NO. 32 • january 2013 • Price Free • www.networkset.net

NetWork Set

First Arabic Magazine For Networks

طريقك الى عالم التكنولوجيا التخيلية

أكثر الشهادات التقنية طلباً لعام 2013

شهادات الحماية SSL Certificate

WIRELESS CUSTOMER QUESTIONNAIRE

عشر طرق يمكن عملها لمنح مخدمك القديم حياة ثانية

FORTIFY IT AND FORGET IT-FORTIDDOS

عشر خطوات يجب أن يعرفه كل مدير شبكة

FIREWALL BUILDER

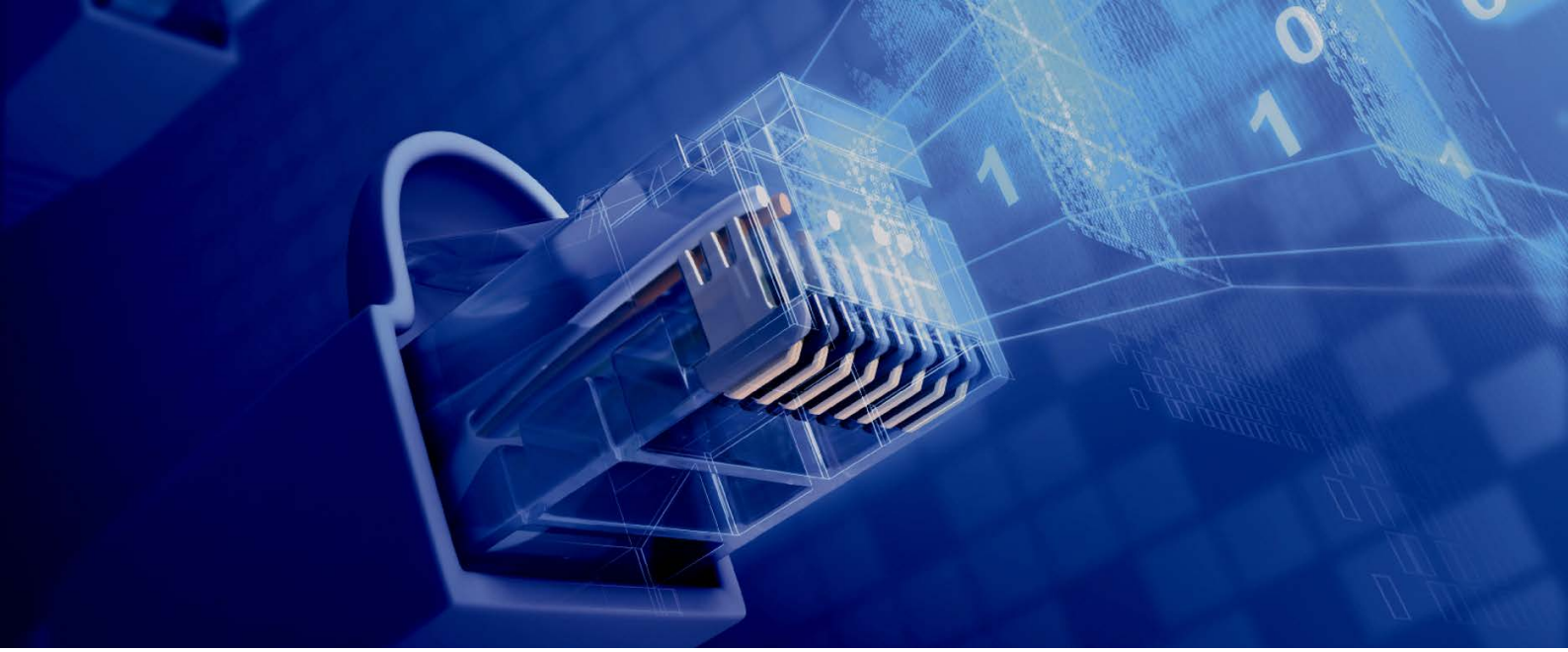
العطاء

إن ما يميز الإنسان عن باقي المخلوقات هو العقل والتفكير والقدرة على اتخاذ القرار والتحكم بالعاطفة، وإذا فكرنا بمشاكلنا الاجتماعية العامة، فنتجاهلها غالبًا؛ على أمل أن تتحسن الأشياء من تلقاء نفسها! أو نصاب بالإحباط بسبب عدم تحقيق النجاح بالوقت المتوقع. ولحل مشاكلنا الاجتماعية البسيطة وفي نفس الوقت هي مؤثرة جدًا، يجب الاعتراف بأننا مخطئين بحق أنفسنا وبحق مجتمعنا ، ومن ثم إيجاد الحلول المناسبة. ما ينقص مجتمعنا العربي هو الاندفاع الذاتي والتضحية وحب الغير وعدم إهدار الوقت والاحترام، مع أن هذه من أسس الإسلام ولكن قليلاً ما نجد من يطبق هذه الأسس. لقد أصبحنا ننظر ، نشاهد ، نشتري ، نستهلك ، وننبهر . ثم ننظر من جديد، نتابع، نشتري، نستهلك ، وننبهر! نحن مجتمع مستهلك ..

هذا يعني أننا خسرنا وقتنا وأموالنا ، فكل شركة تسعى لزيادة عملائها، والشركات الغربية وجدت عميلها هو الشرق الأوسط، فبدون الشرق الأوسط ستتغير موازين الشركات. أسأل نفسي دائمًا لماذا أجد الهاتف أو الحاسب الذي يملكه الغربي متواضعًا جدًا ولكنه يفي بالغرض المطلوب؟ السر هو التفكير بالعطاء والاخلاص بالعمل أكثر من التفكير بالامتلاك والاستهلاك. فكما ستسأل يوم القيامة عن مالك ستسأل عن وقتك وعلمك أيضاً.
كم أشعر بالسعادة عندما أسخر وقتي وعقلي لعمل يرضي اللّه جل جلاله، لأني أعمل بدافع ذاتي ولي هدف أسعى دائماً لتحقيقه وهو تحسين مستوى الثقافة الفردية في المجتمع العربي. مع فريق عربي مبدع، أرى مستقبلا حافلاً بالنجاحات لهذه المجلة وللمدونة.

المهندس أيمن النعيمي وهو مثال للعطاء الحقيقي، أشعر بالفخر به لأنه عربي ومن بلدي وأيضاً المهندسين المشاركين أيضاً لم يبخلوا بوقتهم ومعلوماتهم . تحية شكر من أعماق قلبي لكل المشاركين والقراء، وأتمنى أن ننجح أكثر فأكثر، ولا ننسَ محاسبة أنفسنا كل يوم .

أسامة كامل - سوريا



مجلة NetworkSet مجلة الكترونية شهرية متخصصة تصدر عن موقع www.networkset.net

أسـرة المجلـة

المؤسس	رئيس التحرير
م.أيمن النعيمي	م.أسامة كامل

المحـررون

م.نادر المنسي	م.احمد فتح الله	م.غسان أبو جسار
م.حسام الدين حشيش	م.أحمد خير الدين	---
م.محمد عماد الجغصي	م.خالد الدسوقي	---
م.شيماء الرازق	م.عبد العزيز صبرة	---

التصميـم و الاخـراج الـفني : محـمـد زرقــة

www.networkset.net

NetWork Set

معنى جديد لعالم الشبكات في سماء اللغة العربية

Magazine NetworkSet

أول مجلة عربية متخصصة
في مجال الشبكات

NetworkSet

مدونة عربية متخصصة
في مجال الشبكات

Wiki.NetworkSet

أول موسوعة عربية حرة
و متخصصة في مجال الشبكات

أول مشروع عربي لترجمة
المواد العلمية و التقنية

YouTube

قناة المدونة على يو تيوب

قسم خاص بالأسئلة والاجوبة

FirewallBuilder

كمدير أو مسؤول عن الشبكات غالباً ما يكون لديك أكثر من جدار ناري «فايروول» لأكثر من نوع سواء كان هاردوير أو سوفت وير، والمشكلة التي دائمًا ما نواجهها هى صعوبة التحكم وإدارة هذه الجدران سواءً كان عن طريق وضع سياسات جديدة أو تحديثها أو فحص ومتابعة حالة الفايروول. وتتمنى أن هناك أداة أو برنامج يستطيع أن يدمج كل هذه الجدران تحت منصة واحدة وهذا موجود بالفعل ولكن من المؤكد أن الشركة التى تعمل بها لن توافق على شراء هذا البرنامج بسبب تكلفته المرتفعة ولكننا اليوم سنتعرف على برنامج أكثر من رائع بوجهة رسومية سهلة وبسيطة يستخدم في التحكم وإدارة العديد من الجدران النارية الشهيرة بدون أي تعقيد سواء كان مستخدم البرنامج مبتدئ أو خبير.

البرنامج اسمه Firewall Builder ويعرف أيضاً بـ Fwbuilder ويستخدم كقاعدة مركزية للتحكم في العديد من الجدران من مكان واحد فقط، وقد تحدث في هذه الميزة مدير حماية الجدران النارية في شركة جونيبر وقال عن البرنامج:-

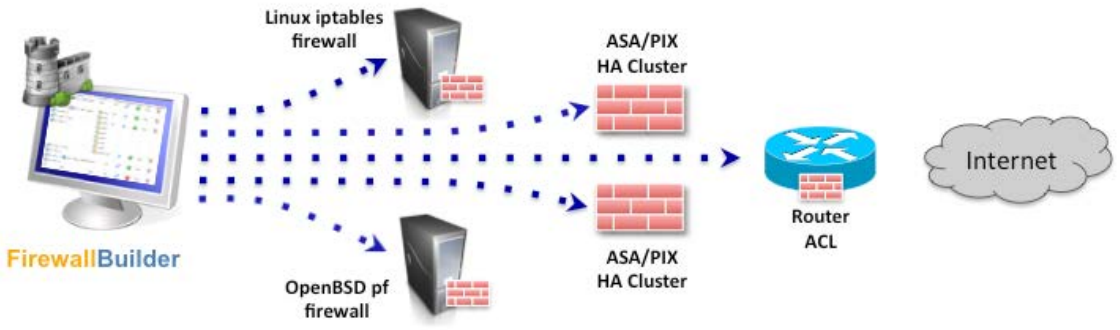
«إن مثل هذه الخيارات التجارية تكون باهظة الثمن من الشركات المنتجة ولكن هذا البرنامج يعتبر أداة إدارية محايدة مع دعم أكثر من منصة وتصميم سهل يسمح بعد ذلك بالتوسع».

وكان تعليق السيد بول ووكر المدير التنفيذى لشركة Oninit على البرنامج كالتالى:-

«مذهل» كيف أصف هذا البرنامج؟ مدير لقاعدة بيانات مسؤولة عن إدارة الشبكة فأنا لا أريد أن أصبح خبيراً في أستخدام Iptables أو Ipfilter أو Cisco PIX أو أي جدار ناري أخر نستخدمه حتى أتعامل معه ولكن هذا برنامج سيجعل حياتي أسهل»

يذكر أن البرنامج منشور تحت نموذج الترخيص المزدوجة (نسخة تجارية ونسخة أخرى للعامة «GPL»).

Firewall Builder



أهم مميزات البرنامج :

1 - صمّم البرنامج لإدارة الجدران النارية بسهولة وأكثر كفاءة، فكل المميزات الموجودة مثل مشاركة الملفات والبحث والاستبدال وكل هذا جعل المديرين يركزوا على سياسات الفايروول وما سيتم السماح أو الرفض البيانات بدلاً من كتابة الأوامر.

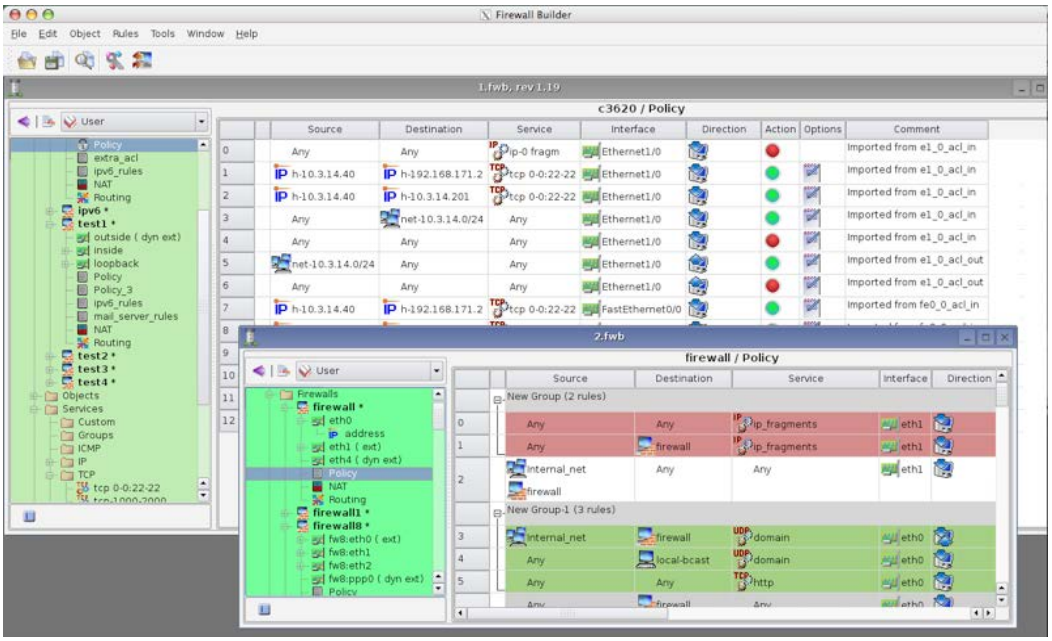
2 - دعم الكثير من المنصات فالجميع يعلم أن سطر الأوامر في الكثير من الجدران النارية قد يكون معقد ويصعب تذكره ولذلك فإن البرنامج بوجهتة الرسومية تستطيع من خلاله العمل بسهولة وإنشاء السياسات المطلوبة بدلاً من الإضطرار إلى البحث على ما نسيته.

