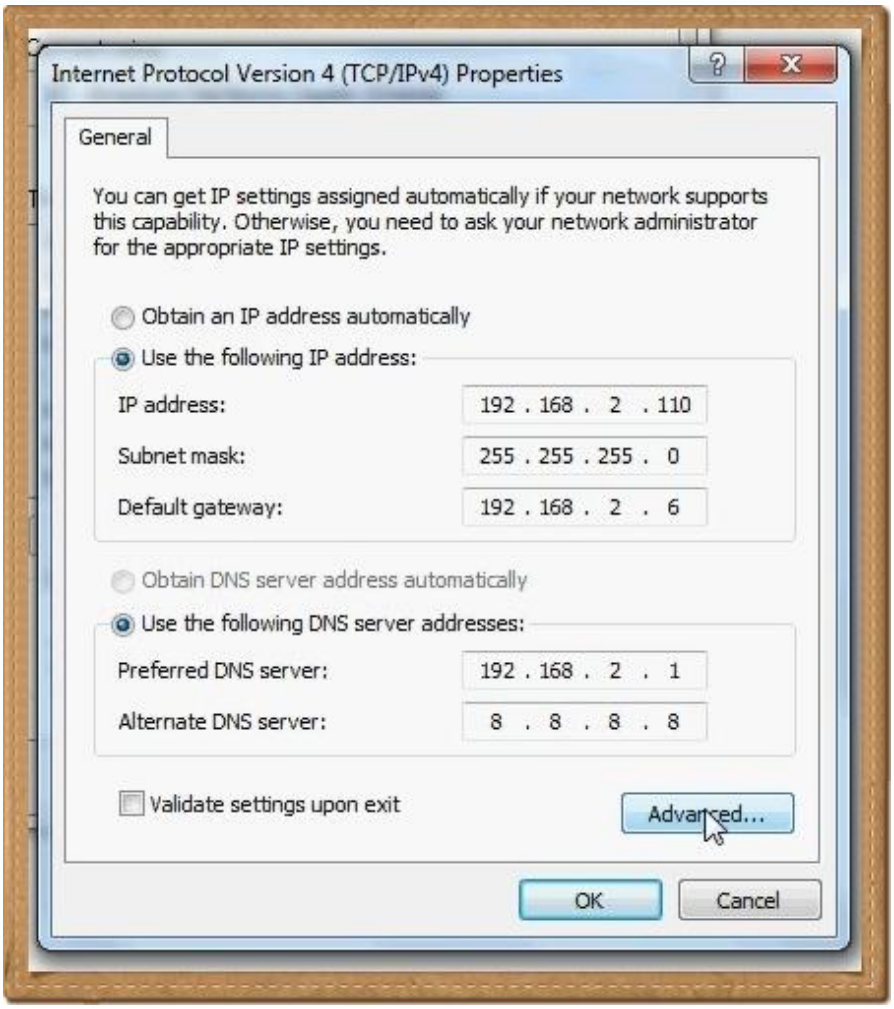
إعدادات عامة

ركزوا معايا الله يهديني ويهديكم

في النهايات السابقة كنا إذا ما أعددنا أرقام الأيبي لأي كلاينت فإننا كنا نضع IP الـ Domain Controller كـ Default Gateway لإننا باختصار لم نتطرق إلى خدمة الإنترنت

كما كنا نضع IP الـ Domain Controller كـ DNS Server وحيد وذلك أيضا لإننا لم نتطرق إلى خدمة الإنترنت

ولكن الآن يمكننا التعمق قليلاً في هذه الجزئية :



IP Address أي بي الجهاز وهو بالطبع لا تغيير فيه عما درسناه

Subnet Mask سب نت ماسك الشبكة وأيضا لا تغيير فيه

Default Gateway رقم سيرفر توزيع الإنترنت أو راوتر الإنترنت

Preferred DNS Server الدي إن إس الخاص بالشبكة المحلية

Alternative DNS Server الدي إن إس الخاص بخدمة الإنترنت وهو ما يتم الحصول عليه من موزع الخدمة أو يمكن إستخدام أرقام International مثل رقم الدي إن إس الخاص بجوجول وهو

8.8.8.8

8.8.4.4

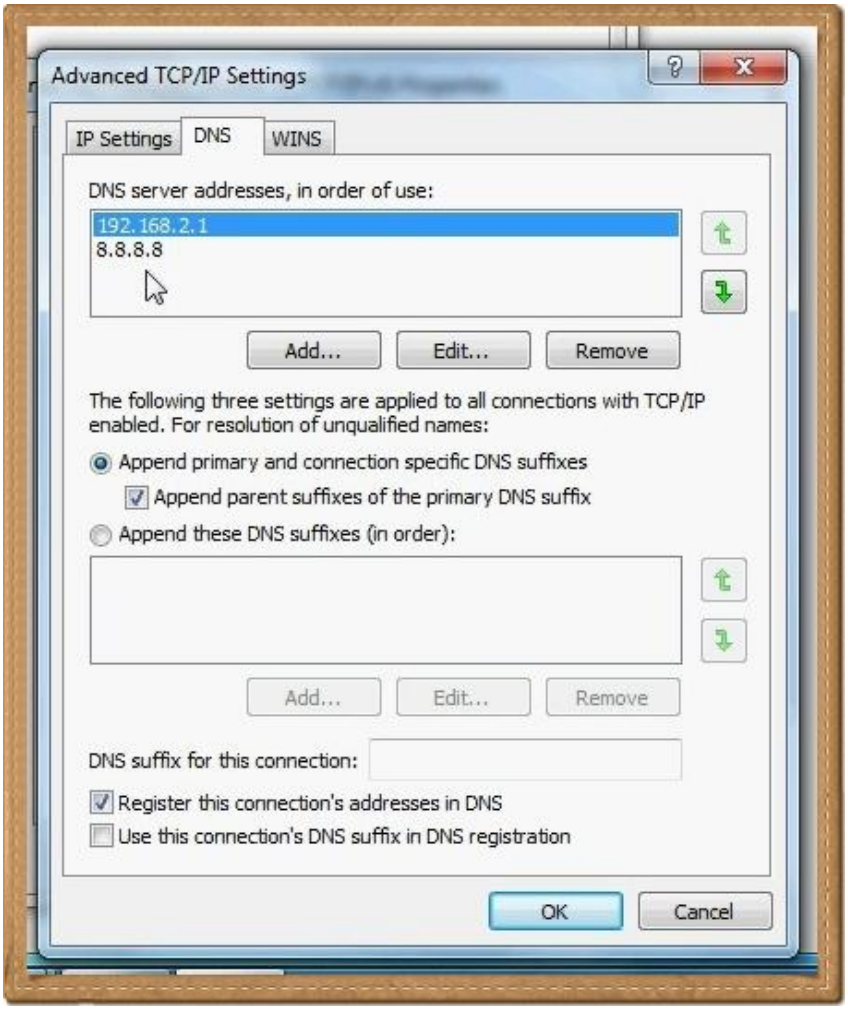
أو رقم الدي إن إس الخاص بمواقع متخصصة في الخدمة مثل Open DNS وسيخصص له فصل خاص لشرح مثل هذه الخدمة إن شاء الله

وممكن أيضا أن تضع اي بي الراوتر أو الفايروول كـ DNS

طيب سؤال بسيط : لو عندك أكثر من جيت واي أو دي إن إس تعمل إيه ؟

بالضغط على زر advanced

يمكن إضافة المزيد



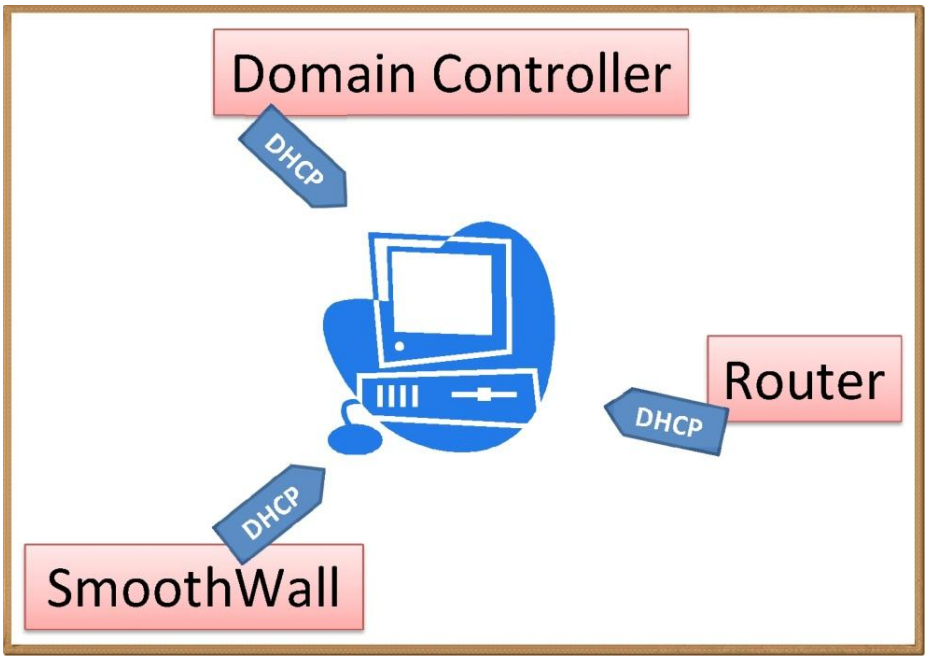
طبعا مش شرط إننا ندخل الأيبيهات للكلاينتس يدوي .. بل من الممكن أن يتم هذا من خلال الـ DHCP من تخصيص الـ Scope الخاصة به لتتوافق مع متطلباتنا السابقه

فوضى الـ DHCP

حذار من فوضى الـ DHCP Servers فقد يتسبب عدم إنتباهك وحذرك لمشاكل كثيرة فمثلا قد تكون شبكتك بها أكثر من سيرفر للفايروول ورغم هذا فنسيانك لخاصية الت DHCP في الراوتر تكون سبباً في قدرة الكلاينت على سحب اي بي من هذا الراوتر والخروج على الإنترنت بدون قيود

طبعا هذا يطلب توافر شروط مثل أن يكون الجهاز معدا ليسحب الـ اي بي أوتوماتيك ويكون الوصول للراوتر متاحا لوجوده معه في نفس الشبكة

الـ DHCP Server كوظيفة كما قلنا يمكننا تفعيلها من أي جهاز



وبالتالي فإذا لم ننتبه نتحدث فوضى عارمة

ماذا سندرس

في الفصول القادمة سنتعامل مع أكثر من بروكسي سيرفر أو جيت واي سيرفر ☺ أو فايروول

فسنبدأ بـ TMG و إدارته من خلال GFI

Windows	Linux
TMG	
GFI	
CCProxy	
AnalogX Proxy	
Kerio Control	
	SmoothWall
	Untangle

ولن نكتفي بهذا بل سنلقي نظرة على سيرفرات وبرامج بديله تعمل Under Windows مثل

CCProxy

AnalogX Proxy

مع ملاحظة أن السيرفرات البديلة البسيطه مثل CCProxy و AnalogX Proxy مسكينة لا تسيطر على الجهاز الذي تعمل عليه ولكنها ضعيفة ☺

- *يعني إيه مسكينة أومسيطرة ؟*

ده تقسيم أنا عملته وأقصد به نوعين :

النوع الأول المسيطر :

وهي السيرفرات التي تسيطر على الجهاز الذي تعمل عليه مثل الأيزا والتي إم جي و سيرفرات الينكس مثل SmoothWall و IPCop و مايكروتيك

وبسبب هذه السيطره يتعذر تخصيص الجهاز ليؤدي وظيفة كسيرفر آخر .. يعني لو حضرتك منزل مثلا TMG أو SmoothWall على جهاز فسيصبح هذا الجهاز بروكسي سيرفر فقط وإنسى إنك تستفيد منه كسيرفر آخر

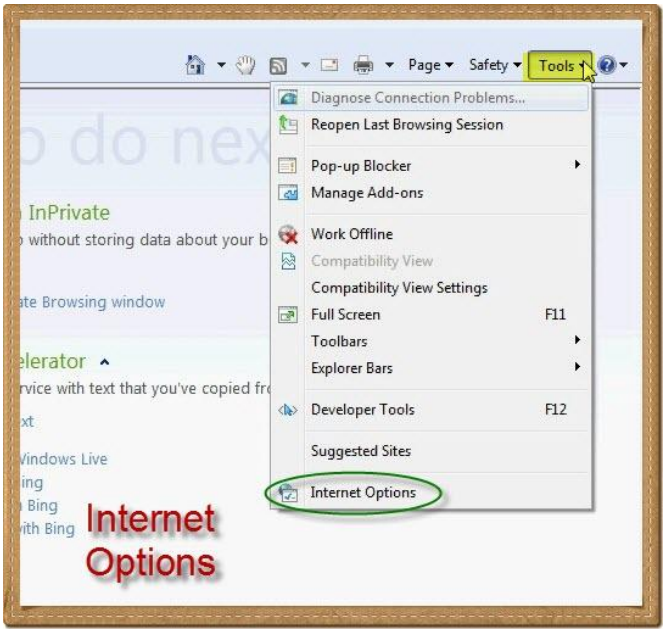
وهنا يتم إستخدام IP السيرفر كديفولت جيت واي للكلاينت كما شرحنا في الصور السابقة

النوع الثاني المسكين :

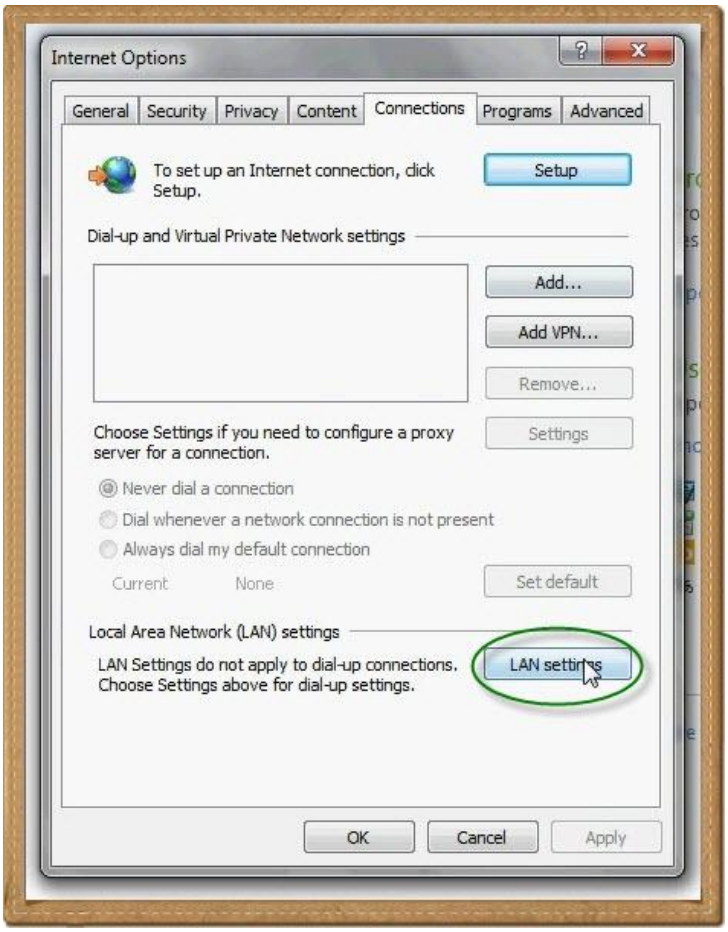
وهي البرامج التي تقوم بوظائف البروكسي وإن كانت أقل في الإمكانيات كما إنها لا تسيطر على الجهاز الذي تعمل من خلاله , بل يمكن أن يتم إعداد برنامج البروكسي على جهازك الخاص مثلا و تعمل عليه بدون أي مشاكل وممكن أيضا أن تجعل هذا الجهاز يؤدي وظائف أخرى مكتبيه أو كسيرفر طباعة مثلا

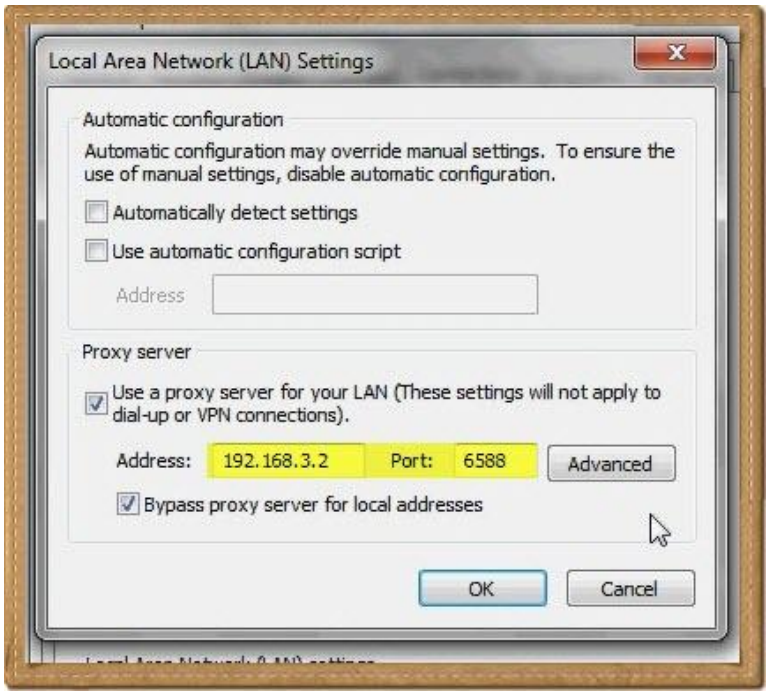
في هذه الحالة قد لا تصلح معك طريقة الـ Default gateway وحدها بل سترجع للزمن سنوات و يتم إعداد الكلاينت للدخول على الإنترنت من خلال إعدادات الإنترنت Internet Options و هي كالتالي :

في الإنترنت إكسبلورر من Tools نختار Internet Options



من Connections تاب نختار Lan settings





رقم الـ اي بي الخاص بالبروكسي سيرفر و البورت هو المنفذ الخاص ببرنامج البروكسي الضعيف والذي سنتعرف عليه في حينه

بعد الإنتهاء من المساكين سنتعامل مع سيرفر محترم جدا إسمه Kerio Control وبيعمل كل حاجات الـ UTM وهو يتميز بشيء عجيب جدا فهو ويندوز ولينكس مع بعض

وبعده ح ناخد سيرفر لينكس صريح وسيكون إن شاء الله SmoothWall

وكمان سيرفر لينكس تاني Untangle

وأخيرا وبعد السيرفرات سنجرب العمل مع Open DNS ثم أهم أداتين للتصفح الآمن وهما حزمة Tor للبروكسي والتشفير وماسنجر Pidgin لإجراء المحادثات المشفرة

بالنسبة للسورسات والبرامج المختصر فكما أعتدت معكم لن أضع روابط أو كراكات , في المقابل فأعتقد أنكم لن تجدوا صعوبة تذكر في معرفة مواقع هذه المنتجات والحصول عليها

الهاردوير المطلوب

طبعا ح نحتاج يكون الجهاز فيه كارتين شبكة ولكن بالنسبة للهاردوير وأعني هنا البروسيسور والرام فإحتياجاتنا كالجدول التالي :

	Processor	Memory
TMG	1.86 GHz Dual Core	2 GB
GFI	1.86 GHz	1 GB
Kerio Windows	1 GHz	1 GB
Kerio Linux	500 MHz	1 GB
SmoothWall	200 MHz	128 MB
Untangle	800 MHz	128 MB

مع ملاحظة :

- هذه المواصفات هي الحد الأدنى المطلوبة بمعرفة الشركات المطورة
- الرام والهارد ديسك أهم حاجة بالنسبة لأي سيرفر خاص بالإنترنت وبصفة عامة فيجب ألا يقل الهارد عن 8 جيجا والرامات عن 4 جيجا بالنسبة للويندوز و 1 جيجا للينكس لضمان أداء جيد
- بالنسبة للمساكين كأمثال CCProxy ماعندهمش مشكله فأي أمكانيات ح تشغل الويندوز ح تشغلهم

اللهم إني أعوذ بك أن أشرك بك شيء أعلمه

وأستغفرك لما لا أعلمه

والله المستعان

سبحانك اللهم وبحمدك , أشهد ألا إله إلا أنت , أستغفرك وأتوب اليك

الفصل الثالث : تي إم جي TMG

التنصيب

أول مرة

ريموت كونترول

خُد فكرة

TMG

التنصيب

الحمد لله والصلاة والسلام على رسول الله

مع أشهر برامج توزيع الإنترنت وأغلاها طبعا TMG من مايكروسوفت

وهو إختصار لـ :

Threat Management Gateway

التطور الطبيعي للأيزا ISA Server و من قبلهم Microsoft Proxy Server

هو جزء من حزمة منتجات تتعلق بالسيكيوريتي تحت إسم Forefront منها :

Forefront Endpoint Protection

Forefront Online Protection for Exchange

Forefront Protection for Exchange Server

Forefront Protection for SharePoint

Forefront Threat Management Gateway

وطبعا مش وقت تقطيع في فروة مايكروسوفت ☺

ولكن فقط ننبه إنك لن تجد صعوبة في الإنتقال من ISA إلى TMG

وأيضا أطمئنك فلن تجد صعوبة في العمل مع TMG إذا لم تكن لك خبرات سابقة مع الـ ISA

- ***السؤال المهم : من أين سنحصل على نسخة TMG لنعمل عليها ؟***

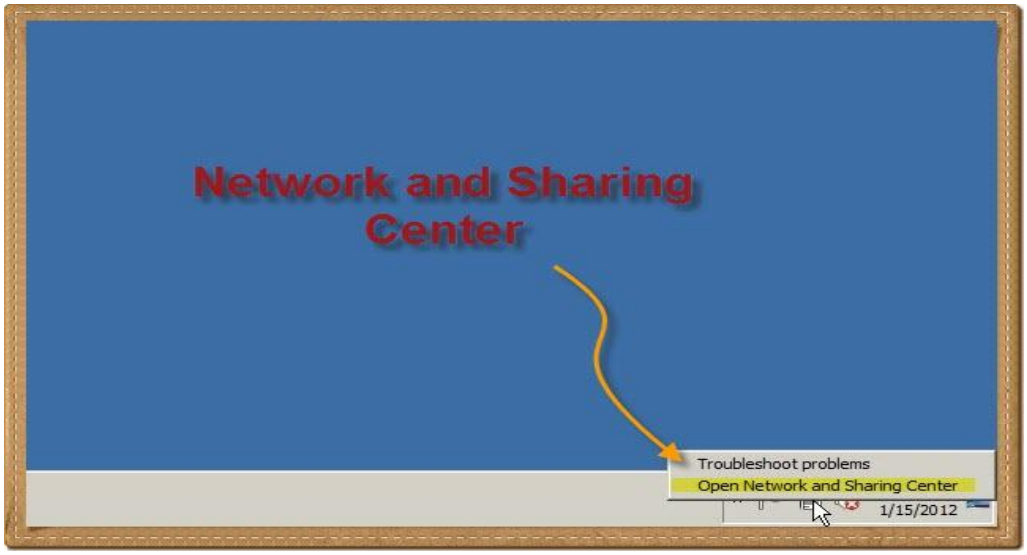
من موقع مايكروسوفت ذات نفسه

أيووووون من موقع مايكروسوفت ح تنزل نسخة تجريبية صالحة لعدة أشهر وبعد مافترة التجربة تخلص تاخد قرار الشراء أو تغير الويندوز وتنزل نسخة تجريبية من جديد ☺ وماتقولش لحد إني نصحتك بكده .

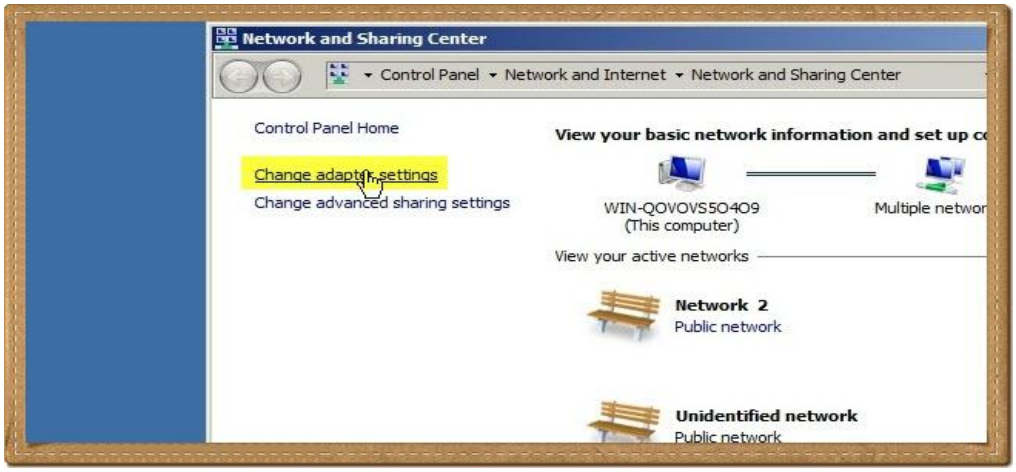
نتوكل على الله

نبدأ في إعداد الجهاز المخصص ليكون TMG Server وهو لازم يكون Server 2008

كليك يمين على أيقونة الشبكة ونختار Network and Sharing Center



ثم نختار Change adapters settings



يجب أن يتوافر في سيرفر التي إم جي حاجتين :

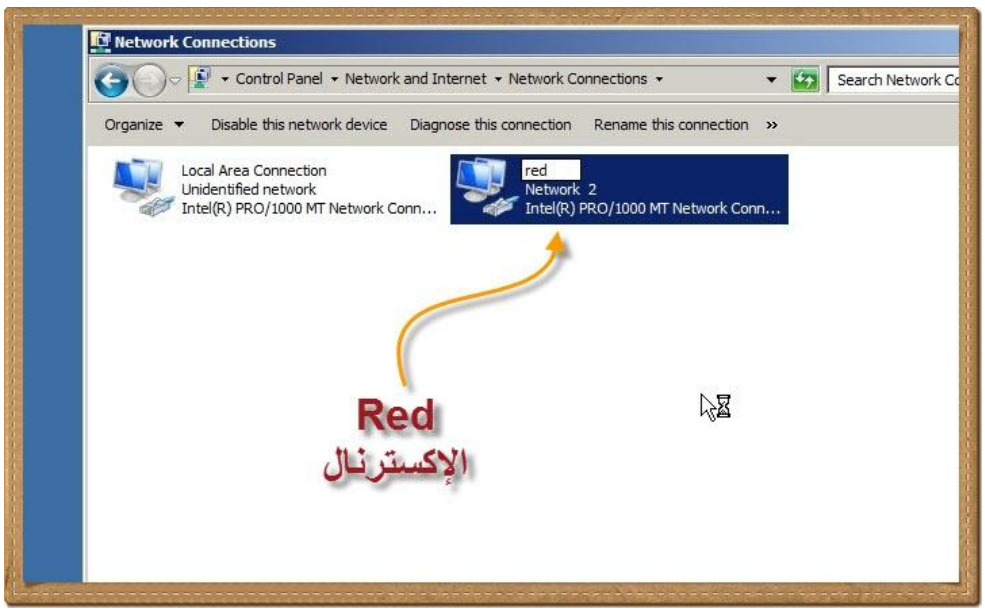
- ألا يكون عضواً في الدومين

يعني لازم يكون Stand alone وحذار من أن تجعله member of domain

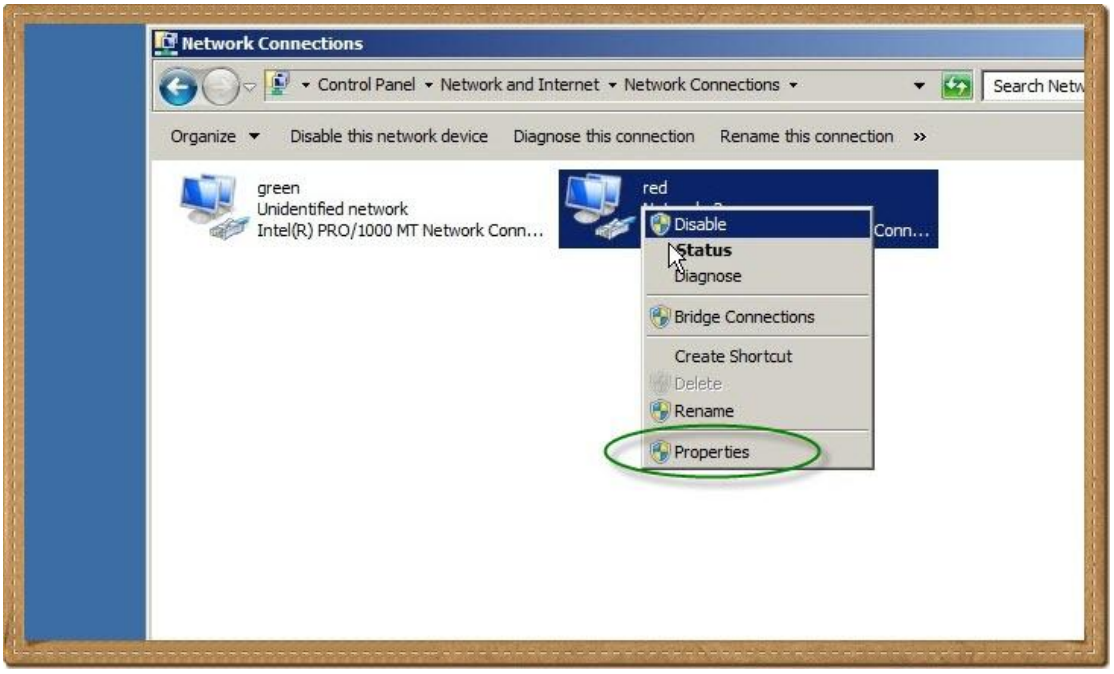
- أن يكون به كرتين شبكه أحدهما متصل بالإنترنت و الآخر خاص بالشبكة الداخلية

كليك يمين على كارت الشبكة المتصل بالإنترنت لعمل Rename

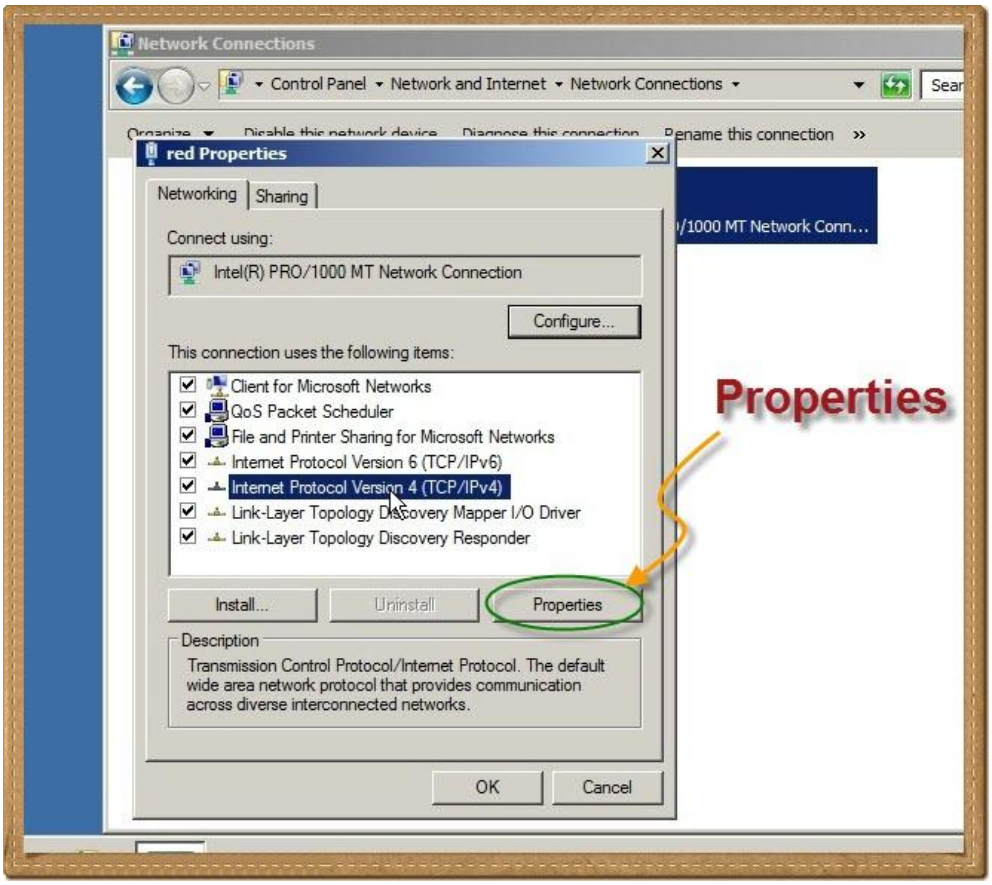
نجعل إسمه Red حتى نتذكر دائما أنه هو المتصل بالإنترنت , طبعا ممكن نترك الإسم كما هو وممكن نختار تسمية أخرى مثلا External



ثم كليك يمين أخرى ونختار Properties

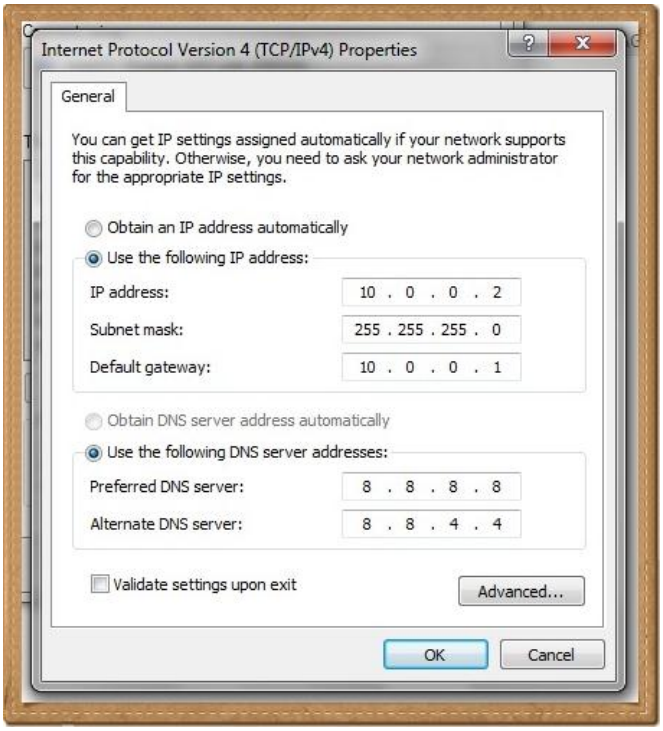


ونبدأ في تعديل الـ اي بي IP V4

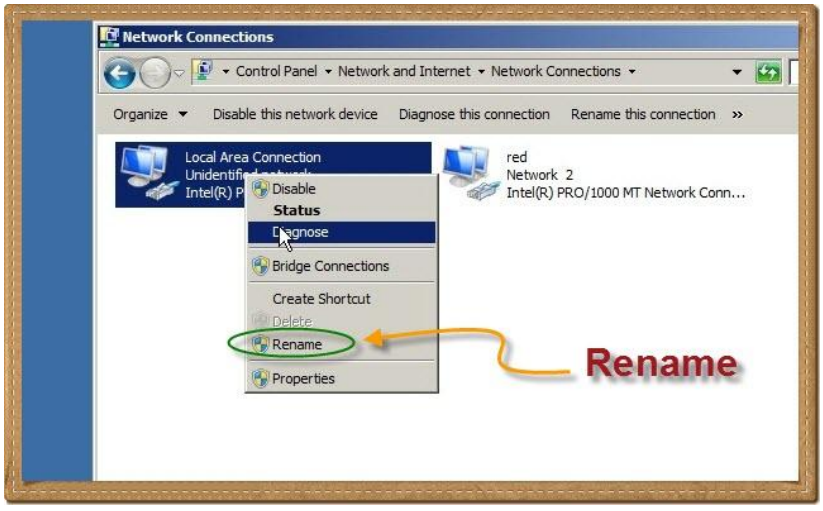


الكارت Red المتصل بالإنترنت وبالتالي سنجعل الـ Default gateway هو اي بي الراوتر و الدي إن إس إخترت أن أستخدم Google DNS

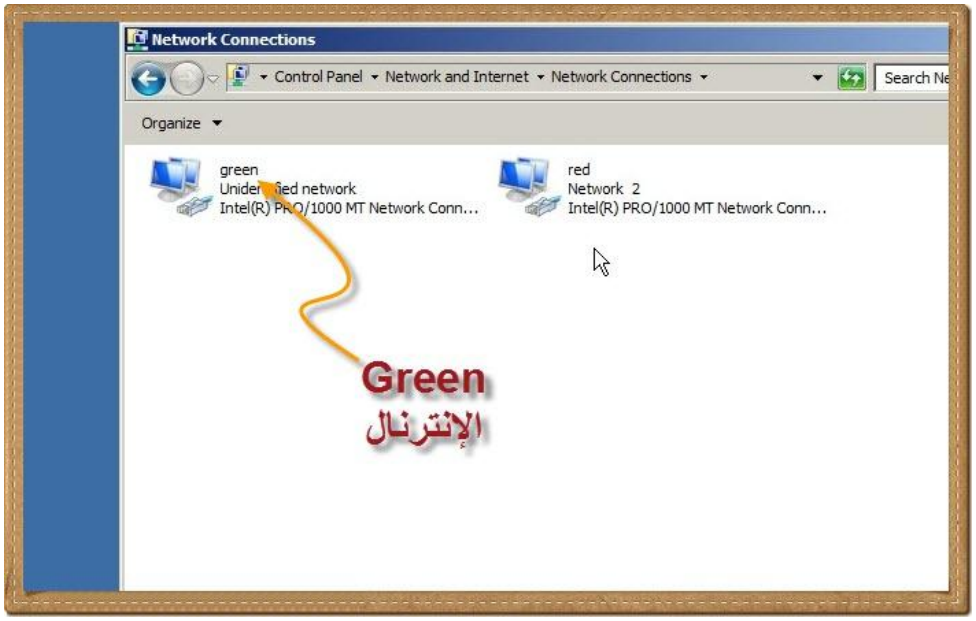
هذا الإعداد بناء على خدمة الإنترنت لديك فلو لديك Real IP خاص من مزود الخدمة سيتم إستخدامه حينها أيضا سيزودك الـ ISP بأرقام جيت واي و دي إن إس خاصة به



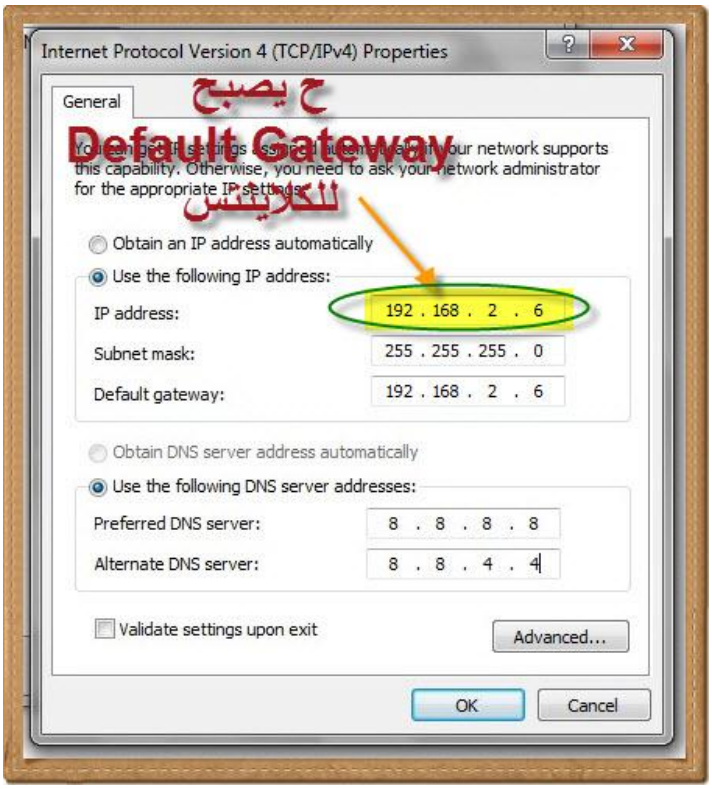
والآن نعيد تسمية الكارت الآخر ليصبح Green والمقصود به الكارت المتصل بالشبكة الداخلية والمسئول عن توزيع الخدمة لأجهزة الشبكة



Green أو Internal أو ماتغيروش لكن خد بالك علشان ماتتلخبطش



ثم تغيير الاي بي ليصبح من نفس نطاق الشبكة الخاصة بك



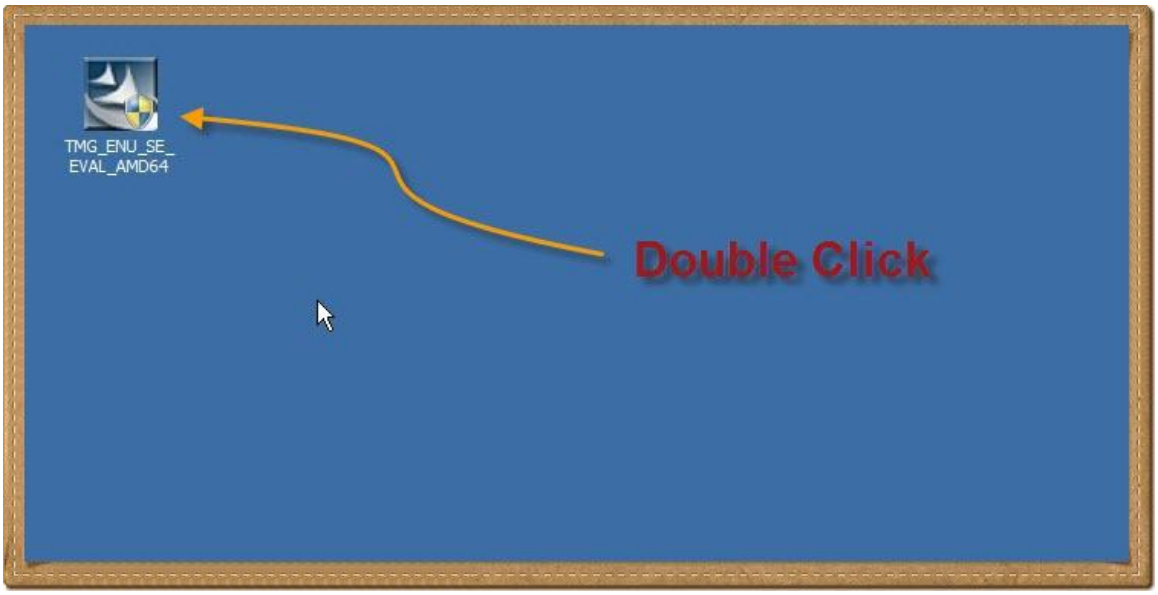
ملاحظة : ماتركزش قوي في الـ DNS أو الـ Gateway الخاص بكارت Green ☺ لإن مالهمش لازمه

نجرب الإنترنت على الجهاز علشان نتأكد

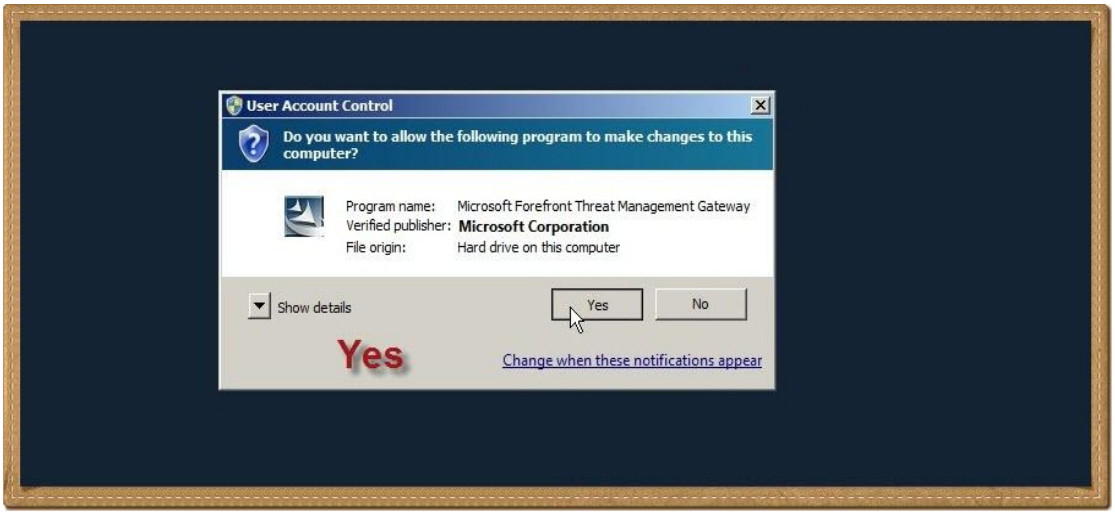
ولو حصلت مشكلة لاقدر الله نبقى عارفين الخطأ ممكن يكون في أي مرحلة

كده إحنا جاهزين وبسم الله نبدأ في الـ Installation

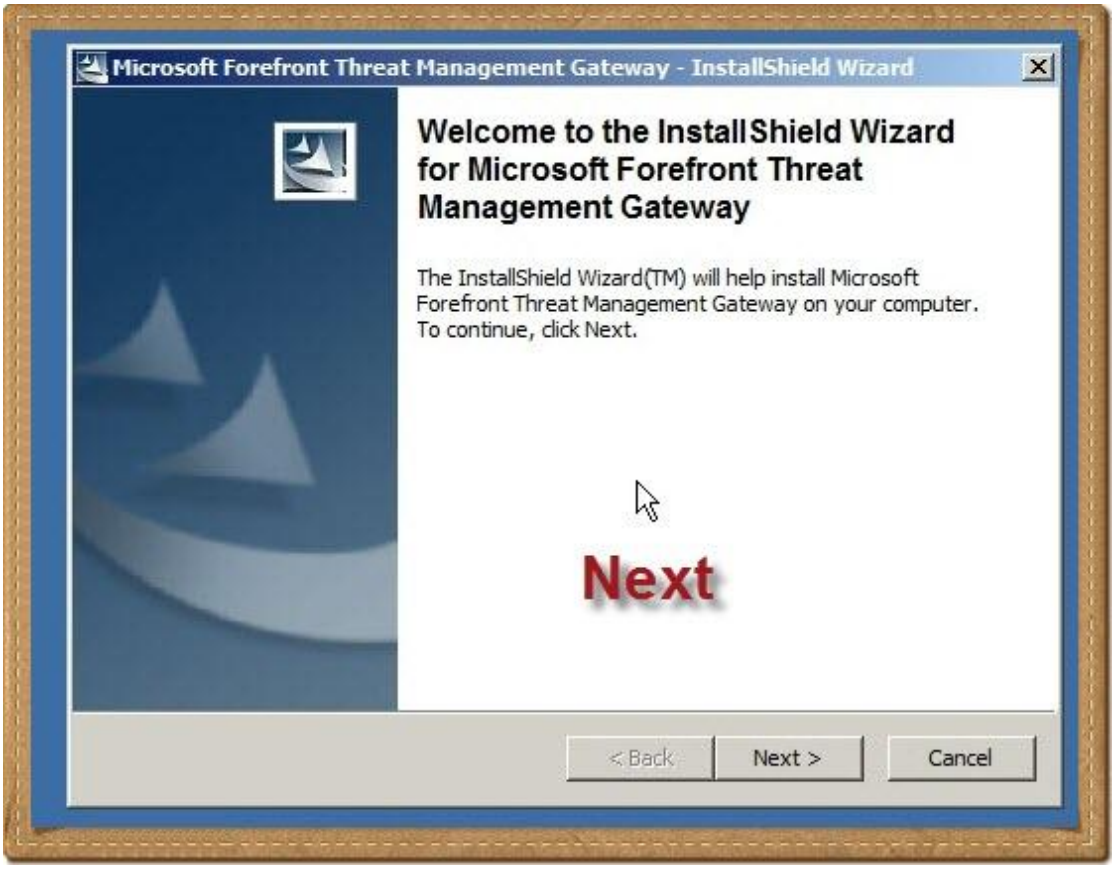
دابل كليك على ملف الـ TMG



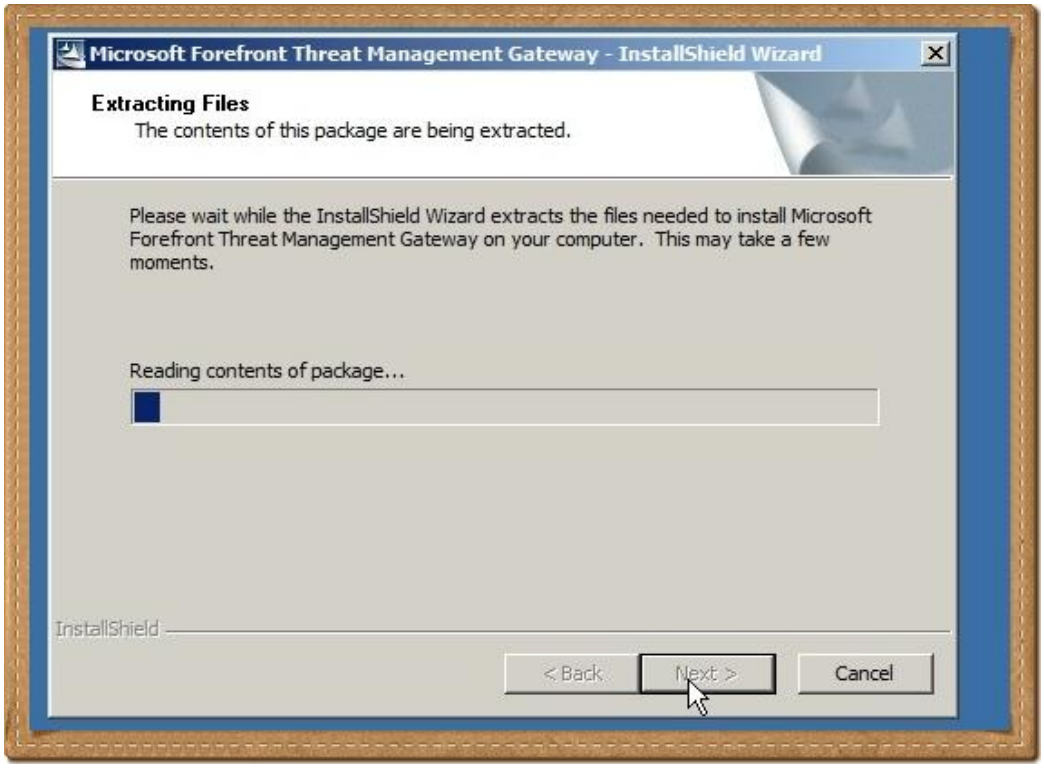
الموافقه على الإعداد



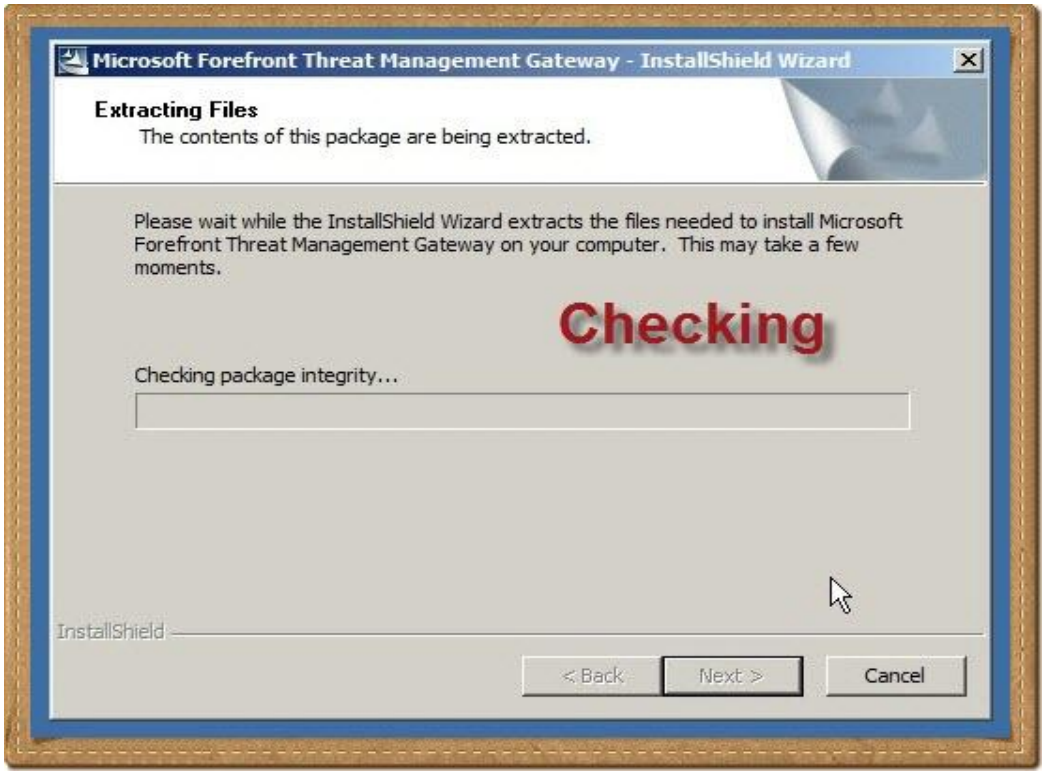
تبدأ المرحلة الأولى من الإعداد بعمل extract للملفات



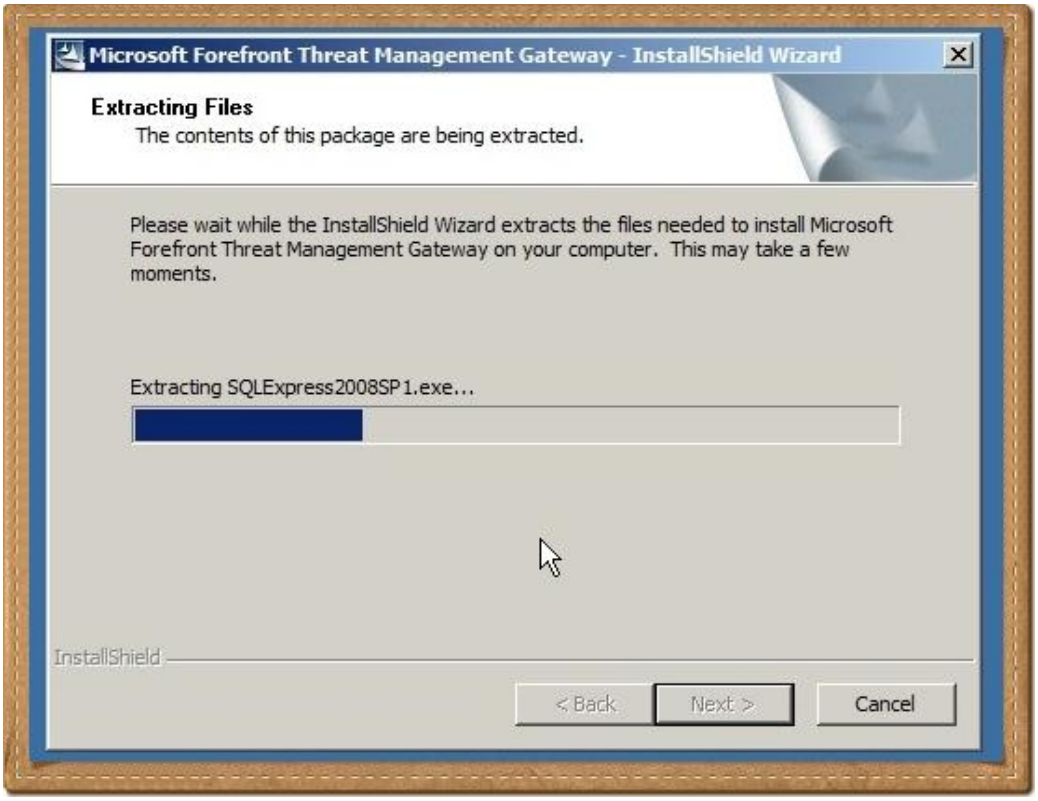
Reading

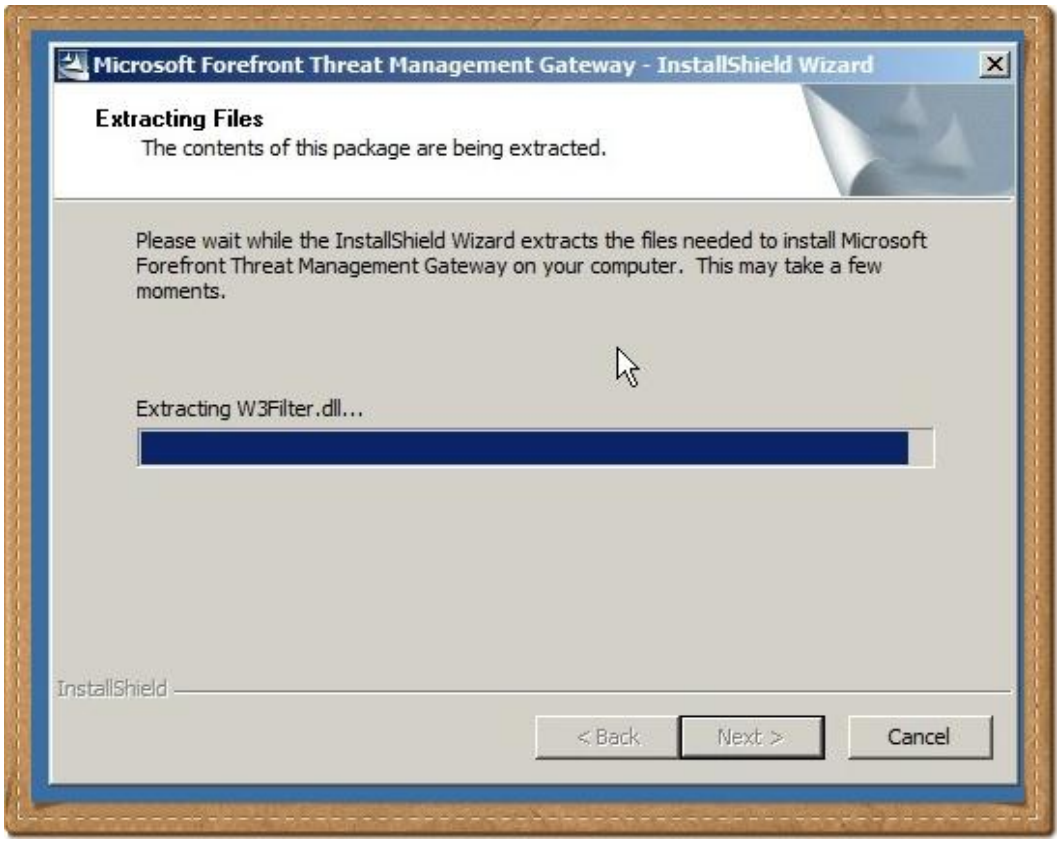


Checking

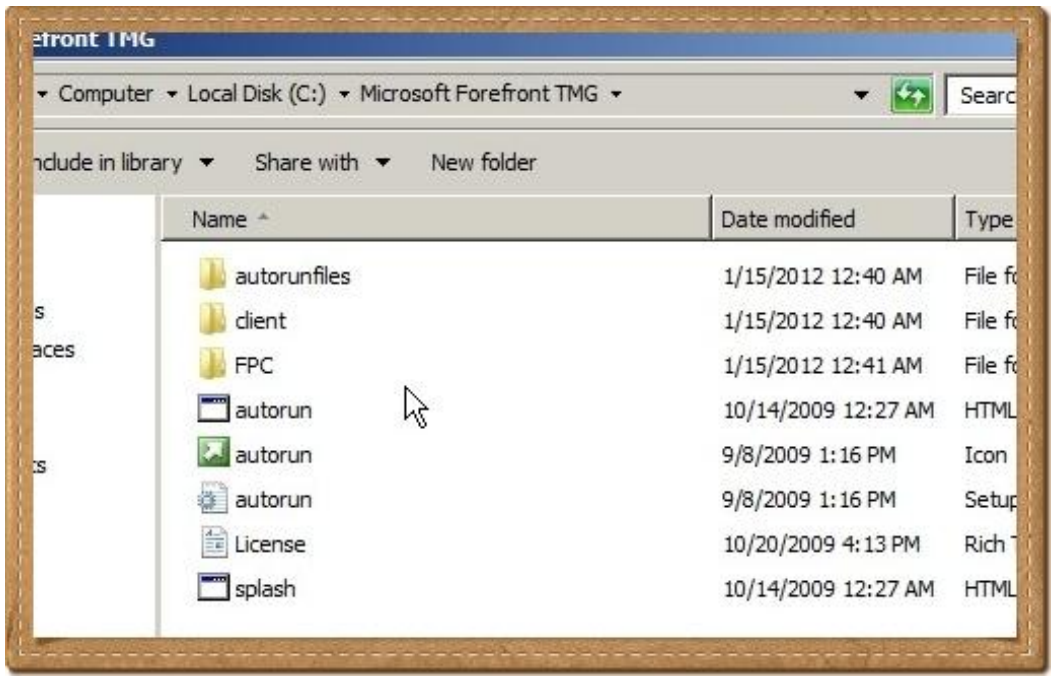


ومعانا ثلاثه Extracting





وبعد ما بيخلص تنتهي المرحلة الأولى من التنصيب وسنجد الملفات موجوده على المسار التالي



ويزارد الإعداد ح يبدأ توماتيكي توماتيكي

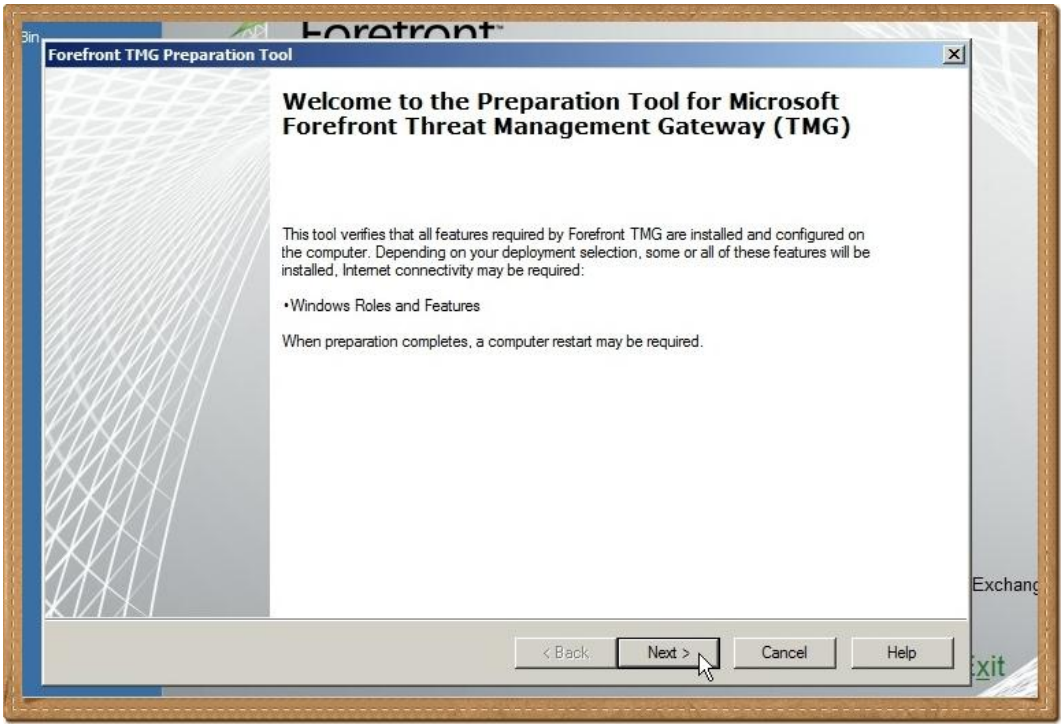
ولكن لو لم يبدأ ف دابل كليك على autorun

من ضمن الأشياء الجميلة جدا في معالج الإعداد Wizard هو الـ Preparation Tool

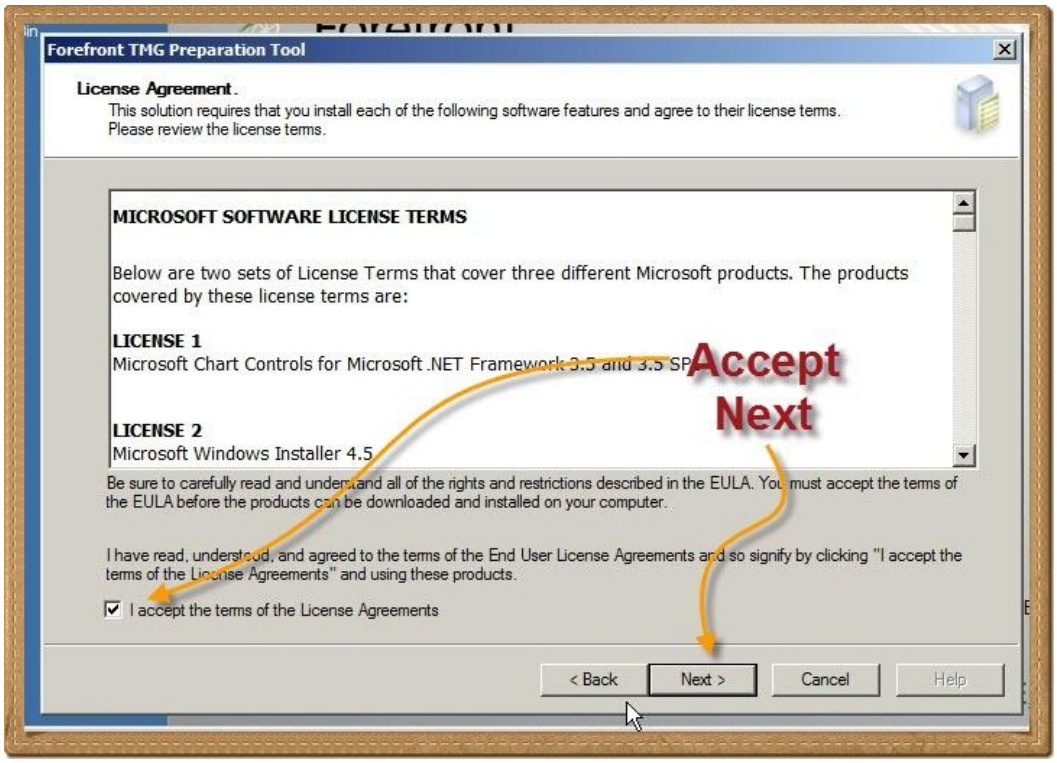
وهو بإختصار معالج يقوم بفحص متطلبات الـ TMG وفي حالة عدم تواجد أي من هذه المتطلبات يقوم بتنصيبها على الجهاز

نختار Run Preparation Tool

ثم Next



نقبل الإتفاقية و Next



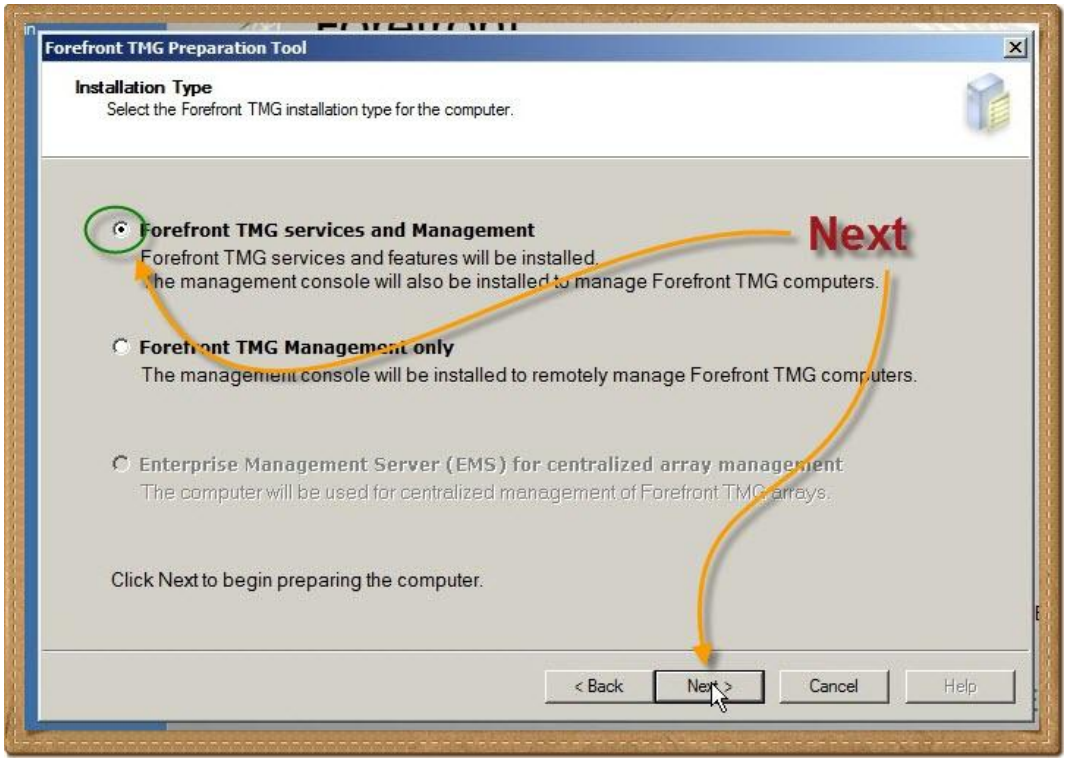
أمام إختيارين :

- تي إم جي بالكامل بالعيش بالسلطات من خلال تنزيل البرنامج وواجهة التحكم وهذا الخيار الخاص بسيرفر TMG
- واجهة إدارة TMG فقط وهو الخيار الذي سنستخدمه لإتاحة إدارة TMG Server ريموتلي من جهاز آخر

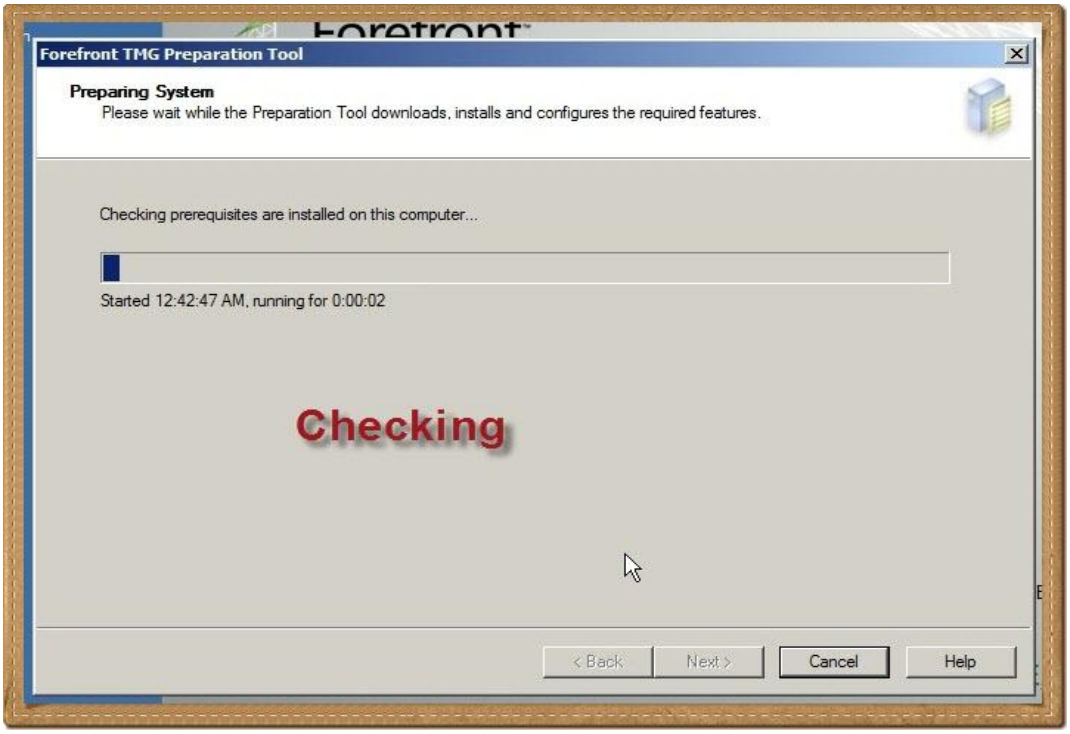
طبعا في حالتنا هذه سيكون خيارنا رقم 1

وإذا أردنا فيما بعد إدارة السيرفر من جهاز أخر سنقوم بإختيار رقم 2 عن الإعداد على الجهاز الآخر

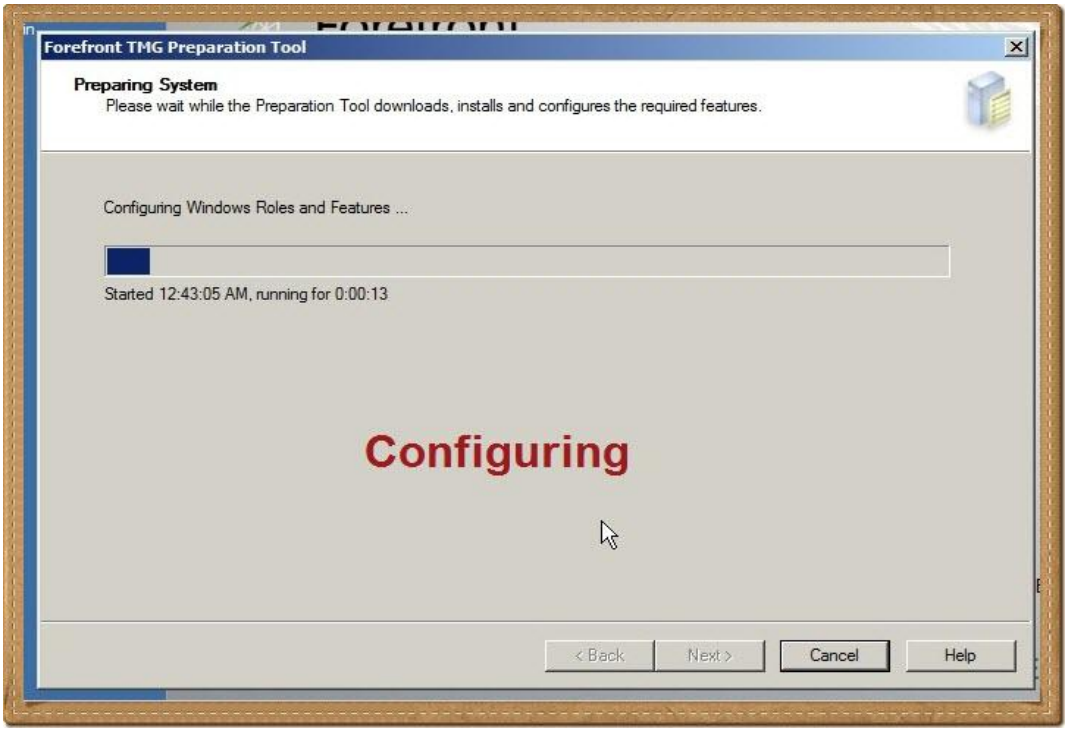
نختار الخيار الأول و Next



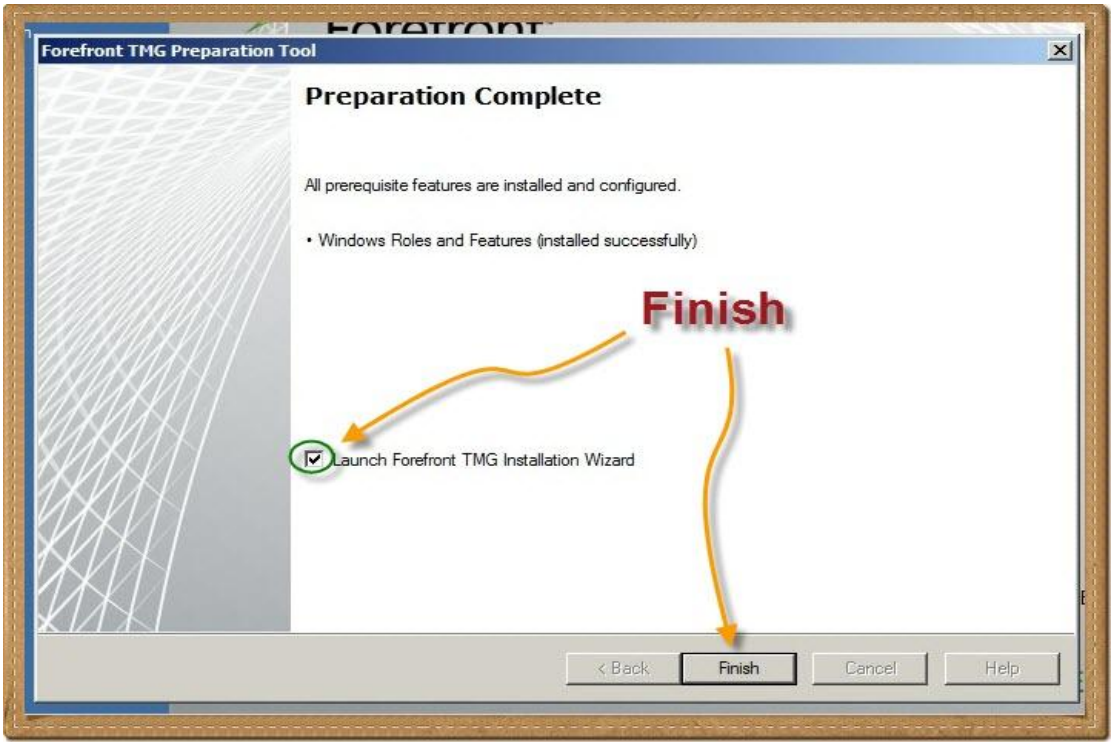
يبدأ في الفحص



والتظبيط والتربيط

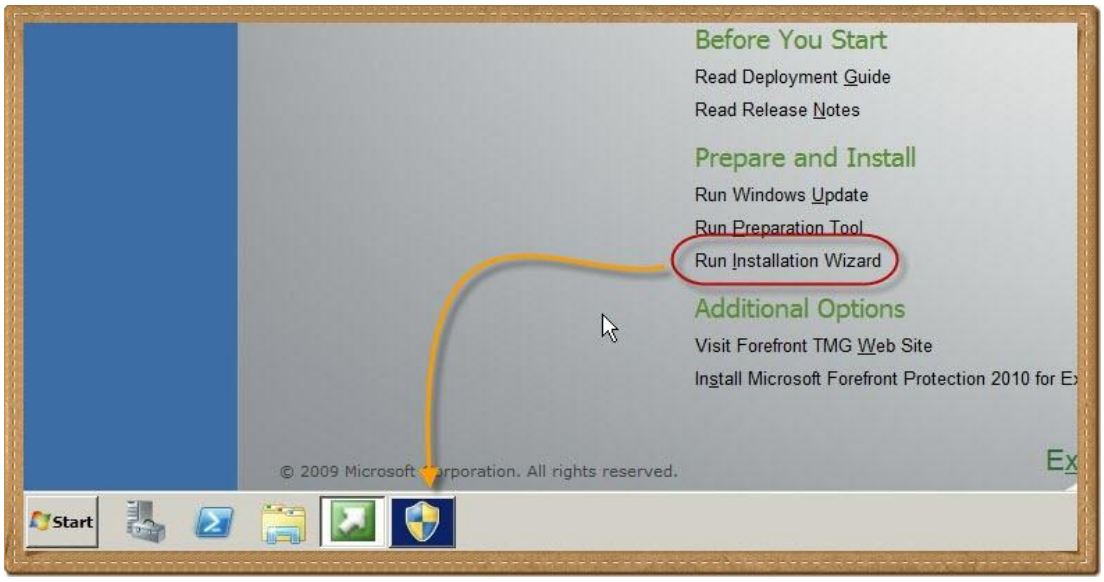


و Finish ليبدأ معالج إعداد TMG كمرحلة ثالثة ونهائية



المرحلة الثالثة وهي الإعداد بجد ستبدأ توماتيكي توماتيكي

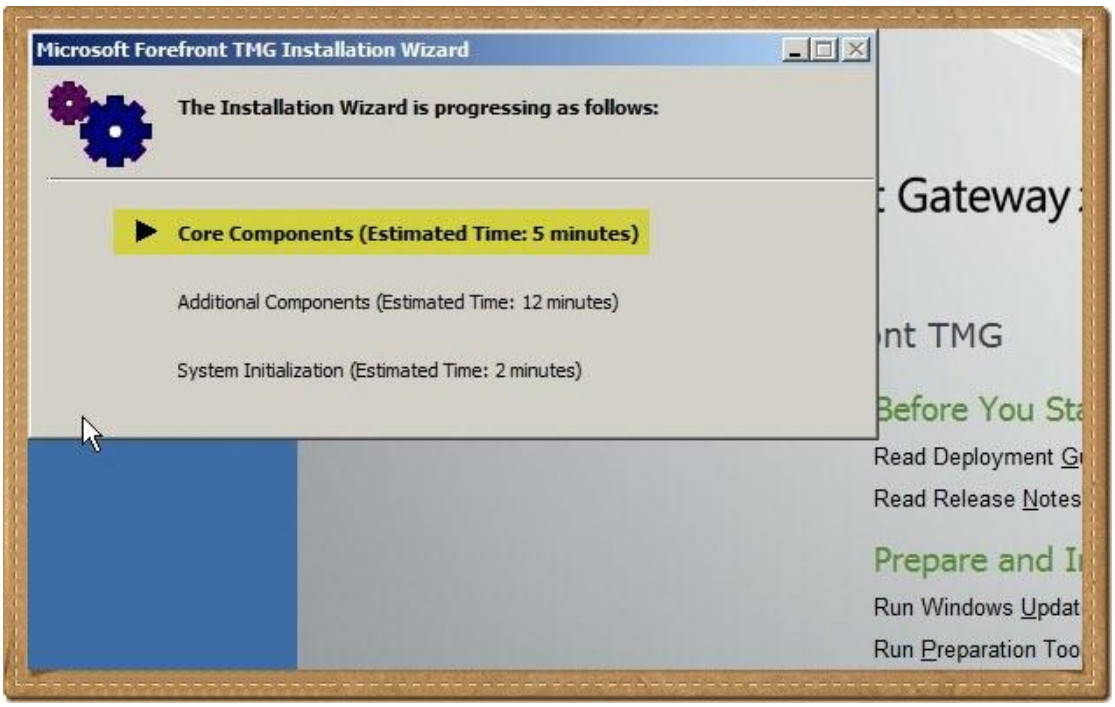
وإن لم تبدأ ولم تكن مستخبيه كما في الصور فيمكنك ببساطه إختيار Run Installation Wizard



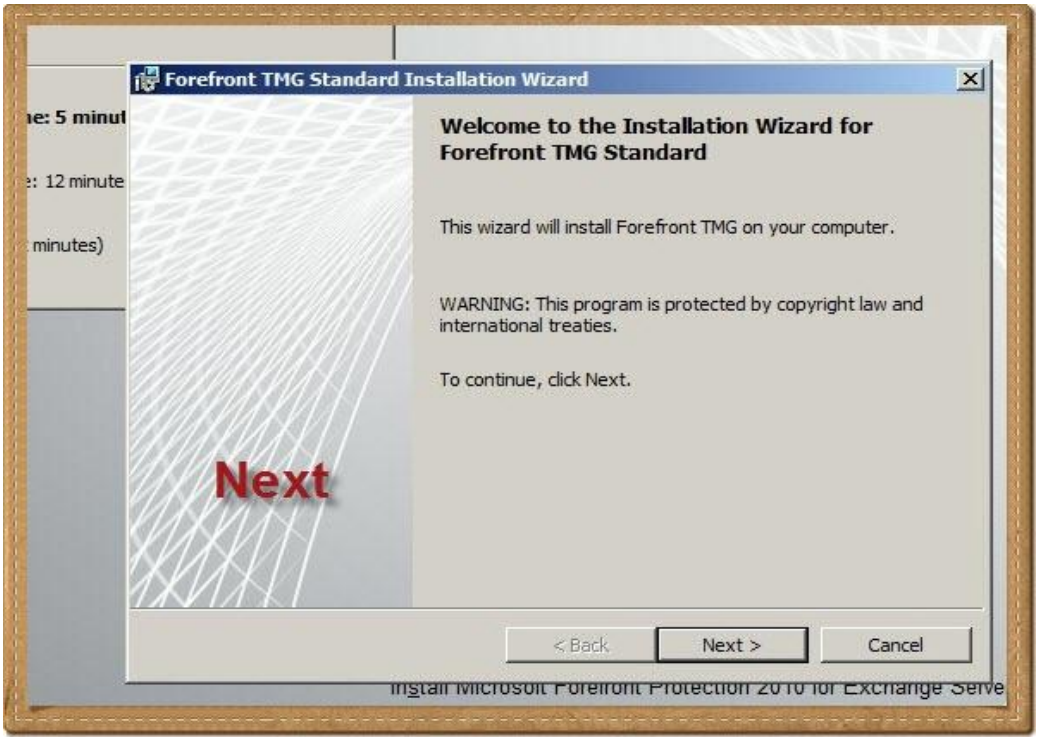
Yes

ويبدأ الجزءالأول من المرحلة الثالثه من الإعداد

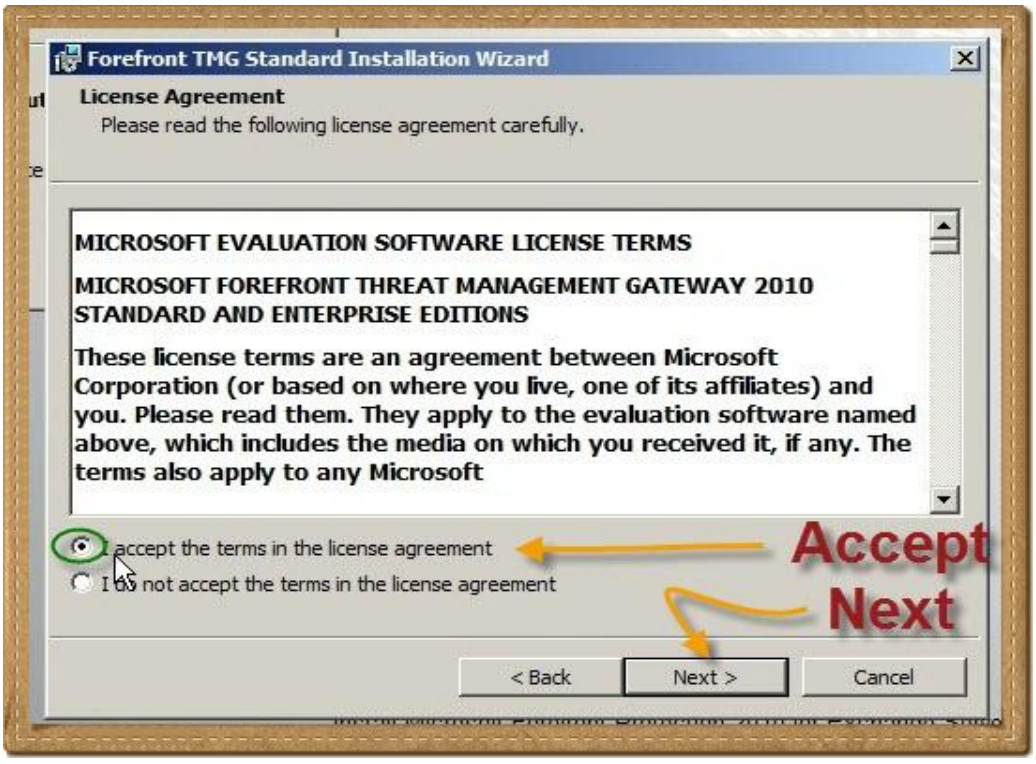
Core Components



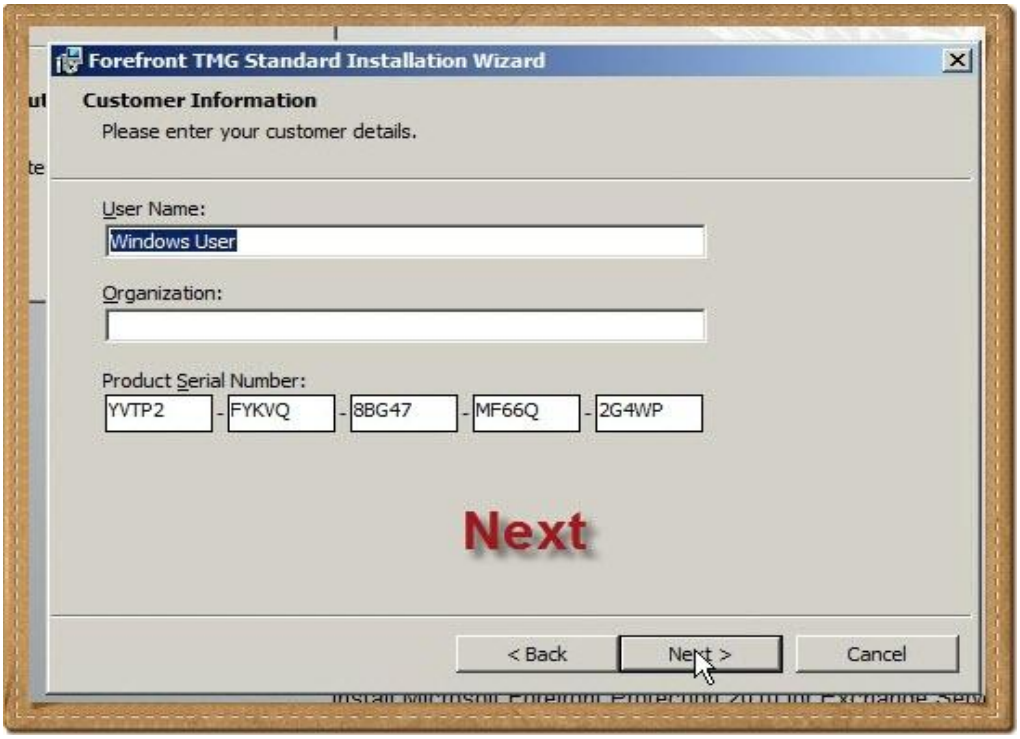
Next



نقبل الإتفاقية و Next



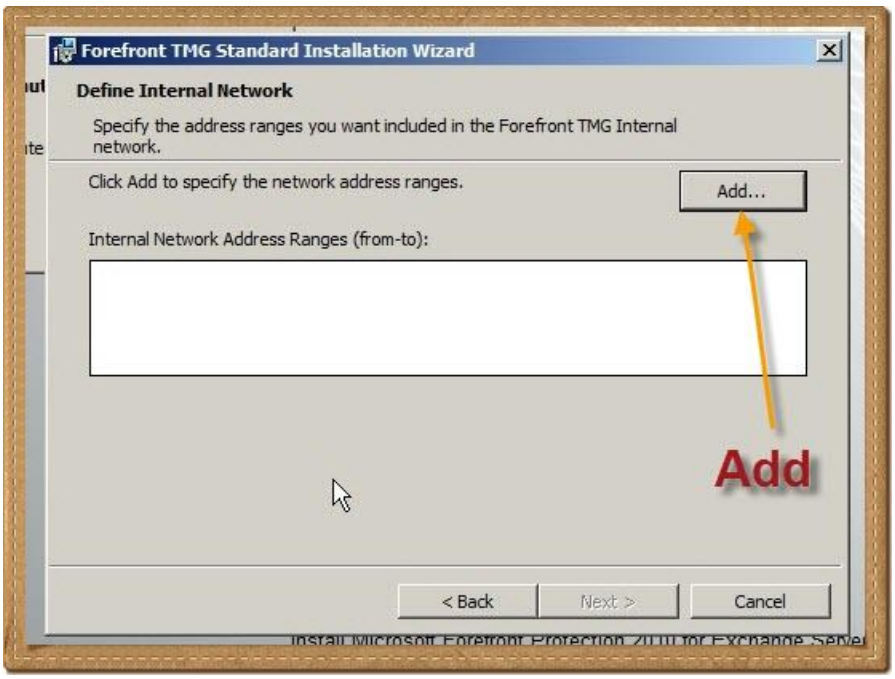
السيريال و Next



نختار مسار التنصيب ثم Next

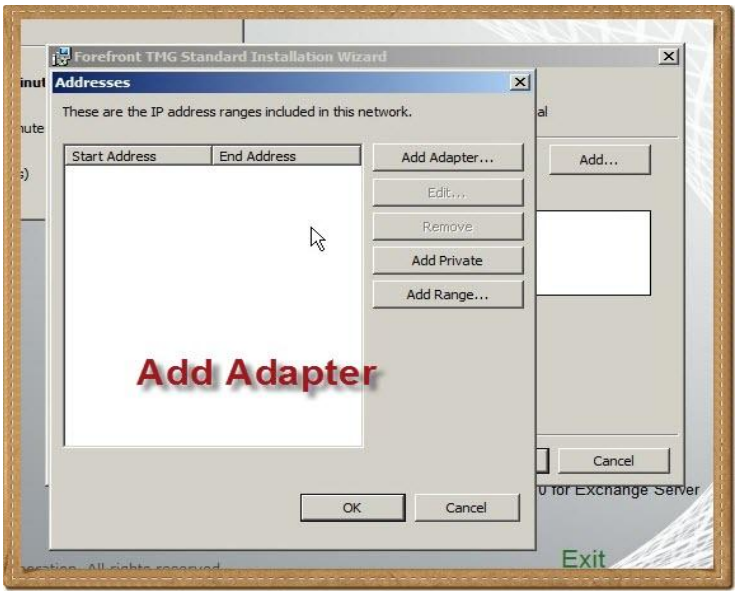
يبدأ الشغل بجد

من هنا لإختيار نطاق الشبكة الداخلية Internal IP Range , نضغط على Add

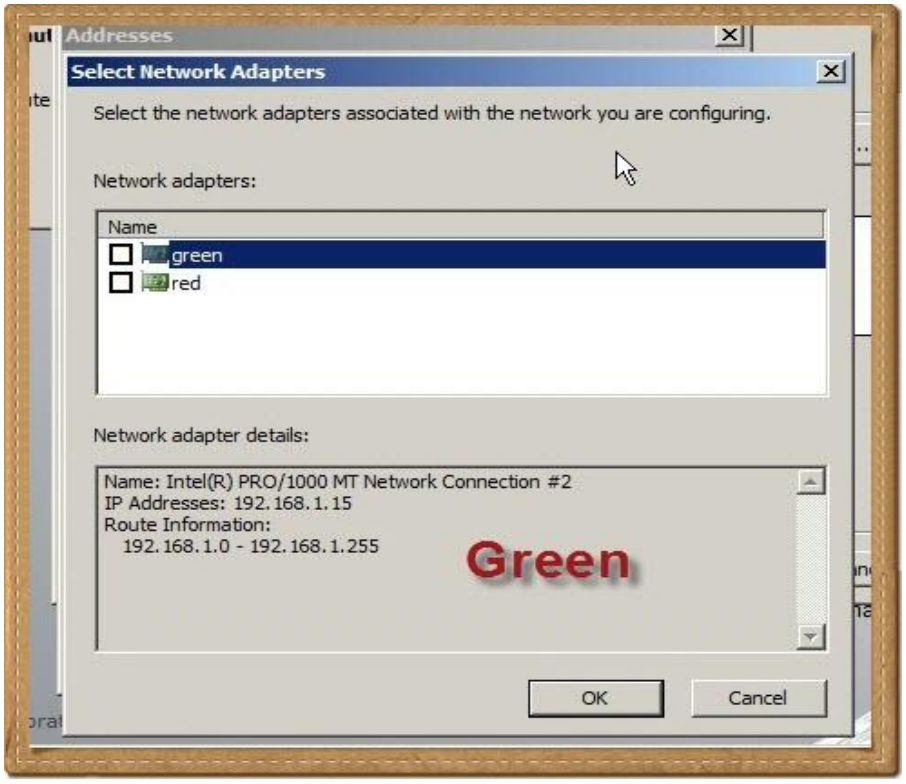


لدينا أكثر من طريقة إدخال الـ range

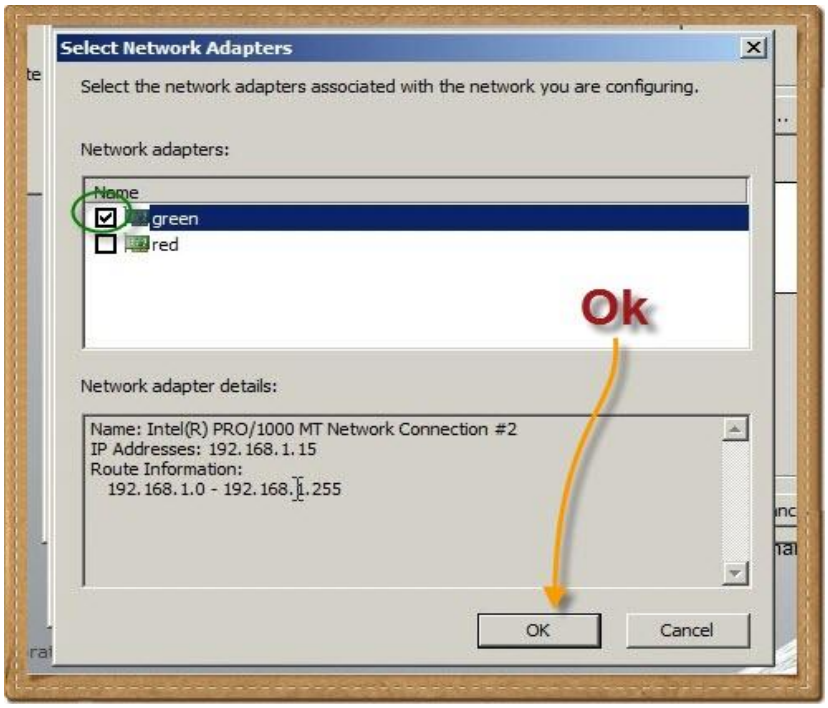
فيمكننا اللجوء إلى الطريقة الأسهل عن طريق الضغط على Add Adaptor لإختيار كارت الشبكة الداخلي وبالتالي سيتعرف المعالج على النطاق الخاص بالشبكة الداخلية