3 - إجراء تغيرات على أكثر من جدار ناري من نفس المكان وهذه الميزة ترتبط بالميزة الأولى وعن طريق البرنامج تستطيع أن تعدل في سياسات الجدران النارية المسؤولة عنها دون الحاجة إلى الحركة بل إن كل شيء يحدث عن طريقة وجهة واحدة فقط.

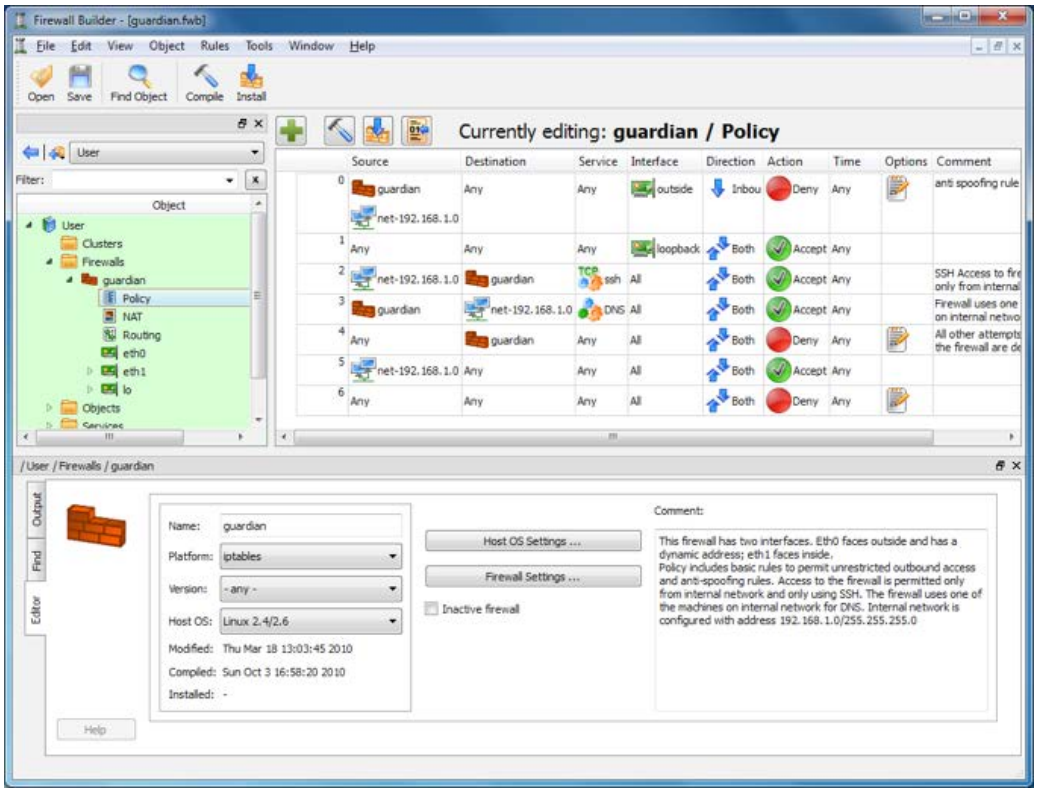
4 - فكرة عمل البرنامج تساعد المديرين أو المسؤولين في الشبكات على تقليل الأخطاء المكلفة والشائعة مثل أخطاء إنشاء سياسات غير صحيحة وهكذا.

5 - عدم الوقوع تحت قبضة الشركات المنتجة والجميع يعلم أن من السهل نقل السياسات التي قد طبقت على فايروول ما ولكن في بعض المنتجات لا يحدث هذا لذلك مع البرنامج يمكن أن تجعل الأمر يعمل تلقائياً وبدون تدخل منك حتى لو كانت قدرات الجهاز الجيد غير متطابقة مع الجهاز الأساسي

6 - الترقية والتحديث بدون أي مشاكل فالجميع قد يعاني من هذه المشكلة فمن الممكن أن تكون الإصدارات الجديدة من جدران الحماية بها مميزات جديدة وذلك يعني أن عليك دراستها ومعرفة الأوامر التى تستطيع من خلالها تشغيل هذه المميزات ولكن أن كنت تستخدم البرنامج فهو يقوم بعد عملية الترقية ببناء قواعد جديدة للميزات المضافة دون الحاجة لإجراء أي تغيير منك.



Firewall Builder



الأنظمة التي يدعم البرنامج الجدران النارية الخاصة بها فهي كالتالي :

1 - iptables الجدار الناري الخاص بنظام لينكس.

2 - ipfilter الجدار الناري الخاص بنظام Sun Solaris, FreeBSD, OpenBSD

3 - ipfw الجدار الناري الخاص بـ نظام MacOS X, FreeBSD

4 - Packet Filter الجدار الناري الخاص بنظام OpenBSD

5 - يعمل أيضاً على أحد الجدران النارية الخاصة بشركة سيسكو وبالتحديد CiscoPIX ويعمل على الـ Cisco IOS Access Control Lists (المرخصة تجارياً)

6 - ويعمل على الجدران النارية الخاصة بمنتجات شركة Linksys (القديمة) وعلى OpenWrt firmware

* في البداية تم إنشاء التطبيق لنظام لينكس ثم بعد ذلك توفرت العديد من الإصدارات للكثير من أنظمة التشغيل الأخرى مثل ويندوز وماكنتوش و فري بي أس دى وتوزيعة أوبن سوزي.

وهذه بعض الفيديوهات التعليمية بها أساسيات استخدام البرنامج مقدمة من الموقع الرسمي :-

http://youtu.be/Q5GPrkwyGxw

http://youtu.be/Q9imdAjjdqQ

http://youtu.be/WezfP_z-L64

http://youtu.be/4Gy5CRjTjkQ

وأخيراً تستطيعون تحميل البرنامج من الموقع الرسمي:

http://www.fwbuilder.org

أو من موقع SourceForge على الرابط التالي:

/http://sourceforge.net/projects/fwbuilder

ولمزيد من المعلومات عن البرنامج يمكنكم زيارة الموقع الرسمي للبرنامج.

10 خطوات يجب أن يعرفها كل مدير شبكة

بعد اتخاذك القرار بدخول عالم تكنولوجيا المعلومات، و بعد تخرجك من الجامعة ما هي أولى خطواتك للدخول إلى هذا العالم؟ ما هي أساسيات هذا المجال؟ ما هي الأشياء التي يجب معرفتها قبل الصدام الأول مع مديرك في مقابلة التوظيف؟ كيف تبدأ و من أين؟

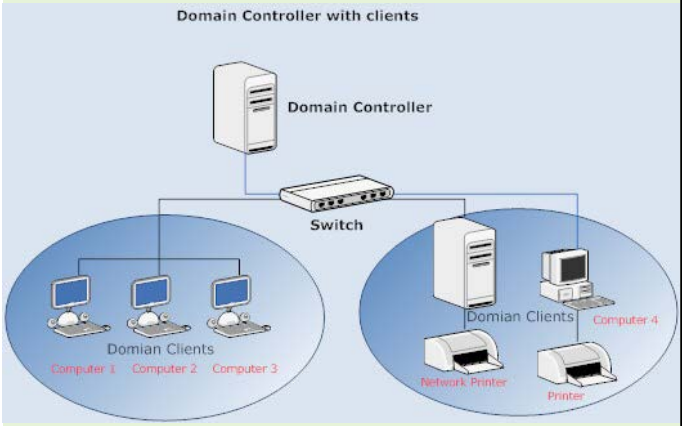
نبدأ بما انتهينا، حيث أن المكان الصحيح للبدء في هذا المجال هو رغبتك بالدخول و الاحتراف في عالم تكنولوجيا المعلومات بشكل عام و تخصصك بشكل خاص، تأكد من رغبتك الجامحة للدخول في هذا المجال لكي تتقن و تبدع أيضًا.

فمثلاً، من البديهي معرفة الـ IP Subnetting ، كذلك معرفة الأساسيات في الـ Switching و الـ routing و الـ firewalling أمر غاية في الأهمية لترسم تصورك حول آلية عمل الشبكة التي سوف تديرها يومًا ما، ولكن ماذا عن الأعمال الروتينية اليومية التي يتوجب عليك القيام بها للحفاظ على أمن و استقرار شبكتك؟ وذلك عملاً بالمثل القائل - الوقاية خير من العلاج - لأن العلاج في كثير من الأحيان يكون باهظ الثمن.

في اليوم الأول من عملك في منصبك الجديد IT administrator ، احرص على اتقان الأعمال التالية لتنجح في هذا المنصب و تكون الترقية بانتظارك، عوضًا عن الجلوس في منزلك و اتقان شرب الشاي.

1 Domain a computer :

يجب أن تتأكد بأنّ جميع الموظفين العاملين في قسم الـ IT مدركين تمامًا كيفية إضافة windows computer للـ domain مع مراعاة جميع القواعد الخاصة بإضافة computers, printers or any other machines للـ domain من حيث أسماء هذه الأجهزة و عدم تكرارها و الحفاظ على الاستقرار في عملية الحصول على الـ IPs و تجنب حصول تعارض.



وهنا يجب عليك وبوصفك مديرًا لهذه الشبكة تحديد أشخاص للقيام بهذه المهمة وإعطاء الصلاحيات اللازمة على مستوى الـ domain controller والحرص على عمل cache credentials للـ Laptops وذلك لتجنب مشكلة الـ Login عندما يعمل هذا الجهاز خارج الشبكة، أيضًا يجب تحديد وتنظيم الأجهزة التي يجب أن تكون في workgroup و السبب وراء ذلك مثلاً الجهاز الذي سوف يعمل Edge Transport Server في منظومة عمل الـ Exchange enterprise server.

2 Troubleshoot printing :

مشاكل الطباعة اليومية، قد تكون من أهم مصادر استنزاف الوقت بالنسبة لك، و ضياع الوقت بالنسبة للموظفين. لذلك يتوجب عليك معرفة جميع المشاكل اليومية للطابعات من إضافة و حذف الطابعات، محلية كانت أو على مستوى الـ domain ، معرفة آلية تعريف الطابعات بشكل نموذجي على جميع أنظمة التشغيل لديك، فمثلا في windows يجب عليك معرفة كيفية إزالة الطابعات من الـ Windows registry في حال تطلّب الأمر.

الطابعات، هي آلات إلكتروميكانيكية، لذا فإن الحركة الميكانيكية المستمرة و اليومية تسبب أعطالاً دائمة على مستوى الـ hardware والتي يمكن تجاوزها بشكل بسيط بالمتابعة اليومية وعدم إهمال أو تأجيل أي من المشاكل التي تطرأ.
ففي الطابعات النقطية مثلا، يجب الحفاظ على مسافة معينة للرأس المخصص للطباعة و التأكد من جودة أشرطة الطباعة و البرمجة الصحيحة للطّابعة .

3 Boot into Safe Mode :

هناك الكثير من الحالات التي تستوجب العمل من خلال الـ Safe mode ، ولهذا السبب يتوجب عليك معرفة كيف تدخل وفي أي حالة تدخل إلى هذا الوضع .

على سبيل المثال لا الحصر، قد يكون أحد الأجهزة ضحية من ضحايا فايروس معين مما يضطرك لاستخدام إحدى الأدوات لإزالته مثل: ComboFix ، هذا يعني أن الـ Safe mode هو الخيار لتشغيل هذه الأداة.
يجب أن يكون F8 من أصدقائك المفضلين، حيث أنك سوف تحتاجه بشكل كثير لحل مشاكل معينة، ابتداءً بالتعارض بين تعاريف الـ Hardware devices انتهاءً بوجود فايروس.
احرص على استخدام Safe Mode With Networking أو Safe mode with USB للاستفادة من أي موارد خارجية يمكن أن تحتاجها في عملية إصلاح أي من أخطاء النظام.
أخيرًا، إحدى أهم النصائح التي أقدمها لك، هي: إذا لم تحسن استخدام الـ Safe mode بمختلف اشكاله فإن مجال الـ IT ليس مجال عملك.

4 Install an OS :

إن عملية تنصيب أنظمة التشغيل وتعريفها يمكن أن تكون من البديهيات إلا أن اختلاف وتنوع أنظمة التشغيل التي تعمل ضمن شبكتك كثيرة.
فمثلا، يجب أن تكون لديك الخبرة الكافية في تنصيب أنظمة التشغيل ابتداءً بـ windows بمختلف الإصدارات، مرورًا بـ Linux وتوزيعاته الكثيرة، انتهاءً بـ MAC .

كما أنه في هذه المرحلة من التطور السريع لتقنية الـ virtualization يحتّم عليك فهم الآلية التي تعمل على أساسها هذه التقنية والقدرة على التعامل مع بعضها، وخير مثال هو الـ VMware والذي أصبح يقدم حلولاً جيدة جدًا للاستفادة من جميع الموارد المتاحة لديك.
كما أن ندرة الموارد أحيانًا تجبرك على تشغيل أكثر من نظام على نفس الجهاز، و بالتالي يتوجب عليك اتقان المهارات المتعلقة في تشغيل عدة أنظمة تشغيل على جهاز واحد.