أمامنا الكارتين Red and Green

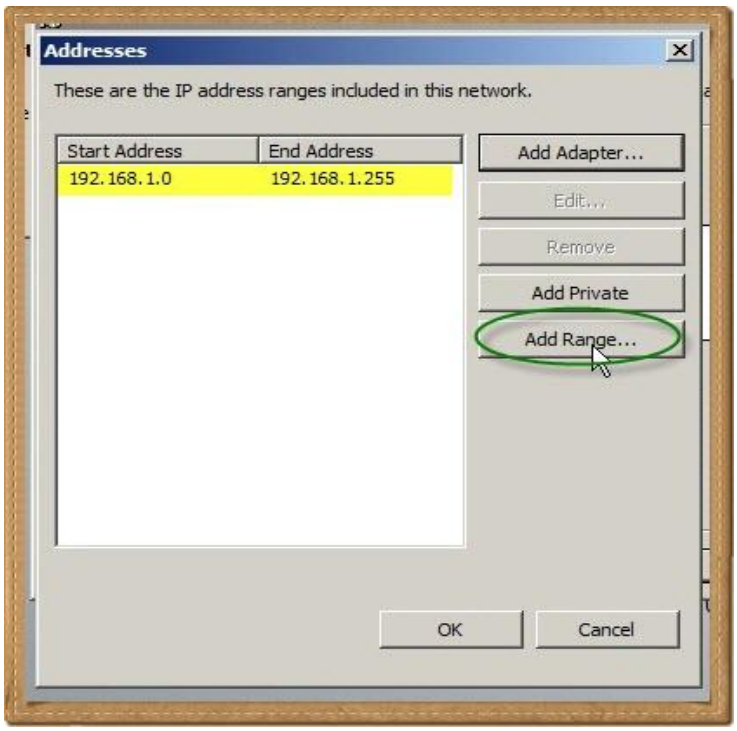


نختار Green ونضغط Ok

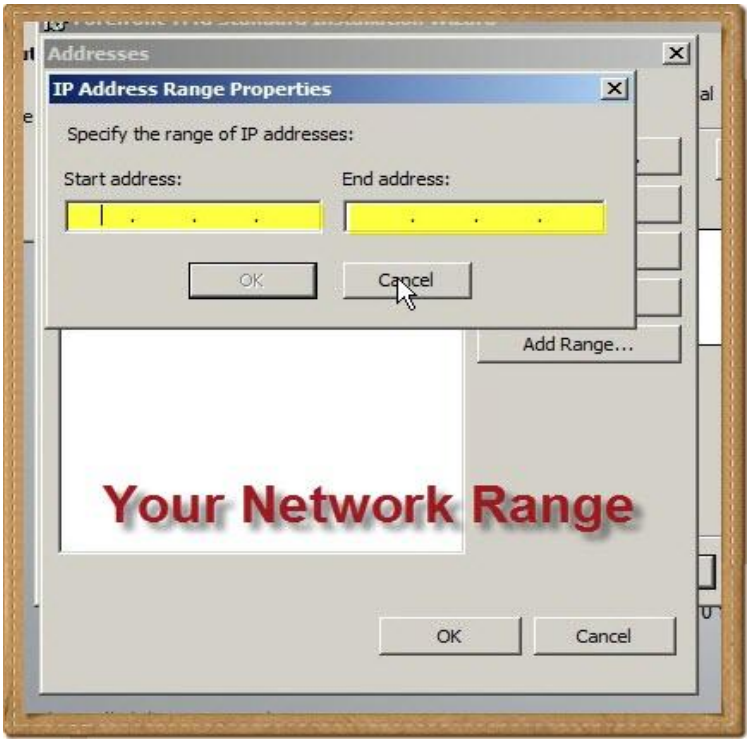


تعرف المعالج على الـ IP Range

أيضا يمكننا إدخال النطاق يدوي , نضغط على Add Range

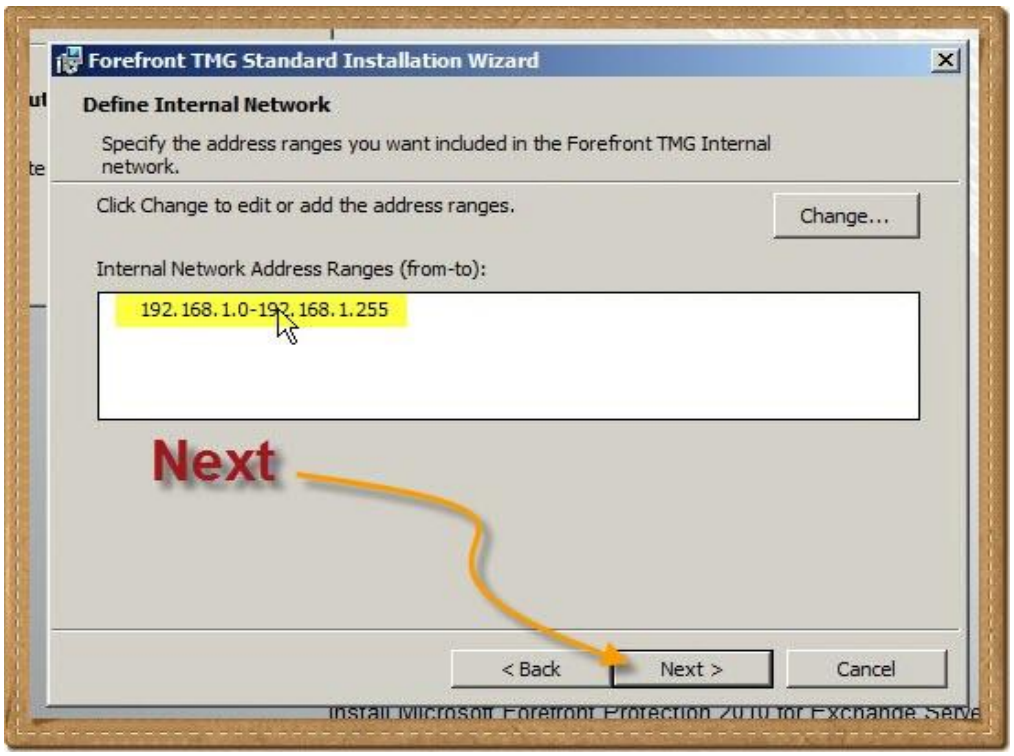


ثم ندخل النطاق Start و End

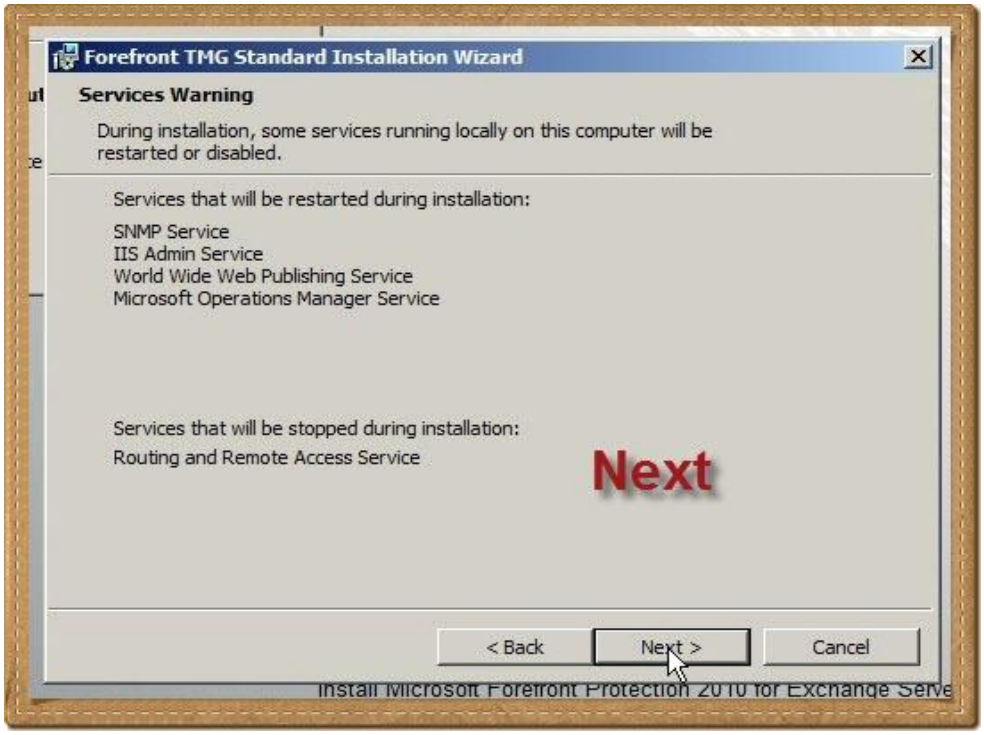


نرجع إلى المعالج وبعد التأكد من صحة النطاق نضغط Ok

ثم Next

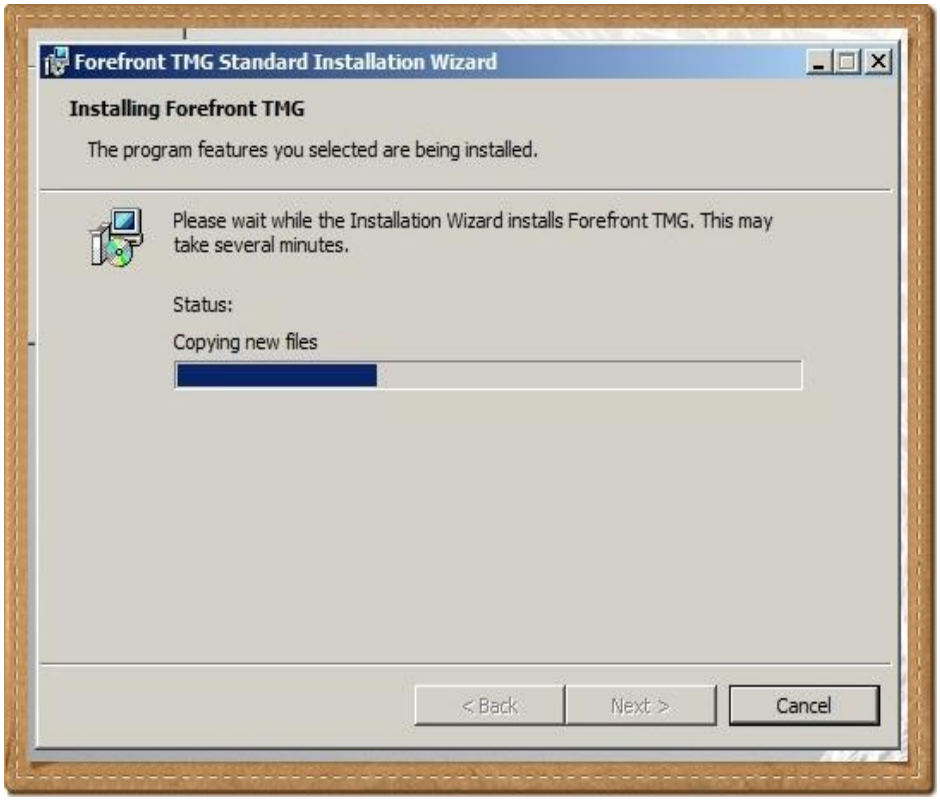


ثم Next

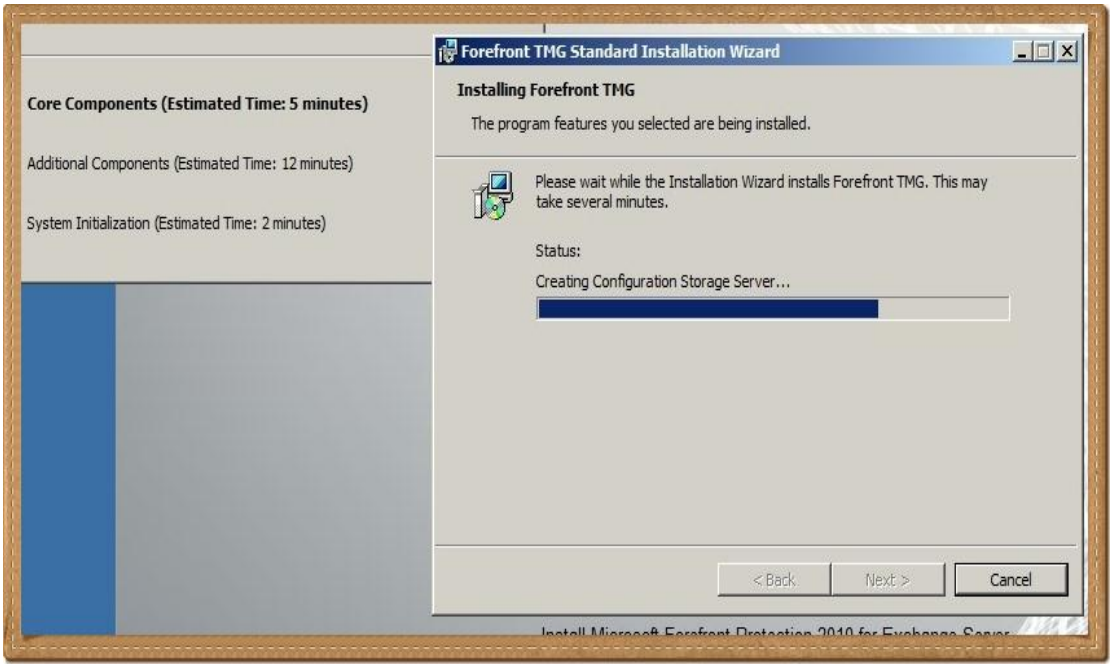


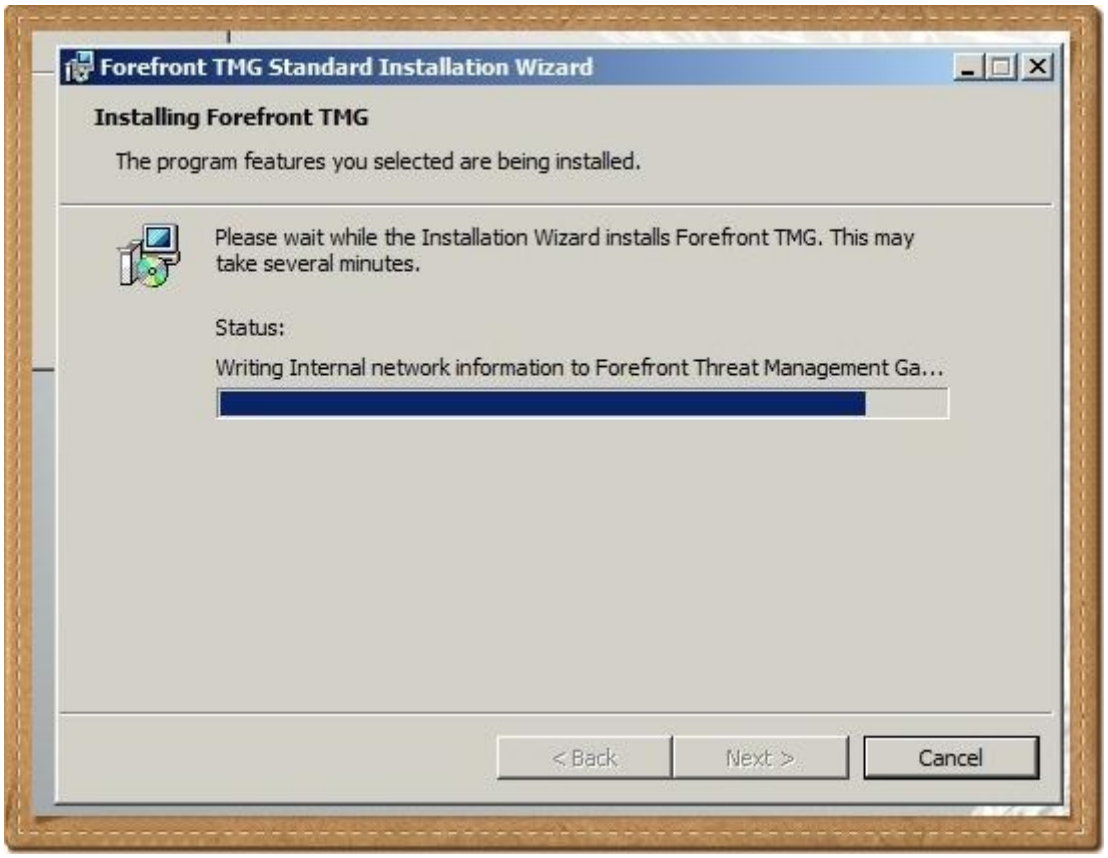
ثم Install

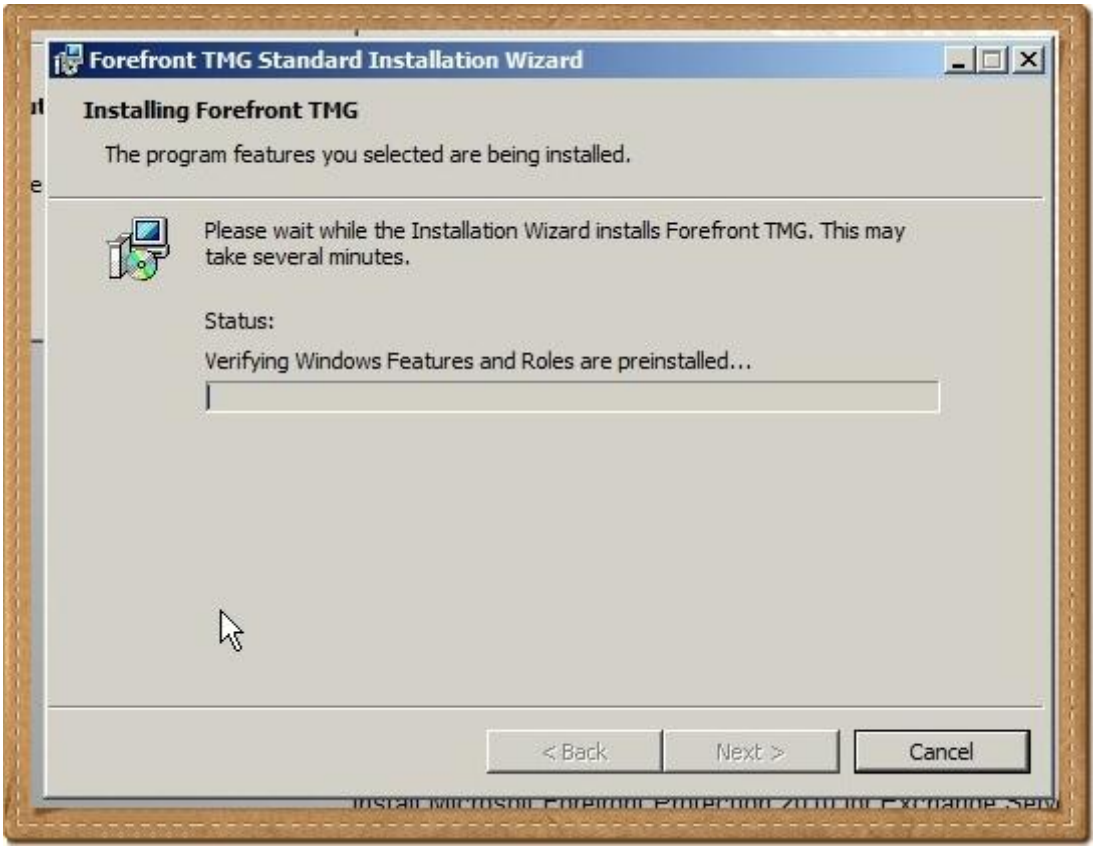
ونقضيها فرجه



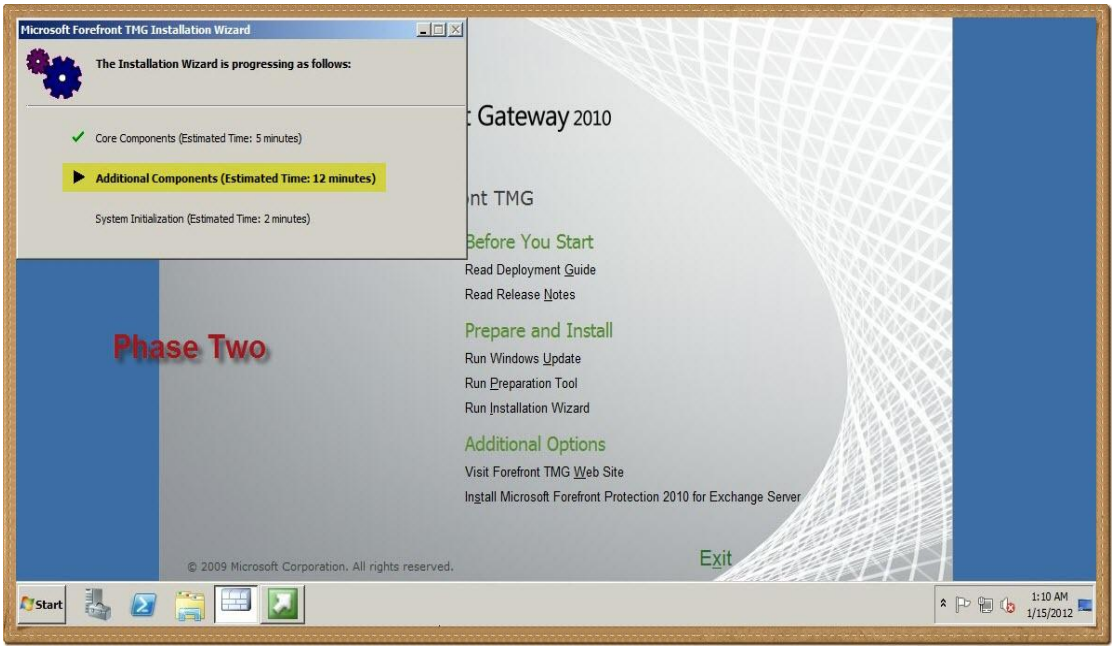
صبراً



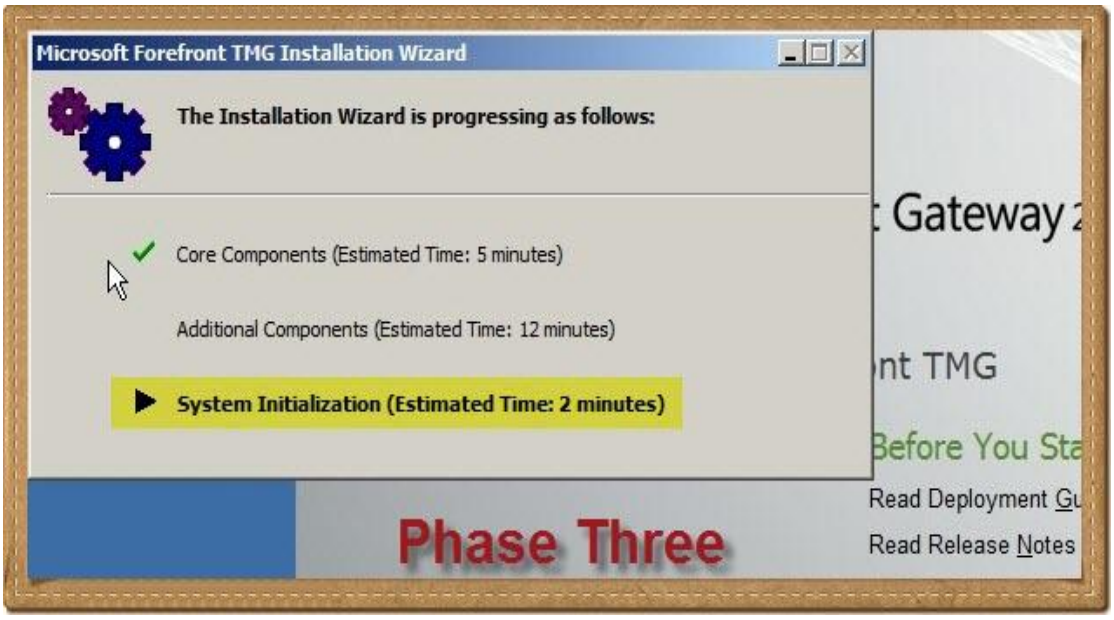

Forefront TMG Standard Installation Wizard
Installing Forefront TMG
The program features you selected are being installed.
Please wait while the Installation Wizard installs Forefront TMG. This may take several minutes.
Status:
Writing Internal network information to Forefront Threat Management Ga...
< Back
Next >
Cancel


Forefront TMG Standard Installation Wizard
Installing Forefront TMG
The program features you selected are being installed.
Please wait while the Installation Wizard installs Forefront TMG. This may take several minutes.
Status:
Verifying Windows Features and Roles are preinstalled...
< Back
Next >
Cancel

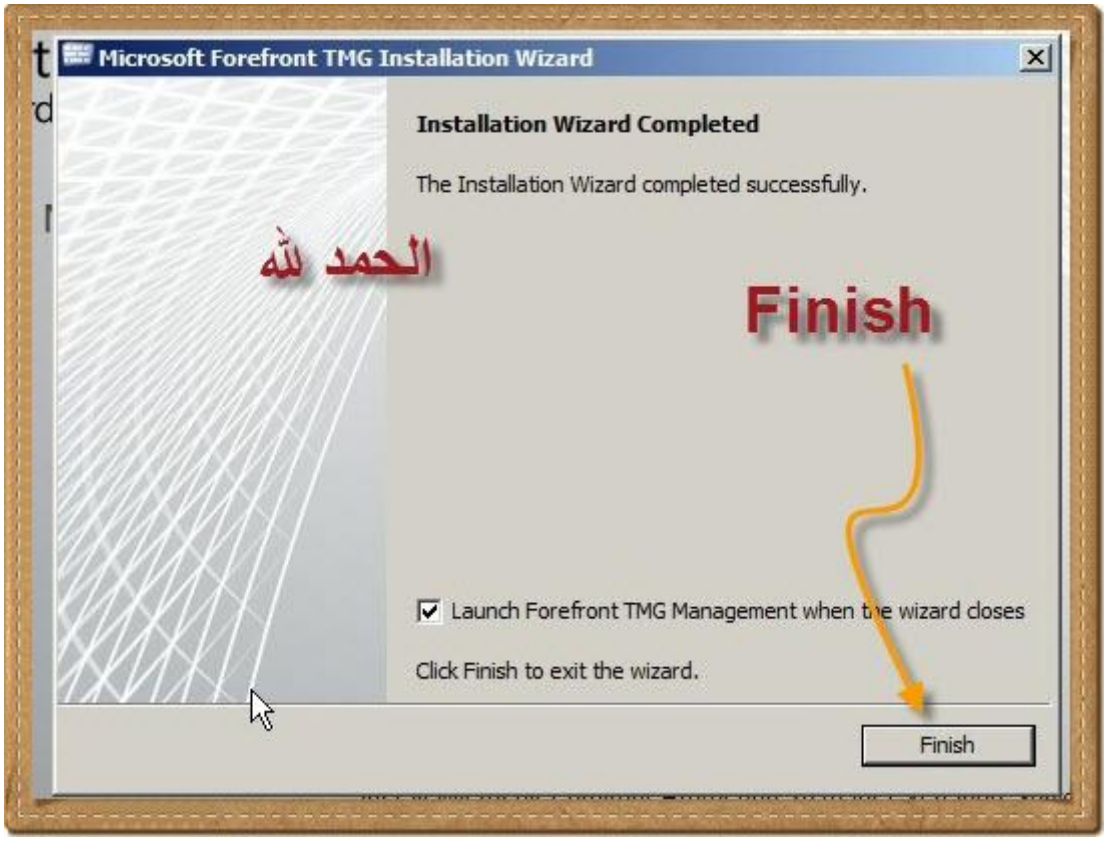
الجزء الثاني من المرحلة الثالثة



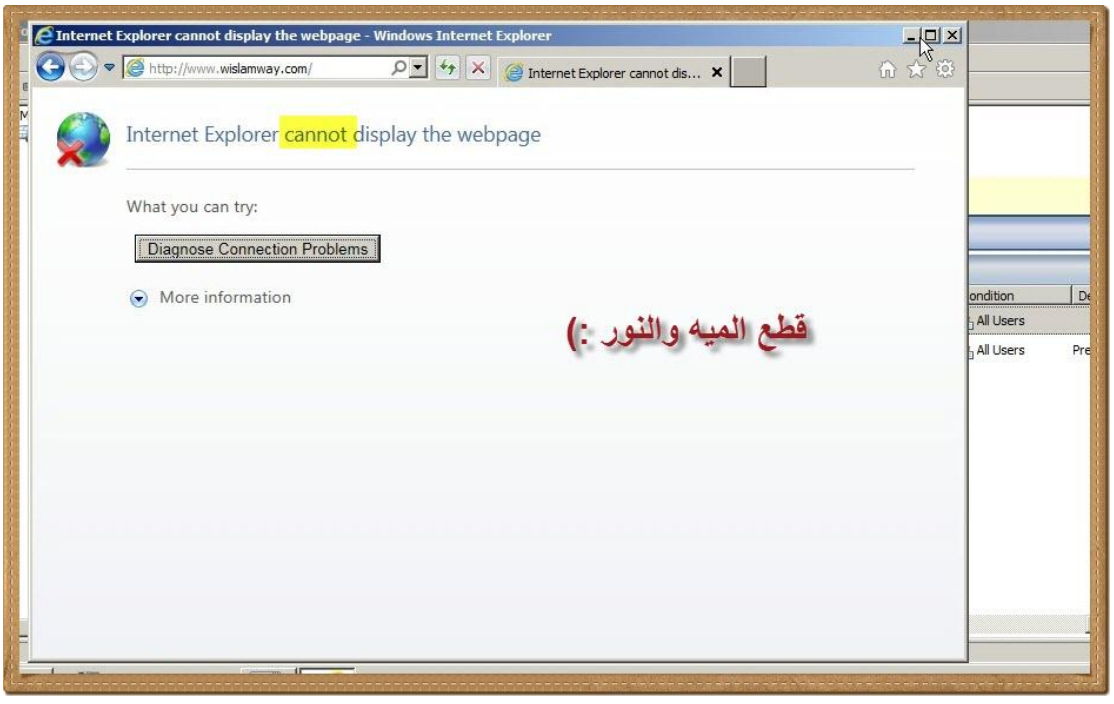
والجزء الثالث والأخير من المرحلة الثالثة والأخيرة



الحمد لله ... وسمعنا أحلى Finish



نجرب الإنترنت ... طبعا مافيش و الدنيا ضلمت



كده الدنيا وقفت ☺

الفصل القادم إن شاء الله نمشيها

اللهم إني أعوذ بك أن أشرك بك شيء أعلمه

وأستغفرك لما لا أعلمه

سبحانك اللهم وبحمدك , أشهد ألا إله إلا أنت , أستغفرك وأتوب اليك

TMG

أول مرّه

—

الحمد لله والصلاة والسلام على رسول الله

نزلنا الـ TMG وقفلنا الدنيا علينا وعلى الناس

- *ليه الدنيا إتقفلت ؟*

ح أقولك :

التي إم جي بيتعامل بصفة أساسية من خلال Rules يقوم الأدمين بإنشائها , وهذه الرولز تحدد من سيفعل ماذا ومتى

منها تقدر تفتح لفلان الموقع الفلاني لأنواع الملفات الفلانية في الأوقات الفلانية

و العكس صحيح

فقط يوجد Rule واحدة تكون Default مع الإعداد وهي الرول الخاصة بإغلاق كل شيء عن كل الناس في كل الأوقات

هذه الرول لا تقبل إلغاء أو تعديل !!!!

ويكون الحل أن نبدأ بعمل رول موازية نفتح فيها كل شيء لنتأكد من إن الدنيا ماشية تمام بعدها نبدأ في تخصيص الرولز من خلال الدروس التالية

عند تشغيل الـ TMG للمرة الأولى يظهر لنا معالج إعداد جميل وظريف

وطبعا لإني دقة قديمة فلن استعمله و سأغلقه

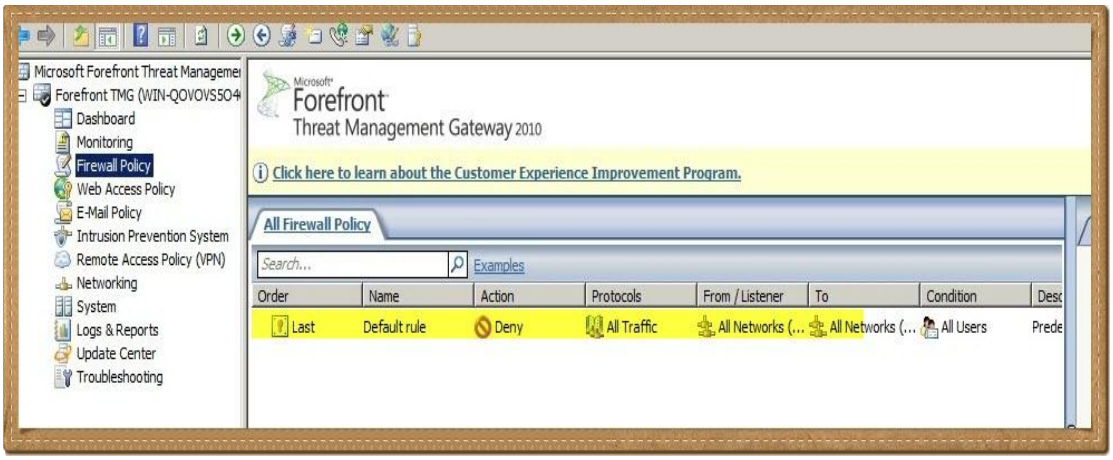
ستظهر لنا الواجهة الرئيسية للبرنامج وهي مشابهة للأيزا

تتيح لنا الواجهة التعامل مع أكثر من TMG سيرفر , سنجد على اليمين سيرفرنا الجميل

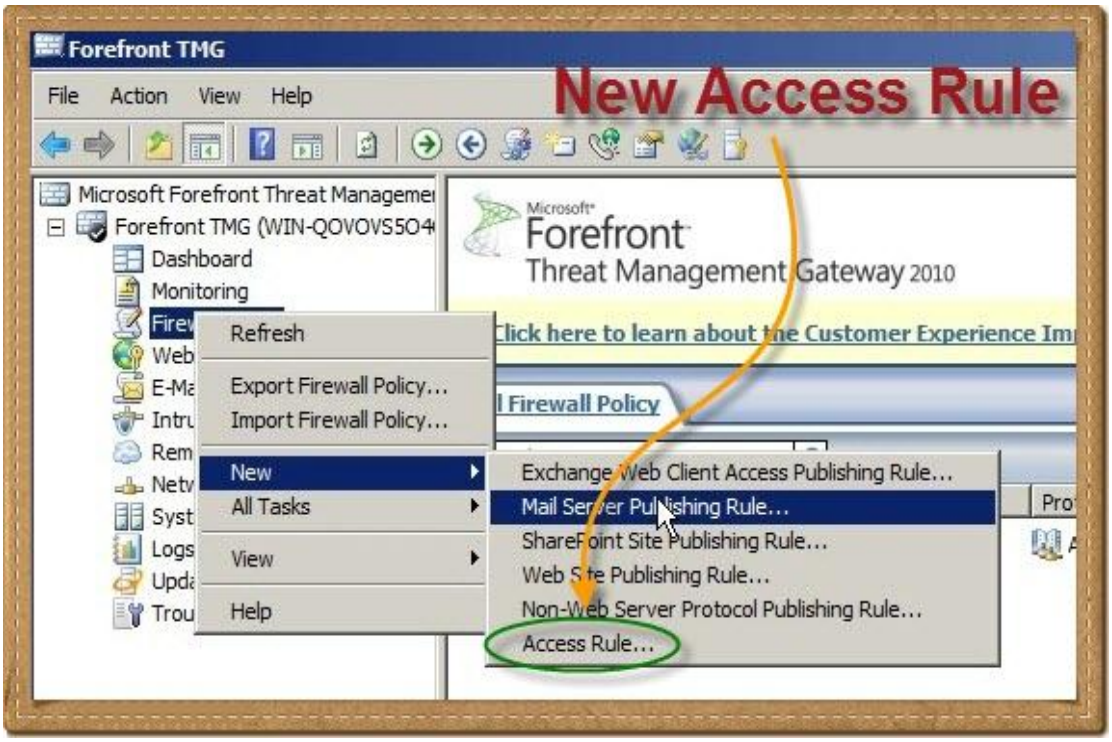
نعمل Expand على السيرفر ليظهر أمامنا الوظائف الرئيسية على اليمين

بالضغط على Firewall Policy سيظهر في الجزء الأوسط الـ Rule التي تكلمنا عنها

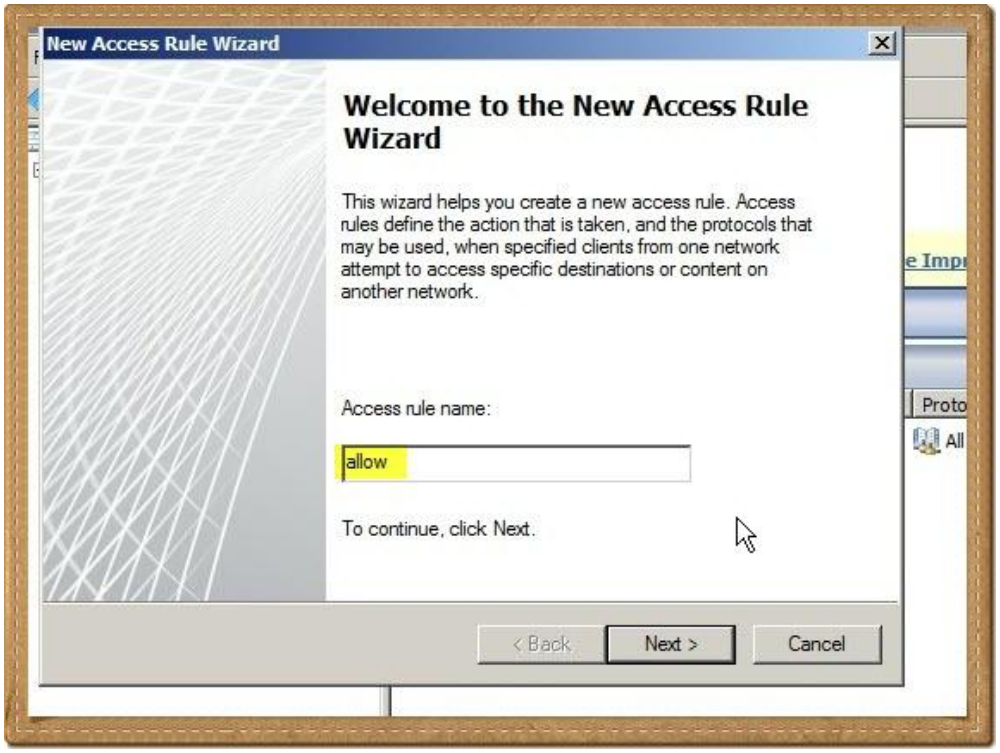
وهي الـ Default Rule اللي قافله كل حاجه



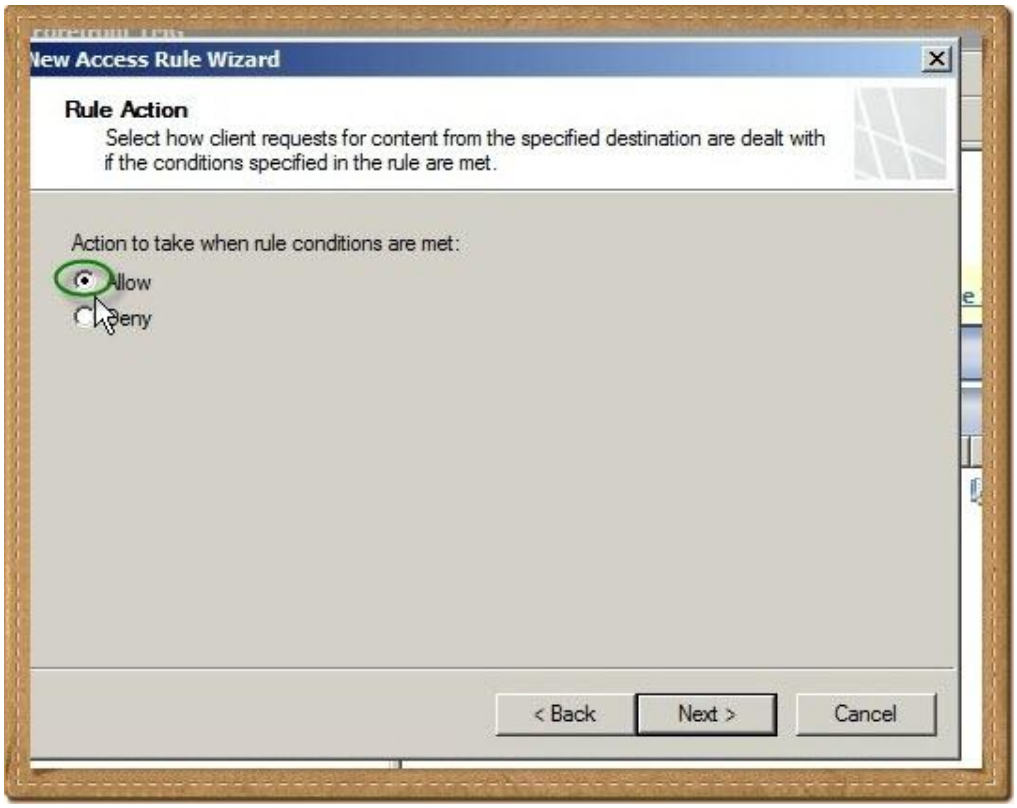
لنبدأ في عمل Rule جديدة : كليك يمين على Firewall Policy ونختار New Access Rule



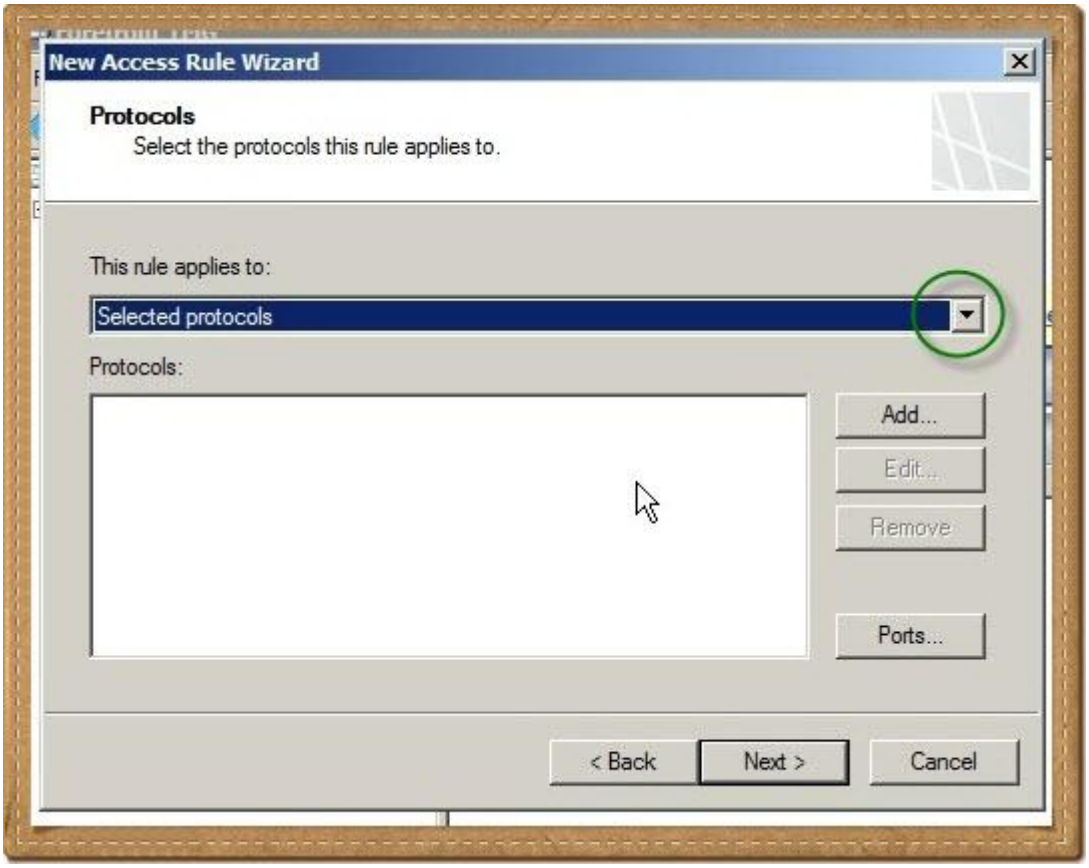
نحدد إسم : Allow



الهدف الأساسي من الـ Rule إيه ؟ .... نختار Allow



على أي بروتوكولات سيتم تطبيق الرول ؟



لدينا ثلاثة إختيارات

All outbound traffic

ح تفتح كل البروتوكولات

Selected protocols

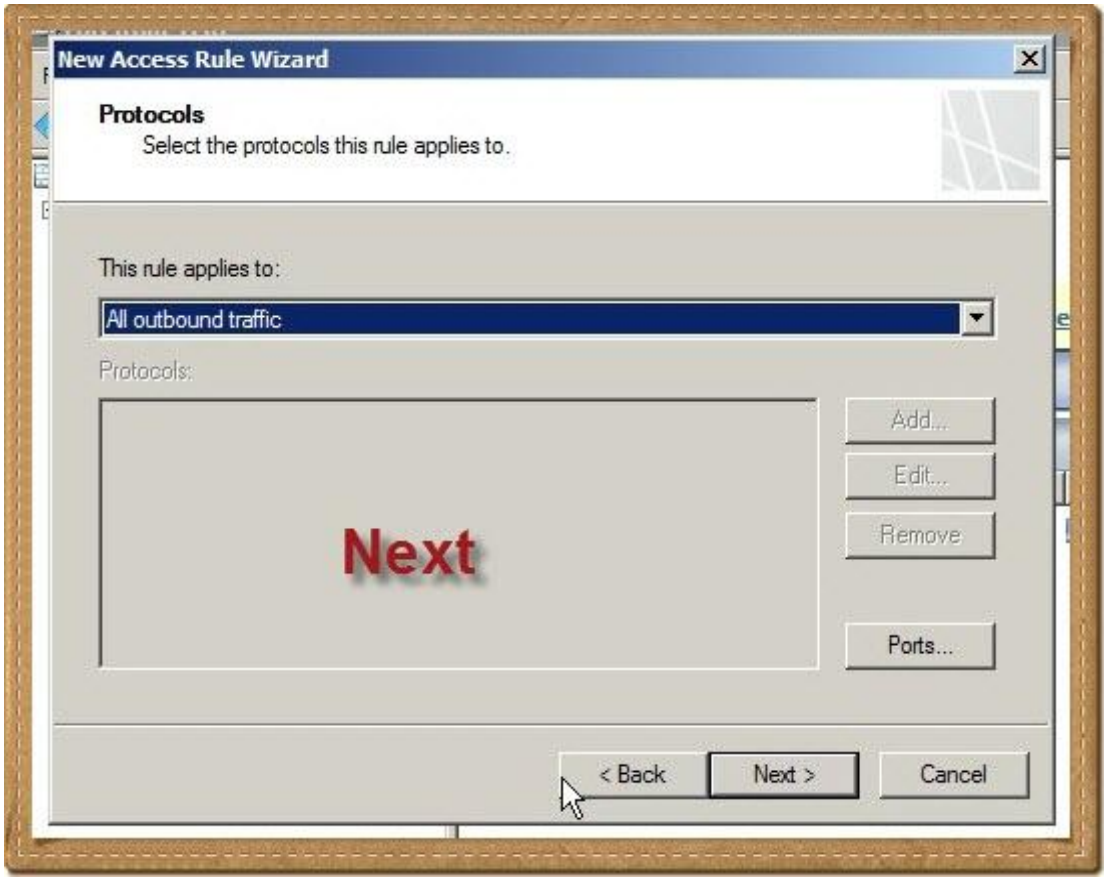
ح تفتح الطريق للبروتوكولات التي سنختارها

All outbound traffic except selected

ح تفتح لكل البروتوكولات عدا ما سنختاره

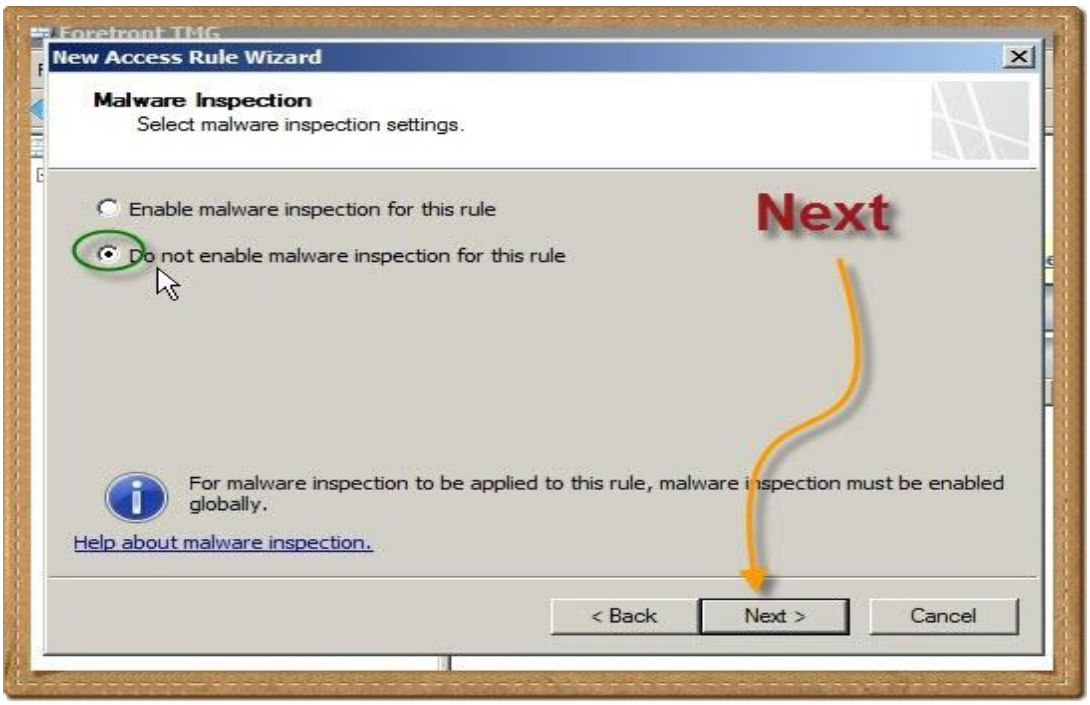
وطبعا بناء على إختيار ح يتحدد البروتوكول اللي ح نختاره ح يتمنع ولا يتسمح

نختار All outbound traffic ونضغط Next

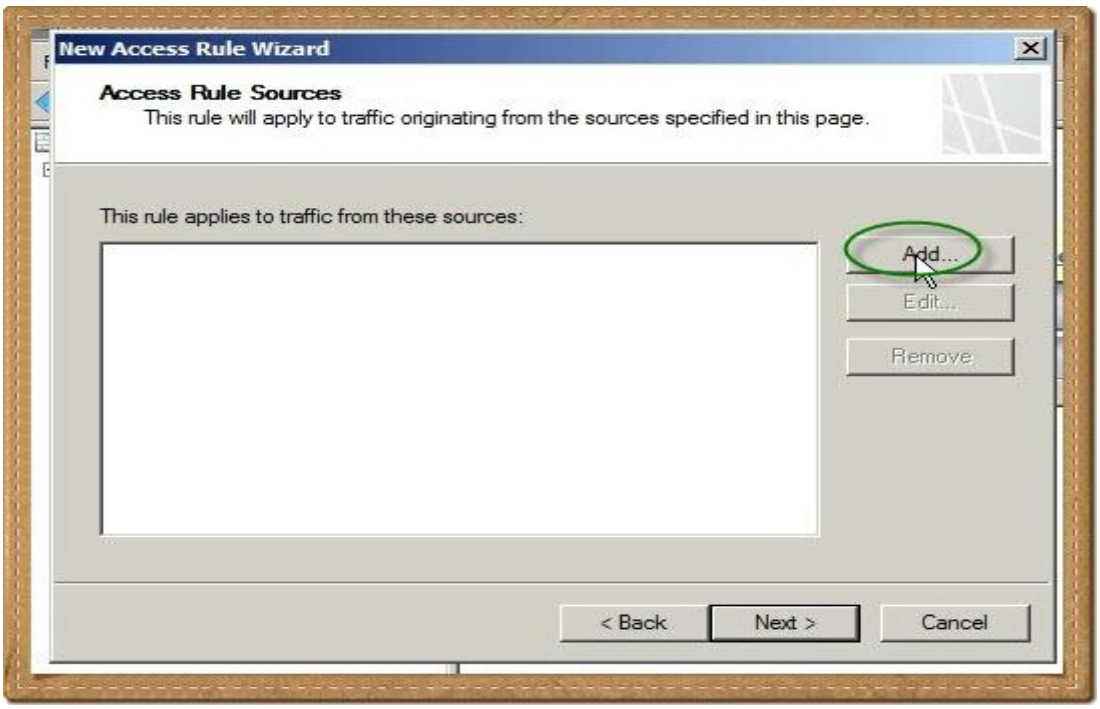


هل سنفعّل Malware Inspection أم لا ؟

نختار لا وسنشرحها فيما بعد



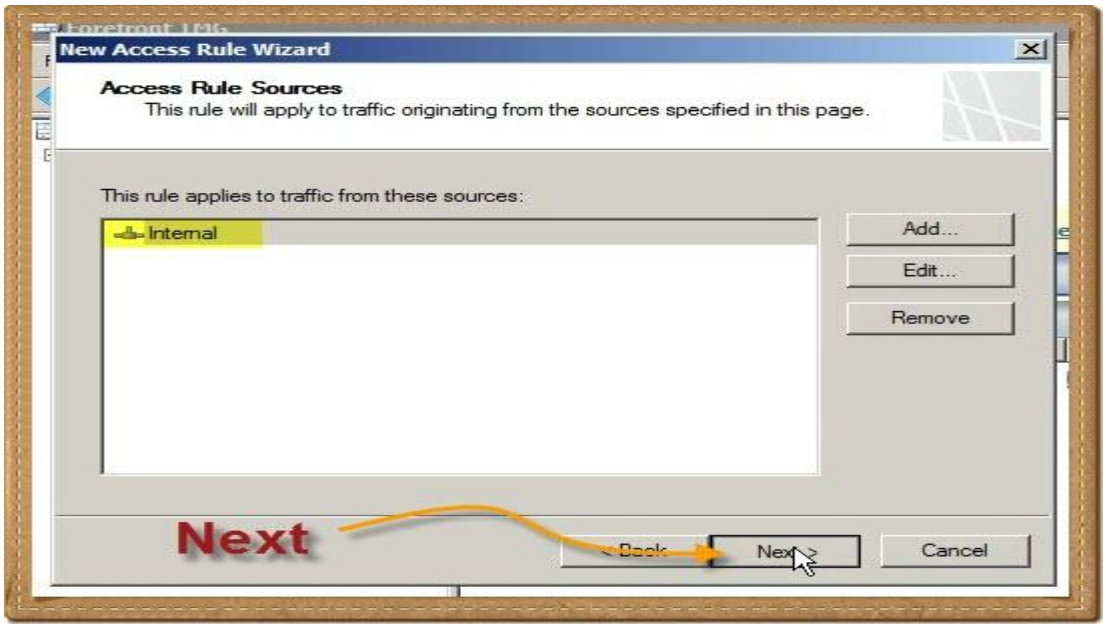
نختار الـ Sources بالضغط على Add



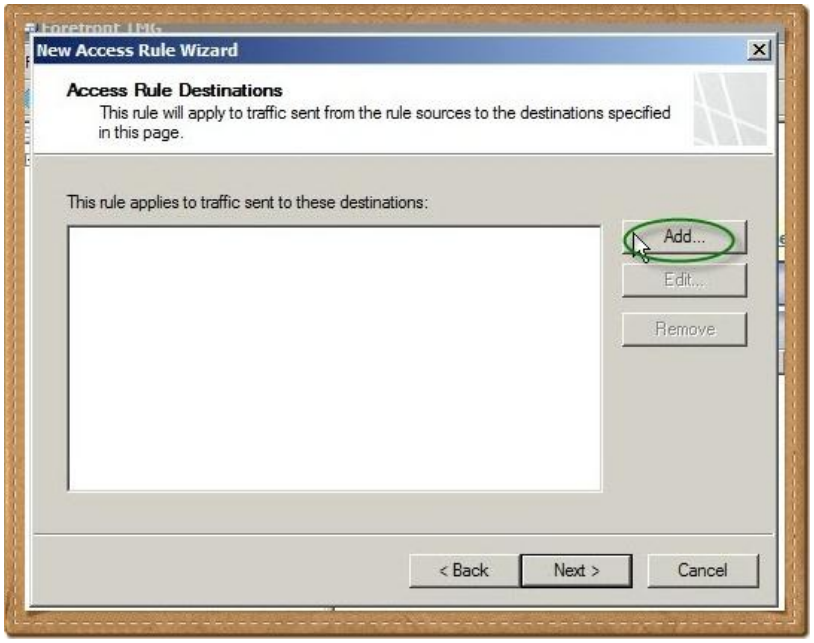
من Networks نختار Internal ونضغط Add

ممكن كمان نختار Local host , ثم Close

Next

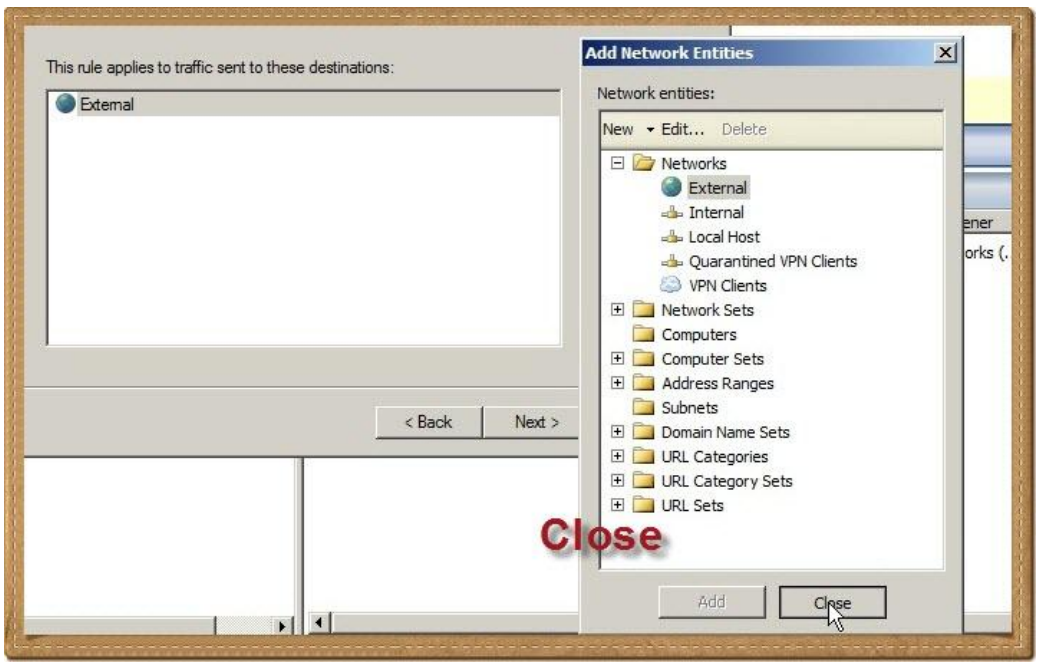


نختار الـ Destinations بالضغط على Add



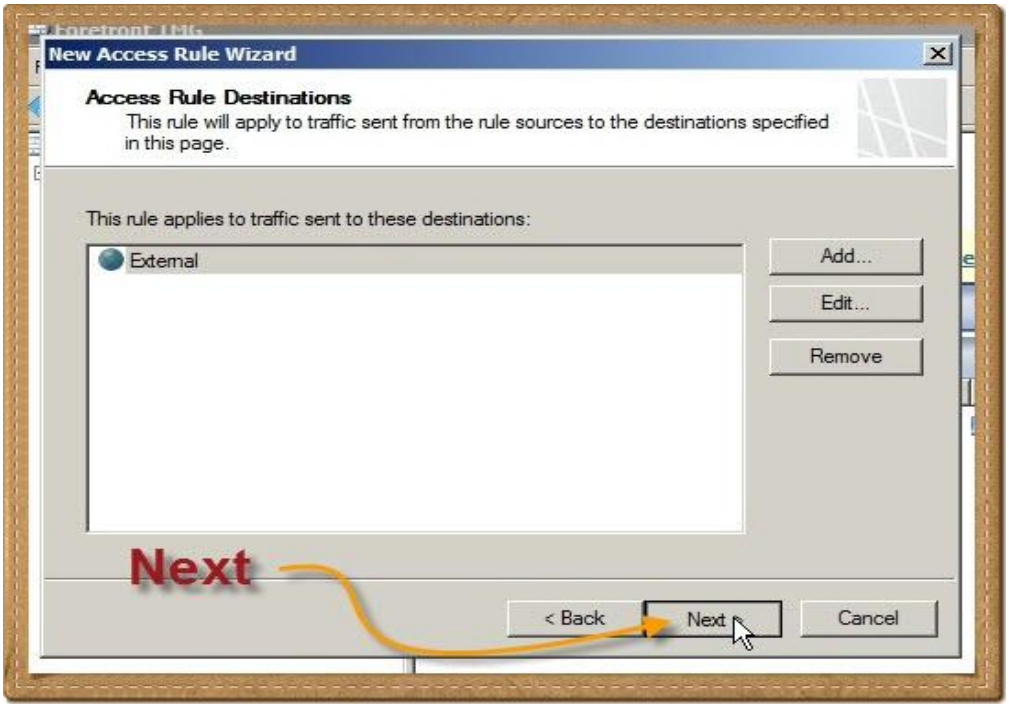
نختار External

ثم Close

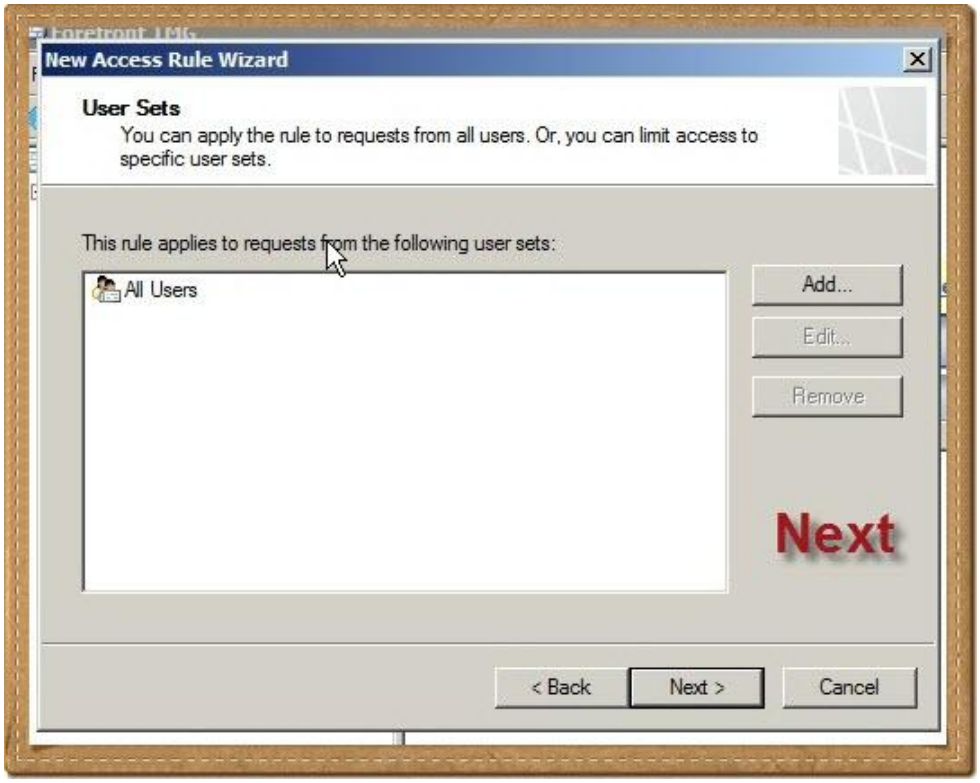


أتمنى أن يكون إتضح لكم ماهو المقصود بالـ Sources والـ Destinations

بإختصار : جاي منين ورايح فين



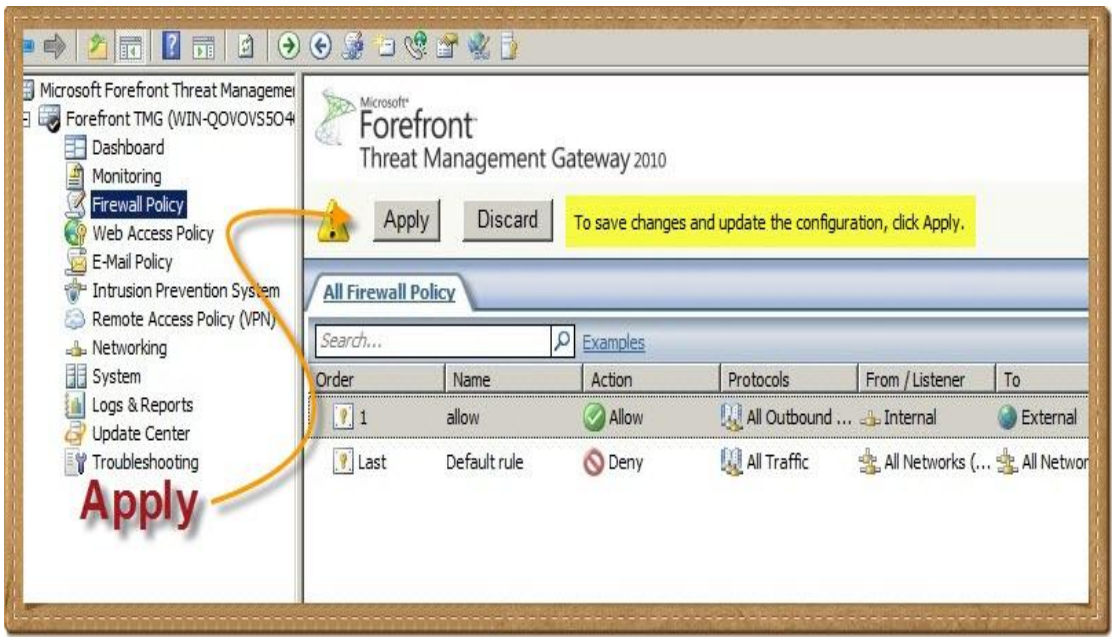
إختيار المستخدمين الذين سيتم تطبيق هذه الـ Rule عليهم , نختار All Users ثم Next



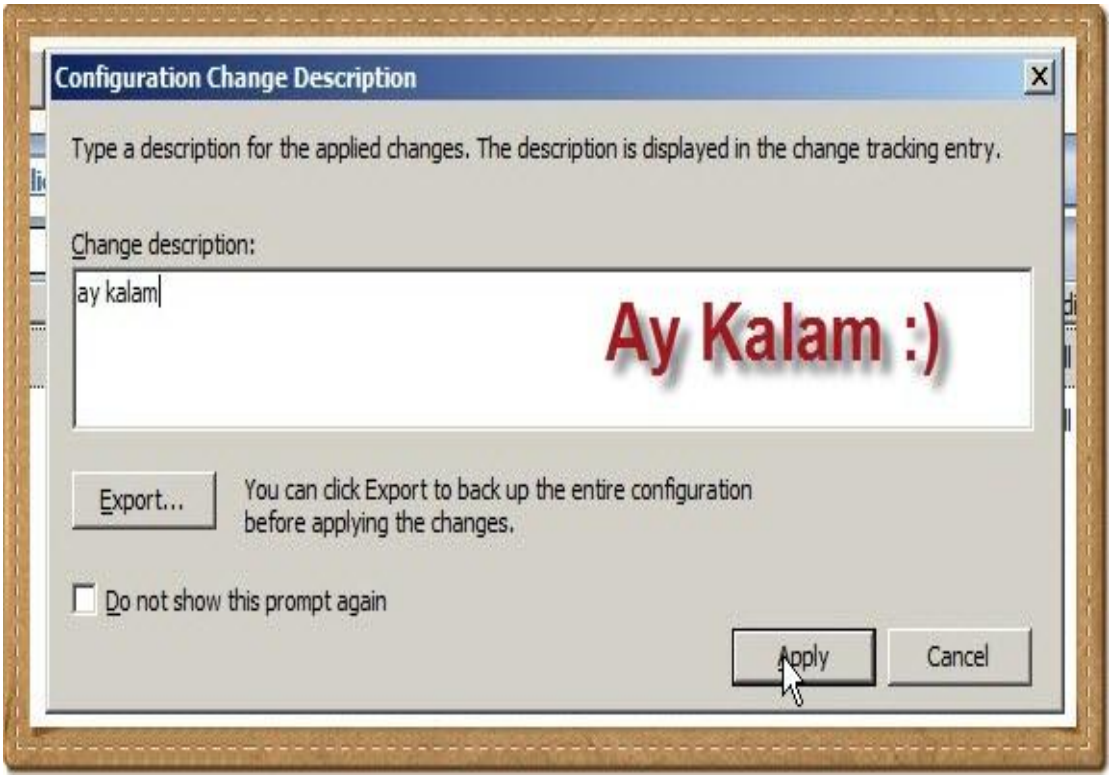
وأخيرا Finish

تم إنشاء الـ Rules وكما نلاحظ أن ترتيبها رقم 1 فالترتيب مهم ولكن نلاحظ أنها غير مفعلة بعد

نضغط Apply لتفعيلها

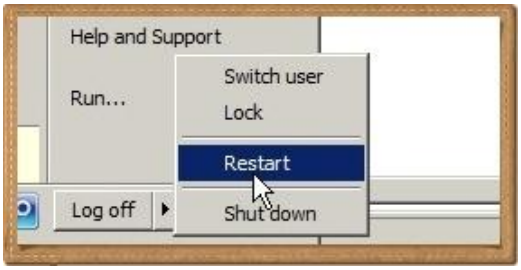


يمكن لنا كتابة ملاحظات بها شرح بسيط لما هو المقصود بالرول , ثم Apply



تم التفعيل , نضغط على Ok

أجمل حاجه تعملها لسيرفر الـ TMG إنك تعمل Restart



بعد كده جرب الإنترنت ح تلاقيه شغال

إنتهى جزء كبير من العمل ولكن هذا غير كاف فقد تحول TMG إلى مجرد موزع للإنترنت ولكنه لن يمنع أي أحد من فعل أي شيء لإننا فتحناها على البحري بسبب الرولز التي عملناها

للخروج من هذه المأزق لدينا حل من إثنين :

- أن نفهم عناصر الـ TMG وبخاصة الـ Rules أكثر وبالتالي نستطيع تخصيص الـ TMG ليحقق سياسة المنشأة
- أن نلجأ إلى برنامج آخر Third Party ليتولى المهمة

وهذا ما سنتناوله بإذن الله

اللهم إني أعوذ بك أن أشرك بك شيء أعلمه

وأستغفرك لما لا أعلمه

سبحانك اللهم وبحمدك , أشهد ألا إله إلا أنت , أستغفرك وأتوب اليك

TMG

ريموت كونترول

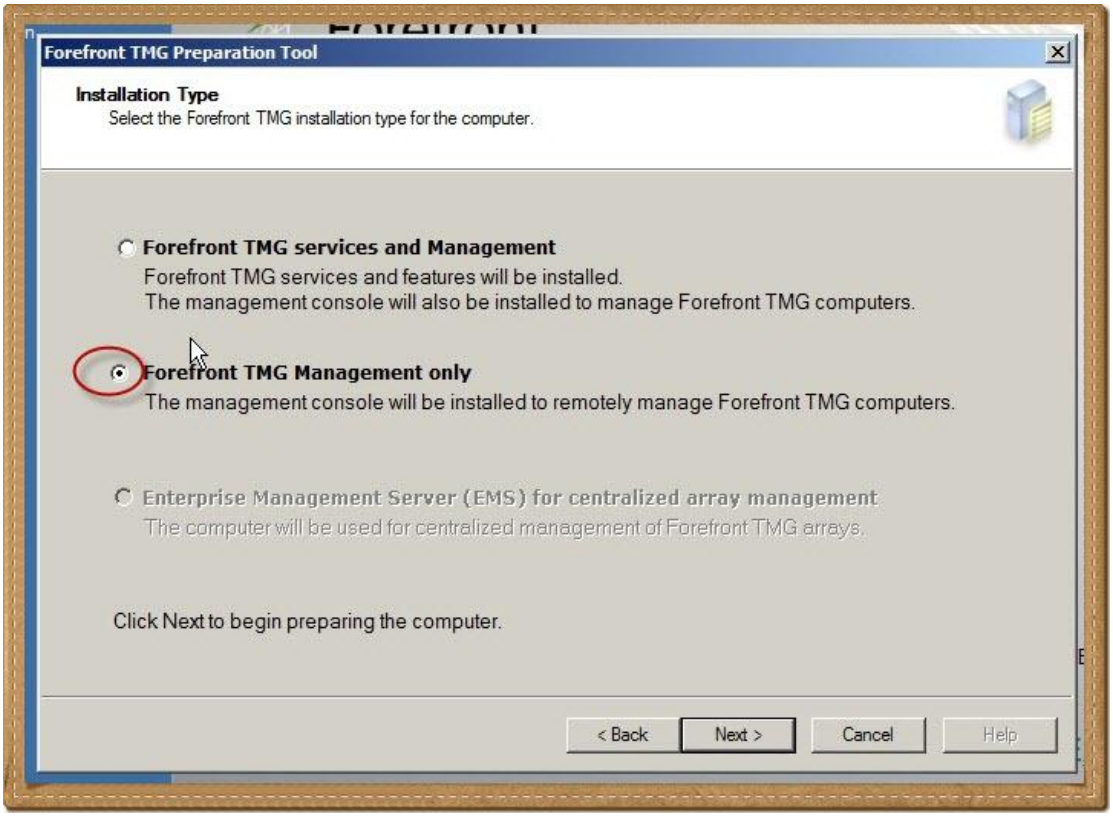
الحمد لله والصلاة والسلام على رسول الله

درس خفيف ولذيذ وهام وهو خاص بإدارة سيرفر الـ TMG (أو أي سيرفر) من بعيد Remotely

توجد أكثر من طريقة لإدارة السيرفر ريموتلي من أي جهاز كلاينت آخر

فيمكن أن ننزل على هذا الجهاز Management Console الخاص بـ TMG مع عمل رول خاصة به على التي إم جي وذلك من خلال الخيار الذي يظهر لنا خلال الإعداد

فنختار الخيار الثاني كما بالصورة ثم Next ونكمل الإعداد



وبعد إنتهاء الإعداد نفتح الكونسول ونختار السيرفر كالتالي

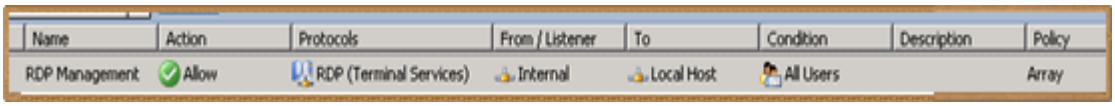
وخلاص على كده

يوجد طريقة أخرى وهي صالحة لإدارة أي شيء على الشبكة أغلبنا يستخدمها بإستمرار , بل إن البعض يفعلها لدخول بعض المستخدمين للعمل على أحد البرامج عن بعد أو للدخول لشبكة العمل أثناء السفر أو من المنزل , وهي

Remote Desktop Connection

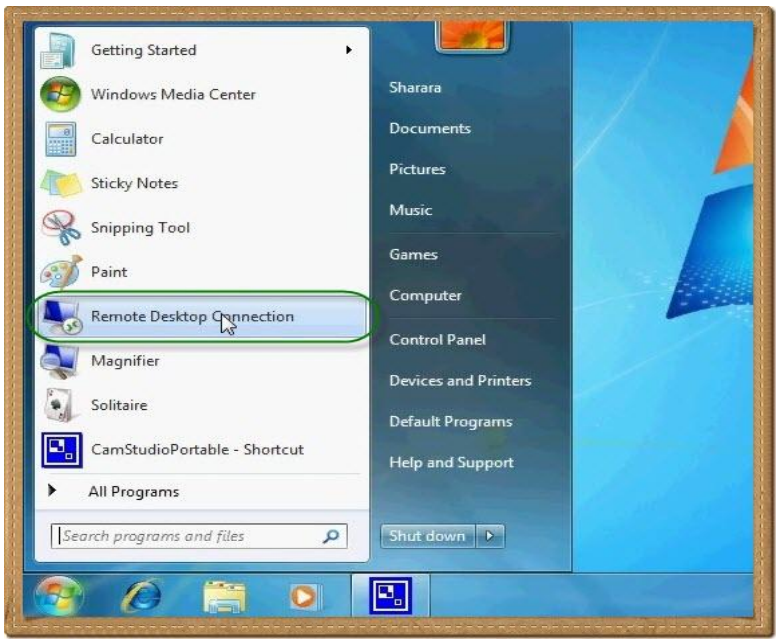
طبعا هذه السيرفس معروفة ومتجربة ولا مجال هنا لشرحها بتوسع ولكن فقط سنتكلم عنها كأداة لإدارة TMG

يحتاج الأمر أولا لعمل Rule بالمواصفات التالية خاصة بخدمة الريموت ديسك توب



نلاحظ هنا إختيارنا للبروتوكول الخاص بالريموت ديسكتوب وهو برتوكول RDP

بعد عمل الرول وتفعيلها فتح Remote Desktop Connection من جهاز الكلاينت



ثم ندخل الاي بي الخاص بالـ TMG Server و Connect

ننتظر

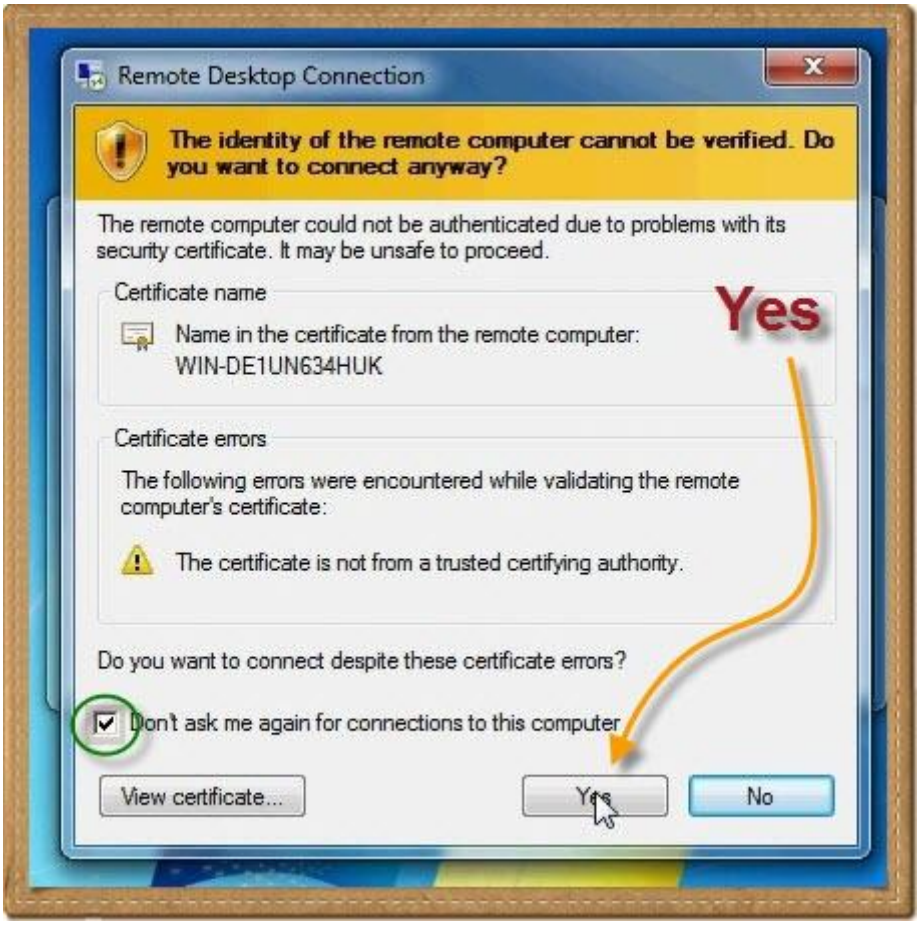
لازم يكون أدمن طبعا على السيرفر , هنا سنختار Use another account

Administrator username and password

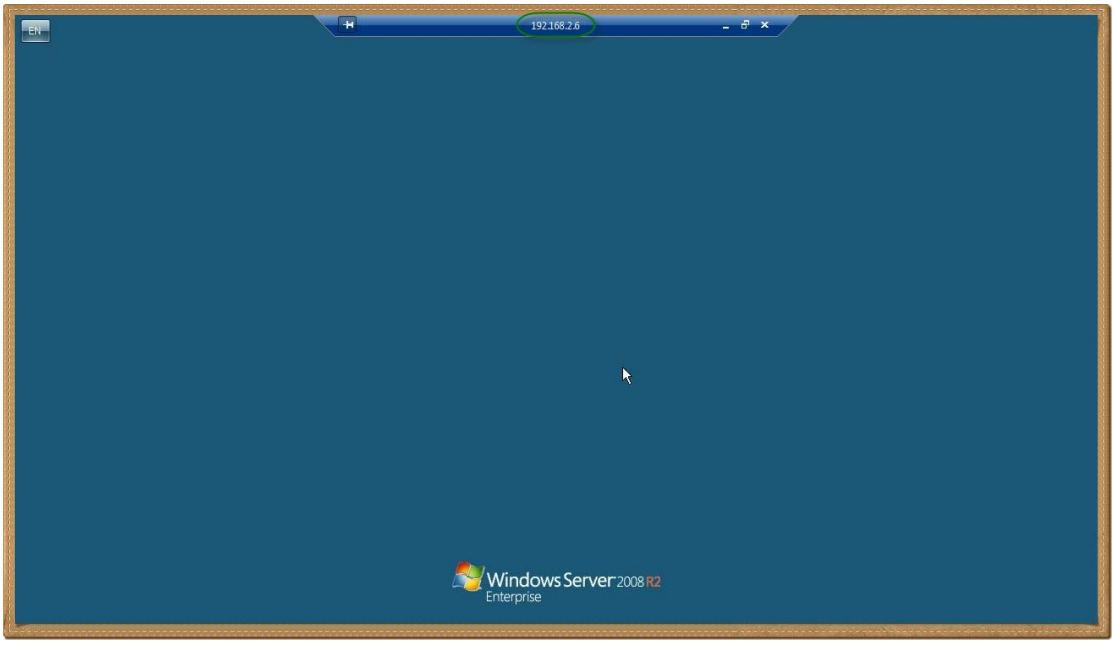
Ok

بـ Connecting

وأخيرا Yes



تم بحمد الله



وكفاية كده النهارده

اللهم إني أعوذ بك أن أشرك بك شيء أعلمه

وأستغفرك لما لا أعلمه

سبحانك اللهم وبحمدك , أشهد ألا إله إلا أنت , أستغفرك وأتوب اليك

TMG

خُد فكره

الحمد لله والصلاة والسلام على رسول الله

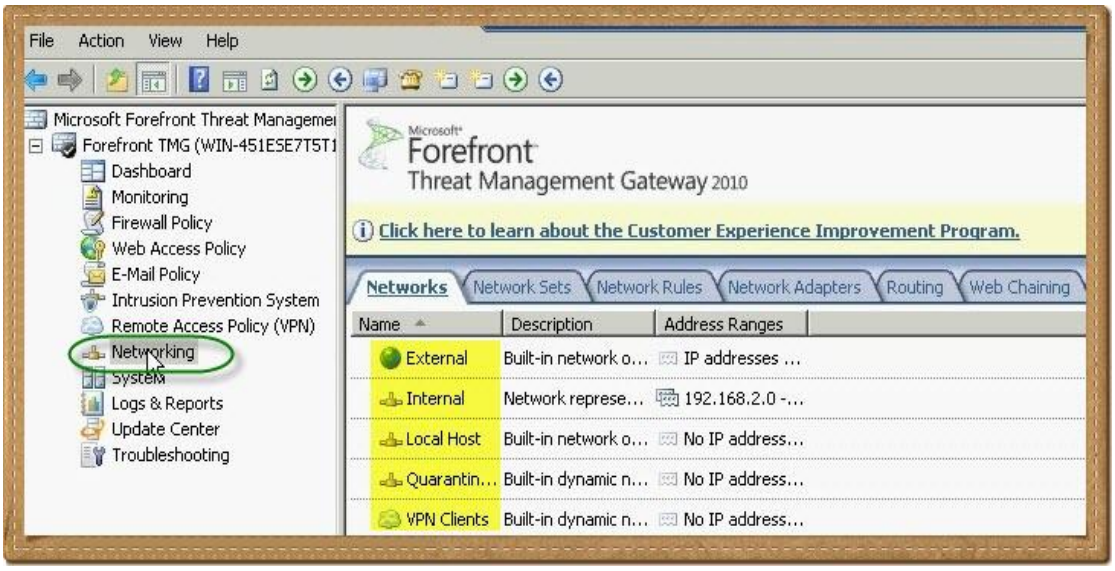
لن تتعلم في هذا الفصل كيفية عمل رول معينة لوظيفة معينة ولكن بمشيئة الله بنهاية هذا الفصل ستصبح ملماً بما هي العناصر التي تتشكل منها الرولز , حينها سيبقى عليك أن تجتهد قليلا وتشغل مخك وممكن كمان تجوجول حتى تستطيع تخصيص الـ TMG بما يحقق سياسة المنشأة

كما ستعرف أيضا الكثير عن هذا السيرفر ووظائفه من خلال التعرف على مكونات واجهة إدارة الـ TMG Server

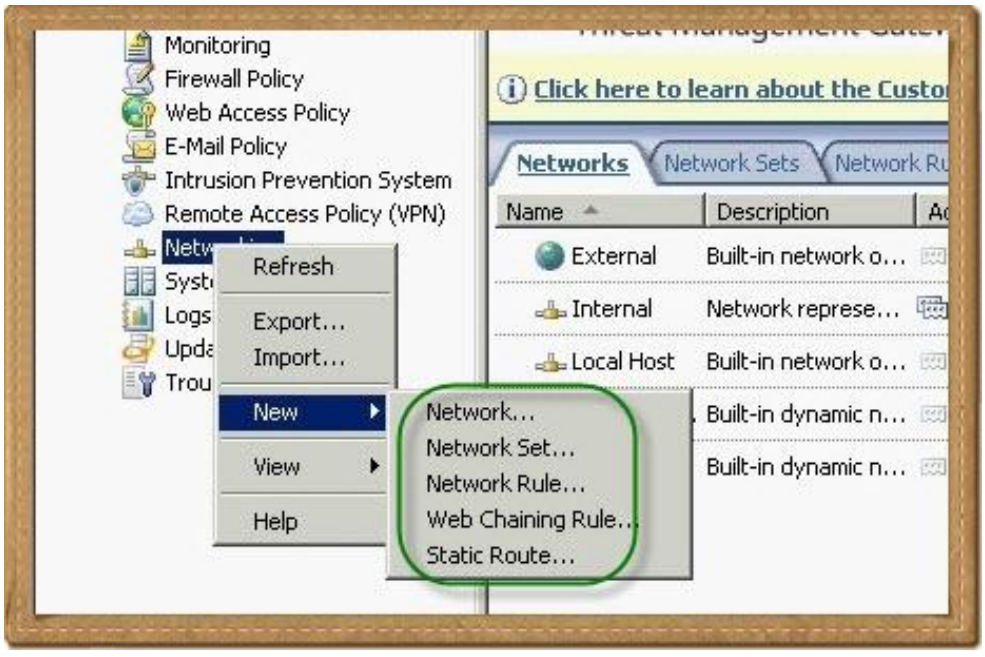
Networking

سنبدأ مع Networking

وهنا يمكننا إدارة عناصر الشبكة كالتي إستخدمناها في Sources و Desinations



كليك يمين ثم New لنستطيع إضافة أي مجموعة أو عنصر



Intrusion Detection

طبعا سيرفر TMG مخصص لإنه بيقاوم الهجمات الخارجيه

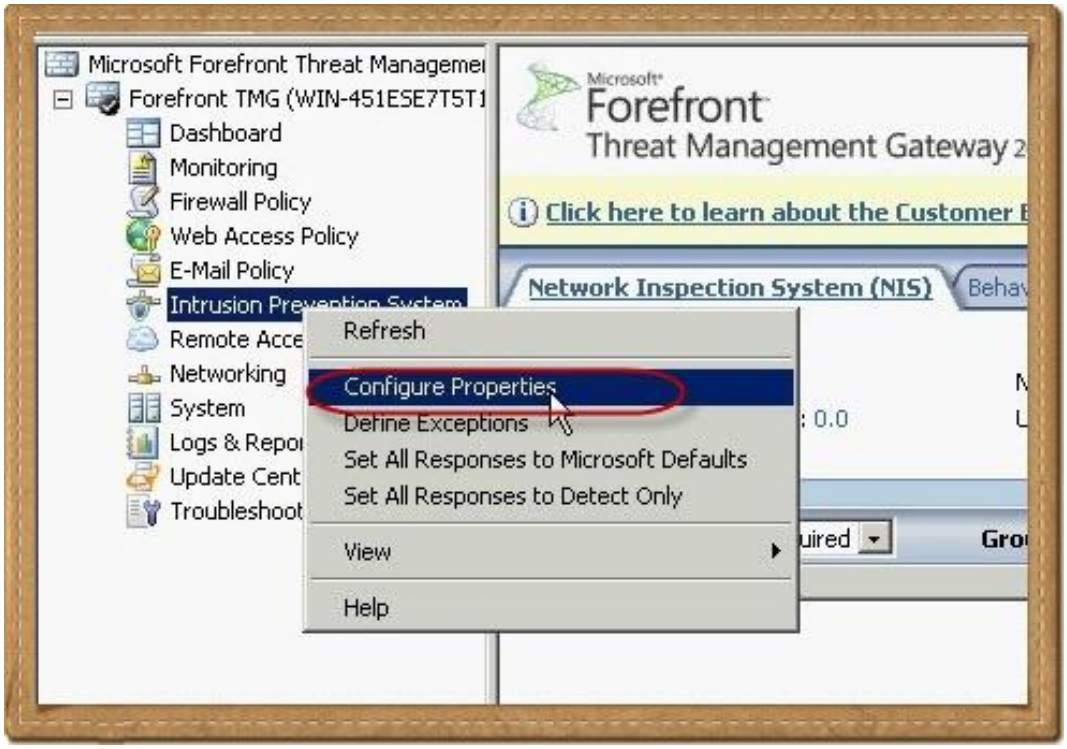
ومهمته الأساسية محاولة حماية الشبكة من هذه الهجمات

وده بيركز على أسلوبين أو جزئين :

Intrusion Detection

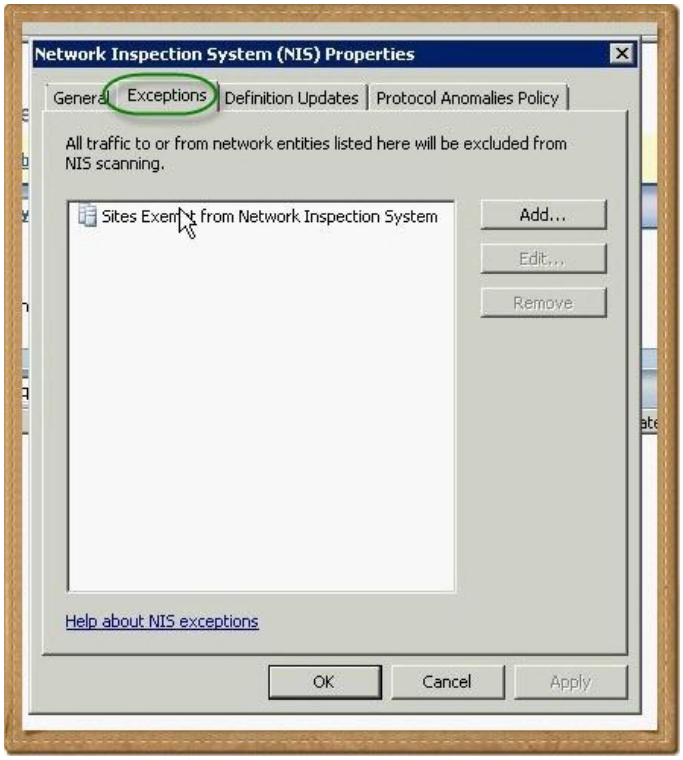
Network Inspection System (NIS)