5 Manage users in Active Directory :

إن عملية إدارة الشّبكة من خلال الـ Active directory هي مما لا شك فيه عملية ذات أهمية كبيرة وتستطيع القيام بها ببساطة إذا كان عملك على مستوى مستخدم واحد أو اثنين أو حتى أكثر وصولاً إلى عشرة مستخدين يوميا بتطبيق الـ action الذي تحتاجه مثل، adding, removing, editing, locking, unlocking, or just resetting passwords ولكن، ماذا لو كانت هذه التغيرات وغيرها يجب تطبيقها على ما يفوق الـ 100 مستخدم؟ من الخطأ اتباع الطرق التقليدية في الـ active directory للتعامل مع كل مستخدم بشكل منفصل عن طريق الـ GUI (graphical user interface) ، فهي إهدار الوقت سوف يكون كبير جدًا.

تخيل أنك تقوم بعمل resetting passwords لمئة مستخدم! بعملية حسابية للوقت الذي تحتاجه لإتمام ذلك يكون، بفرض تحتاج لـ 10 ثوانٍ فقط لكل مستخدم ، فأنت تحتاج حوالي 17 دقيقة لـ 100 مستخدم! ولكن عندما تكون خبيرًا بالتعامل مع الـ power shell مثلا فأنت تحتاج إلى 30 ثانية للقيام بذلك!.
ما أردت قوله، يجب اكتساب مهارات بالتعامل مع الـ Active directory لتسهيل و تسريع عملية إدارة المستخدمين و الموارد الأخرى الموجودة في شبكتك.

كما يجب الأخذ بعين الاعتبار جميع أنظمة التشغيل الموجودة والتي لا تستطيع التخاطب مع الـ Active directory وتنصيب البرامج والبروتوكولات الهجينة اللازمة للتخاطب مع بعضها لتتمكن من السيطرة والتحكم بشكل كامل بمختلف الموارد و الأجهزة الموجودة لديك.

6 Reset a password on a server :

تغيير الـ Administrator password للسيرفرات هو أمر ضروري في حالات كثيرة، ولكن ليس بسهولة تغيير الـ password لمستخدم ما عن طريق الـ active directory ، فمثلا عندما تريد إعادة تشغيل واستثمار أحد السيرفرات والتي كانت في حالة Offline لوقت طويل ولا تعلم ماهي الـ Administrator password فانت بحاجة إلى استخدام العديد من الأدوات لوضع password جديدة لتتمكن من تشغيله.

لذا إن معرفة طرق تغيير الـ Administrator passwords أمر حيوي جداً وسوف تستخدمه كثيرًا على مختلف أنواع السيرفرات Windows, Linux, MAC .

7 Create an Outlook profile/account :

أحد أهم برامج البريد الالكتروني كما هو معروف Microsoft Outlook ، والذي لابد عنه بوجود الـ Exchange server فهو البرنامج الشهير والمفضل لدى المستخدمين، لذا يتوجب عليك الإحاطة وبشكل كامل بالأخطاء التي من الممكن أن يظهرها.
فمن الضروري مثلا معرفة كيفية إصلاح العطب الذي يصب الـ PST file ، وكيفية انشاء الحسابات التي تستخدم جميع أنواع البروتوكولات كالـ HTTP, POP3, IMAP

8 Run chkdsk :

هناك العديد من الحالات التي تستوجب عمل Run chkdsk للـ hard disk drive ، كفقدان بعض ملفات الإقلاع مثلا، أو بعض القطاعات المعطوبة في الـ hard disk drive.
لذا يجب الإلمام بجميع البرامج التي تستخدم في هذا المجال، ومعرفة الـ commands التي تمكنك من إصلاح هذا النوع من الأعطال بشكل أوتوماتيكي لأنه وفي معظم الحالات لا تستطيع استخدام الـ GUI.

9 Schedule a Windows Server backup

إحدى أهم المهام التي سوف تعمل على متابعتها يوميًا هي الـServers Backup ، فمن الضروري والمهم جدًا التأكد يوميًا من أن الـ Backup يعمل بشكل صحيح و منتظم.

يمكن استخدام أدوات مخصصة لعملية الـ Backup ، كما يمكن استخدام البرامج الموجودة أصلا في أنظمة التشغيل على اختلافها، إلا أن الشيء المهم الذي يتوجب أخذه بعين الاعتبار هو أن تكون برامج النسخ الاحتياطي لا تتطلب إعادة تشغيل أو ما شابه.

مع تطور تقنيات النسخ الاحتياطي، أصبحت من الأمور البسيطة والتي تعمل بشكل أوتوماتيكي إن أردت، فيما نذكر عمليه استخدام الـ Tape فيما سبق لتخزين البيانات.

نجد اليوم أنه لا داعي لاستخدام الـ Tape بوجود تقنيات مثل SAN.

احرص على عمليات النسخ الاحتياطي على مستوى الـ Software و الـ Hardware .

10 Clear space on a C drive :

يجب التأكد بشكل دائم من أن المساحة المتوفرة على القرص C من السيرفرات كافية.

و التأكد من عدم وضع الملفات الخاصة، كذلك البرامج التي لا يتطلب و جودها على القرص C تحديداً.

وذلك لأن الأخطاء الناجمة عن هذا الأمر غالباً ما تكون غير مفهومة و يتطلب اكتشافها بعض الوقت، حيث أنك سوف تفكر بأي مسبب آخر عدا هذا.

لذا احرص على استخدام أدوات لتنظيف القرص C باستمرار كالـ temp files, internet history . . باستخدم CCleaner مثلاً.

السيرفرات التي تشغّل oracle مثلا تقوم بنسخ ملفات كثيرة على القرص C كالـ history ، لذا يجب حذفها بشكل مستمرلتجنب الـ Server Crash أو فقدان ملفات معينة.

SIP

من منّا لا يستخدم برامج المحادثة الشهيرة مثل Google Talk, Windows Live Messenger Skype, إن كان في المحادثات الصوتية أو في المؤتمرات المرئية أو في نقل وتبادل الصور والموسيقى؟ ولكن هل فكرت يومًا كيف تعمل تلك التطبيقات وكيف تنتقل البيانات الخاصة بها ومن هو البرتوكول المسؤول عن إقامة جلسات الاتصال الصوتي ونقل البيانات الصوتية؟

قبل البدء بالحديث عن بروتوكول بدء الجلسة SIP لنتكلم قليلاً عن تقنية VOIP ماهي وكيف تعمل ؟

VOIP واختصارها Voice Over IP وتعني نقل الصوت عبر شبكة الانترنت التي تعتمد بروتوكول IP لنقل المعطيات، حيث يتم نقل المعطيات ضمن الطرود عبر الشبكة بشكل مشابه تمامًا لنقل المعطيات الأخرى بواسطة Packet Switching ، تمر عملية نقل الصوت عبر الانترنت عبر عدة مراحل :

1 - تأسيس الاتصال.
2 - رقمنة الصوت « تحويل الصوت من إشارة تماثلية إلى رقمية ».
3 - تغليف الصوت ضمن الطرود Packet.
4 - توجيه الطرود عبر الشبكة.
5 - تحليل المعلومات الصوتية.
6 - إعادة توليد الصوت وتوجيهه حتى يصل وجهته.
7 - استقبال الطرود ومن ثم تحليلها واستخراج المعلومات الصوتية منها.
8 - تحويل الإشارة الرقمية إلى تماثلية «صوت».
9 - إنهاء جلسة الاتصال.

إن عملية تأسيس الاتصال التي تتم في البداية تتم بواسطة signaling protocol ومن ثم يأتي دور بروتوكولات التحكم بالاتصال مثل H232 أو SIP أو MEGACO وغيرها .

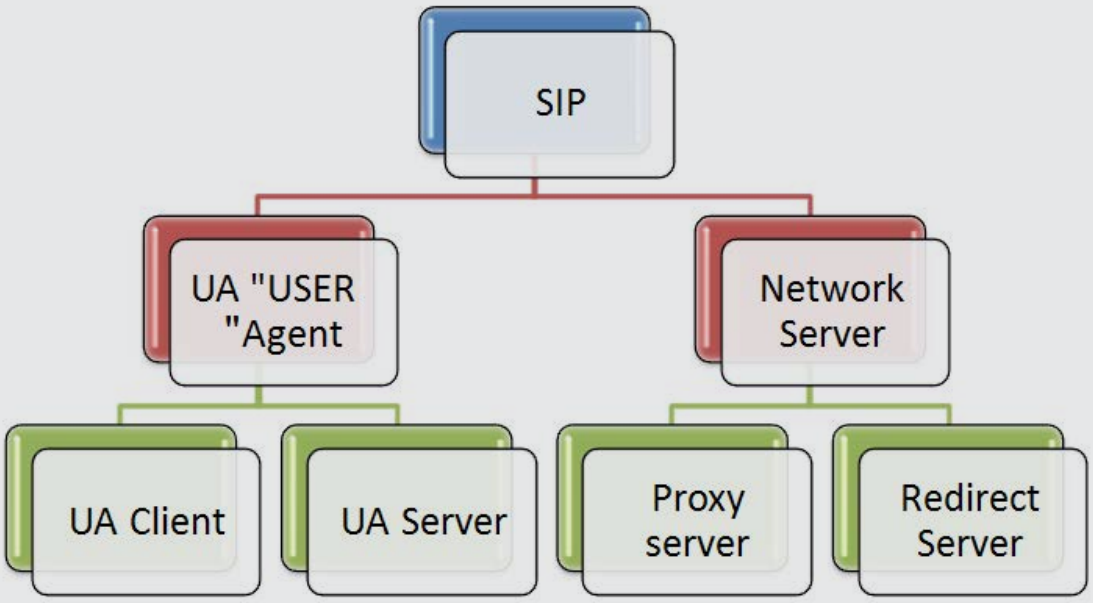
SIP Session Initiation Protocol أو كما يسمى بروتوكول بدء الجلسة تم تطوير هذا البروتوكول من قبل فريق عمل هندسة الانترنت IETF، وهو معرف ضمن المعيار RFC 3261.

يعتبر بروتوكول SIP بروتوكول بسيط مقارنة بقرينه H232 كما أنه يتمتع بمرونة عالية من حيث كونه مستقلاً عن نمط الوسائط المتعددة التي يتم إرسالها بواسطته «صوت صورة ، فيديو»

عندما نتحدث عن بروتوكول خاص بـ VOIP فنحن نتكلّم عن أمرين أساسيّين هما تبادل للمعطيات الصوتية وإصدار أوامر إشارات التحكم اللازمة ، من حيث البنية فإن بروتوكول SIP يشبه إلى حدٍّ كبير بروتوكول HTTP من حيث طريق صياغته للرسالة وترويسته ، يتم إرسال رسائل هذا البروتوكول وفق أحد بروتوكولات طبقة النقل TCP,UDP , يعتبر SIP وحده بروتوكول ناقص فهو يحتاج إلى مساندة من قبل بروتوكول للنقل بالزمن الحقيقي وذلك على اعتبار أن البيانات التي يتم نقلها صوتية ، فيجب أن تتم بالزمن الحقيقي وذلك كما ذكرنا بالتعاون مع RTP(Real Time Protocol) .

مكوّنات بيئة عمل SIP:

بعد أن رأينا وصيف بسيط لهذا البروتوكول، سنرى الآن ما هي المكونات اللازمة لعمله:
يتألف SIP من عدة مكونات مبينة بشكلٍ هرمي كالتّالي:



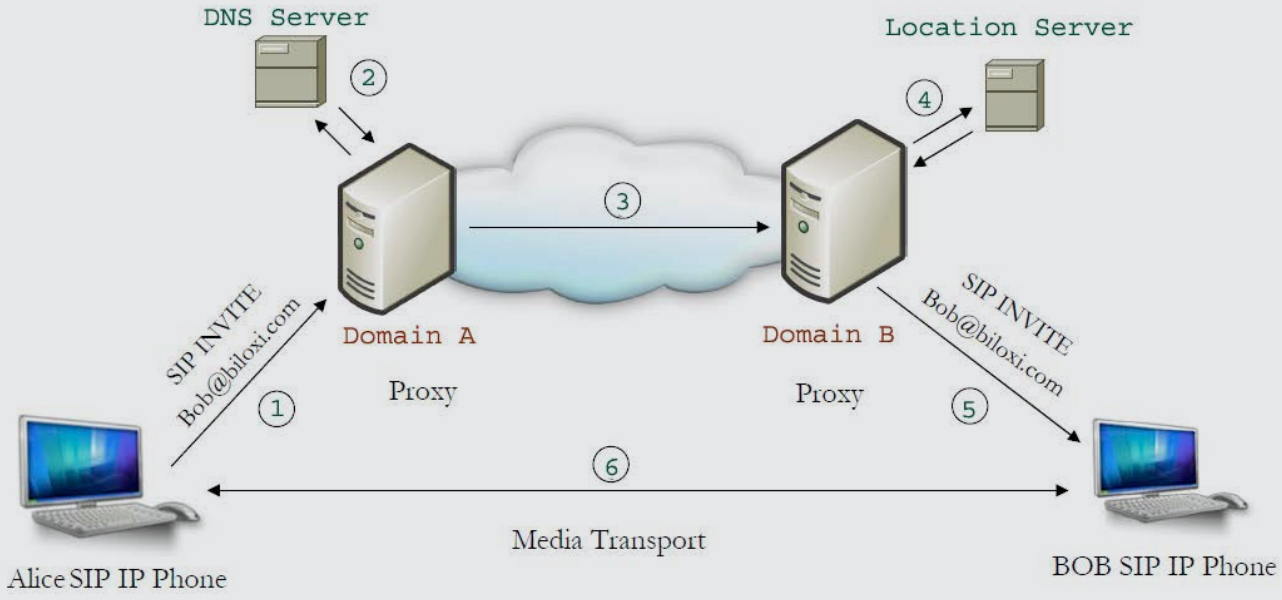
لنرى الآن ما هي وظيفة هذه المكونات :

User Agent: ويتألف بدوره من مكونين: عميل الزبون وعميل المخدم ، يقوم عميل الزبون على إرسال طلبات SIP ويرد عليه عميل المخدم .

Proxy server: يلعب دور الوسيط بين المستخدمين، يتصرف بالنيابة عن العميل ويحتوي على توابع كلا من الزبون والمخدم، يستطيع تفسير ترويسة الطلبات الموجهة عبره وإعادة كتابتها قبل أن يعيد تمريرها، ويعمل على توجيه الرسائل إلى موقع المستخدم الحالي ويستطيع مقابلة الأسماء Name Mapping بالعناوين IP .

Redirect Server: مخدم إعادة التوجيه يعمل على إعادة توجيه الطلبات إلى عنوان URL آخر قادر على أن يخدم الطلب ، يفيد هذا المخدم في حالات توزيع الحمل.

المخطط التالي يوضح خطوات إقامة الاتصال بين النقطتين:



SIP

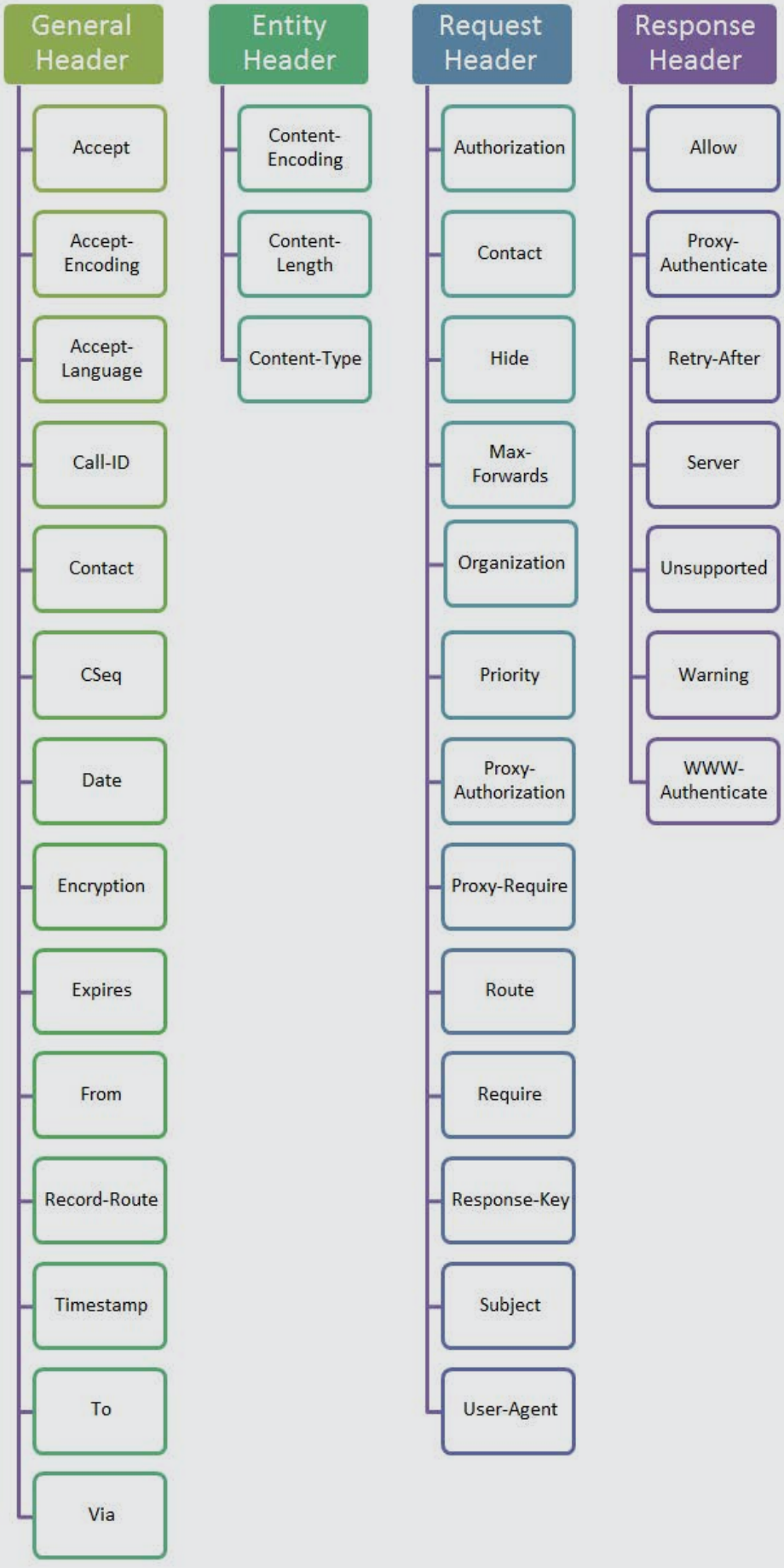
رسائل SIP

يستخدم بروتوكول sip نوعين أساسيين من الرسائل هما طلبات إقامة الجلسة الصادرة من الزبون والرد الذي يعود من المخدم ، كل رسالة من الرسائل السابقة تتضمن ترويسة يتم التصريح ضمنها عن معلومات حول الاتصال.

تقسم ترويسة البروتوكول إلى 4 مجموعات أساسية وهي:

1 - General Headers
2 - Entity Headers
3 - Request Headers
4 - Response Headers

المخطط التالي يوضح المعلومات التي تندرج تحت كل نوع من أنواع الترويسات السابقة:



SIP

بالتأكيد لن نستطيع الإحاطة بشكل كامل بالمعلومات السابقة ولكن يمكن أن نتعرف على بعضها وماهي وظيفتها من خلال هذا الجدول المختصر:

الترويسة	التوصيف
To	تحدد هوية الطرف المرسل إليه.
From	تحدد هوية الشخص المرسل.
Subject	تحدد طبيعة المكالمة.
Via	الطريق الذي يسلكه الطلب.
Call-Id	معرف وحيد خاص لكل زبون.
Content-Length	يمثل طول الرسالة كاملة "ممثلاً بالترميز الثماني".
Content-Type	تحدد نمط الوسائط التي تتضمنها الرسالة "صوت ، فيديو".
Expires	تحدد تاريخ صلاحية الرسالة.

رسائل الطلبات

وتضم 6 أنواع من الرسائل وهي:

1 - INVITE
2 - OPTIONS
3 - ACK
4 - BYE
5 - REGISTER
6 - CANCEL

رسائل الرد

وتكون حسب رسالة الطلب التي وردت ، حيث يتم إرسالها استجابةً لطلب تم إرساله وتشير إلى نجاح أو فشل الدعوة بما في ذلك حالة السيرفر،

وتصنف الردود ضمن 6 أصناف رئيسية وهي:

1 - Informational
2 - Success
3 - Client-Error
4 - Client-Error
5 - Server-Error
6 - Global Failure

ضمن كل تصنيف من الأصناف السابقة يوجد عدد من الأكواد يمكن أن نأخذ منها اقتباسات سريعة مثل:

Class	Code	Explanation
Informational	100	Trying
	180	Ringing
Success	200	OK
	300	Multiple choices
Client-Error	400	Bad request
	404	Not found
Client-Error	408	Request timeout
	409	Conflict
	420	Bad extension
	411	Length required
Server-Error	500	Internal server error
	502	Bad gateway
	504	Gateway timeout
Global Failure	600	Busy everywhere
	604	Does not exist anywhere

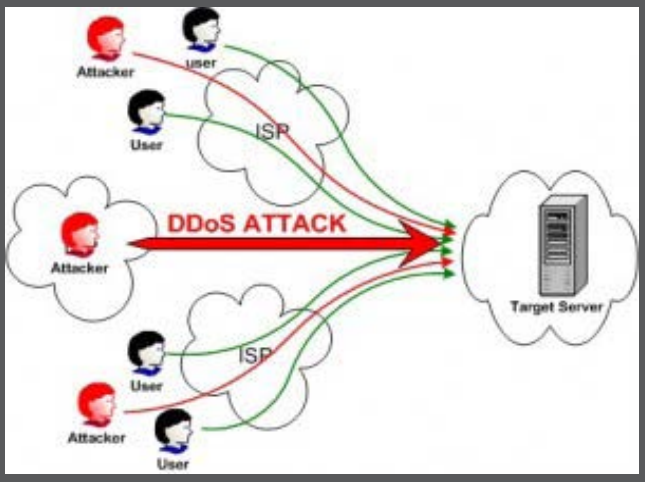
FORTIFY IT AND FORGET IT- FOR TIDDOS

إن توفير الحماية لأجهزة الشبكة يعتبر تحدٍّ من الدرجة الأولى ويتزامن عمر هذا التحدي مع بداية تواجد واستخدام الشبكة العنكبوتية أو ما يعرف بالانترنت وكلما تقدمت التكنولوجيا المستخدمة كلما زادت مخاطر التعرض للهجمات حيث أن تقدم التكنولوجيا يتبعه تقدم فى طرق تأمين الشبكة مما يجعله بمثابة تحدٍّ للمخترقين لاستخدام الأساليب الجديدة وإظهار الثغرات والعيوب التي يمكن من خلالها خلق تهديد لشبكة الكمبيوتر .

لذلك يناقش هذا المقال واحدًا من أهم وأخطر الهجمات المعروفة ألا وهو DOS attack والذي بدوره تطور ليمثل خطورة أكثر بكثير كما هو معروف بـ DDOS attack . سنتحدث عن طبيعة هذا الهجوم والغرض منه وكيفية مواجهته باستخدام FortiDDOS.

• ما المقصود بـ DOS attack :

هو ذلك الهجوم الذى ينوي فيه الهاكر استنفاذ كل خدمات الشبكة ليترك بقية المستخدمين الشرعيين غير قادرين على الدخول للشبكة أو استخدام أي من خدماتها وتكبيد الشركة خسائر مالية ضخمة إضافة إلى الإطاحة بمصداقيتها.



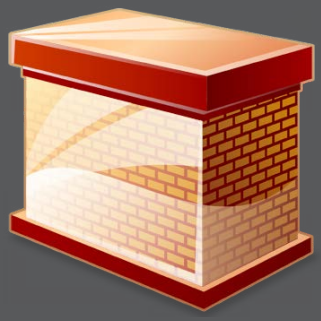
• كيف يبدأ الهاكر بـ DDOS؟

يتم ذلك عن طريق كتابة برنامج بسيط ولكن بواسطة شخص متخصص غالبًا ما يكون هاكر محترف، يقوم هذا البرنامج بإرسال نفسه ولكن بشكل خفي إلى مئات بل آلاف الأجهزة. بعد وصوله بنجاح إلى الهدف يطلق على الجهاز المستقبل اسم Agent or Zombie لأن هذه الأجهزة ستتولى مهمة بدء الهجوم على النظام المستهدف أو الضحية نيابة عن الهاكر . لو حدث وتمكن الهاكر من إرسال هذا البرنامج إلى شبكة كمبيوتر ليصيب جميع أجهزتها أو بعضها، حينئذ تسمى هذه الشبكة بـ BotNet

• استراتيجيات الدفاع:

Firewalls - يمكنها حل بعض المشاكل حيث أنه باستخدام الفايرول يمكننا السماح فقط للمستخدمين المصرح لهم بالدخول ومنع الآخرين ولذلك فهو يعتبر جزءًا هام وقيم من استراتيجيات التأمين ولكن في حالة بعض السيرفرات مثل Public web servers and eCommerce servers تجد أن هذه السيرفرات لا يمكنها معرفة منْ من المستخدمين سيقوم بزيارتها مسبقًا وبالتالي فإن فكرة استخدام Firewall Access List لن تجدي نفعًا . قد يقترح البعض أنه عن طريق الفايرول يمكننا غلق بعض

البروتوكولات ولكن المشكلة الأكبر أن DOS attack يستخدم ports مصرح بها مثلا (for TCP port 80 web servers) مما يعني أن غلق هذا البورت سيمنع كل HTTP traffic الشرعي من الوصول للسيرفر والذي بدوره يسهل مهمة الهاكر وإتمامها بدون أي عناء يذكر.



ومن هنا يمكننا تلخيص دور الفايروول فى إمكانية صد single DOS attack وعدم قدرته على مواجهة DDOS القادم من آلاف الـ Zombies حيث أن كلاً من هذه الأجهزة التي تقوم بالهجوم ترسل legal packet التي حتما ستجتاز الفحص الدقيق خلال الفايروول لأن المشكلة ليست في محتوى الباكيت ولكن فى عددها ومعدل وصولها والذي دائما ما يفوق قدرة الشبكة على التعامل معها.

Router access control list-

بنفس الطريقة السابق ذكرها مع الفايروول فإن الراوتر بإمكانه السماح بدخول من له الحق ومنع من يجب منعه ولكن معروف أن الوظيفة الرئيسية للراوتر هى توجيه الباكيت ولذلك فإن إجبار الراوتر على القيام بـ Layer 2,3,4 and 7 inspection بالتأكيد سوف يقلل من أداؤه بسبب استهلاك الكثير من memory and processing capabilities وبالتالي تقليل network throughput .