كليك يمين على Intrusion Prevention System **ونختار** Properties

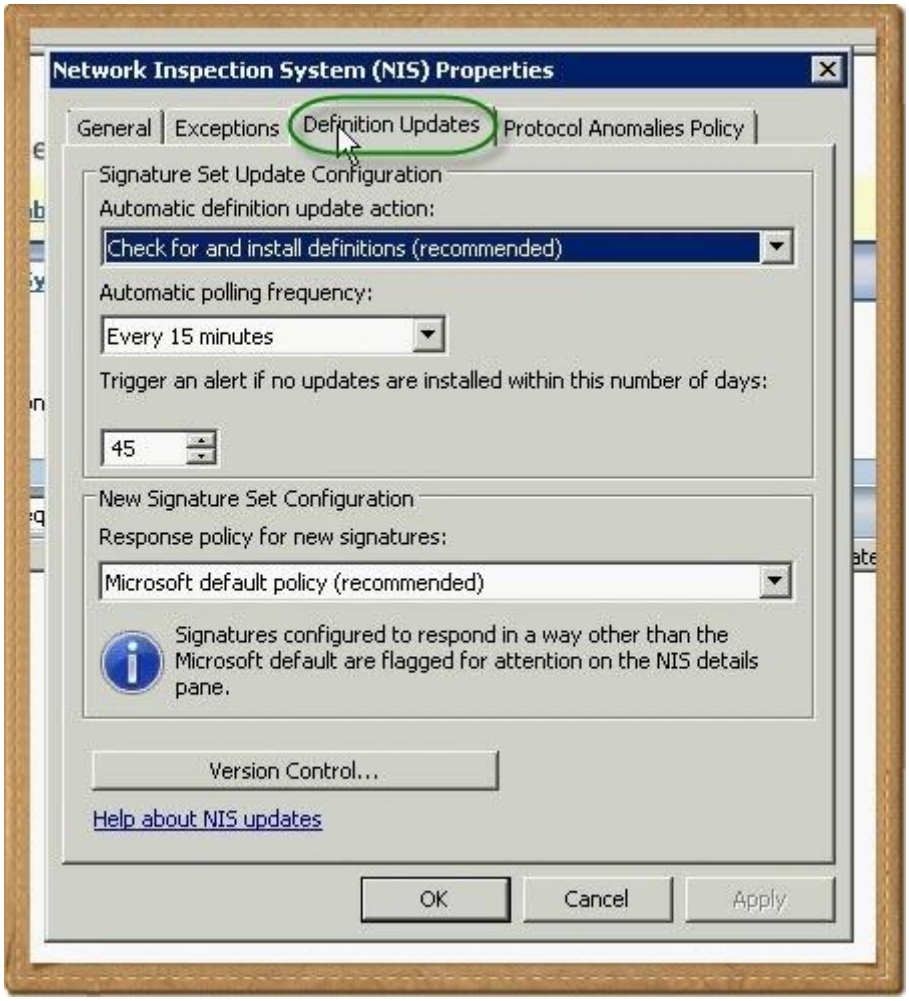


ثم Enable للـ Network Inspection System أو NIS

نقدر نستثني من الـ Inspection أي نيتوورك



أو نغير إعدادات الأبديت



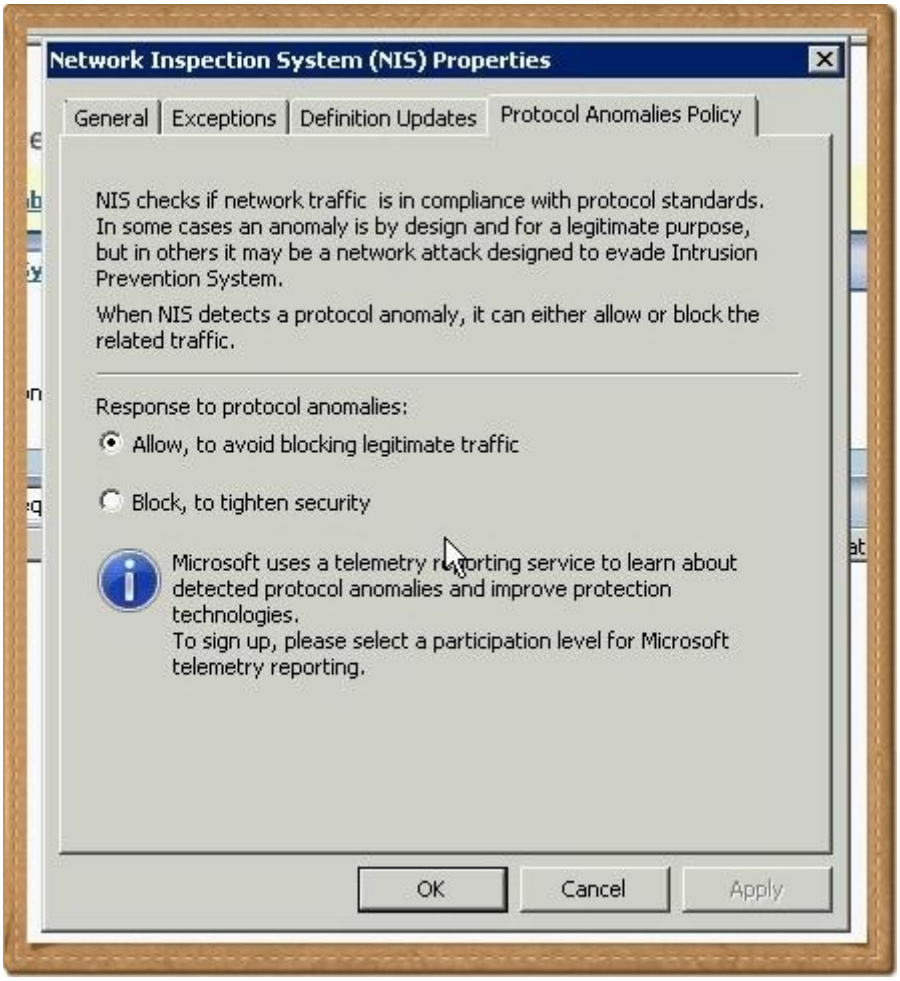
ومن هنا بنحدد سلوك الـ NIS مع البروتوكولات الغير مطابقة للمعايير قياسية وكيف سيتعامل معها بـ Allow أو Block

والفكرة هنا تتعلق بهذه البروتوكولات فقد تكون سليمة وغير ضارة ولكن بها بعض الشذوذ نتيجة خطأ من المطور أو عن قصد وقد تكون هذه البروتوكولات ضارة

فإذا سمحت بها فسوف يقلل هذا الترافيك وفي المقابل قد يعرضك للخطر

وإذا منعتها فسوف ترفع درجة الحماية ولكن قد تعطل برامج تتعامل معها

ويبقى القرار لك

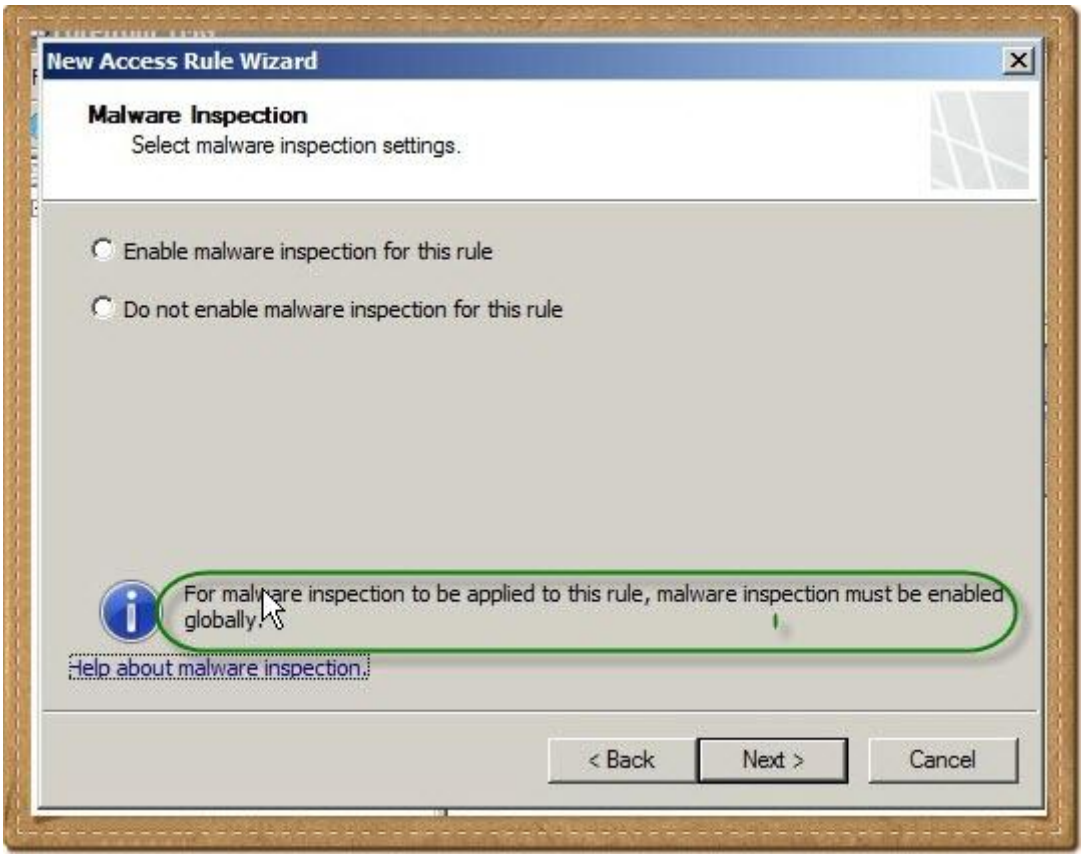


Malware Inspection

عند عمل الـ Rule سألنا المعالج عن خيار Malware Inspection

وقتها إخترنا Don’t enable for this rule

وكما هو واضح بالملاحظة أنه لتفعيل malware Inspection للرول يجب تفعيلها أولا على مستوى السيرفر ككل



تعالوا نتفسح شويه في الـ TMG ونشوف إزاي نفعل Malware Inspection على مستوى التي إم جي

وإزاي نتحكم فيها وبعدها ممكن لو أردنا أن نفعلها عندإعداد الرولز

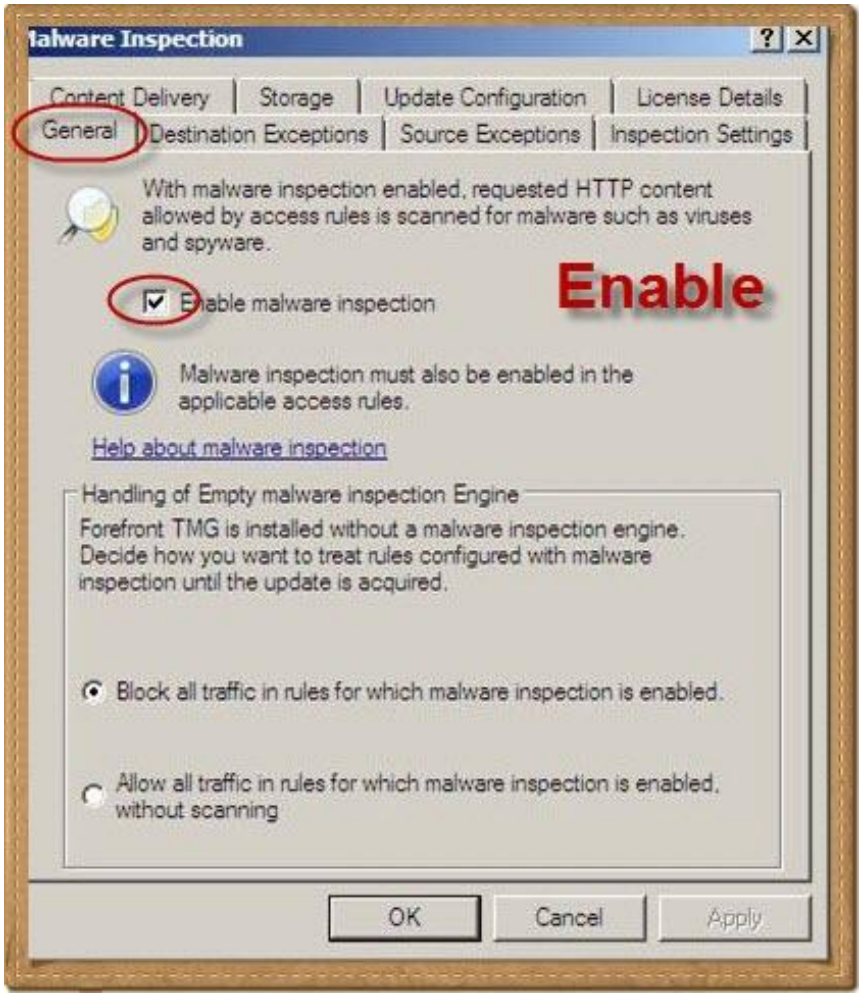
على اليسار نختار Web Access Policy

ثم إلى أقصى اليمين

ومن tasks

نختار Configure Malware Inspection

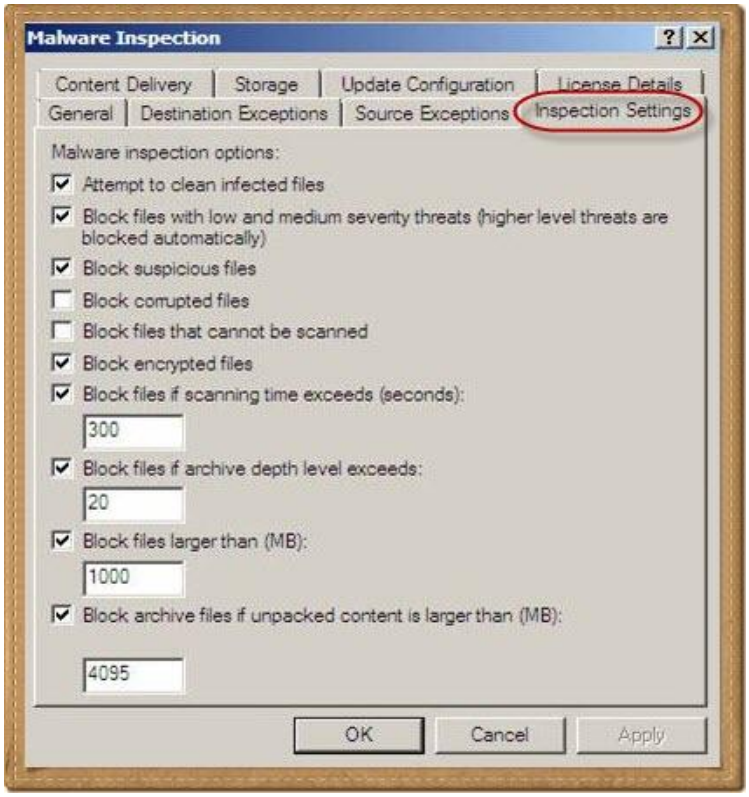
من هنا نختار Enable لتفعيلها للسيرفر



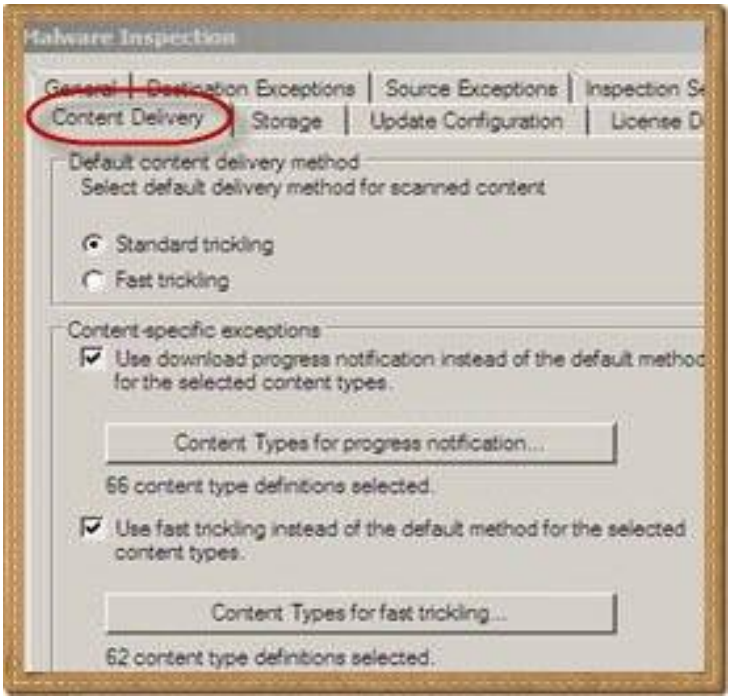
Add Exceptions

وهنا تكون في الإتجاهين Destination و Source فيوجد تبويب Tab لكل منهما

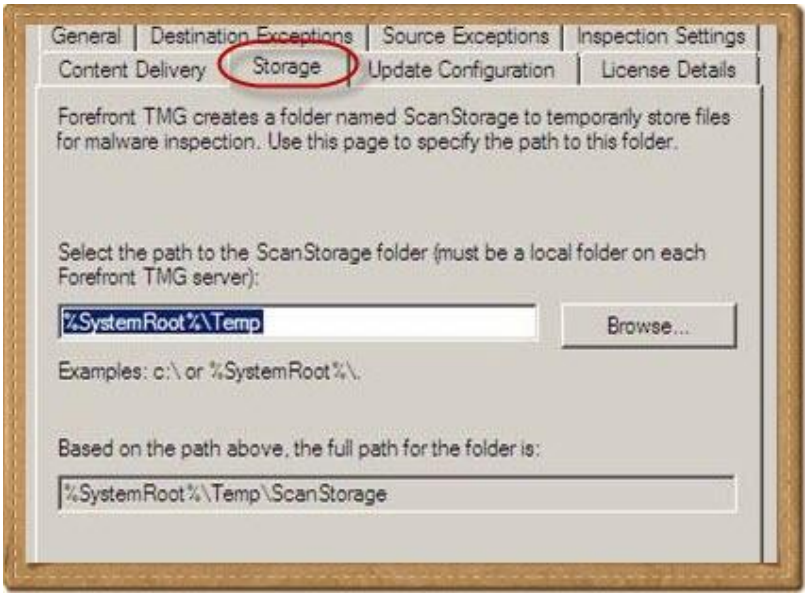
إعدادات التشغيل



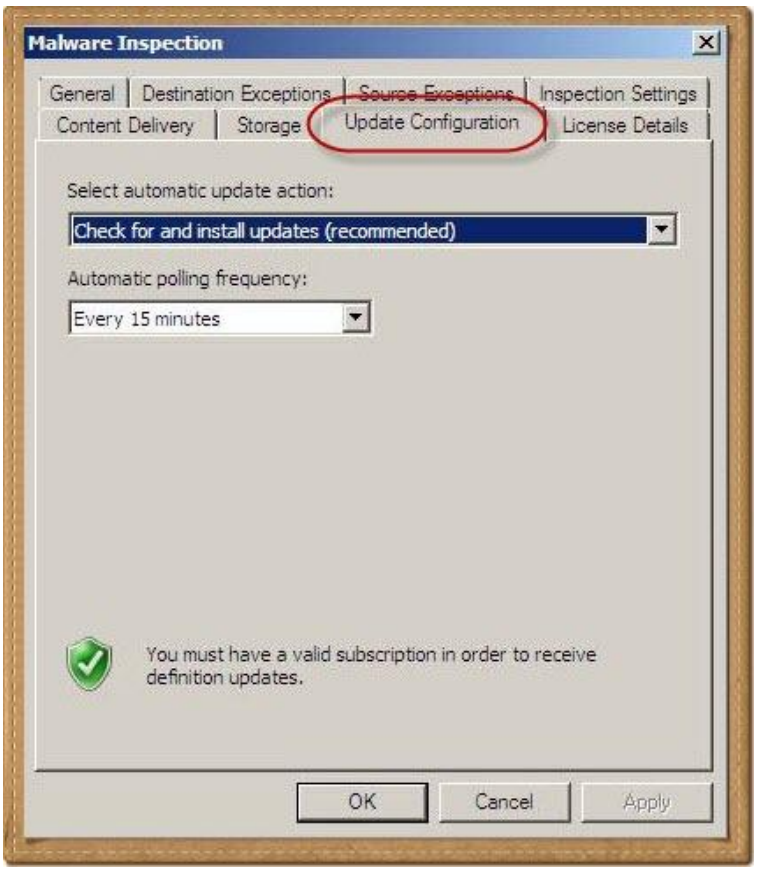
كيف يتم التعامل مع العناصر التي يتم فحصها



مكان الفولدر المؤقت الذي سيتم وضع الملفات فيه أثناء فحصها



إعدادات الأبديت



والكلام اللي يزعل , إنها محتاجه License خاصه بيها

عموما بالنسبة لتفعيل NIS و Malware Inspection فإذا كان الكونيكشن عندك بطيء أوعدك

إنه ح يزداد بطء وستقضي عمرك في إنتظار السنين وصبر التنين ☺

Networks, Protocols, Users

أثناء إنشاء الرول قابلنا إختيارات تتعلق ببعض العناصر مثل

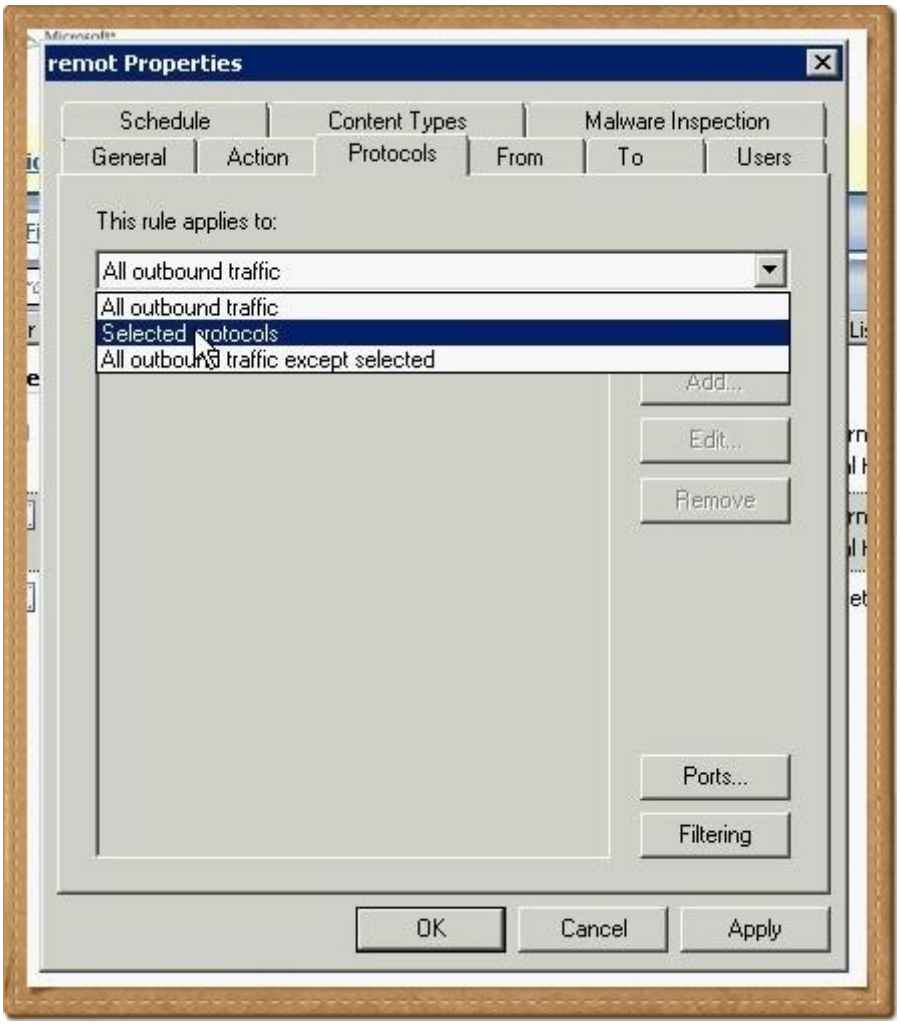
البروتوكولز Protocols

و النيتووركس Networks

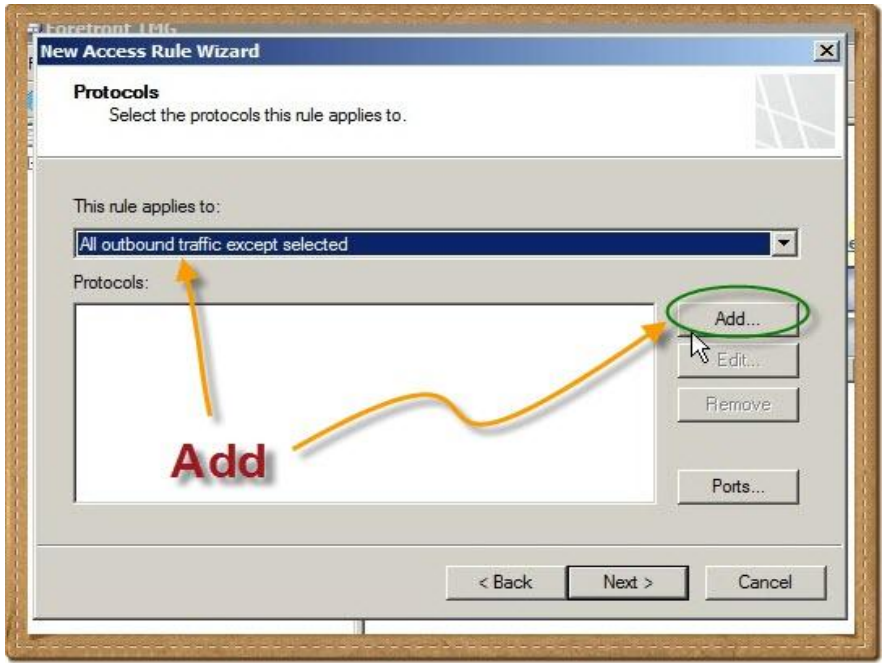
و اليوزرز Users

فعلى سبيل المثال هنا يسأل عن أي البروتوكولات سينطبق عليها الرول أو لن يطبق عليها ,

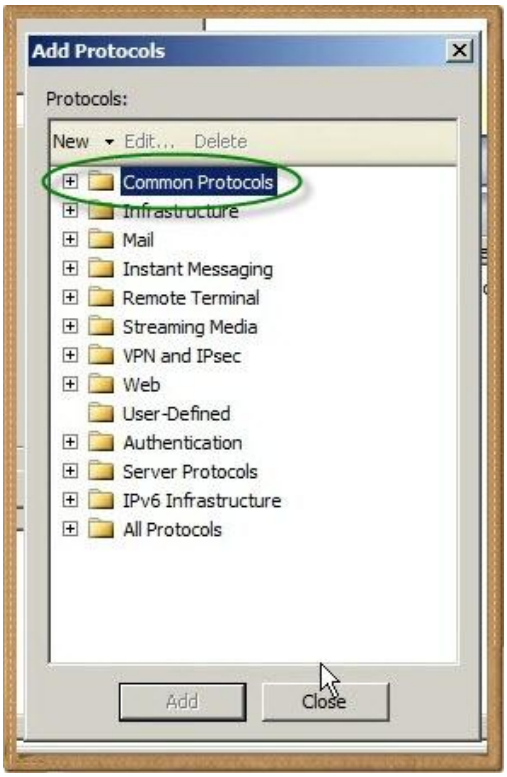
وكما شرحنا فإنه هناك ثلاثة إختيارات



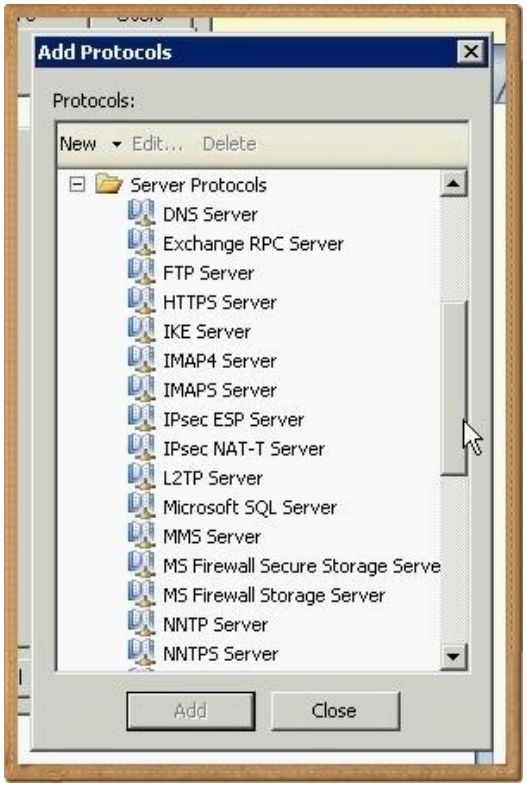
إذا إخترنا على سبيل المثال إستثناء بعض البروتوكولات من تطبيق الرول فبالطبع يجب أن أحدد هذه البروتوكولات بالضغط على Add



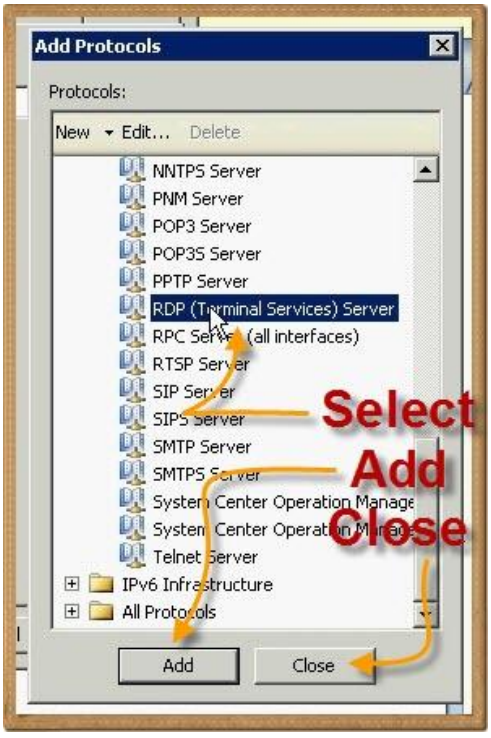
ومن ثم إضافة هذه البروتوكولات من خلال Common Protocols



وإختيار البروتوكولات



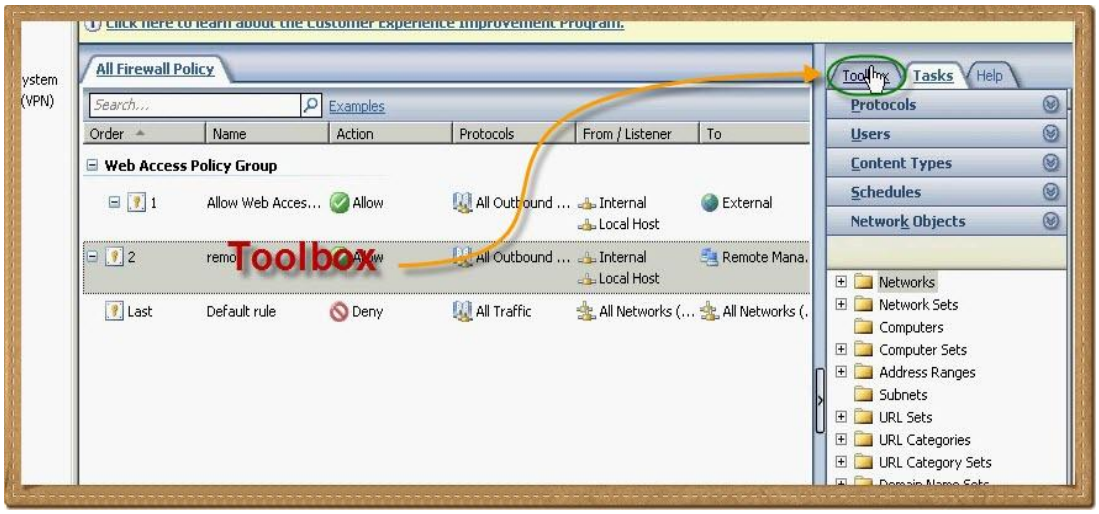
ثم إغلاق النافذة بعد الإختيار



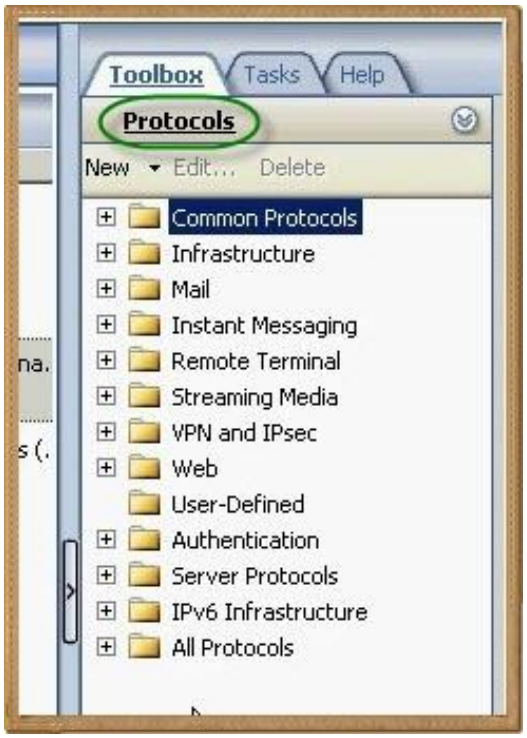
- *سؤال : هل يمكن إدارة قائمة البروتوكولات ؟*

نعم وباقي العناصر أيضا

على اليمين نختار Toolbox سنلاحظ أن كل مجموعات العناصر وتصنيفها موجوده



فمثلا هنا الـ Protocols

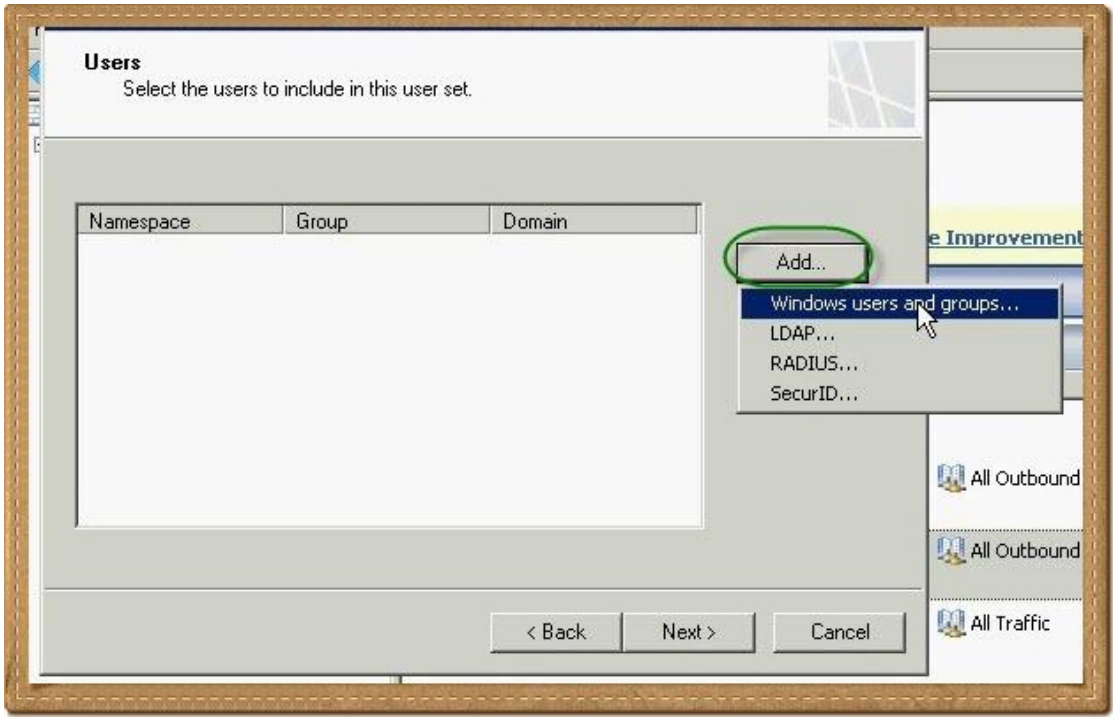


وايضا من هنا يمكننا إضافة المستخدمين وتصنيفهم في مجموعات

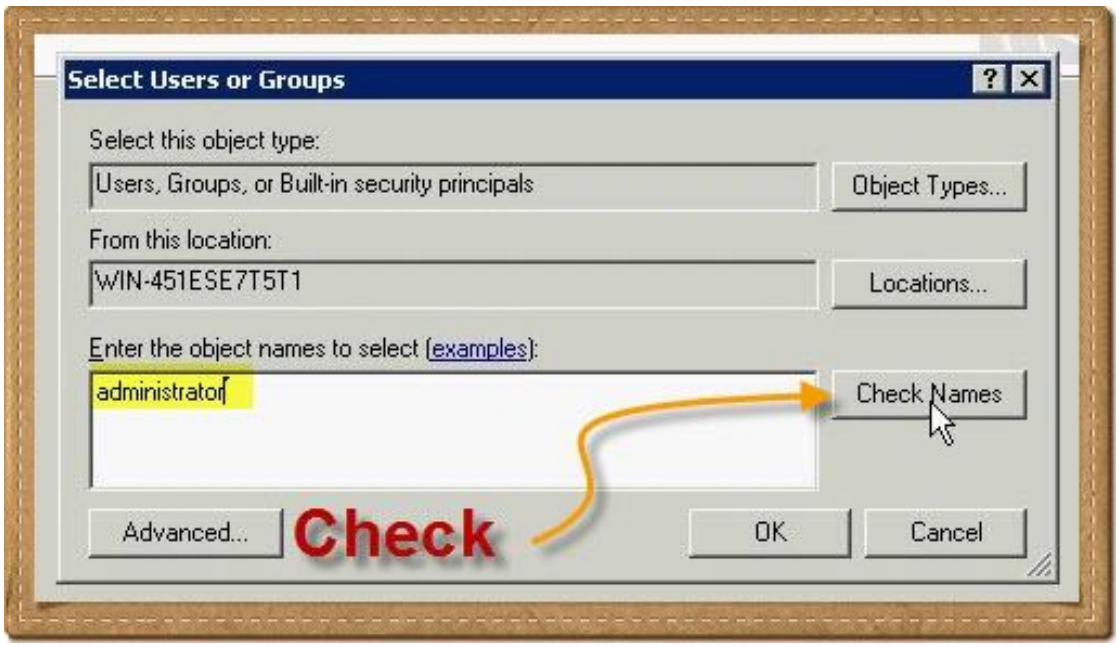
نختار New

نختار إسم للمجموعة

ثم Add Windows Users and Groups



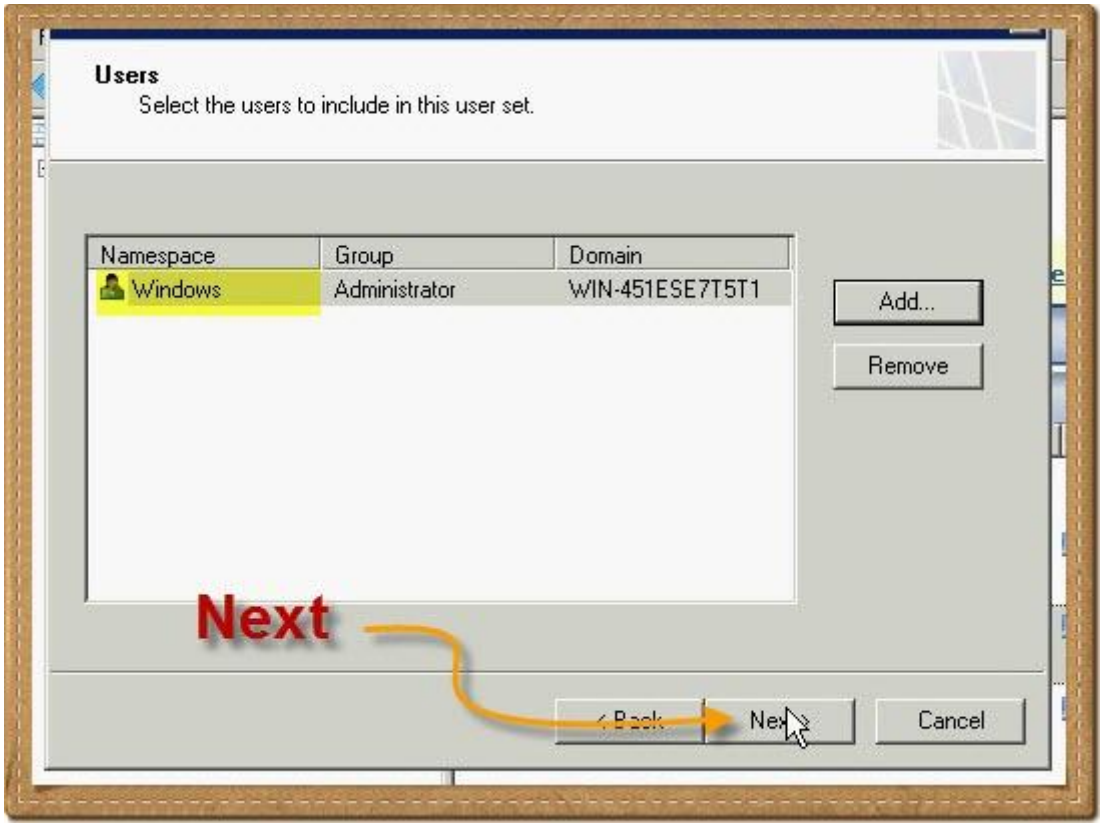
نبحث عن المستخدمين



ثم Ok

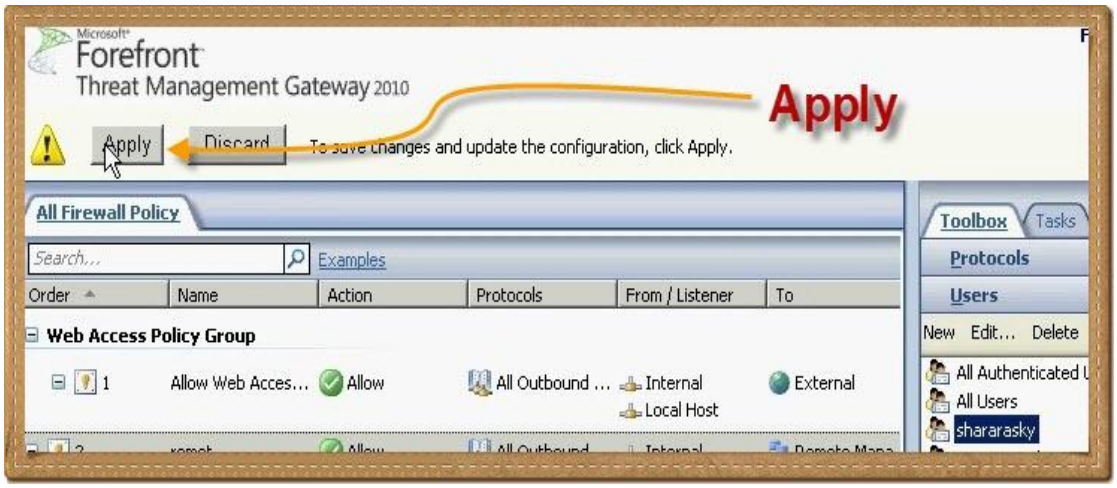

Select Users or Groups
Select this object type:
Users, Groups, or Built-in security principals
Object Types...
From this location:
WIN-451ESE7T5T1
Locations...
Enter the object names to select (examples):
WIN-451ESE7T5T1\Administrator
Check Names
Ok
Advanced...
OK
Cancel

ثم Next

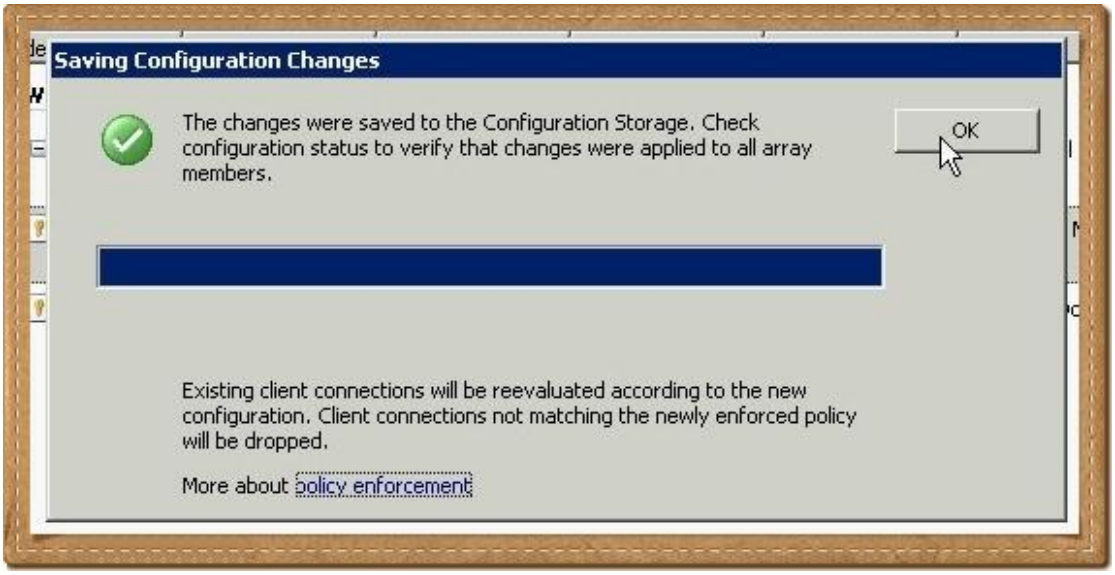

Users
Select the users to include in this user set.
Namespace
Group
Domain
Windows
Administrator
WIN-451ESE7T5T1
Add...
Remove
Next
< Back
Next >
Cancel

و Finish

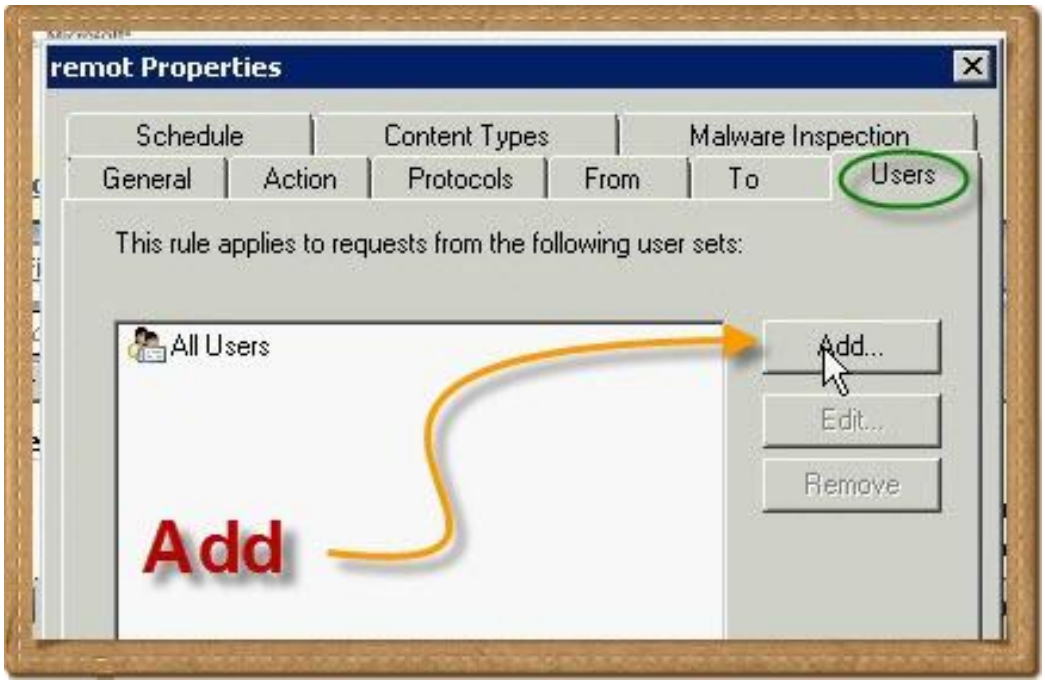
وأخيرا Apply



تم التفعيل



والآن كلما تعاملنا مع الخيارات الخاصة بالمستخدمين



سنجد المجموعة التي أنشأناها ويمكننا إستخدامها

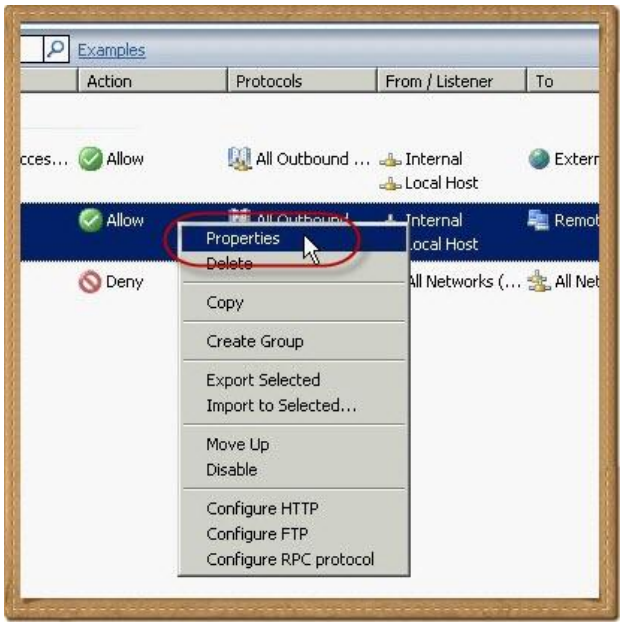
مجموعة shararasky

من هنا أيضا يمكننا إضافة أنواع ملفات أو إعادة تصنيفها في مجموعات

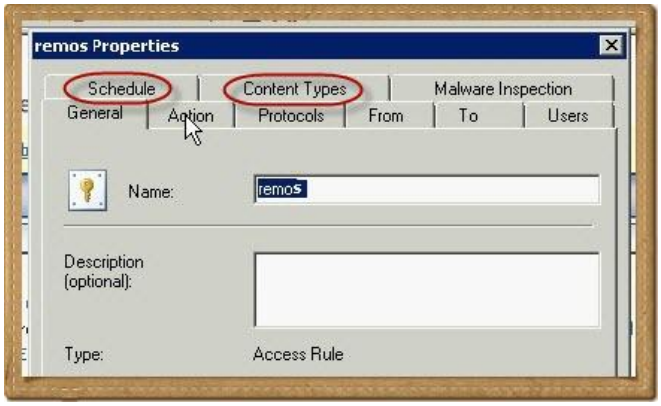
بالطبع ذلك بنفس الطريقة السابقة فنقم بإختيار New كما يمكننا أن نختار أي مجموعة ونضغط على Edit لتعديلها

Rule Properties

بعد إنشاء الرول وتنشيطها يمكننا تعديلها , كليك يمين على الرول ونختار Properties



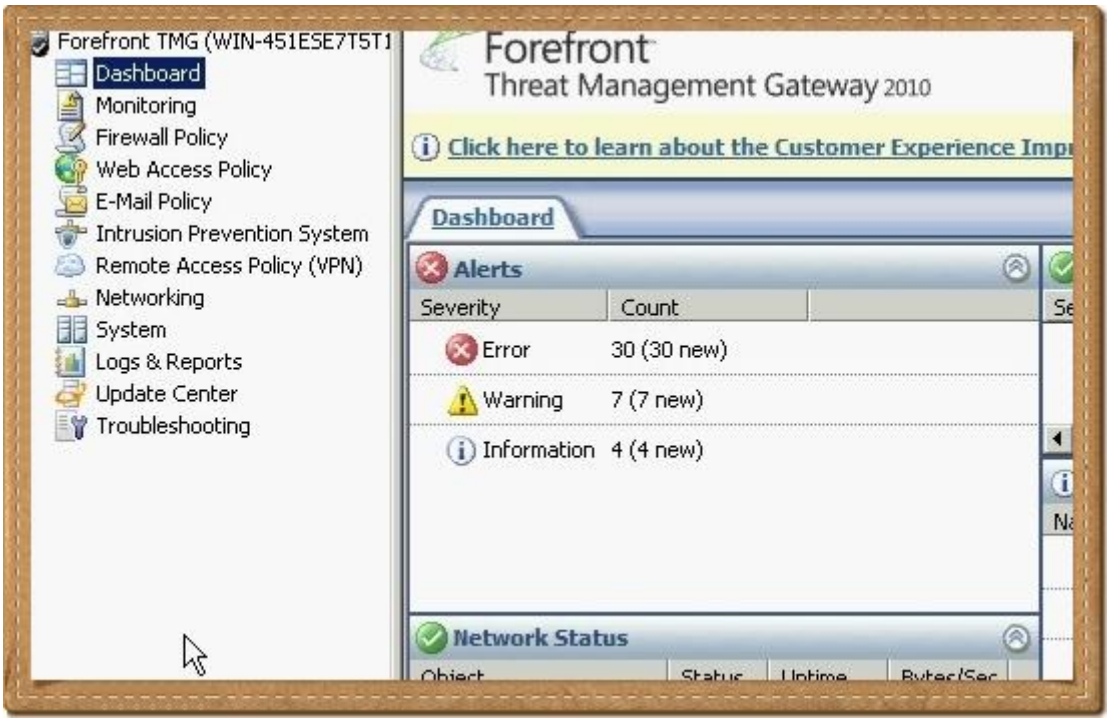
نلاحظ وجود تاب هامه جدا وهي Content Types وهي تتيح لنا أن نمنع أنواع معينة من الملفات أو نسمح بها حسب طبيعة الرول Allow أو Deny



كما توجد إمكانيه لربط ساعات عمل الرول من خلال وضع جدول زمني Schedule لها عن طريق Schedule Tab

Dashboard

نافذة خاصة بعرض الإيفنتس Events واللوجز Logs التي تهم أدمين السيرفر



Monitoring

عرض التنبيهات الخاصة بالسيرفر مثل التنبيهات Alerts وحالة الخدمات Services

بالطبع لم نتطرق إلى كل إمكانيات الـ TMG ووظائفه ... شدوا حيلكم وتطرقوا أنتم بدون كسل وبقليل من الجوجوله

هذا الجزء كان هو الأخير الخاص بشرح TMG ولكنه ليس الأخير المرتبط به

فمن الفصل القادم إن شاء الله سنبدأ العمل مع برنامج هام جدا لإدارة TMG وهو برنامج GFI Web Monitor وهو برنامج رائع وسهل جدا وستستغني به إذا أردت عن الكثير من وظائف TMG

والله الموفق والمستعان

اللهم إني أعوذ بك أن أشرك بك شيء أعلمه , وأستغفرك لما لا أعلمه

سبحانك اللهم وبحمدك , أشهد ألا إله إلا أنت , أستغفرك وأتوب اليك

الفصل الرابع : GFI Webmonitor

التنصيب

خُد فكرة

GFI Webmonitor

التنصيب

الحمد لله والصلاة والسلام على رسول الله

مما لا شك فيه إن الـ TMG كفاير وول وبركسي رزل للغايه والرزالة دي سلاح ذو حدين

فمن ناحية جيده : لتوفيره الحماية الكافية للشبكة ضد أخطار عدة كما شرحنا

ومن ناحية سيئة : صعوبة تعامل الأدمينيستراتور معه و مع مصطلحاته المعقدة

وبخاصة إذا وجدت نفسك مضطرا للتعامل مع جمل من نوعية : الباك فرونت لما بيكونكت على الفرونت إند بيحصل كوليجن في الجلوبال بوليسي وده لازم تستعمل معاه شيربوينت علشان تواجه الأتاك

ما اعرفش بصراحه إيه حكاية طفلي مايكروسوفت اللي بينطوا قدامنا كل ما نفكر نتعامل مع منتجاتها : SharePoint – SQL Server

طبعا الخزعبلات ح تزيد في النهاية الخاصة بالإيميل لما نتعامل مع Exchange وساعتها ح يزيد إحساسك بإن منتجات مايكروسوفت أصبحت غاية وليست وسيلة

برضه مش ح نقطع في فروة مايكروسوفت وخلينا في نفسنا

من مميزات TMG ومن قبله ISA هو وجود باقة طيبة من المنتجات تتعامل معه ومع وظائفة وهي ما تفضل مايكروسوفت أن تطلق عليهم Third Party

بعض هذه المنتجات تتخصص في عرض تقارير لإستخدام الـ TMG وسلوك المستخدم

و بعضها الآخر يستفيد من رزالة TMG كسيرفر Gateway مع تبسيط عمليات الفلتره والتحكم في الرولز والبعض الآخر يقوم بالمهمتين وأشياء أخرى ومنها GFI Webmonitor يعني نقدر نقول بيستفيد من الـ Engine ويتخطى الواجهة و بيعمل تقارير وكمان سكان للفايروس فوق البيعه

وهو ما سنشرحه في هذا الباب لأهميته.

البرنامج GFI Webmonitor for ISA and TMG وهو من إنتاج شركة كبيييرة جدا ولها منتجات رائعة للشبكات وهي شركة GFI , بجد يا شباب كل ما بادخل موقع الشركة دي ممكن أقضي ساعات أتفرج على منتجاتها الرائعة

ممكن يكون كتير منكم ماسمعش عنها وللأسف دي مشكلة تربية مايكروسوفت ومصطلحها المريب : Third Party

عموما في أكثر من شركة رائعة بتقدم منتجات قوية جدا للشبكات منها :

GFI – Emco – Kerio - Pointdev

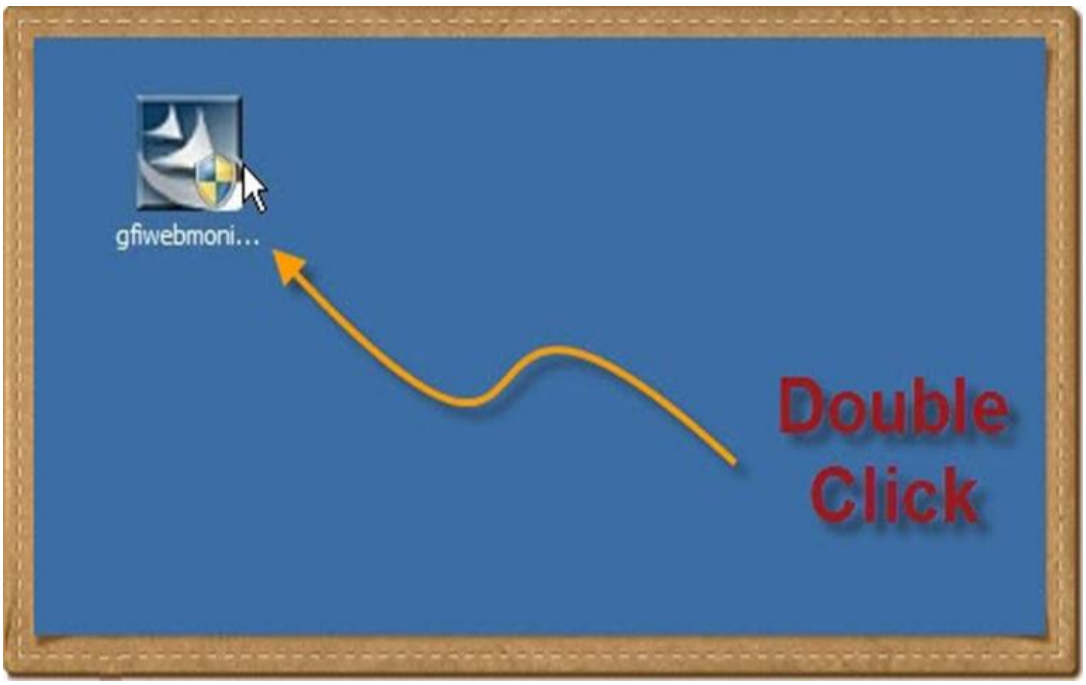
ممكن تضيعوا من وقتكم الثمين ساعة أو إثنين وتاخدوا فكره وتشتروا بكره

في إصدارات حديثة للبرنامج ولكن في الشرح سأعمل على إصدار قديم لسبب بسيط هو إني لم أتوصل إلى نسخ أحدث مكركره ☺

ولنبدأ على بركة الله

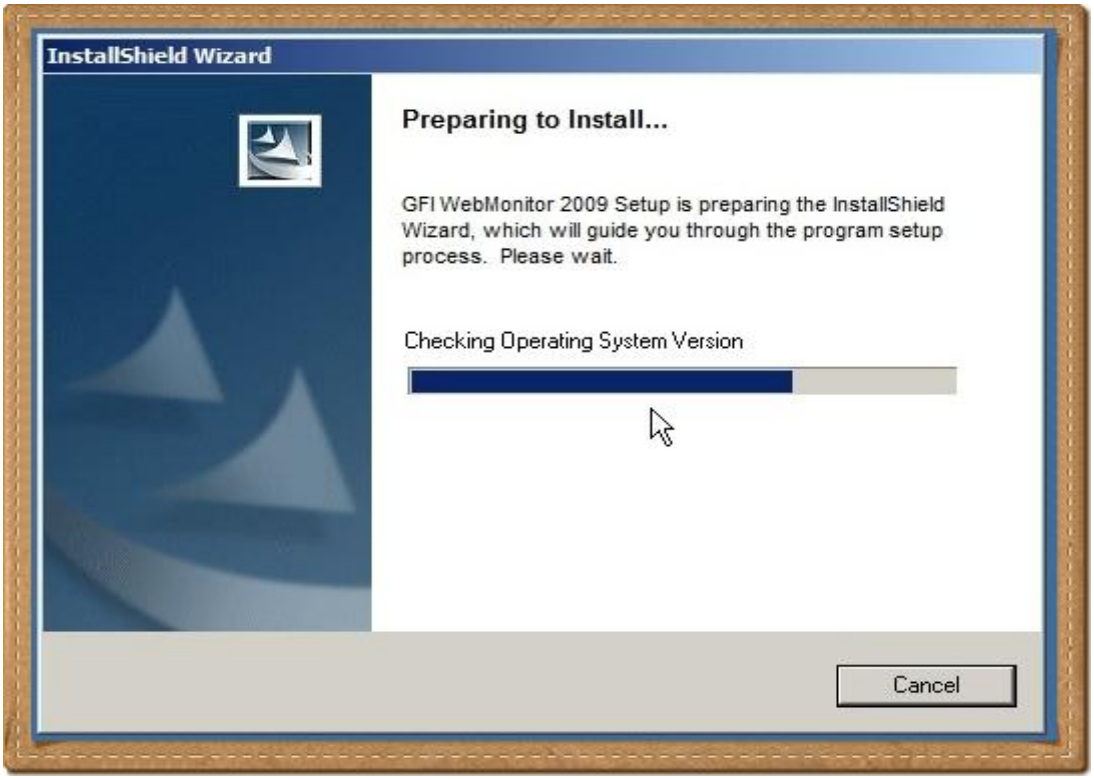
طبعاً الـ GFI يتم تنزيله على الـ TMG Server

.... دابل كليك



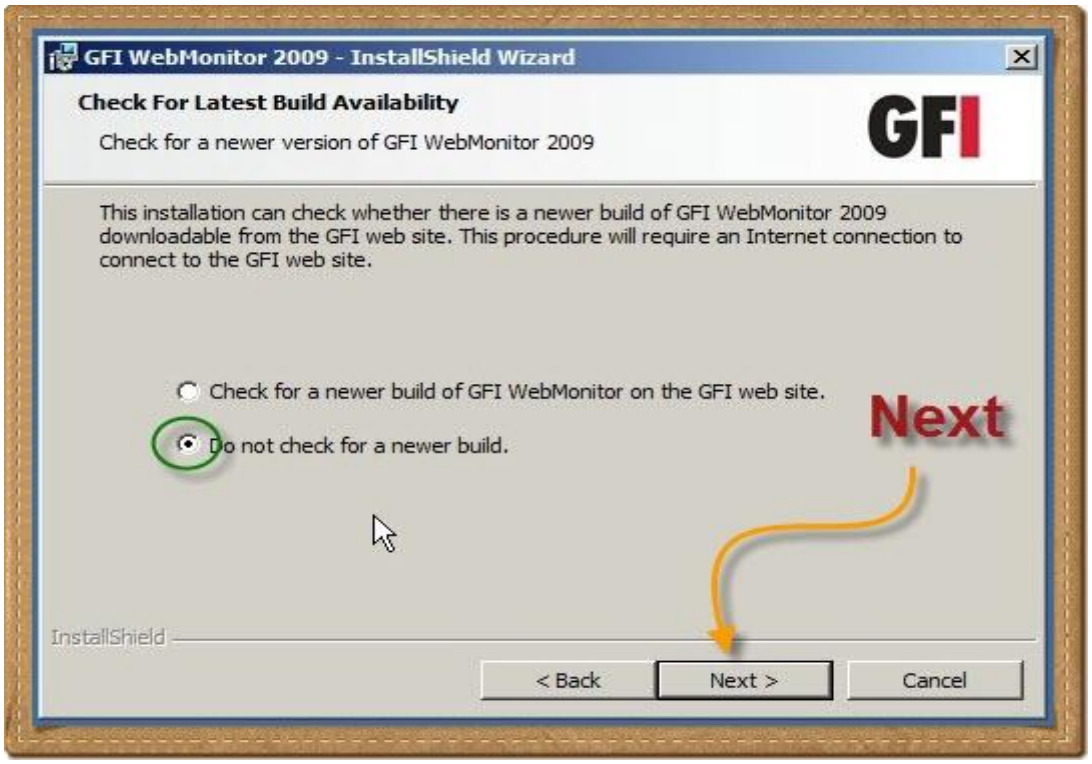
وطبعا Yes

ونسيبه يـ Checking براحته

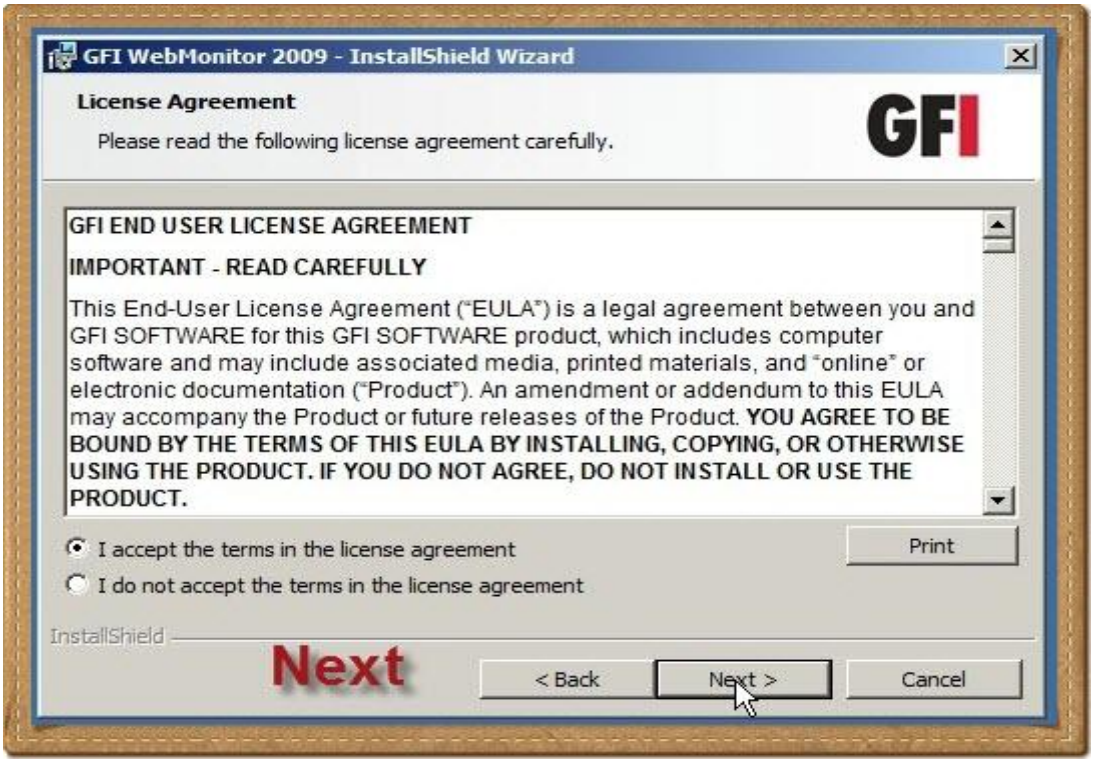


و Next

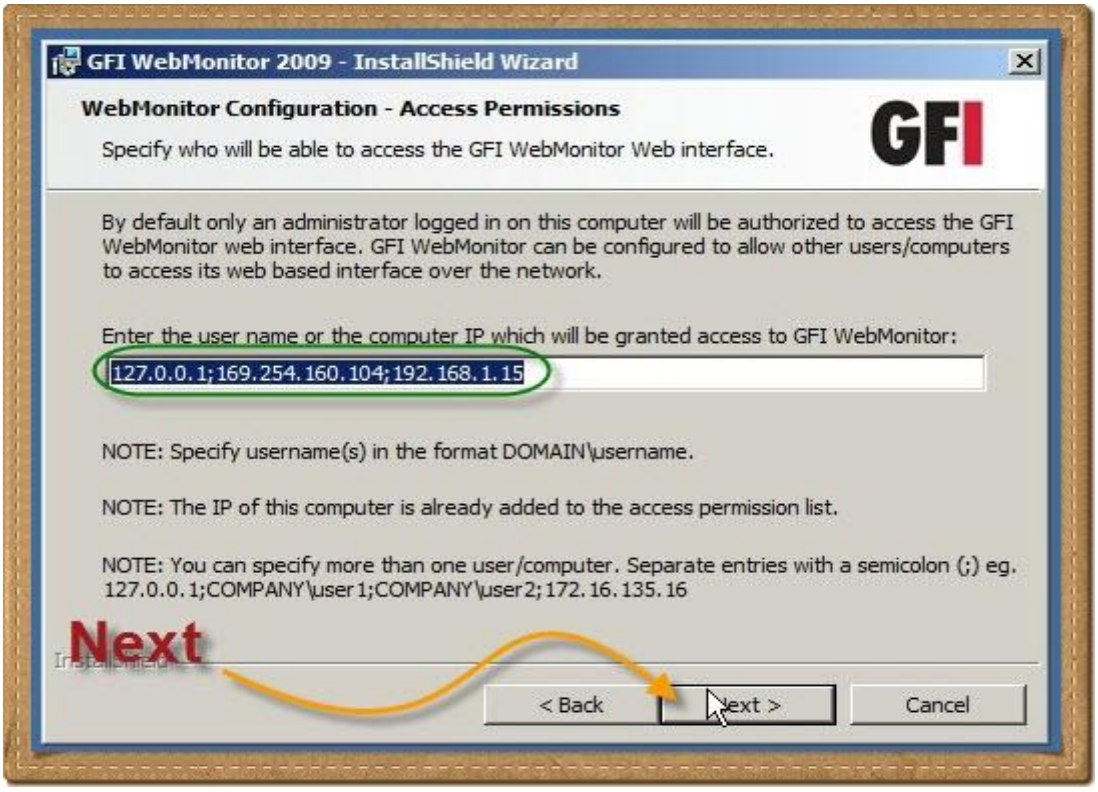
وبلاش يدور على أبديت إلا لو إنت في السليم و مالكش في المكركر , ثم Next



نقبل الإتفاقية و Next

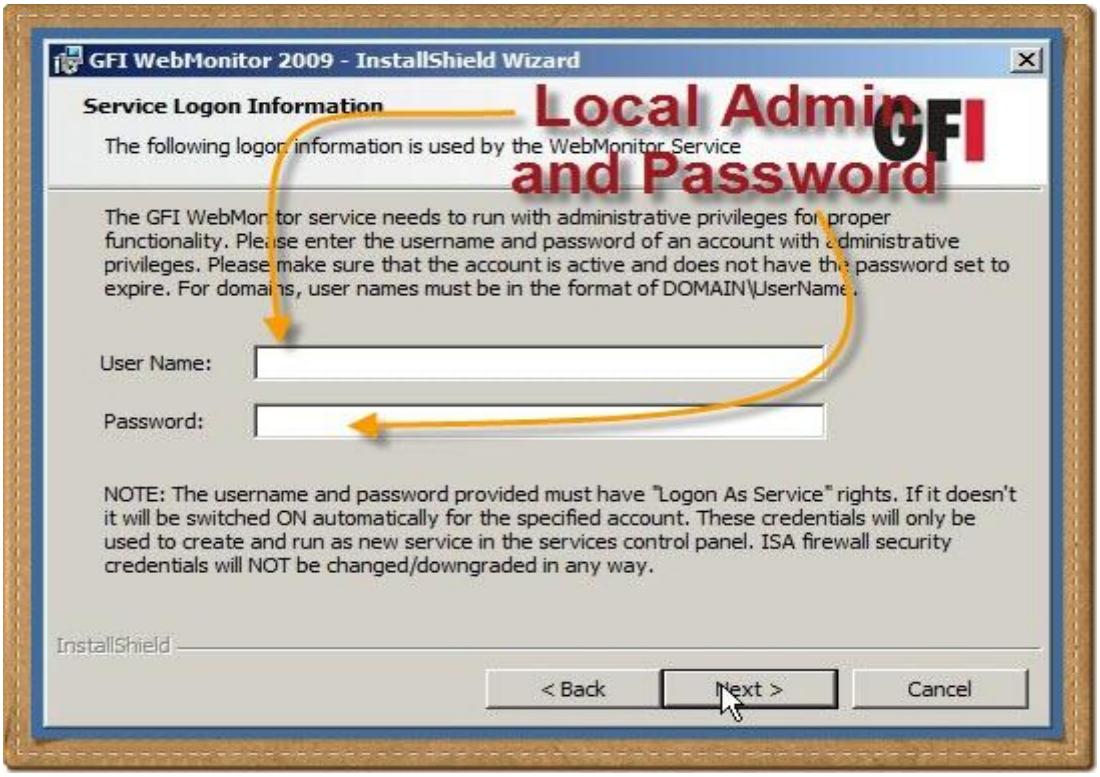


الـ اي بيهات الخاصة بالأجهزة اللي ح تدير منها الـ Server ريموتلي وممكن نعدلها بعدين

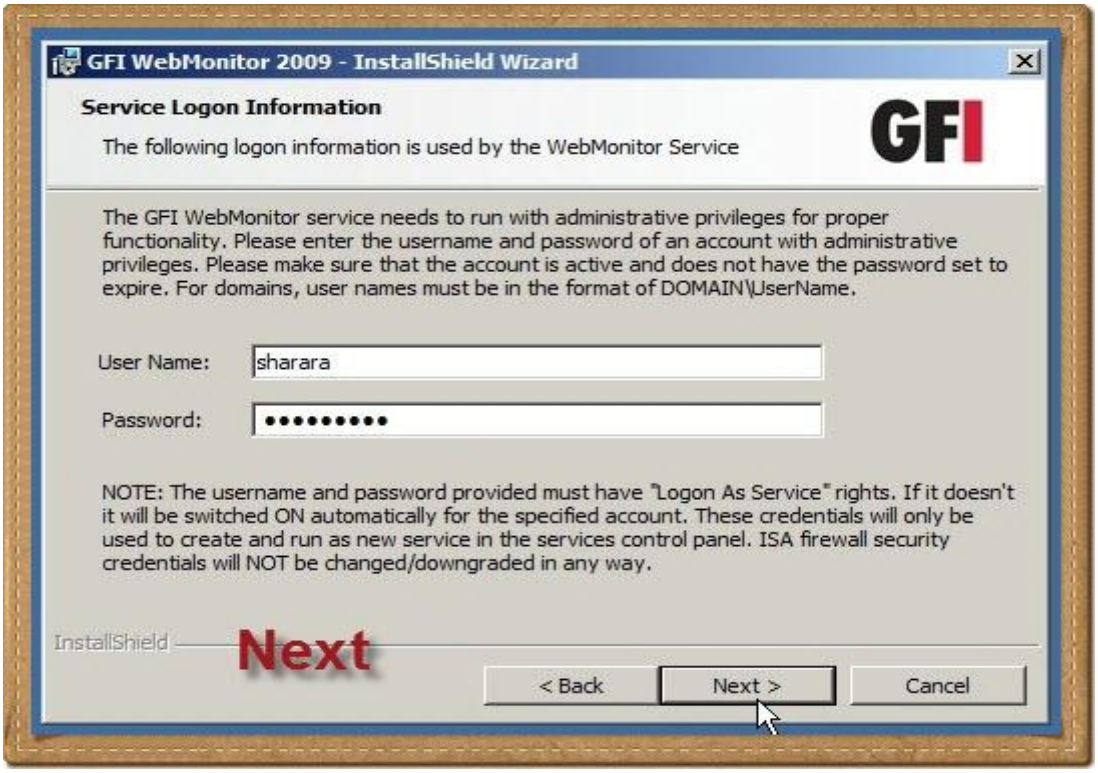


المهم هنا هو Serial النسخة ولو Trial ح يبقى مكتوب Evaluation , وبعدين Next

مهمة جدا : Administrator Username and Password للـ TMG Server



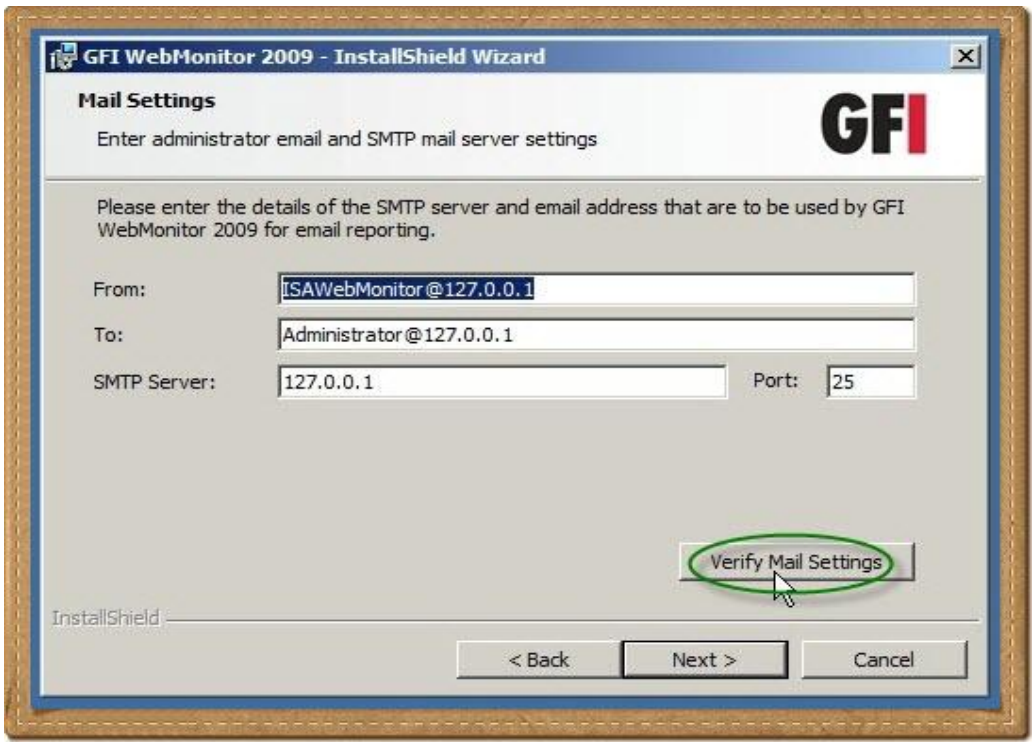
Next



لتفعيل خاصية إرسال إيميل للأدمين لإرسال التقارير نحتاج لإدخال بيانات سليمة

وبعد إدخال الإعدادات يمكننا التأكد منها من خلال الضغط على verify Mail Settings

لو مش عايزين أو مش عارفين أو ح نظبطها بعدين يبقى نكبر دماغنا وندوس Next



Next

Install


GFI WebMonitor 2009 - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
GFI
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
Install
InstallShield
< Back
Install
Cancel


GFI WebMonitor 2009 - InstallShield Wizard
Installing GFI WebMonitor 2009
The program features you selected are being installed.
GFI
Please wait while the InstallShield Wizard installs GFI WebMonitor 2009. This may take several minutes.
Status:
Unregistering COM+ Applications and Components
InstallShield
< Back
Next >
Cancel

وأخيرا Finish

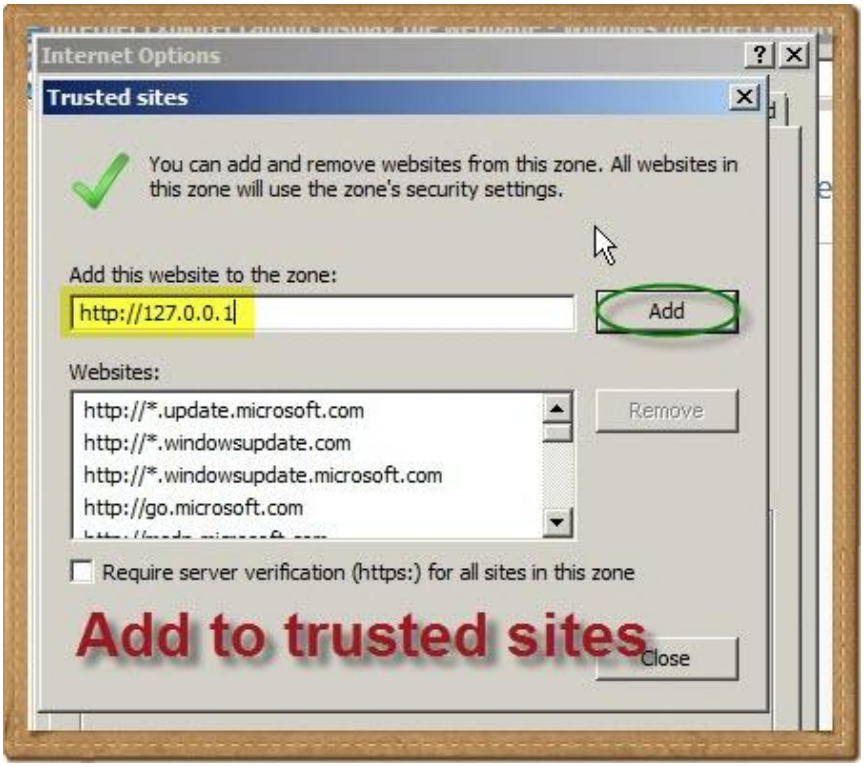
إنتهينا من الإعداد

وطبعا لإننا شغالين على Server 2008 وهو بالطبيعي بيقفل كل حاجة فالأمر قد يحتاج قبل أن نحاول الدخول على واجهة الـ جي إف أي إننا نعمل حركة صغيرة

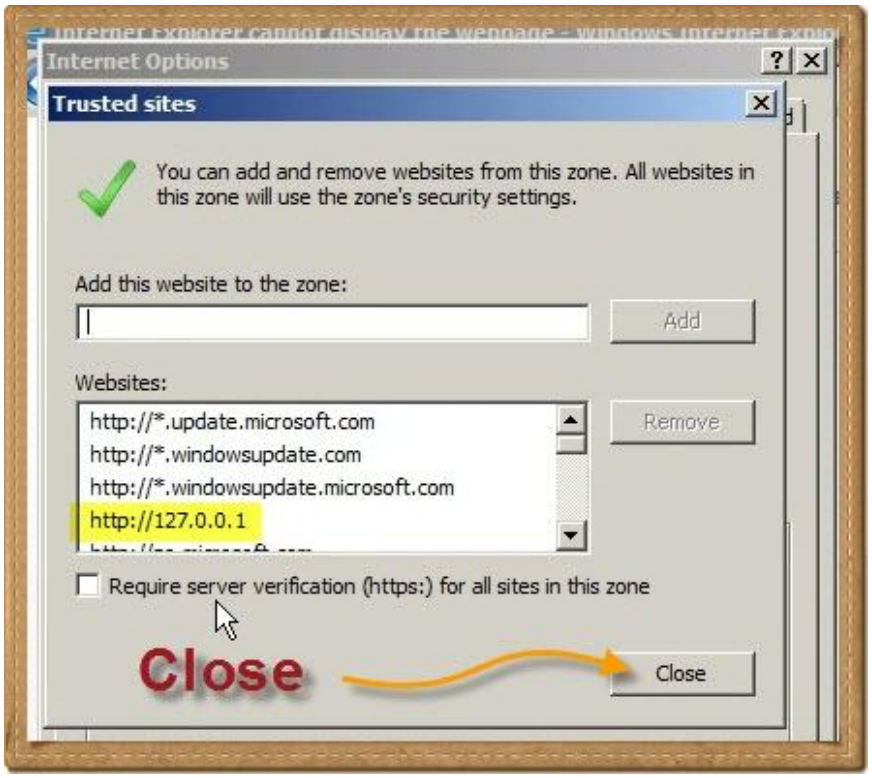
من الإنترنت أوبشن

في Security Tab نختار Sites ثم نضغط على Sites

وإضافة الـ Localhost IP وهو 127.0.0.1 للـ Trusted Sites



ثم Close



و Ok

والآن للدخول على واجهة برنامج GFI Webmonitor

نفتح المتصفح ونذهب إلى monitor.isa أو 127.0.0.1:1007

كما يمكننا الدخول أيضا من خلال الـ Shortcut الخاصة بالبرنامج في قائمة البرامج

يمكننا الدخول على واجهة GFI من أي جهاز بالشبكة شريطة أن يكون متاح له ذلك ثم نكتب الـ اي بي الخاص بالـ TMG مع رقم البورت الخاص بـ GFI وهو 1007 في المتصفح أو بكتابة monitor.isa في المتصفح

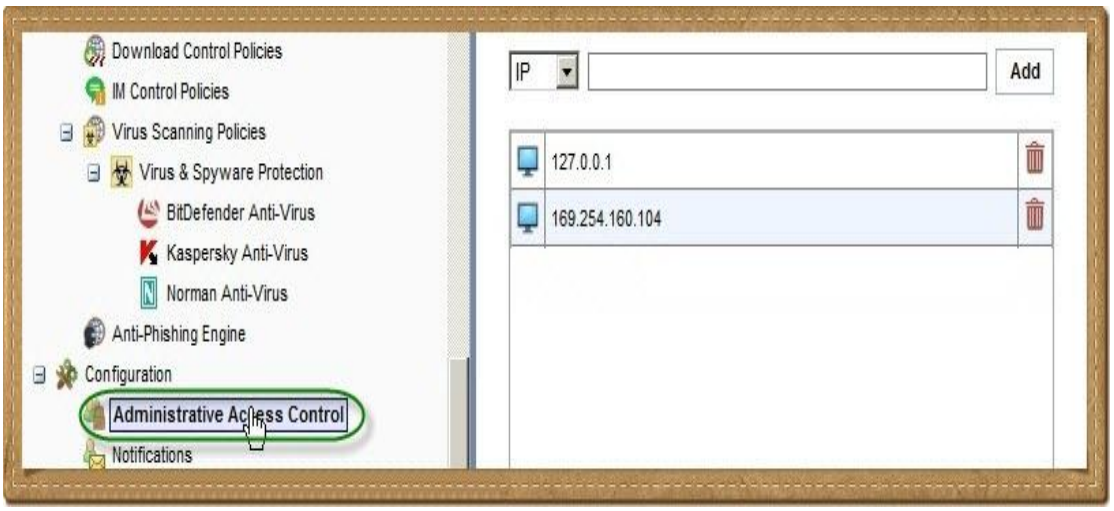
قد لا تعمل هذه الطريقة فلا تضيع وقتك وببساطه يمكنك الدخول عن طريق ريموت ديسك توب كونيكشن كما شرحنا من قبل

أول ما يواجهنا

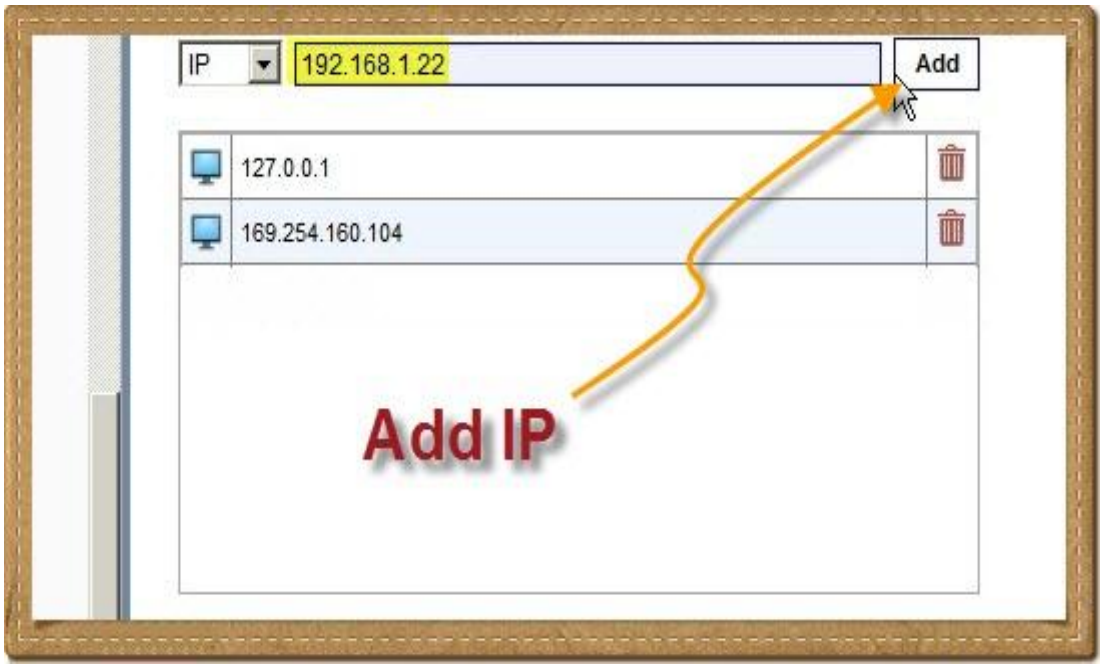
قبل أن ننتهي من هذا الدرس نتعرف سريعا على كيفية إضافة تصريح لبعض الأجهزة لإدارة GFI من خلالها

على اليسار من Configuration

نختار Administrative Access Control

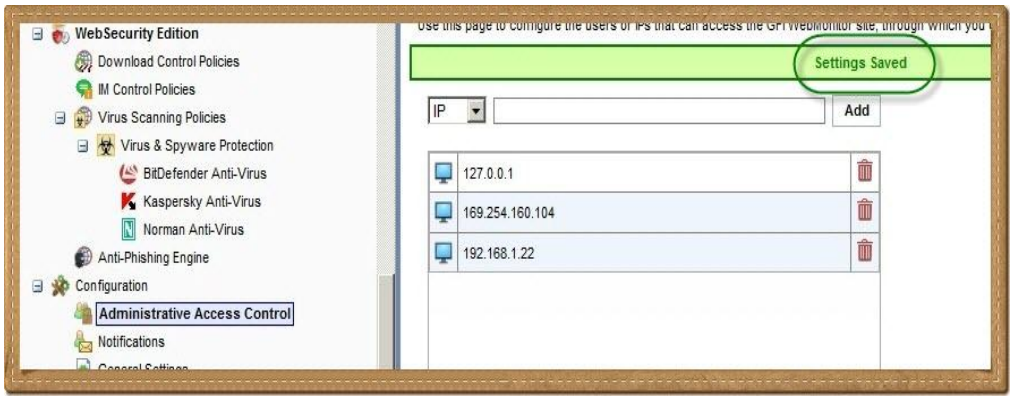


ثم نضيف الـ IP الخاص بالجهاز الذي نريد الدخول منه ريموتلي على GFI لإدارته



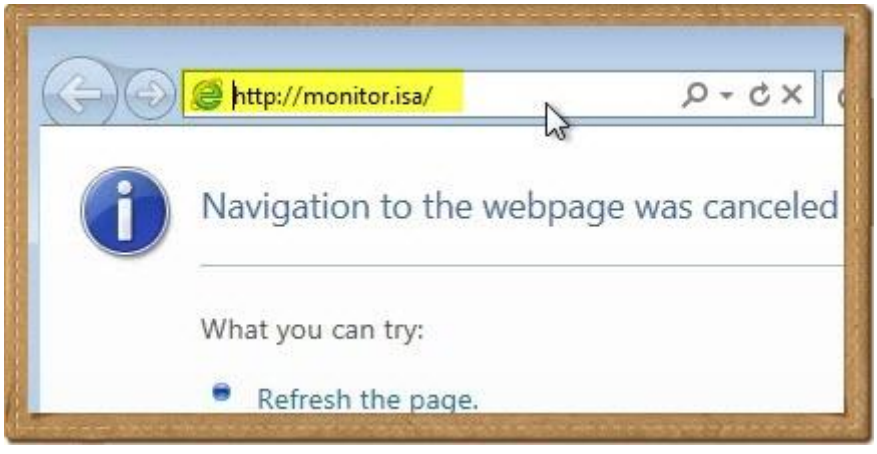
و Save Settings

تم الحفظ ونرى بالأسفل الأجهزة التي لها حق إدارة GFI



وكما قلنا يمكن الدخول من المتصفح عن طريق رقم الـ اي بي الخاص بالسيرفر أو كتابة monitor.isa

والأسهل والأضمن Remote Desktop



وكفايه كده

ونكمل إن شاء الله في الصفحة الجاية

اللهم إني أعوذ بك أن أشرك بك شيء أعلمه

وأستغفرك لما لا أعلمه

سبحانك اللهم وبحمدك , أشهد ألا إله إلا أنت , أستغفرك وأتوب اليك

GFI Webmonitor

خُد فكره

الحمد لله والصلاة والسلام على رسول الله

سيدنا محمد , وعلى آله وصحبه ومن والاه

عندما بدأنا العمل على TMG لاحظنا أنه أنشأ By Default رول قافله كل حاجه , إحنا ماسكتناش وعملنا بعدها Rule فاتحه كل حاجه

ح نوقف شريط الـ TMG هنا ومش ح نعمل رولز جديدة عليه ولكن سنوكل هذه المهمة للـ GFI

بعد الإنتهاء من تنصيب GFI Webmonitor بيقوم مع نفسه بعمل رولز خاصة به على TMG في المقابل فإنه يصبح هو أداة التحكم الخاصة بك فيمكنك من خلاله السيطرة على حركة الإنترنت وعمل رولز وفلاتر خاصة به وبإسلوبه وطبعا يتيح نظام للتقارير جيد للغاية

من غير كلام كتير خلينا في العملي

نفتح الـ GFI سواء ريموتلي أو من السيرفر ذات نفسه , وأياً كانت طريقة الريموتلي ☺ فدي مش مهمة لكن المهم إننا نخش على البورنامج

Virus Protection

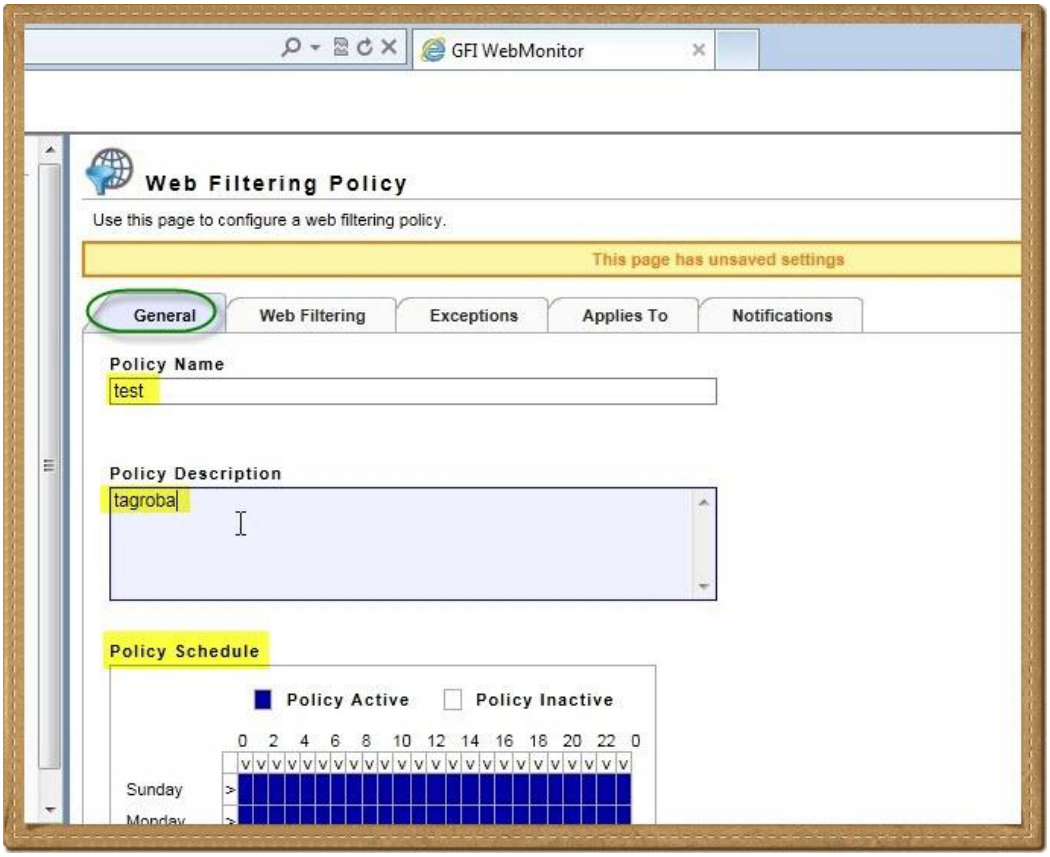
أول ما يلفت نظرنا في GFI هو خاصية الـ Virus and Spyware Protection وكما يتضح فإنها تتعامل مع أكثر من أنتي فايروس يمكننا تعطيلهم جميعا أو بعضهم

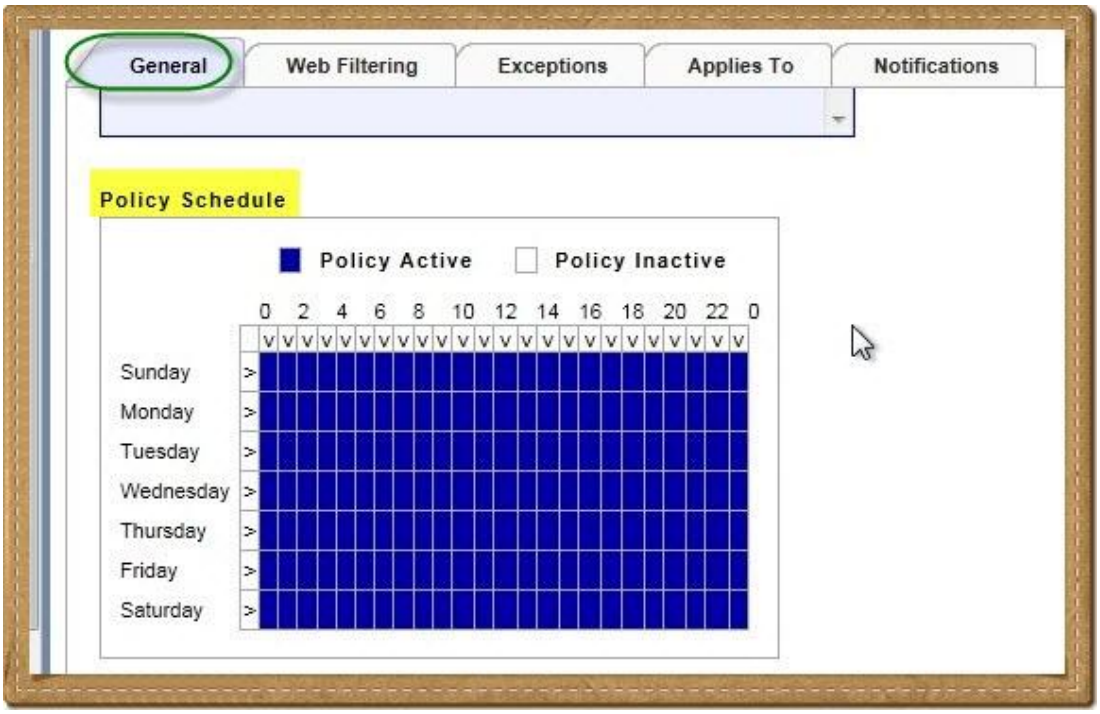
Web Filtering Policies

من هنا يمكن إنشاء بوليسيز Policies أو رولز Rules ولكن بطريقة بسيطة للغاية

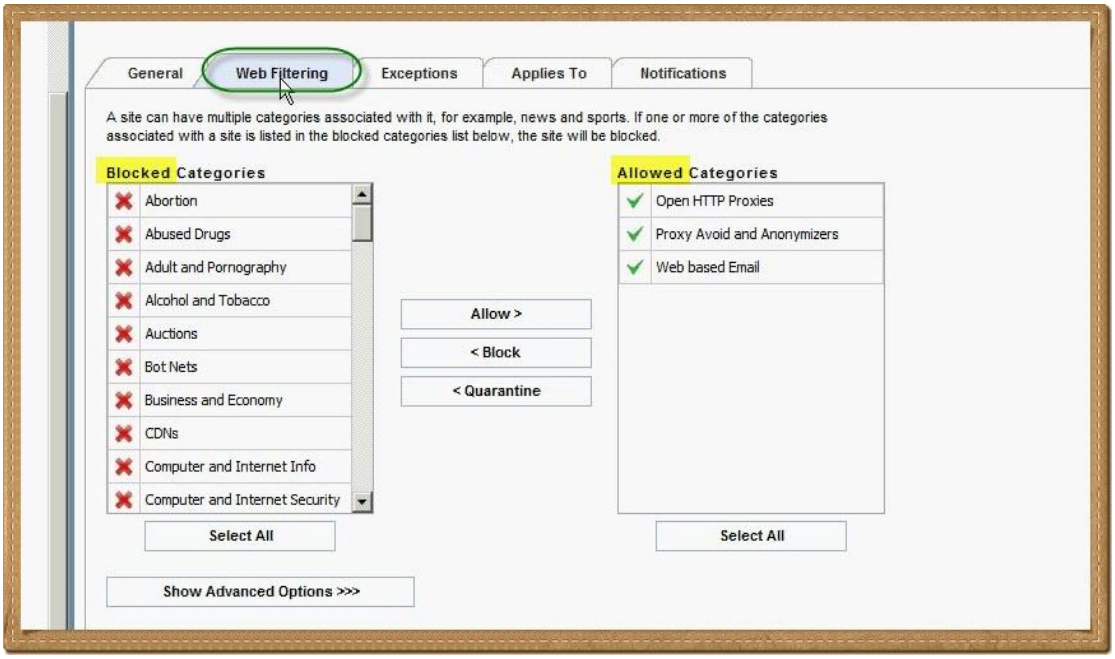
نضغط على Add Policy

من General إسم البوليسي وشرح بسيط لها وجدول زمني يحدد متى تكون مفعلة أو معطلة





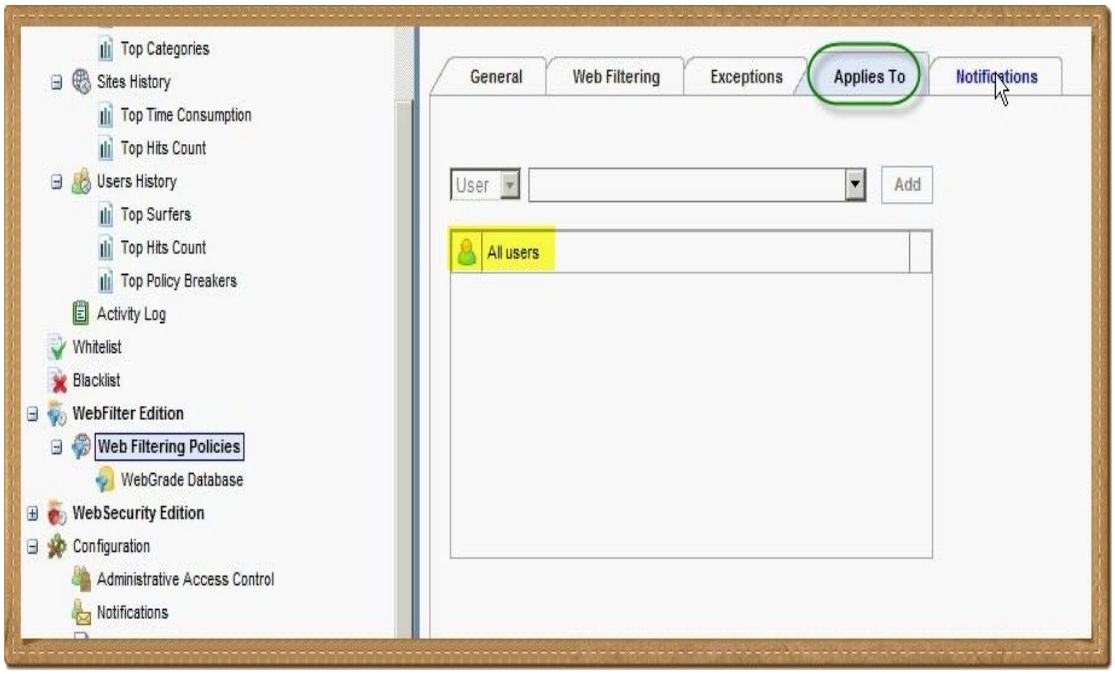
من Web Filtering نحدد ح نعدي إيه ونوقف إيه



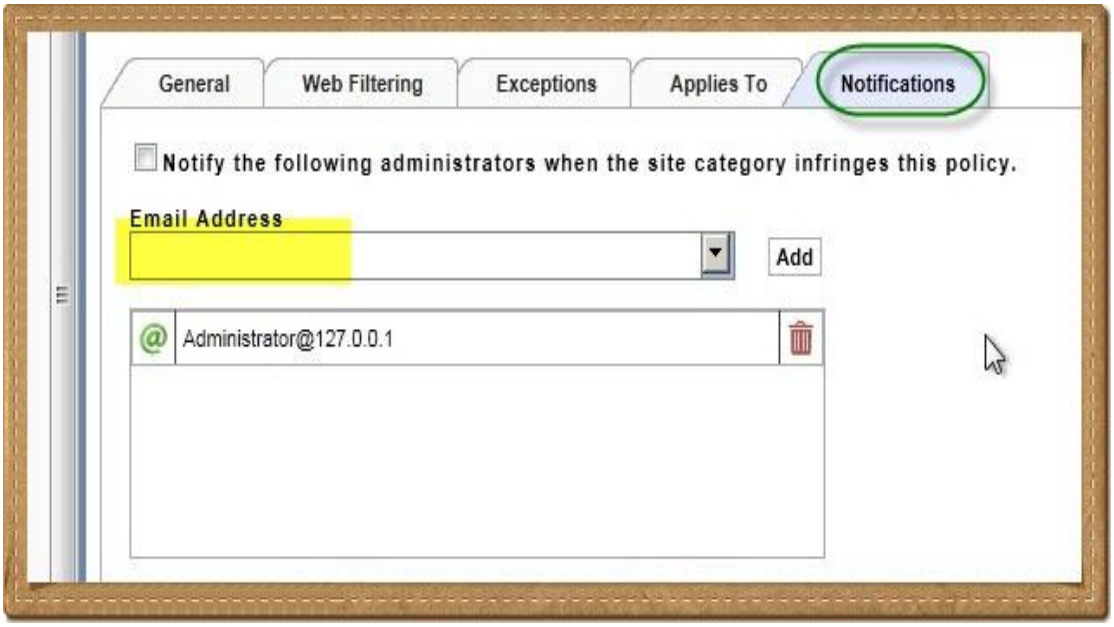
Exceptions لإستثناء مواقع من تطبيق البوليسي

Applies To تتيح لنا تحديد على من سيتم تطبيق البوليسي يمكننا إختيار أسماء مستخدمين أو أرقام IP على سبيل المثال

أو تطبيقها على جميع المستخدمين

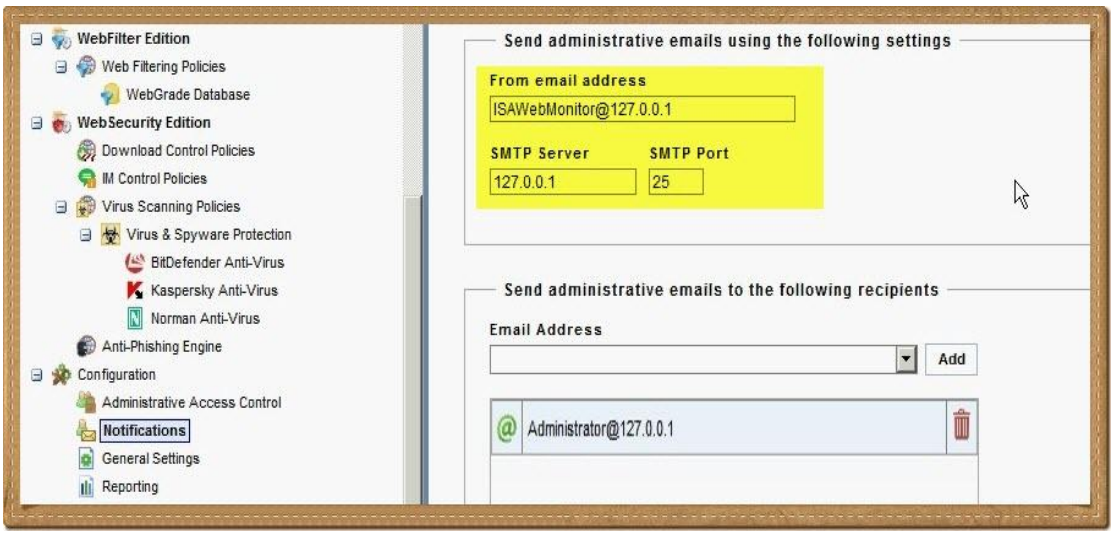


ومن هنا يتم إضافة إيميل الأدمين ليراسله البرنامج في حالة وجود محاولات لمخالفة الـ Policy



طبعا تفعيل هذه الخاصية يتطلب إعداد الإيميل كما طلب منا المعالج أثناء الإعداد

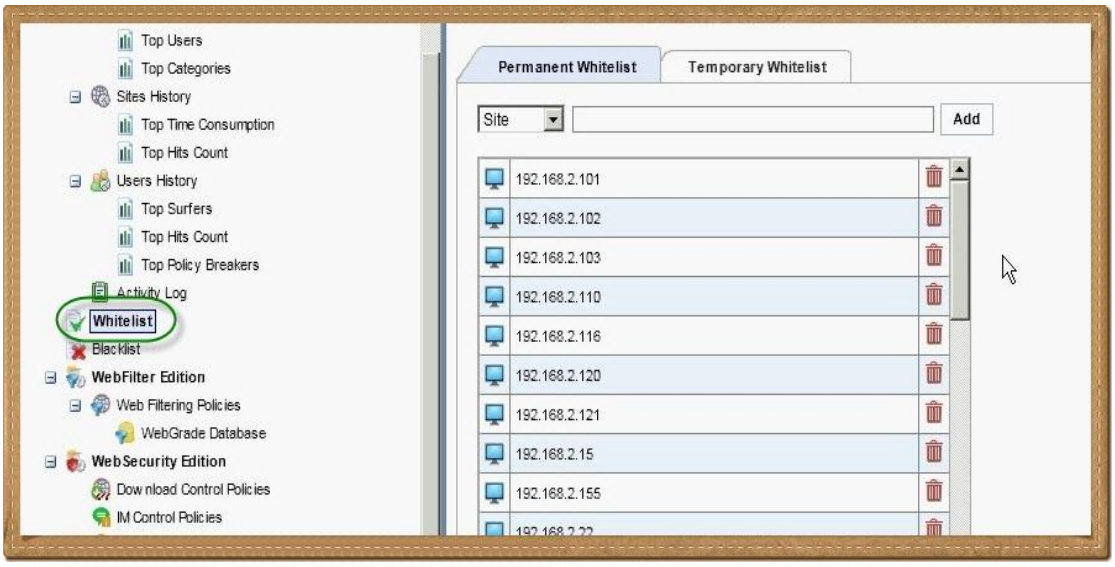
أو من هنا



وطبعا Save Settings

Whitelist

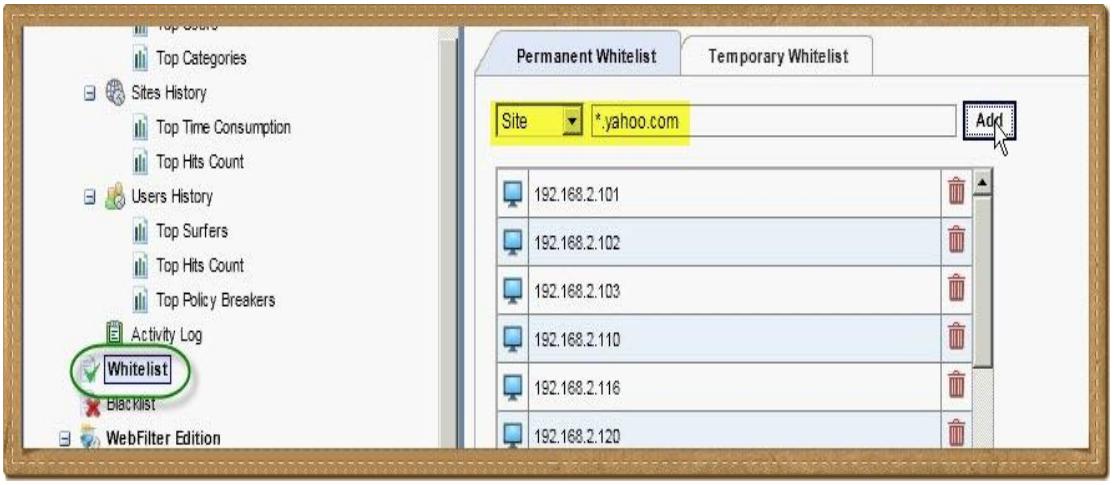
نوع آخر من أنواع السيطرة والتحكم وهو القوائم البيضاء والسوداء



بالفكاكة والفهلوة نقدر نفهم إن المقصود بالـ Whitelist هو العناصر اللي ح يتفتح لها الطريق

سواء كانت هذه العناصر مستخدمين أو أجهزة أو مواقع

هنا سنجرب إضافة موقع yahoo.com

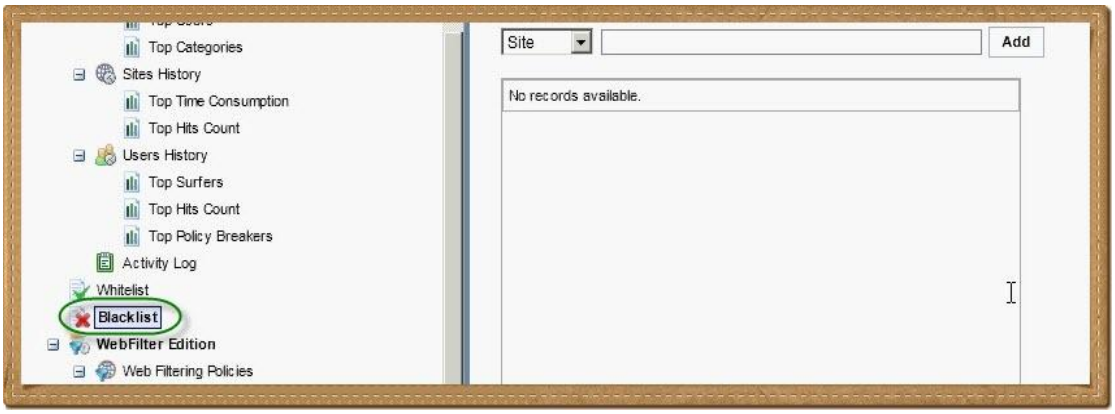


و save وخلاص ☺

بالفكاكة والفهلوة نقدر نفهم إن المقصود بالـ Whitelist هو العناصر اللي ح يتفتح لها الطريق سواء كانت هذه العناصر مستخدمين أو أجهزة أو مواقع

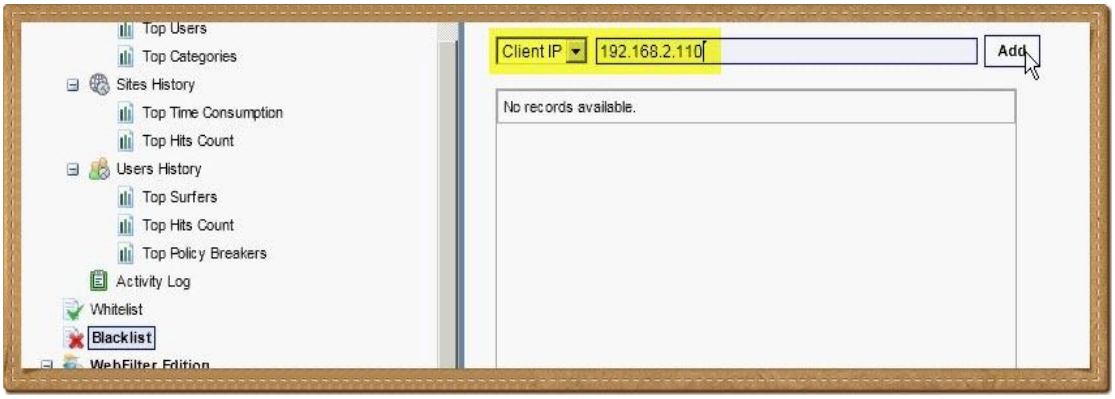
Blacklist

الأهم من الوايت ليست هو الـ Blacklist وطبعا لإنه من ضمن بدائل رولز الـ TMG



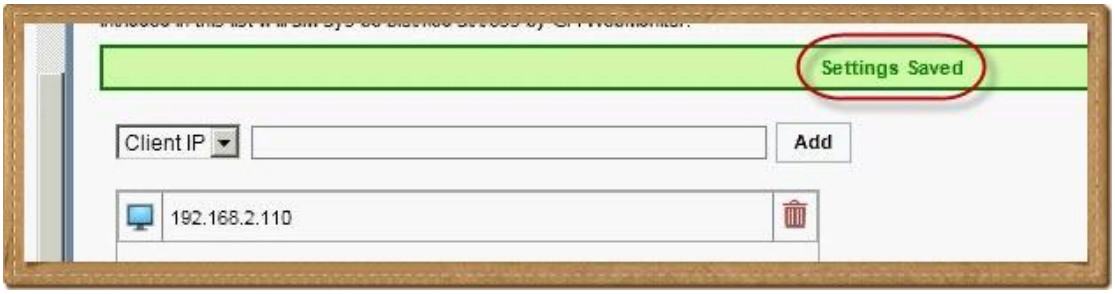
يمكننا أيضا إضافة IP أو User أو Site

هنا سنعمل بلوك للجهاز 192.168.2.110



و Save

وبكده أي حاجه تتعلق بجهاز الكلاينت 192.168.2.110 ح تتقفل



لاحظوا إننا في أي مكان من GFI نقدر نضغط على علامة الـ Trash علشان نمسح

Download Control

من هنا التحكم في الرولز الخاصة بالداونلوود

Anti-Phishing Engine

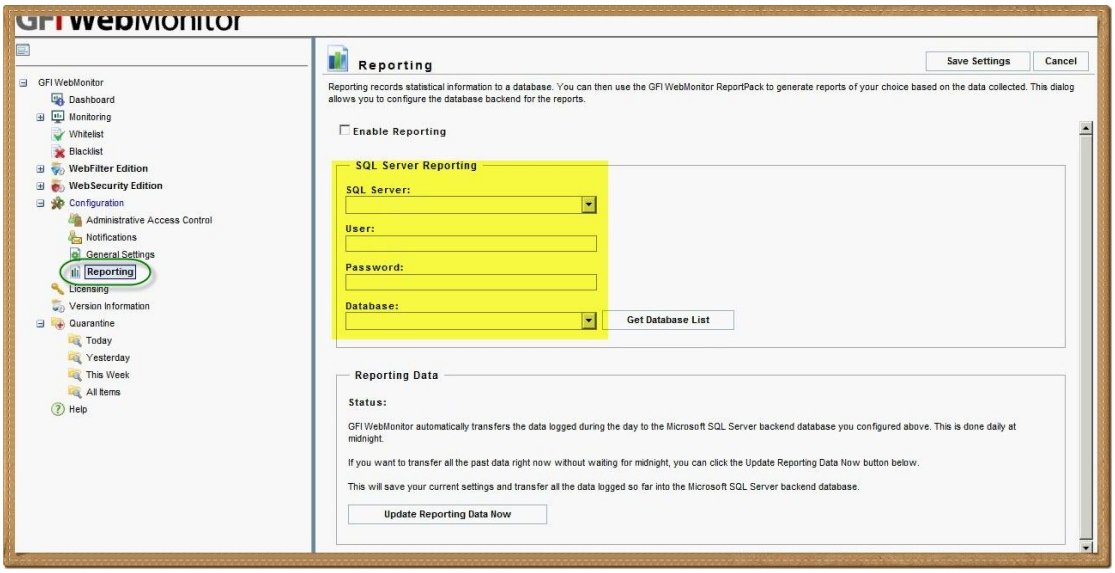
للمواقع الشريرة

Reporting

هامة جدا جدا

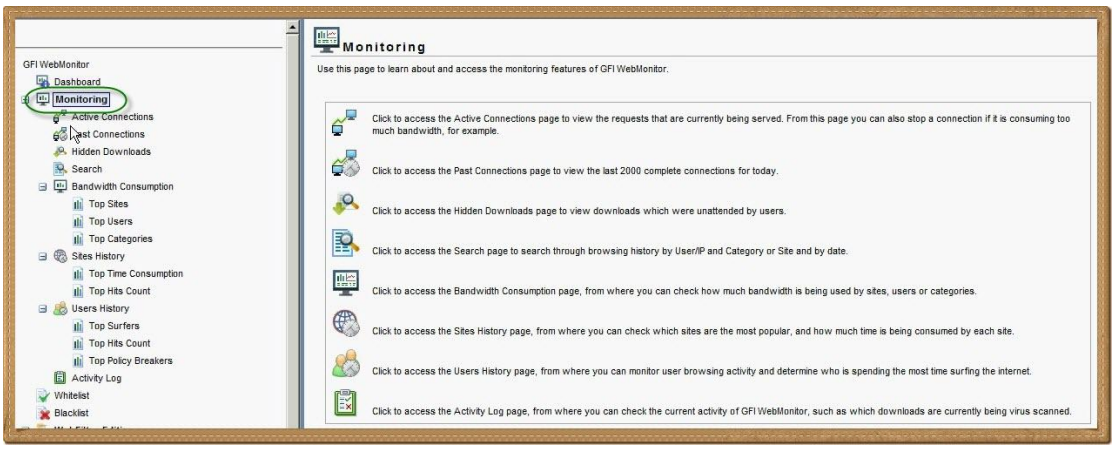
يمكن ربط البرنامج بقاعدة بيانات SQL لتخزين ومعالجة تقارير البرنامج فيها

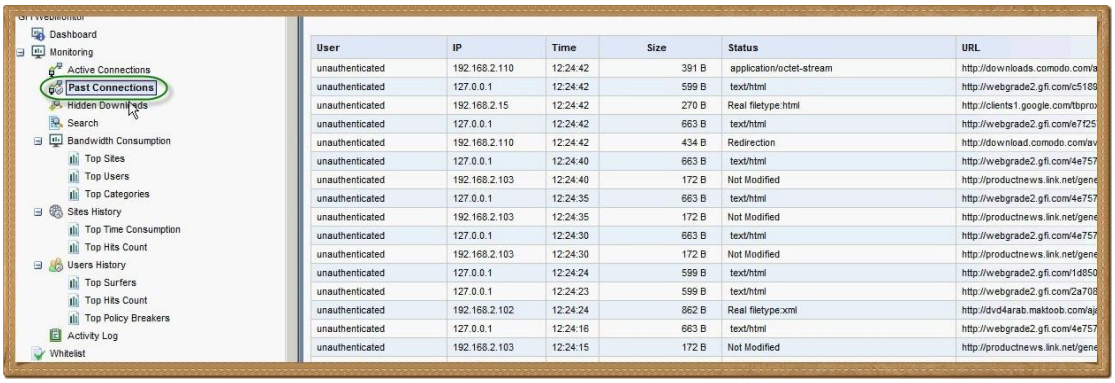
جامدة جدا جدا



Monitoring

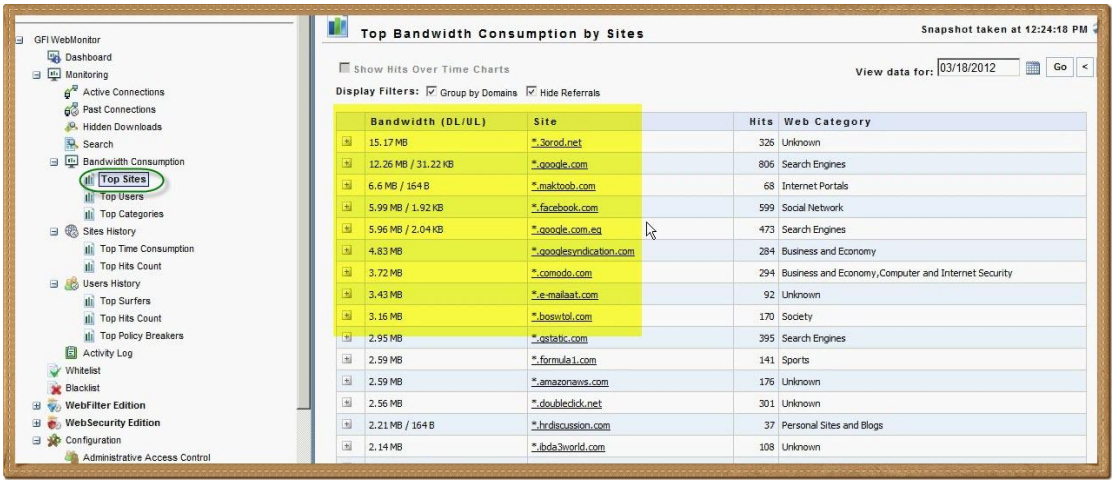
يمكنك تخصيص GFI للمراقبة و التقارير فقط وعمل الرولز على الـ TMG وحينها أيضا ستجده في غاية الأهمية ولعل بساطة الـ GFI هي ما أغنتني عن الحديث عن الـ Logs والـ Reports في TMG





أيضا يمكنك البحث من هنا عن أنشطة المستخدمين

ومن أهم أنواع التقارير هي Top Sites



وبكده نكون إنتهينا بفضل الله وتوفيقه من شرح الأجزاء الرئيسية في الـ TMG والـ GFI

اللهم إني أعوذ بك أن أشرك بك شيء أعلمه

وأستغفرك لما لا أعلمه

سبحانك اللهم وبحمدك , أشهد ألا إله إلا أنت , أستغفرك وأتوب اليك

الفصل الخامس : المساكين

CCProxy

AnalogX Proxy

المساكين

CCProxy

الحمد لله والصلاة والسلام على رسول الله

سيدنا محمد , وعلى آله وصحبه ومن والاه

من أهم مشاكلي مع مايكروسوفت إنها تعطي إنطباع لمستخدميها إنها المنتج الوحيد التمام وأي حاجة غيرها فلا وألف لا

وعلشان مانقعش في الفخ فقد تعرفنا في هذا الكتاب على منتجات لشركات أخرى

ولكن أيضا إذا كانت دنيا الشبكات ليست مايكروسوفت فقط فإنها أيضا ليست مايكروسوفت وجي إف أي وكيريو فقط

بل يوجد مالا يعد ولا يحصى من برامج البروكسي والفاير وول ولا أتحدث هنا عن منتجات تعمل تحت بيئة لينكس ولكن أتحدث عن برامج للويندوز تقوم بمهام البروكسي والجيت واي والفايروول

تتنوع هذه المنتجات مابين مجاني وبفلوس

ومابين مفتريه ومسكينه

في هذا الفصل نلتقي مع أحد البرامج المسكينة وهو برنامج موجود في السوق منذ سنوات CCProxy

البرنامج لايمكن مقارنته بما استعرضناه في الفصول السابقة

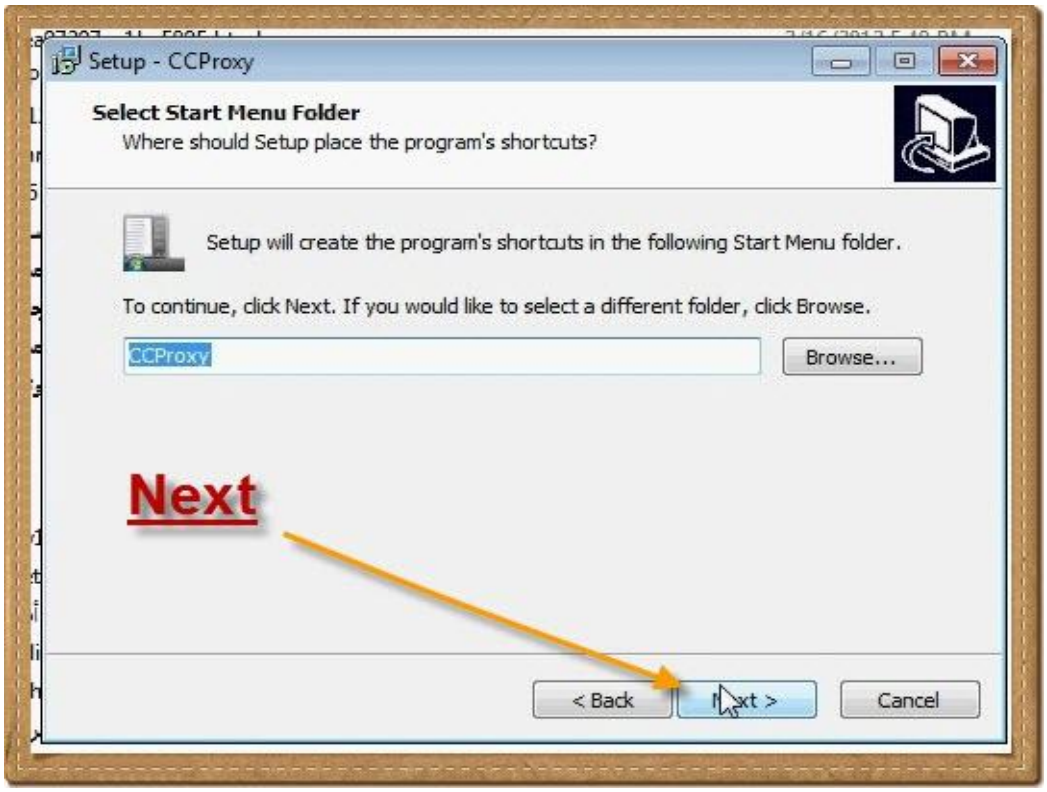
ولكنه يوفي إحتياجات الشركات الصغيرة التي لا تحتاج لوضع رولز معقدة لإستخدام الإنترنت ولا يوجد لديها ميزانية لتخصيص سيرفر لهذه المهمة وقد يكون أيضا ليس لديها موظف يتخصص كأدمينيستراتور له

دابل كليك على ملف البرنامج

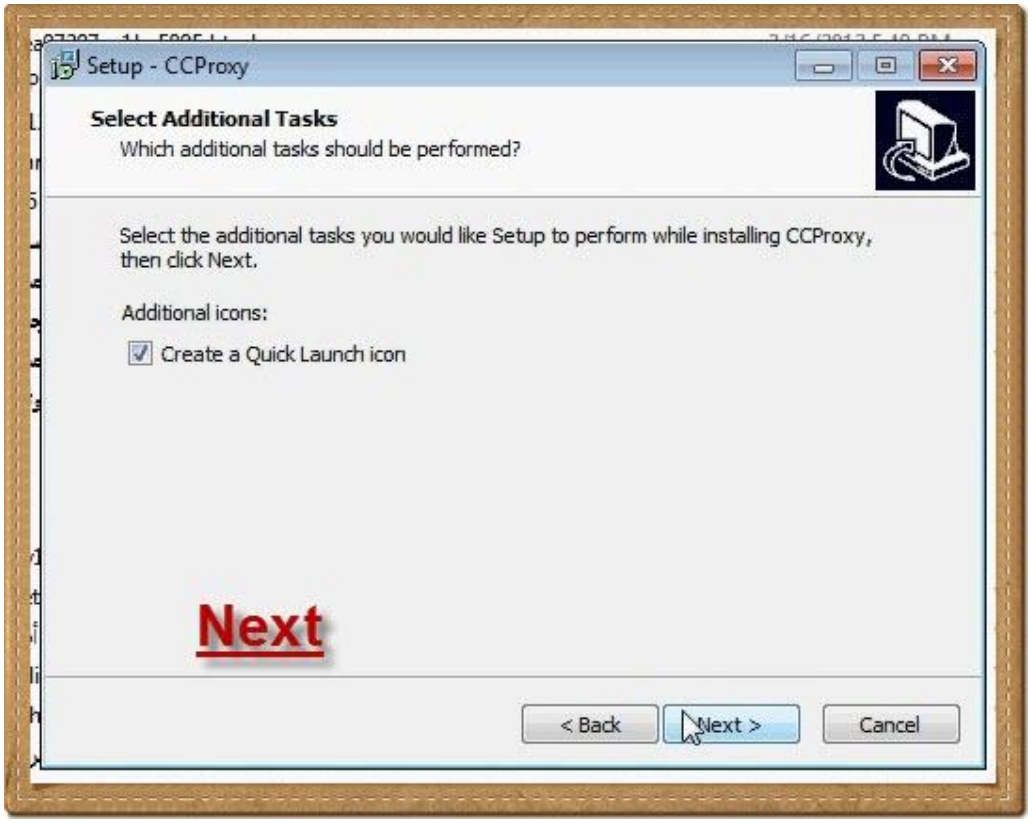
و Next

تحديد مكان إعداد البرنامج ثم Next

وكمان Next

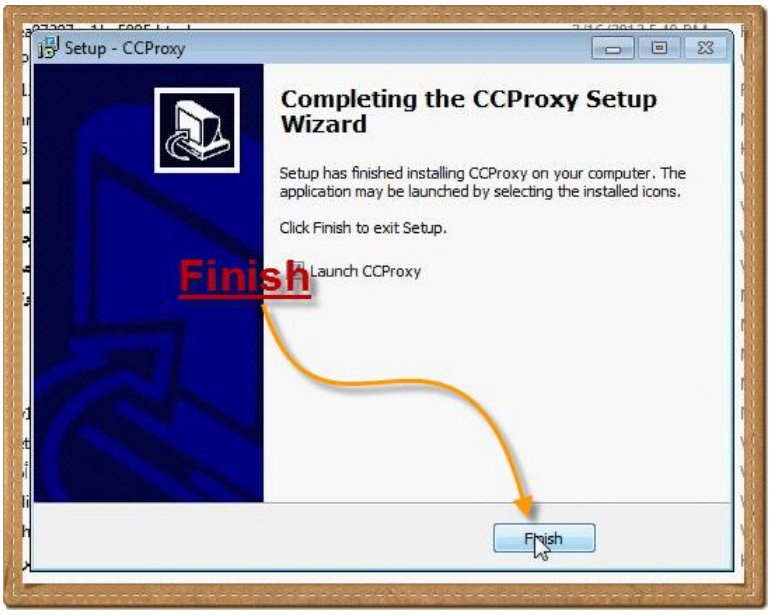


و Next

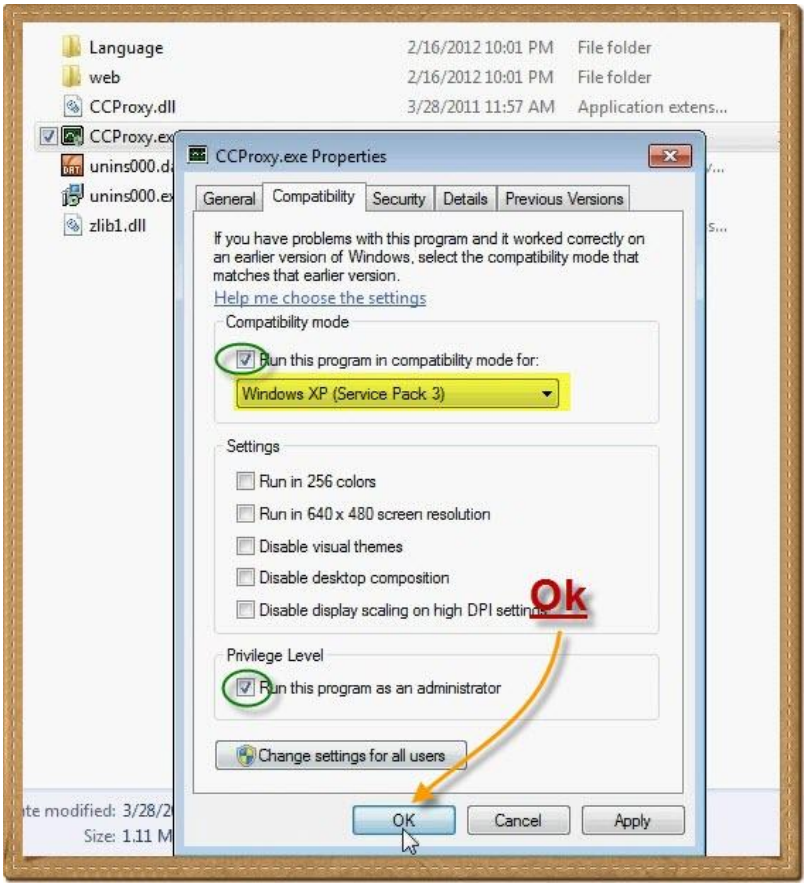


وأخيرا Install

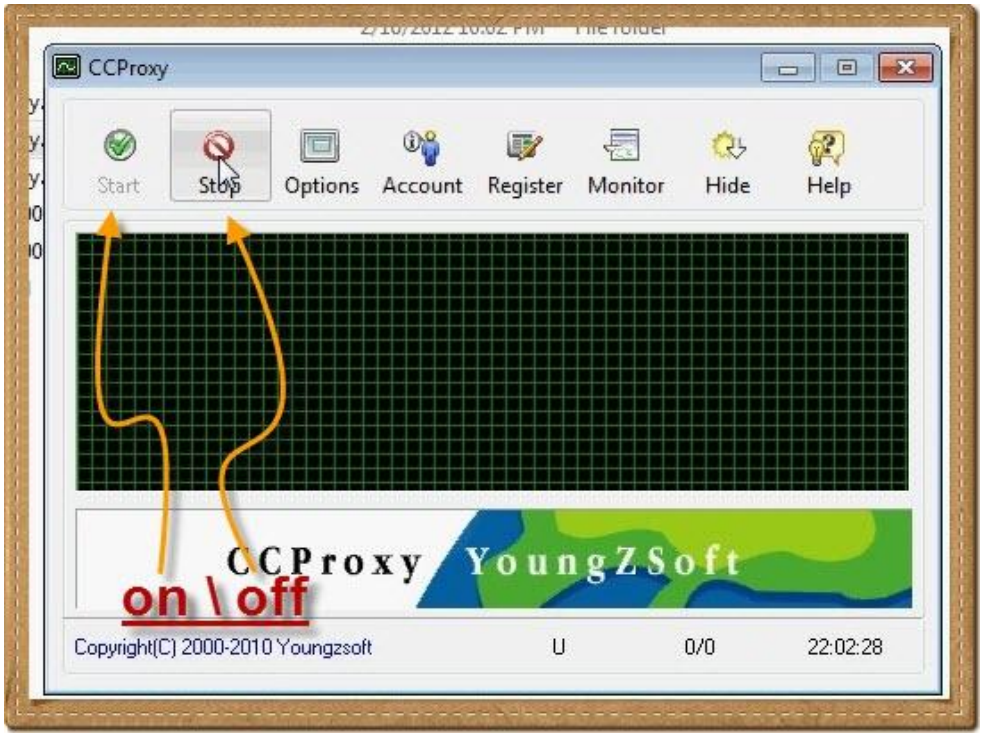
و Finish



قبل ما تشغل البرنامج إذا كنت بتشتغل على ويندوز 7 وواجهتك مشكلة مع البرنامج فلتذهب إلى فولدر البرنامج ثم كليك يمين على ملف الـ Exe وتختار Properties وتغير التوافقية Compatibility ثم Ok

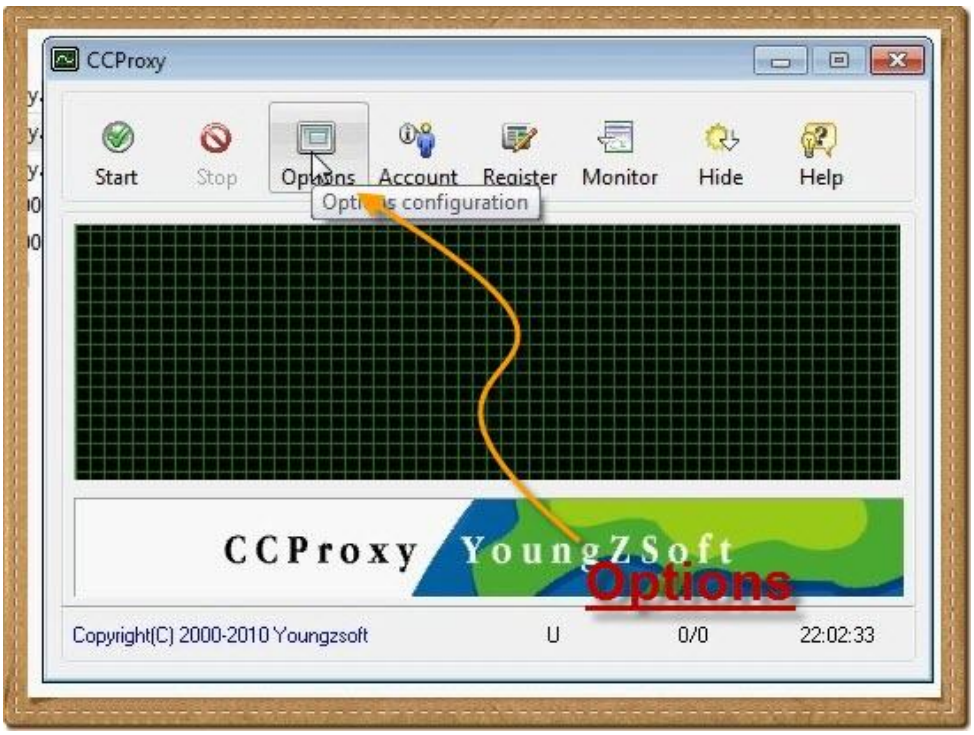


عند فتح البرنامج والواجهة الرئيسية بها Start و Stop لفتح البروكسي أو إيقافه



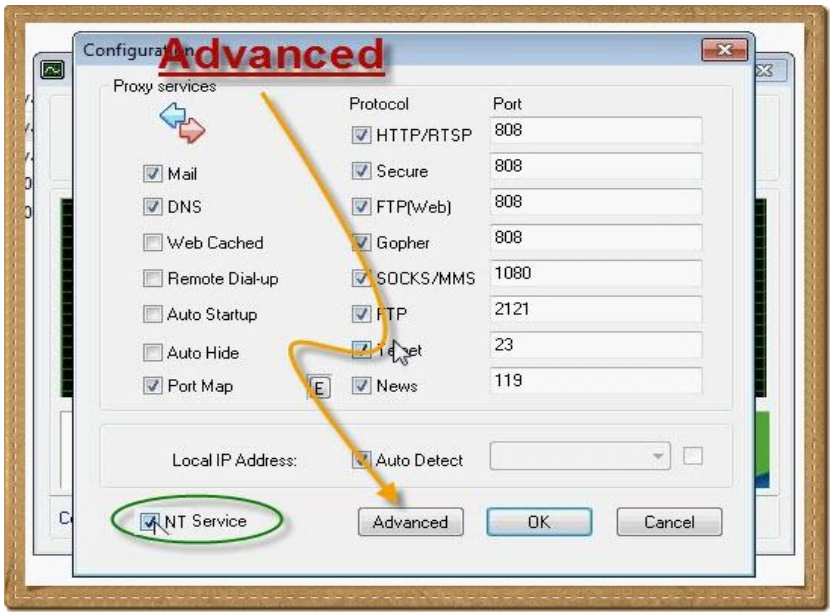
ثم Options ....

نضغط عليها



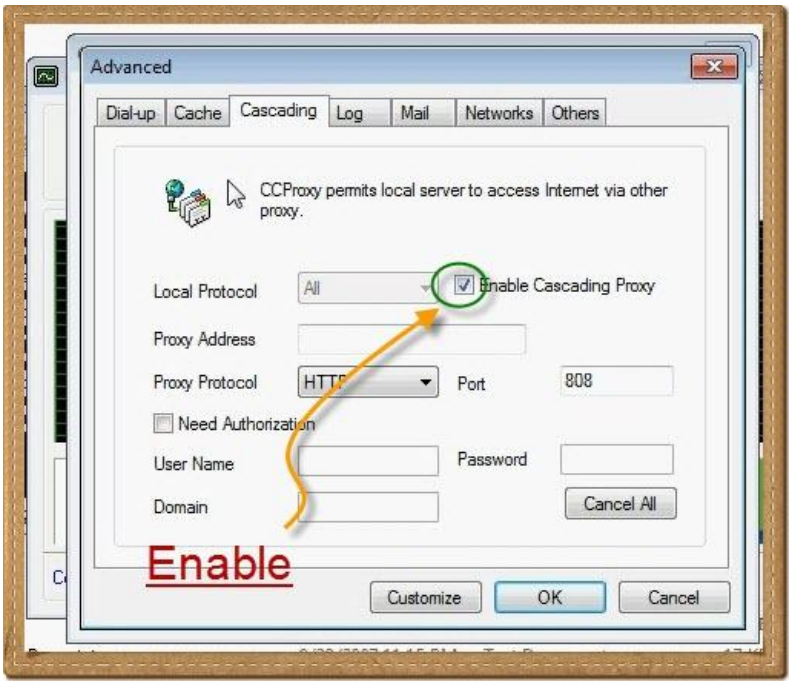
إختيار NT Service يجعل البرنامج يعمل دائما تلقائيا كـ Service في الخلفية

كما نرى هنا البروتوكولات التي يدعمها البرنامج وهناك إمكانية لتنشيطها وتغيير البورت الذي ستستخدمه لتوزيع الخدمة ... نضغط على Advanced



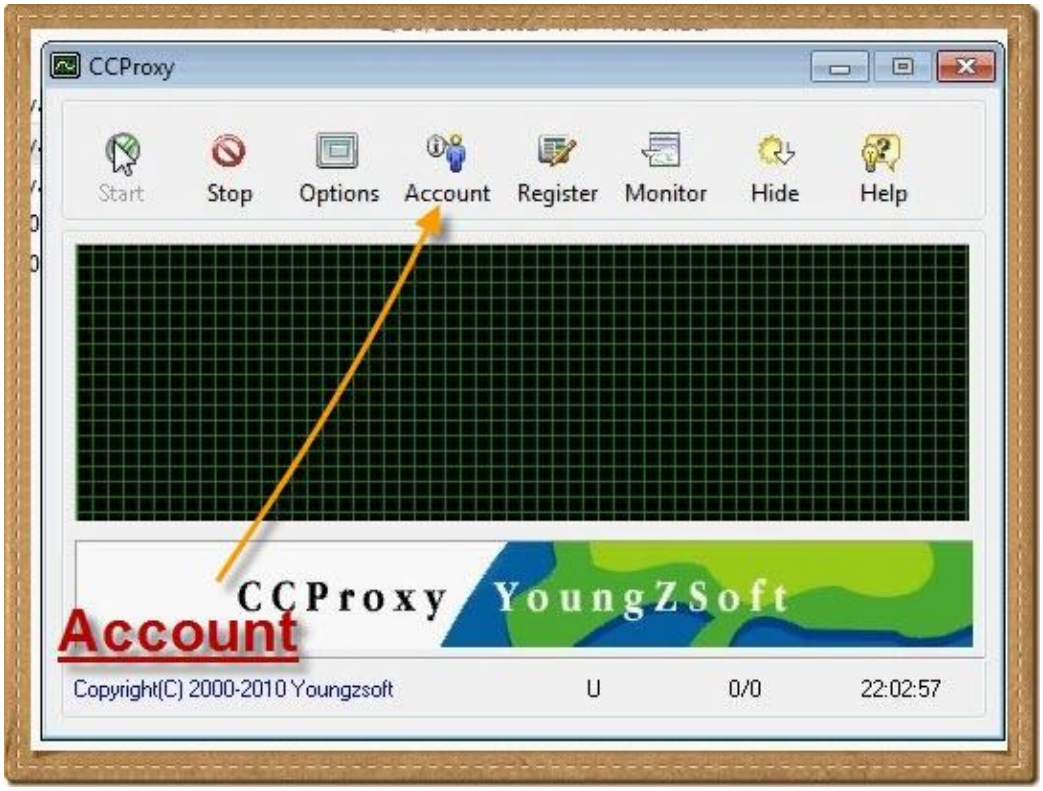
ومن هنا تفعيل خاصية Cascading Proxy وهي تتيح تشغيل بركسي من داخل بروكسي أعلى

يعني بإختصار البروكسي CCProxy ياخد الإنترنت أو يعطيه لسيرفر آخر وليكن Kerio Control

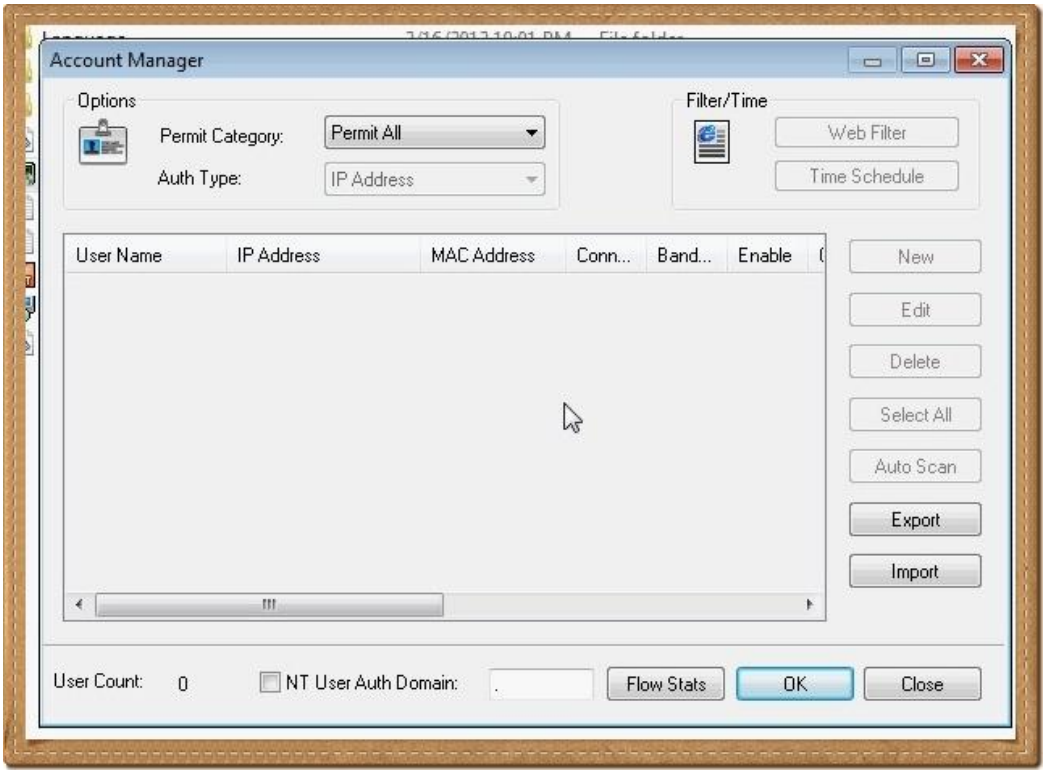


إعدادات اللوج الخاصة بسلوك المستخدمين وحركة الإنترنت

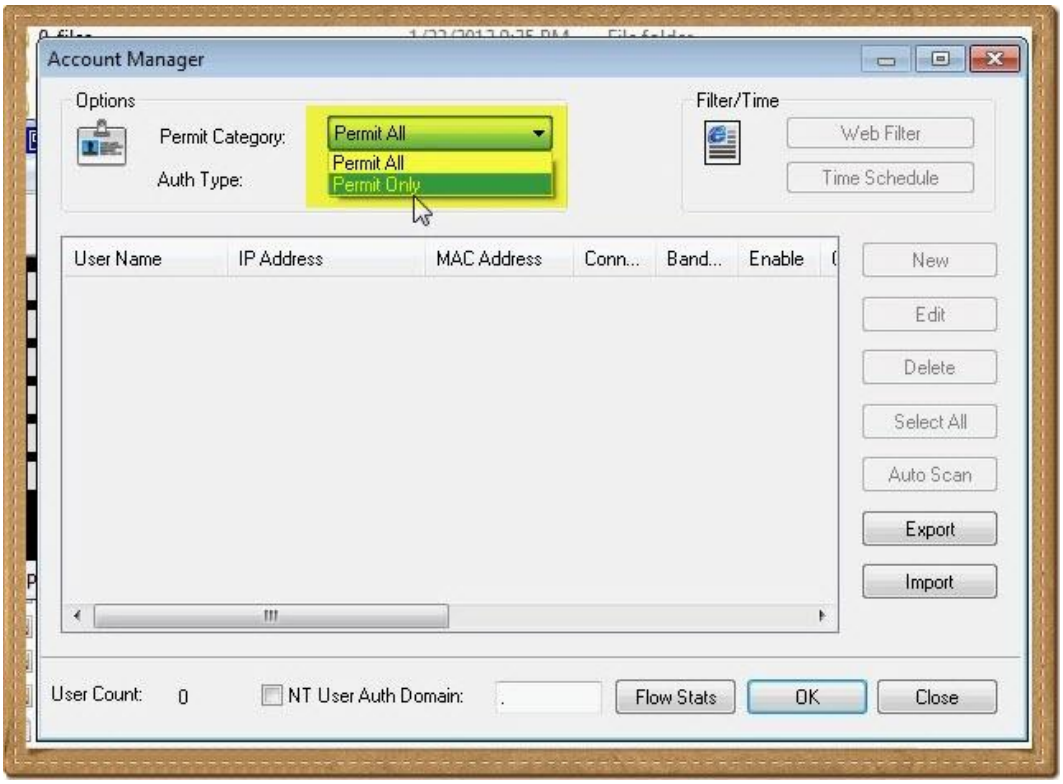
التحكم بالمستخدمين وعمل ما يشبه الرولز أو البوليسي لهم من Account



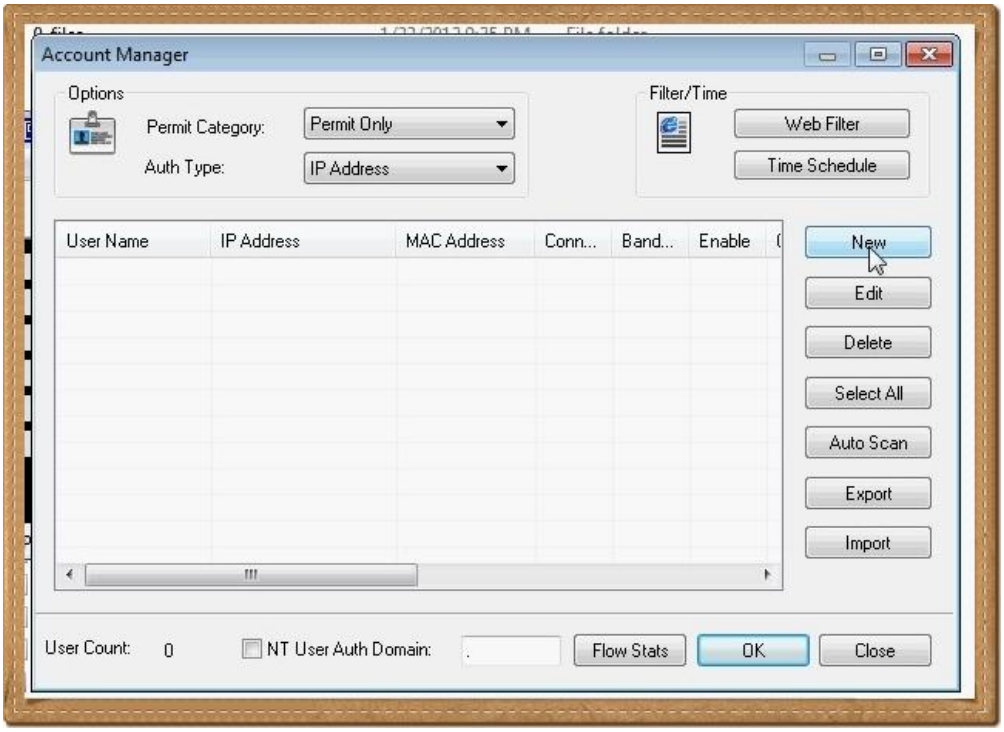
إختيار السماح للكل Permit All مفعل تلقائيا وهو لا يحتاج لإعدادات أخرى



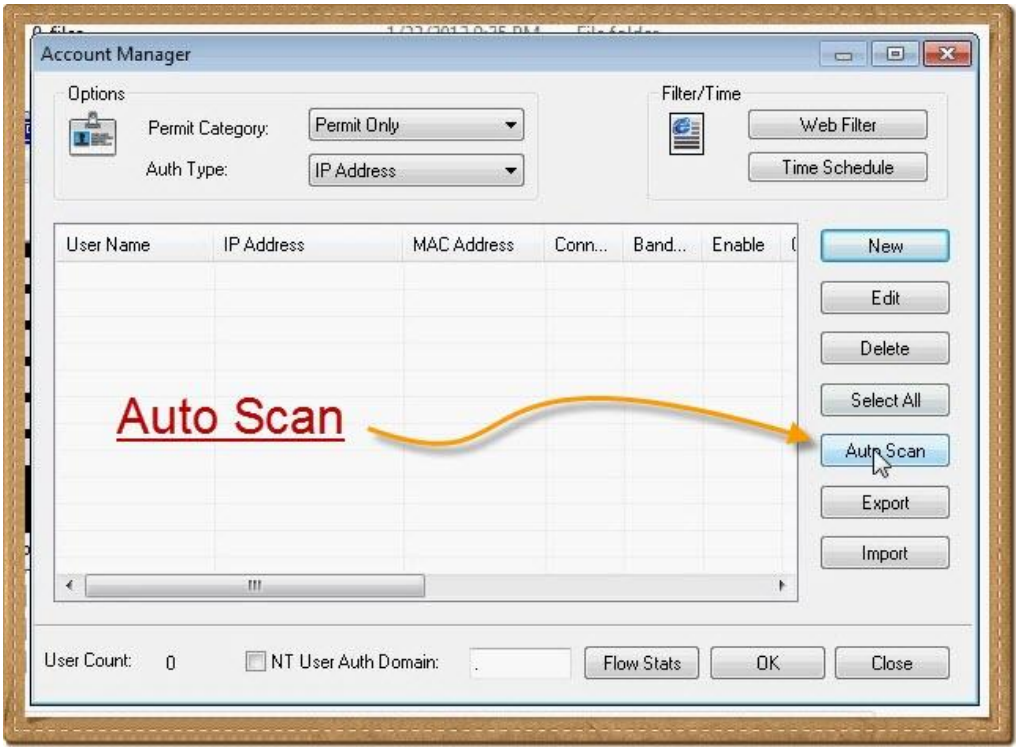
لبدء التخصيص نختار Permit Only



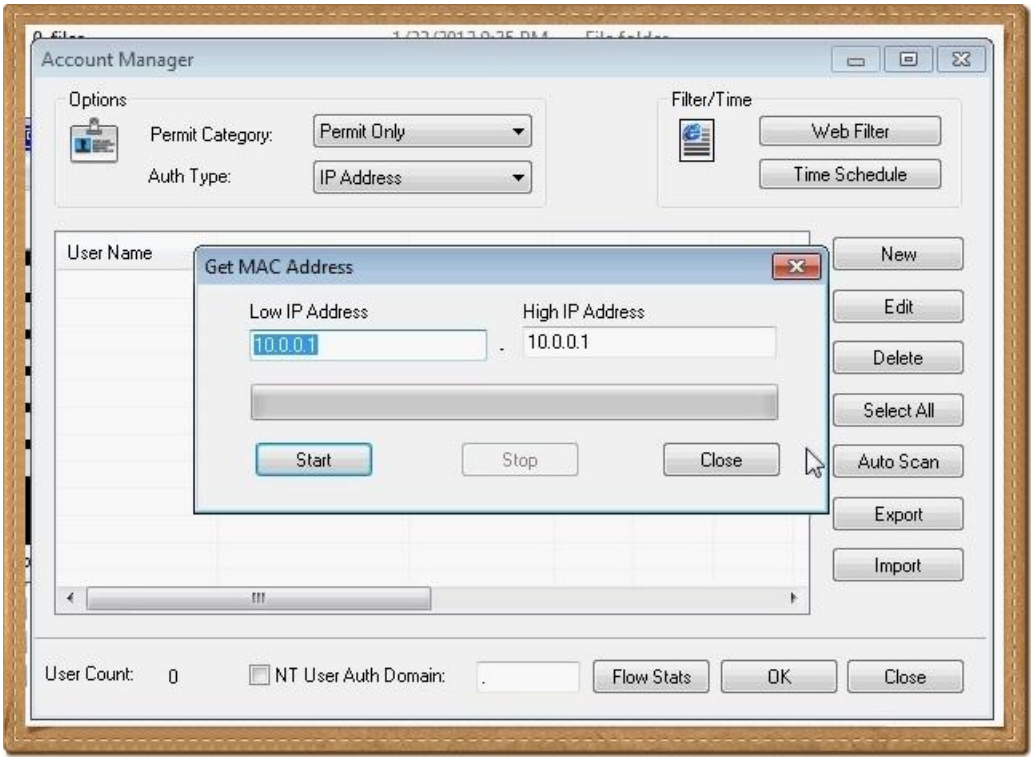
وبالتالي سيمكننا إضافة مستخدمين ثم تطبيق فلاتر وقواعد عليهم



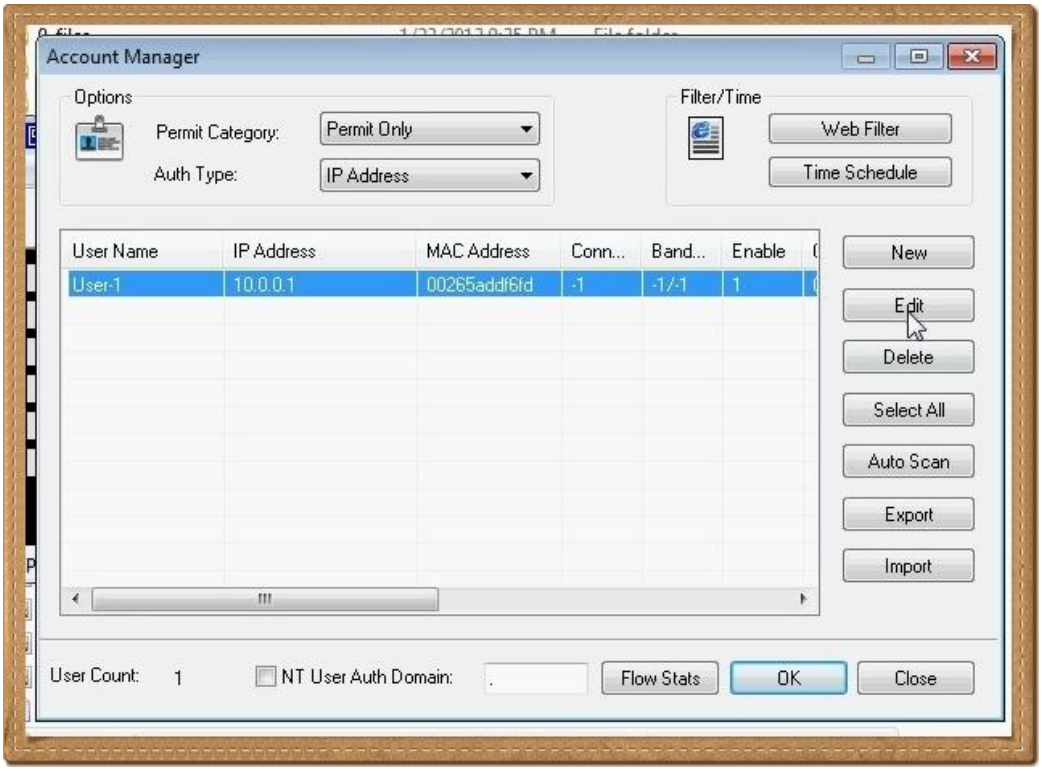
نضغط على Auto Scan ليتولى البرنامج تحديد الـ اي بيهات الخاصة بالأجهزة الموجودة على الشبكة



في حالتنا لم يجد إلا جهاز واحد , لاحظ أنه يبحث في الأجهزة الموجودة Live فقط



تم إضافة الجهاز وهو هنا بمثابة مستخدم وبالضغط على Edit لتعديل القواعد الخاصة به

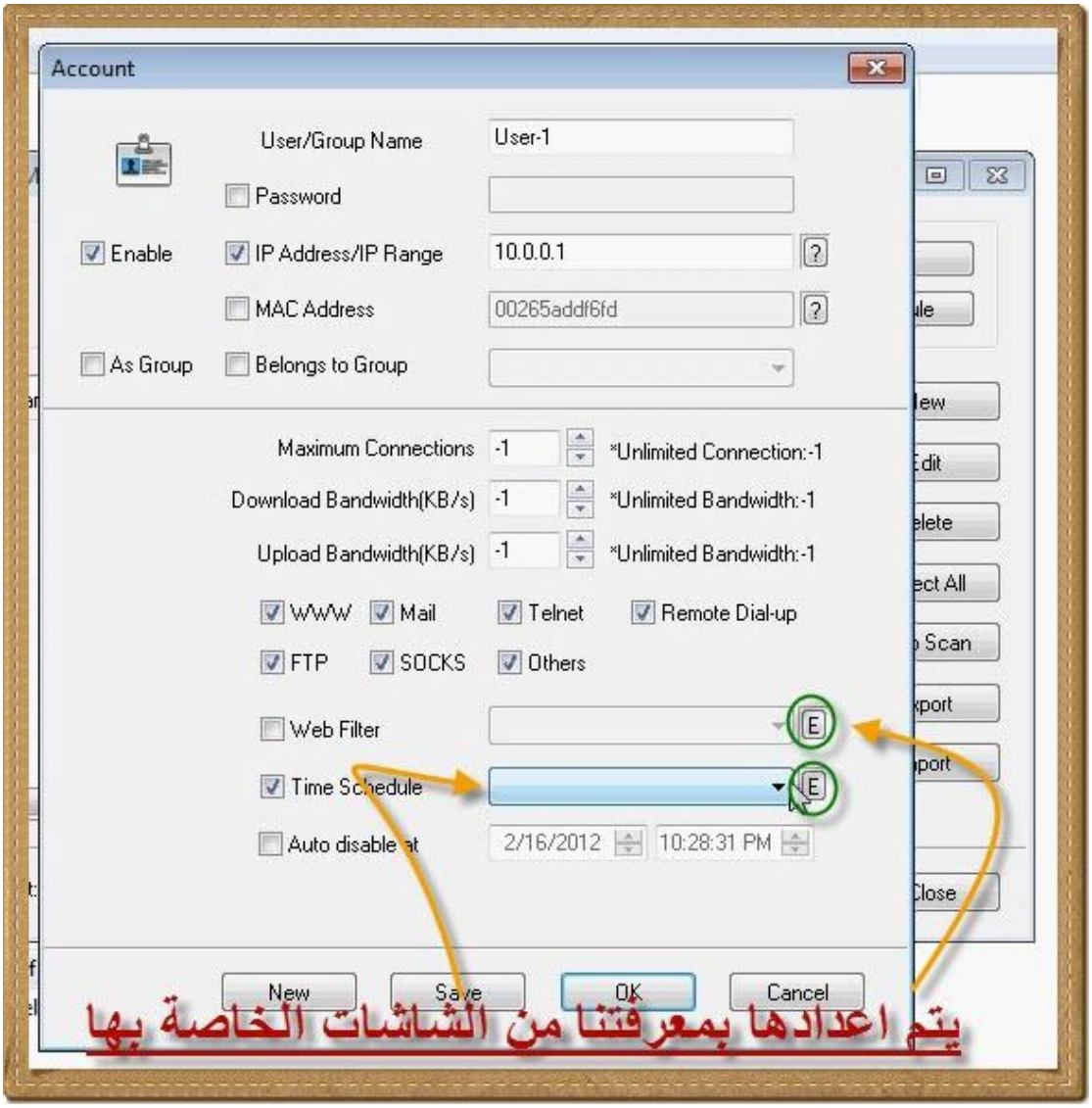


يمكننا مثلا تحديد أي فلتر سيتم تطبيقه على المواقع التي سيتعامل معها

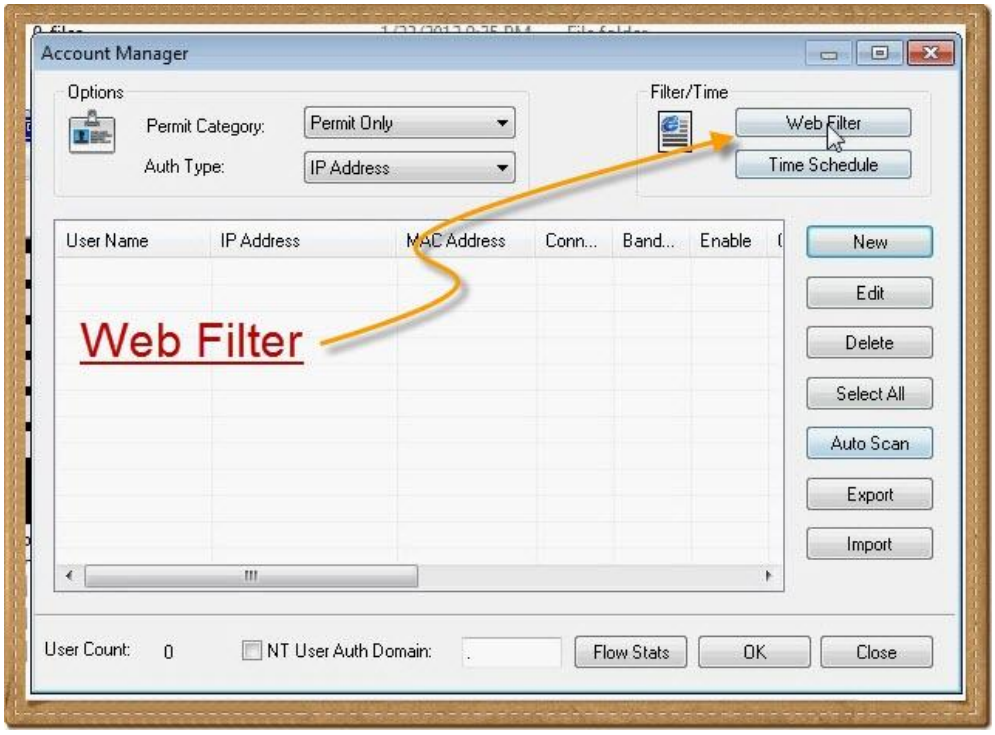
أو الجدول الزمني له

وذلك بالضغط على حرف E لإنشاء فلتر أو قاعدة أو جدول

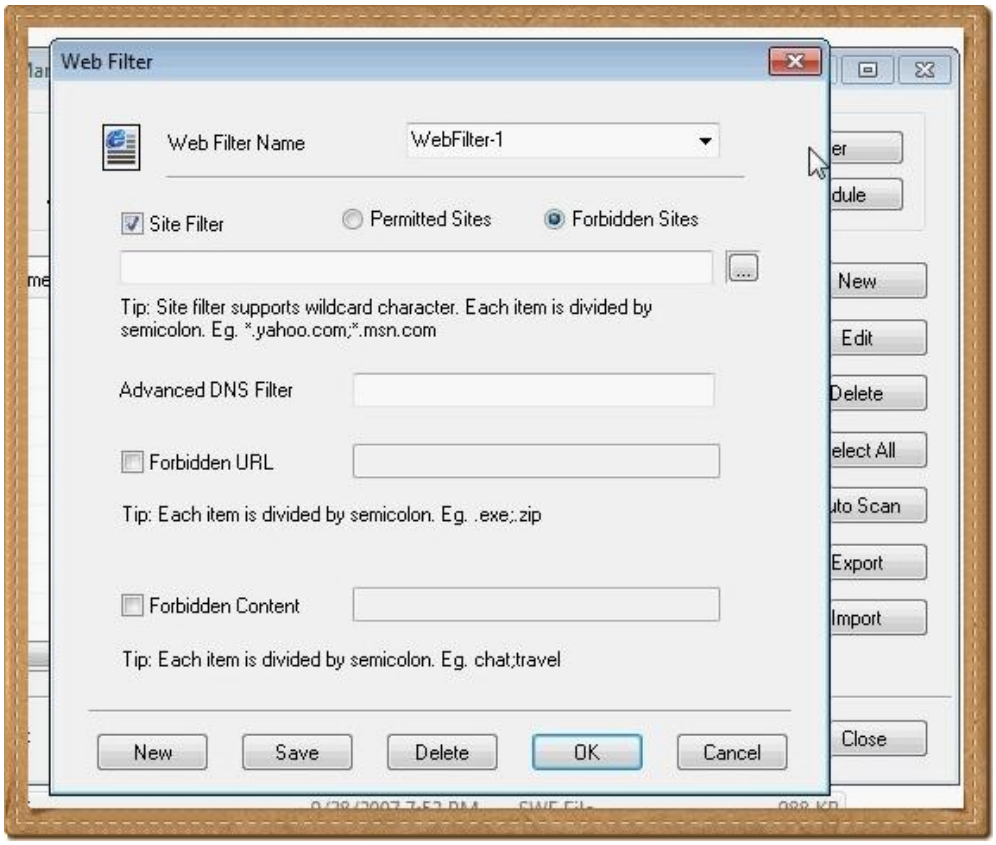
يمكننا أيضا إختيار قاعدة منشأة من قبل



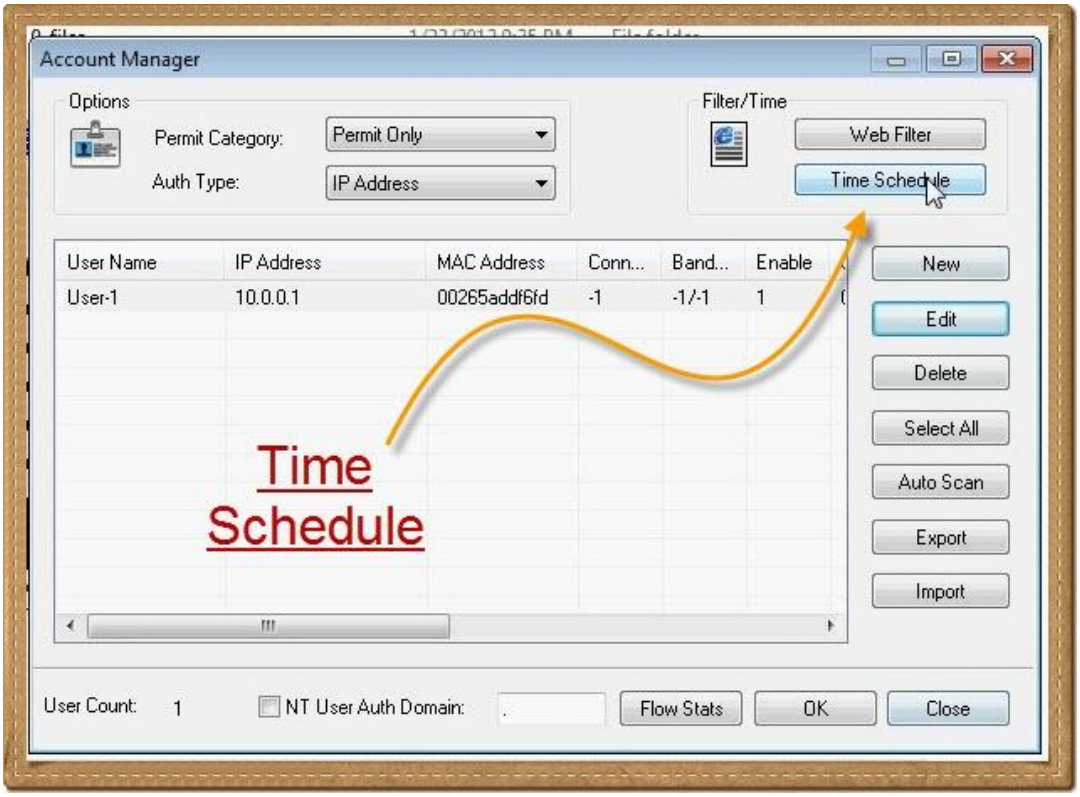
من هنا أيضا يمكن إنشاء الفلاتر والقواعد والجداول



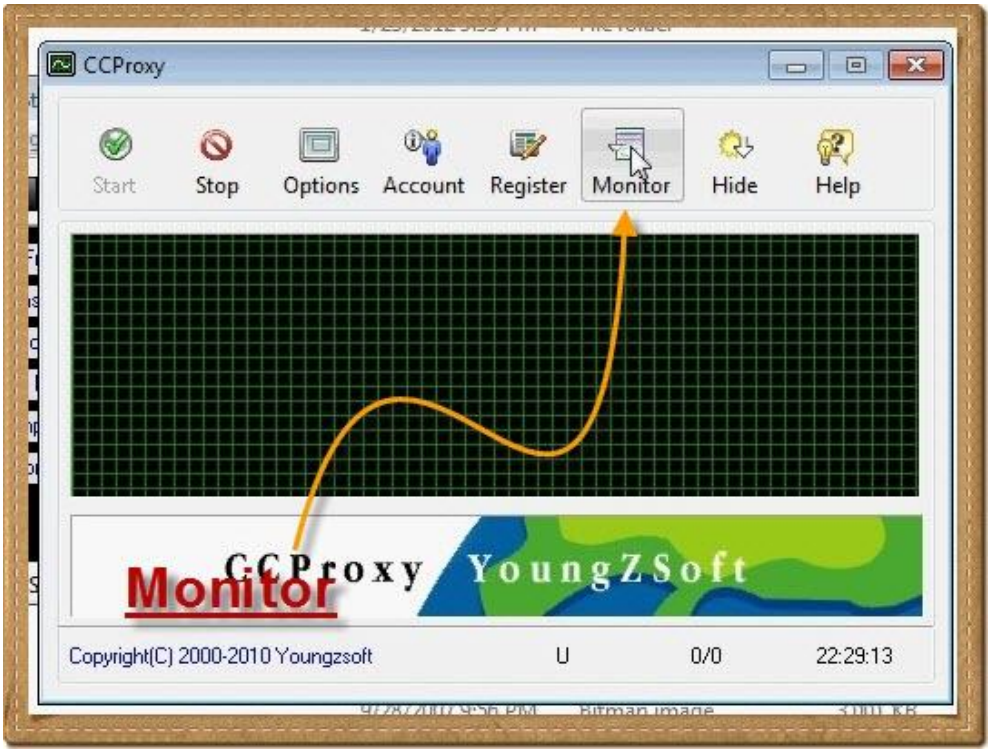
لإنشاء Web Filter



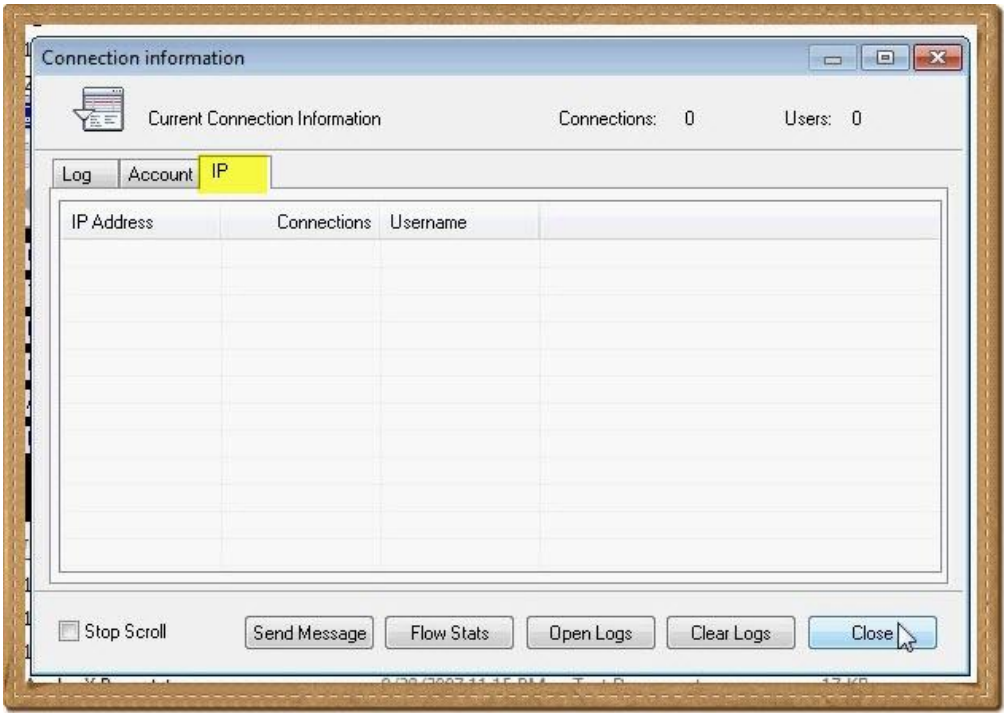
ومن هنا لإنشاء Time Schedule



من الشاشة الرئيسية يمكننا الدخول على خاصية Monitor



وهي تعرض موقف فوري وللحصول على لوج Log File يتم الحصول عليه من المجلد الذي أعددناه ليتم حفظ اللوج فيه في خطوة سابقة



بالنسبة لإعداد الكلاينت للحصول على الإنترنت فسيتم بطريقة الإنترنت أوبشن " المسكينة"

البرنامج لا يعتمد عليه إلا في حالات معينة وهو ممكن يسد زنقه زي مابيقولوا وبخاصة إنه ممكن يشتغل على أي جهاز عليه ويندوز ولا يأخذ شيء يذكر من موارد الجهاز

اللهم إجعلني خيراً مما يظنون واغفر لي مالا يعلمون

اللهم إني أعوذ بك أن أشرك بك شيء أعلمه وأستغفرك لما لا أعلمه

سبحانك اللهم وبحمدك , أشهد ألا إله إلا أنت , أستغفرك وأتوب اليك

المساكين

AnalogX Proxy

الحمد لله والصلاة والسلام على رسول الله

سيدنا محمد , وعلى آله وصحبه ومن والاه

لو إنت معتقد إن CCProxy هو أصغر برنامج لتوزيع الإنترنت فإسمح لي أقولك : عيب عليك

في هذا الفصل سنتعامل مع : أصغر مقاس رجالي ☺

بروكسي فائق الصغر والإمكانيات

وعلشان نمنع الحسد ومن باب خدوهم فقرا يغنيكم ربنا نلتقي مع AnalogX Proxy

مش مستحمل رغي كتير ولا شرح كتير

دابل كليك

ونوافق على الإتفاقية

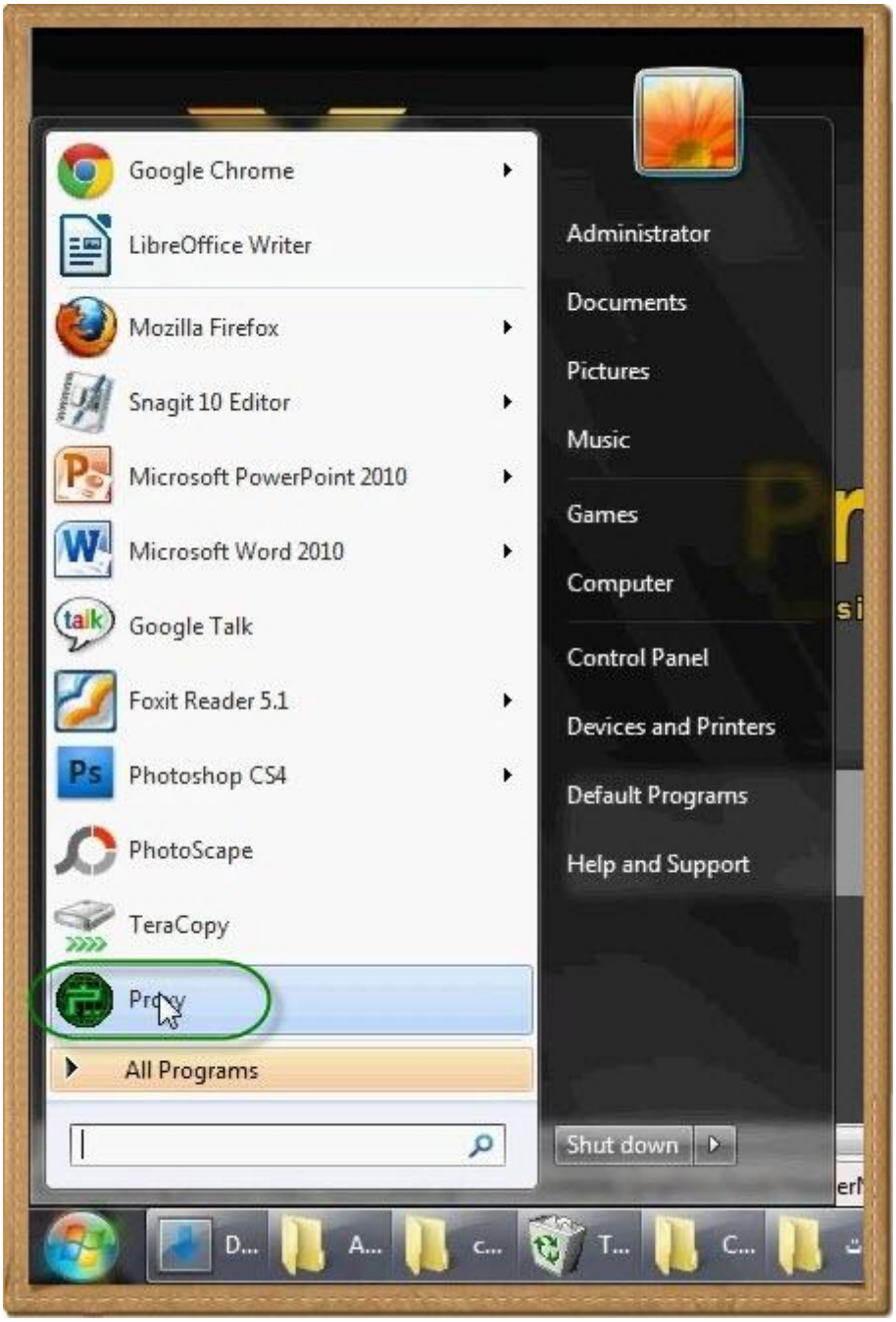
ثم Continue

أيوه متأكد Yes

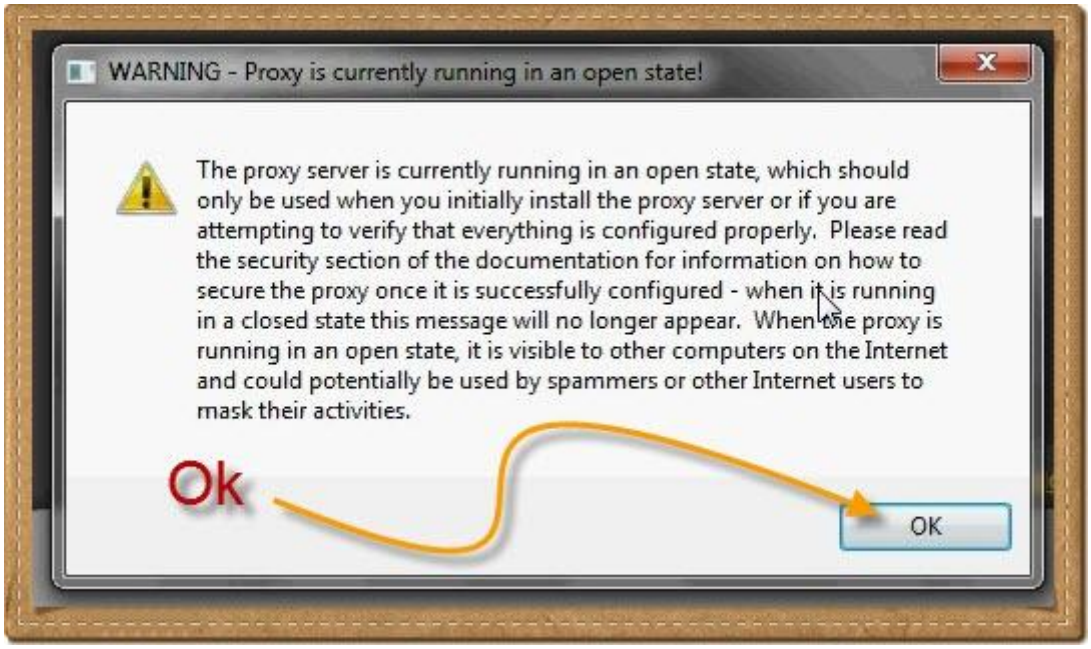
توافق أو ترفض ده قرارك

الـ Installation كان صعب قوي وطويل ☺

تشغيل البرنامج من الـ ستارت مينيو



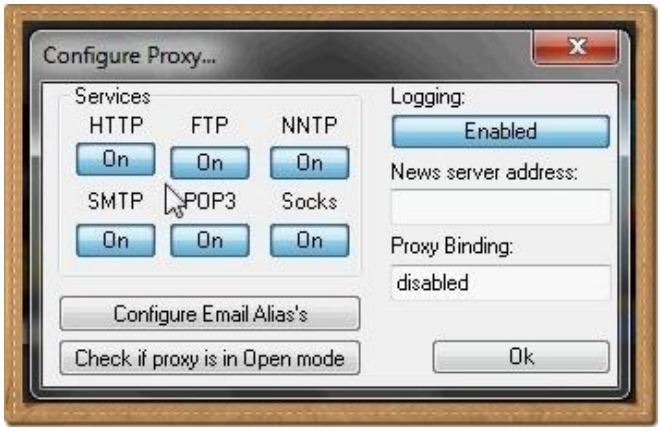
تحذير .... Ok



كليك يمين على أيقونة البرنامج

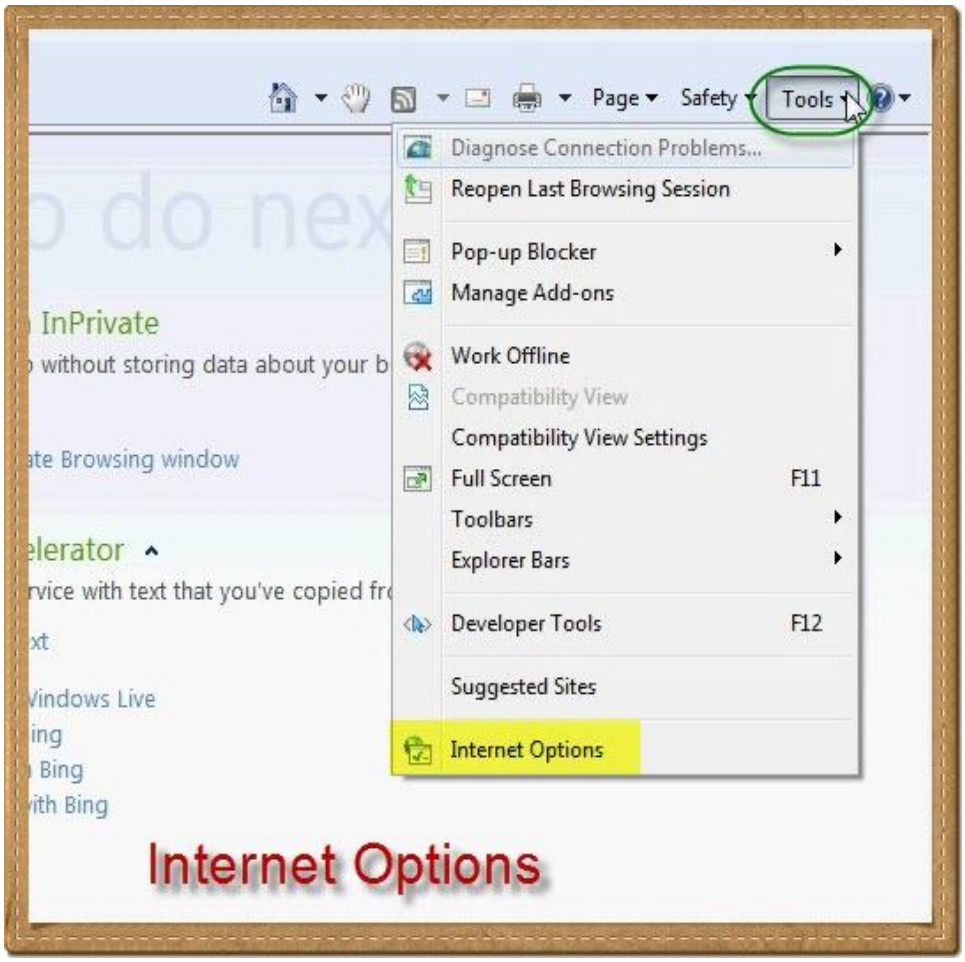
ثم Configure

بلاش تريقه .. هو ده الـ Configure



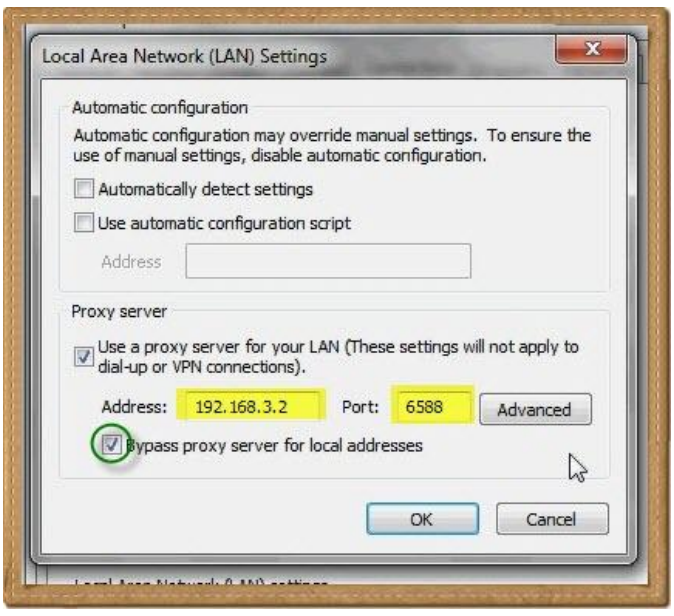
بس كده

ولإعداد الكلاينت للدخول على الإنترنت بطريقة المساكين Internet Options من Tools



Lan Settings من Connections

اي بي الجهاز اللي عليه AnalogX Proxy ورقم البورت ده Default ما بيتغيرش



بس خلاص وح نروح بدري النهارده

اللهم إجعلني خيراً مما يظنون واغفر لي مالا يعلمون

اللهم إني أعوذ بك أن أشرك بك شيء أعلمه وأستغفرك لما لا أعلمه

سبحانك اللهم وبحمدك , أشهد ألا إله إلا أنت , أستغفرك وأتوب اليك

الفصل السادس : Kerio Control

التنصيب

خُد فكرة

Kerio Control

التنصيب

الحمد لله والصلاة والسلام على رسول الله

سيدنا محمد النبي, وأزواجه وذريته وأهل بيته

تعاملنا مع GFI Web monitor ورأينا كيف توجد منتجات عملاقة غير ما تنتجه مايكروسوفت

واليوم مع منتج رائع وقوي ومنافس لـ TMG

وهو Kerio Control الذي كان يعرف سابقا بـ Kerio Win route

هو فايروول قوي للغاية ويتميز بشيء عجيب جداً جداً إنه ويندوز و لينكس , يعني كده تسليك وكده توليع