على أي حال فهناك العديد من المقترحات للحد من هذا النوع من الهجوم مثل استخدام antivirus software او IDS او IPS سواءً سوفت وير أو هاردوير وكلها بالطبع حلول هامة جداً وفعالة في تأمين الشبكة ولكن لو تحدثنا عن DDOS attack ناتج عن برنامج مكتوب بمهارة شديدة فإن كل من الحلول السابقة لن تصمد كثيراً قبل انهيار النظام وتوقف الخدمات.

- **إذا ما الحل؟**

قبل الكشف عن أي تكنولوجيا مستخدمة بفاعلية لمواجهة DDOS attack سنتعرض مسبقا لأحد أهم الطرق المستخدمة في مثل هذه الأجهزة وهو ما يعرف NBA «network behavior analysis» systems

مهم جداً أن ندرك أن كل ما يفرق الترافيك الطبيعي الشرعي والترافيك الناتج عن DOS attack هو معدل إرسال الترافيك فكلاهما Legal وكلاهما لا يحتوى على malicious attack requests ولذلك يمكننا تلخيص الفارق بعبارة واحدة هامة جداً متكررة عن الحديث عن مثل هذه الأنظمة وهي «differences are in intent not in content».

لذلك نحن بحاجة إلى وسيلة يمكن من خلالها التعرف على المعدل الطبيعي من الترافيك الخاص بكل شبكة وبناءً عليه يمكن التنبؤ بزيادةٍ غير طبيعية في حجم هذا الترافيك في حالة ما إذا كانت هناك محاولة للهجوم على الشبكة والتصرف بناءً على العديد من الـ settings التي يحددها مدير الشبكة .

هنا يتلخص دور FortiDDOS وهو أحد الأجهزة الحديثة للشركة العملاقة Fortinet والمستخدم بشكل فعال في صد هجمات DDOS.

FortiDDOS Overview

كمساهمة لتأمين الشبكة بشكل متكامل طورت شركة فورتي نت منتجها الجديد والمعروف باسم FortiDDOS للحماية من هجمات DOS & DDOS فهو يوفر حماية غير متوقفة حتى من تلك الهجمات الجديدة والغير معروفة بـ signatures فهو في الأساس لا يهمه محتوى الترافيك كما سبق وذكرت «focuses on intent not content», كما أنه ينظر إلى الباكيت بشكل اجمالى حيث انه يراقب معدلها غالبا لكل ثانية على مدار فترة زمنية محددة وقياس هذا المعدل يتم لكل من layer 2,3,4 and 7 وبعد انتهاء هذه المدة من مراقبة ومتابعة الباكيت يكون الجهاز قد كون قاعدة بيانات خاصة بالمعدل الطبيعي المعتاد للشبكة ما يخالف ذلك او ما يتعدى الـ threshold المعين مسبقًا يعتبر محاولة من محاولات

الهجوم . مثال : لو فرضنا ان هناك فايرول أدمن قام بوضع rule تنص على إتاحة وصول الترافيك إلى UDP port 1434 فإن أي ترافيك أيًا كان حجمه سيمر إلى هذا البورت بغض النظر عن معدله.
على الجانب الآخر وبفرض FortiDDOS admin قام بوضع نفس ال rule سيجد أمامه الخيار الأهم وهو تحديد معدل الترافيك فيمكنه أن يقول أن الترافيك لهذا البورت مسموح ولكن بشرط ألا يتعدى 10 packets فى الثانية الواحدة مثلا وعليه فإن أي ترافيك يتعدى هذا المعدل سيتم حجبه فورًا.

- **بعض الخصائص المشتركة بين firewall & FortiDDOS**

باستخدام FortiDDOS هناك امكانية لوضع بعض rules على الترافيك الخاص بكل Layer 3,4 and 7 كما هو الحال في الفايرول0

Layer3 ACL- يمكن من خلالها التحكم فى أنواع معينة من الباكيت في الاتجاهين من وإلى الشبكة ويشتمل ذلك على :

Specific protocols
Fragmented packets
Specific source address
Specific countrie

مفيدة في حالة web server خلف fortiDDOS تستطيع فتح ICMP and TCP ومنع باقي البروتوكولات.

Layer 4 ACL-
Specific TCP ports
Specific UDP ports
Specific values of ICMP types/codes

على مستوى layer 3 كان من الممكن غلق بعض packets والسماح للأخرى ولكن باستخدام Layer4 ACL يمكننا إضافة رقم البورت وطبقًا للمثال السابق يمكننا إضافة port 80 ليصبح traffic TCP port 80 هو فقط المسموح به وماعدا ذلك فهو حتمًا ممنوع.

Layer 7 ACL- بإمكانك التحكم فيما يلي

Certain URLs
Hosts
Agents
Referes
Cookies

- **ما الفرق بين FortiDDOS ، IPS**

FortiDDOS أو أي NBA system آخر يعتبر في الأساس IPS ولكن يضع في المقام الاول معدل الترافيك بالإضافة إلى أن هذه النوعية من الأجهزة لا تعتمد في اكتشافها لحدوث attack على وجود attack signature ولذلك فإن الصفة الأساسية التي تميز هذه الأنظمة عن غيرها هي أنها غير معرضة لحدوث attack zero-day كما في حالة ips لو صادف attack جديد لم يسبق أن تعرض له بسبب أنه لا يوجد أي signatures فى ips database ينطبق عليها مواصفات هذا الهجوم. الأهم من ذلك أنه أحيانًا يتلاعب الهاكر بـ ips عن طريق توجيه هجوم من خلال ترافيك مضغوط ومشفر أو حتى مقسم إلى أجزاء عندها ينخدع ips ويسمح لهذا الترافيك بالمرور لأنه لا يمثل له أي ضرر ظاهري .

- **مراحل التشغيل**

هناك مرحلتين أساسيتين عند البدء بتشغيل FortiDDOS

1- مرحلة التعليم الأساسي initial learning period
هي مرحلة جمع المعلومات عن النظام المتواجد والمفترض أنه محمي بدرجة كافية وتستمر هذه

المرحلة من 2-14 يوم ويجب التأكد من عدم تعرض النظام لأي هجوم خلال هذه المرحلة لذلك نؤكد على ضروة أن يكون النظام محمي بأي طريقة آخرى .في هذه الفترة يتعرف الجهاز على طبيعة وحجم الترافيك اليومي في فترات الذروة كبداية الأسبوع وأيضًا في الإجازات حيث أنه لا يتدخل في منع أي باكيت من الدخول او الخروج وبذلك يكون كـ detection mode .

2 - مرحلة التعليم المستمر Continuous learning

بعد انتهاء المرحلة الأولى من التعلم ندخل في المرحلة الثانية والتي تعتبر بمثابة Prevention mode حيث تكون اكتملت الرؤية لدى الجهاز وبدأ بالتعرف على كل خفايا الشبكة وبإمكانه تحديد ما إن كان الترافيك المار خلال الشبكة في وقت معين طبيعى أم مثير للشكوك وبذلك فهو يضمن حماية تامة ومستمرة للشبكة «7/24» وبدون داعي لتدخل الادمن .

ماذا أيضًا؟

الكثير يعلم أن الهاكر بإمكانه استخدام بعض الأساليب لخداع security system أحد هذه الأساليب هو الخروج عن الشكل الطبيعي للباكيت بمعنى التلاعب بـ standards of protocols وهذا ما يعرف بـ network anomaly. يساعد FortiDDOS بالتعرف على مثل هذا النوع من الشذوذ عن المألوف على مستوى layer 3,4,and 7 لكل مما يلي:

* Header anomaly
* state anomaly
* rate anomaly

header anomaly-

وأتمنى أن تلتمسوا لي العذر لصياغتها باللغة الإنجليزية فجميعها أشياء من أساسيات النتوورك التي يصعب صياغتها باللغة العربية:

Layer 3 header anomalies

- IP Version other than 4 or 6
- Header length less than 5 words
- Incorrect header checksum
- Source or Destination address equal to Local Host (loopback address spoofing)
- Source address is equal to Destination (Land attack)
- End of packet (EOP) before 20 bytes of IPV4 Data
- Total length less than 20 bytes
- EOP comes before the length specified by Total length
- End of Header before the data offset (while parsing options)
- Length field in LSRR/SSRR option is other than (3+(n*4)) where n takes value greater than or equal to 1
- Pointer in LSRR/SSRR is other than (n*4) where n takes value greater than or equal to1
- For IP Options length less than 3

Layer 4 header anomalies

- Invalid TCP/UDP/ICMP checksum
- Invalid TCP flag combination
- Urgent flag is set then the urgent pointer must be non-zero
- SYN or FIN or RST is set for fragmented packets
- Data offset is less than 5 for a TCP packet
- End of packet is detected before the 20 bytes of TCP header
- EOP before the data offset indicated data offset
- Length field in Window scale option other than 3 in a TCP packet
- Missing UDP payload
- Missing ICMP payload

Layer 7 header anomalies

- Undefined opcode in HTTP header
- Unknown opcode in HTTP header
- Invalid HTTP version

2-TCP state anomaly

يستطيع منع أي باكيت خارج TCP window الخاصة بالمستلم أو منع أي باكيت لا تنتمي لـ TCP connection موجود بالفعل. جدير بالذكر أن FortiDDOS لديه القدرة على تخزين مليون TCP connections في نفس الوقت على الذاكرة الداخلية الخاصة به. وغيرها الكثير لكن الأكثر تخصصًا في هذه النقطة هو stateful firewall .

3-Rate anomaly

وهو الهدف الأساسي الذى يركز عليه fortiDDOS كما سبق وتحدثت عنه.

fortiDDOS family* حيث أن هذا المنتج يعتبر حديث الإصدار فهو لا يوجد منه الا 3 موديلات جميعها مشتركة فى آلية العمل ولكن بإمكانيات متفاوتة.

1-FortiDDOS 100A

2 LAN Interfaces (Copper/SFP), 2 WAN Interfaces (Copper/SFP) Total Network Interfaces
1X1TB HDD Total Storage Capacity
1 Gbps Throughput

2- FortiDDOS 200A

4 LAN Interfaces (Copper/SFP), 4 WAN Interfaces (Copper/SFP) Total Network Interfaces
2TB (1TB HDD x2) Total Storage Capacity
2 Gbps Throughput

3- FortiDDOS 300A

6 LAN Interfaces (Copper/SFP), 6 WAN Interfaces (Copper/SFP) Total Network Interfaces
2TB (2 x 1TB HDD) Total Storage Capacity
3 Gbps Throughput

شهادات الحماية
SSL Certificate

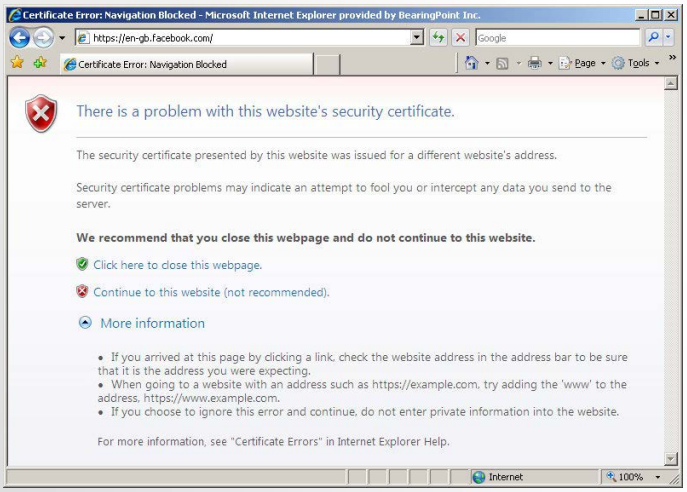
تكلمت في مقالات سابقة عن مواضيع تم الذكر فيها عن ضرورة إنشاء ssl certificate
ولكن في هذا العدد سوف اتطرّق لشرح شهادة الحماية أوماتسمى بـ ssl ومالفائدة منها أيضاً .

لنعد قليلاً إلى مقالات سابقة حيث تم الحديث عن خدمة الـ RPC والتي تؤمن لي الوصول من بعيد للخدمات التالية:
Exchange، ActiveSync، Outlook Web App
Outlook Anywhere، Web Services

ولكن لم أذكر كيفية إنشاء شهادة الحماية وربطها مع Exchange Server وهو الذي سوف يكون محور موضوعنا.
عندما يكون لدينا Exchange Server (بريد داخلي) الذي يعتبر من الخدمات الداخلية، أي أنه فقط في الشركة ، وبالخدمات التي تم ذكرها نؤمن الوصول من بعيد لاستخدام البريد الخاص بالشركة.

الهدف أولاً من إنشاء الشهادة :
- معرفة إن كان المستخدم يستحق الثقة، أي يستطيع استخدام Exchange Server من خارج الشركة أم لا.

ملاحظة :
- معظمنا ينتبه عند تصفحنا لمواقع يتم فيا ذكر اسم مستخدم أو كلمة مرور نلاحظ في مكان العنوان خط أحمر ونلاحظ أنه أصبح الرابط يبدأ بـ Https في هذه الحالة أعلم أنك تستخدم ssl



- تستخدم الـ SSL مع جميع برتوكولات Exchange Server ماعدا : IMAP , POP3 أي ليسوا آمنين .

أنواع SSL والفرق بينهم :
1 - self-signed SSL certificate : تتميز بأنها آلية و لا تحتاج إلى أي خبرة أو مجهود ولها ميزة أخرى أنها ليست مكلّفة . ولكن ماهي عيوبها ؟
- لايمكن تطبيق Outlook Anywhere معه.
- ليست آمنة.
- يجب على المستخدم عندما يقوم بالدخول إلى صفحة الإيميل الخاص بالشركة أن يقوم بتثبيتها

بنفسه (توقع وجود مستخدمين لا يملكون أي خبرة بمجال التعامل مع الكمبيوتر).

2 - public-key infrastructure : ويطلق عليها اختصاراً PKI)المفتاح العام (وهي أن يقوم قسم ال IT الخاص بالشركة بصناعة شهادة خاصة بالشركة بنفسهم، من باب التوفير، ومن باب زيادة الحماية ولكن من مشاكل هذه الخطوة :

- العملية صعبة جداً وليست بالأمر السهل.
- وبالنهاية توجد نفس المشكلة السابقة على المستخدمين تثبيت الشهادة بنفسهم.

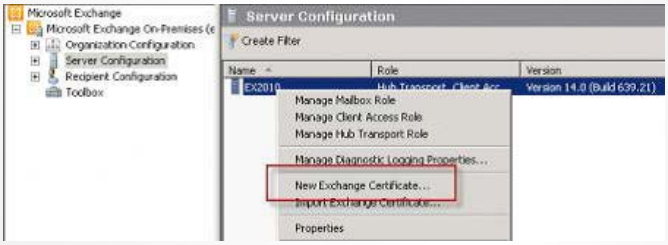
3 - Trusted CA : وهي شراء شهادة جاهزة من موقع معترف به وموثوق و يوجد العديد من المواقع التي تقوم بهذه الخدمة منها GoDaddy- Digicert : .

- وتتمز هذه الطريقة:
- بأنها الأشهر.
- أكثر أماناً .
- لا تحتاج إلى خبرة المستخدم في تطبيقها .
- يتم إدارة الشهادات المنشأة والتعديل عليها من الـ IIS .
- كيفية صناعة الشهادة في Exchange Server 2010

على سبيل المثال لدينا الدومين التالي:
Networkset.net

1 - ندخل Exchange Server 2010 ثم :

Exchange Management Console ☞ Server Configuration ☞ (Right Click) ☞ New Exchange Certificate



2 - ندخل اسم الشهادة الذي نريده مثلا : RPC Networkset exchange

3 - ثم التالي وبعدها سوف يتم تفعيلها وإضافتها على الخدمات التالية :

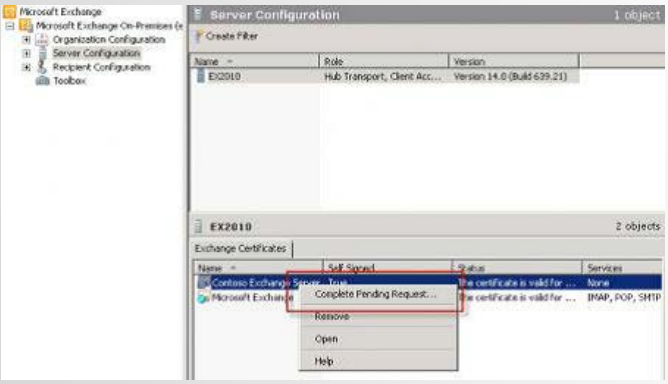
Outlook Web App , ActiveSync , Exchange Web Services , Outlook Anywhere

4 - ثم تظهر لدينا حقول من أجل تعبئة معلومات الشركة وهي معلومات روتينية ولاتفيد، ومكان تخزينها والمكان اختياري.

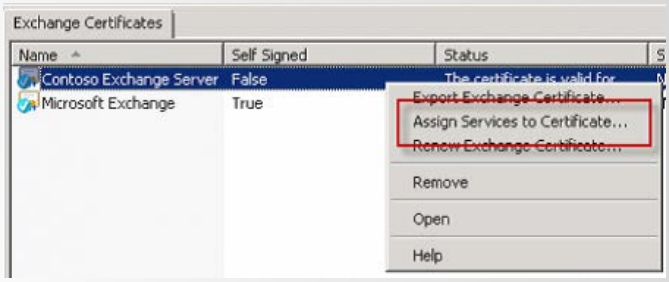
5 - الآن نكون قد انتهينا من إنشاء الشهادة من خلال Exchange.

6 - أما تفعيل الشهادة من :

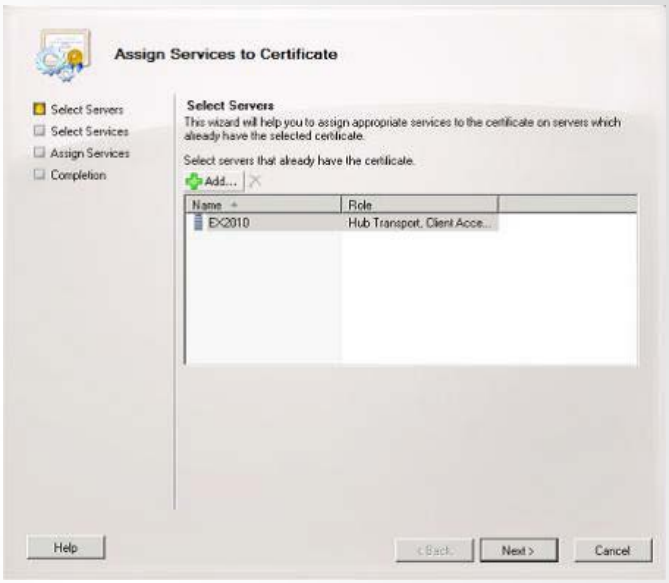
Exchange Management Console ☞ Server Configuration ☞ (RightClick) ☞ Complete Pending Request



7 -تحديد مكان حفظ ملف ثم OK
8 -الآن نريد ربط هذه الشهادة بالخدمات التي لدينا من خلال :



9 - اختيار السيرفر:

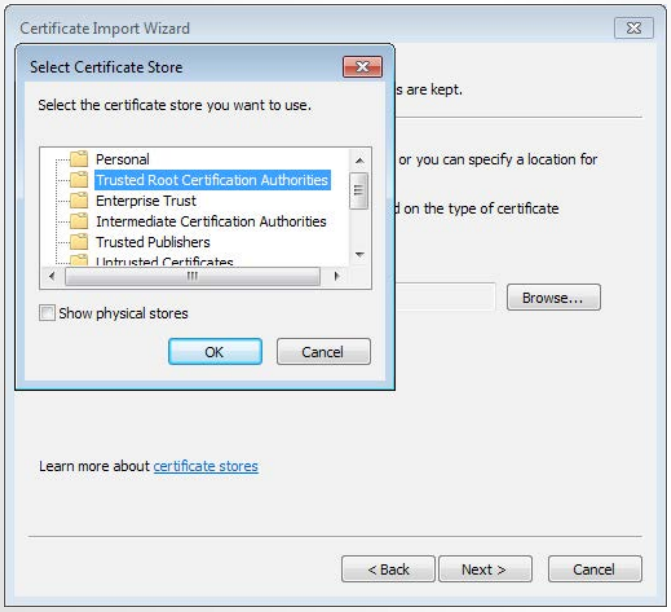


10 - Next وبعدها Complete

وبهذه الحالة أصبح لدينا شهادة خاصة بالخدمات الموجود في Exchange من أجل الدخول الموثوق الآمن إلى بريد الشركة من خلال تنصيب الشهادة على الأجهزة التي تريد بأن تعمل خارج الشركة والدخول إلى داخلها .

- عملية تنصيب الشهادة على الحاسب :

عند إنشاء الشهادة نستطيع تصديرها لملف يتم جهاز المستخدم بأن يفهمها ليتم تنزيلها ووضعها في Trust Root Certification .



وبالنسبة لاستيراد الشهادة إلى أنظمة الهواتف النقالة : IPhone, Android , symbian الاستيراد تلقائيًا عند تعريف بريد جديد لك .

Windows Phone يجب تنزيل الشهادة على الجهاز يدوياً.

WIRELESS CUSTOMER QUESTIONNAIRE

تعتبر أول خطوة في عمل شبكة لاسلكية هي تحديد متطلبات العميل عبر توجيه الأسئلة إليه، فمجرد اتصاله بك و اخبارك بأنك المناط بك عمل الشبكة فلابد أن تعرف ماذا يريد و أين و كيف.

و في حالة قيامك بعمل الشبكة نتيجة فوز الجهة التي تعمل بها بمناقصة تمديد شبكات لاسلكية فإن متطلبات العميل ستجدها موجودة في كتاب المواصفات و لكنها ليست تفصيلية و غير كافية للبدء في عمل الشبكة فهو فقط يحدد في مواصفاته الخدمات التي يريدها و الأجهزة التي يرغب بتواجدها و الأماكن التي ستقوم بعمل فيها الشبكة مع تحديد آليات عمل التشغيل و الصيانة و غيرها من الأشياء الإدارية و يترك لك أنت تحديد طوبولوجية الشبكة و كيفية توزيع الأدوار على الأجهزة. بل أنت من يحدد أنواع الأجهزة و الشركات المصنعة لها و لذلك فإنه بمجرد بدء العمل لابد أن تكثّف جلساتك و حواراتك مع العميل لمعررفة متطلباته جيدًا.

فلكل مؤسّسة أو شركة متطلبات محددة لعمل شبكة لاسلكية بعض هذه المتطلبات يستطيعون التعبير عنها و يعرفونها و بعضها قد لا يعرفونها و ستعرفها عبر مناقشتك لهم. لذلك في غالب بل كل الشبكات اللاسلكية أو اللاسلكية تتغير وجهة نظر العميل عند مناقشته للجهة التي ستصمّم و تنفّذ مشاريع شبكيّة فربما يريد تصميم معين و تقنعه أنت بتصميم أفضل، و ربما يريد نوعية أجهزة معينة و تقنعه أنت بنوعية أفضل و قد يحتاج فقط شبكة نقل بيانات وانترنت فقط و تقنعه أنت بسهولة عمل شبكة هاتف عبر شبكة الوايرلس VOIP .

و لذلك فأنت مضطر أن تسأل كثيرًا جدًا و تستفسر عن كل صغيرة و كبيرة و تتجول في كل مكان يحتاج توصيل شبكة لاسلكية له و هذا ما سنتكلم عنه هنا و هو تحديد متطلّبات العميل في الشبكات اللاسلكية عبر سؤاله Customer Questionnaire وهي إحدى مراحل ما قبل تخطيط الشبكات اللاسلكية Pre-Site Survey و يعتبر جزء من أحد فصول منهج تخطيط الشبكات اللاسلكية في تراك CCNP Wireless و هو حقيقة أمتع منهج في الشبكات اللاسلكية عمومًا.
و سنتعرف هنا على أهمية توجيه الأسئلة للعميل و

توصيف التطبيقات التي تستطيع أن تتحملها الشبكات اللاسلكية مع موائمة الشبكة اللاسلكية و ربطها مع الشبكة الحالية للعميل.

و العميل هو ذلك الشخص أو الجهة التي ستأخذ منها مالاً لتنفذ أعمالاً محددة و هذه الأعمال له فيها وجهة نظر و لك أيضا وجهة نظر قد تكون وجهتي نظرتكما مختلفتان و قد تكون متفقتان، و قد يكون هناك نقاط خلاف و اتفاق، و دائمًا ما يبدأ العمل و ليس هناك نقاط خلاف إطلاقًا و هذا سينشأ بالحوار و تعدد الأسئلة.

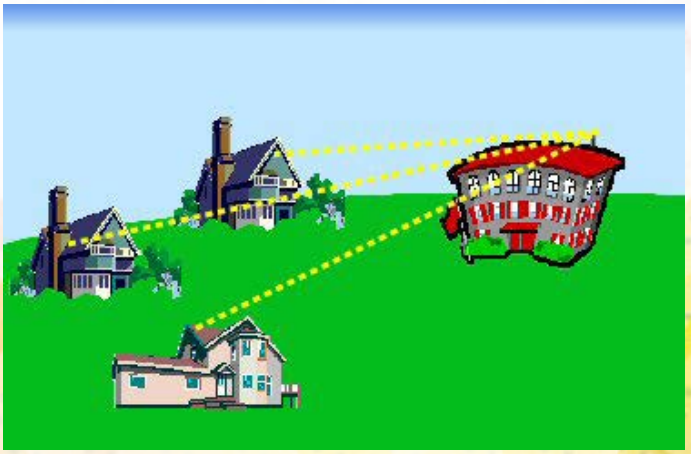
إذن فأول وسيلة للوصول إلى متطلبات العميل هي الأسئلة Customer questionnaire

ما هي وسيلة الإتصال بالعميل ؟

أول سؤال تحتاج إجابته من العميل سواءً كان مؤسسة صغيرة أو كبيرة أو شخص هو عن الطريقة التي ستتبادلون بها ما يتعلق بأعمال الشبكة من ورقيات و مخططات و غيرها.

فمن غير الممكن أنه كلما احتجت منه سؤالاً أو احتاج منك عملاً أن يعقد اجتماع فهناك أشياء تستطيع أن تنهيها بالهاتف أو عبر الإيميل.