بإختصار يوجد من Kerio أكثر من أصدارة فمنه نُسخ تعمل تحت ويندوز ونسخ أخرى تعمل كلينكس

نُسخ الويندوز تعمل على الويندوز سفن بكفاءة وتنصيبها عبارة عن : نكست نكست

بالنسبة لنسخ اللينكس فهي تعمل كـ Appliance يعني بتاخد الجهاز من بابه ويصبح الجهاز خاص بها

للتسهيل يوجد على موقع الشركة نسخ appliance جاهزة للعمل من خلال برنامج VMware أو Parallel من غير ماتوجع قلبك في تنصيب وحركات

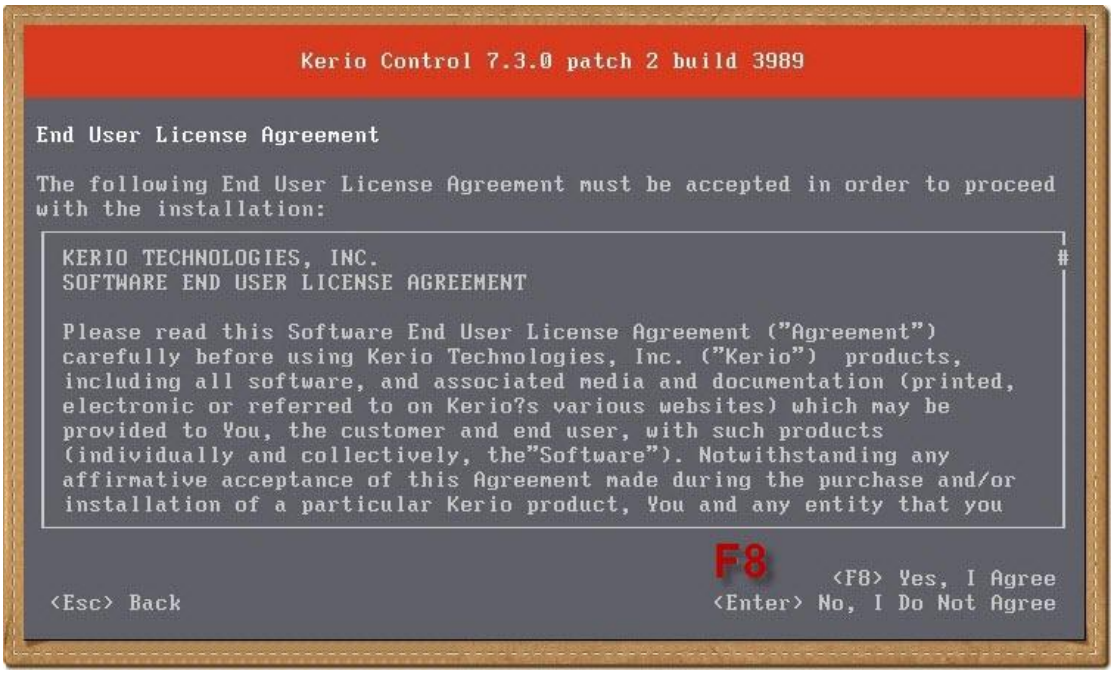
سنعمل بإذن الله مع نسخة اللينكس أو Kerio Control Appliance فتنصيبها شيق وهي فرصة لنا لندخل إلى اللينكس من بوابة منتج ويندوزي

النسخة تكون في صيغة ISO نحرقها على إسطوانة ونعد الجهاز أبو كارتين ليعمل بووت منها

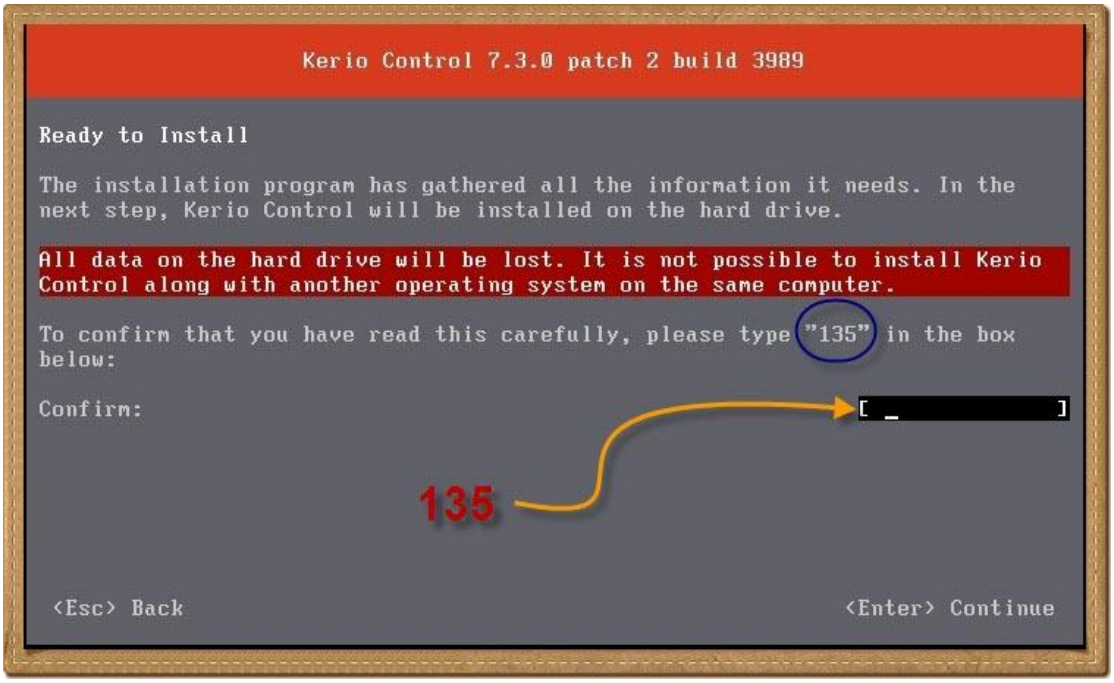
بسم الله يبدأ العمل , نختار الإنجليزية ونضغط Enter

وطبعا Wait

لقبول الإتفاقية نضغط F8



ح يمسح كل حاجة على الهارد .. لو ماعندكش مانع اكتب الرقم ثم Enter



لو عندك مشكلة غير الهارد ☺

دعه يعمل في صمت

وهنا Enter علشان يعمل ريبوت

ماتدوسش على حاجه

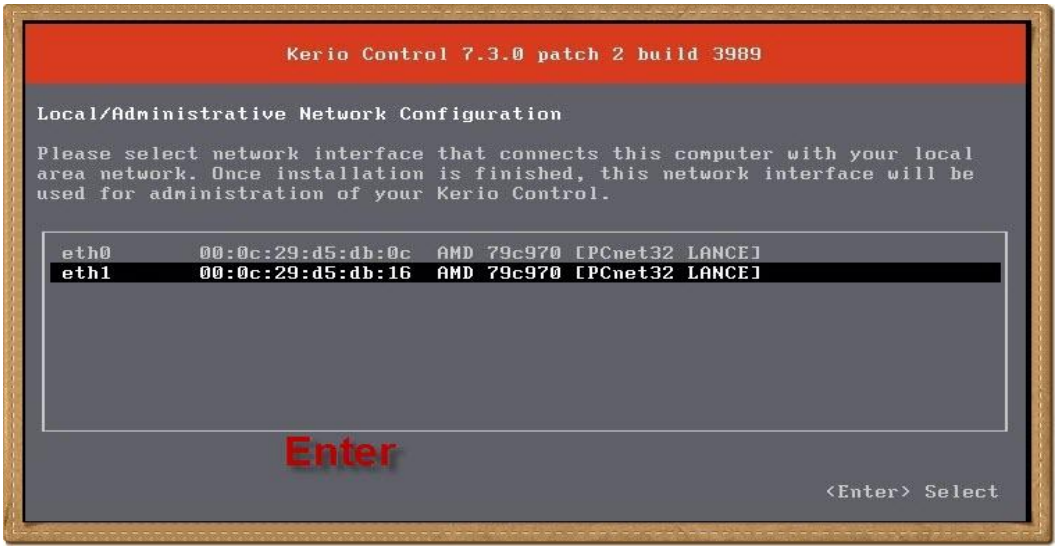
من الشاشة القادمة سنكون : دخلنا في الجد , يطلب منك إعداد الكروت وأيهما يتصل بالإنترنت External وأيهما للشبكة الداخلية Internal أو Local

External = Red = Internet و Internal = Green = Local

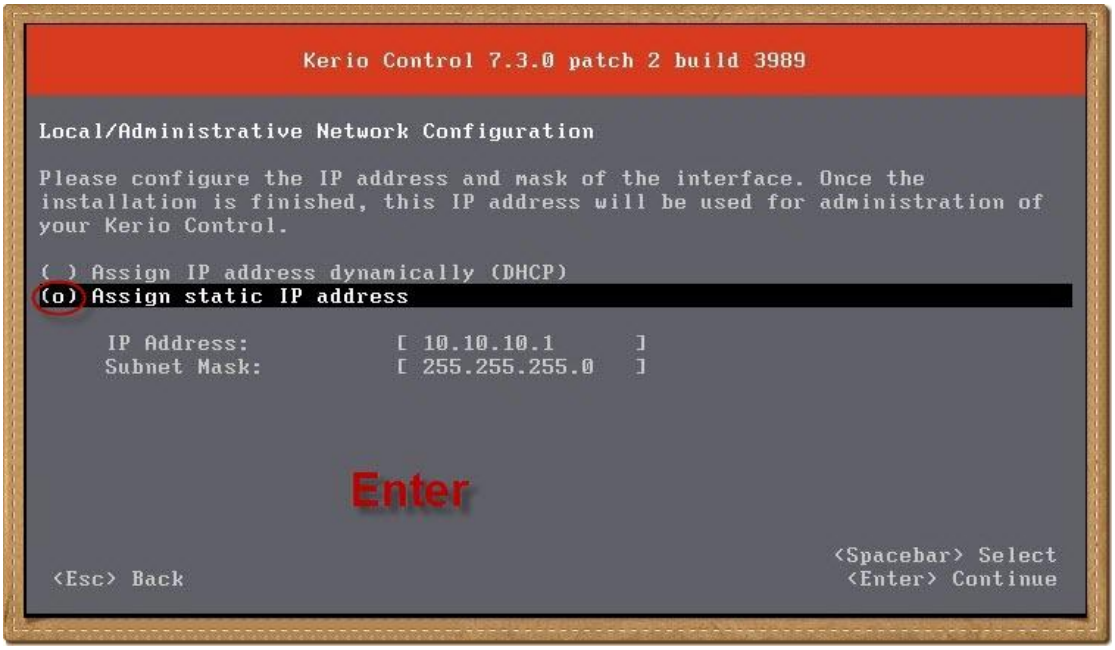
إذا وقعت في مأزق أي الكارتين External أو Internal فلن تجد أمامك إلا الماك أدريس Mac Address لذا يجب أن تعرف الماك الخاص بأحد الكرتين على الأقل قبل البدء

سيطلب منك إعداد الكارت الإنترنال وسنتعرف عليه من خلال الـ Mac Address

نختار الكارت ثم Enter

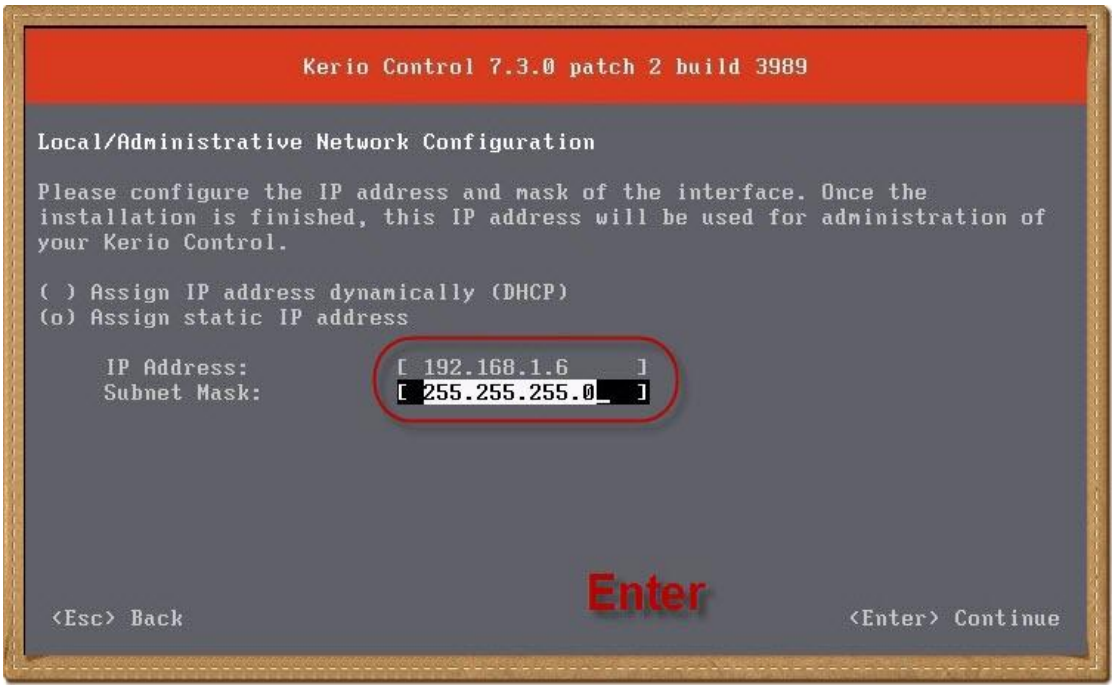


نختار إدخال الـ اي بي يدويا Static IP



طبعا هذا الـ اي بي سيصبح Gateway للكلاينتس

نضغط Enter بعد الإنتهاء



تلقائيا ح يكون الكارت الآخر هو الـ External ويمكننا تغيير إعداداته فيما بعد

نضغط Enter للإنتهاء من الإعداد

وكمان Enter

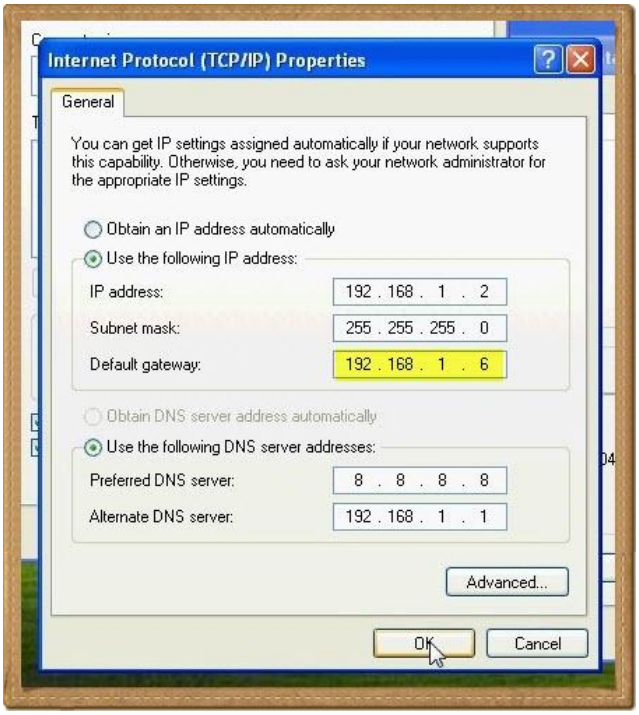
وبكده ح ندخل في مرحلة جديدة

وهي التعامل مع الجهاز من خلال Web Administration

عن طريق الدخول ريموتلي بالـ URL الموجود بالصورة

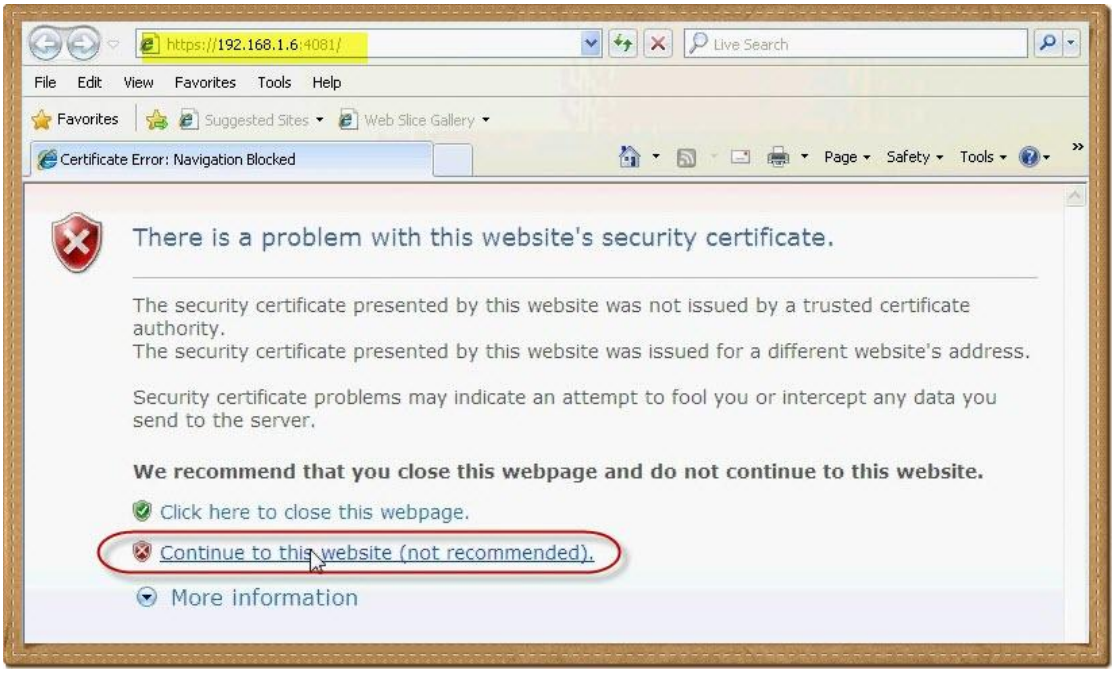
غالبا بالنسبة لسيرفرات اللينكس تتم إدارتها ريموتلي من خلال واجهة Web تعمل على المتصفح من خلال أي جهاز متصل بالشبكة

من غير كلام كتير نفتح جهازنا , وأعني بجهازنا هو جهاز عليه ويندوز ومتصل بالشركة وعايزين ندير الـ Kerio منه , نراجع إعدادات الشبكة ونركز في الـ Default Gateway

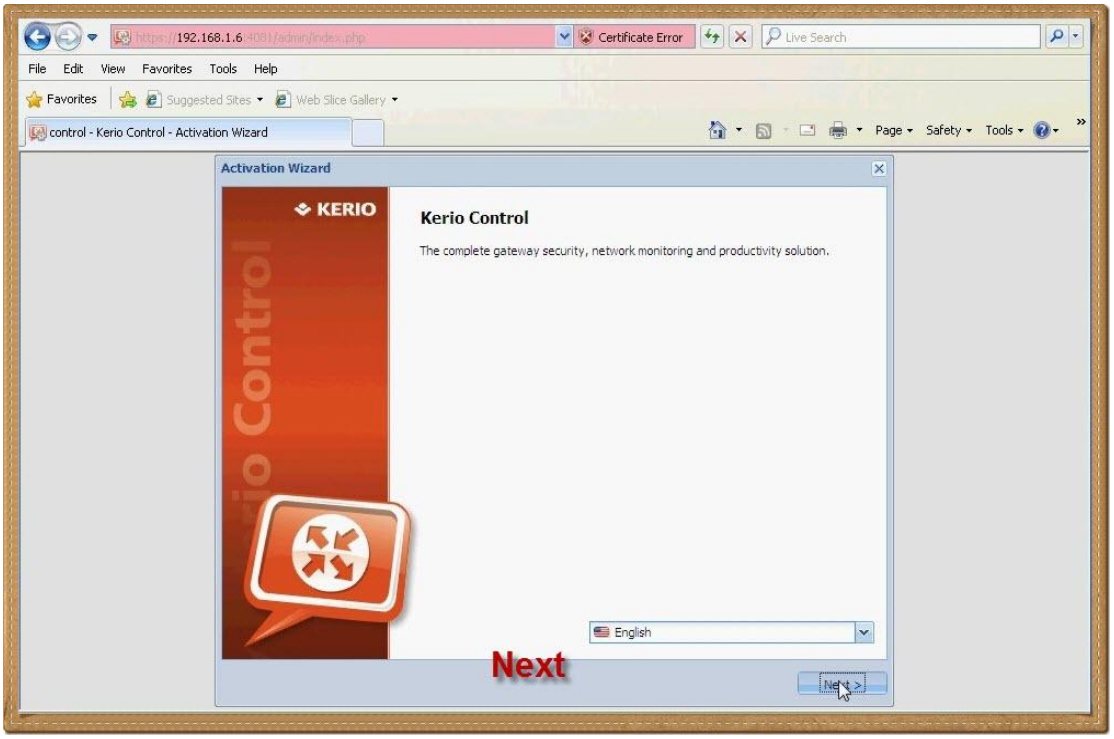


نفتح المتصفح ونكتب الـ URL وهو عبارة عن اي بي الـ Kerio Server وبورت 4081

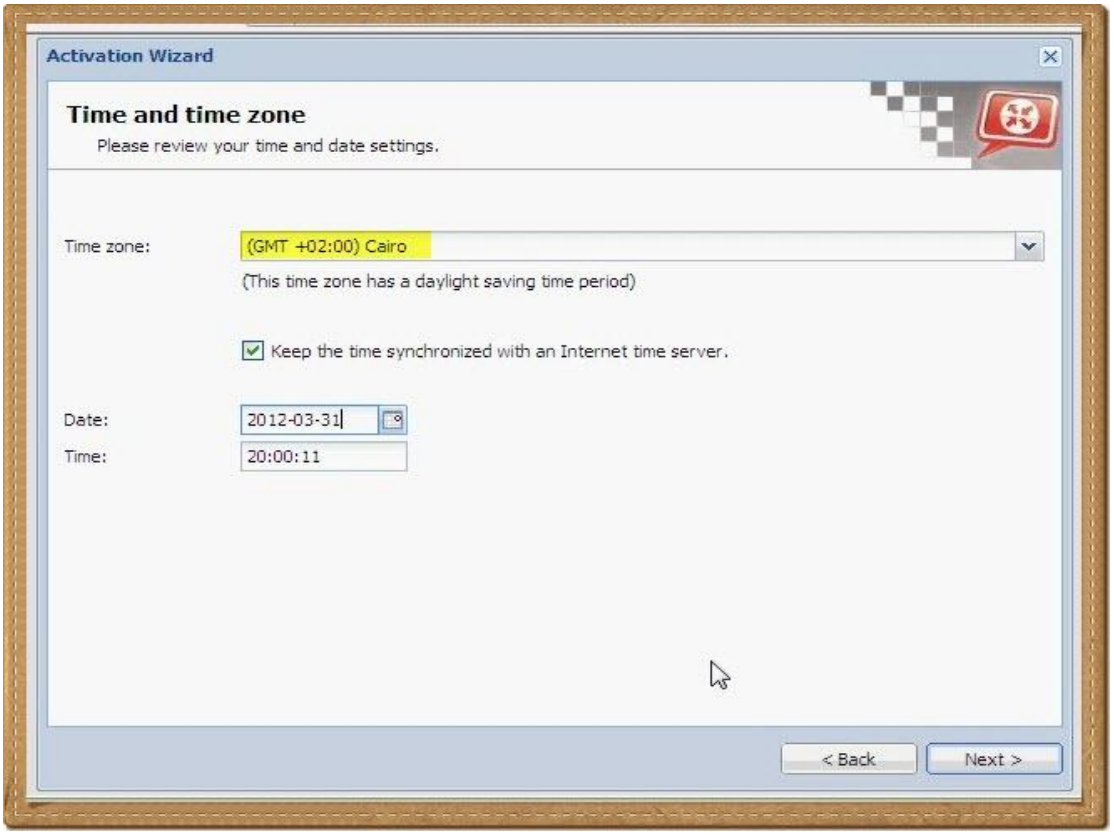
نختار Continue to the website



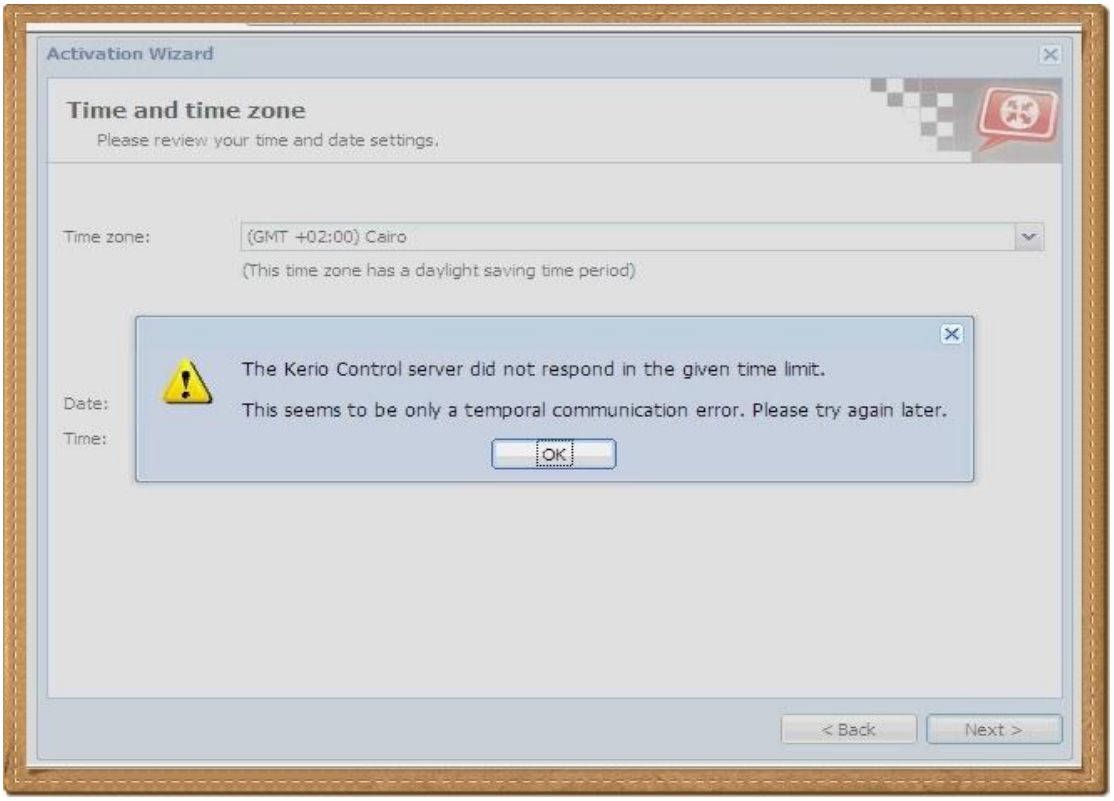
نجحنا في الإتصال ونكمل آخر مرحلة من الإعداد , طبعا Next



إعداد التوقيت و Next



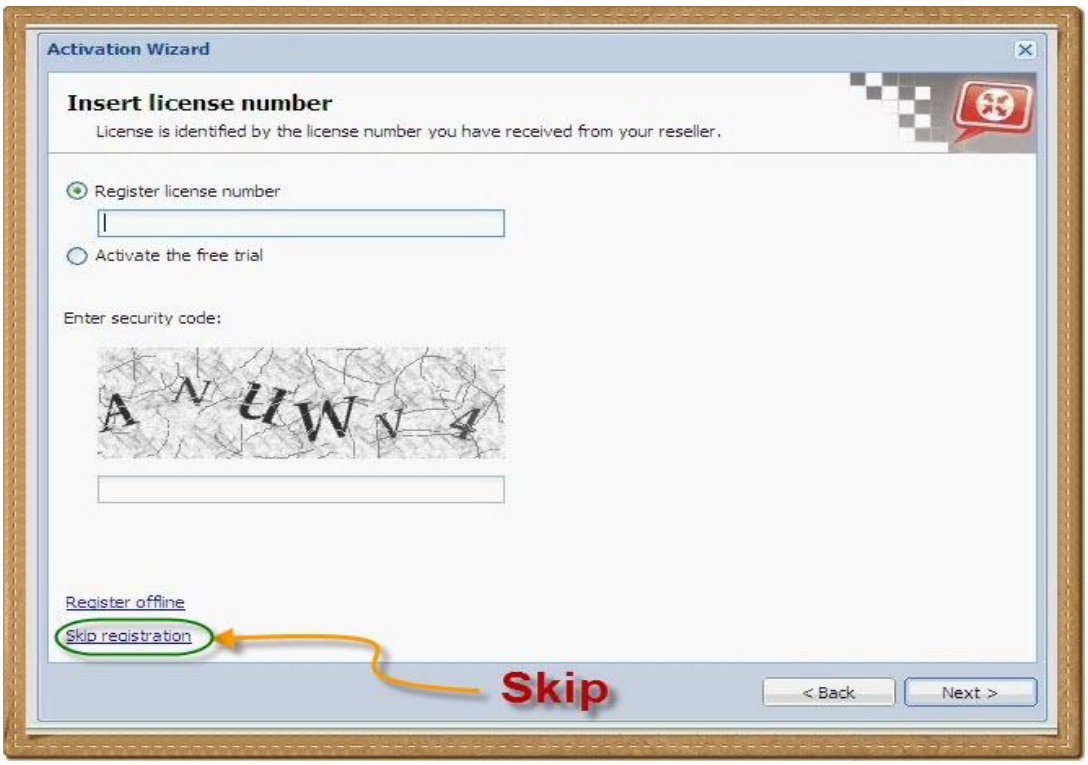
ممكن يقابلك Error



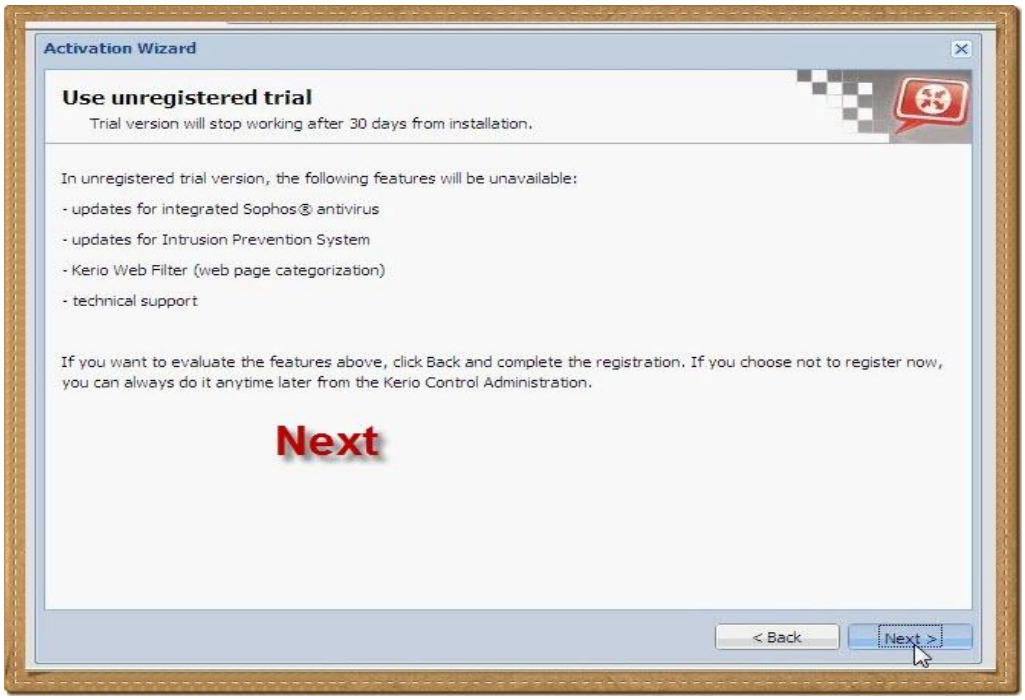
لتلافي الـ Error إلغي خيار الـ Sync الخاص بالتوقيت وبعدين Next

لو عندك Serial إكتبه أو إختار إنك تخليها نسخه Trial وتسجل حساب

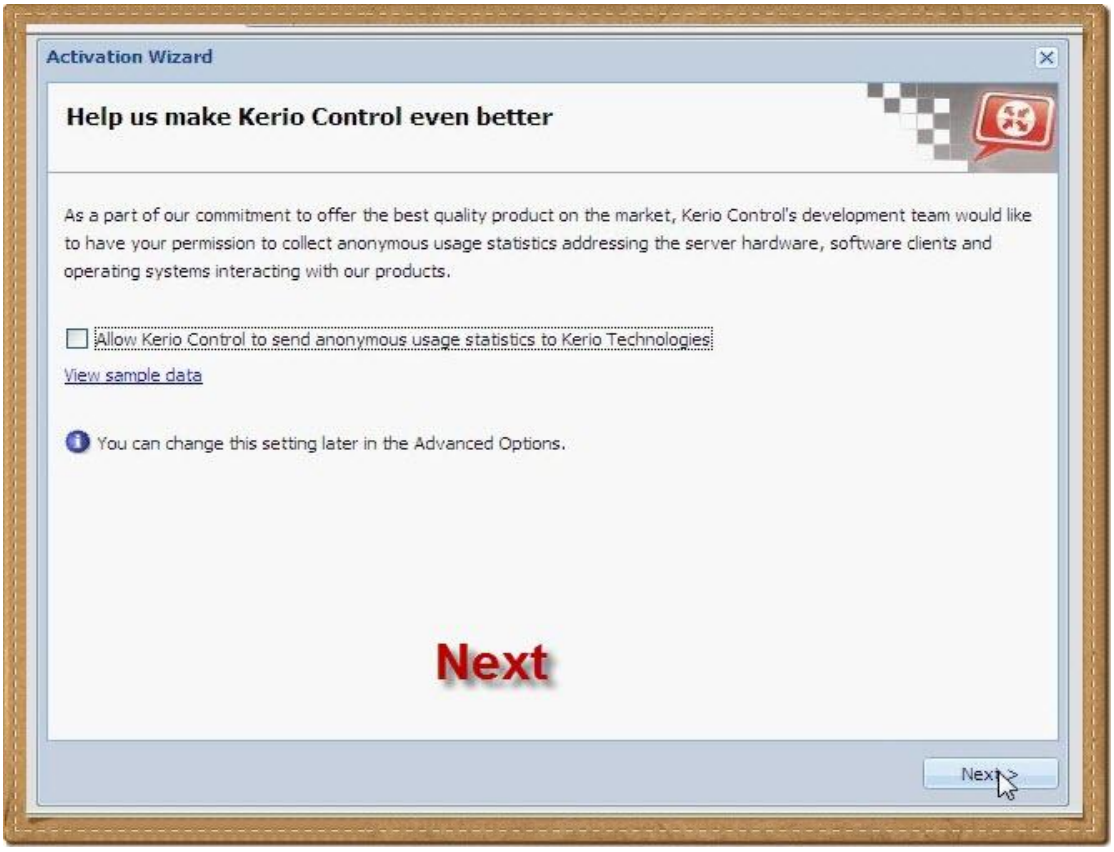
عن نفسي سأختار Skip Registration



نسخة مجانية لمدة 30 يوم وجزء كبير من إمكانياتها لا يعمل . Next



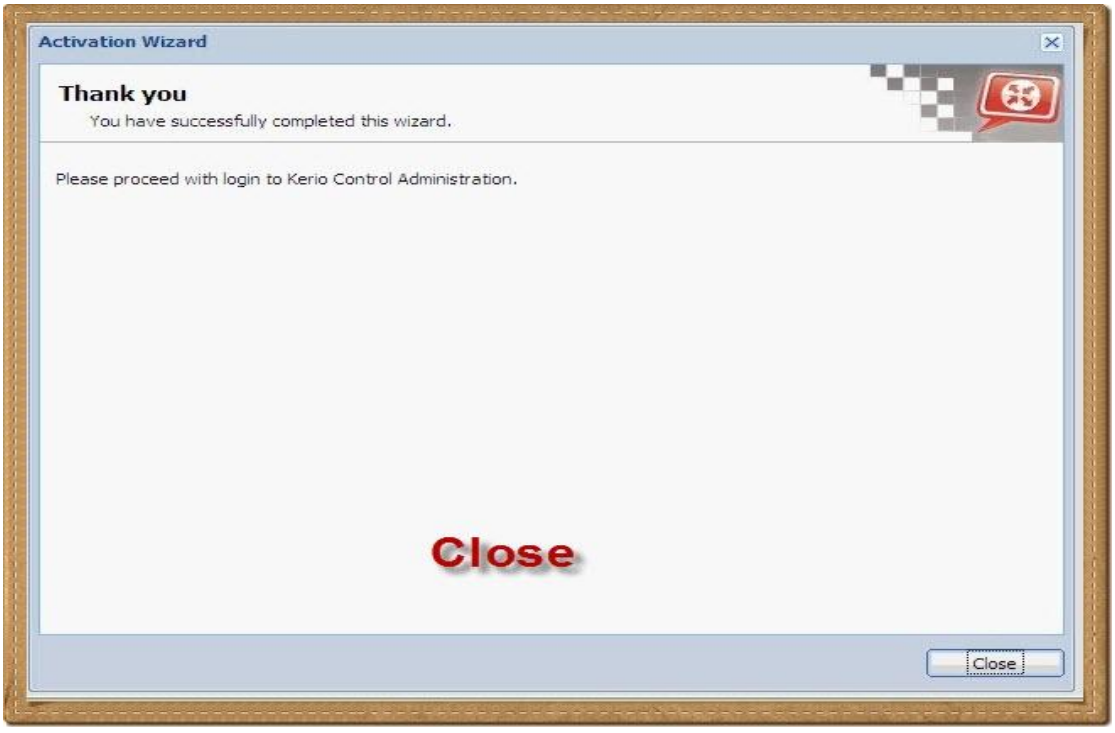
Next



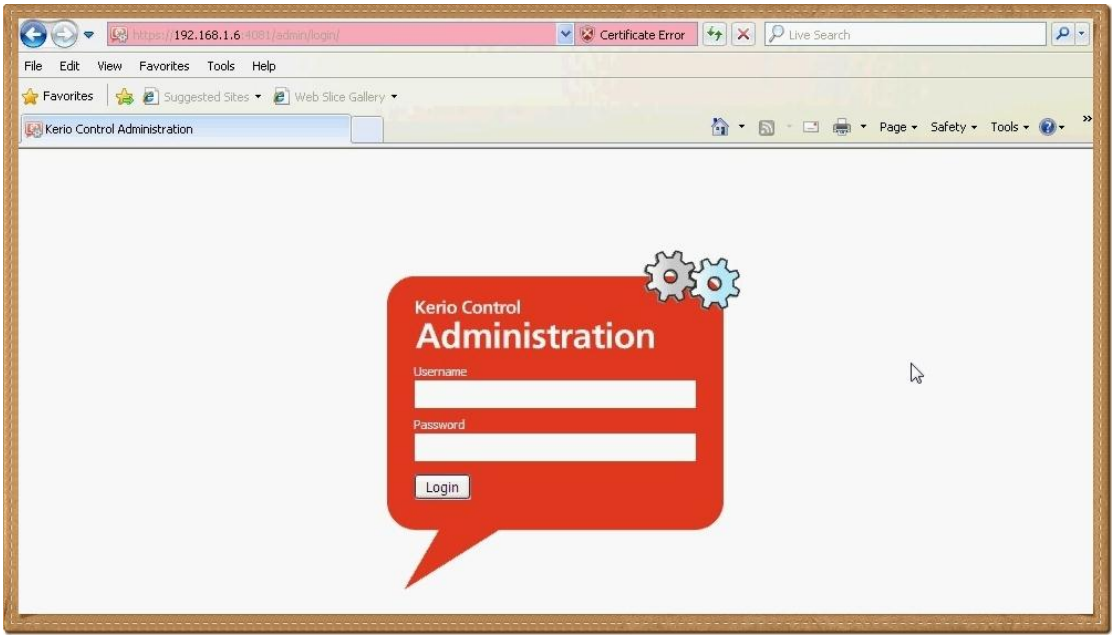
تحديد كلمة سر للـ Admin

وأخيرا Finish

و Close

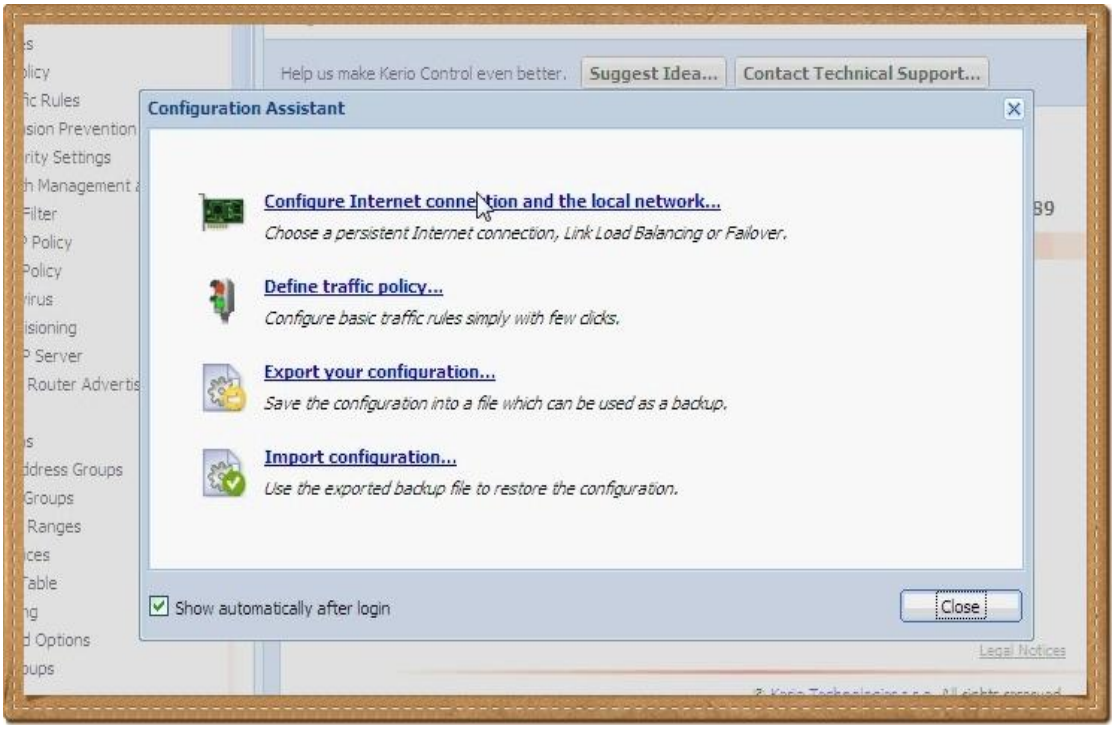


سيطلب منك إسم المستخدم وكلمة السر



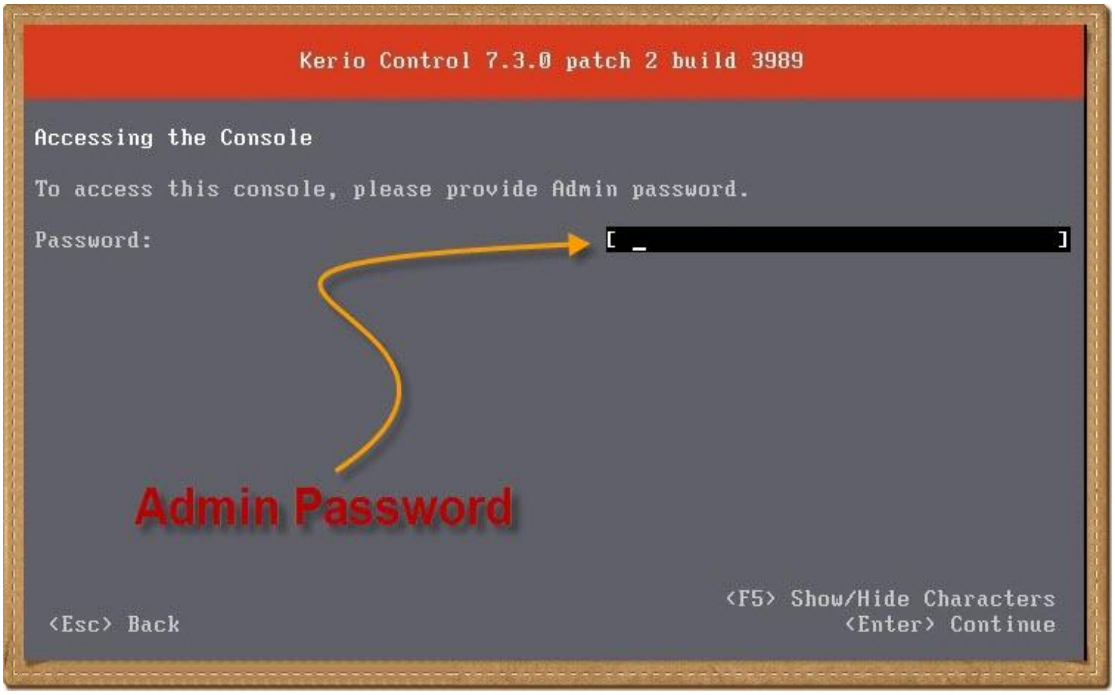
Admin والباسوورد

معالج لمساعدتك , إقفله مش مشكله لإن كل ده تقدر تعمله من الداخل



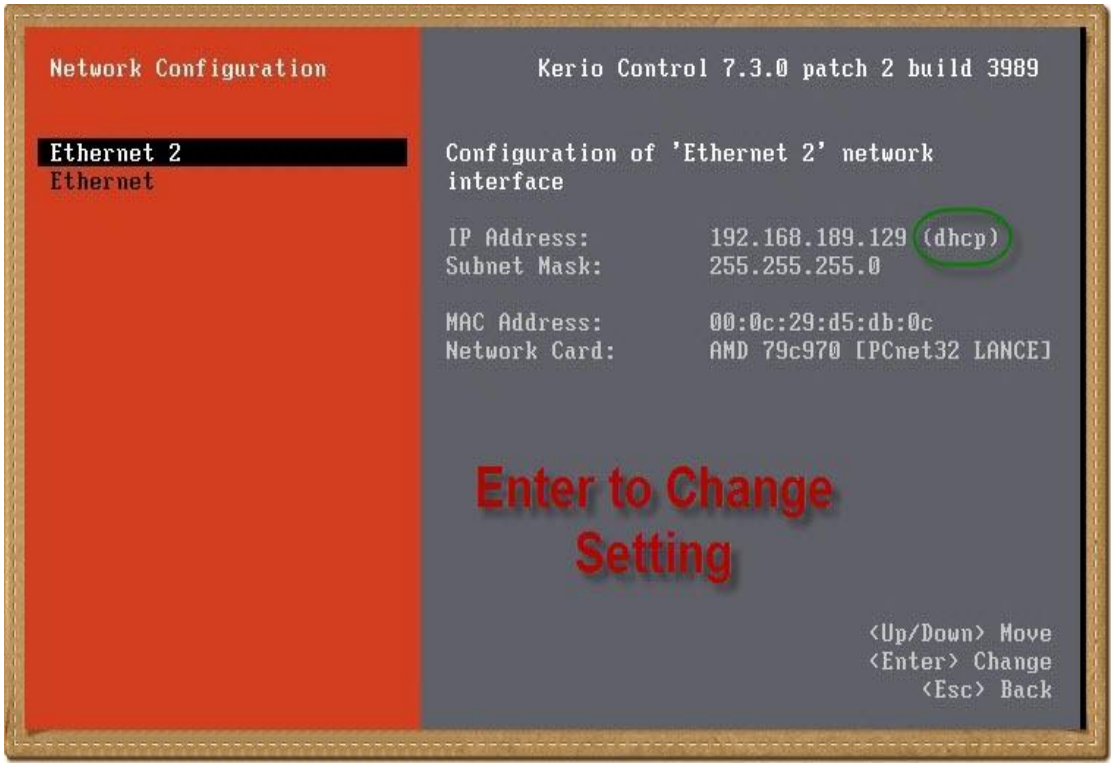
نرجع لجهازنا نبص بصه أخيره , نضغط Enter

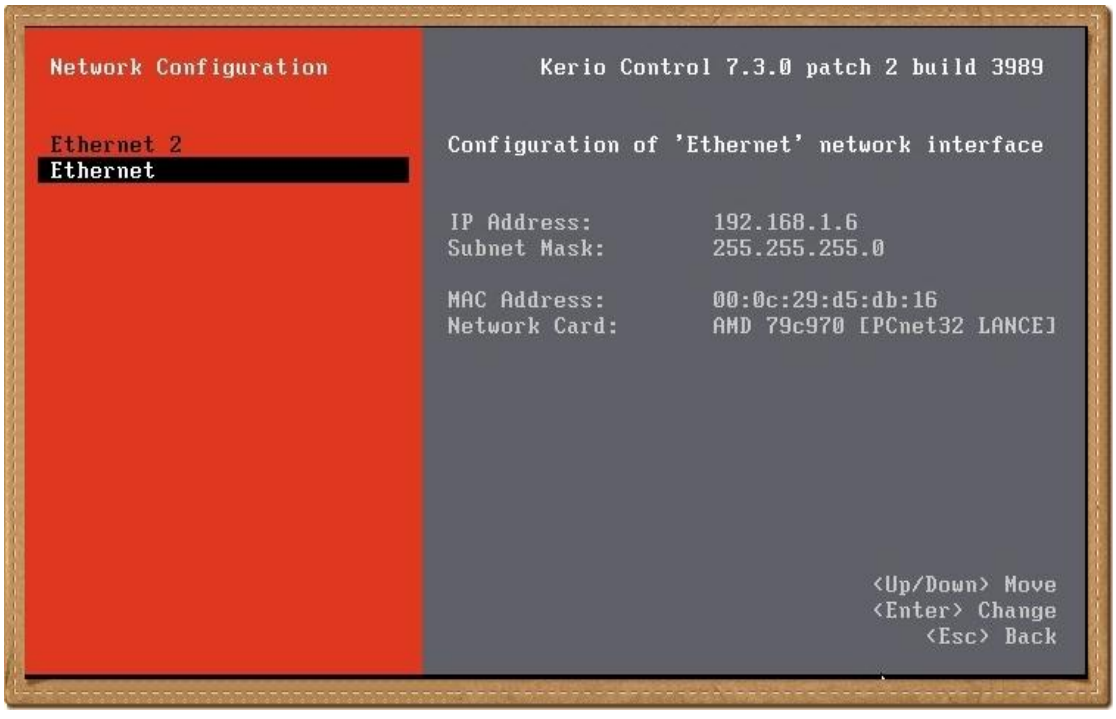
سيطلب كلمة السر للأدمن

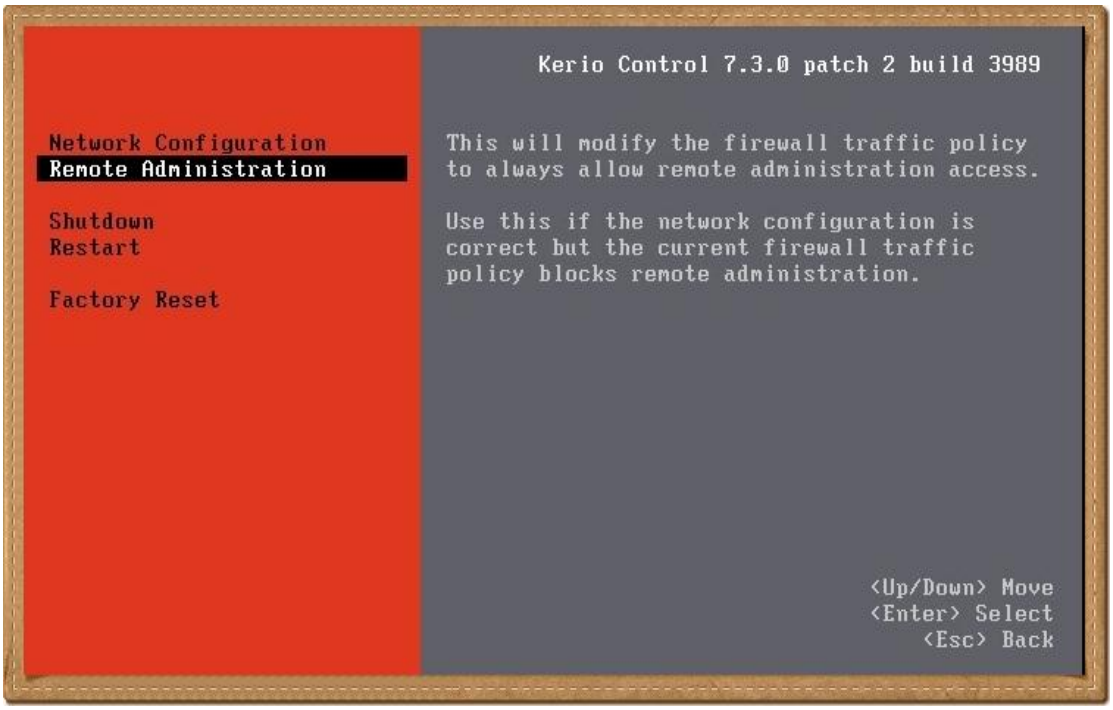


ومن هنا يمكننا تعديل إعدادات الكروت ثانية , نضغط Enter

ياريت مانلعبش في حاجه





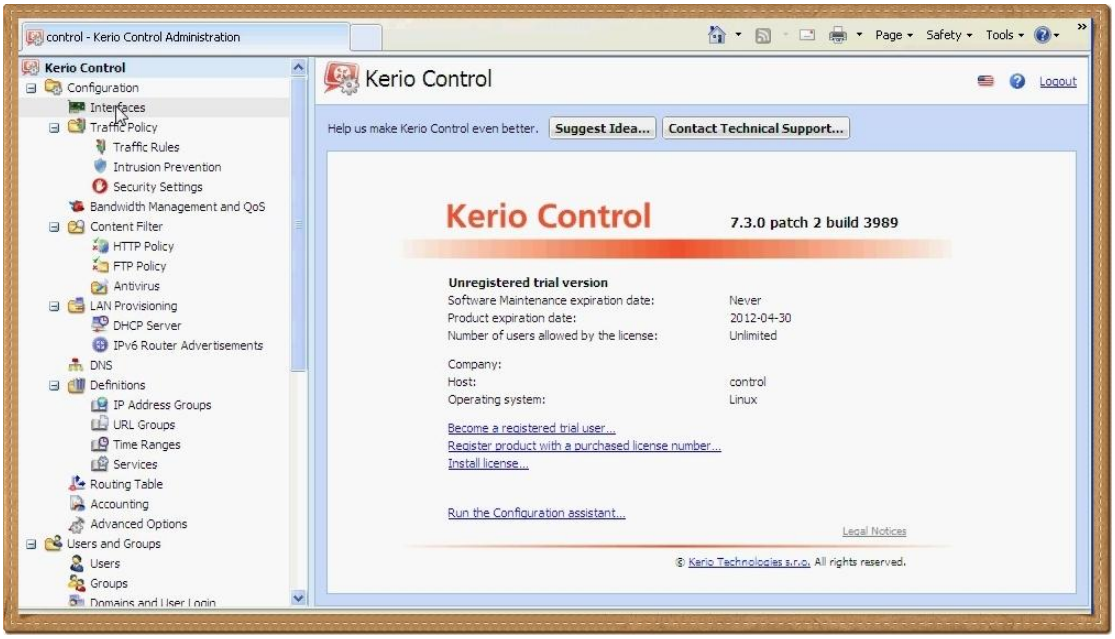

Kerio Control 7.3.0 patch 2 build 3989
Network Configuration
Remote Administration
Shutdown
Restart
Factory Reset
This will modify the firewall traffic policy to always allow remote administration access.
Use this if the network configuration is correct but the current firewall traffic policy blocks remote administration.
<Up/Down> Move
<Enter> Select
<Esc> Back


Kerio Control 7.3.0 patch 2 build 3989
Kerio Control is running on this computer. To change settings, please point your browser to:
https://192.168.1.6:4081/admin
<Enter> Access Console

وهنا Shutdown و Restart

أو Factory Reset

وكفايه كده



وإن شاء الله ناخد فكره في الفصل القادم

اللهم إجعلني خيراً مما يظنون واغفر لي مالا يعلمون

اللهم إني أعوذ بك أن أشرك بك شيء أعلمه وأستغفرك لما لا أعلمه

سبحانك اللهم وبحمدك , أشهد ألا إله إلا أنت , أستغفرك وأتوب اليك

Kerio Control

خُد فكره

الحمد لله والصلاة والسلام على رسول الله

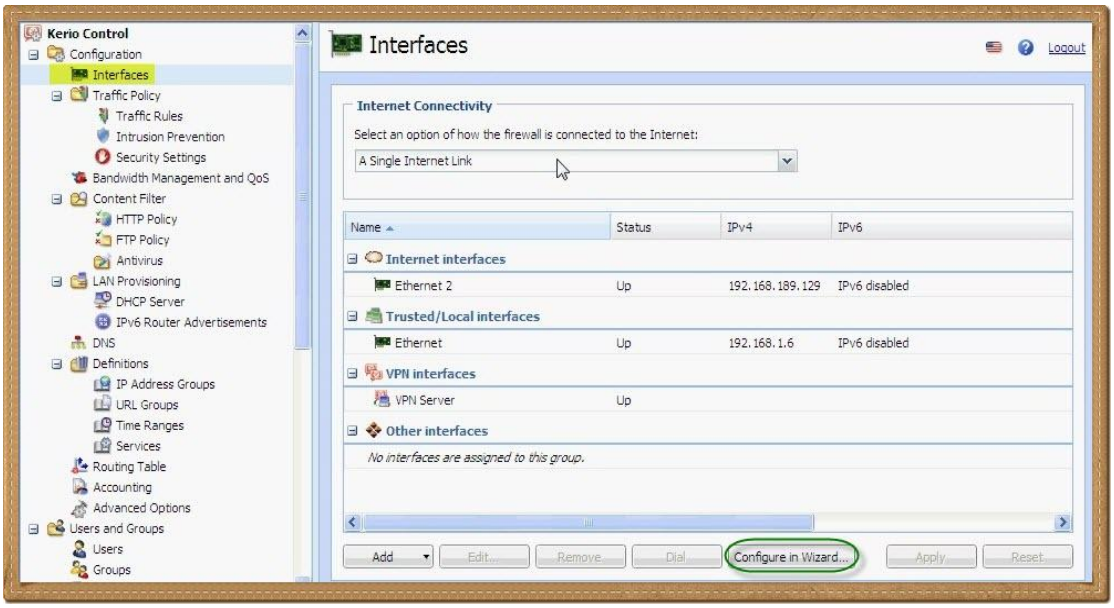
سيدنا محمد النبي, وأزواجه وذريته وأهل بيته

إنتهينا من تنصيب Kerio Control وبقي أن نتمشى داخله شويه , يعني ناخد فكره ونشتري بكره

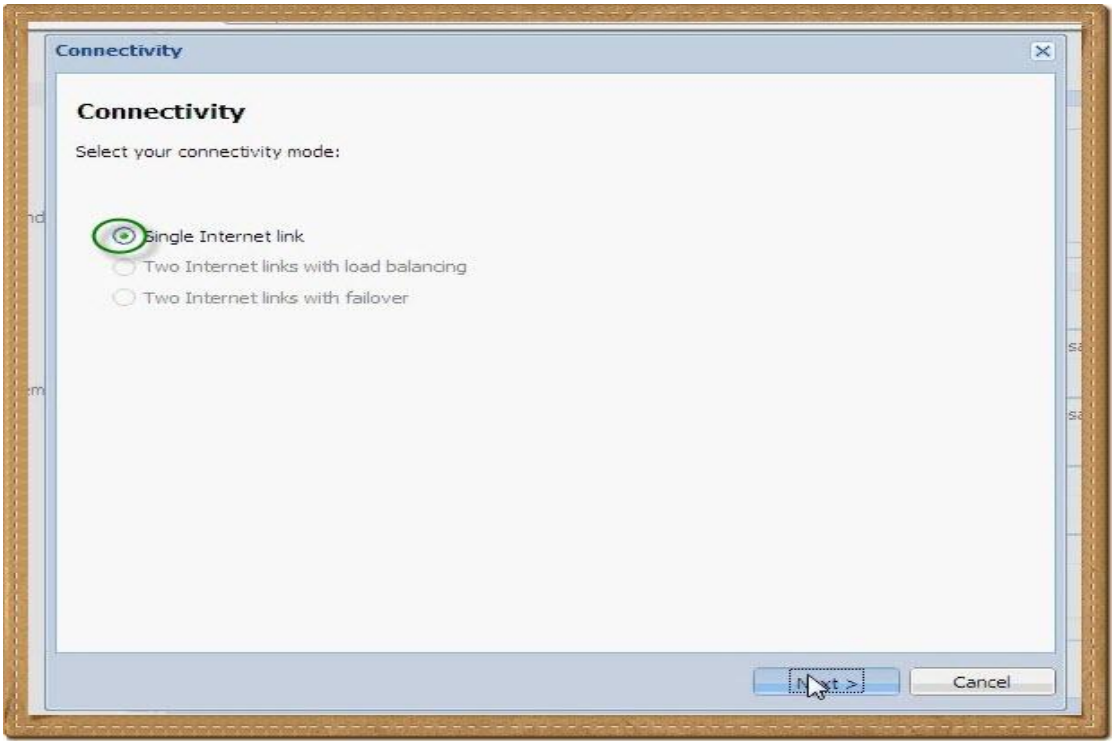
مادمنا إنتهينا من التنصيب فالعمل سيكون Remotely كما بدأنا في نهاية الدرس السابق

على جهازنا نكتب الـ URL في المتصفح وبعد إدخال اليوزر نيم والباسوورد نتوكل على الله

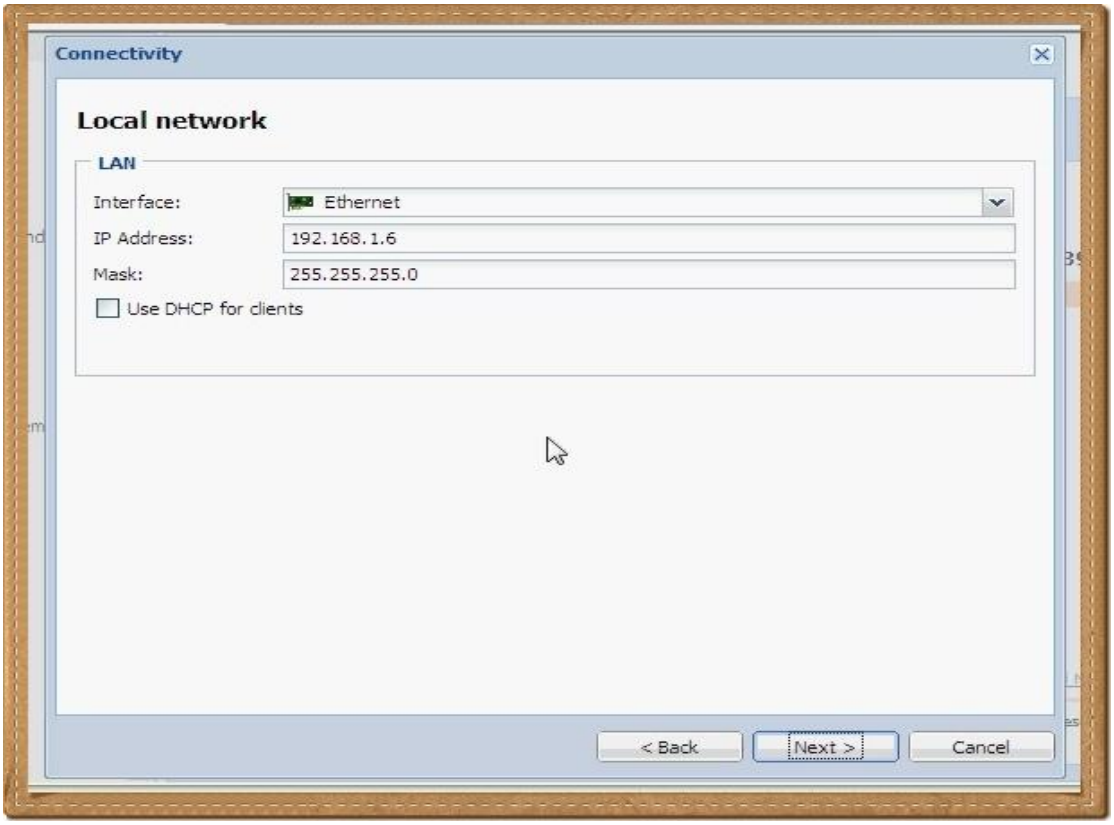
هنا الشاشة الخاصة بالـ Interfaces وتتعامل مع الكروت ونوعية الإتصال , نضغط على Configuration Wizard



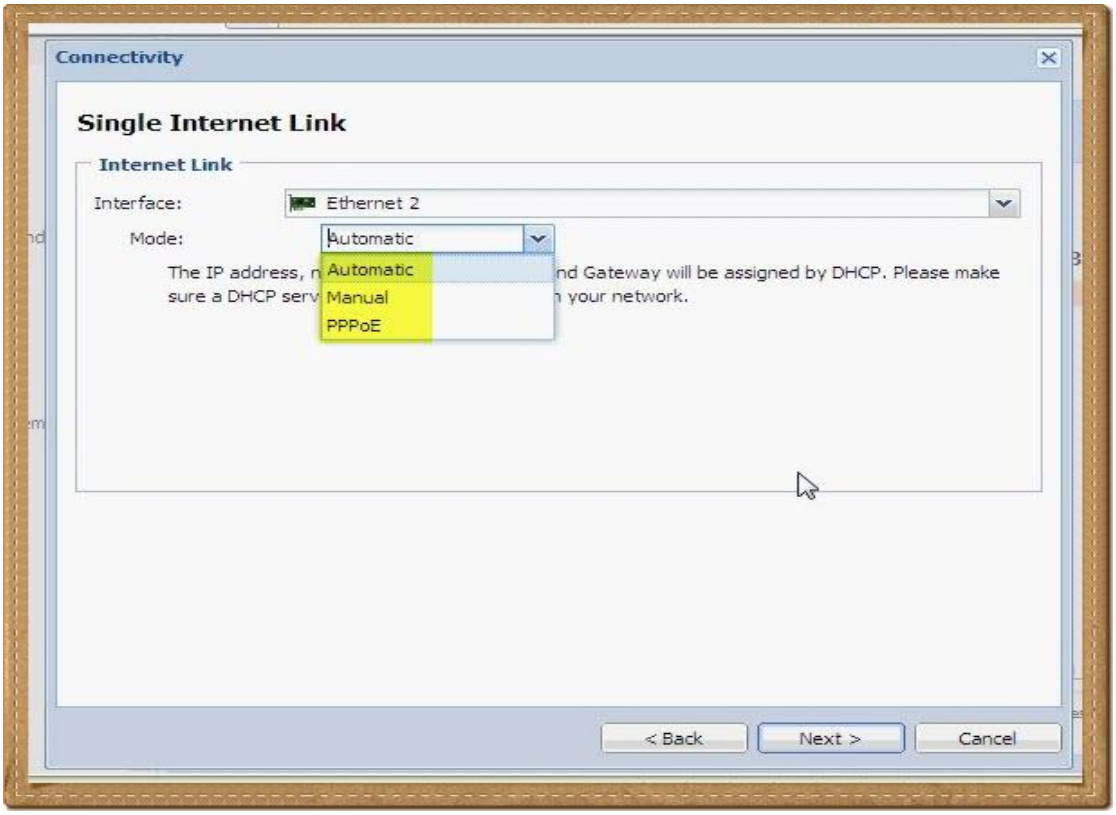
لا يوجد لدينا أي خيارات وهذا طبيعي فالجهاز متصل بكارت داخلي وآخر خارجي فقط



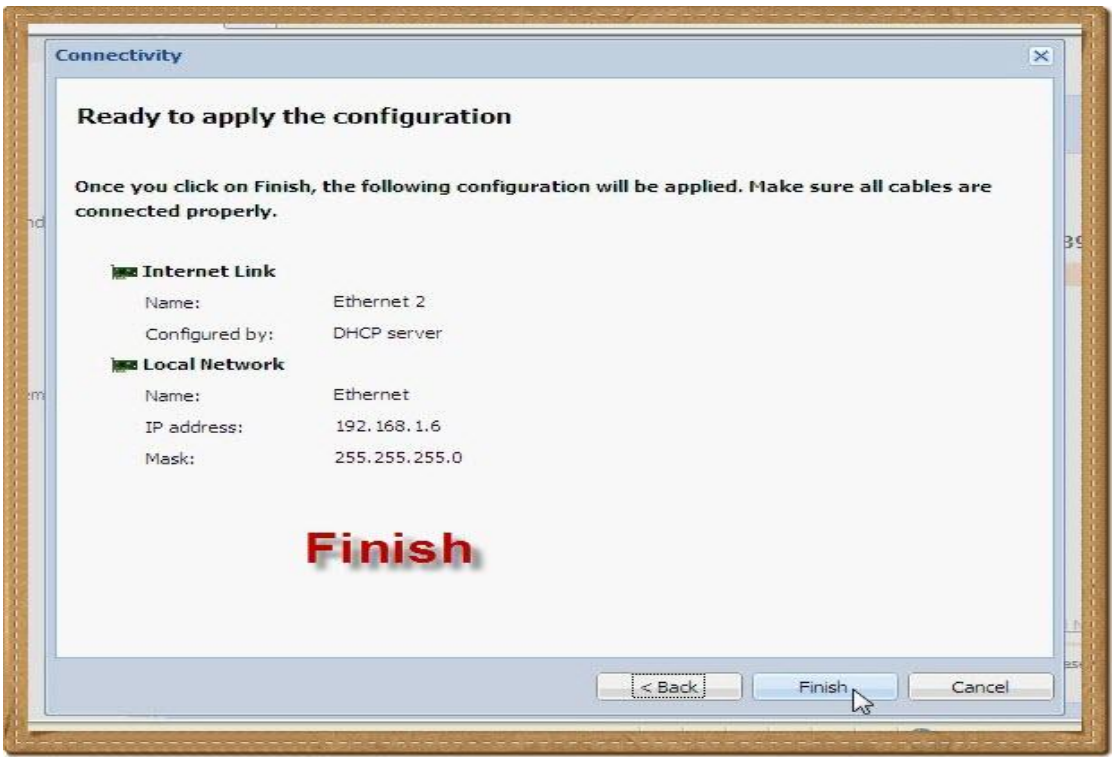
الكارت الـ Internal وإعداداته



الكارت الخارجي External وإعداداته

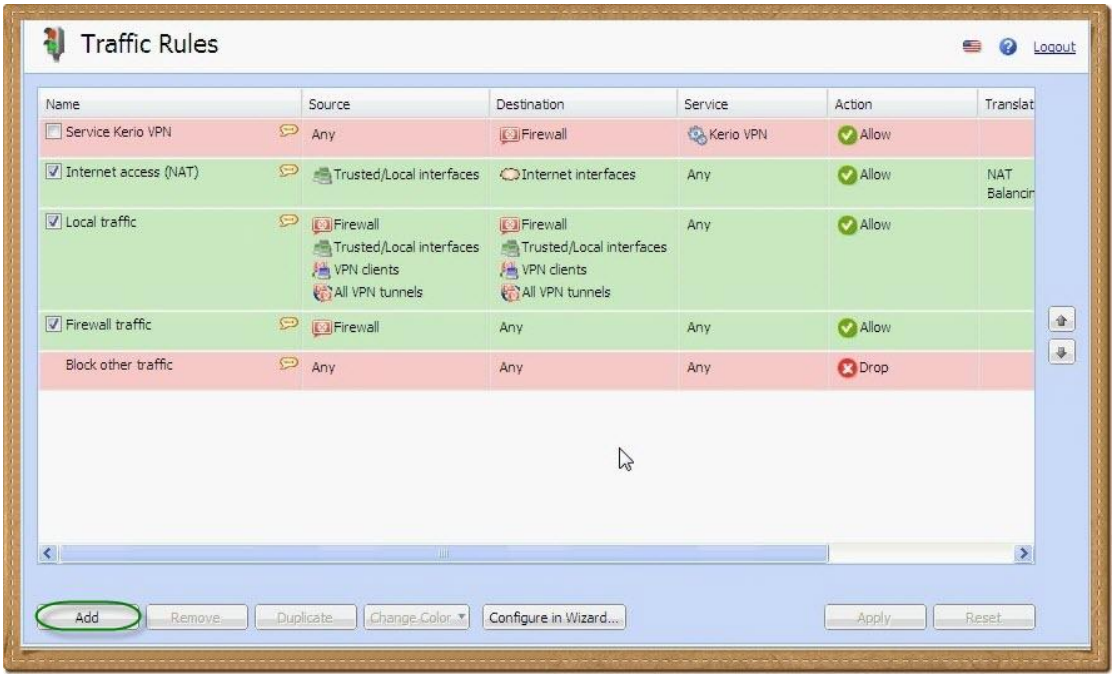


وFinish



الـ Traffic Rules

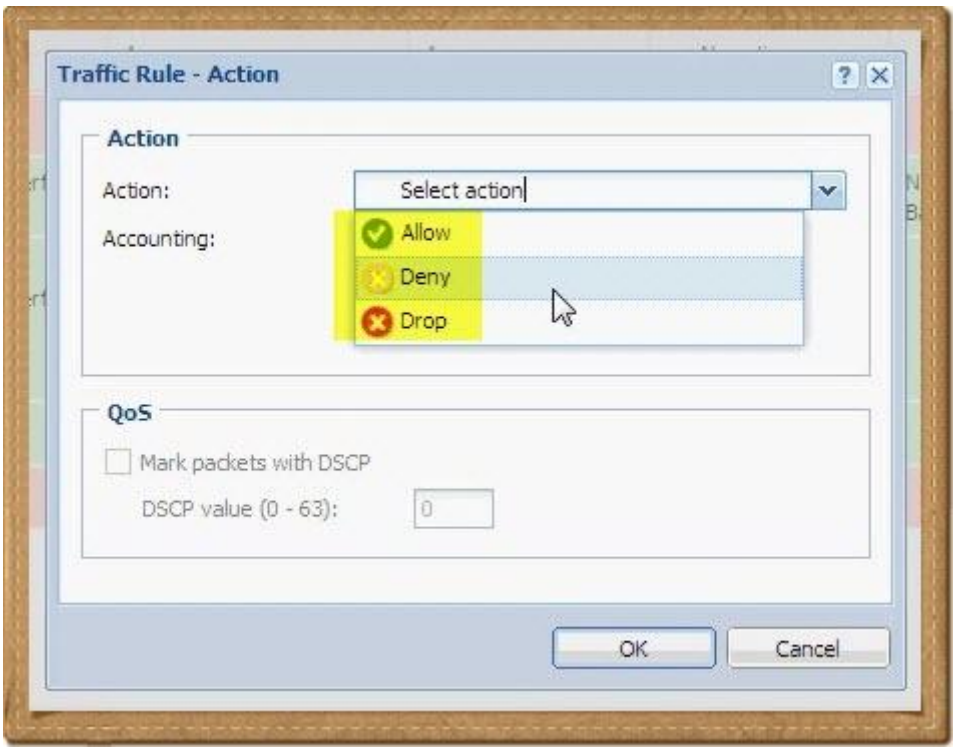
لإضافة Rules نضغط على Add أو يمكننا إستخدام المعالج Wizard



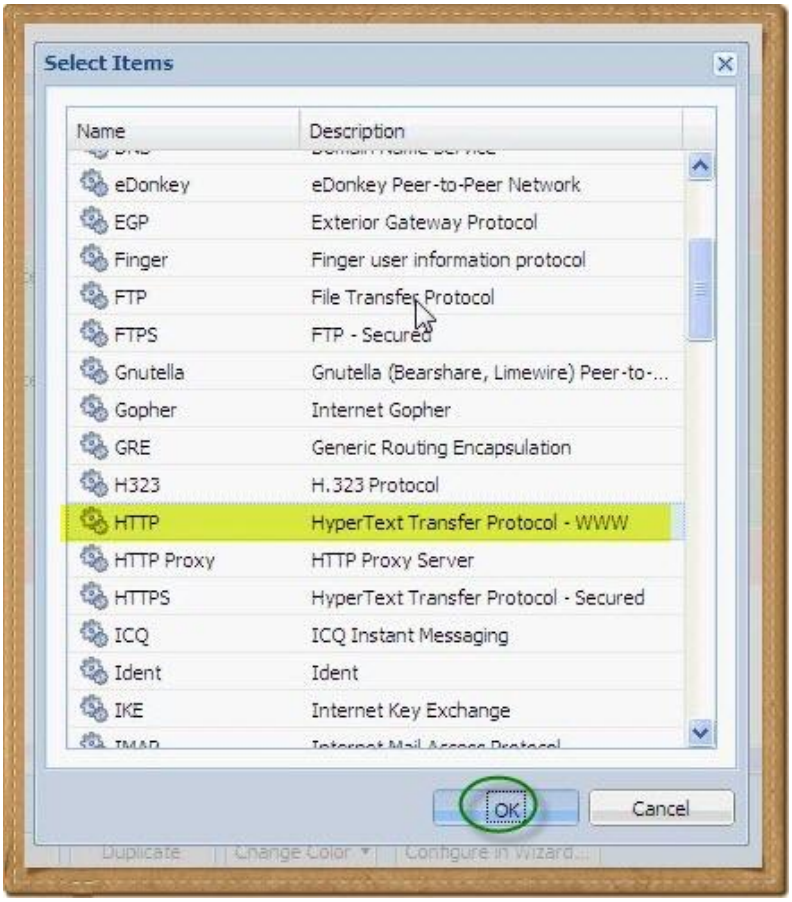
تغيير إسم الرول الجديدة

علامة صح بجوار الرول تعني تفعيلها

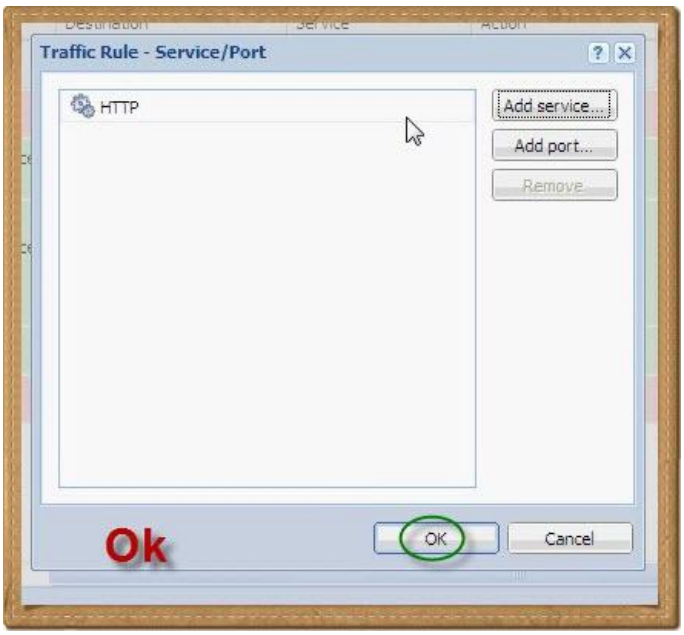
دابل كليك على أي جزء من الرول لتعديله , نجرب تعديل الـ Action



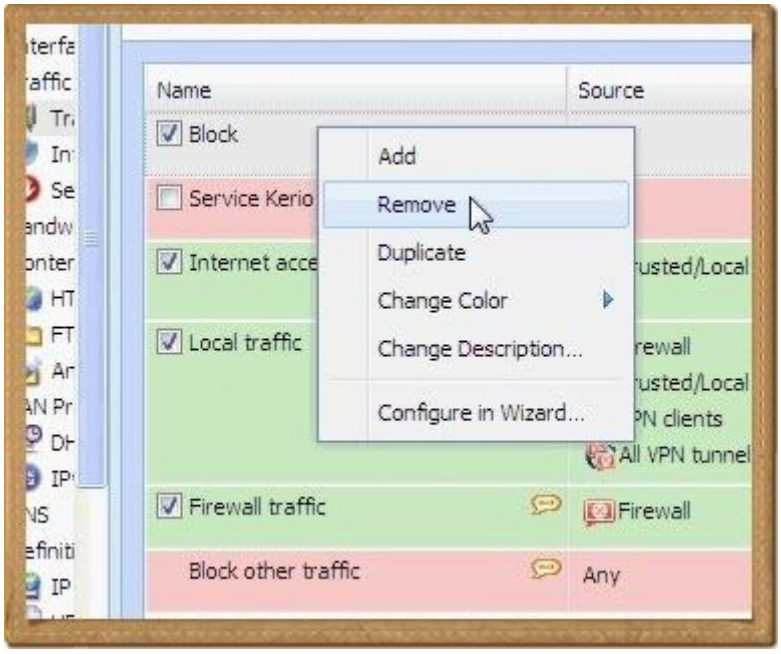
ومن هنا سنختار البروتوكول الذي ستطبق عليه الرول ونضغط Ok



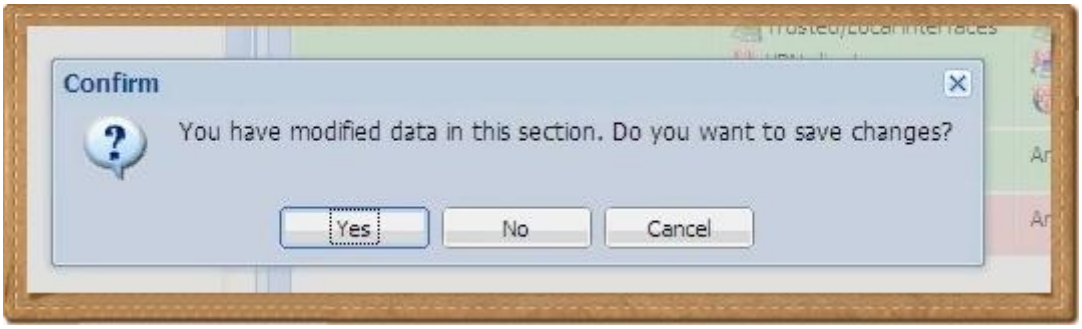
من الممكن إضافة المزيد أو تحديد بورتات معينه , كفايه كده



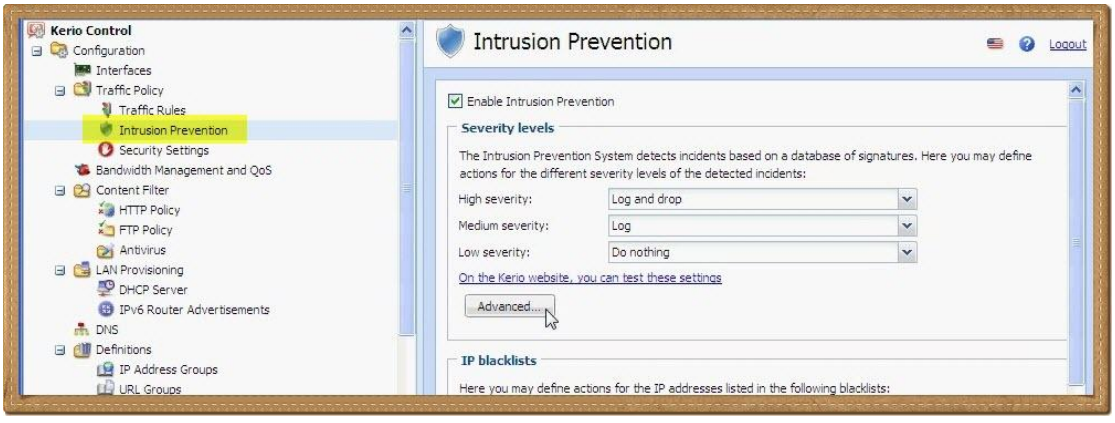
كليك يمين على الرول لوظائف إضافية , إمسح يابني



رسالة التأكيد هذه ستقابلنا دائما



وهنا خاصية Intrusion Prevention كالموجودة في TMG

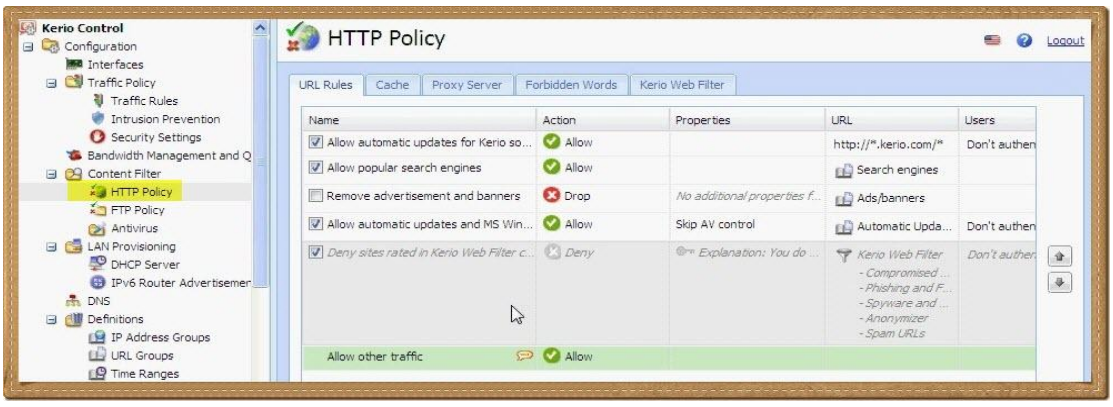


والـ Security Settings

لاحظ التعامل فيه مع الـ Mac Address لأجهزة الكلاينتس , نقدر نمنع أو نسمح لجهاز أو مجموعة

كنت أتمنى أن يكون به خاصية الـ Scan للشبكة لعرض الأجهزة المتاحة

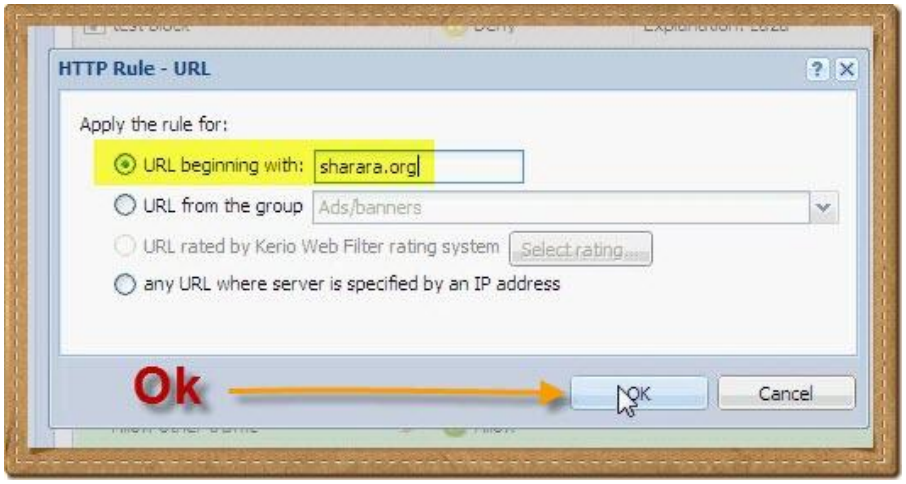
والآن : الفلاتر , إضافة فلتر من الأسفل كالسابق



نوع الفلتر , نختار Deny لإني بحب الـ Deny جدا

الرسالة التي ستظهر للمستخدم عند تطبيق الفلتر

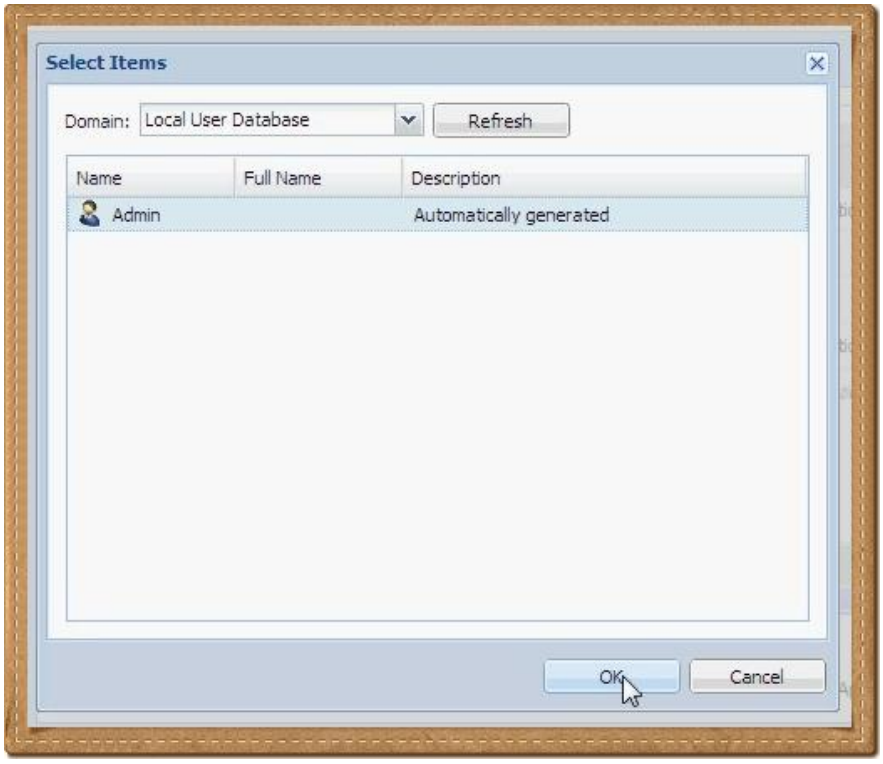
إخترنا Deny وهنا سنحدد ماهي المواقع التي سيتم التطبيق عليها



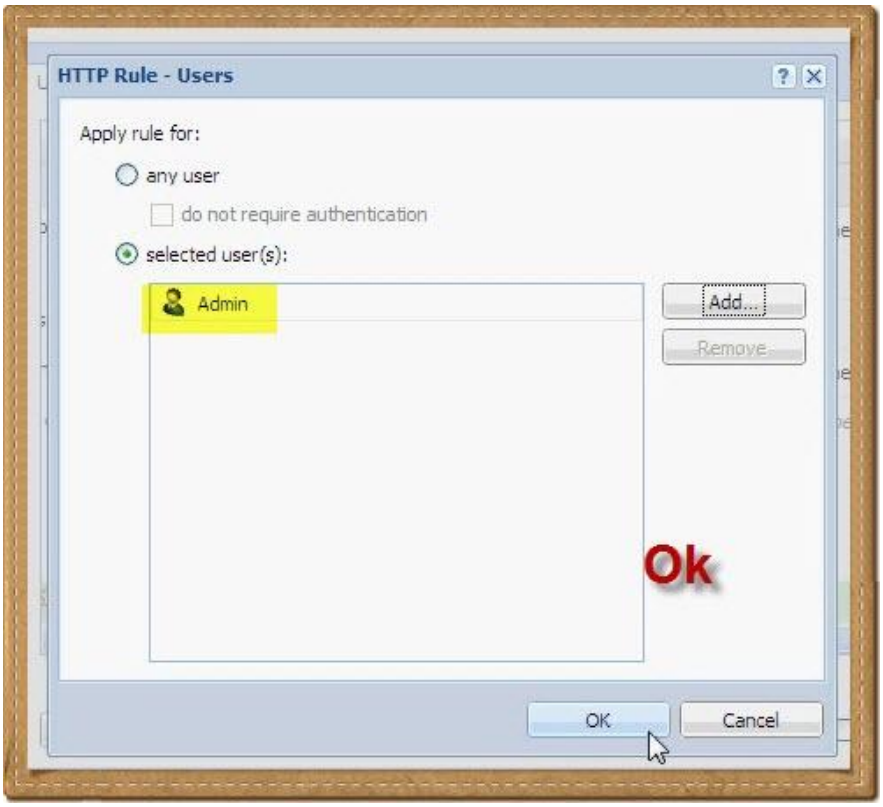
ومين المستخدم اللي ح يتمنع عنه

Add لإضافة مستخدم

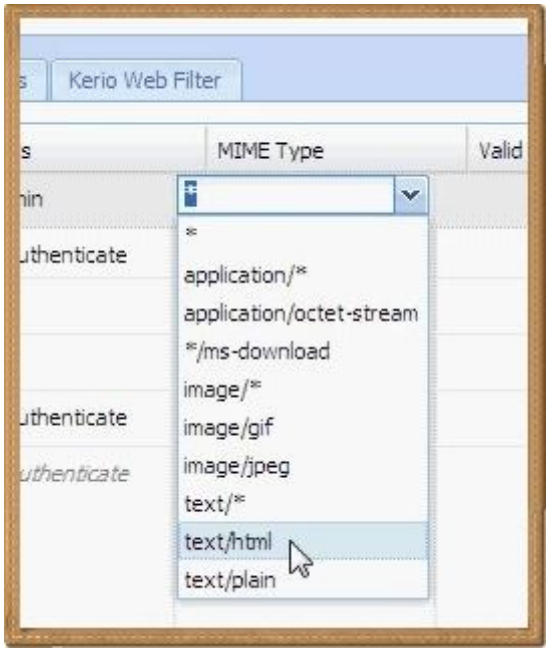
نختار الـ Admin



و Ok



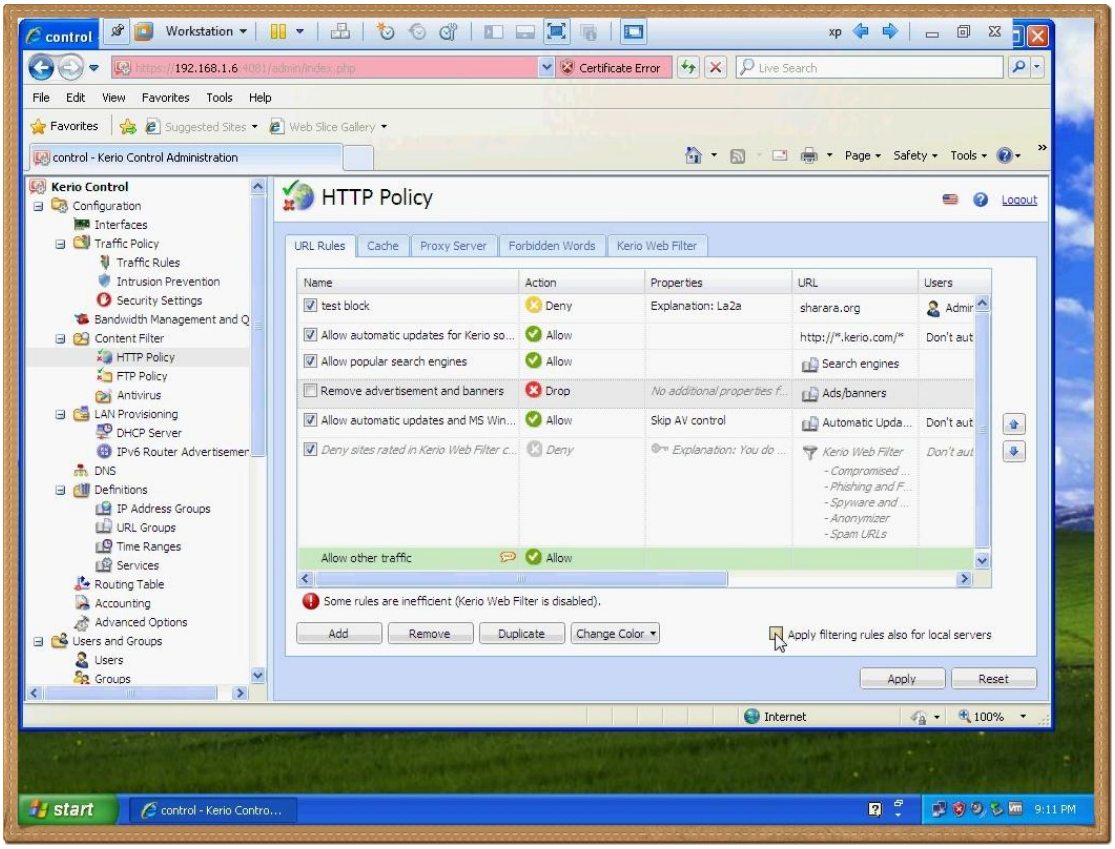
ماهي أنواع الملفات التي ستمنع , MIME Types



متى سيتم تطبيق الفلتر

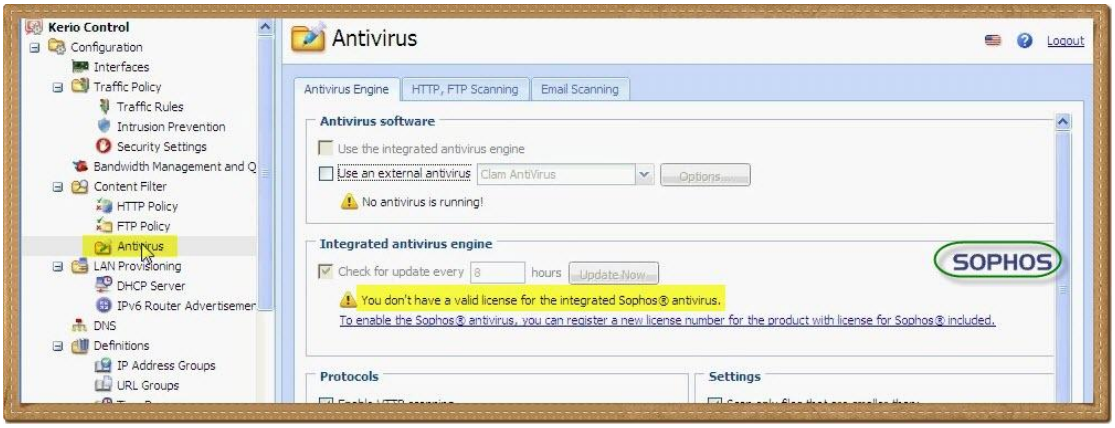
فلتر عجيب يمنع الأدمن من موقع sharara.org بصراحه عيب

إمسح يابني

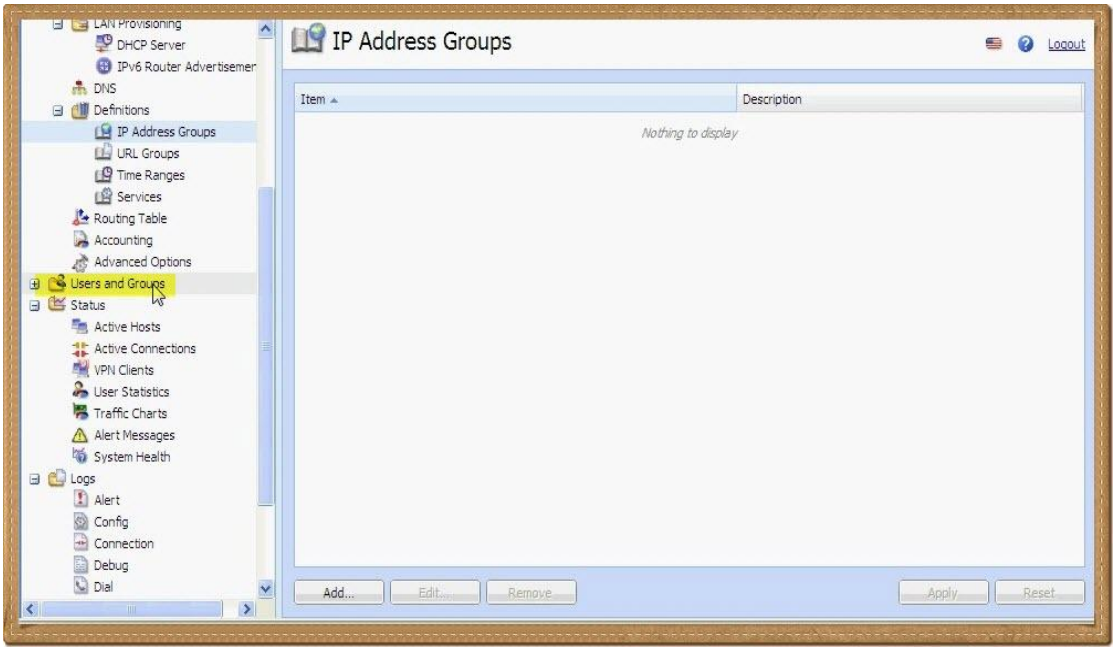


وهنا الأنتي فايروس

يمكنك إضافة الأنتي فايروس الخاص بك أو إستخدام البيلت إن الخاص بالسيرفر وهو Sophos ولكن محتاج إنك تدفع فلوس

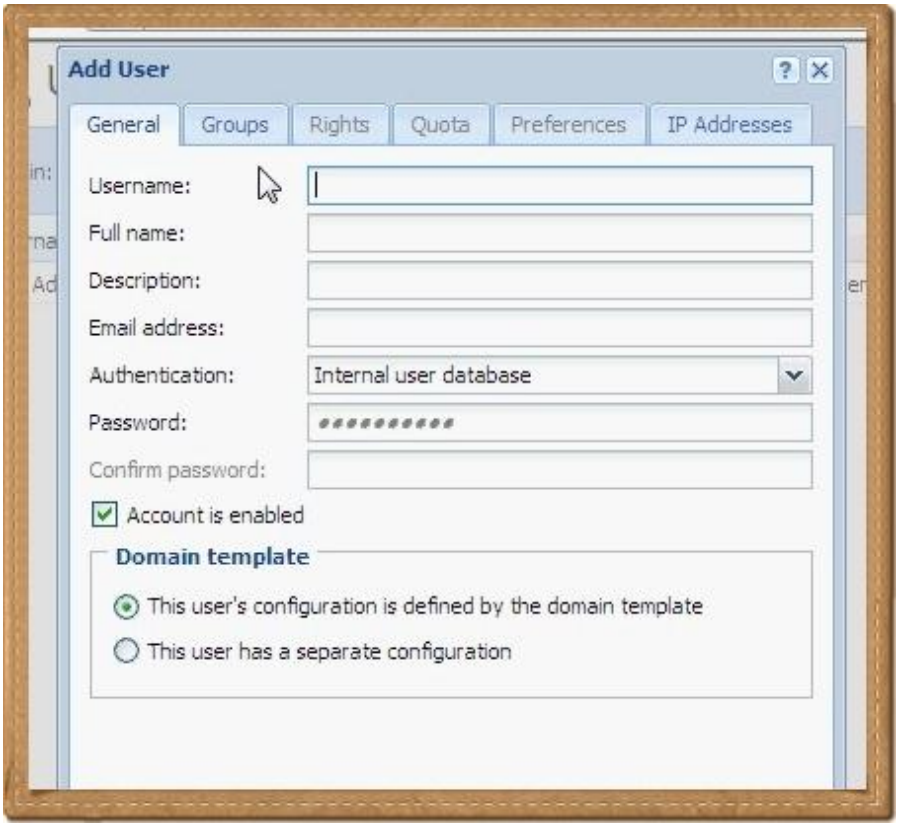


هام جدا : إدارة الـ Users



لا يوجد إلا الأدمين

إنشاء الحسابات وتحديد خصائصهم



ومن هنا إبتدينا في التقارير

واللوج والتنبيهات

أعتقد إن فصل بعد الآخر تتضح الأمور والمصطلحات بالنسبة لكم ومع إنتهاء الكتاب أتمنى ألا يكون من الصعب عليكم التعامل مع أي سيرفر ووضع القواعد والفلاتر والسياسات التي تتوافق مع شركتكم

إن شاء الله في الصفحات القادمة مع لينكس صريح مش بوشين

اللهم إجعلني خيراً مما يظنون واغفر لي مالا يعلمون

اللهم إني أعوذ بك أن أشرك بك شيء أعلمه وأستغفرك لما لا أعلمه

سبحانك اللهم وبحمدك , أشهد ألا إله إلا أنت , أستغفرك وأتوب اليك

الفصل السابع : SmoothWall

التنصيب

الإضافات

SmoothWall

التنصيب

الحمد لله والصلاة والسلام على رسول الله

سيدنا محمد , وعلى آله وصحبه ومن والاه

والآن مع لينكس أصلي مش كده وكده زي Kerio

ماتقلقش إن شاء الله مش ح تتوه مع لينكس وأكواده وحركاته

ح تلاقي الموضوع بسيط وبالتدريج ح تتعود عليه وغالبا ممكن تستغنى عن TMG

قبل ما ندخل في الموضوع والعملي أعرفكم إنه بالنسبة للفاير وول والبروكسي يوجد أكثر من توزيعة لينكس مشهورين وحلوين وولاد حلال وأغلبهم بيقوم على حاجه إسمها Squid ودي بتتعامل مع الكاش Cash وهما بيضيفوا فلاتر و طبعا GUI

مش مهم تعرف ده كله دلوقتي

المهم إنك تعرف أشهر 3 توزيعات هم :

SmoothWall

IPCop

Untangle

بالنسبة لـ SmoothWall و IPCop فهما شبه بعض جدا و خطوات إعدادهم متشابهة ولكن الفرق إن SmoothWall يحظى بإهتمام أكبر من الشركة المطورة له ولا يعاني مما يعانيه IPCop من إهمال

سأبدأ في هذا الفصل مع SmoothWall ثم إضافاته وبعدها سنتحدث عن Untangle في فصل آخر إن شاء الله

عايزك تعرف كمان إن SmoothWall و IPCop بيرضوا بقليلهم , يعني بيشتغلوا على أي جهاز تتخيله من أول 486 لو تتذكروه وأقل رامات في الدنيا وكمان ممكن تسيب الجهاز شغال شهرين من غير ما يقولك : عايز أرستر يا عمو

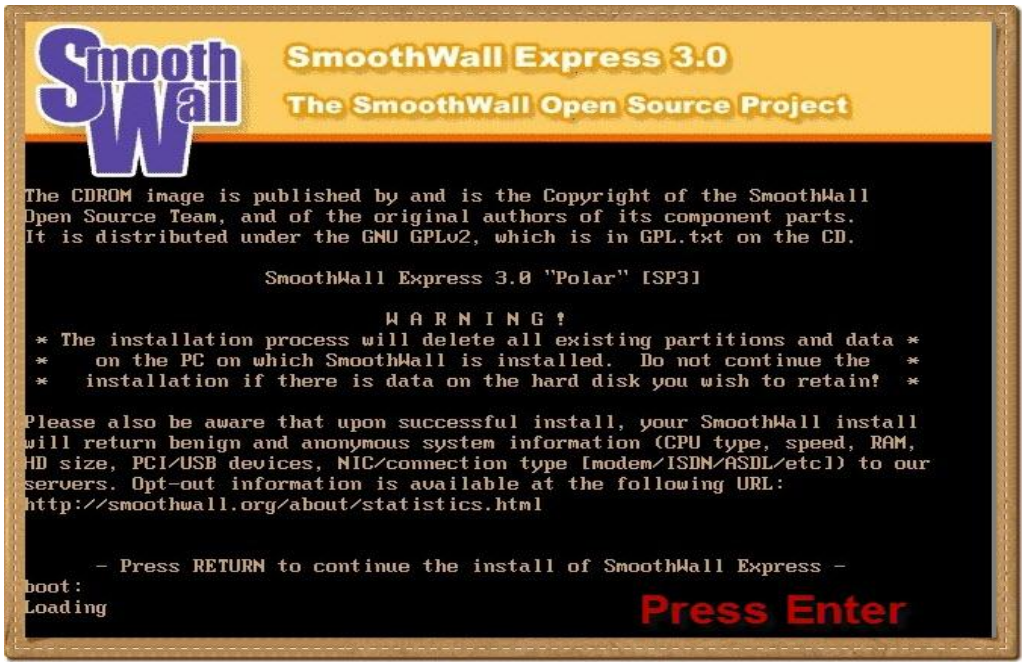
ملحوظة : لا أعتبر مايكروتيك من توزيعات الفايروول فهو راوتر أكثر منه فايروول

نتوكل على الله ومن موقع SmoothWall نقم بتنزيل الإصدار الأخير SmoothWall بصيغة ISO

ونحرقه على إسطوانه

ونعمل Boot على الجهاز منها

نضغط Enter

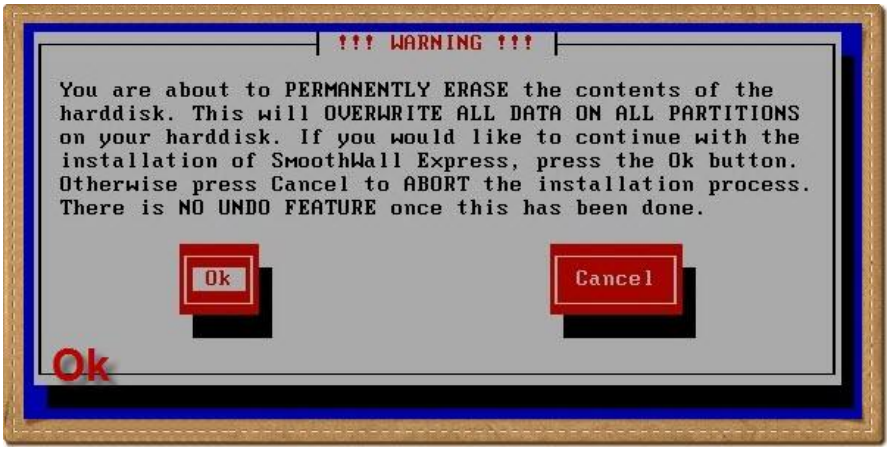


ونصبر شويه

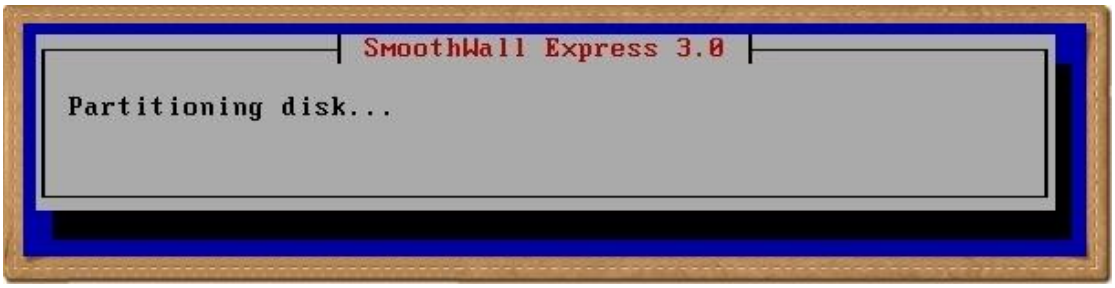
ثم Ok , لايوجد ماوس ولكن نستخدم Enter للإستمرار

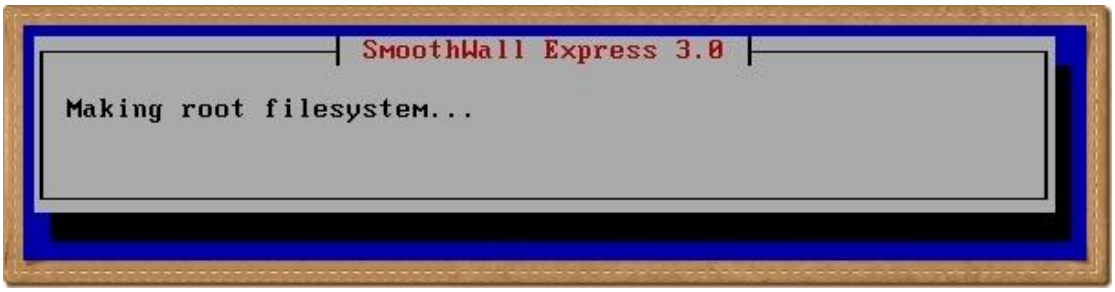
ثم Ok

ثم Ok

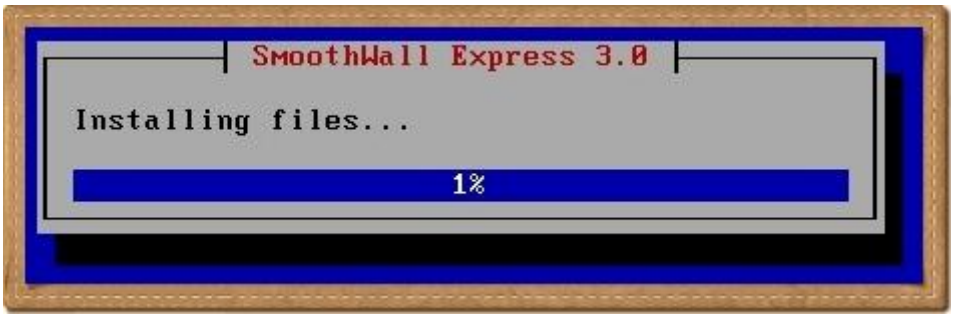


صبراً

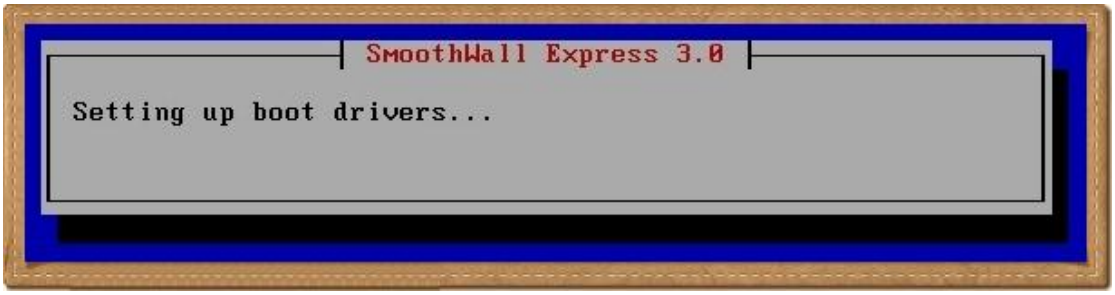




مش ح ياخد كتير



هانت



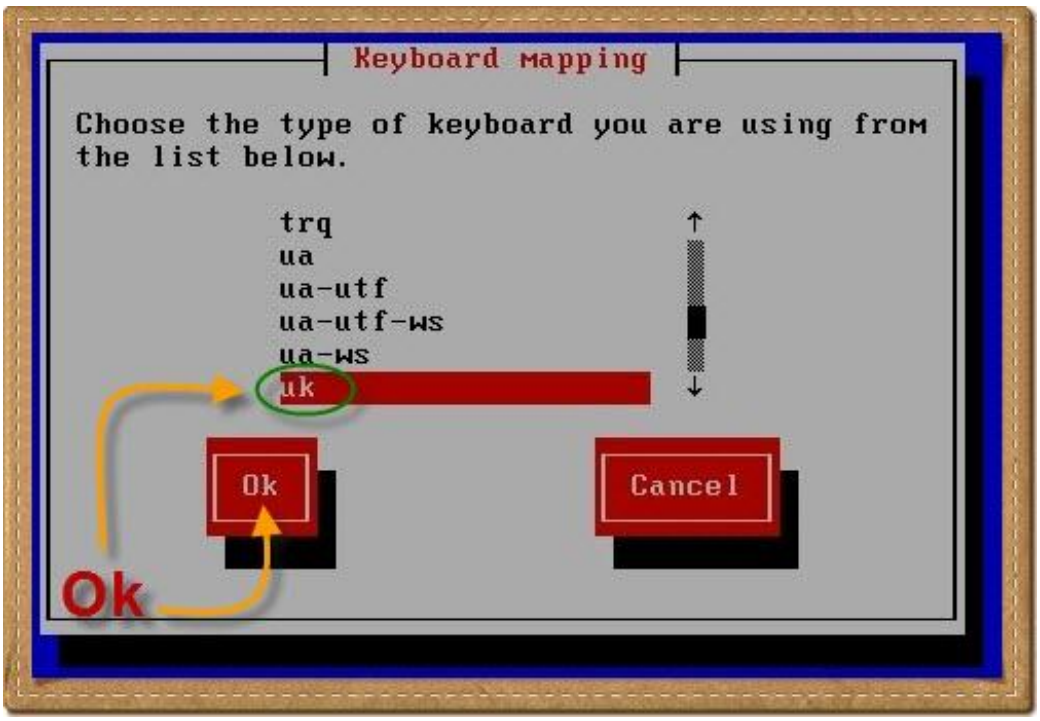
خلاص كده وكده ..

واحد Ok هنا لو سمحت

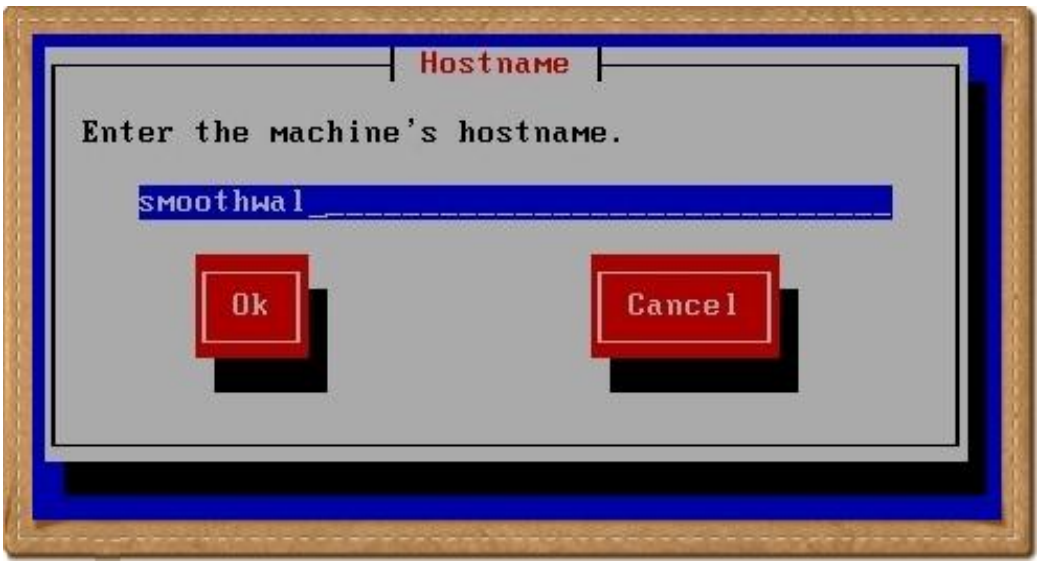
المره دي : No لإنه بيسألك لو عايز تعمل Restore

إختار اللغة و Ok

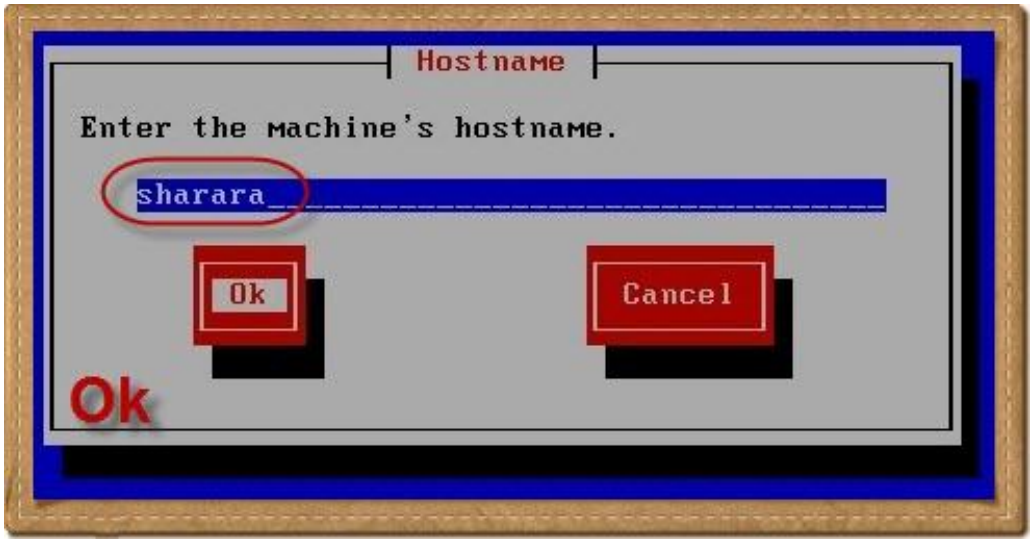
تعود أن تتحرك بين الإختيارات بأسهم الكي بورد ثم Enter لتأكيد الإختيار والإستمرار



ح تسمي المحروس إيه ؟



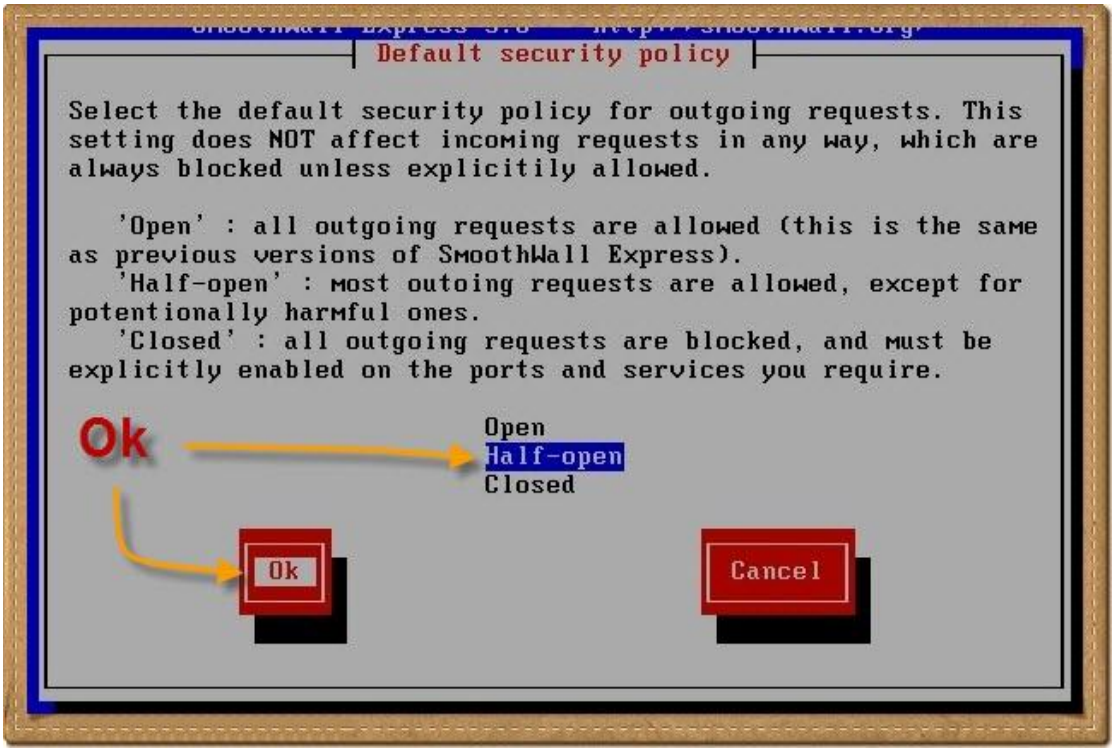
Sharara



لو أول مره ولسه بتجرب إختار Open

وبعدين لما تجمد قلبك إختار Half أو Closed

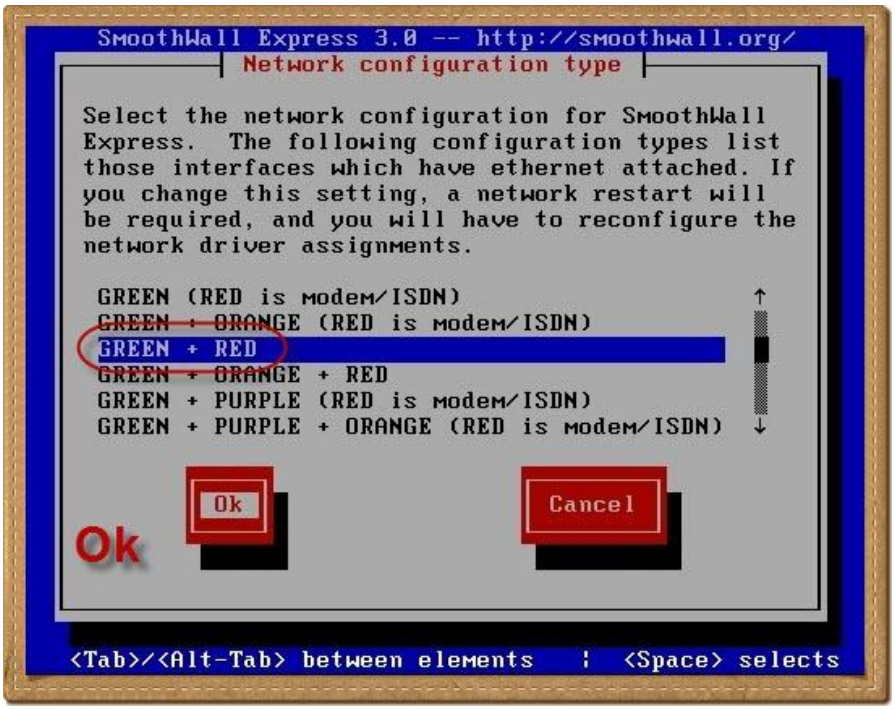
وتقدر تعدلها بعد الإعداد



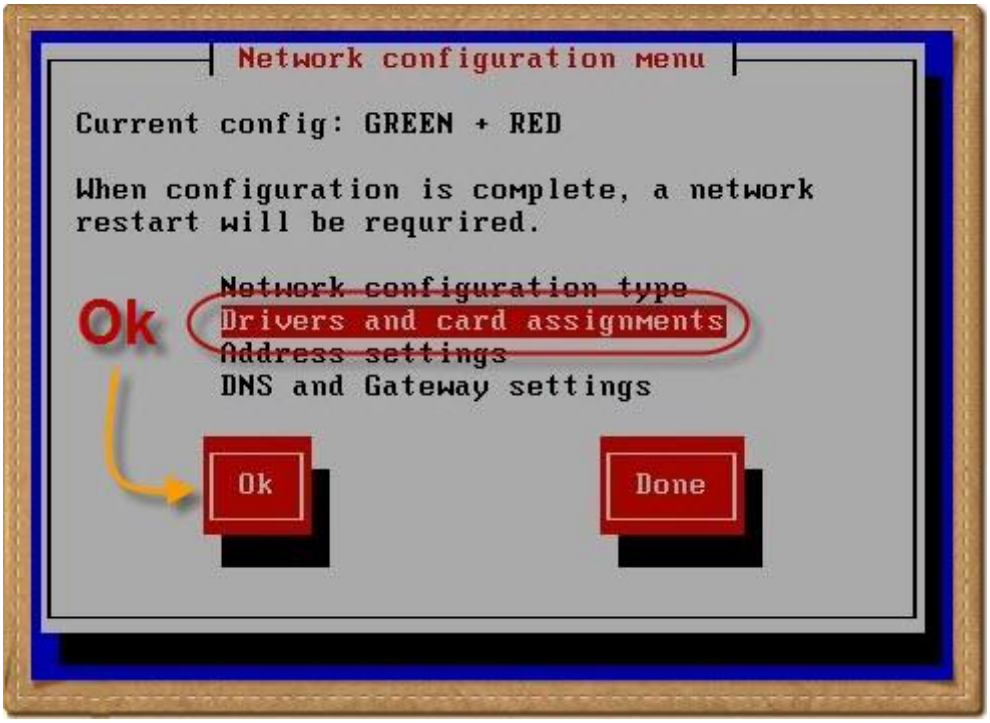
إبتدينا في الجدّ .. نختار Network Configuration Type ثم Ok

يوجد أكثر من نوع لإعدادات الشبكة

سنختار Green + Red وهي كما تعودنا تعني كارت متصل بالشبكة الداخلية وآخر بالإنترنت

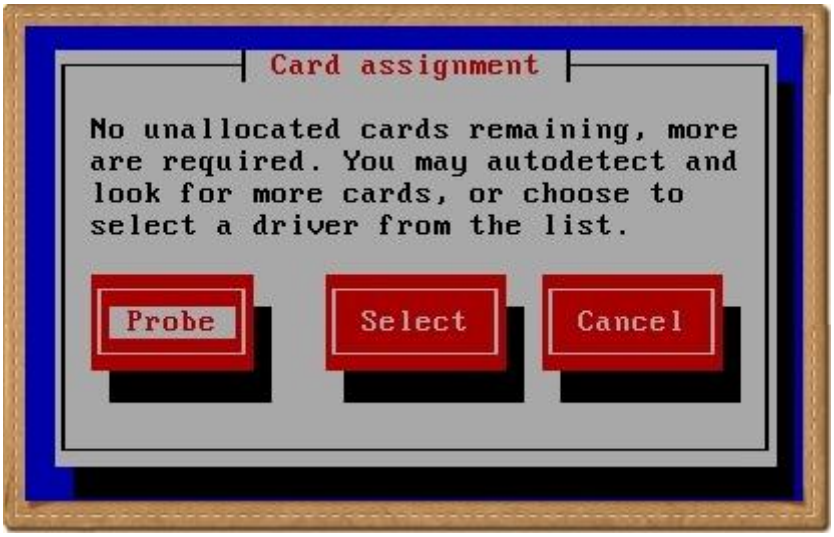


والآن تعريفات الكروت وهي هامة جدا



مهم جدا أن تضغط هنا Ok حتى يمكنك تحديد أي الكرتين Green وأيهما Red

نختار Probe وسيبدأ المعالج في البحث عن تعريفات الكروت



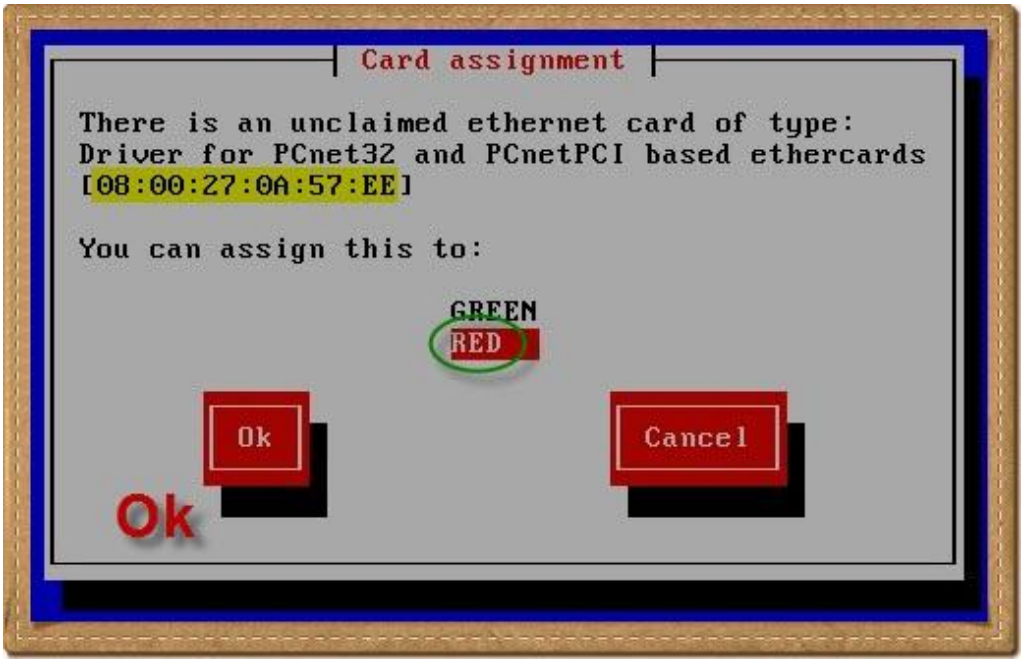
ثم Ok

من الهام جدا تحديد أي الكرتين هو الـ Red والآخر Green

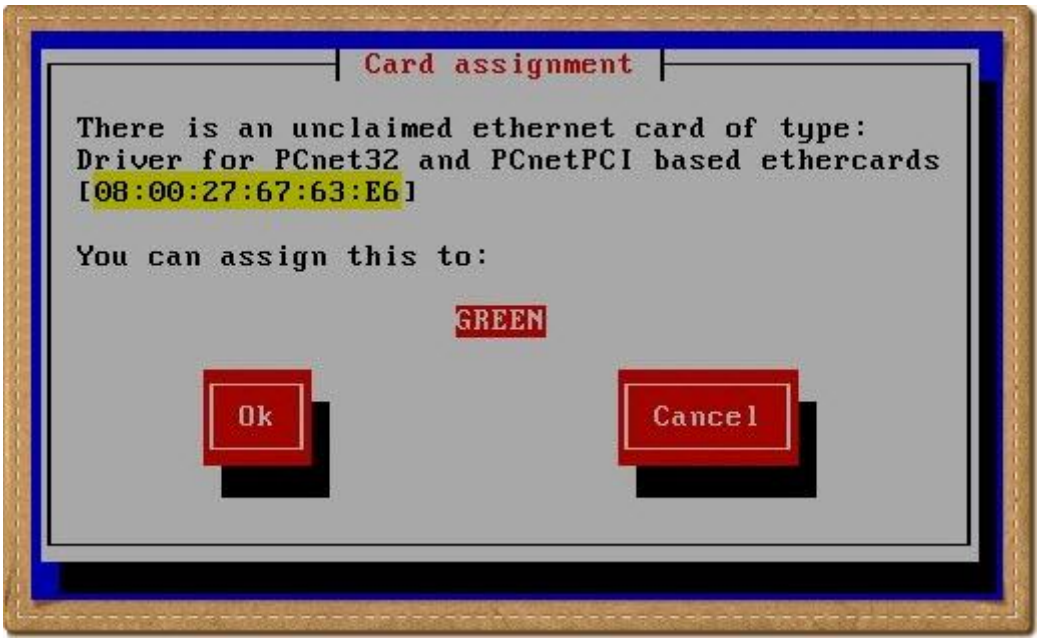
الـ Red يجب أن يكون متصلا بالراوتر أو البروكسي الأعلى ويفضل أن يكون إتصال مباشر أو على سويتش خاص

للخروج من المأزق يجب أن نعرف الـ Mac Address لأي من الكارتين

بتعرفنا على الماك أدريس نختار تخصيصه أحمر او أخضر , ثم Ok

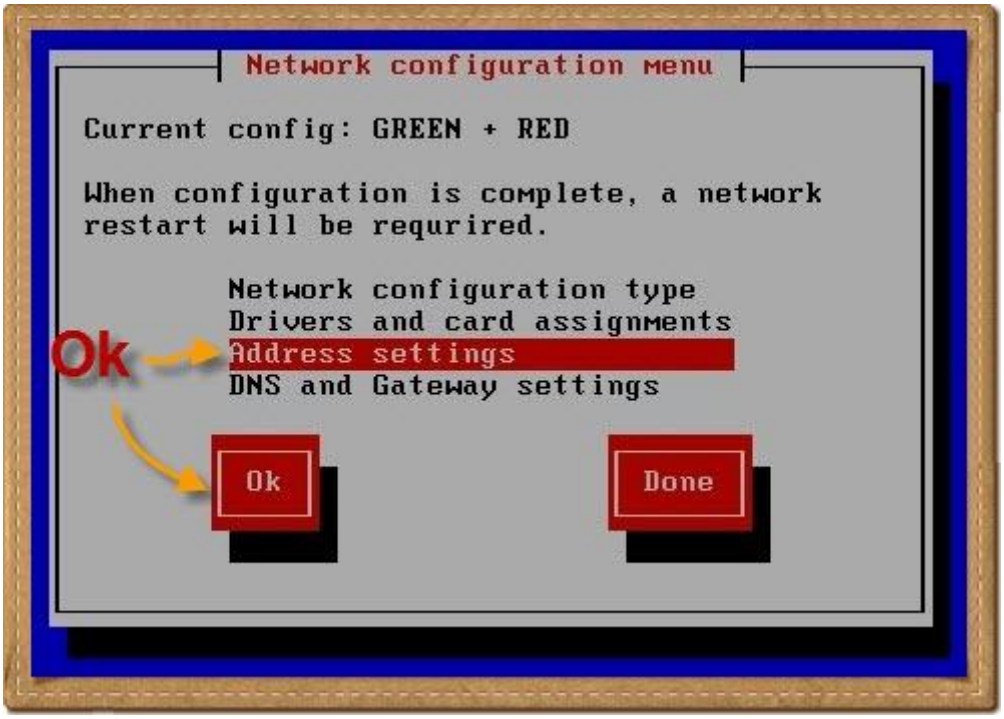


وطبعا الكارت الآخر Green مادام الأول Red ثم Ok



خلاص أهم جزئية في مرحلة الإعداد من وجهة نظري

تظبيط الـ اي بيهات Address Settings نختارها و Ok



بالنسبة للـ Green IP فهو سيصبح Default gateway للكلاينتس لذا نختار IP يكون من النطاق المستخدم لدينا وطبعا لايكون هذا الـ اي بي مستخدم أو موجود داخل DHCP Scope

نبدأ بـ Green

بيقولك خد بالك ...Ok

بالنسبة للكارت الأخضر فهو لن يحتاج إلا إلى IP و Subnet mask فقط فهو لن يحتاج بالطبع إلى DNS للشبكة الداخلية ولا Gateway

هنا سيتم إدخال الـ IP

تأكد جيدا مما ستدخله

ثم Ok

والآن لإعداد كارت الـ Red

ركز هنا

إذا كان الراوتر مفعل به خاصية DHCP فيمكنك أن تختار هنا نفس الخاصية فيقوم الراوتر بمنح اي بي للكارت الأحمر

الأفضل أن يتم إدخال الـ IP يدوي Static IP وبخاصة إذا كنت تحصل على Real IP من مزود الخدمة

التحرك بالأسهم كما تعودنا أما الإختيار فيتم بالضغط على السبيس بار وستظهر علامة النجمة أمام إختيارك

في حالة إدخال الـ اي بي Manual فستحتاج إلى Gateway و DNS , ليه ؟

ماتنساش إن الكارت ده متوصل بالإنترنت وطبعا ح يحتاج الجيت واي والدي إن إس علشان يعيش و يخلي الكلاينتس يعيشوا معاه ☺

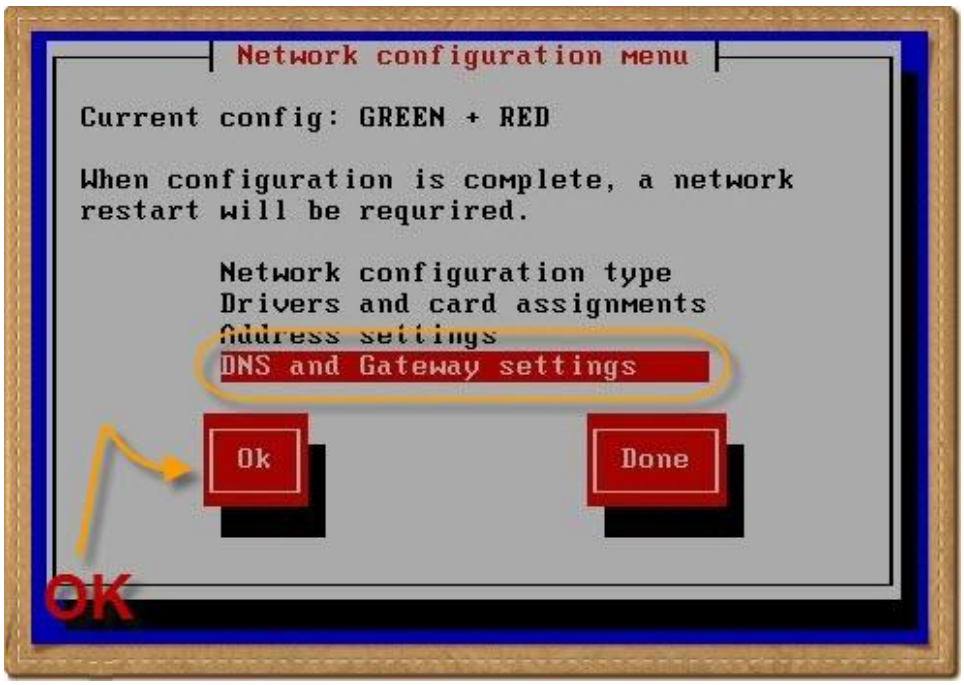
سأختار DHCP

ثم Ok

Done

إذا إخترنا للكارت Red اي بي Manual

فيجب أن ندخل هنا لإدخال الـ Gateway و الـ DNS



ومادمنا قد سبق وإخترنا DHCP .... فعلشان كده : لف وارجع تاني

Cancel

أخيرا Done

أي حاجه تقدر تعدلها بعدين

إديها Finished

ركز في اللي جاي

تحتاج للعمل مع SmoothWall إلى نوعين من حسابات المستخدم :

أدمين Admin تدير به السيرفر ريموتلي من واجهة الويب الخاصة به

رووت Root وهو الذي تتعامل به مع أوامر Shell وستحتاجه بشده عند تنصيب الإضافات

مش عايز أحبطك ولكن غالبا عدم التركيز في التفرقة بين كلمات السر للحسابين المختلفين ح تخليك تنزل SmoothWall أكتر من مره علشان كده ياريت تركز قوي ومافيش مانع تكتبهم على ورقه , ولو مش واثق قوي ممكن تخليهم في الأول عبارة عن أرقام وبعدين تغيرهم

نبدأ مع كلمة سر الأدمن admin password

طبعا سيطلب منك كتابة الـ Password ثم تكرارها

أدخل الباسوورد وكررها

ثم Ok

دي مش نفس الشاشه ☺

دي أختها الخاصة بالـ Root Password , إتلخبطت فيها كتيييير

وبالمناسبة هي بتتكتب كده : إتلخبطت وجايه من لخبطة

فلو سمحت ماتكتبهاش إتلغبط أو إتلغبطت

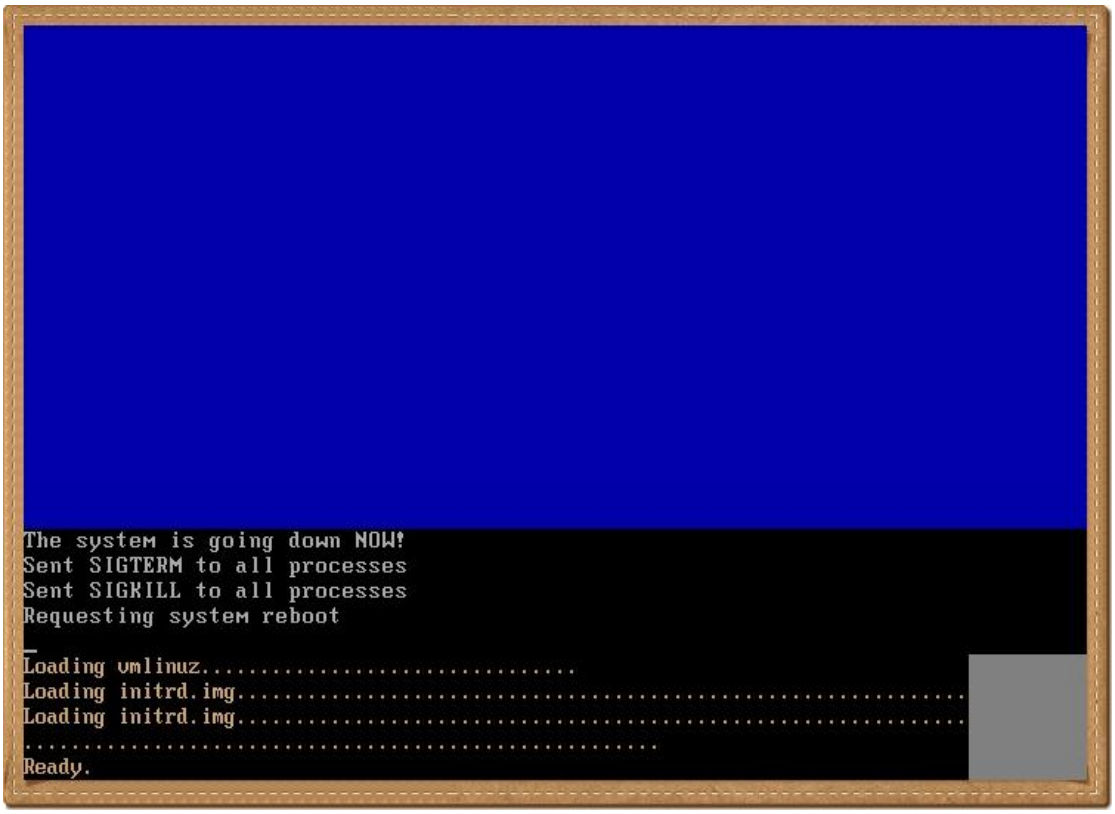
كلمة السر وكررها

ثم Ok

ثم Ok

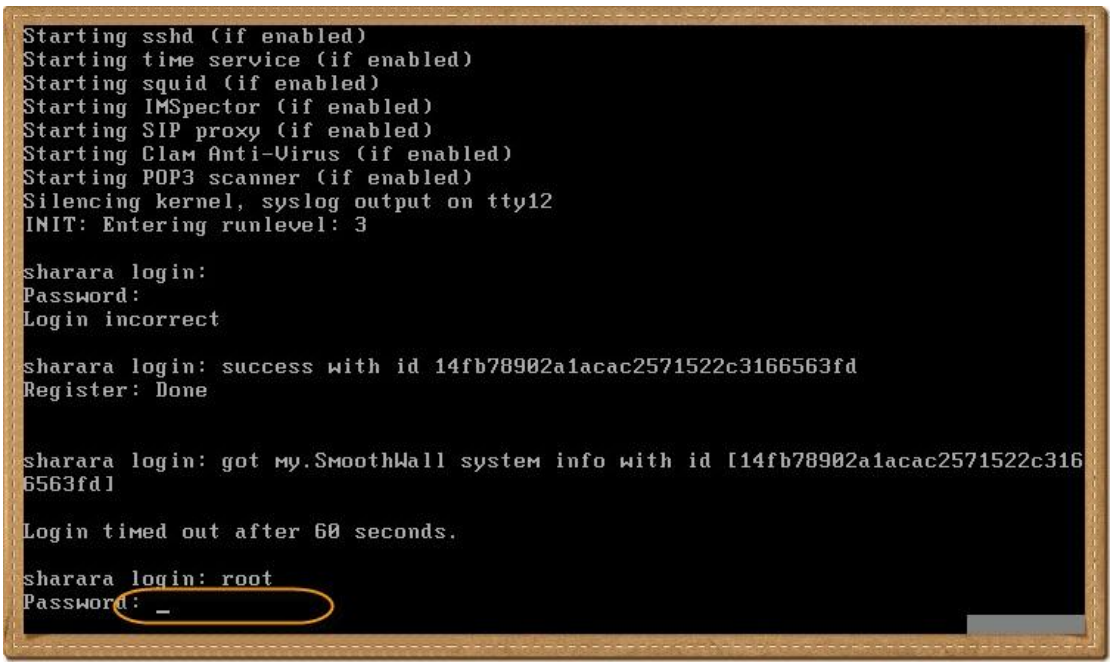
ثم Reboot وخلاص بجد

بيـ Boot



علشان يطمئن قلبك إدخل الـ Root user name and password

إكتب Root ثم Enter ثم الباسوورد ثم Enter



عند كتابة الباسوورد مش ح يبان أي شيء وإنت بتكتبها , إكتبها بتركيز و Enter

أزرق وأحمر وأخضر وكده يبقى تمام جدا ونروح على الجهاز اللي ح ندير منه

خد نفس عمييييك وجهز نفسك لمرحلة الإدارة

على أي جهاز متصل بالشبكة مع الـ Green Card

وطبعا ح نعمل له الـ Default gateway بالـ Green IP للـ SmoothWall وهو في حالتنا 192.168.1.16

نفتح البراوزر ونكتب الـ URL الخاص بالسيرفر وعندنا هنا أربعة بدائل

- بالنسبة للـ Http العادي نكتب إسم السيرفر وبورت 81 , أو اي بي السيرفر وبورت 81

يعني

http://sharara:81

http://192.168.1.16:81

أنا أُفضل إستخدام الـ IP

- وبالنسبة للـ Https فسنستخدم بورت 441

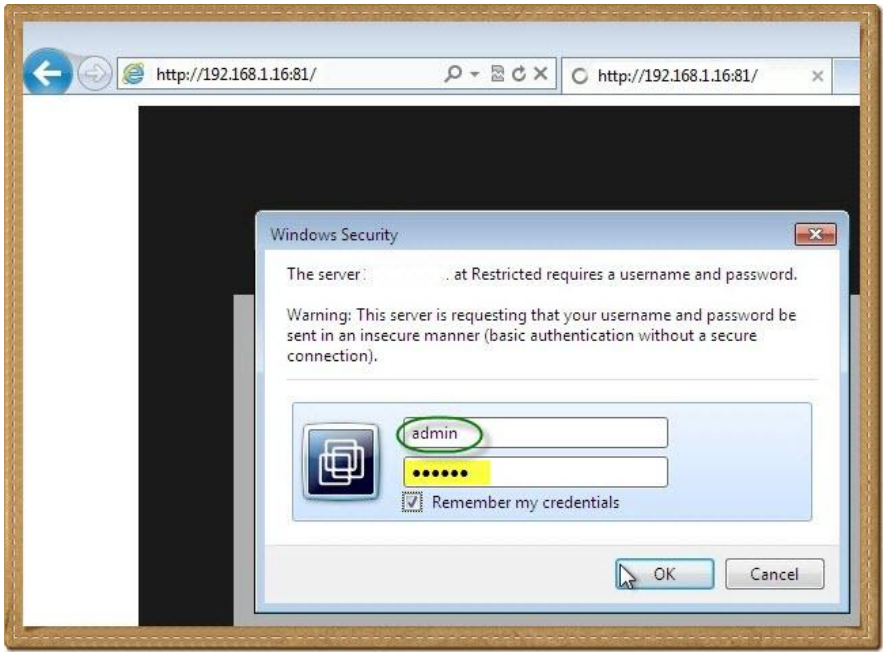
https://sharara:441

https://192.168.1.16:81

وأيضا أُفضل الـ IP

طبعا إسم السيرفر و الـ اي بي ح تجعله حسب إعدادات الـ SmoothWall اللي عملتها سعاتك مش اللي عملتها سعاتي في الشرح

الحمد لله طلعت قماش , إدخل Admin ثم الباسوورد الخاصة به اللي إنت نسيتها ☺



الحمد لله على فضله وكرمه

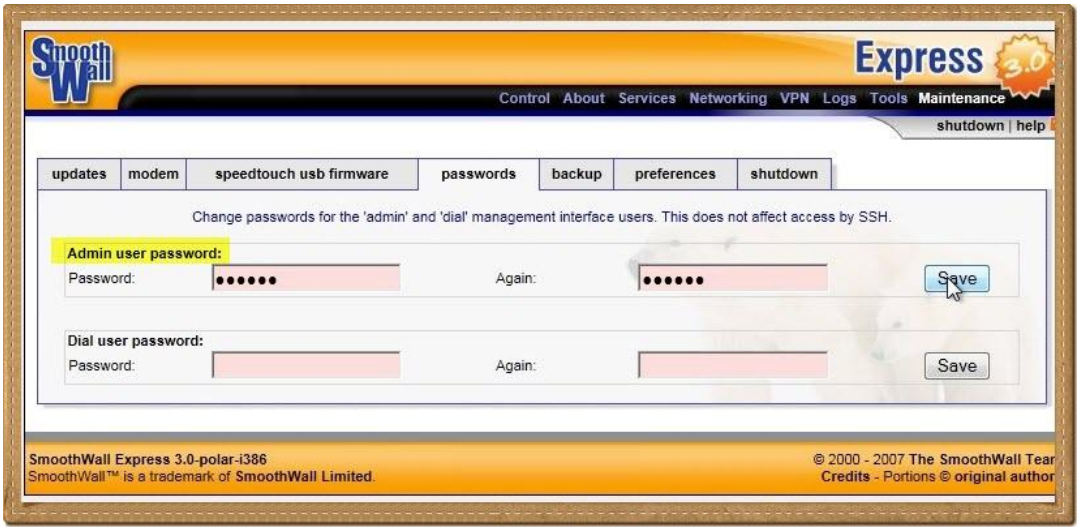
إتفسح براحتك لكن ماتبوظش حاجه

من هنا مثلا قائمة Maintenance وهي للمهام التي تتعلق بإدارة السيرفر

يمكنك مثلا من هنا تغيير الـ Admin Password

ماتنساهاش تاني

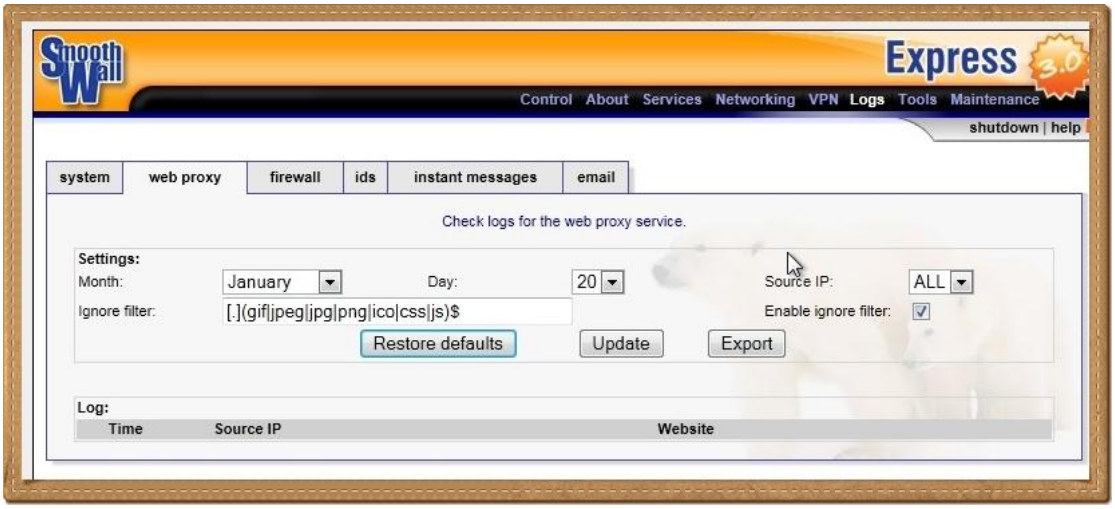
تغيير الرووت باسوورد محتاجة تتعامل بأوامر الينكس



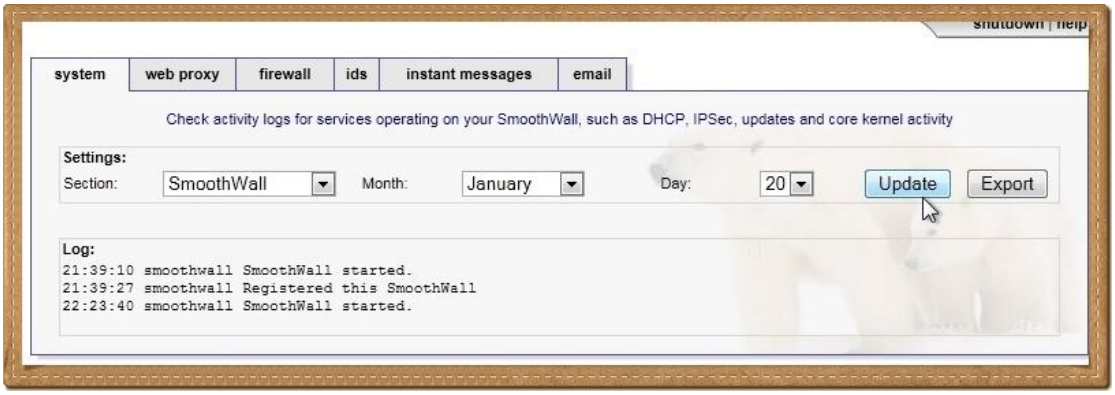
ويمكن أيضا عمل باك اب للسيرفر وهو أمر هام جدا

وكمان Shutdown و Reboot

و Log



وكمان Log



طبعا لو جربت الإنترنت على الكلاينت ح يشتغل معاك

وبس خلاص

لكن مش بس خلاص قوي

ح افهمك

لو إعتمدت على الـ SmoothWall بالشكل ده مش ح ينفعك بدرجة كافية ولكن إذا كنا انتهينا من شرح السيرفر فإننا لم نتحدث عن الإضافات الخاصة به

أهم ميزة في الـ SmoothWall وكمان IPCop هو وجود الإضافات Add-ons يمكن إضافتها للسيرفر وتضيف له وظائف هاااائلة جدا

يوجد إضافات لعمل كل شيء تحتاجه على السيرفر علشان كده مش بس خلاص قوي

الصفحة الجايه مع الإضافات إن شاء الله

اللهم إجعلني خيراً مما يظنون واغفر لي مالا يعلمون

اللهم إني أعوذ بك أن أشرك بك شيء أعلمه وأستغفرك لما لا أعلمه

سبحانك اللهم وبحمدك , أشهد ألا إله إلا أنت , أستغفرك وأتوب اليك

SmoothWall

الإضافات

الحمد لله والصلاة والسلام على رسول الله

سيدنا محمد , وعلى آله وصحبه ومن والاه

من أهم الأشياء المطلوبة في سيرفر البروكسي أو الفايروول أو الUTM أيا كان هو وجود فلاتر أو رولز أو بوليسيز

المهم إنك بالبلدي كده تقدر تتحكم في مين ح يعمل إيه وإمتى

وده إحنا إتعاملنا معاه في الفصول اللي فاتت مع أنواع مختلفة من السيرفرات

وعلشان تقدر تعمل كده بتوسع على SmoothWall ح تحتاج تضيف له إضافات Add-ons تقوم بالمهام المطلوبة مثل فلترة المواقع أو أنواع الملفات أو المستخدمين

يمكنك أيضا إضافة Open VPN

أو إضافة ترفع كفاءة التقارير

أو أنتي فايروس

أو عمل نسخة باك اب في صيغة ISO جاهزة للتنصيب

يوجد فقط شيئان مهمان بالنسبة للإضافات :

- عدم توافق الإضافة أحيانا مع ترقيات السيرفر مما قد يحدث إنهيار للسيرفر
- صعوبة تنصيب الإضافات وبخاصة أننا سنعمل في بيئة لينكس وأغلبنا لايعلم عنه شيئا

بالنسبة لعدم التوافق فحلها هو الحذر ثم الحذر فلا داعي للتسرع في ترقية إصدارة السيرفر قبل أن تتأكد من توافق الإضافات المثبته عليها مع الترقية وبصفة عامة فقبل الترقية يجب إزالة الإضافات ثم الترقية ثم تنصيب الإضافات من جديد مع الإحتفاظ بنسخ Backup للرجوع إليها

أما بالنسبة لتنصيب الإضافات فإن شاء الله ستصبح سهلة جدا بنهاية الفصل

نتوكل على الله ونفتح صفحة الويب التي ندير منها السيرفر

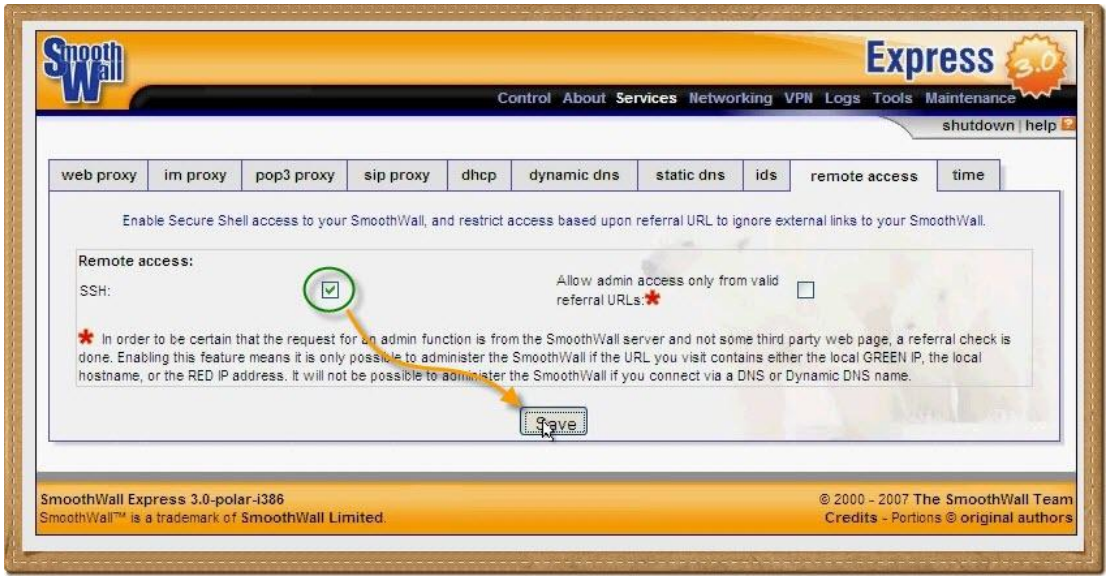
لاحظ أن الدخول بال Admin

من واجهة المستخدم نختار قائمة Tools ومنها External Access

نعمل Enable للـ SSH

ثم حفظ

وبكده نقدر ندخل ريموتلي على أوامر لينكس



والآن مع فقرة الساحر قصدي مع تنصيب الإضافة

- *لو إحنا على جهاز ويندوز وعايزين ننصب برنامج ح نعمل إيه ؟*

نجيب البرنامج ثم ننصبه

وهذا هو ما سنفعله ولكن بتوسع قليلا

الأول نجيب الإضافة :

سنعمل على أهم إضافة للـ SmoothWall وهي إضافة Advanced Proxy التي تتيح إمكانيات رائعة للتحكم في سلوك المستخدم على الإنترنت

ننزل الإضافة من موقعها على الإنترنت ونتأكد أنها الإصدارة المطابقة لإصدارة SmoothWall

غالبا ما تكون الإضافات مضغوطة بصيغة tar

وقبل أن ندخل على ثانياً لننصب الإضافة يجب نقل الإضافة من الجهاز الذي نعمل من خلاله إلى جهاز الـ SmoothWall ولإننا نتعامل مع لينكس فسنحتاج إلى برنامج وسيط نتصل من خلاله بهارد ديسك الـ SmoothWall ومن ثم وضع ملف أو ملفات الإضافة لتنصيبها

أغلب برامج الـ FTP يمكنها الإتصال بالسيرفر ومن ثم نقل الملفات إليه ولكن أفضلهم بلا نزاع هو برنامج بسيط جدا إسمه WinSCP يعمل من خلال الويندوز ويسمح لنا بالإتصال باللينكس ما يميزه أيضا وجود مجموعة من الخواص الإضافية سنتعامل معها في حينه

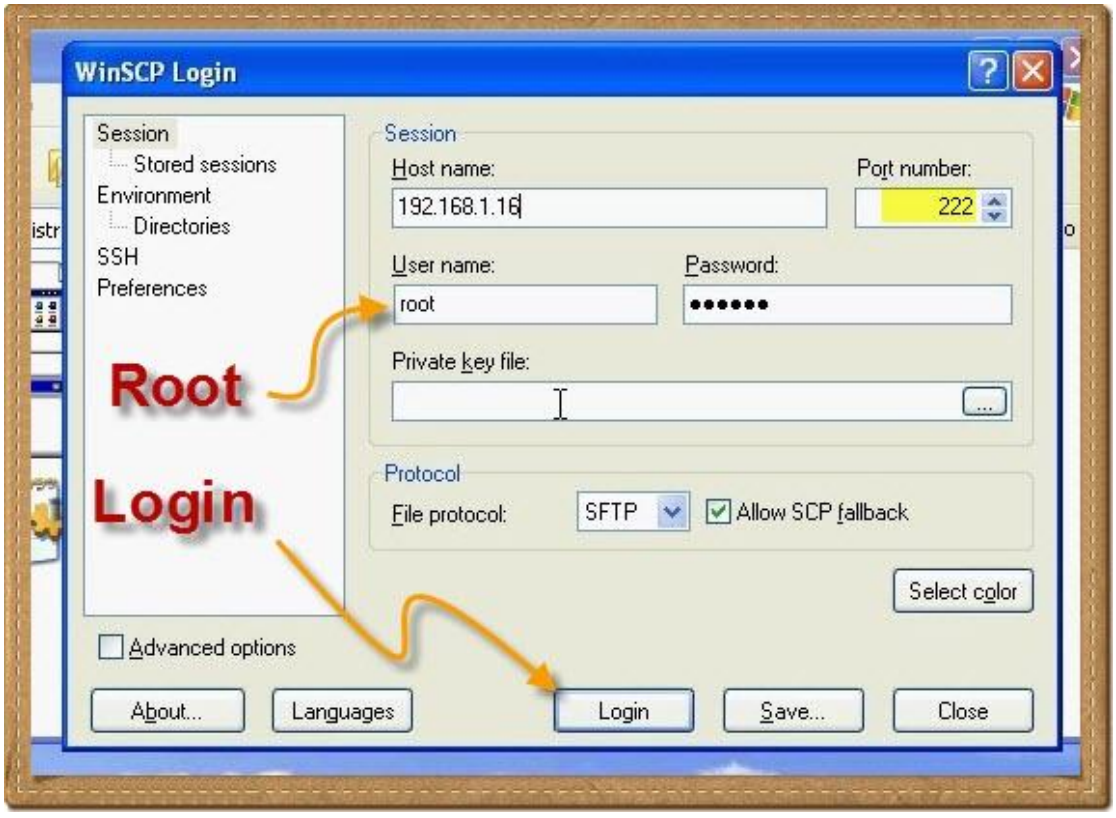
بدون تنصيب دابل كليك على WinScp.exe

كأي برنامج FTP يطلب منا بيانات الدخول على الـ SmoothWall لاحظ هنا أننا سنستخدم بوتوكول SFTP

الدخول سيتم بإستخدام حساب الرووت وليس الأدمن والبورت هو 222

تذكر الأدمن للدخول على واجهة الويب والرووت للدخول بإستخدام SSH

بعد إدخال البيانات إضغط Login



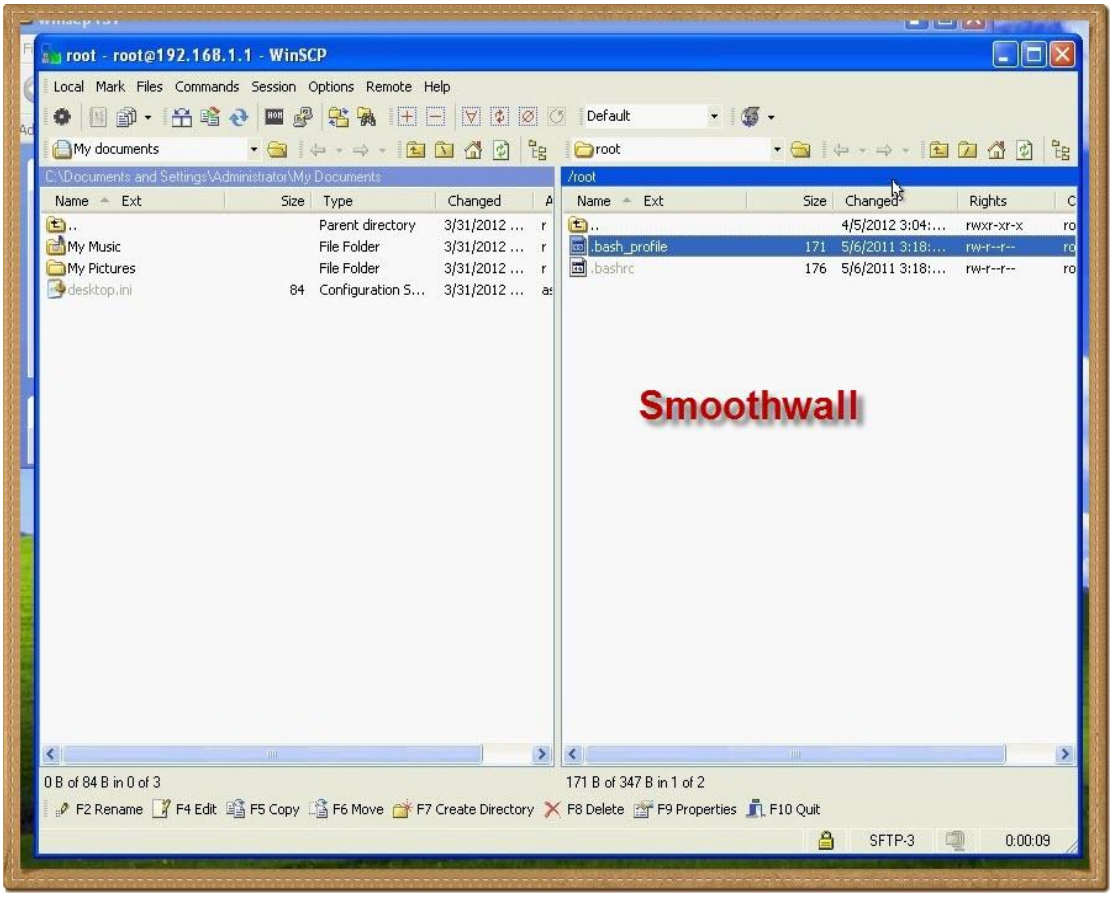
Yes

بحمد الله تم الإتصال

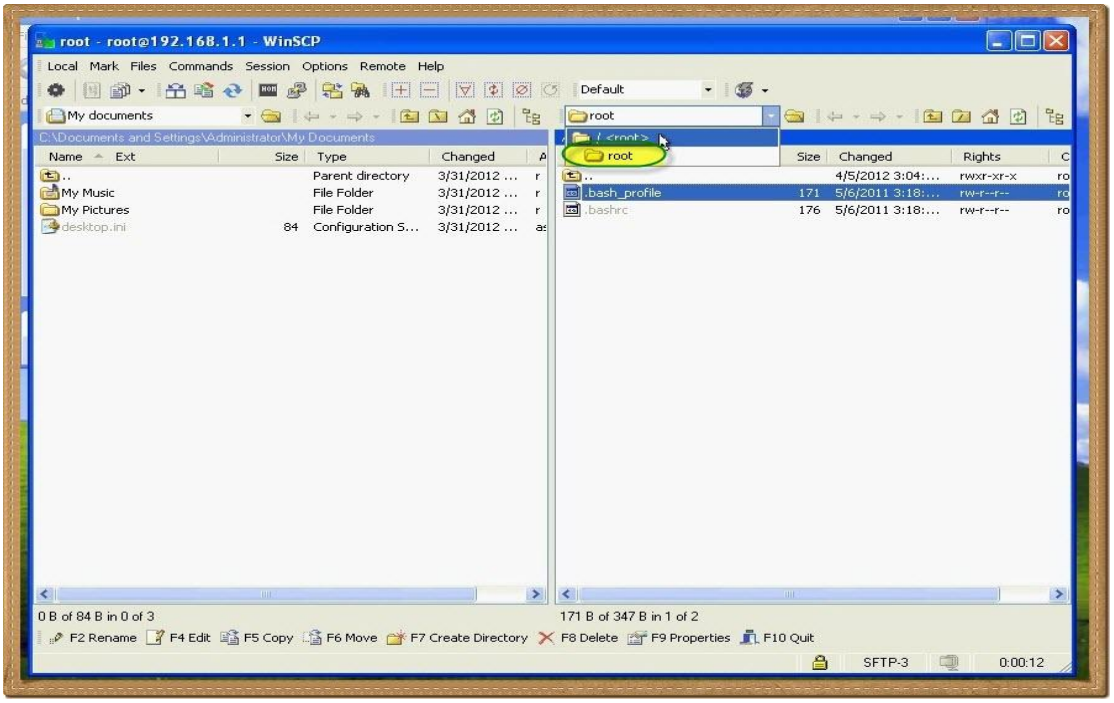
إذا كنت قد تعاملت مع برامج FTP من قبل ستعرف إن جهاز الـ SmoothWall يمكننا تصفحه من الناحية اليمنى

ومحتويات جهازنا على الناحية اليسرى

من ضمن المهارات للتعامل مع هذه البرامج نقل الملفات بين الجهازين يتم طبعا بإستخدام السحب والإفلات Drag and Drop من جهازنا للجهاز التاني أو العكس



نضغط في المربع الأعلى لتصفح كامل مجلدات الجهاز



وضع ملفات الإضافات سيتم في مجلد tmp أو أي مجلد آخر

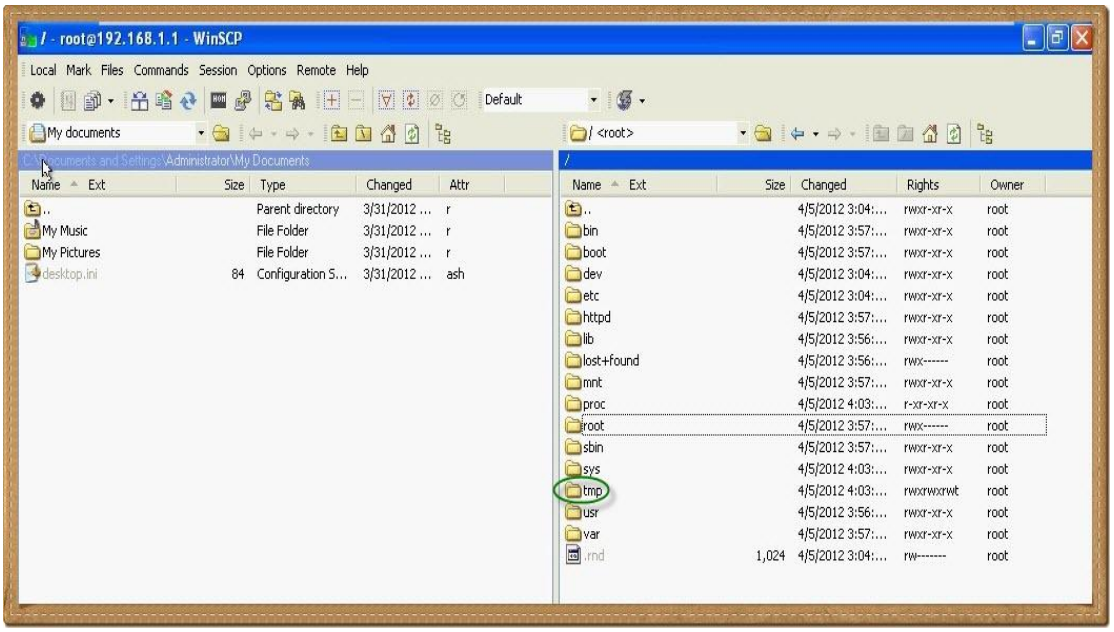
ويمكننا إذا أردنا إضافة مجلد آخر والعمل من خلاله مالم تطلب منك تعليمات تنصيب الإضافة العمل من مجلد محدد

- هي ح تطلب إزاي ؟

هو أنا ماقلتلكش إنك لازم تقرأ تعليمات التنصيب الخاصة بأي إضافة

- لأ

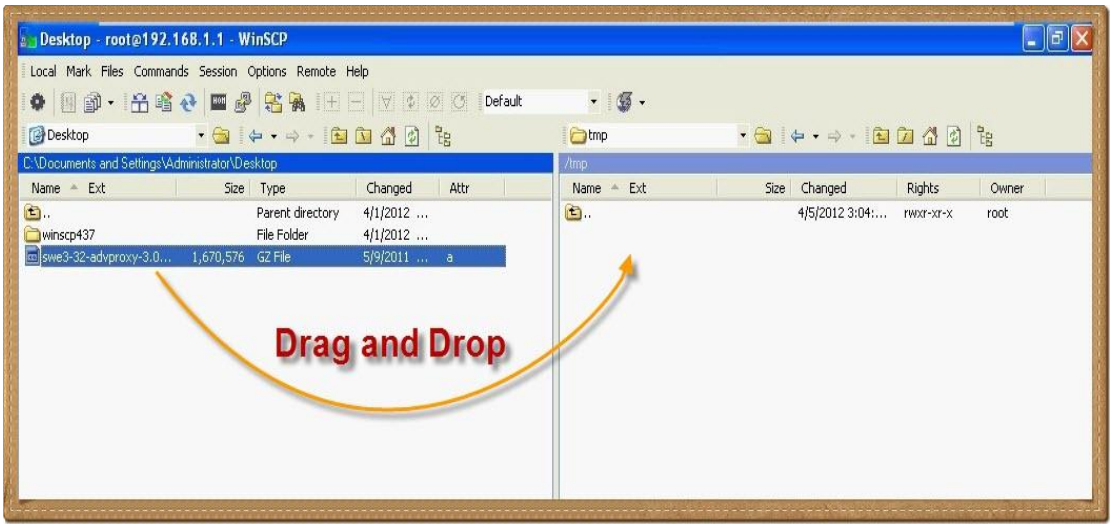
إعتبرني قلتلك



دابل كليك على فولدر tmp

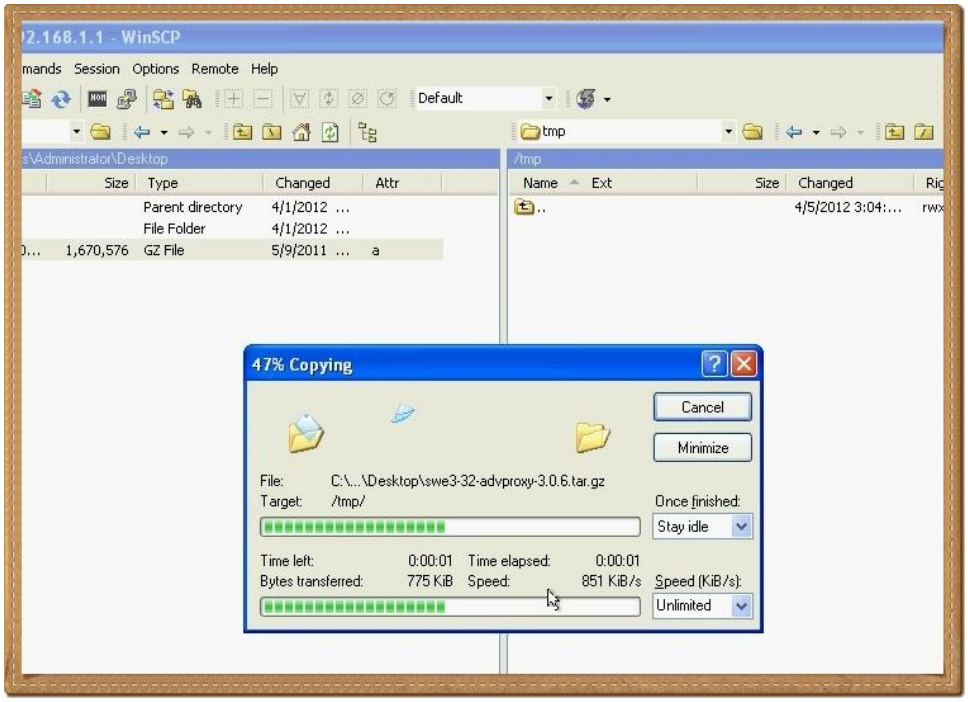
ملف الإضافة موجود على الديسك توب بصيغة tar

نتصفح جهازنا من الناحية اليسرى حتى نصل إلى الديسك توب ثم نسحب الإضافة للناحية اليمنى



قد يأخذ النقل لحظات , ماعلينا المهم إنه ينقل

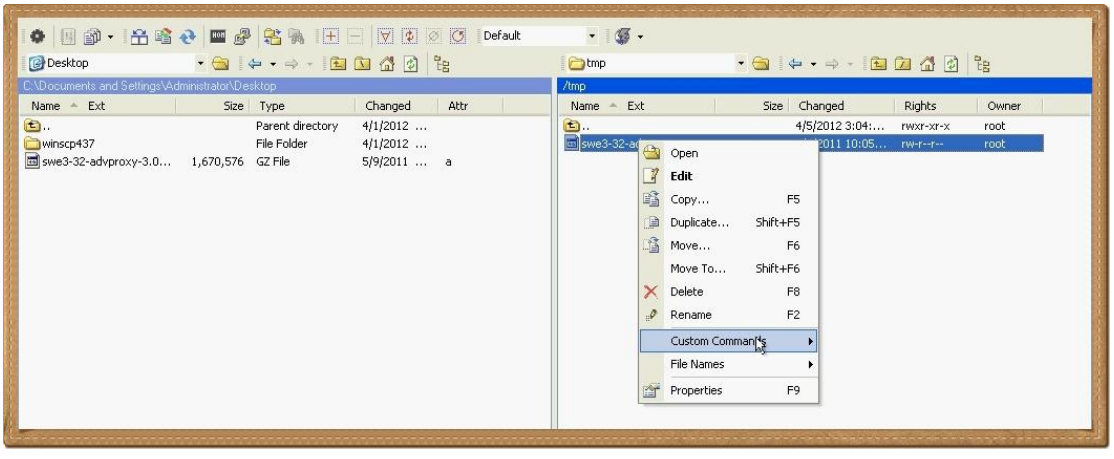
بينقل



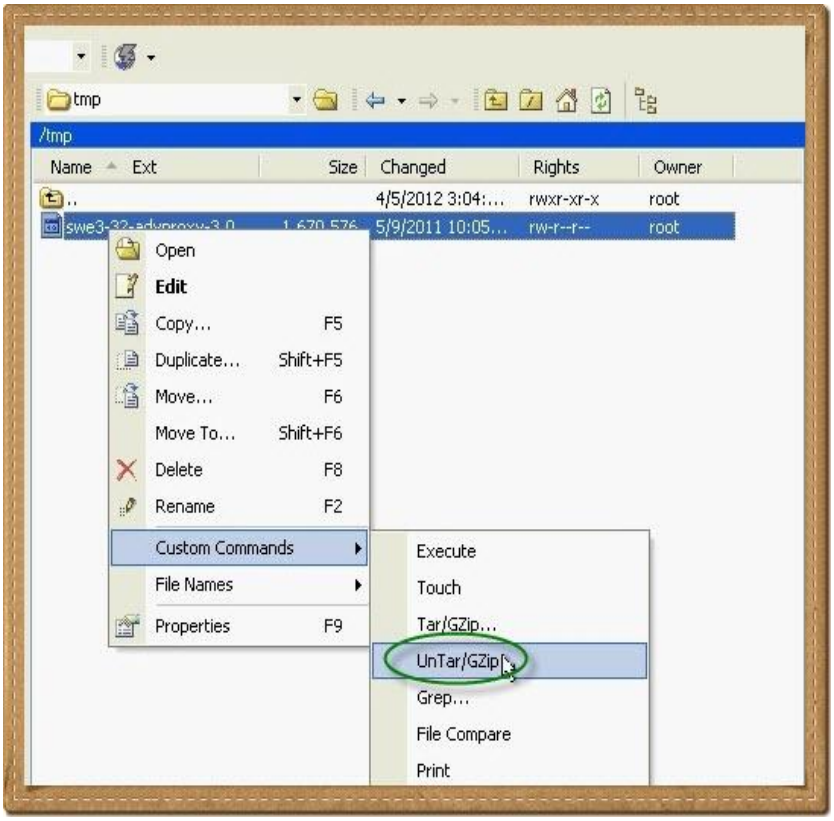
والآن نقلنا الملف إلى جهاز الـ SmoothWall ولكن ننصب الإضافة بقي خطوة أخيرة وهي فك الضغط عن الملف وهذا سيتم من خلال طريقتين :

- فك الضغط بإستخدام برنامج WinSCP
- فك الضغط على الويندوز قبل نقل الملف ومن ثم نقل المحتويات مفكوكة جاهزة

<u>بالنسبة للطريقة الأولى :</u> من الناحية اليمنى كليك يمين على ملف الإضافة ونختار Custom Commands



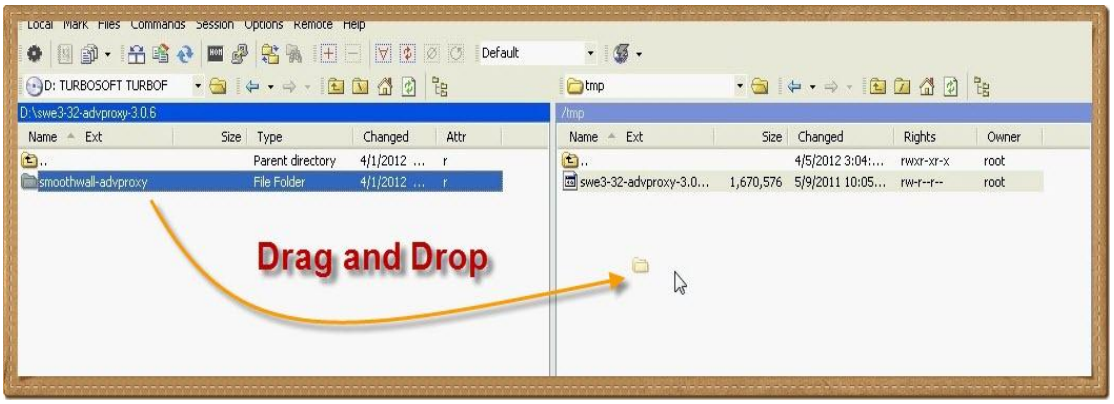
ثم UnTar



<u>أما الطريقة الثانية</u> : فهي التي أفضلها

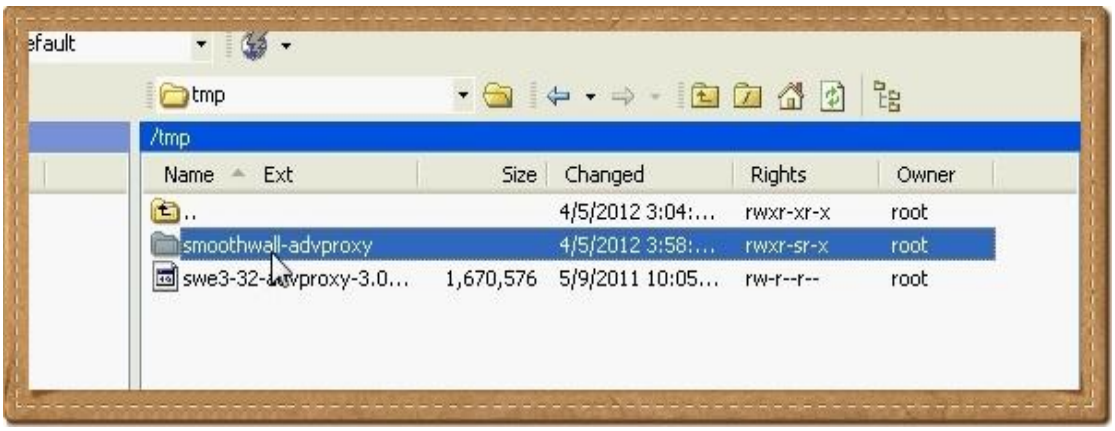
وهي بإستخدام برنامج فك ضغط ويفضل 7Zip ثم فك الملف المضغوط على الويندوز عادي خالص ونقل المجلد الناتج عن فك الضغط عادي خالص إلى سيرفر SmoothWall بنفس الطريقة Drag and Drop

إلى مجلد tmp

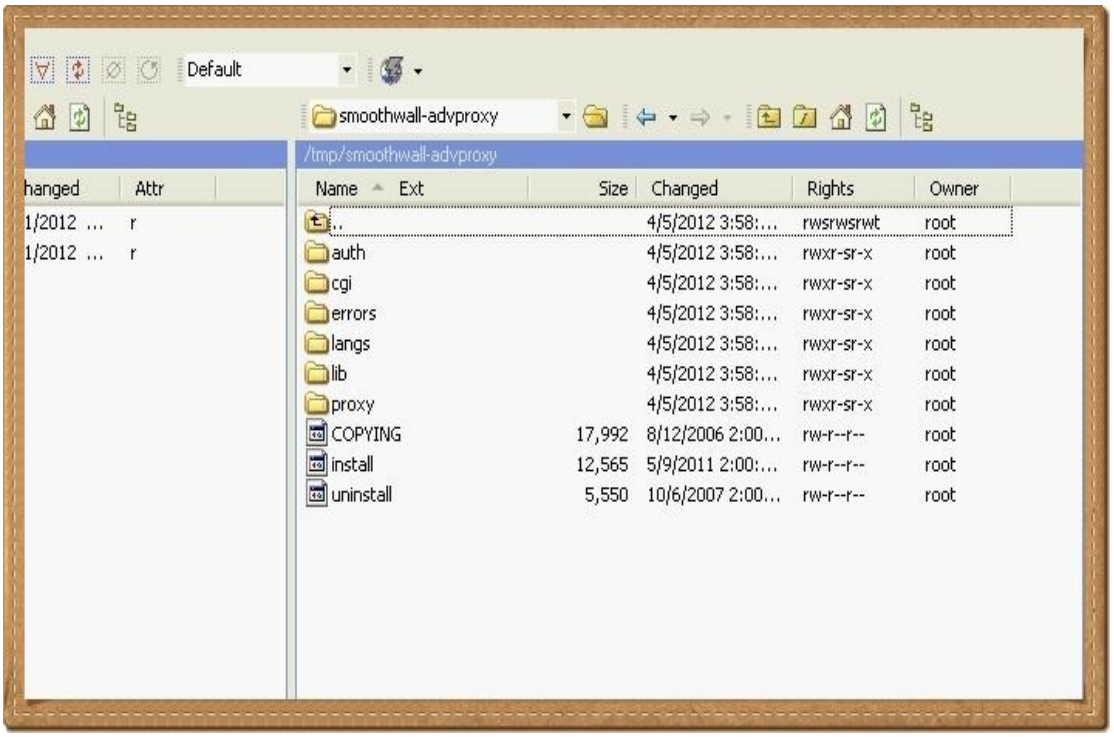


نجد هنا المجلد الخاص بالإضافة بعد أن فككنا الضغط ونقلناه إلى السيرفر

دابل كليك لفتحه



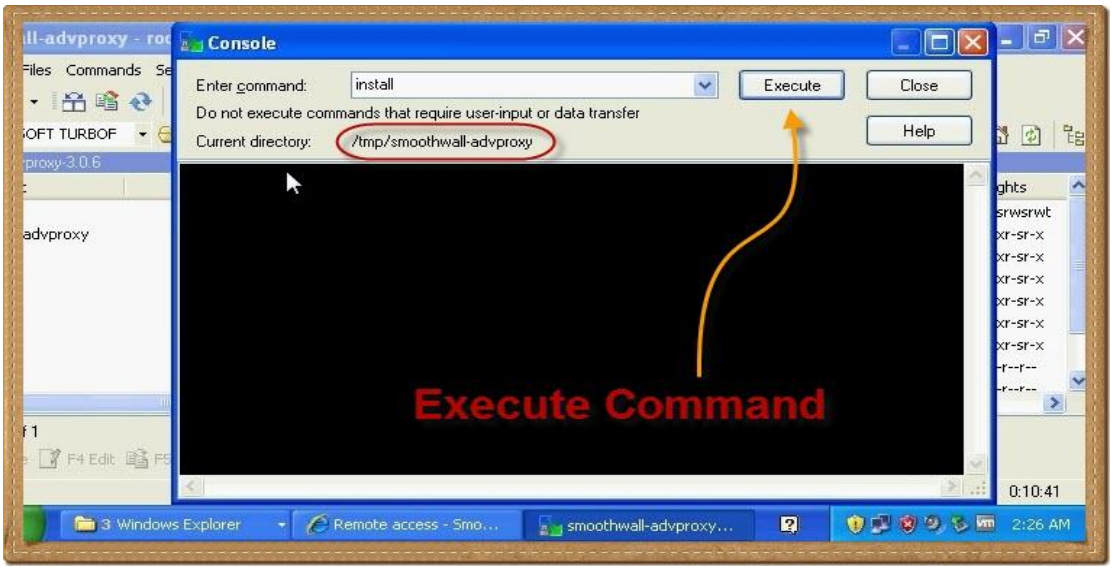
تنصيب الإضافة سيتم من خلال ملف Install وبرضه ليها طريقتين