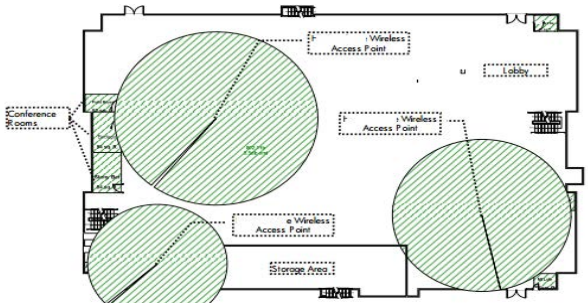
كم عدد المواقع التي سيتم ربطها لاسلكيا ؟



يكون هذا السؤال غالبًا عند عمل شبكة لجهة صغيرة حيث أنك لو كنت قد استلمت العمل عبر مناقصة فإن هذا السؤال ستكون إجابته في كتيب المناقصة الذي استلمته من قبل و إجابة هذا السؤال سيتحدد معه غالب التكلفة الكلية للشبكة و التي ستحمل على عدد الأجهزة التي ستتواجد في هذه الأماكن.

كذلك سيحدد ذلك طبيعة ربط المواقع هل سيتم ربطها لاسلكيًا بشبكة لاسلكية خارجية؟ أم سيتم الإتصال بينها وبين إدارتها عبر WAN؟ و ما يستلزم ذلك من توفير أو إنشاء خدمة WAN مثل DSL أو VPN MPLS أو Frame relay أو أنه سيتم تمديد كابلات فايبر لربط هذه المواقع عبر شبكة إيثرنت سريعة Metro Ethernet

ما هي طبيعة أو طبولوجية الموقع ؟

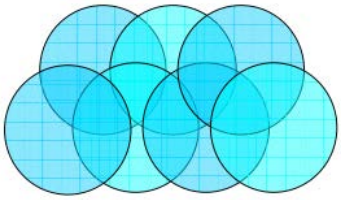


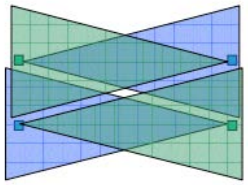
الشبكات اللاسلكية لا تفضل كثرة العوائق و المباني في الموقع و لذلك فإن تصميم الشبكة يأخذ في الحسبان تمامًا عدد المباني و شكلها و توزيعها و لذلك فأنت تحتاج مخطط تفصيلي لمباني كل موقع موضح عليه الأبعاد لترى أين ستضع أجهزتك و كيف ستستمد الطاقة الكهربية و هل ستحتاج إلى أجهزة أكسس بوينت داخلية indoor أم خارجية outdoor كذلك سيتم تحديد عدد الخلايا و مداها و القنوات الترددّية التي ستوجد بها.

كم عدد المستخدمين و المستفيدين و صلاحياتهم في الشبكة ؟

هذا السؤال سيفيديك في تحديد عدد أجهزة الأكسس بوينت و كثافة توزيعها و تحديد عدد VLAN التي ستستخدمها و صلاحية كل مجموعة في كل VLAN كذلك سيعوزك هذا إلى احتمالية استخدام سيرفرات ولوج أو أجهزة ولوج لاسلكية مع ربطها بسيرفر Active Directory .

ما هو نطاق الشبكة اللاسلكية ؟





لن تصل إشارة الشبكة اللاسلكية إلى جميع المستخدمين بنفس القوة فعند عمل شبكة بمعدل نقل بيانات معين فإن القريبين من الشبكة سيستفيدون من هذه السرعة و تبدأ السرعة في الخفوت كلما ابتعدت عن مصدر الإشارة

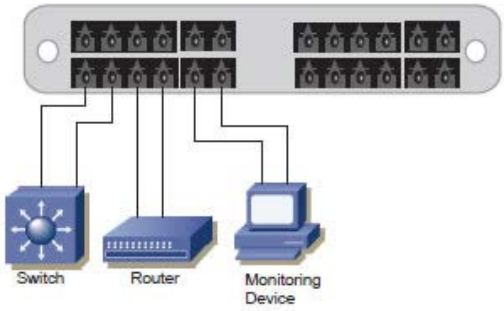
و هو ما يسمى بالمعدل الفعلي لنقل البيانات أو الإنتاجية اللاسلكية throughput و لذلك فأنت ستحتاج إلى وضع مصدر بث الإشارة هوائي أو أكسس بوينت بالقرب من الجهة ذات الفضلية العليا للإستفادة من الإشارة و كذلك استخدام معيار لاسلكي ذو معدل نقل بيانات عالي مثل 802.11n الذي يصل معدل نقل البيانات فيه إلى 600 Mbps

كذلك قد يعوزك استخدام هوائيات أو مكررات لنقل الإشارة إلى أماكن أبعد و سيحدد شكل المكان نوع الهوائي فإن كان دائري أو مربع ستحتاج إلى هوائي omnidirectional لتوزيع الإشارة في جميع الإتجاهات و إن كان طرقة أو طريق ستحتاج إلى هوائيات high directional و هكذا.

ما هي طريقة التأمين المفضلة ؟

يتراوح التأمين بين شبكة مفتوحة أو مشفرة بـ WEP ثم WPA ثم استخدام سيرفرات خاصة بالتأمين فهناك أماكن لن تحتاج الي تأمين بيانات الشبكات اللاسلكية مثل أن تقوم بعمل شبكة انترنت لاسلكية في مقهى أو مطار أو مكان خدمة عامة و هنا ستخسر عملك لو ضايقت المستخدم بطلب كلمة مرور و هناك أماكن أخرى سيحتاج العميل أن يكون حازمًا في أمر التأمين و التشفير مثل الشبكات اللاسلكية في شركة ذات صلاحيات متفاوتة أو عمل شبكة لاسلكية في عمارة.

ما هي الشبكة القائمة حاليا ؟



إنه الصداع الأكبر في دماغ المصمّم حيث أن شبكات سيسكو اللاسلكية لها متطلبات خاصة في الشبكة الموجودة لأنها و بوضوح ليست شبكة لاسلكية كاملة بل إن سيسكو تطلق عليها شبكات لاسلكية على أساس أن ولوج المستخدمين إليها لاسلكيًا أما الأكسس بوينت فهو متصل سلكيًا UTP بسويتشات لأخذ اعداداته و الطاقة الكهربية عبر POE و هذه السويتشات متصلة جميعًا بسويتش مركزي عبر كابلات فايبر أو UTP و هذا السويتش المركزي متصل سلكيًا فايبر أو UTP بفتحة توزيع في جهاز الكنترولر و الذي يحوي عدة فتحات توزيع كل منها متصل بالشبكة بنفس الترتيب هذا.

و هذا الكنترولر و عشرات أو المئات غيره متصلين سلكيًا عبر WAN بسيرفر WCS و الذي يتحكم فيهم جميعا.

إذن فأنت تحتاج إلى شبكة بها سويتشات POE و تعمل بسرعات أقلها الجيجا إيثرنت و كابلات فايبر و موائمات لها و يصعب أن تجد شبكة بها هذه المتطلبات حاليًا. و لهذا، عند تقديم عرضك لعمل هذه الشبكة لا تقدم عرض بتوفير أكسس بوينت و كنترولر فقط بل تقدم كل ما تحتاجه الشبكة من كابلات و كبائن و سويتشات و غيرها و الذي سيكون أضعاف أجهزة الشبكة اللاسلكية.

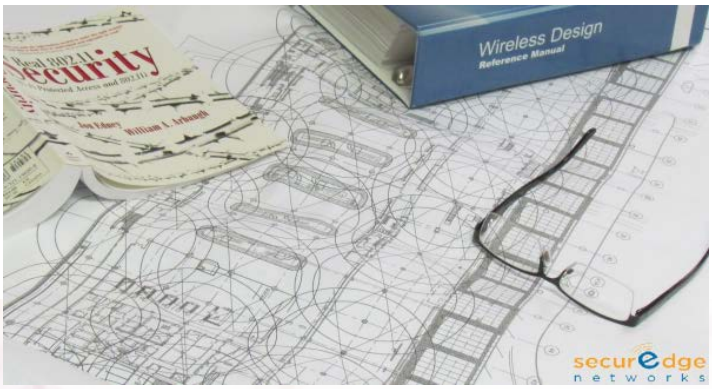
هل هناك أجهزة لاسلكية في نطاق الشبكة التي ستقام ؟

لابد من معرفة هل لدى العميل أجهزة تساعده للدخول للشبكة؟ أم أن الموقع سيحتاج أجهزة؟ أم أن الأجهزة ستحتاج فقط ترقية بإضافة كروت لاسلكية؟

و من ناحية أخرى، هل المعايير اللاسلكية التي ستوجد في الشبكة ستدعم المعايير اللاسلكية الموجودة في هذه الأجهزة؟

أيضا، هل يريد دعم الاتصال من خلال أجهزة PDA؟ و كذلك دعم خدمات الصوت عبر الشبكة VOIP.

هل لدي العميل مخططات حديثة للمكان ؟

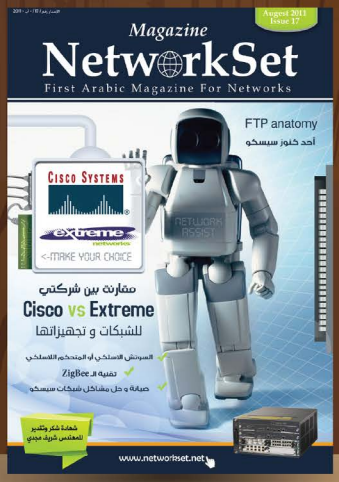


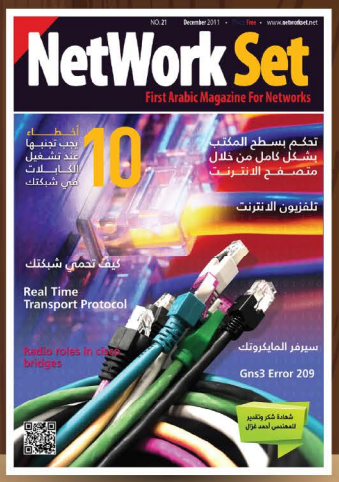
المخططات الهندسية سلاح قديم للمهندسين على اختلاف أنواعهم و في الشبكات اللاسلكية سيكون المخطط ملازمًا لإدارتك للشبكة اللاسلكية حيث ستحتاج البرمجيات التي ستدير و تراقب الشبكة مثل AirMagnet Survey و برنامج سيسكو WCS مخططات شاملة للمواقع لبيان أماكن الأكسس بوينت و لأغراض أمنية و تنظيمية أخرى.

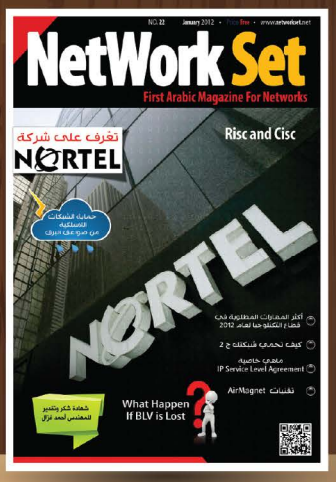
و ستكون مضطر لعمل هذه المخططات إن لم تكن موجودة. بل ربما تحمل على المناقصة و هناك برمجيات تساعدك في هذا مثل MS Visio و الأوتوكاد و غيرها إلا أن اختيارك للبرنامج الذي سيدير الشبكة ستراعي فيه استخدام برمجيات الرسم لتعامله مع امتدادات خاصة أو تقوم بتحويل أنواع الملفات إلى أخرى. فمثلاً بينما يتعامل WCS مع ملفات بنوع JPEG GIF CAD PNG JPG و غيرها فإن Airmagnet يتعامل مع BMP DIP DWG DXF EMF VSD و غيرها.

انتهت المقالة لكن لم تنتهي الأسئلة و أنت و شطارتك فكل سؤال ستستخرج منه إجابة جديدة سيسهل عليك الكثير في عمل الشبكة و سيجعل العميل أكثر رضًا عن هذه الشبكة .