<u>الأولى من خلال أوامر اللينكس</u> : نتأكد أننا موجودين داخل المجلد الذي به ملف Install

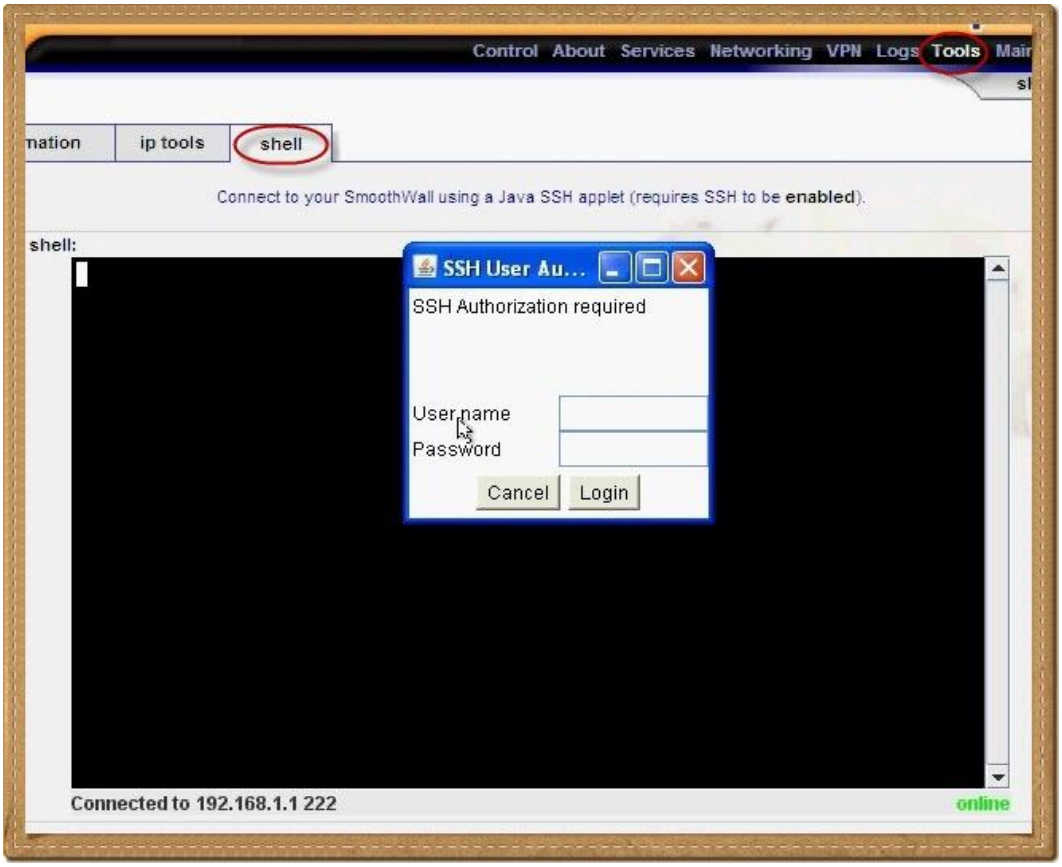
ونختار Open Terminal من Commands

ستفتح نافذة الأوامر للينكس ويتم كتابة الأوامر ثم Execute



يمكننا التعامل مع هذه الأوامر أيضا من واجهة الويب الخاصة بإدارة الـ SmoothWall

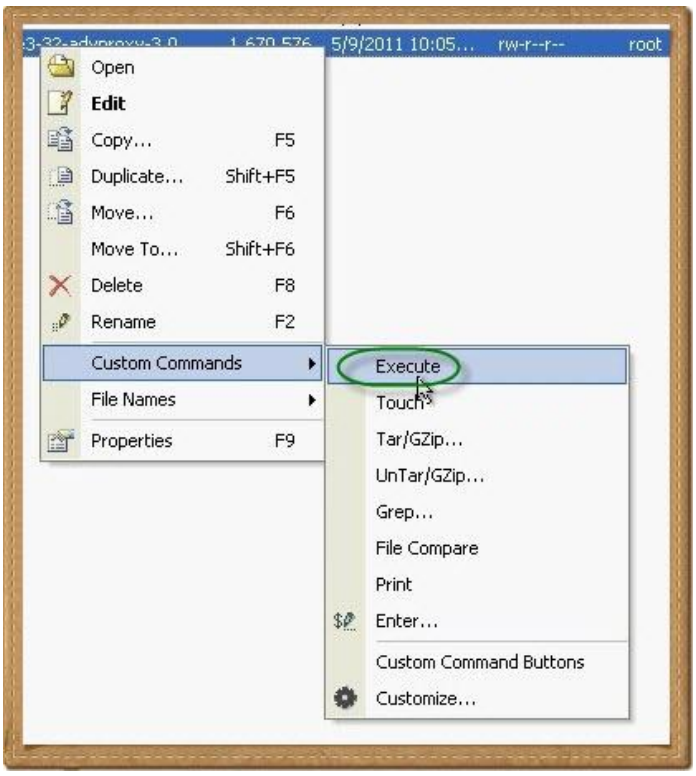
من Tools نختار Shell



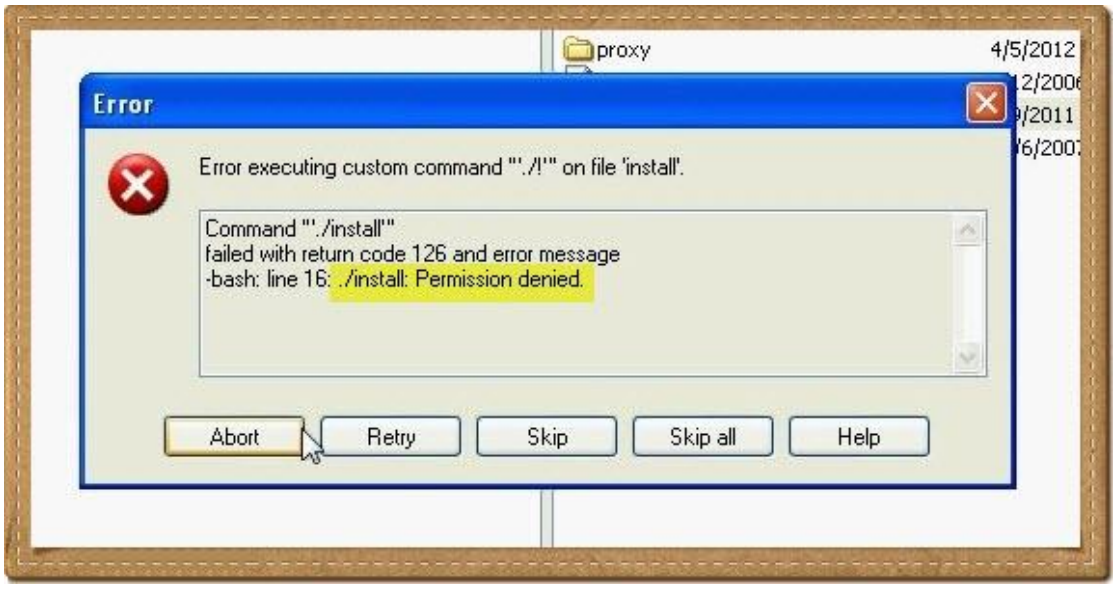
سيطلب منا أن نكون Root

سيبك من الكلام ده كله وخلينا في الطريقة الثانية

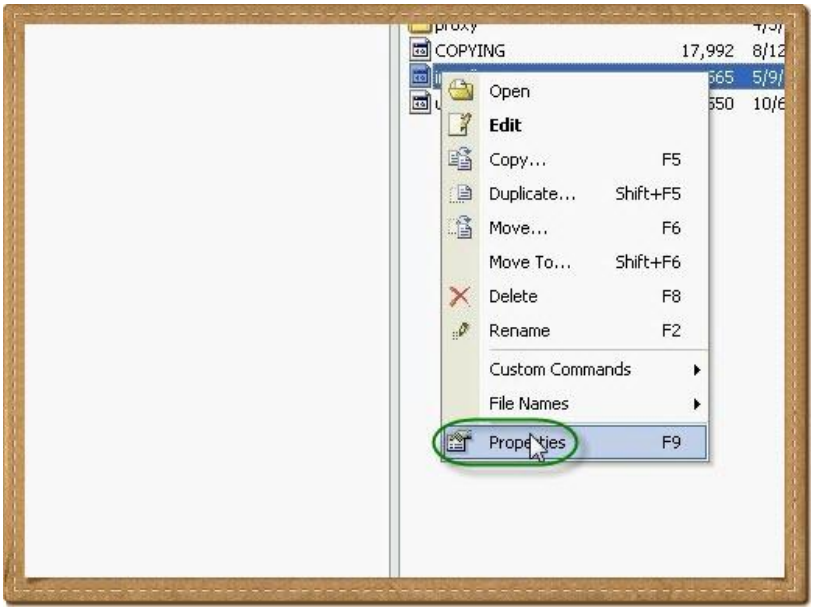
إرجع للبرنامج وكليك يمين على ملف Install ومن Custom Commands إختار Execute



رسالة الخطأ تعمدت وضعها حتى نعتاد على قراءة هذه الرسائل ومانخافش منها , هناك خطأ في الـ Permission

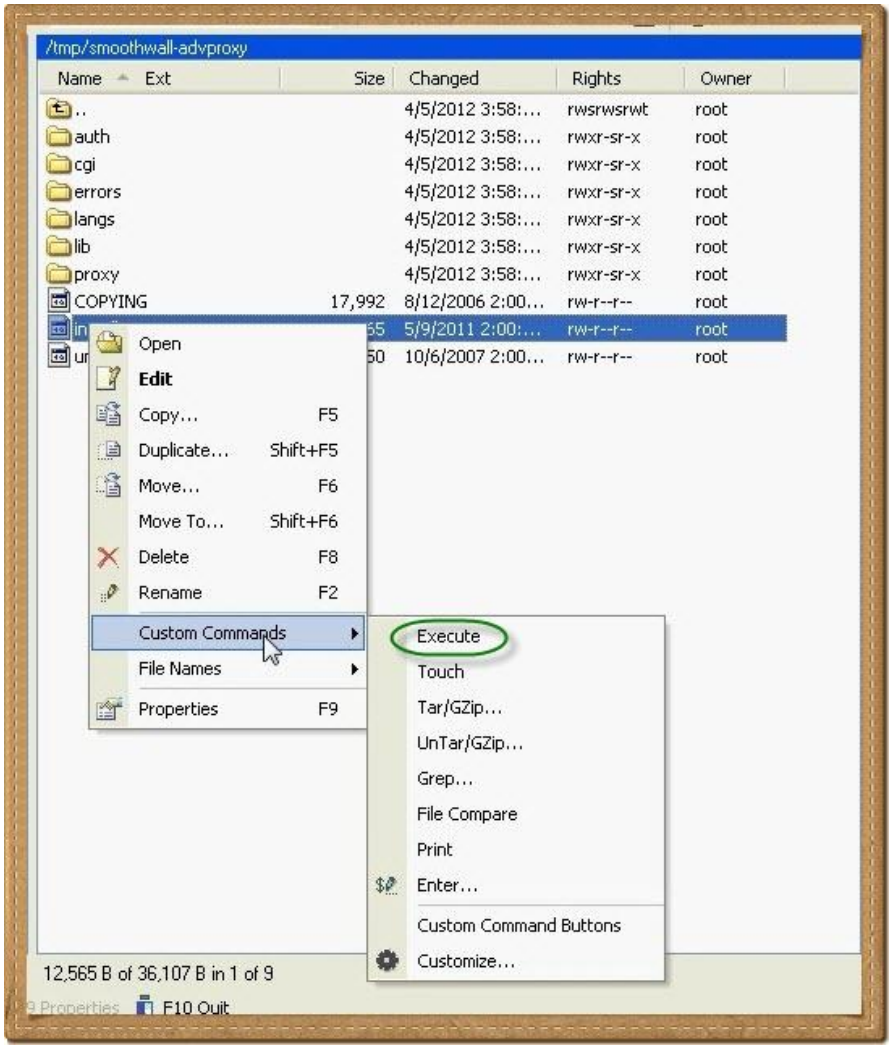


لتعديل الـ Permission كليك يمنين على الملف أو الفولدر المطلوب تعديله ونختار Properties



لم أهتم كثيرا بنوعية الـ Permission المطلوب فتحتها على البحري أسهل ولكن لو ظهرت أمامك مثل هذه الرسائل يجب عليك البحث والجوجوله لإختيار التصاريح المطلوبة بدقة

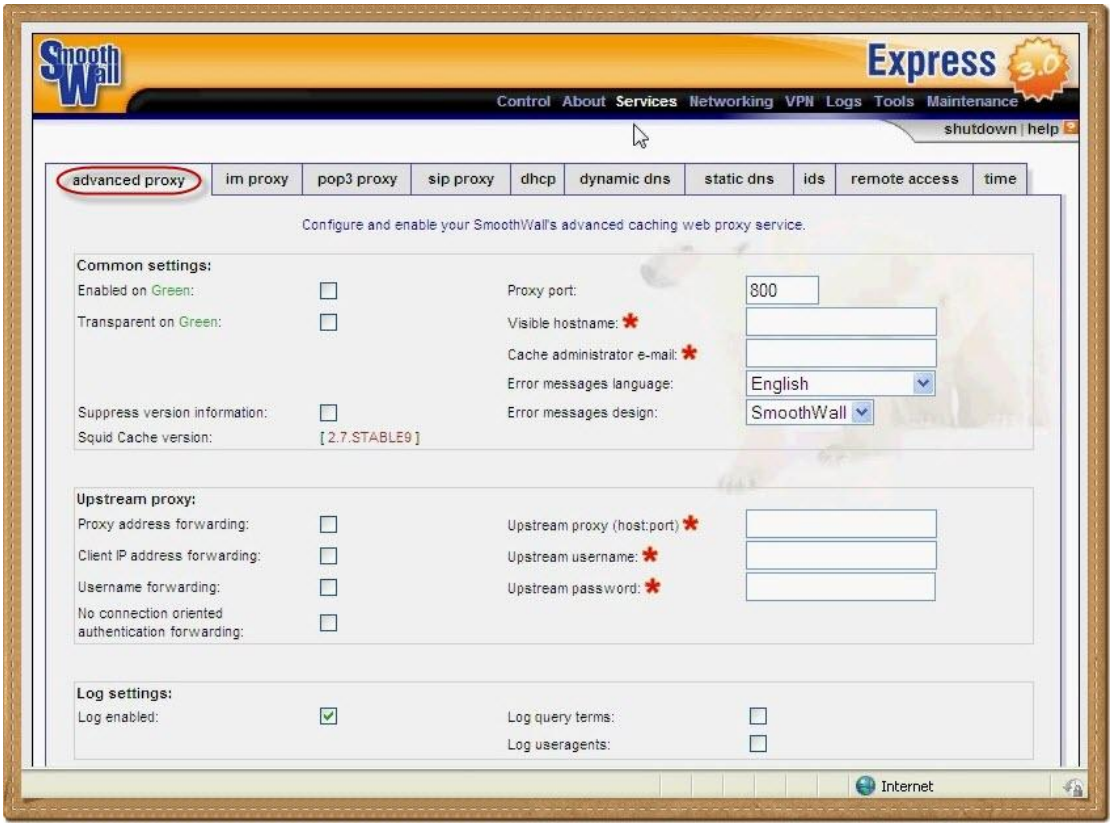
نجرب ثانية



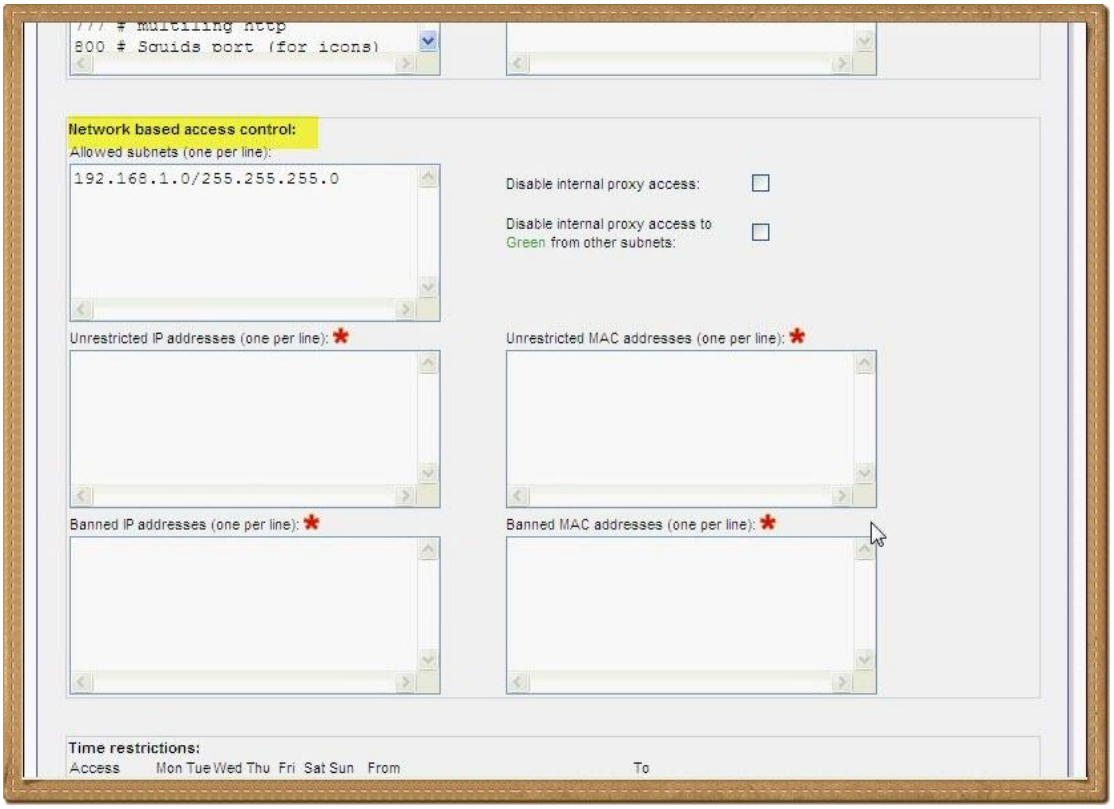
تمام

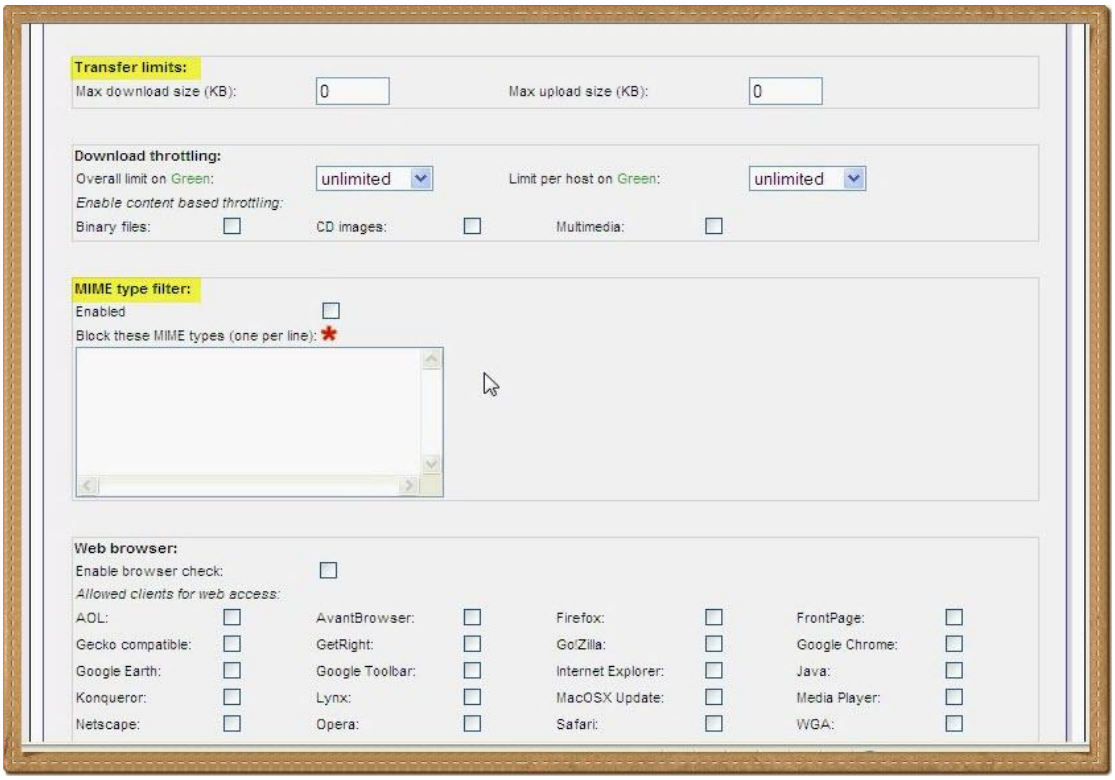
نفتح واجهة إدارة SmoothWall وفي Services سنجد Advanced Proxy

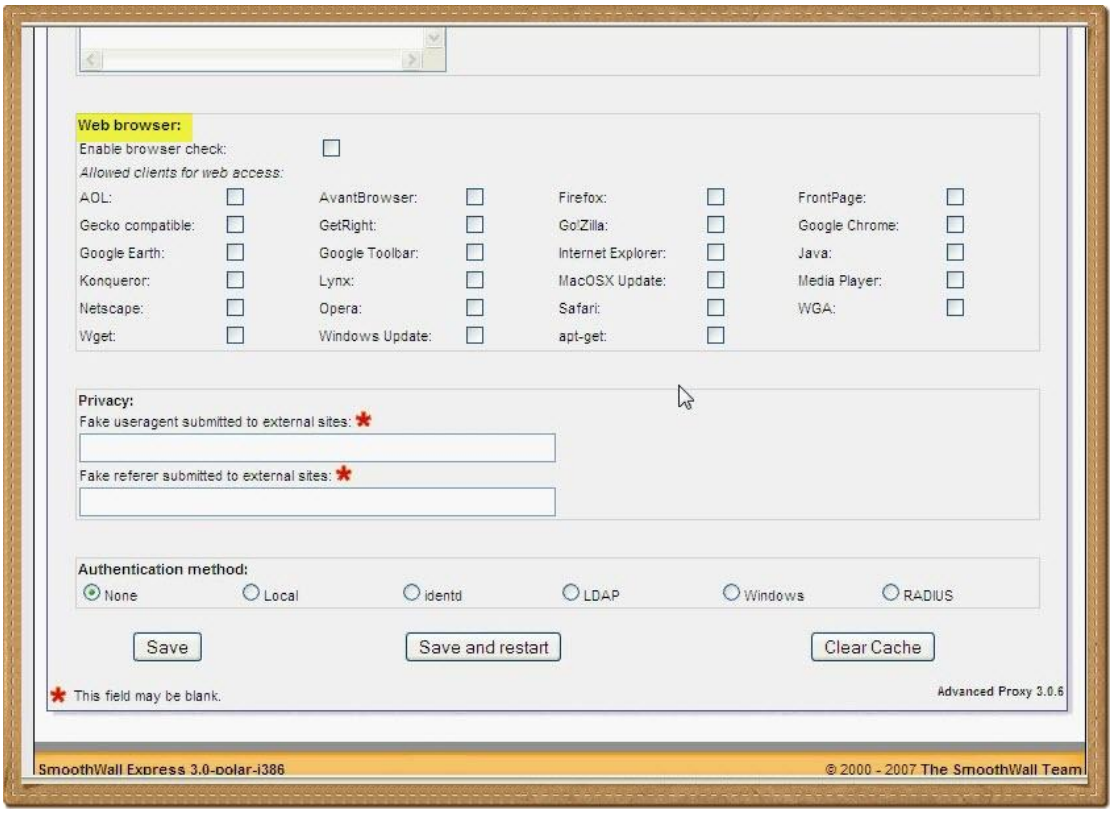
ماشاء الله إضافة جميلة جدا جدا



مش محتاجه شرح فقط ركزوا على ما وضعت له علامات صفراء






Web browser:
Enable browser check:
Allowed clients for web access:
AOL:
AvantBrowser:
Firefox:
FrontPage:
Gecko compatible:
GetRight:
Go!Zilla:
Google Chrome:
Google Earth:
Google Toolbar:
Internet Explorer:
Java:
Konqueror:
Lynx:
MacOSX Update:
Media Player:
Netscape:
Opera:
Safari:
WGA:
Wget:
Windows Update:
apt-get:
Privacy:
Fake useragent submitted to external sites:
Fake referer submitted to external sites:
Authentication method:
None
Local
identd
LDAP
Windows
RADIUS
Save
Save and restart
Clear Cache
This field may be blank.
Advanced Proxy 3.0.6
SmoothWall Express 3.0-polar-i386
© 2000 - 2007 The SmoothWall Team

يوجد الكثير من الإضافات المفيدة جدا مثل :

URL Filter

Open VPN

DansGuardian Content Filtering

Ad Zapping

وغيرها الكثير كما يوجد بعض المنتديات العربية تحاول التخصص في شرح SmoothWall و IPCop

الموضوع محتاج منك إجتهاد وفي المقابل ستحصل على فايروول رائع وبديل لـ تي إم جي يعمل على جهاز لايتعدى ثمنه 200 جنيه

اللهم إجعلني خيراً مما يظنون واغفر لي مالا يعلمون

اللهم إني أعوذ بك أن أشرك بك شيء أعلمه وأستغفرك لما لا أعلمه

سبحانك اللهم وبحمدك , أشهد ألا إله إلا أنت , أستغفرك وأتوب اليك

الفصل الثامن : Untangle

Untangle

الحمد لله والصلاة والسلام على رسول الله

سيدنا محمد النبي, وأزواجه وذريته وأهل بيته

سنختم الحديث عن السيرفرات بسيرفر لينكس وهو Untangle وهو يتعامل مع الإضافات (يسميها Apps) بصفة أساسية فهو بخلاف SmoothWall يطلب منك بعد إنتهاء الإعداد إختيار الـ Apps التي ستستخدمها , السيرفر مجاني ولكن إضافاته جزء منها مجاني والجزء الأهم بفلوس

مشكلة Untangle أنه تقيل شويتين بعكس الـ SmoothWall وهو كما ذكرت توزيعة لينكس مطورة من Debian

أغلب توزيعات اللينكس الشهيرة يمكنها العمل كبروكسي بقليل من الخبرة والجوجلة والفهلوة لكن غالبا ح تتضطر تتعامل مع أوامر الـ Shell

عموما أنا ماحبيتش الـUntangle

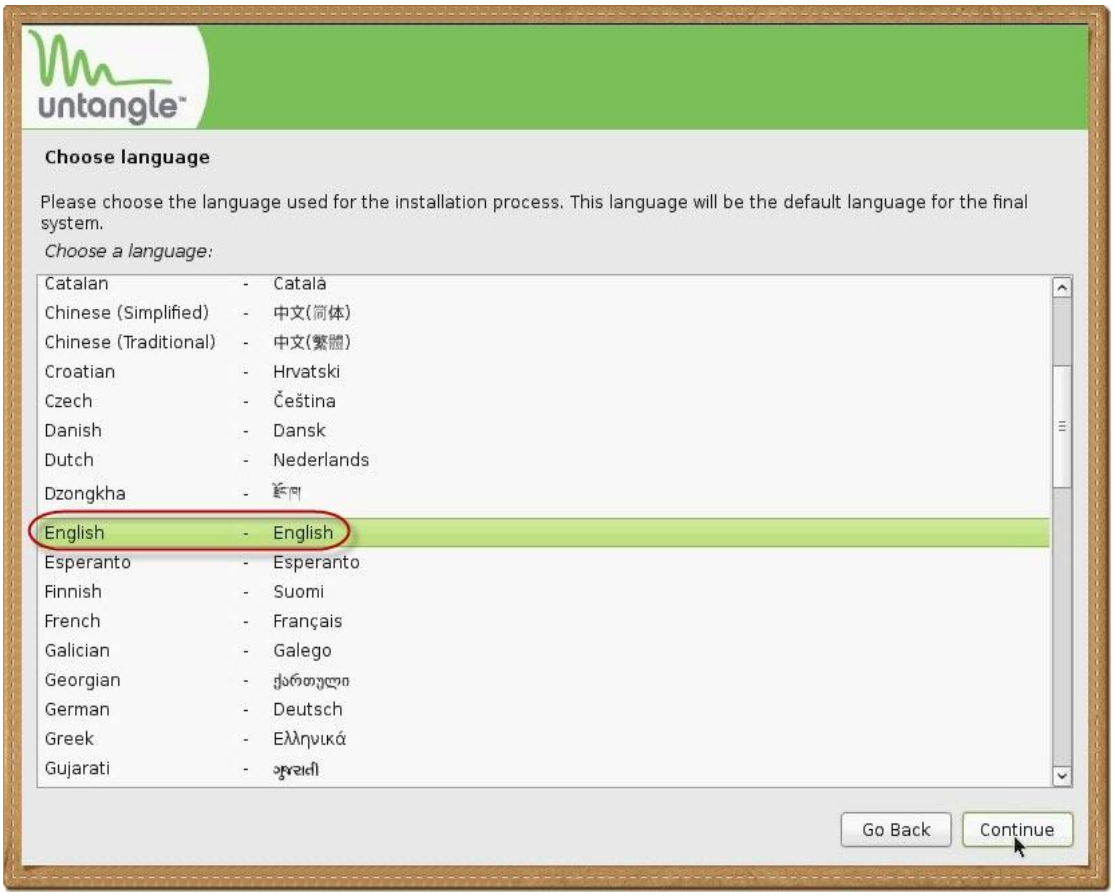
ماعلينا , ننزل النسخة ونحرقها ونبوت الجهاز عليها

نختار Expert Mode و Enter

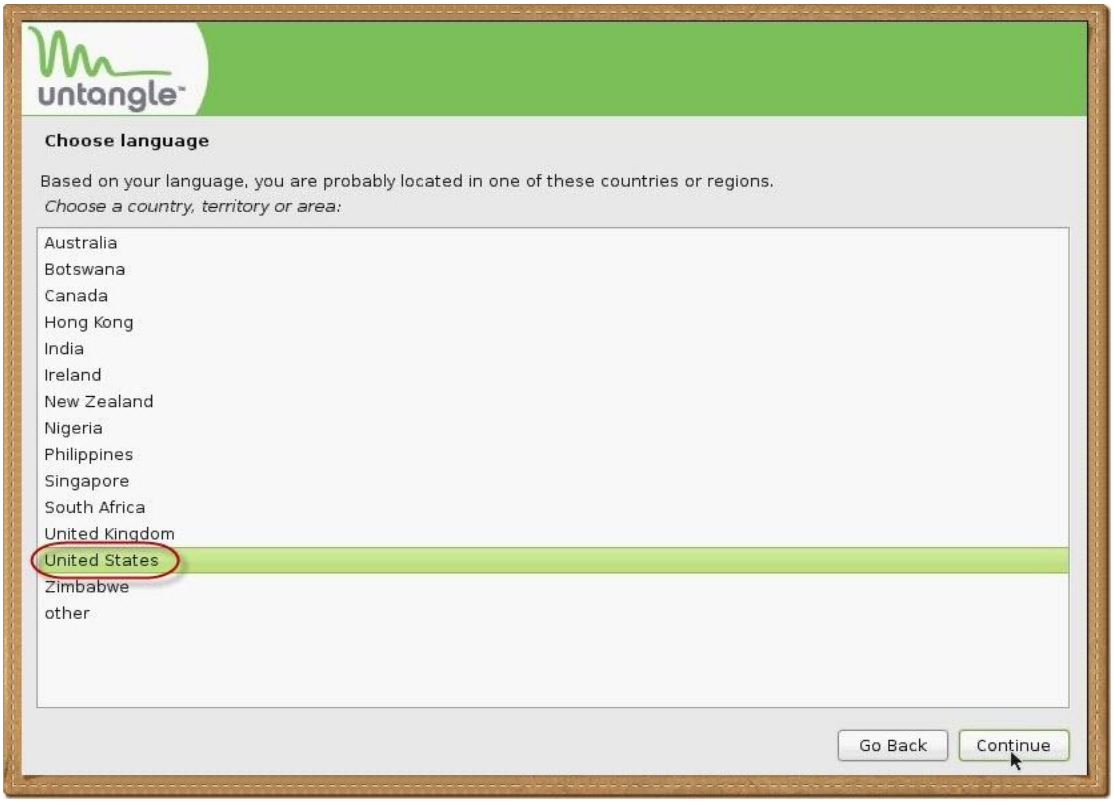
بيبووت

نختار English

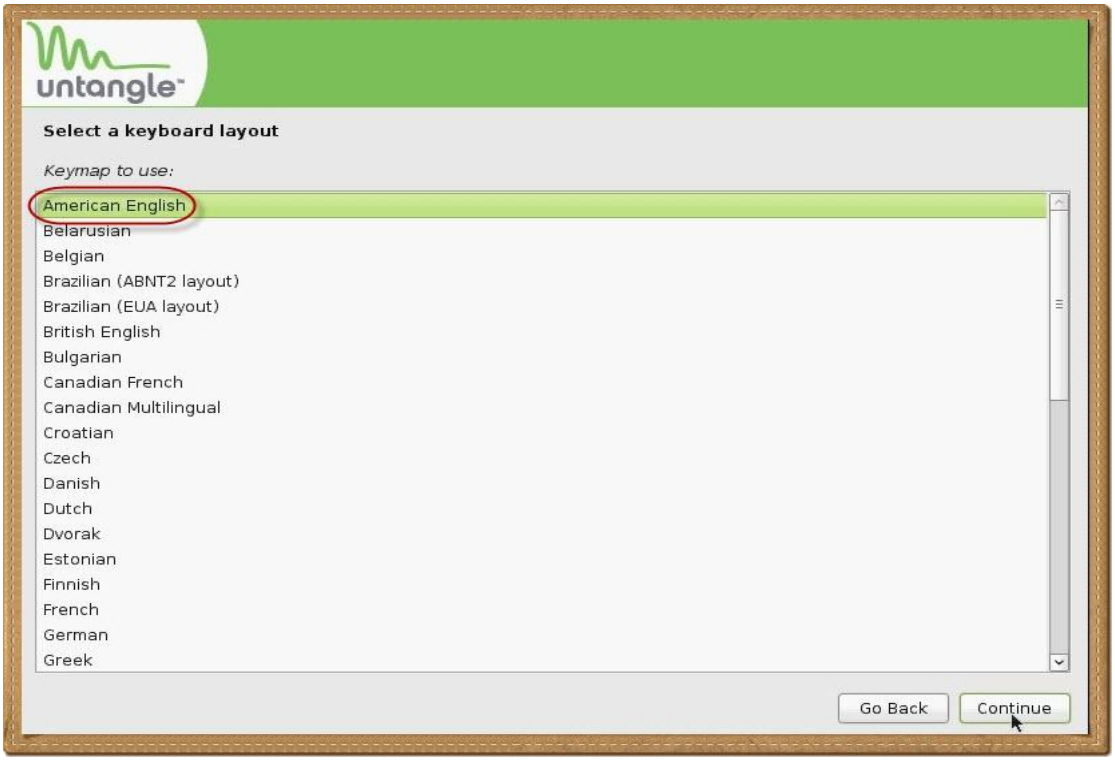
و Continue



أي حاجة ثم Continue

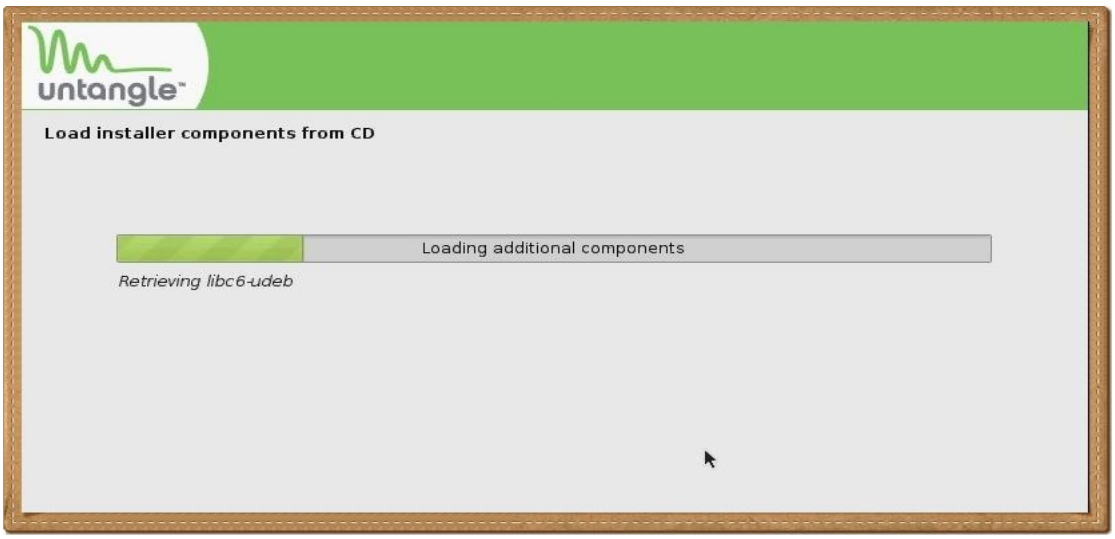


اللغة طبعاً English

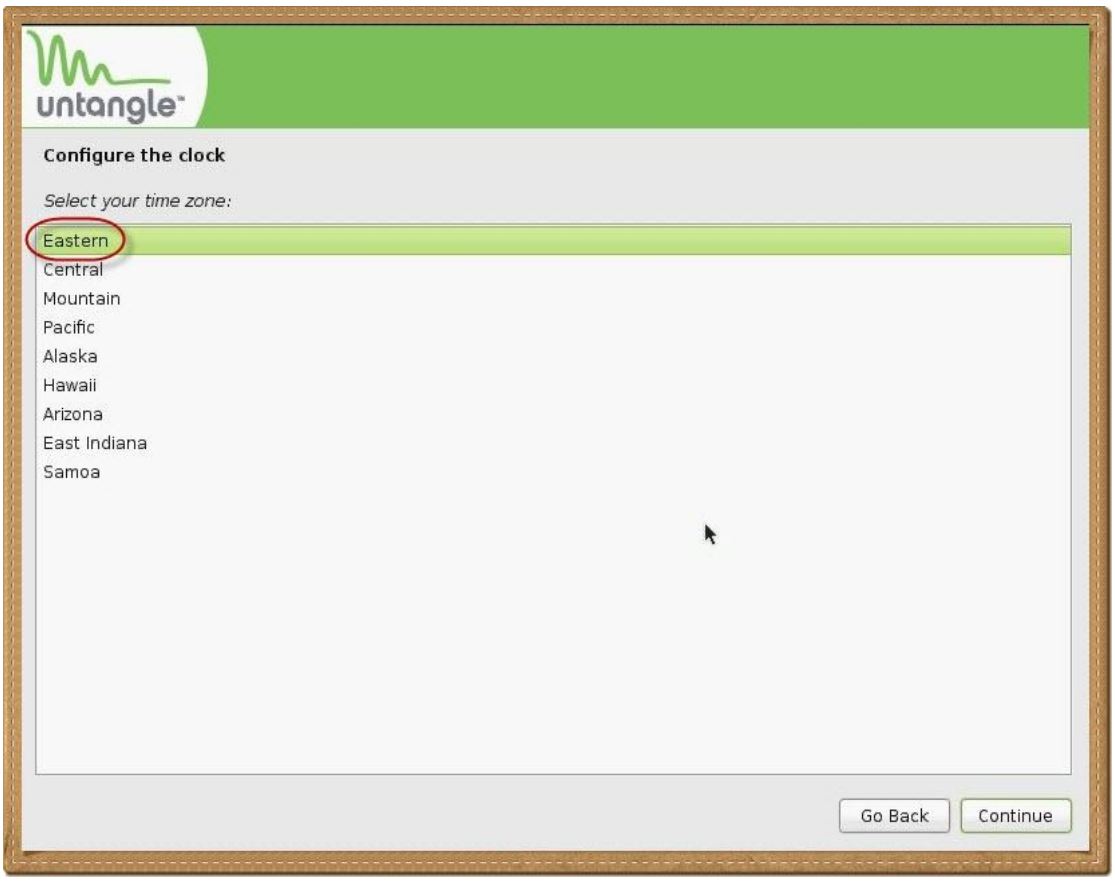


نسيبه يشتغل

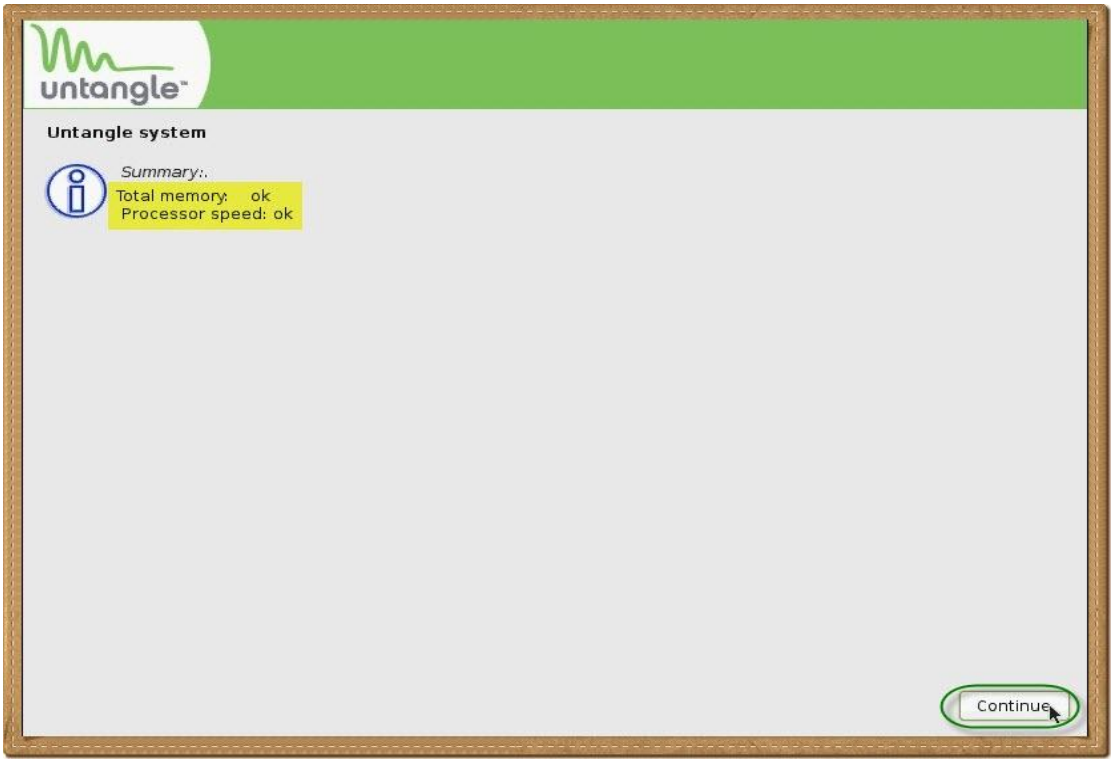
بطيييييييي ء



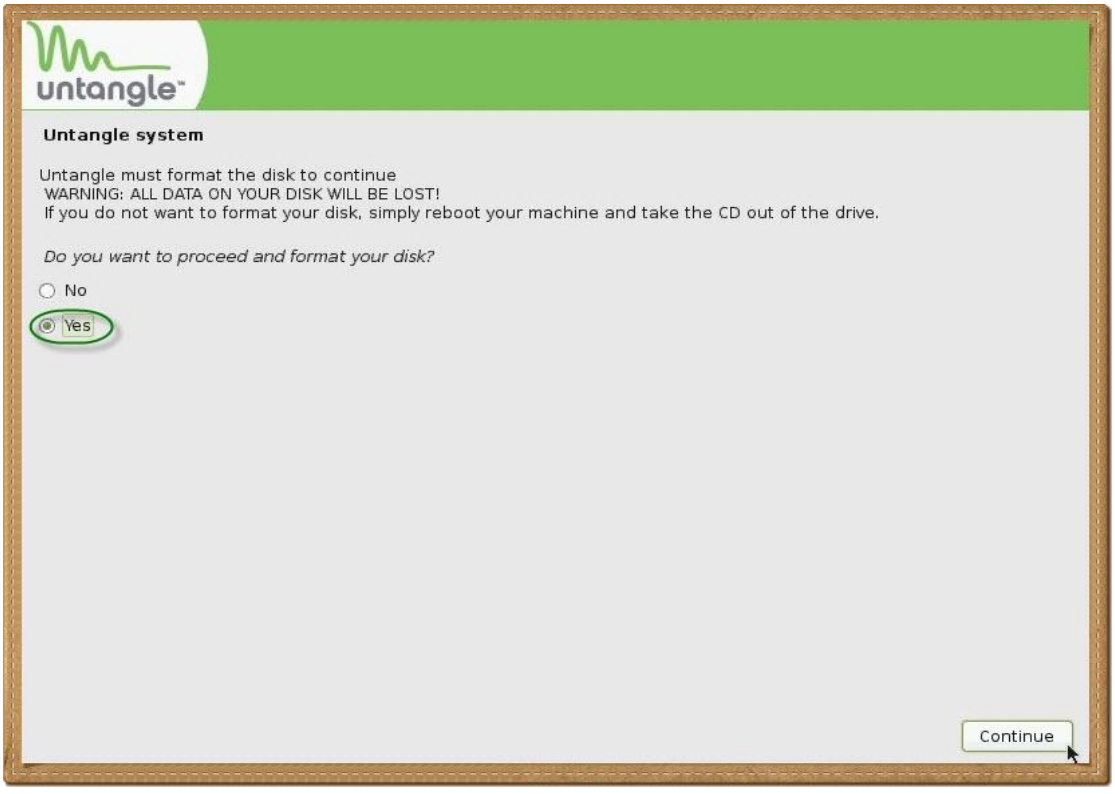
التوقيت أي حاجه

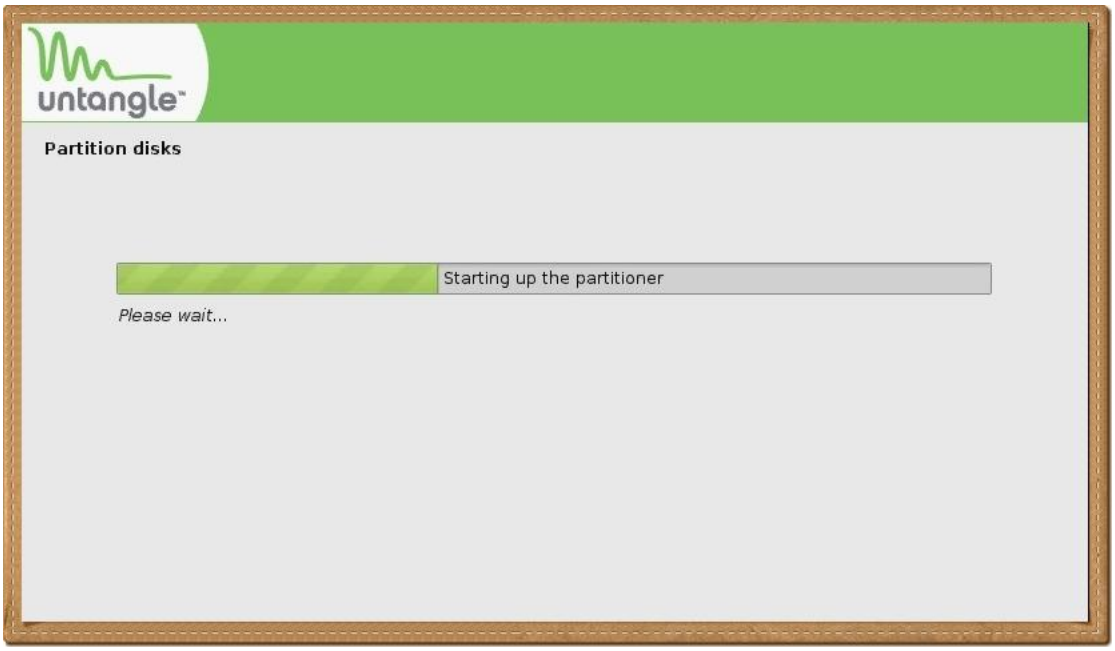


Continue

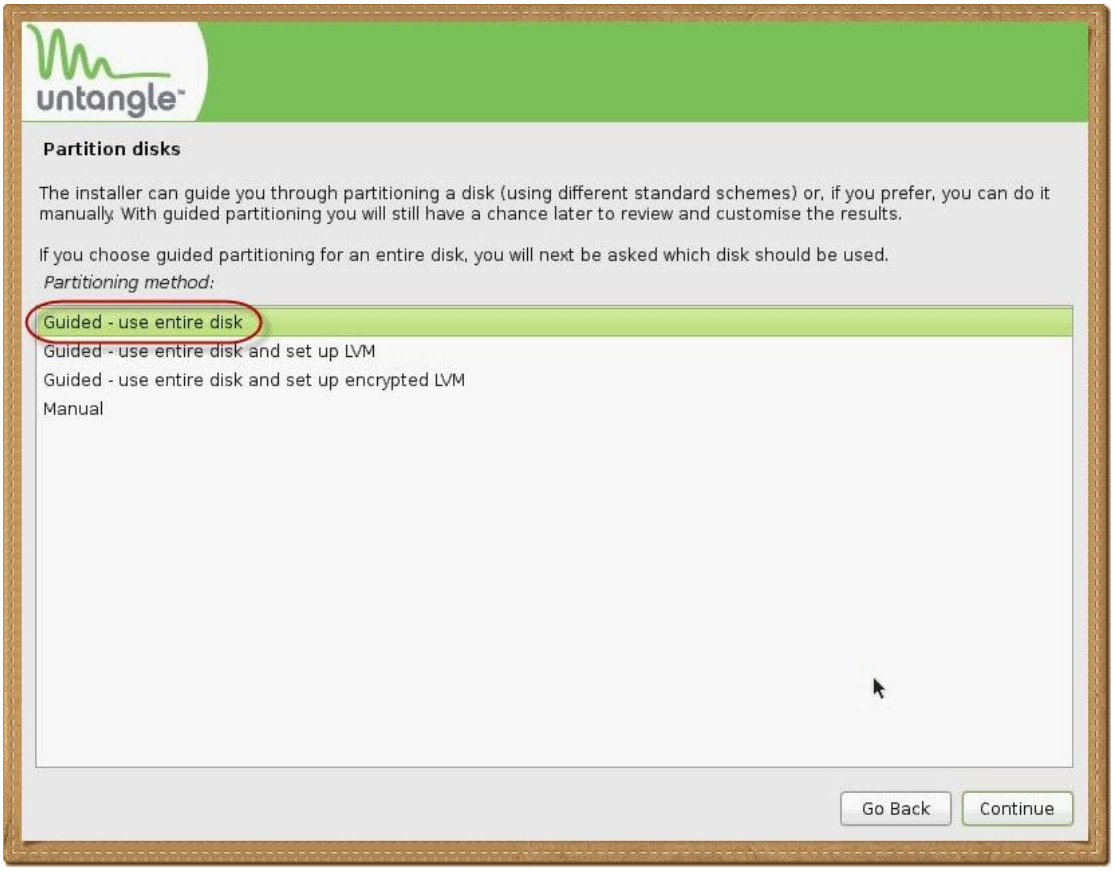


Yes للموافقة على الفورمات

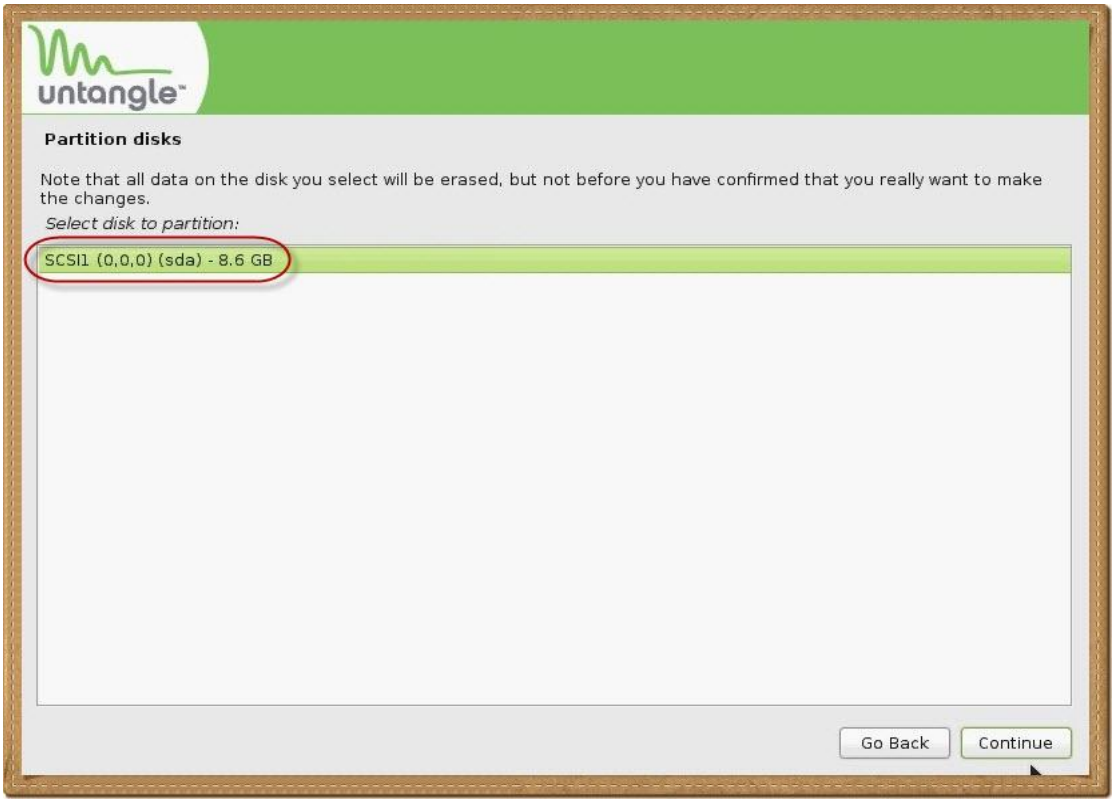


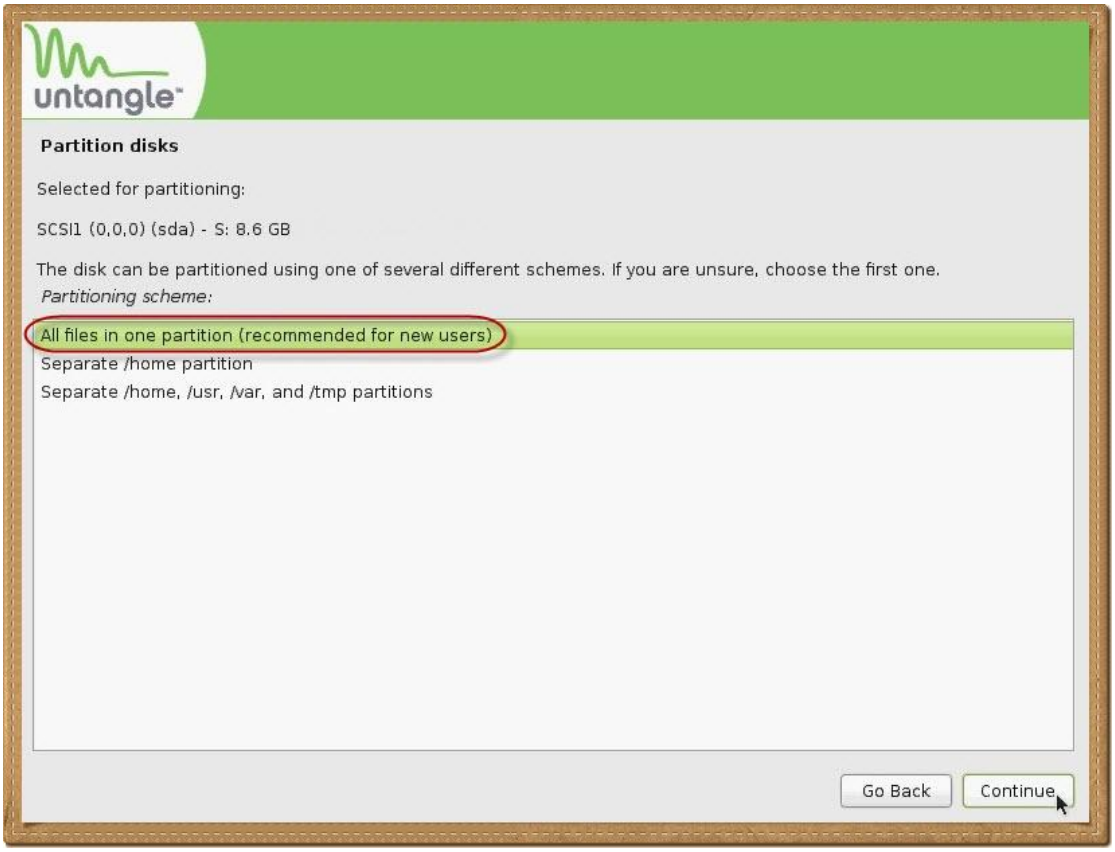


تقسيم الهارد , إذا ماعندكش خبرة باللينكس إعمل زي الصور

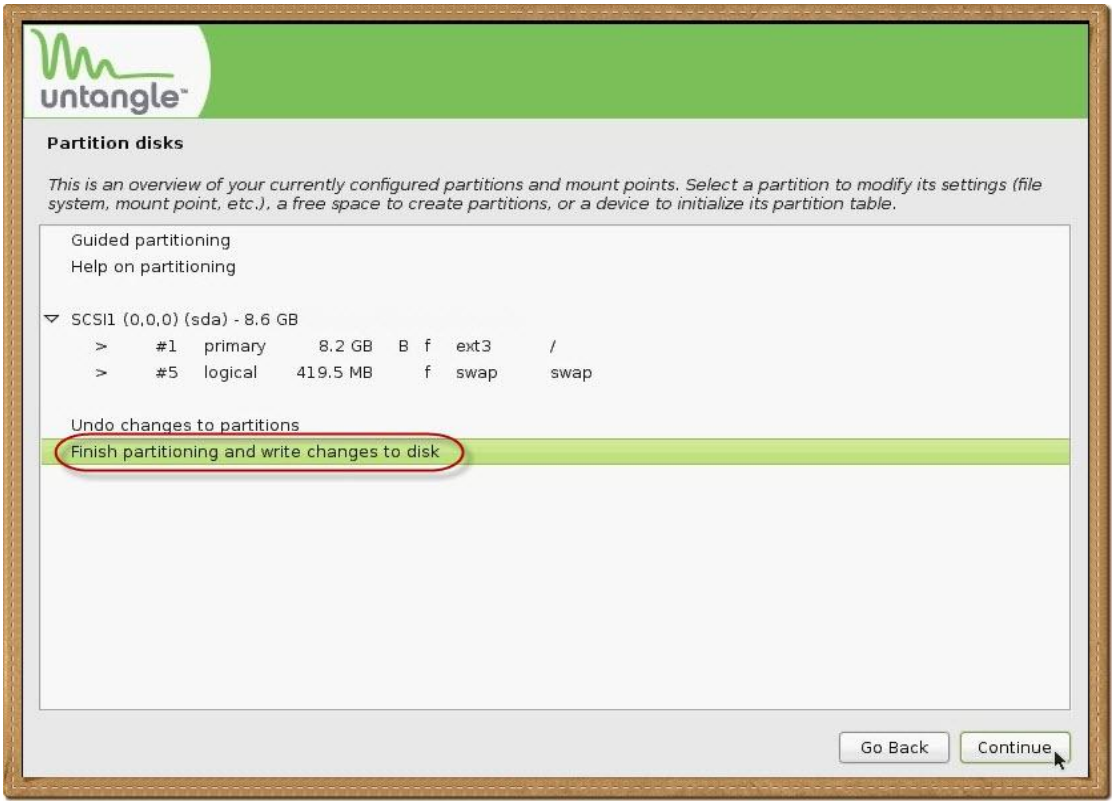


هو هارد واحد ح نختاره

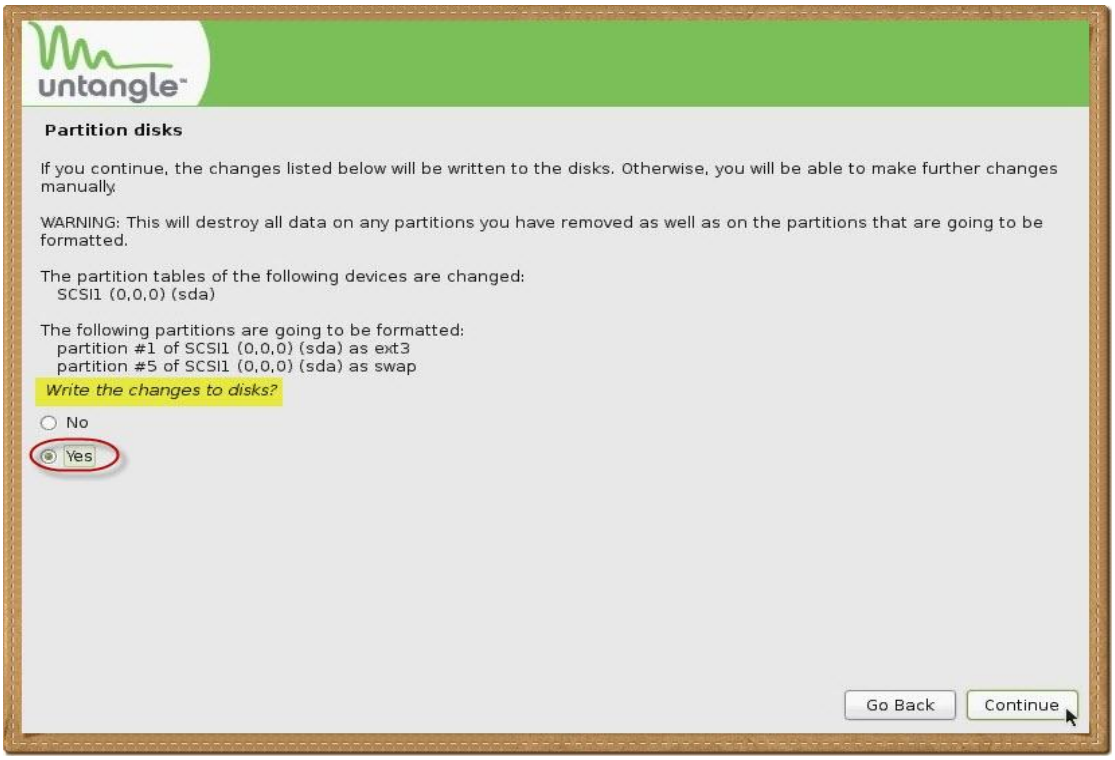


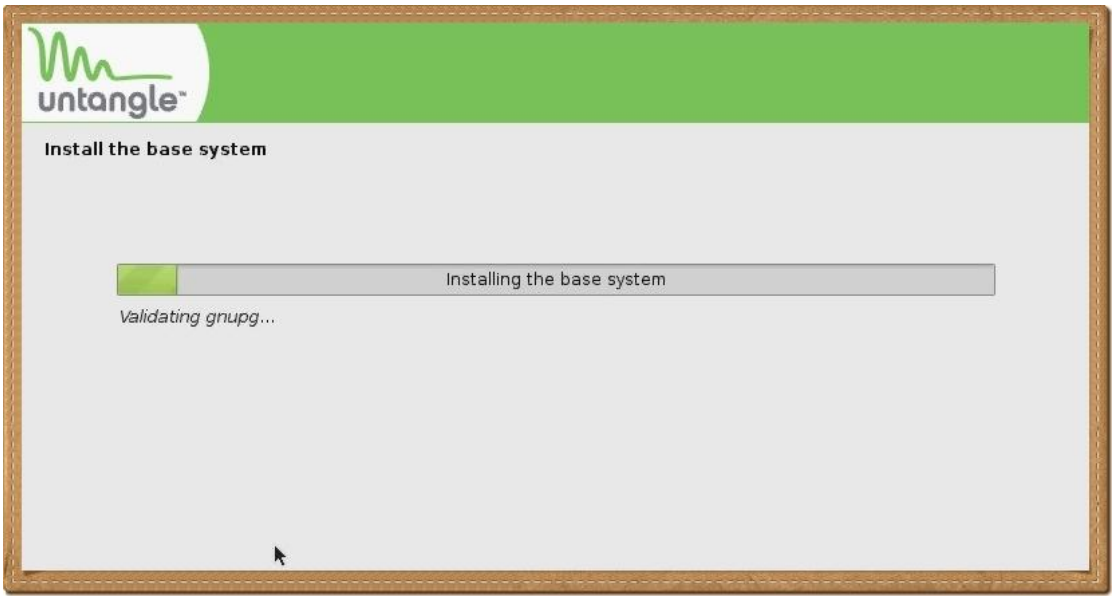


وافق على الكلام المهم الكبير ده و Continue



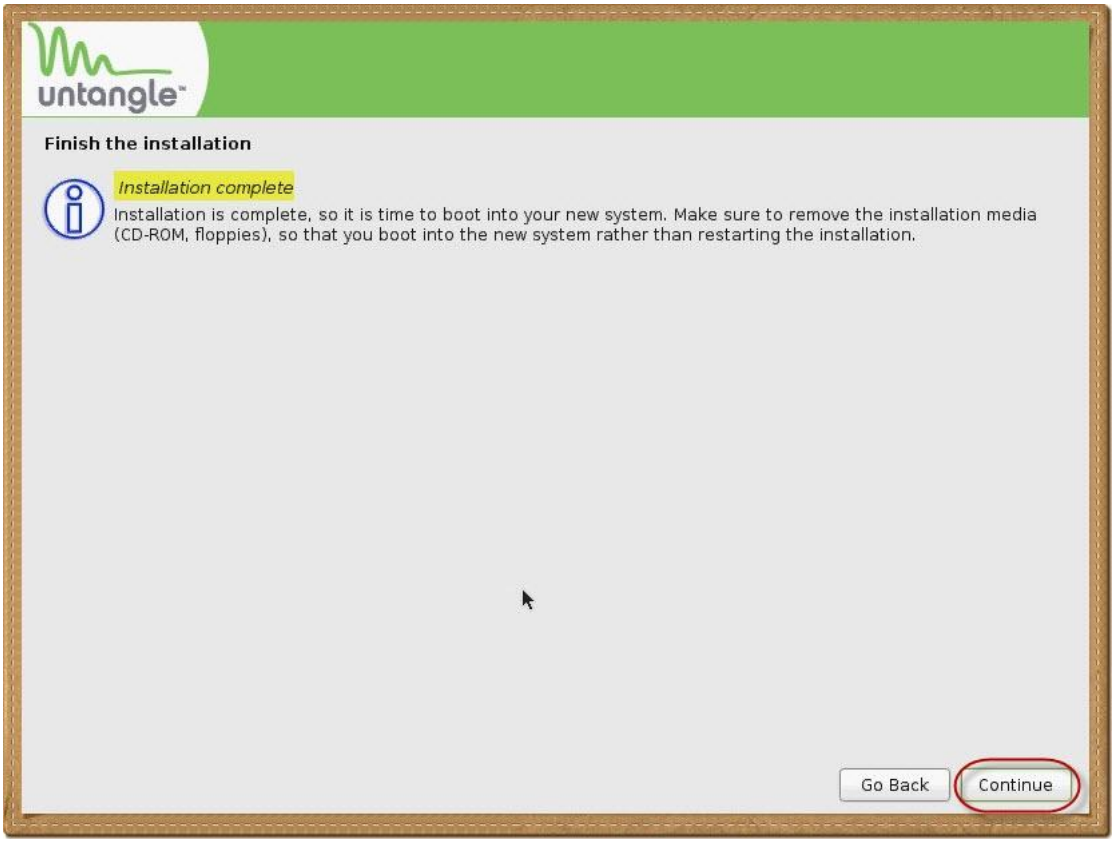
ياعم والله موافق , Continue أصعب في الكتابه Next أسهل





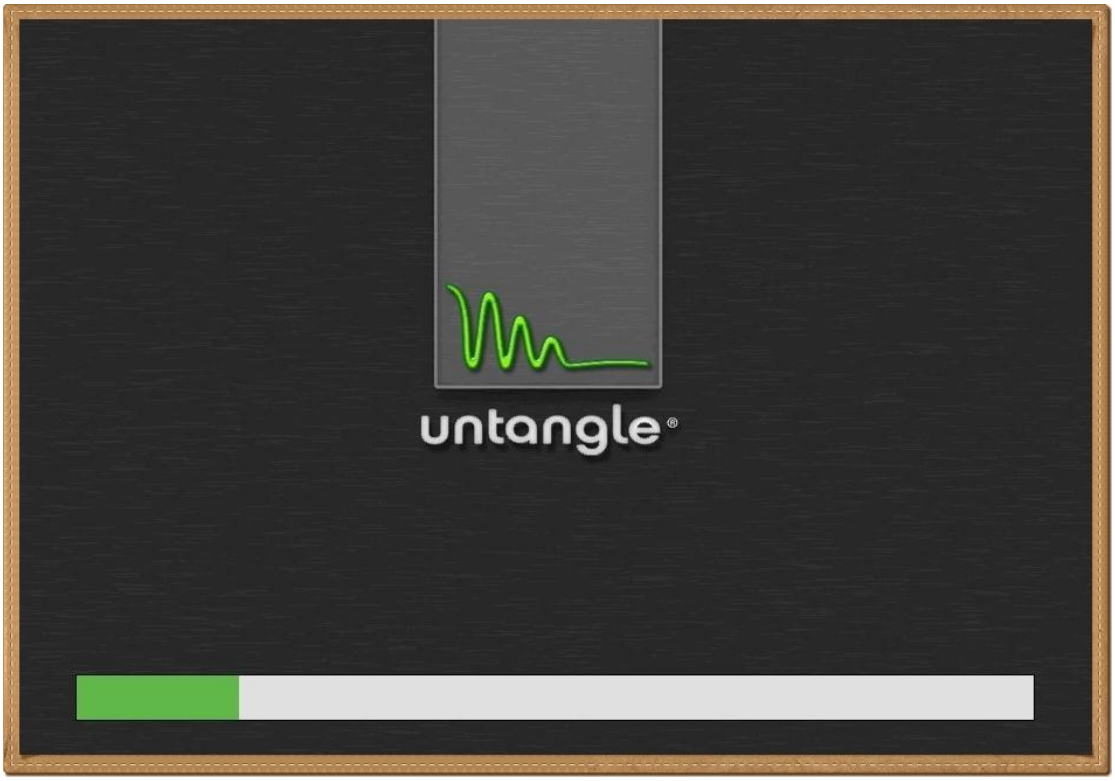
الـ Continue الأخير

وبعدها ريبووت



أول إختيار أو الثاني ثم Enter

براحته



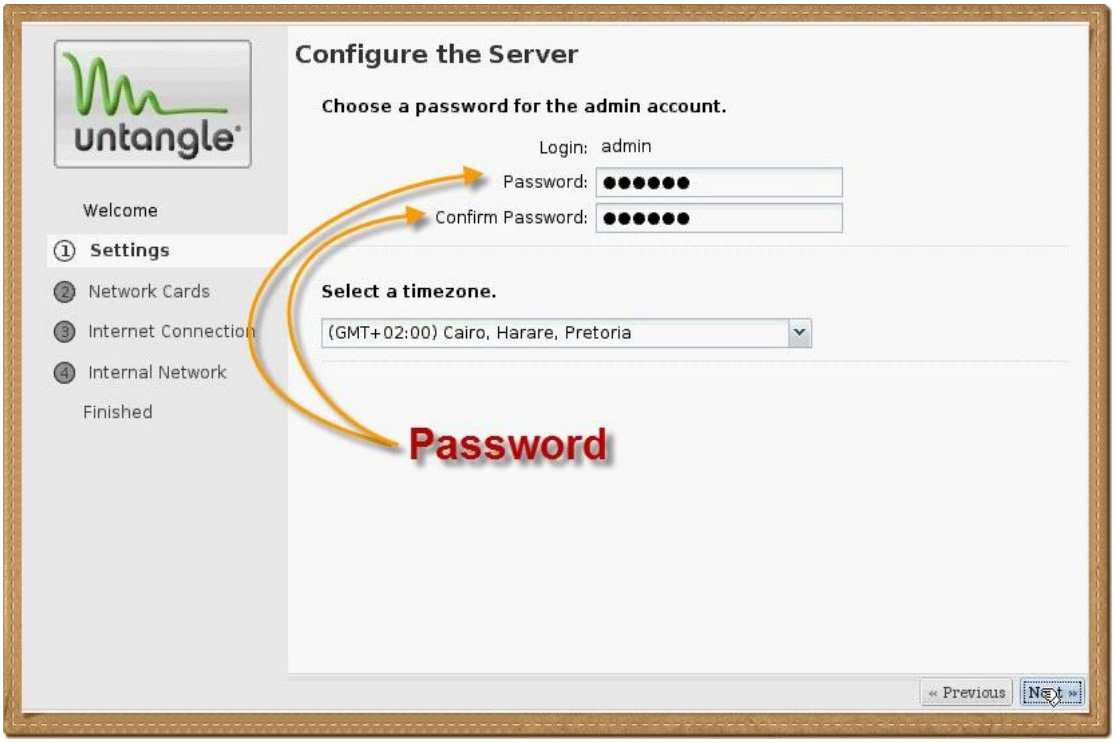
ماتزهقش

اللغة تاني ☺

ثم Next

Next

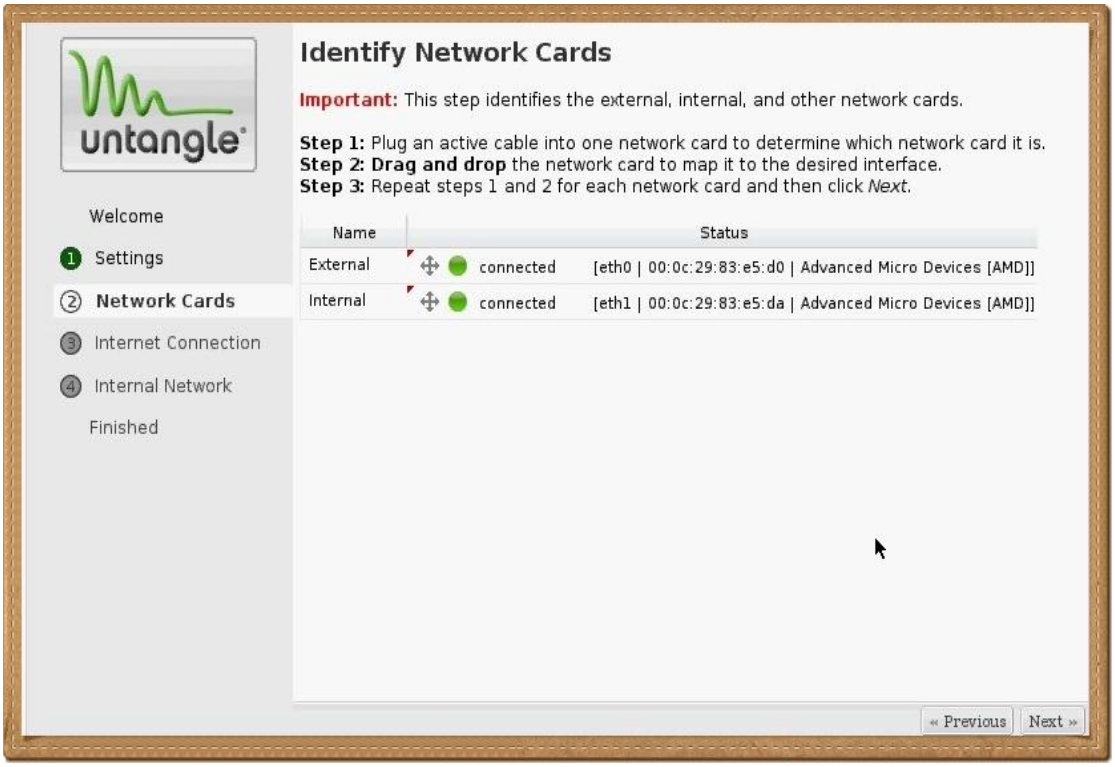
كالعادة Admin باسوورد



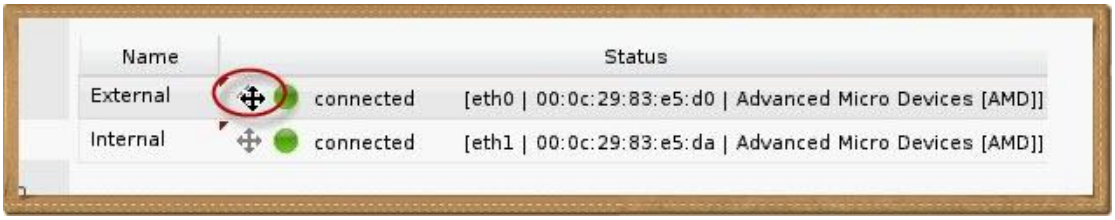
ونسيبه يشتغل

أهم شيء كما تعودنا هو إعدادات كروت الشبكة External و Internal أو أخضر وأحمر

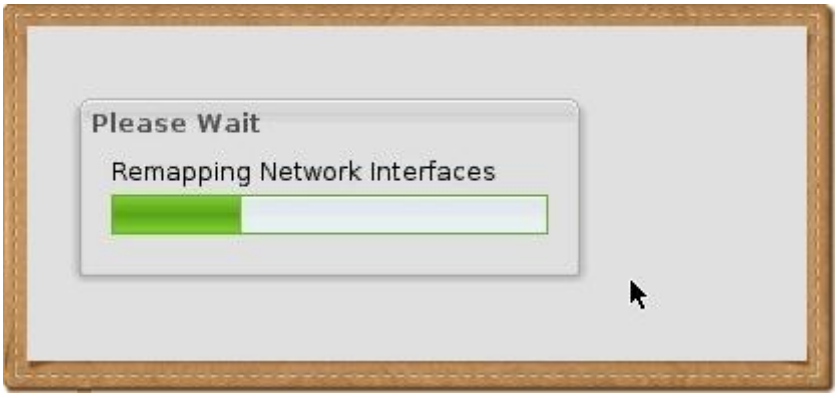
أيا كان حتى لو سميناهم بكيزة وزغلول



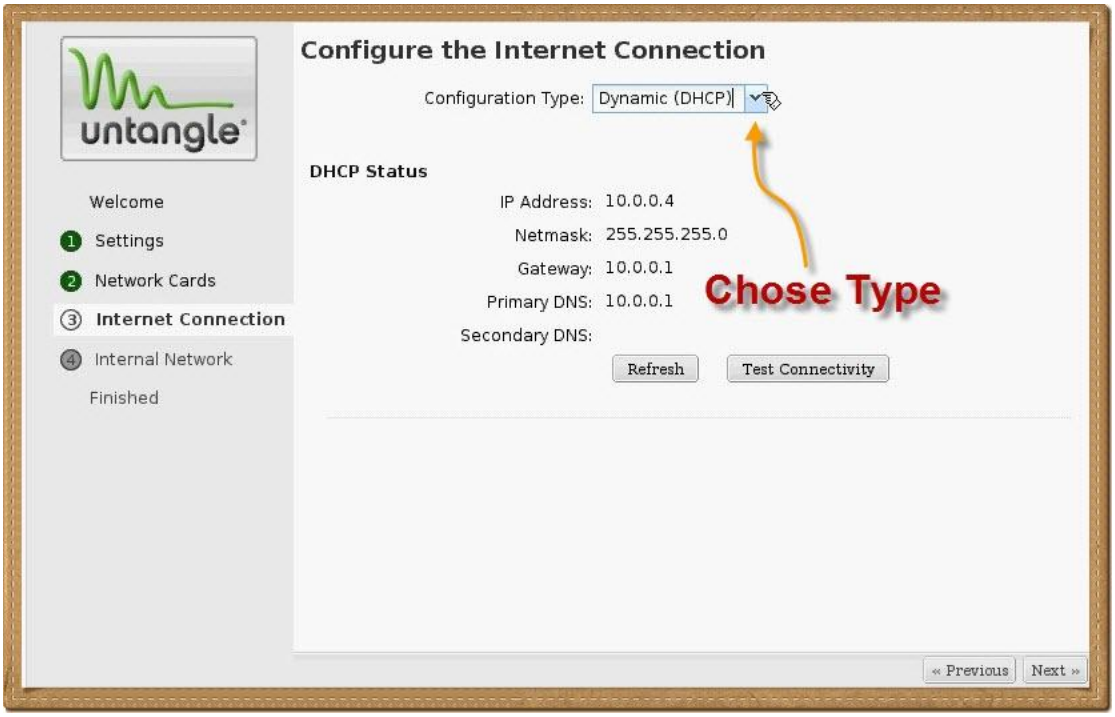
لتحويل الكارت من External إلى Internal أو العكس نستخدم السحب الضغط بالماوس على علامة زائد أمام الكارت وسحبه إلى المكان الآخر



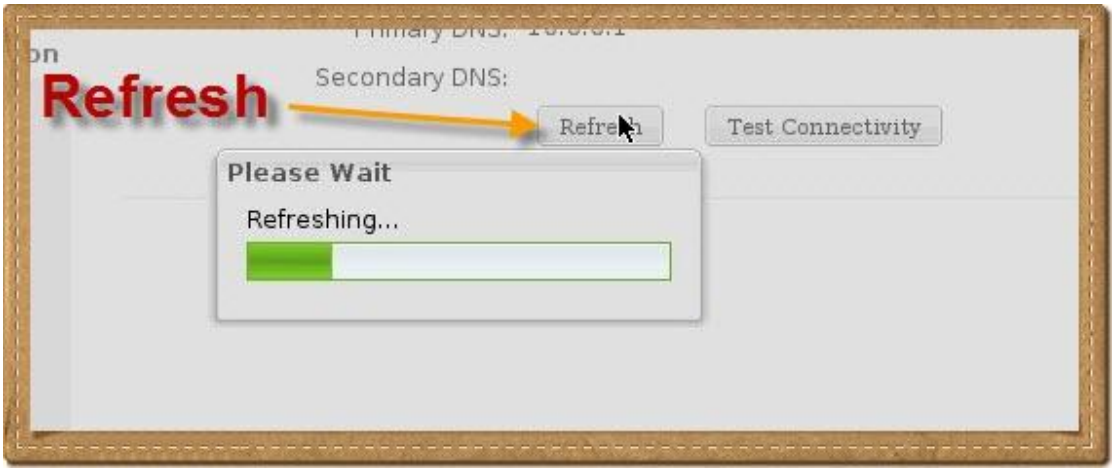
وبرضه بعد مانخلص نضغط Next ونسيبه يشتغل



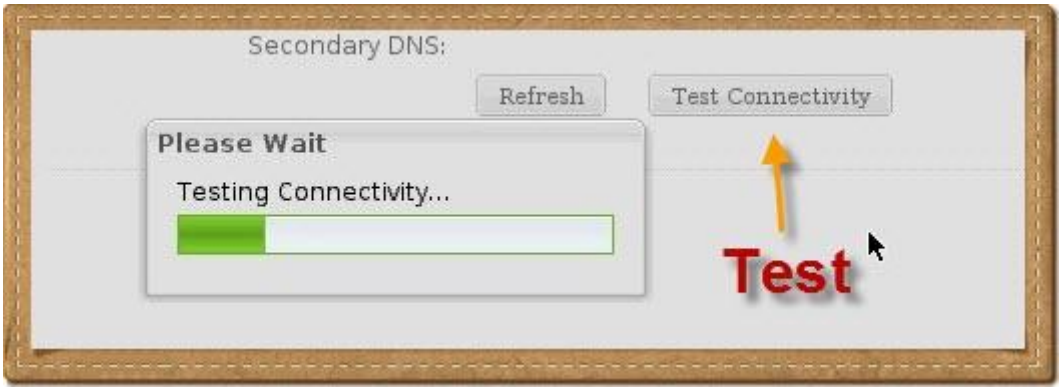
إعدادت كارت الإنترنت External , كالعادة الإختيار بين Manual DHCP و PPPOE



بعد الإنتهاء نضغط على Refresh

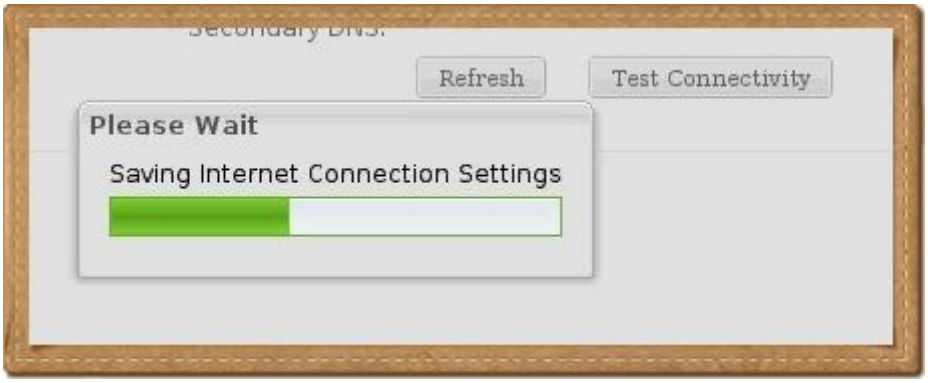


وللتأكد أن الإنترنت متصل بالكارت نضغط على Test Connectivity



تمام

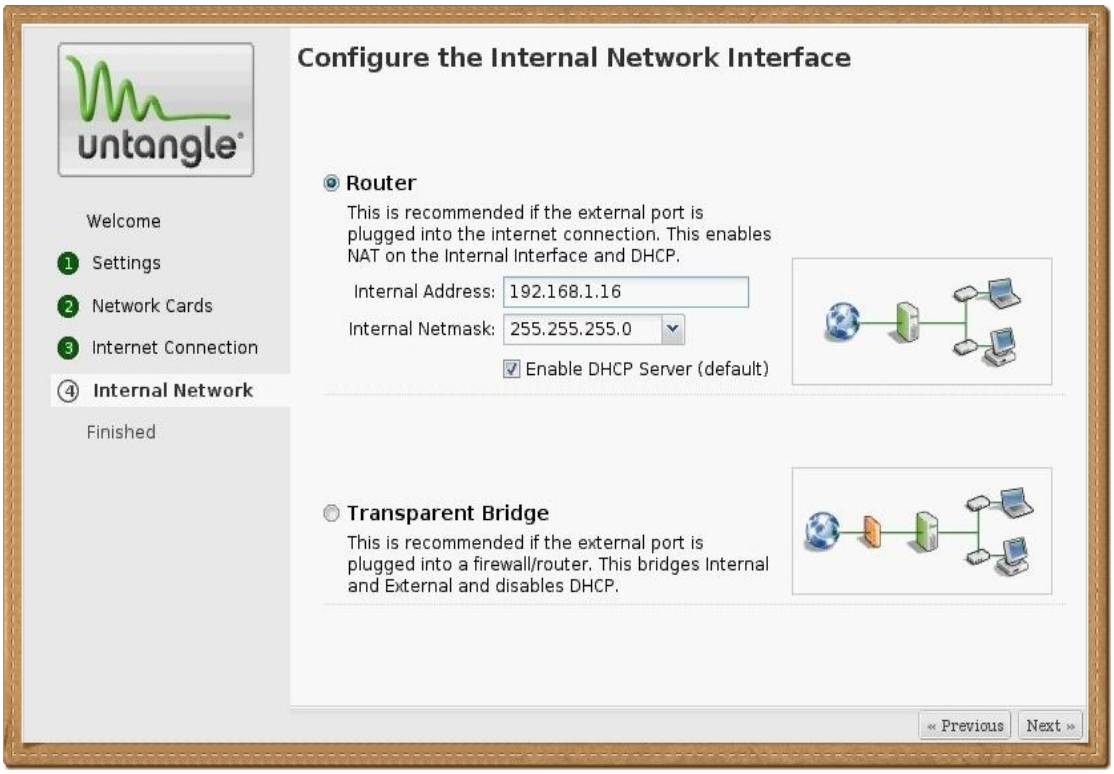
ونكست ونسيبه يشتغل



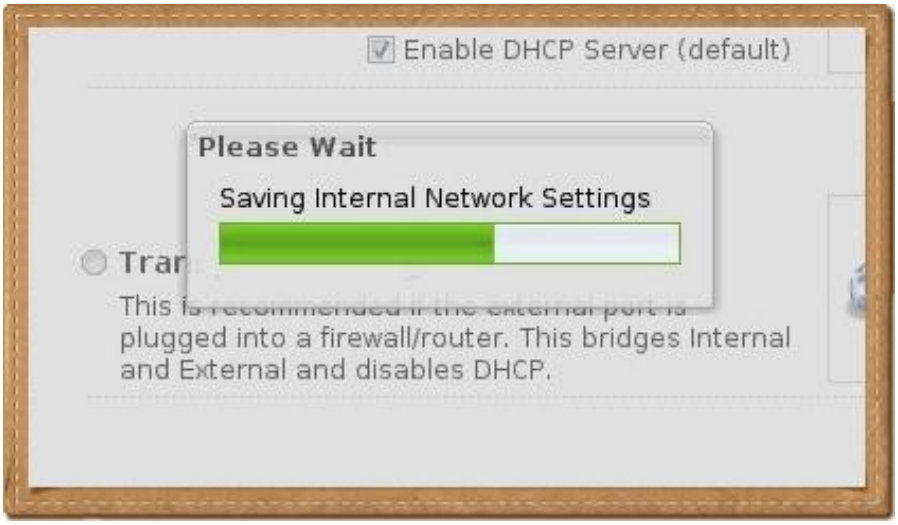
أمامنا نوعين من أنواع الشبكات

- السيرفر متصل بالإنترنت مباشرة
- أو يوجد قبله فايروول

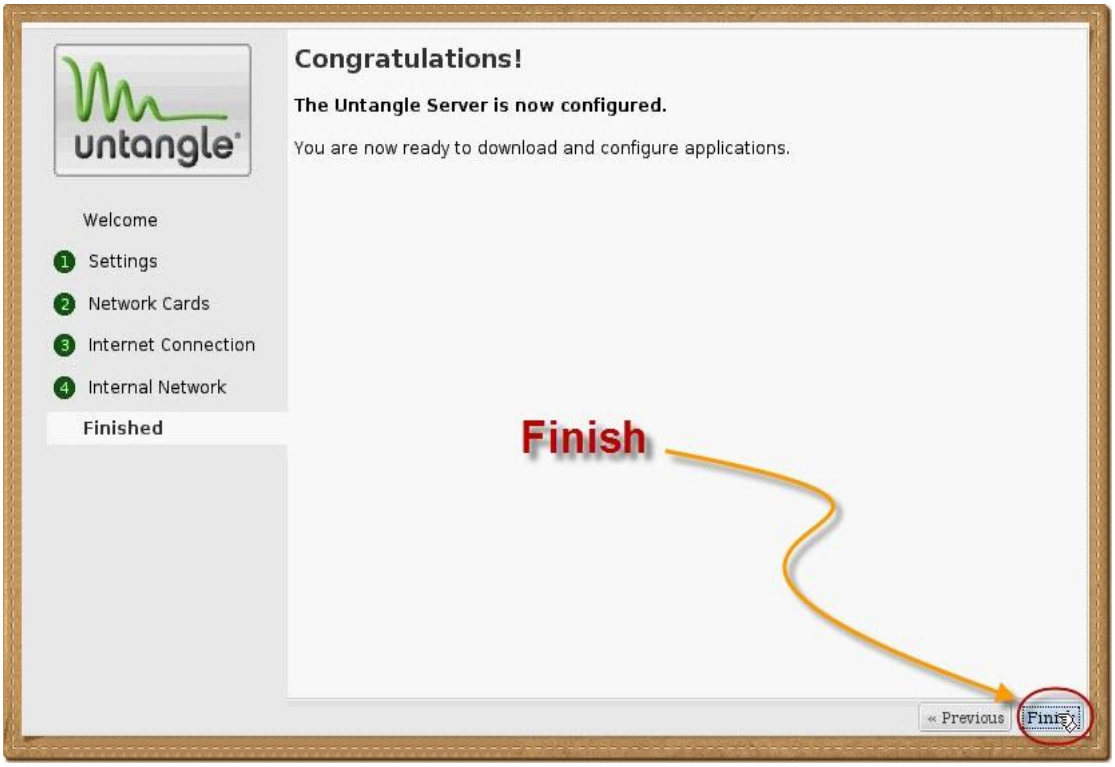
نختار الخيار الأول وإعدادت الكارت الداخلي



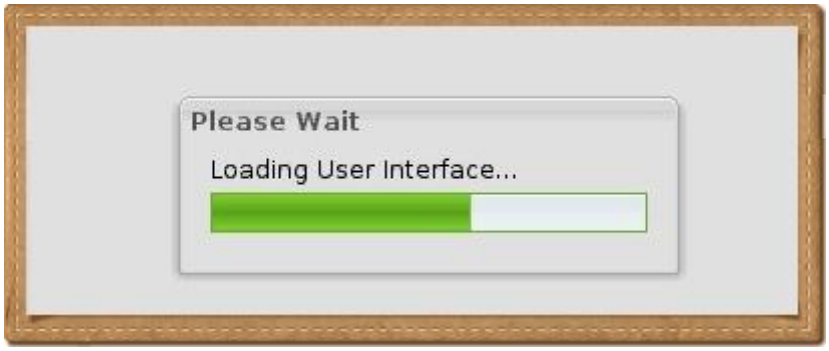
وطبعا : نسيبه يشتغل



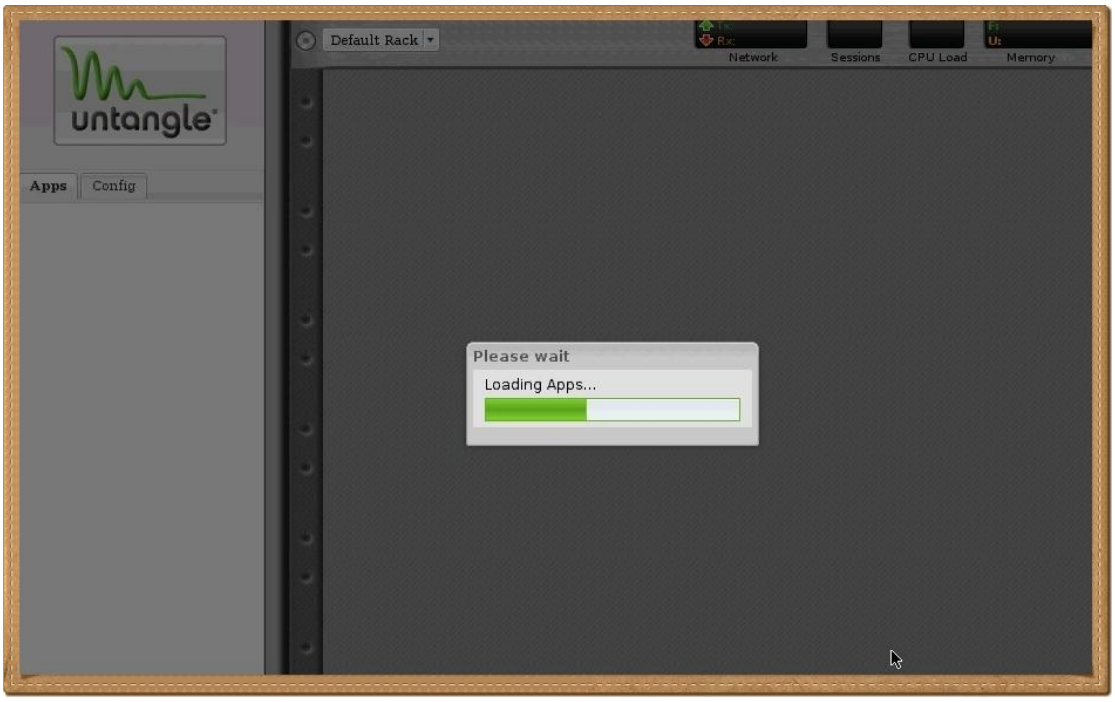
خلاص Finish



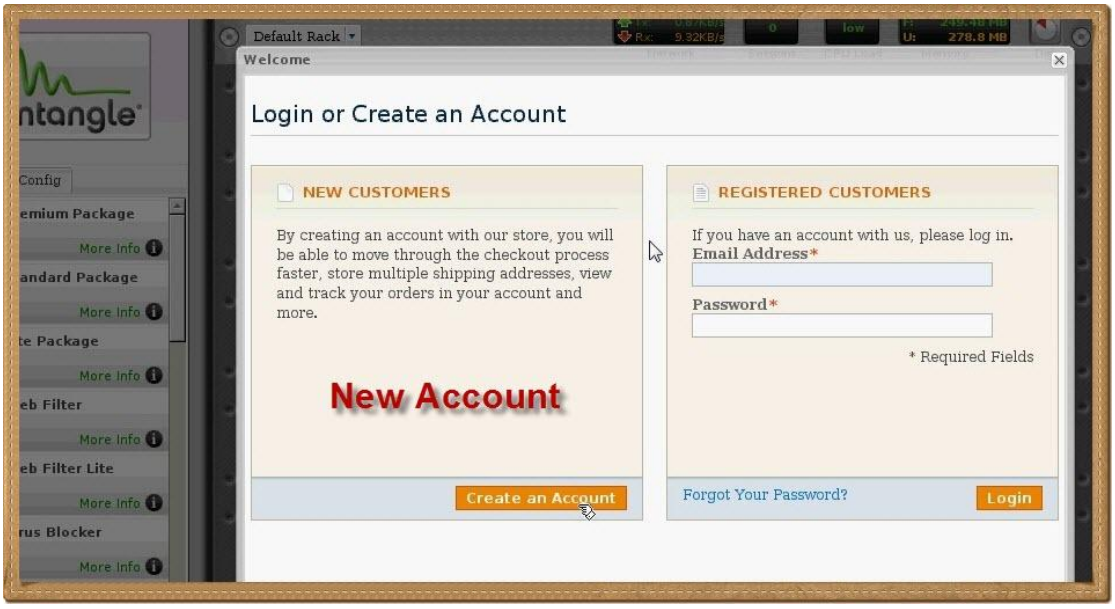
ونصبر شويه



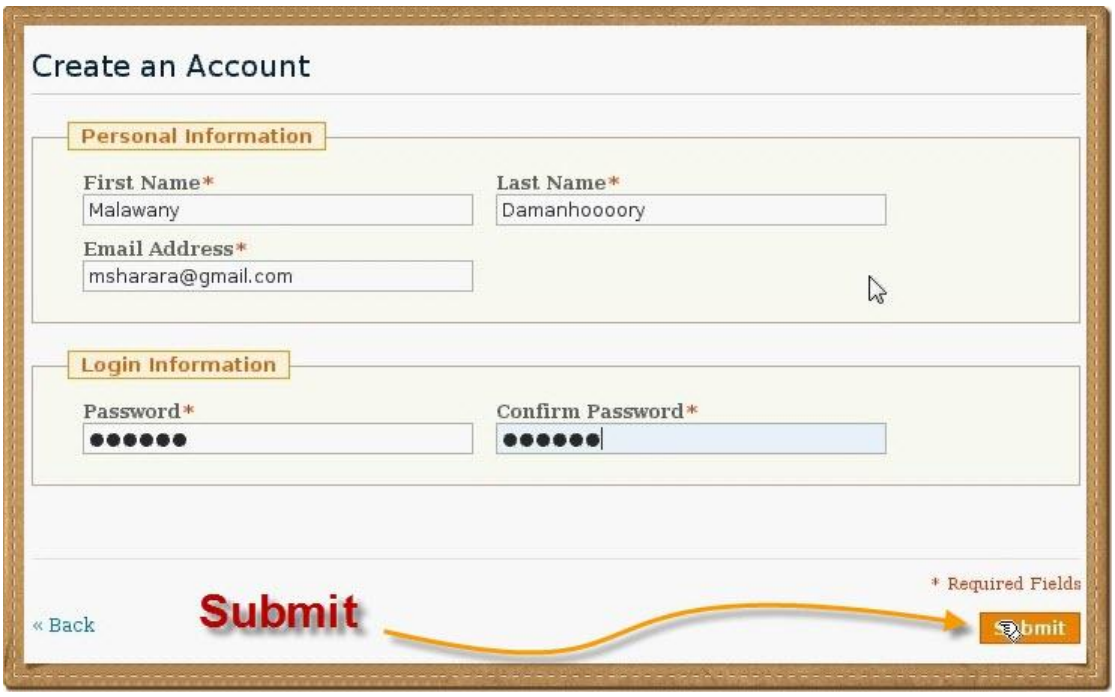
قلتلكم بطيء



يجب عليك عمل حساب على موقع Untangle , هذا الحساب الذي من خلاله ستحصل على الإضافات Apps سواء مجانية أو مدفوعة

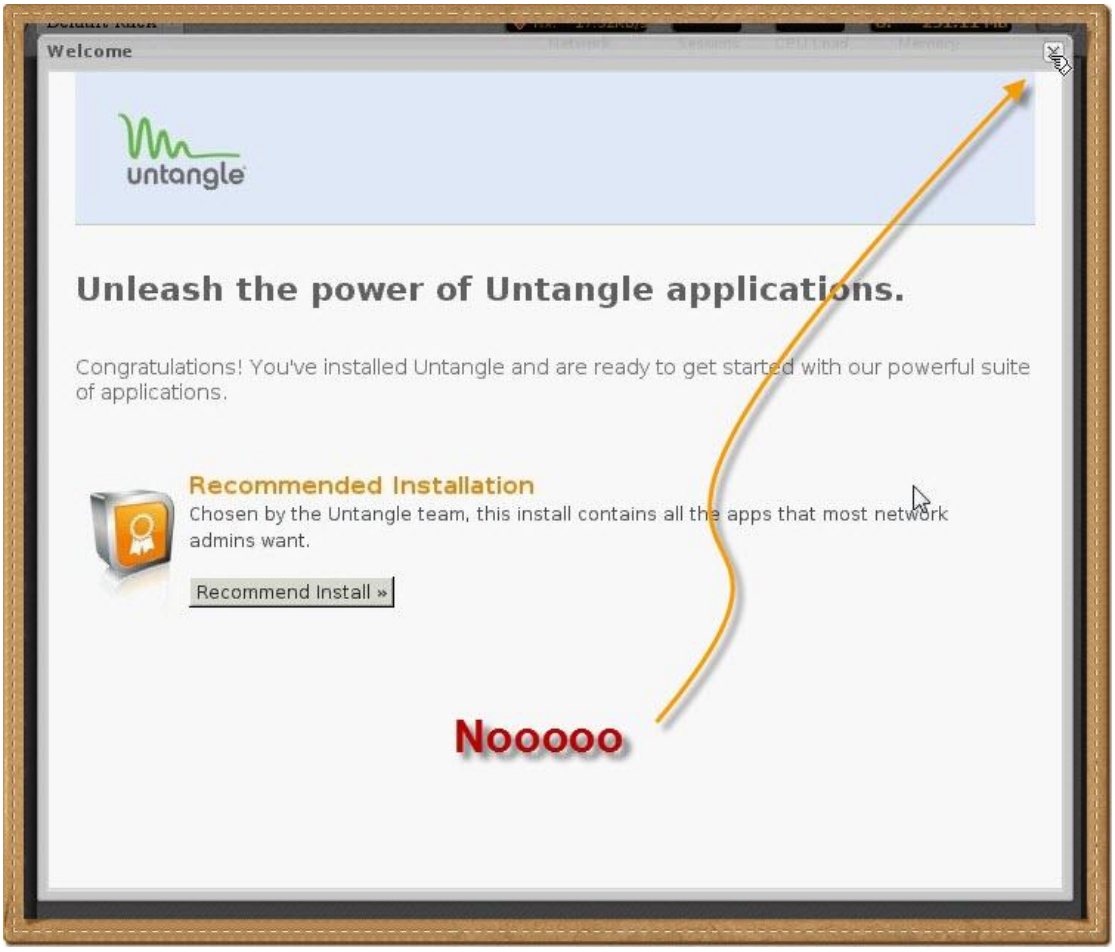


عملية التسجيل سهلة للغاية



وهنا الدخول بالحساب الجديد

لا تختار تنزيل حزمة البرامج هذه ,إخلع يامعلم



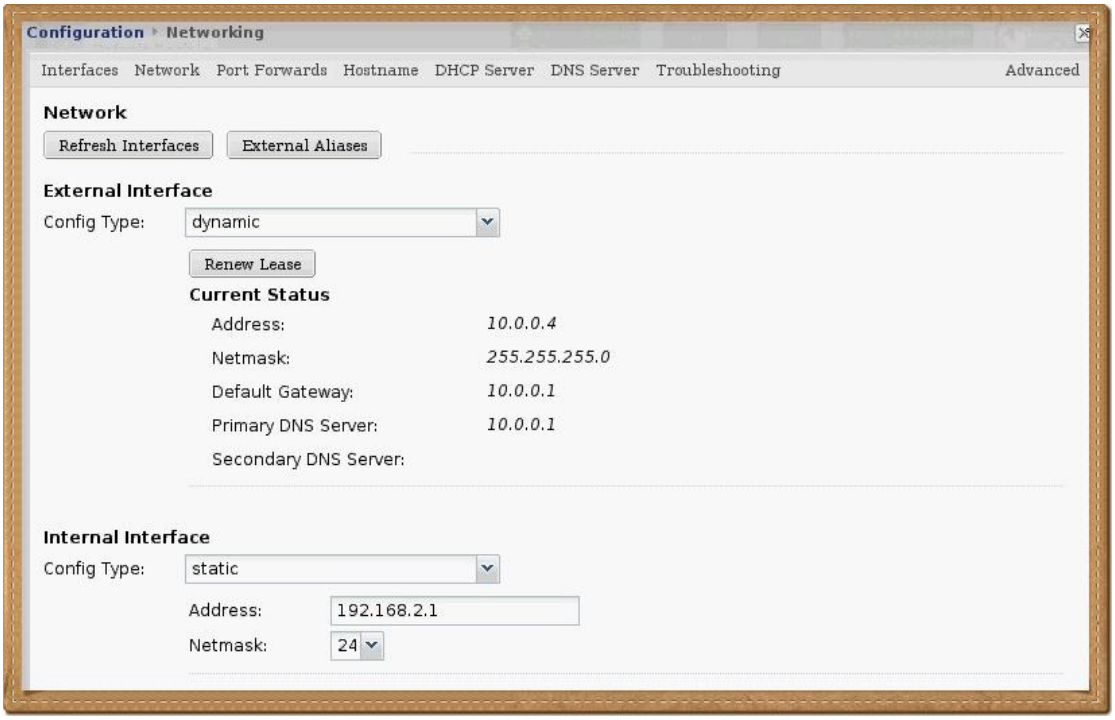
دي الواجهة الرئيسية من الأعلى ح تلاقي Monitor للـ Connection والترافيك والهارد والرامات

على اليسار يوجد تبويب Config لإعدادت الجهاز كإسم المستخدم واي بيهات الكروت

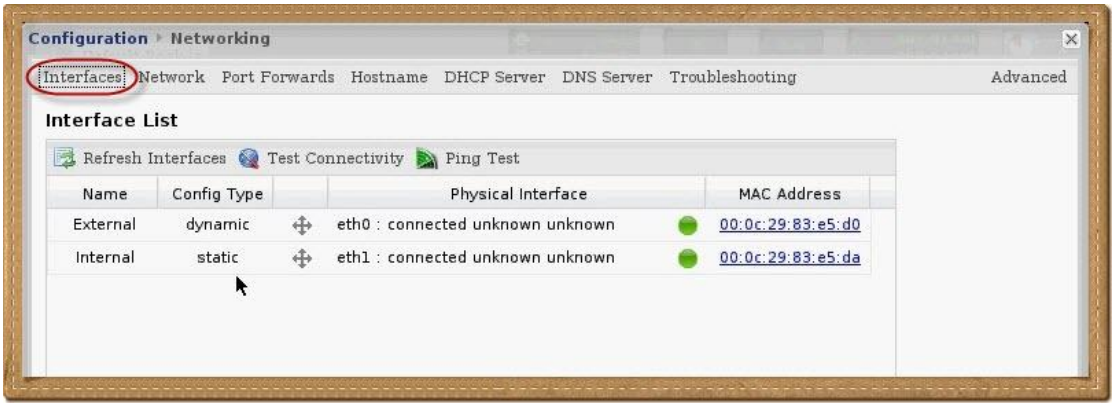
كما يوجد تبويب Apps ومنه ح ننزل الإضافات

نجرب من Config الدخول على Networking

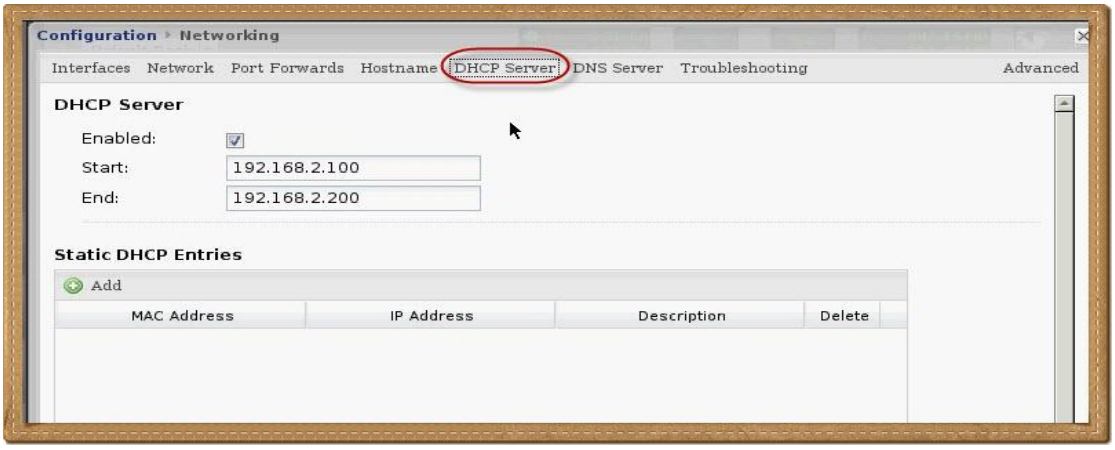
إعدادات سريعة



من تبويب Interfaces تغيير أنواع الكروت كما رأينا من قبل



وهنا إعداد الجهاز للعمل كـ DHCP Server

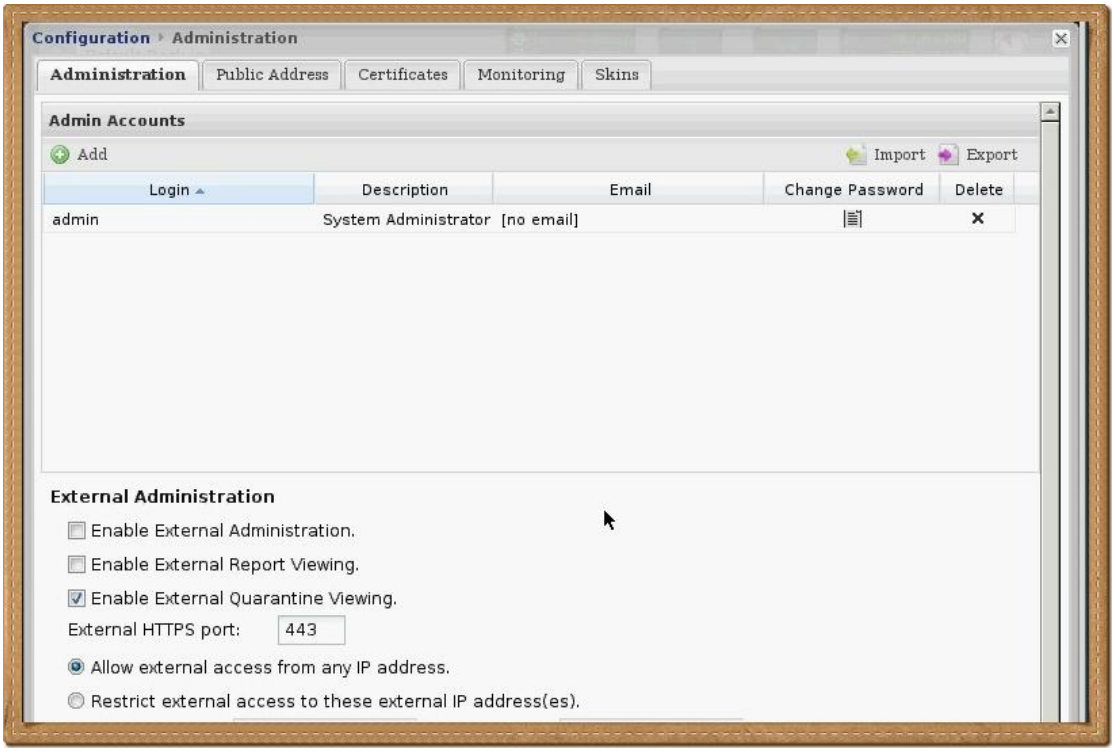


خيار Administration

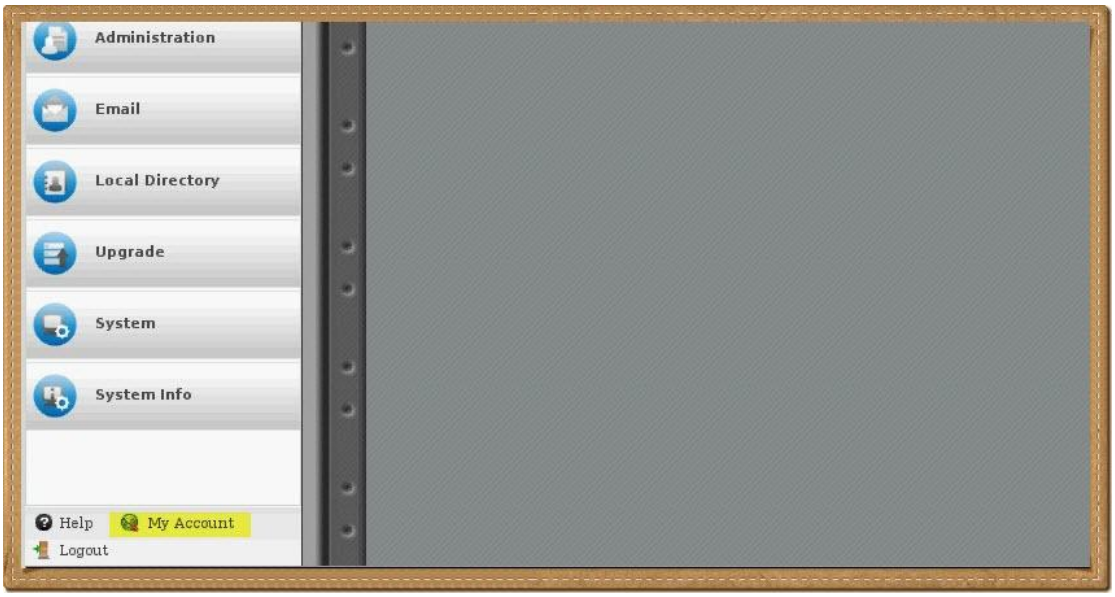
إضافة مستخدمين

وحركات

وكده



بالضغط على My Account نعدل إعدادات حسابنا على Untangle



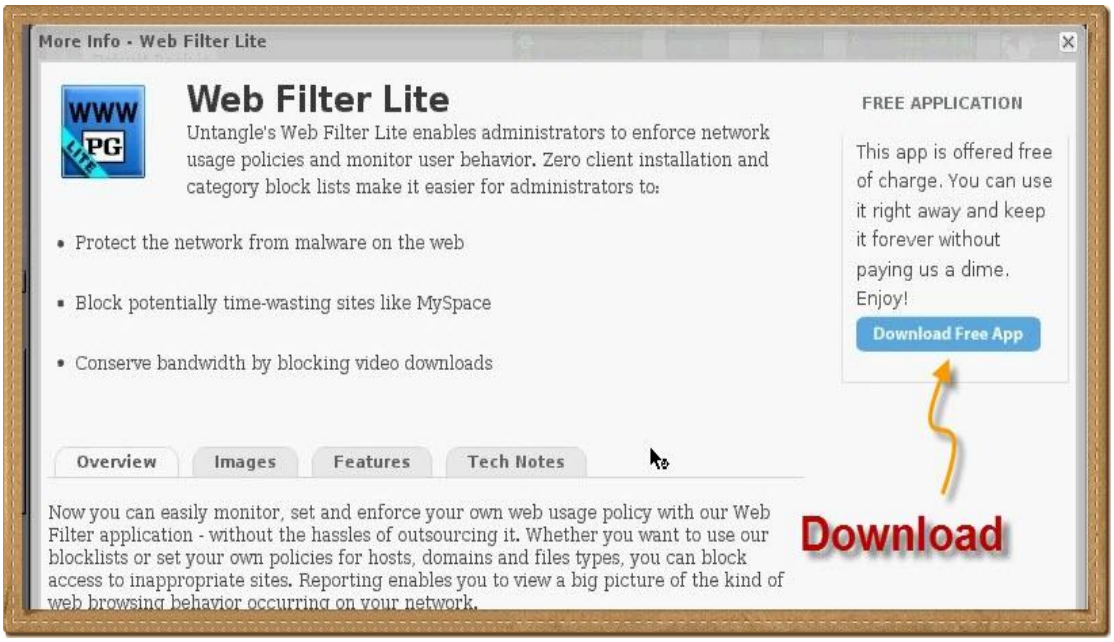
ندخل على تاب الـ Apps من هنا إختيار الإضافات فكما نرى السيرفر لايحتوي على أي شيء ندير الخدمة من خلاله

الـ Premium Package هي التي إقترحها علينا وقلت لك إخلع ياعم

غالبا إذا رأيت كلمة Lite فاعلم أن الإضافة مجانية ولكنها بالطبع محدودة الخصائص

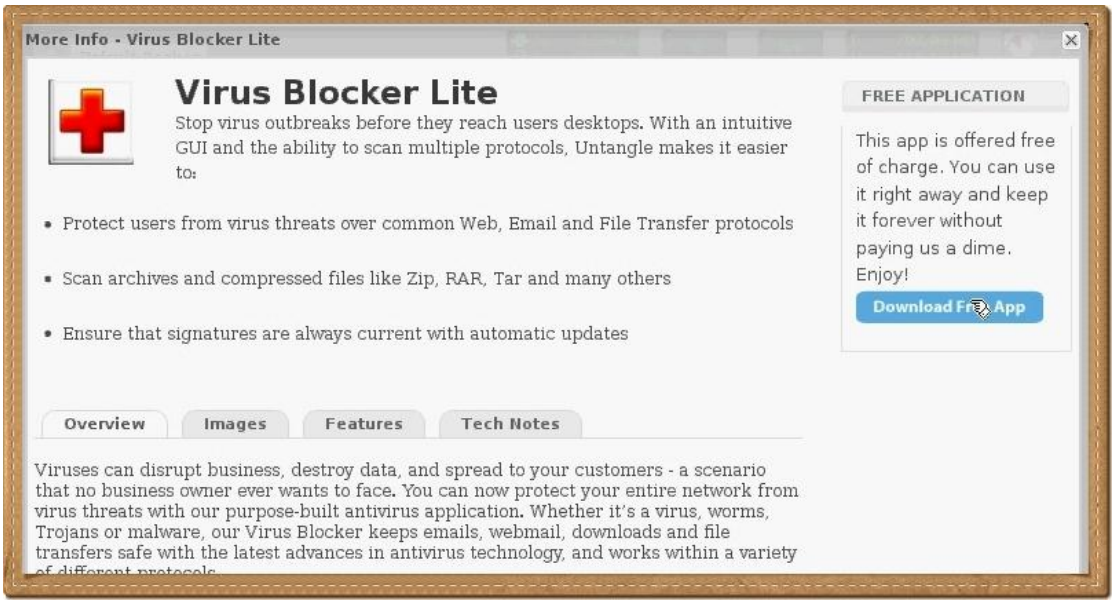
نختار مثلا Web Filter Lite

يفتح لنا صفحة خاصة لشرح الـ App وتنزيلها



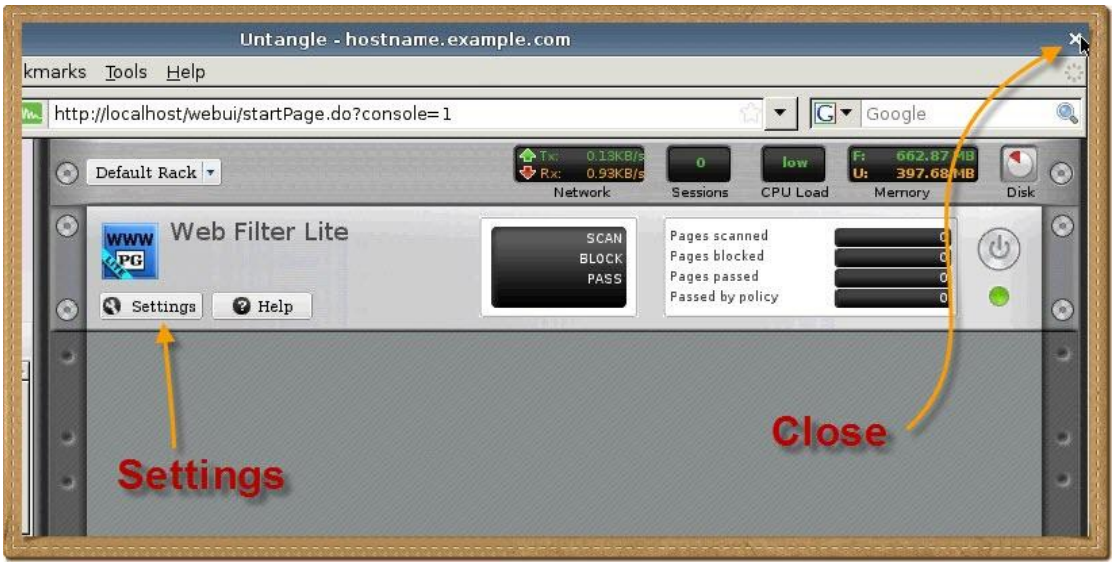
بدأت في النزول وسيتم تنزيلها بدون تدخل منا

وهنا إضافة للفايروسات



بعد إنتهاء الإضافة من التنزيل يمكننا الدخول على الـ Setting الخاصة بها والعمل كما تعودنا

عند إغلاق الصفحة الرئيسية نعود إلى شاشة سنراها كثيرا

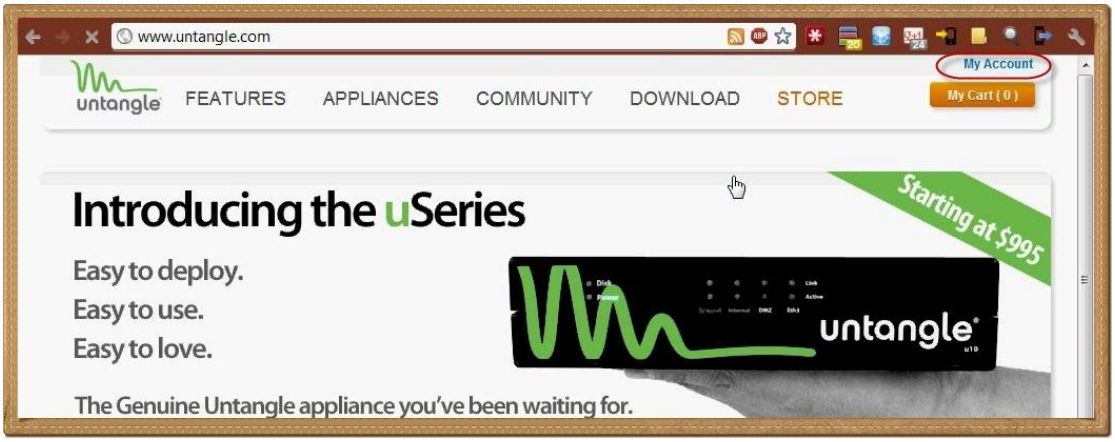


للعودة إلى شاشة التطبيقات وإدارة السيرفر نختار Launch Client وطبعا باقي الأزرار مفهومة ومش ح اشرحها

أخيرا قبل ترك السيرفر هذه شاشة الدخول

وطبعا نفرق بين يوزر نيم ندخل بيه على السيرفر وبين الحساب الخاص بموقع Untangle

موقع Untangle على الإنترنت

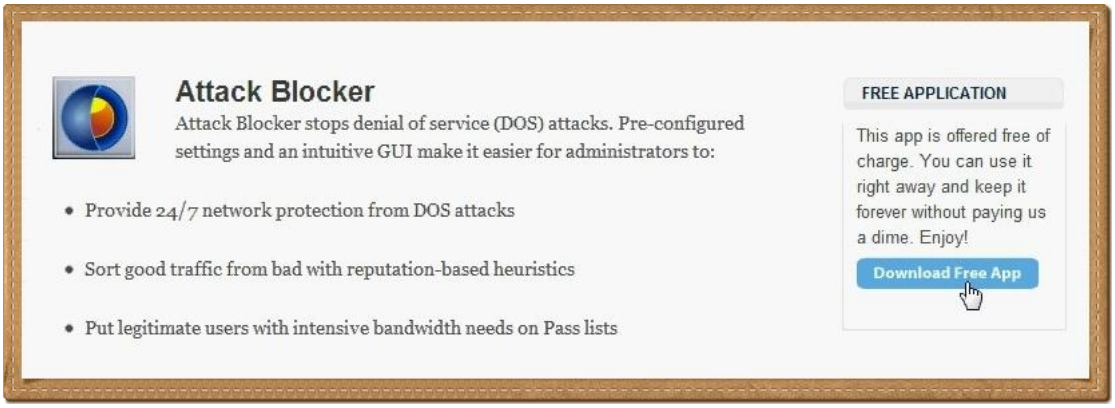


يمكنك دخوله بحسابك السابق إنشاؤه

ومنه بالدخول على رابط Store

تجد الـ Apps المجانية أو المدفوعة

بس كده



لاحظ أنني لم أعمل ريموتلي على هذا السيرفر فمن مميزاته القليلة أنه يمتلك واجهة GUI

أتمنى بنهاية هذا الفصل ألا يقف أمامكم أي عقبة في التعامل مع أي جهاز أو برنامج يتعامل مع وظائف :

- Gateway
- Proxy
- Firewall
- UTM

اللهم إجعلني خيراً مما يظنون واغفر لي مالا يعلمون

اللهم إني أعوذ بك أن أشرك بك شيء أعلمه وأستغفرك لما لا أعلمه

سبحانك اللهم وبحمدك , أشهد ألا إله إلا أنت , أستغفرك وأتوب اليك

الفصل الثامن : السرية التاااامة

Open DNS

Tor Project

Pidgin

السرية التاااامة

Open DNS

الحمد لله والصلاة والسلام على رسول الله

سيدنا محمد , وعلى آله وصحبه ومن والاه

أفضل دائما إستخدام Google DNS , فهذه الخدمة أفضل بلا شك من إستخدام الأرقام الخاصة بمزود الخدمة وذلك لأسباب عديدة منها :

- ثبات مستوى الخدمة
- السرعة الملحوظة في تلبية الطلبات

جوجول ليست الوحيدة التي تقدم خدمة Public DNS أو Cloud DNS فشركات عدة تقدمها ومنها شركة Amazon ولكنها تقدمها بإشتراك سنوي

يوجد أيضا العديد من المواقع تقدم هذه الخدمة بخواص رائعة منها إتاحة الفرصة للعميل لتخصيص الخدمة فيمكنك حجب المواقع الإباحية أو مواقع العنف و الجريمة أو حتى أي موقع تريد عن طريق هذه الخدمه

فعلى سبيل المثال يوجد على الإنترنت إعلانات تتحدث عن حجب المواقع الإباحية من خلال الإنترنت بدون برامج عن طريق رقم DNS محدد

أشهر موقعين لخدمة الـ Cloud DNS هما : OpenDNS – DynDNS

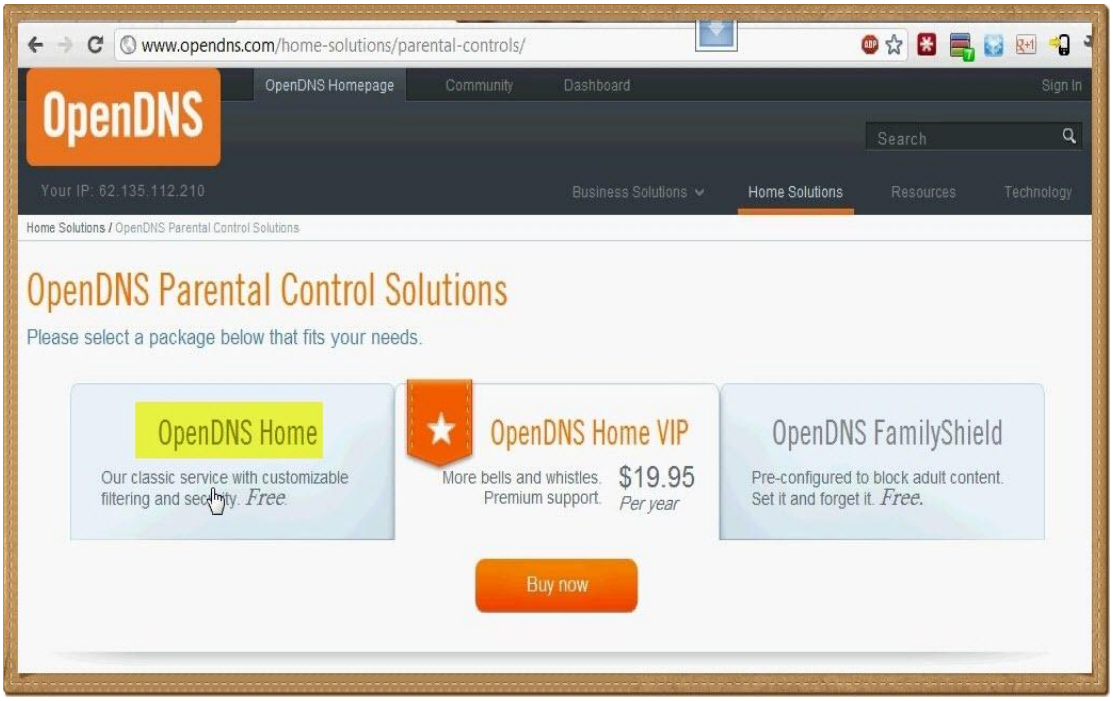
قد يكون الموضوع به قدر من الغموض وبمشيئة الله سيتلاشى هذا الغموض في الصفحات التالية

نفتح الموقع يوجد أكثر من باقة مدفوعة ولكن خلينا في أبو بلاش

نختار For Home

Parental Control

ثم OpenDNS Home



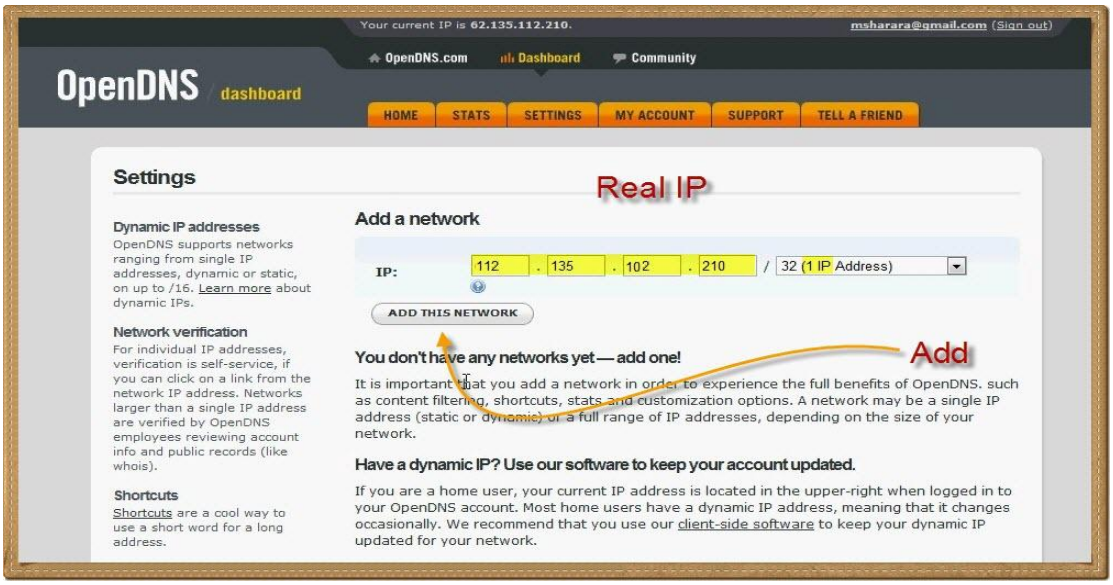
و Sign Up Now للتسجيل في الخدمة

طبعا عمل registration مش محتاج شرح

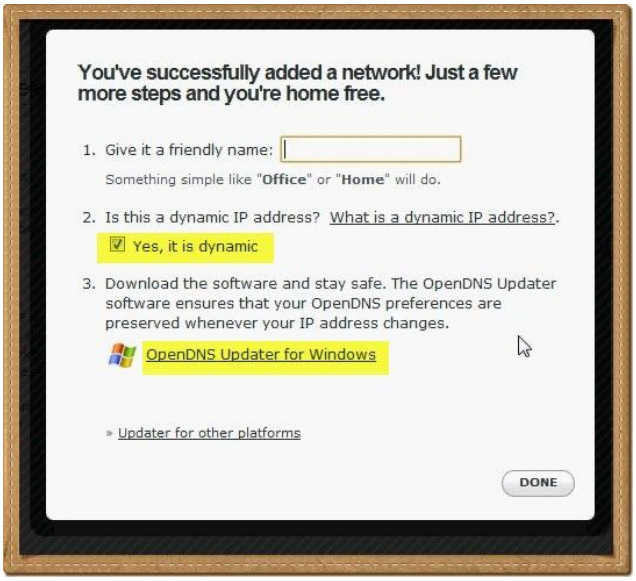
نتوكل على الله ونعمل Login

من هنا إضافة الـ IP الخاص بنا كشبكة خاصة تابعة لإشتراكنا وهنا أمامنا حالتين :

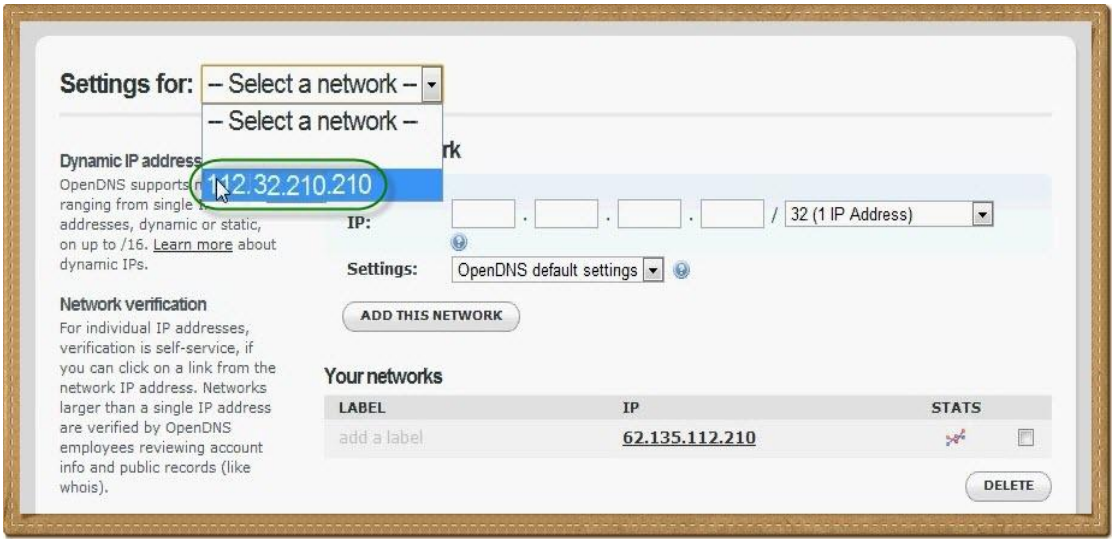
- أن يكون دخولنا على الإنترنت بـ Real IP نحصل عليه من مزود الخدمة وساعتها سنضيف الرقم كما هو موضح
- أن يكون دخولنا الإنترنت بـ Dynamic IP كحال أغلبنا حيث يتغير اي بي الجهاز كلما إتصلنا بالإنترنت هنا يجب علينا تنزيل برنامج اسمه OpenDNS Updater من الموقع مهمته ربط حساب المستخدم بالإنترنت مهما تغير رقم الـ IP



يمكننا تسمية الشبكة وتحديد نوعية الـ IP كونه Dynamic أو Real

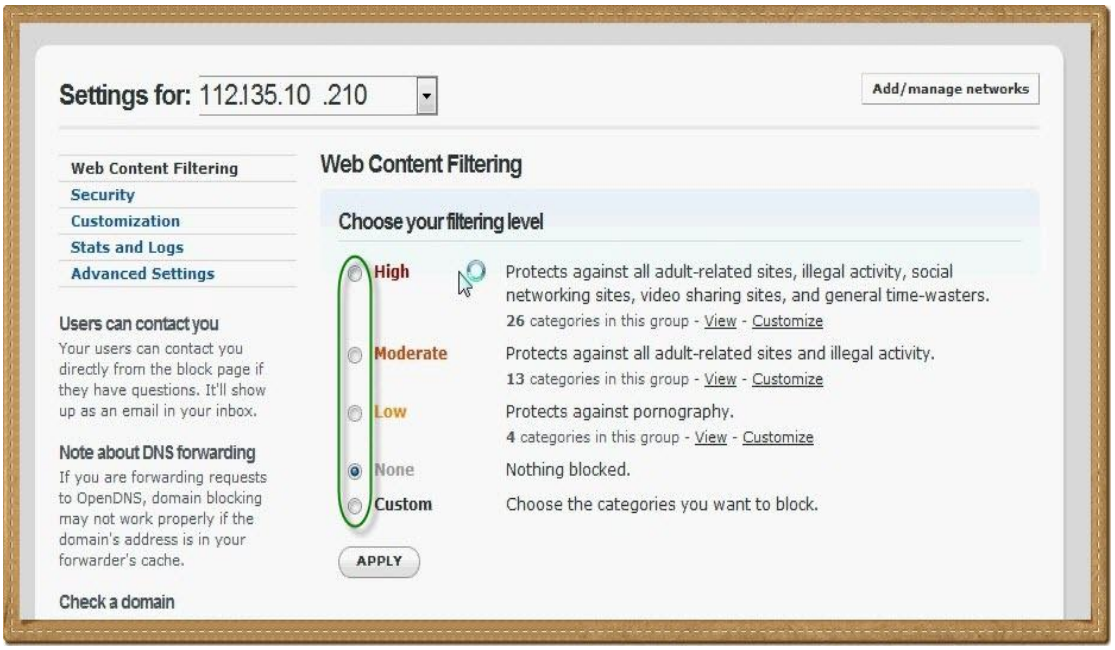


بعد إضافة الـ اي بي يمكننا تخصيص الفلاتر الخاصة به

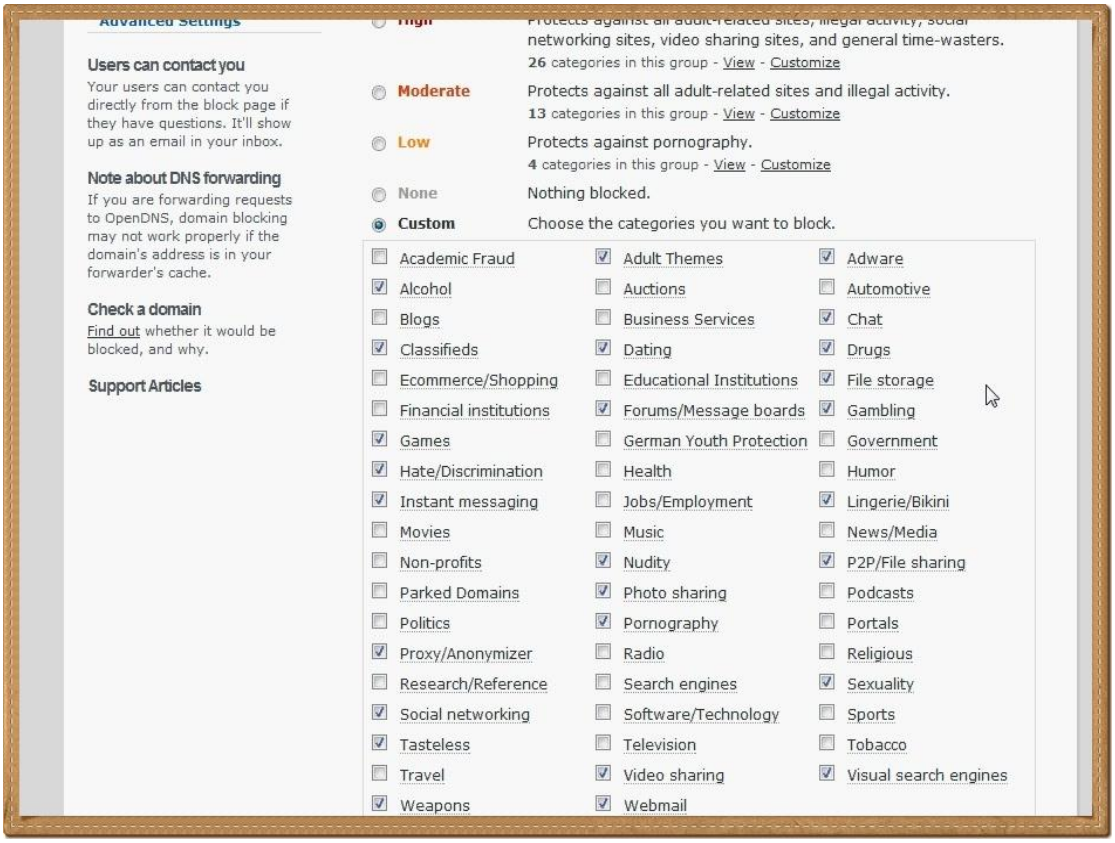


نختار بين أكثر من مستوى للـ Web Filter

طبعا أكثرهم تشددا High وأقلهم None



بالضغط على Custom يمكننا تخصيص نوعية المواقع الممنوعة



كما يمكننا أيضا منع Block موقع محدد أو إتاحته دائما Never Blockبغض النظر عن محتواه

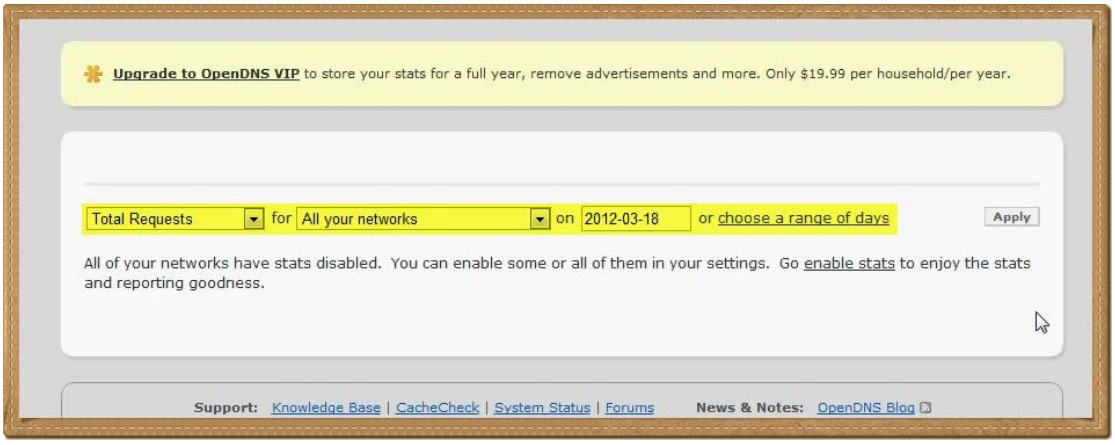
هنا سيتم السماح لموقع shararasky.com دائما

بالضغط على Delete لإلغاء الرول

كما يمكننا أيضا منع موقع نهائيا Sharara.org

دي أخرتها تقفلوا موقعي

من State نقدر نشوف اللوج



طبعا الباقات المدفوعة إمكانياتها وخصائصها أكثر بكثير للدرجة التي يمكنك الإعتماد عليها في عمل رولز كامله تتحكم فيما يسمح للمستخدم بزيارته من مواقع

قد تكون الفكرة غير واضحة تماما للبعض ولكن أحاول توضيحها : بدلاًمن فلترة المواقع عن طريق البروكسي سيرفر ستتيح للمستخدم الوصول إلى الإنترنت ومن ثم سيتم توجيه كل الترافيك ليكون من خلال الـ DNS الخاص بإشتراكك في موقع OpenDNS وبالتالي يتحكم الموقع فيما سيتم تنفيذه من طلبات معتمداً على ما أعددته كفلتر

اللهم إجعلني خيراً مما يظنون واغفر لي مالا يعلمون

اللهم إني أعوذ بك أن أشرك بك شيء أعلمه وأستغفرك لما لا أعلمه

سبحانك اللهم وبحمدك , أشهد ألا إله إلا أنت , أستغفرك وأتوب اليك

السرية التاااامة

Tor Project

الحمد لله والصلاة والسلام على رسول الله

سيدنا محمد النبي, وأزواجه وذريته وأهل بيته

بإختصار مافيش حد مابيتراقبش على الإنترنت

إن شاء الله سأتحدث يوما ما عن بعض التفاصيل حول من يراقبنا وكيف يراقبنا

بصفة عامة فالمراقبة أو التجسس تبدأ من الراجل اللي إنت واخد منه وصله لغاية المخابرات الأمريكية

لا يوجد حل نهائي أو آمن يمنع التجسس عليك أو مراقبتك نهائيا ولكن يوجد حلول تصعبها وتجعل مراقبتك أمراً صعبا وليس مستحيلاً

من ضمن الحلول هو دخول الإنترنت من خلال بروكسي

- طيب ماهو كل اللي شرحناه كان بروكسي ؟

أقصد بروكسي خارجي تدخل عليه وهو يحولك على المواقع اللي إنت عايزها وكده أغلب اللي بيحاولوا يراقبوك أو يمنعوك مش ح يعرفوا إنت رايح فين

يضاف مع البروكسي التشفير وإستخدام متصفح آمن

أقوى حل من وجهة نظري هو مشروع تور Tor Project وهو مشروع غربي غير حكومي ح نشرحه في هذا الفصل

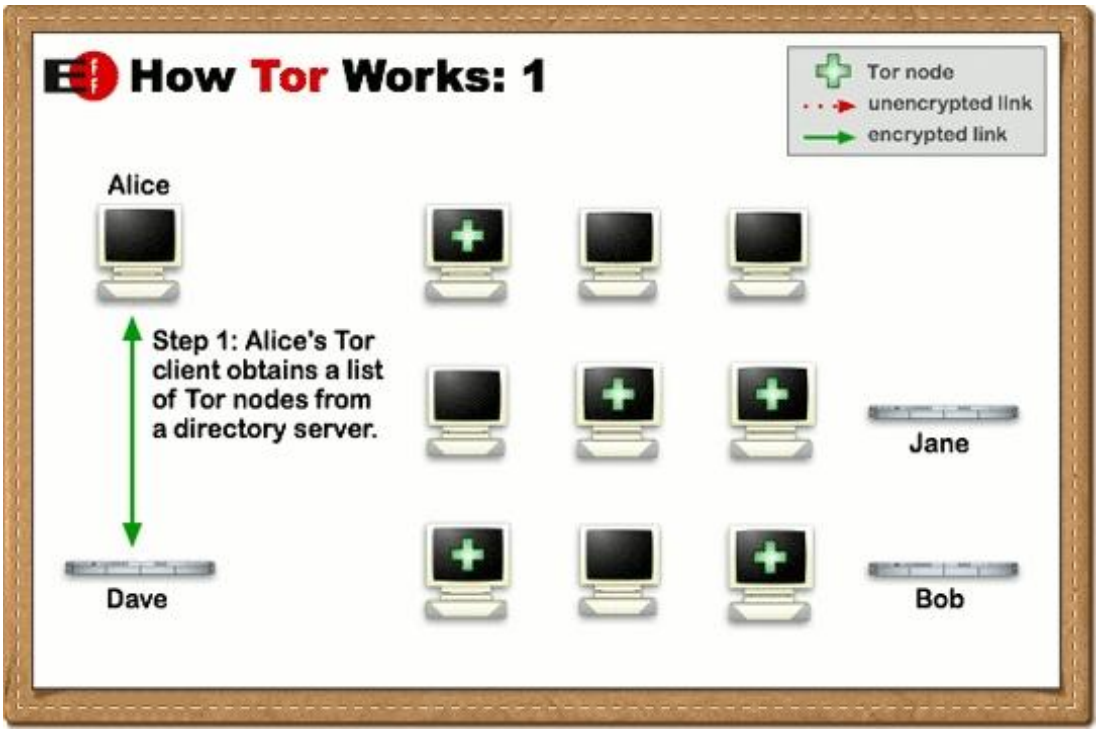
وبغض النظر عن تخصصك أو نشاط شركتك فأعتقد إنك لازم يكون عندك حل مثل هذا لتطبيقه فلا حدود للتجسس وهو ليس مقصورا على الجهات الأمنية بل قد يتجسس عليك المنافسون وهو مايسمى : التجسس الصناعي

كما أنك ستحتاجه أيضا حفاظا على كلمات السر الهامة فأعتقد إنك ليس مستعداً لتكون كلماتك السرية كأدمين لإيميل شركتك مخزنة عند مزود الخدمة ☺ أنا ماليش دعوه وماقلتش حاجه

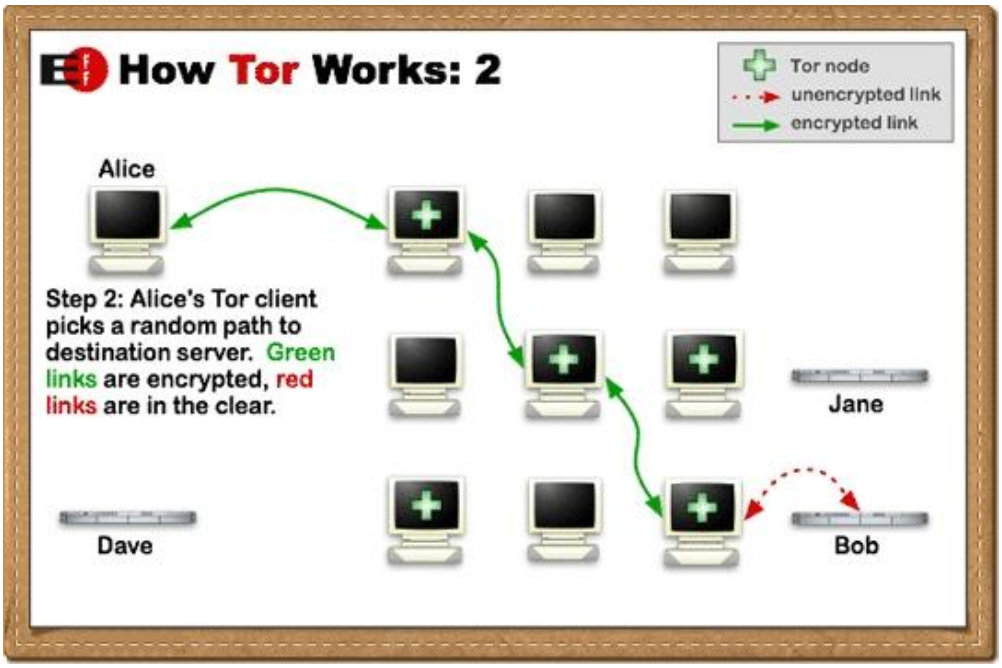
كما ذكرنا فإن مشروع تور هو مشروع غير حكومي تحرري تدعمه عدة جهات

تعالوا نتخيل معا السيناريو الحالي من موقع torproject.com وهو خاص بمستخدم إسمه Alice يستعمل Tor ويريد الدخول أو إجراء محادثة مع Bob و jane

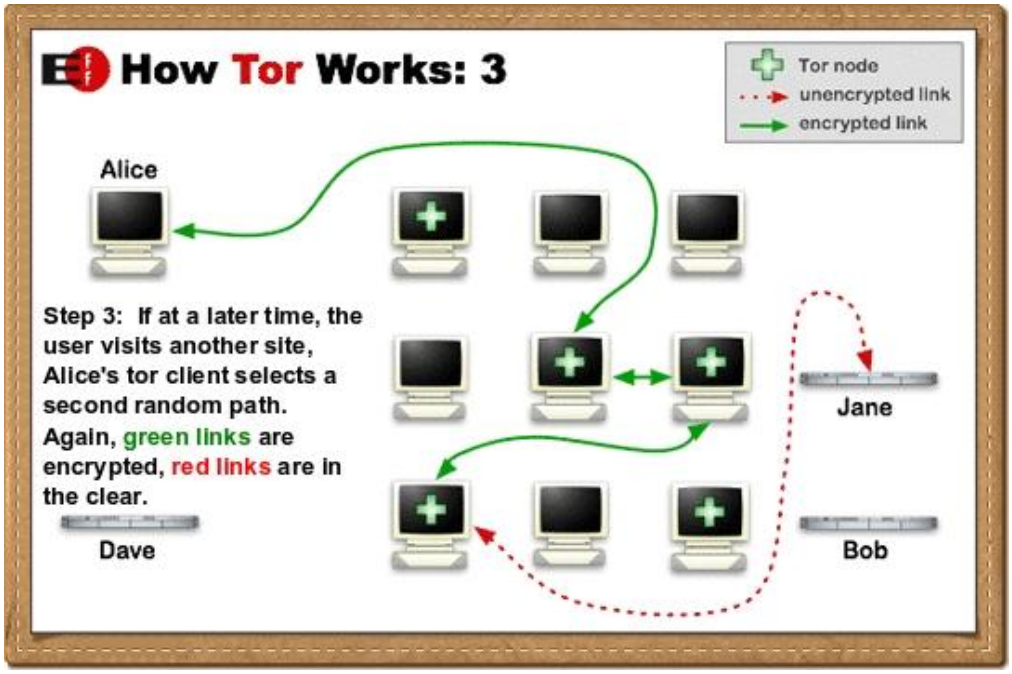
يطلب تور من أحد الوكلاء Dave وهو بمثابة Directory Server أن يمده قائمة بالأجهزة التي يمكن المرور من خلالها



يبدأ جهاز Alice المرور بمسارات عشوائية مشفرة من خلال أجهزة Tor المنتشرة في أنحاء العالم حتى يصل إلى Bob ونلاحظ هنا أن إتصال Bob غير مشفر إلا لو إستخدم هو أيضا Tor ولكن رغم عدم التشفير فإن تنقل الباكيت عبر أكثر من مسار سيصعب جدا عملية التتبع ومن ثم محاولة فك التشفير



عند إتصال Alice بـ Jane يأخذ مسارا آخر مختلف وهكذا



بالمناسبة الشعار الموجود بأعلى يسار الصور السابقة هو شعار منظمة

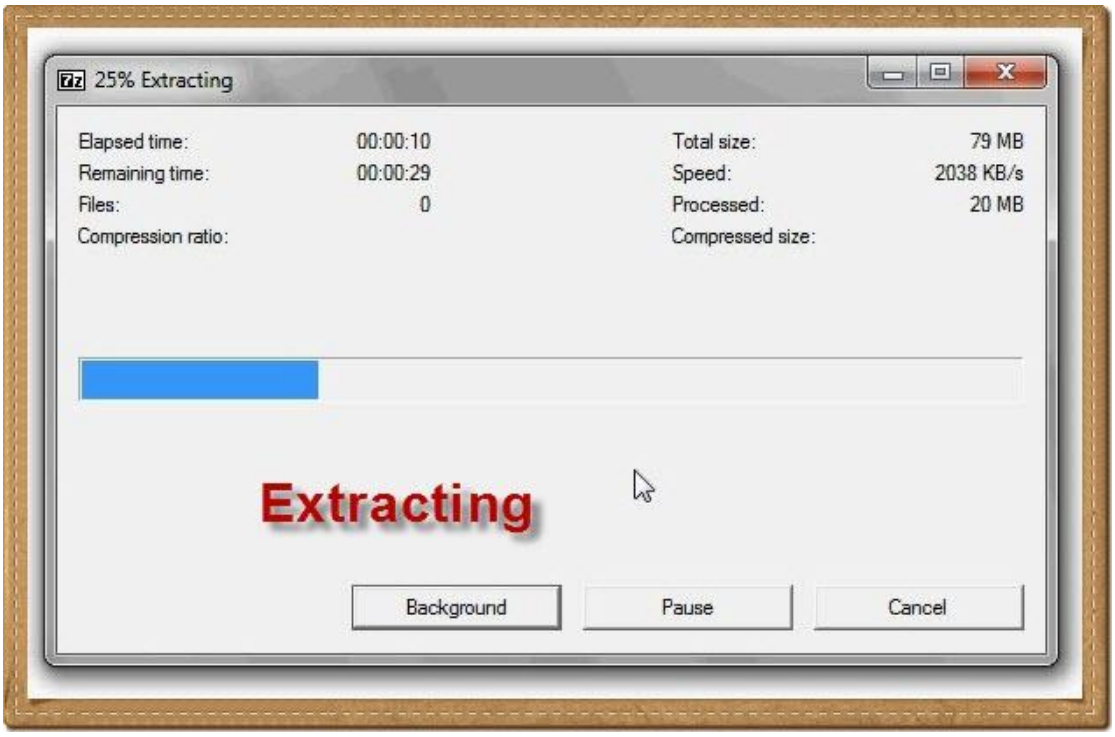
Electronic Frontier Foundation (EFF)

وهي منظمة معنيه بالدفاع عن حرية الإنترنت والحركات وكده وموقعها eff.org

ماعلينا ندخل في العملي , من موقع تور ننزل حزمة Tor Browser Bundle

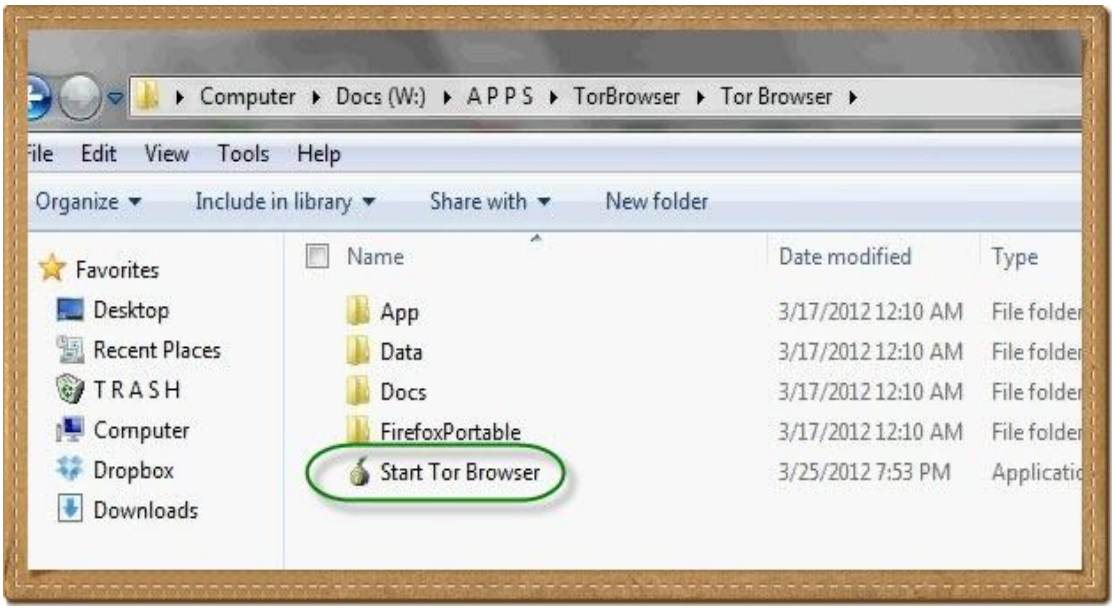
ثم Double Click

الحزمة بورتابل , نختار مكان فك الملفات ويمكننا بالطبع فكها على الفلاش ميموري



نفتح مجلد البرنامج

نضغط على Start Tor Browser

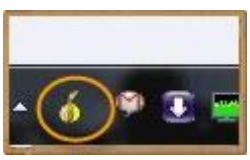


الزتونه بتاعة تور هو برنامج Vidalia

وهو أول حاجه ح تتفتح وسيبدأ في فتح إتصال

ماتلعبش في حاجة

البصلة صفراء

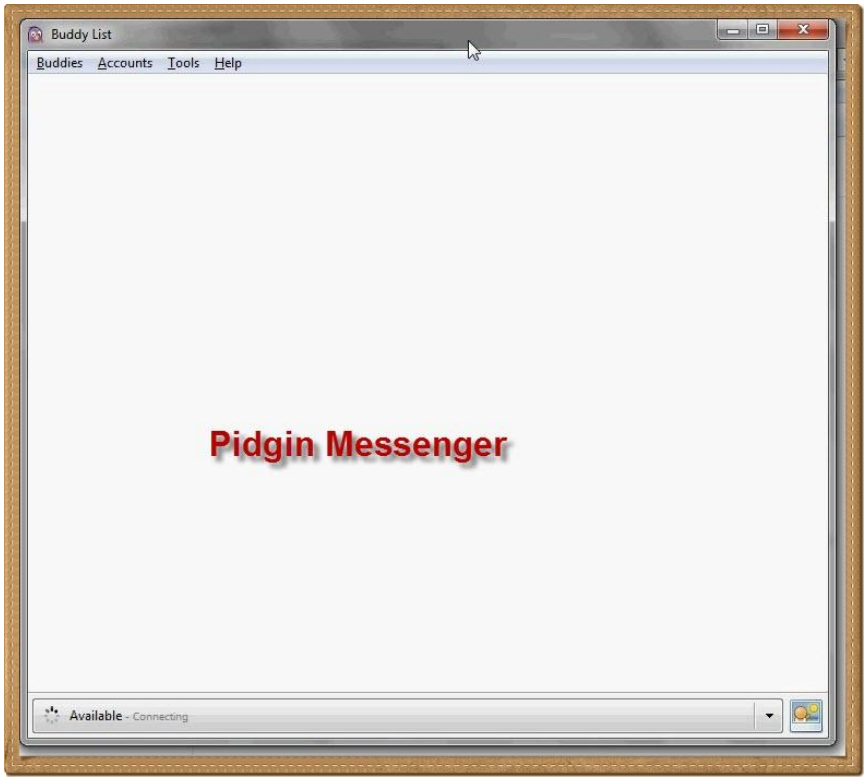


لما تتحول لخضراء يبقى طريقك أخضر

Connected

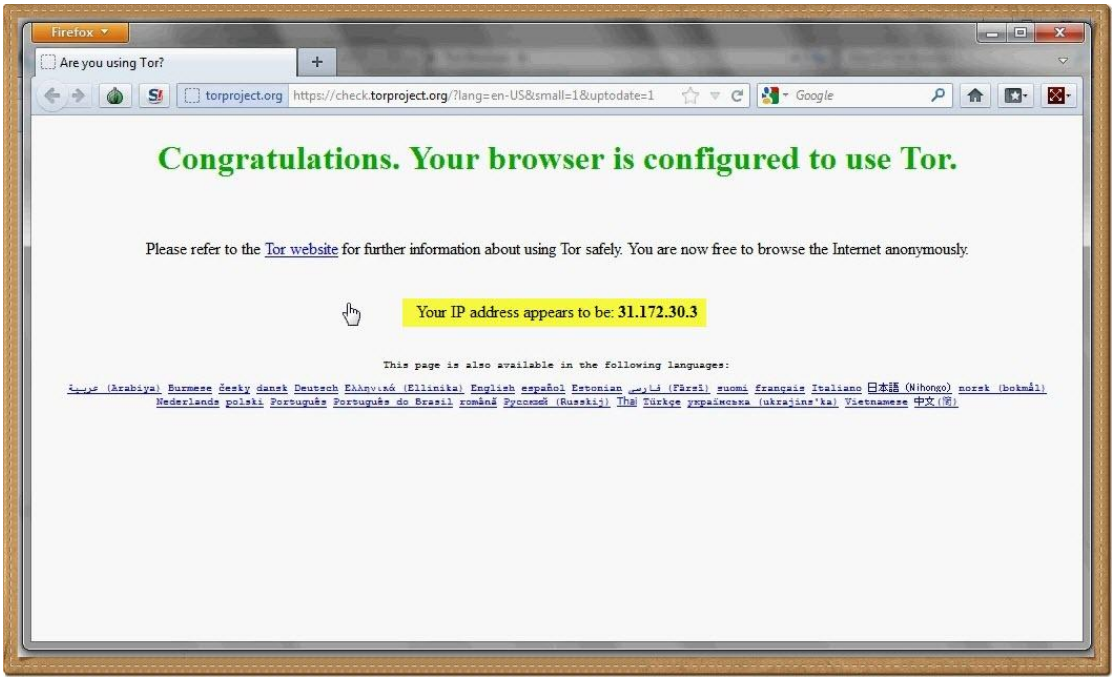
سيفتح تلقائيا ماسنجر Pidgin وهو ما سنشرحه تفصيليا في الفصل القادم

ممكن تقفله

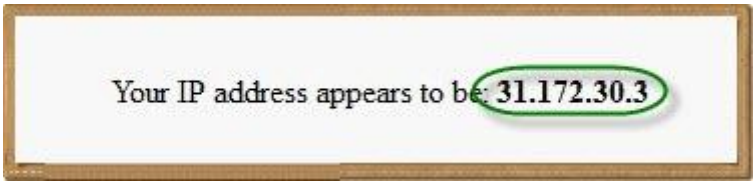


ونسخة من Firefox وهي التي سنتصفح الإنترنت من خلالها

لاحظ أن صفحة البداية تخبرك بأنك نجحت في الإتصال من خلال Tor



الـ اي بي الخاص بك سيظهر أنك من هامبورج بألمانيا ولكن ماتفرحش قوي لإنه بيتعرف إنه خاص بـ Tor



نسخة المتصفح تستخدم ثلاثة إضافات وهي :

- HTTPS Everywhere
- NoScript
- TorButton

أول وثاني إضافة ممكن نضيفهم على أي نسخة فايرفوكس لكن الإضافة الخاصة بتور وهي أهم مافي الموضوع توقفت عن دعم أي نسخه لفايرفوكس كما أنها لاتدعم الـ Chrome حتى الآن وبالبلدي كده لازم تستخدم النسخة الموجوده ضمن الـ Tor Bundle

لو حبينا نلعب شوية نذهب من أي متصفح عادي إلى أي موقع لكشف الـ اي بي

الأفضل أن نستخدم Check.torproject.org سيظهر الـ اي بي الحقيقي

زي ماقلنا الزتونه هي Vidalia ماتحاولش تلعب فيها في الأول

وأخيرا الإغلاق

نصيحة أخيرة : لا تكتفي بـ Tor في التصفح , خليك ذكي وإستعمل متصفح عادي جدا وادخل من غير بروكسي على المواقع العادية وبالتوازي خصص Tor للمواقع الهامة

مثلا لو رئيس مجلس إدارة شركة والمنافس عايز يراقبه ح يثيره ويثير ريبته أن يكون كل الترافيك الخارج من جهازه مشفر وإلى بروكسي علشان كده لما يستخدم متصفح عادي ومعاه تور ساعتها ممكن جدا اللي بيراقبه مايأخدش باله ... بجد مش هزار

لو قلتلكم إن تور بدأ كمشروع تابع للبحرية الأمريكيه ياترى ح تزعلوا ؟؟؟

اللهم إجعلني خيراً مما يظنون واغفر لي مالا يعلمون

اللهم إني أعوذ بك أن أشرك بك شيء أعلمه وأستغفرك لما لا أعلمه

سبحانك اللهم وبحمدك , أشهد ألا إله إلا أنت , أستغفرك وأتوب اليك

السرية التاااامة

Pidgin

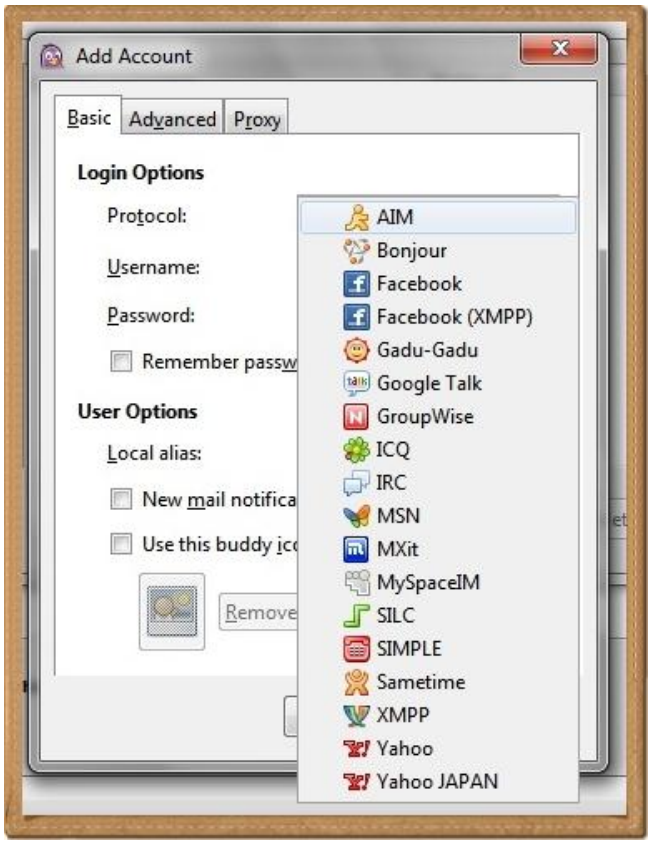
الحمد لله والصلاة والسلام على رسول الله

سيدنا محمد النبي, وأزواجه وذريته وأهل بيته

مش لدرجة إننا نشرح ماسنجر بصراحه تبقى عيبه ,حتى لو كان ماسنجر هايل و بأستخدمه بإستمرار

لكن ح نشرح ميزة هامة جدا في الماسنجر ده ويتميز بيها وهي التشفير

الماسنجر هو Pidgin وهو بيدعم كل البروتوكولات اللي تتخيلها



ده بالإضافة إلى إمكانية إضافة بروتوكولات أخرى عن طريق تنزيل إضافات للماسنجر

أيوه .... هو كمان ليه إضافات ومنها إضافة مهمة إسمها OTR إختصاراً لـ Off The Record

ننزل الماسنجر والإضافة ونبدأ التنصيب أولا لـ Pidgin Messenger

يفضل أن نعمل على نسخة الـ Offline Installation

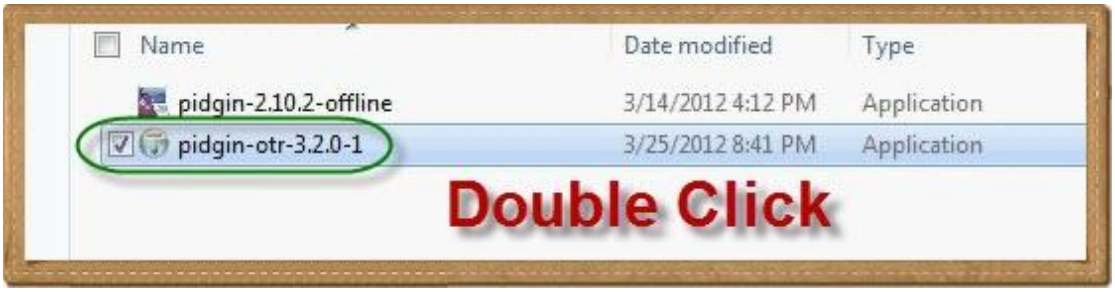
دابل كليك على Pidgin

و Ok

وطقم نكستات

و Finish

ثم دابل كليك على ملف الإضافة

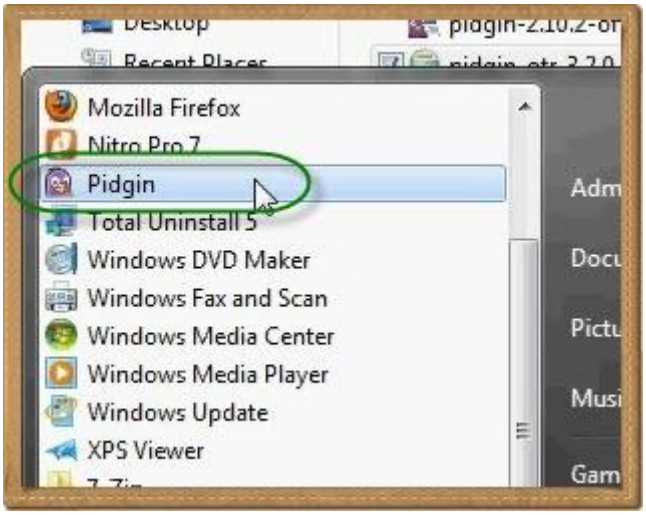


المعالج الجميل الظريف

طبعا Next و Next وكده

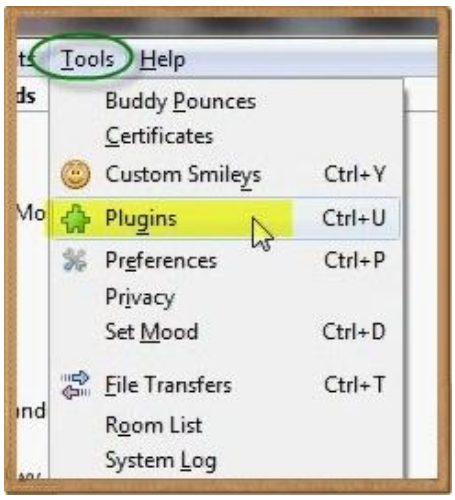
و Finish

نفتح البرنامج

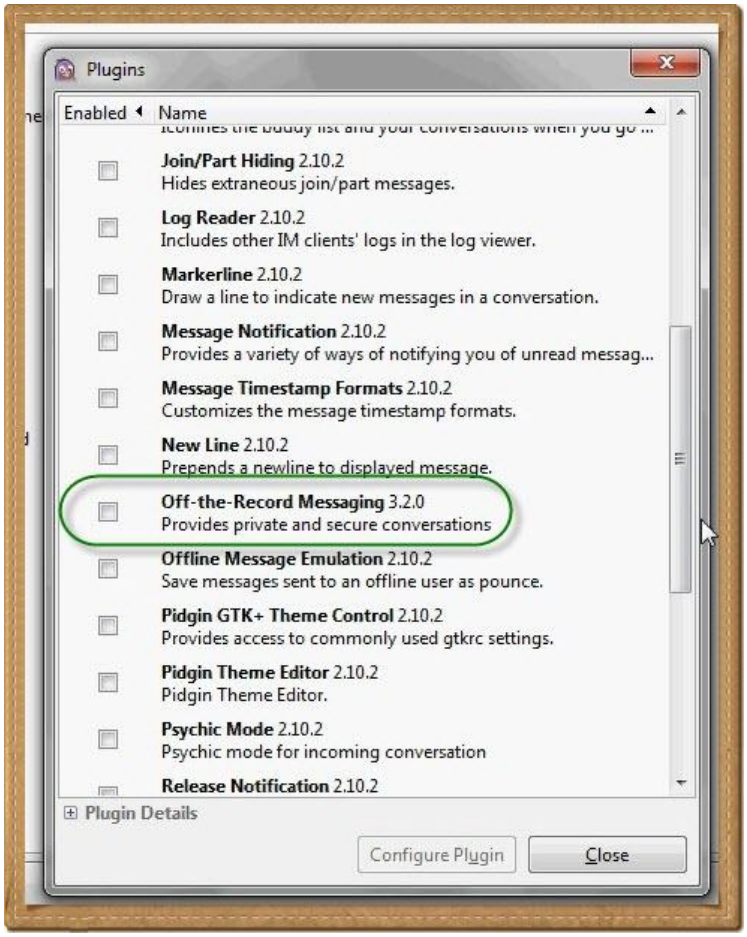


إضافة الحسابات سهل ولن نتحدث عنه وإذا قابلتك عقبات فعند جوجول الحل الأكيد

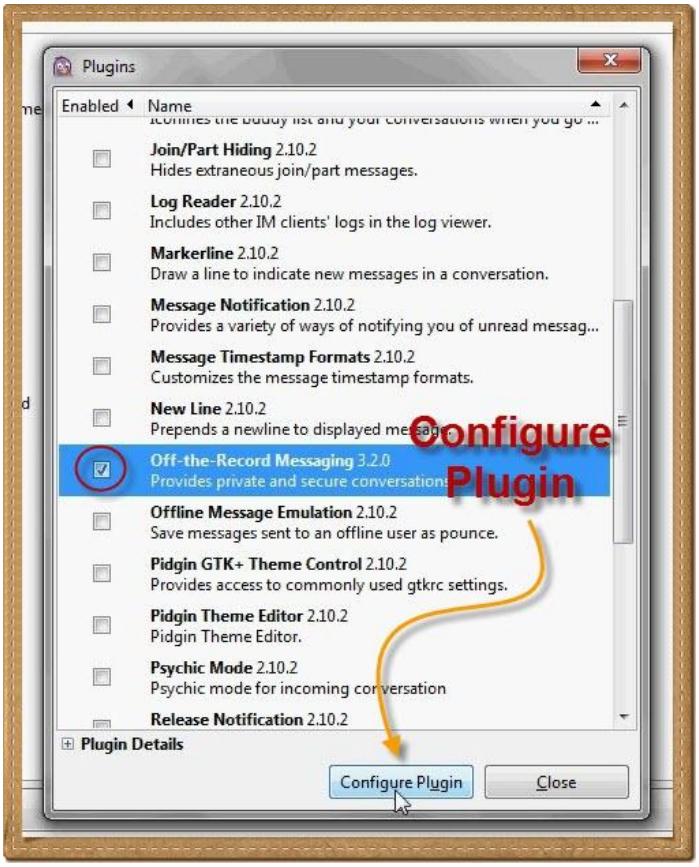
من Tools **نختار** Plugins



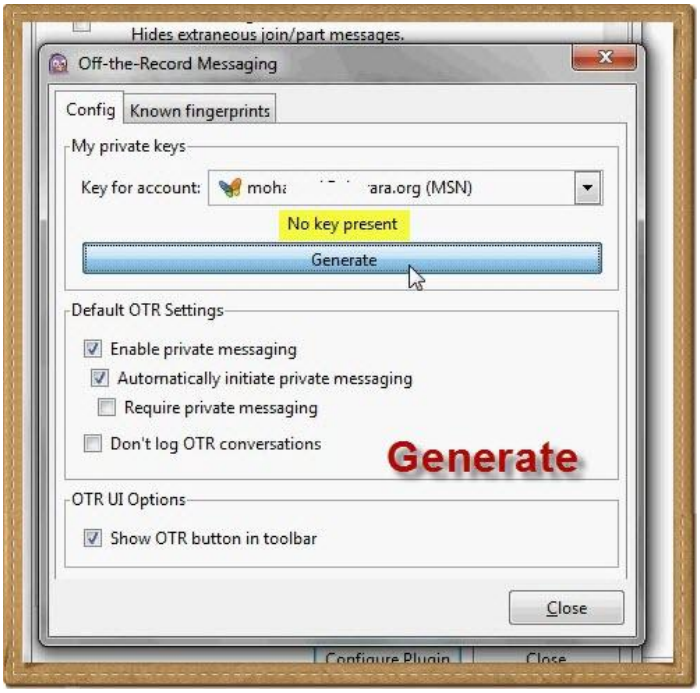
نختار Off The Record



ثم Configure Plugin

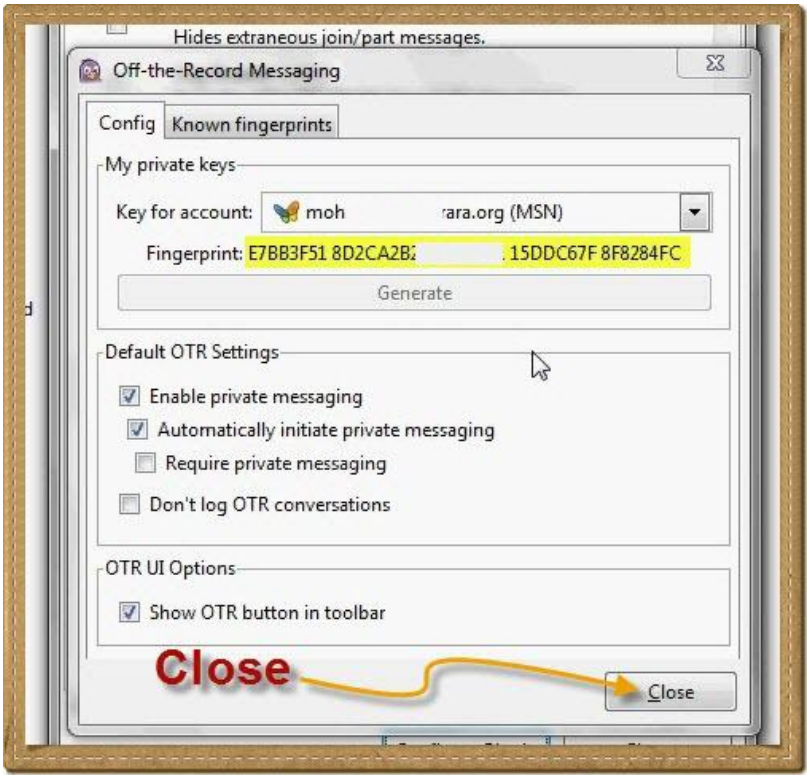


نختار الحساب الذي سنستخدمه في المحادثات المشفرة ونضغط Generate

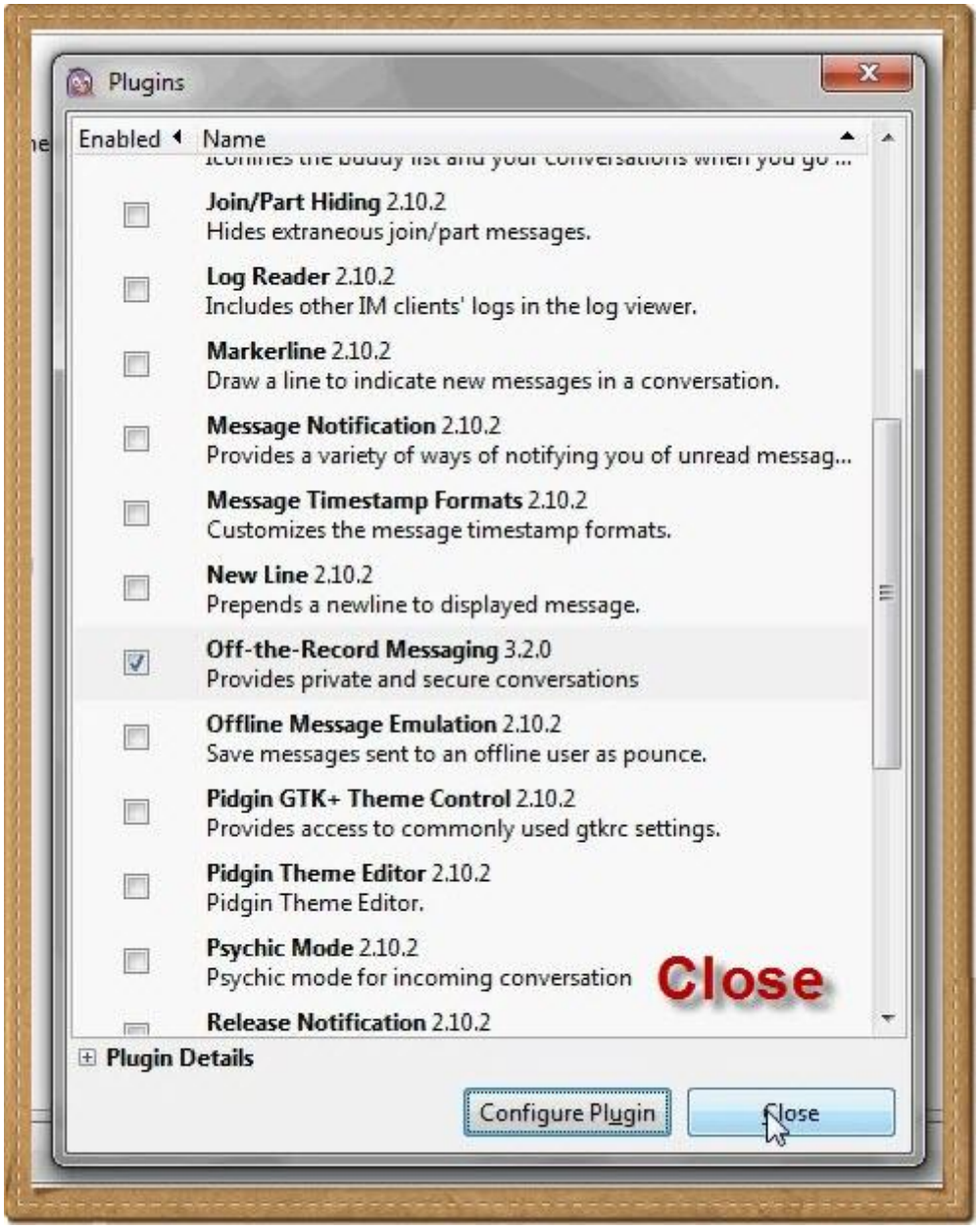


Done

الرقم الكبير الذي ظهر هو الـ Fingerprint الخاص بحسابك وسترى كيف ستستخدمه فيما بعد



نقفل لنبدا المحادثة



المحادثة بالطبيعي لها طرفين على الأقل وطبعا علشان تتشفر محادثه فالمفروض إن التشفير يكون من الطرفين يعني بالفكاكة كده لازم يكون الإتنين عندهم Pidgin ومتفعله فيه OTR

لذلك لإستخدام تشفير المحادثات يجب أن تتم الخطوات السابقة على جهاز الطرف الآخر

السيناريو التالي عباره عن محادثه بين sheen و meem وسنرى كيف سيتم التشفير

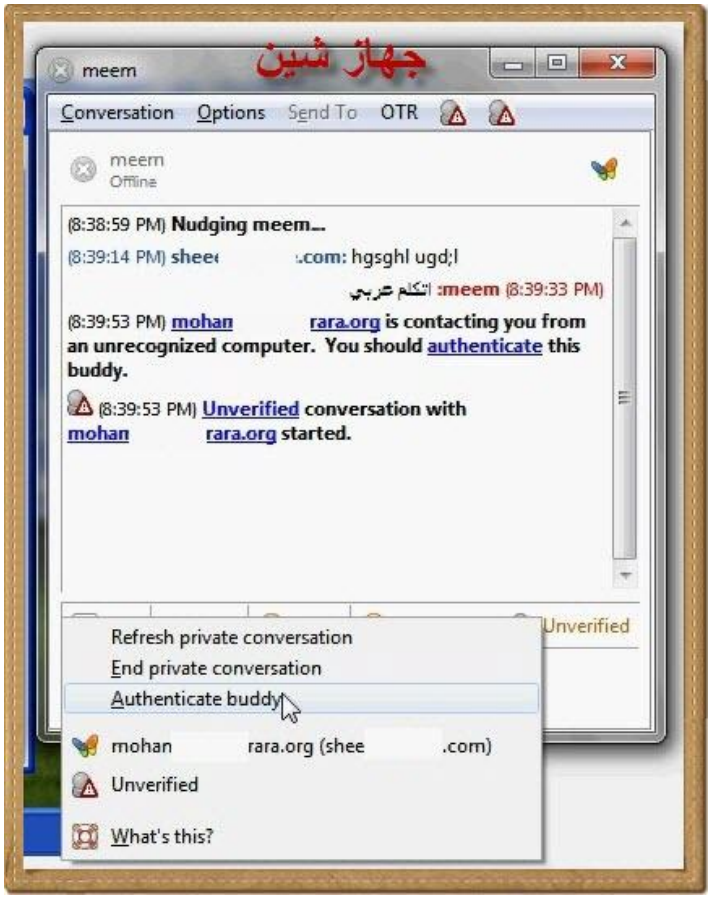
المحادثة مازالت غير مشفرة كما هو واضح Not Private

لنبدأ التشفير يضغط أحد الأطراف meem على Not Private ويختار Start Private Conversation

سيحاول الماسنجر أن يطلب من الطرف الآخر sheen قبول هذا

تظهر رسالة على جهاز sheen تطلب منه عمل Authenticate

بالضغط على كلمة Authenticate أو من قائمة Unverified يختار Authenticate Buddy



يوجد ثلاث بدائل للـ Authenticate

Shared Secret وهو سر يتفق عليه مسبقا بين شين وميم

فيكتب sheen السر ويضغط على Authenticate

يتم إرسال إستفسار شين إلى ميم

على جهاز ميم تظهر رسالة تسأله عن السر اللي بينه وبين شين

لازم يكون السر مطابق تمام في الجهازين , يكتب السر ويضغط Authenticate

رسالة تفيد بالتأكد من شخصية الطرف الآخر

البديل الثاني لـ Authenticate هو أن تسأل سؤال للطرف الآخر وتضع إجابته ويجب أن يجيب الطرف الآخر إجابة متطابقة

تظهر رسالة لميم بتسأله : إسم خالك إيه

يجيب على السؤال

ويديها Authenticate

آخر طريقة بوضع رقم الـ Fingerprint اللي قلنا ح نستخدمه

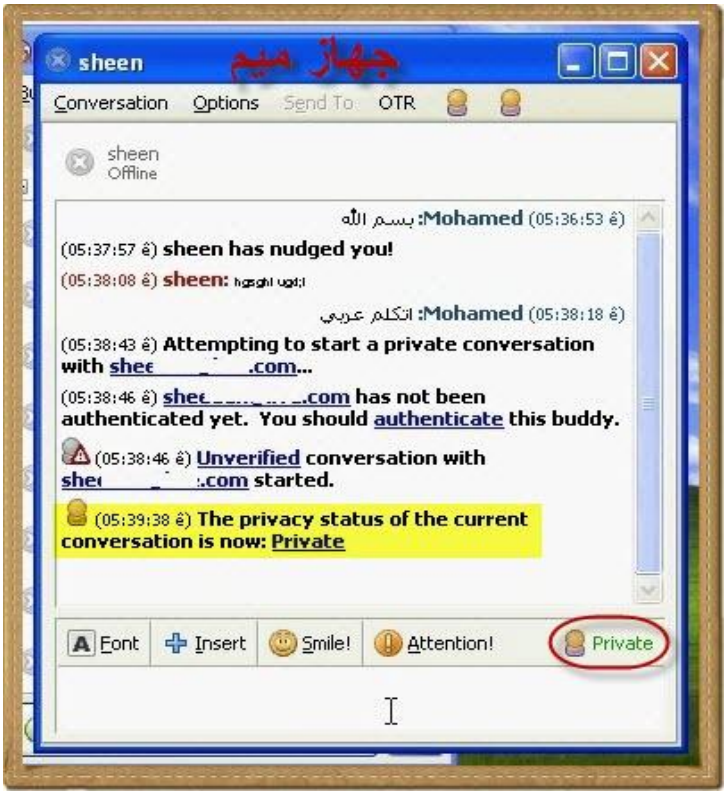
وفي هذه الطريقة يجب أن يكون الطرف الآخر يعرف رقم الفينجر برينت الخاص بك حتى إذا ما سأله البرنامج هل هذا الرقم هو الـ Fingerprint الخاص بصاحبك ميم يعرف يجاوب

أيا كانت الطريقة المختارة فالنتيجة إما التأكد من شخصية من تحدثه أو لا

بعد إتمام الـ Authentication والتأكد من شخصية الطرفين

تظهر رسالة على الشات تخبرنا بأنه تم تشفير الرسالة وأن المحادثة Private

The Privacy status of the current conversation is now Private



وتقدر تطلب ساندوتشات لانشون براحتك

يوجد في ماسنجر Google Talk خاصية إسمها Off the Record , هذه الخاصية مختلفة تمام

عن الإضافة التي استخدمناها مع Pidgin

خاصية Off the Record في Google Talk تعني أن تكون المحادثة بين الطرفين غير

محفوظة لذا فهي لا تتفق مع إضافة Pidgin إلا في الإسم فقط

وبكده إنتهى الكتاب ولله الفضل والمنّه

اللهم إجعلني خيراً مما يظنون واغفر لي مالا يعلمون

اللهم إني أعوذ بك أن أشرك بك شيء أعلمه وأستغفرك لما لا أعلمه

سبحانك اللهم وبحمدك , أشهد ألا إله إلا أنت , أستغفرك وأتوب اليك