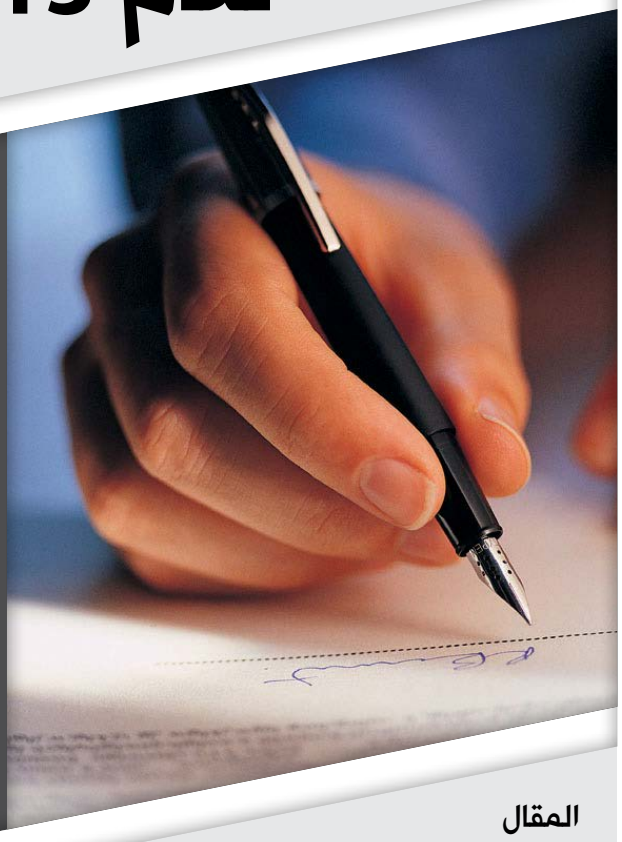
Network Set Magazine Gallery







أكثر الشهادات التقنية طلباً لعام 2013



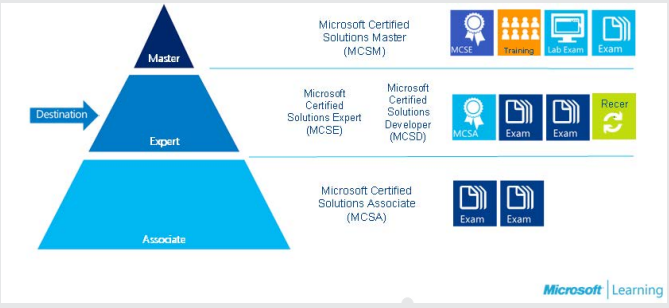
قبل حلول عام 2013 بأيام قليلة وصلني عبر البريد الألكتروني تصنيف لأهم الشهادات التقنية الخاصة بعالم الـ IT من موقع TechRePublic الشهير بمقالاته وأطروحاته في مجال الـ IT بشكل عام، ومن هنا وجب الإشارة إلى أن هذا الترتيب لم يأتي من مخيّلتي أو من اطلاعي على الساحة العملية للواقع العربي وقد تستغرب لو قلت لك أن بعضًا من هذه الشهادات لن يصل إلى العالم العربي قبل عدة سنين فهو مبني على نتائج غربية خالصة 100 ٪ لكن باعتقادي أن الإنسان الناجح والذي يفكر بالمستقبل ويفكر في كيفية التميّز العلمي، سوف يفيه الترتيب وسوف يحرص على متابعة ودراسة أحد هذه الشهادات التي أعتبر بعضًا منها (الشهادات التي اطلعت عليها) شهادات في غاية الاحترام كما سوف نرى وقبل أن أبدأ في مقدمتي حول أكثر الشهادات طلبًا وجب الإشارة إلى أن المقال لن يكون مترجمًا بل مصاغا بطريقة جديدة وكاملة إعتمادًا على المعلومات التي أجمعها من كل شهادة.

المقال كما قلت فرصة لك لكي تبدأ بوضع أهدافك لعام 2013 من خلال استهداف بعض الشهادات التي تنمّي من مستوى معرفتك وتزيد من قدراتك العلمية وتحسن من فرص حصولك على فرص وظيفية، فعادة مايواجه الطلاب والدارسون تحديًا كبيرًا في اختيار أفضل وأهم الشهادات التقنية المفيدة المطلوبة لعام 2013 لكن بعد هذا المقال لن تقلق بهذا الخصوص فالباحثين والخبراء والمتابعين للساحة العملية وضعوا لك أفضل وأكثر خمس شهادات مطلوبة لعام 2013

ومن الضروري أن تعلم أن الترتيب لايعني أي شيء ولايعطي أي أولوية بين الشهادات :

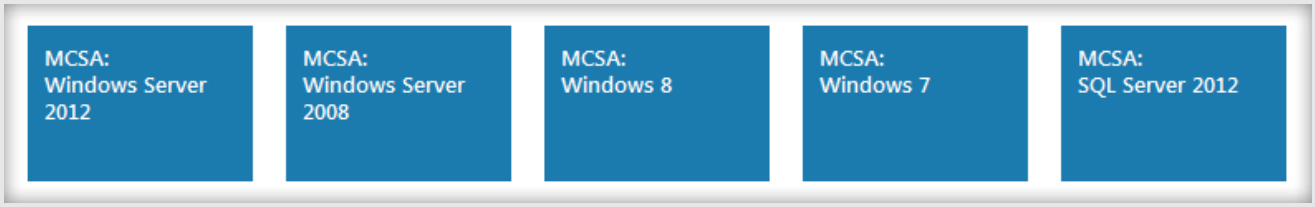
MCSA
(Microsoft Certified Solutions Associate)

هل أستغربت مثلي للوهلة الأولى وأنت تقرأ MCSA ؟ الحقيقة أول لحظة قرأت أسم هذه الشهادة في هذا المقال قلت في نفسي هناك خطأ، لكن ما أن تعرفت على التعريف الكامل لأسم الشهادة حتى أدركت أن مايكروسوفت بدأت تطور من نظام الشهادات لديها وبدأت تعتمد على نظام سيسكو (النظام الهرمي) فالآن لدى مايكروسوفت ثلاث مستويات وهي Associate, Expert, Master ولو أمدنا الله بالعمر والقوة فسوف يكون لي مقال احترافي حول التطورات التى حصلت في عالم مايكروسوفت.



ملاحظة: ربما تكون هذه التعديلات جديدة بالنسبة لي فأنا غير متابع لسوق الشهادات التقنية وبالأخص مايكروسوفت.

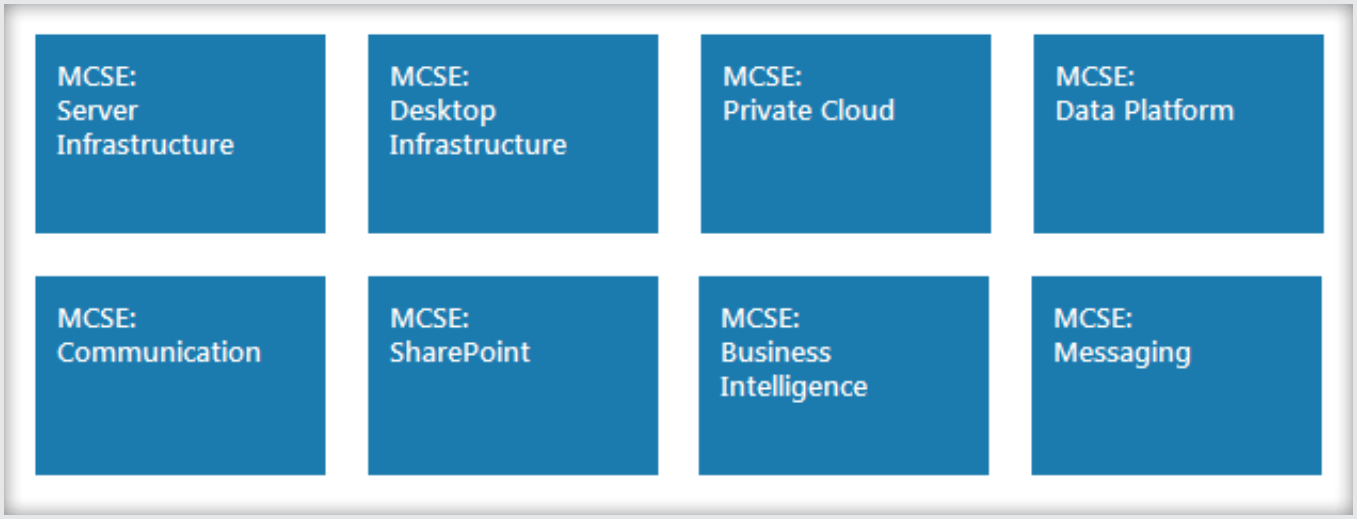
الـ Associate بالنسبة لمايكروسوفت سوف تكون أكثر تعقيداً من نظام سيسكو فالأخير كان عبارة عن امتحان واحد كافي للحصول على المرحلة الأولى لكن مع مايكروسوفت سوف تحتاج إلى عدة امتحانات لتحصل على احدى شهاداتها، لشهادة الـ MCSA الجديدة هناك خمس خيارات وهي :



لكل شهادة هناك عدد معين من الامتحانات فعلى سبيل المثال الـ MCSA 2008 or 2012 تحتاج منك امتحان ثلاث شهادات للحصول عليها وبعدها سوف تكون مؤهل للحصول على الـ MCSE بينما شهادة Win 7 or 8 تملك امتحانان فقط.

MCSE
Private Cloud

الـ MCSE أو Microsoft Certified Solutions Expert متواجدة معنا أيضا في هذا المقال، للـ MCSE هناك ثماني شهادات مختلفة والتي هي امتداد للشهادات التي رأيناها في الـ MCSA وهي موضحة بالصورة التالية :



لكل شهادة من الشهادات المذكورة هناك مراحل وامتحانات يجب خوضها وتعلمها لكن سوف نركز على واحدة من تلك الشهادات الثمانية وهي شهادة MCSE Private Cloud, للحصول على هذه الشهادة يجب خوض خمس امتحانات مختلفة على مستوى ويندوز سيرفر 2012 وهي على النحو الآتي :

1	Installing and Configuring Windows Server 2012	410	Microsoft CERTIFIED Solutions Expert Private Cloud
2	Administering Windows Server 2012	411	
3	Configuring Advanced Windows Server 2012 Services	412	
4	Monitoring and Operating a Private Cloud with System Center 2012	246	
5	Configuring and Deploying a Private Cloud with System Center 2012		

وتأتي أهمية الكلاود في الوقت الحالي مع التنامي الكبير لحجم الطلب التي بدأت تفرضه الشركات الكبيرة لأحداث غيمات خاصة لكل شركة إعتمادًا على المصادر الموجودة لدى تلك الشركات، دخول مايكروسوفت إلى جانب بعض الشركات مثل كومبيتيا وشهادة CCP المقدمة من شركة cloudschool أضاف للكلاود تحديات ومهارات جديدة يمكن لأي متخصص اكتسابه بحصوله على تلك الشهادات الأحترافية والتخصصية

PMP
(Project Management Professional)

ربما يتخيل إليك بأن شهادة مثل PMP بعيدة كل البعد عن مجال الـ IT إلا أن الواقع العملي الغربي والعربي مغاير تمامًا لهذه الحقيقة، فلقد أصبح الطلب على هذه الشهادة كبيرًا جدًا وخصوصًا على الساحة العربية التي بدأت دخول مجالات تقنية واسعة ومن الضروري لأي مشروع كبير أو متوسط وجود مدير يشرف عليه يديره بالطريقة الصحيحة من خلال وضع

خطة العمل المتكاملة التى تضمن للمشروع بأن يسير بشكل منظم ومنتظم مراعيًا المدخول المالي والمصادر المتاحة لميزانية الشركات المديرة لأي مشروع.

الـ PMP تمدك بمهارات كثيرة جدًا وربما لايسعني أن أذكرها لك في مقال واحد ولن أبالغ لو قلت لك أن تأثير هذه الشهادة على حياتك الشخصي سوف يكون موجودًا أيضا، فهي تعلمك إدارة وقتك وعملك وحياتك وتساعدك على التقليل من الكلفة المترتبة على أي مشروع وتساعدك في الاستفادة من مصادرك الموجودة بشكل أكبر ولن تتخيل حجم شهادة مثل هذه كيف يمكنها أن تضفي على سيرتك الذاتية من قوة معنوية عند التقديم لأي وظيفة في العالم أجمع فهي تصنف من بين الشهادات الأكثر احترامًا في العالم وحاملها يعتبر شخص مختلف عن أشخاص كثر لكن تبقى المشكلة في هذه الشهادة أنها ليست من النوع الذي تستيقظ يومًا ما وتقول أريد أن أكون PMP !!!, لا أبدًا فأي شهادة تحظى باحترام واسع في العالم تحتاج إلى متطلبات لا يقدر الجميع على تأمينها وأولها هو وجوب وجود 4500 ساعة في مجال إدارة المشاريع.

VCP
(VMware Certified Professional)

في الدراسة الأولى التي قدمناها على NetworkSet أحتلت هذه الشهادة المركز الرابع في الترتيب لأكثر الشهادات طلباً على الساحة العربية كما حصلت على موقع بحسب دراسة 2012 لأكثر الشهادات طلبًا وها هي تعود مجددًا في عام 2013 لتثبت نفسها. تعتبر هذه التّكنولوجيا بمثابة اختراع، فالمصنّعون شغْلهم الشّاغل هو

تصنيع سيرفرات أسرع وأسرع، يمكنها تخزين الكثير من الداتا ومع ذلك نجد الكثير والكثير من هذه السيرفرات يوجد فى الداتا سنترز ومع ذلك لا تحمل سوى كسور بسيطة من سعتها التخزينية الافتراضية التي تتيح استخدام أكثر من سيرفر افتراضي على نفس السيرفر الحقيقي، سوف تستمر فى التّطور والزيادة فى الأهمّية ما دامت المؤسّسات مهتمة بتحسين استثمار السّعات التّخزينيّة للسيرفرات الحقيقية.

VMWARE تعتبر من أهم أنواع السوفت وير المستخدمة في تكنولوجيا الـ Virtualization إن لم تكن هي الرائدة فى ذلك. حصولك على هذه الشهادة يعطى صاحب العمل الثّقة الكبيرة فى قدرتك الحالية والمستقبلية في تصميم وبناء وتشغيل بيئة متكاملة من السيرفرات الإفتراضية باستخدام الـ vmware .أيضًا إذا تحدثت مع أي شخص مسؤول عن أي داتا سنتر سوف تكتشف مدى أفضلية الـ vmware على Microsoft's Hyper-V ولكن هذا لا يمنع من وجود بعض المحترفين فى هذا المجال والذين يفضلون حلول ميكروسوفت على أساس أنها تحسن من الأداء وتساعد فى سد الفجوات .

CISSP (Certified Information Systems Security Professional)

يتوجب على أي شركة أو منظمة حماية أنظمتها، وتأمين بياناتها وإغلاق أكبر قدر ممكن من الثغرات المتاحة في شبكاتها، ومن هنا دائما تأخذ المساحة الأمنية لأي شركة مكانة كبيرة وتأتي شهادة الـ CISSP لتضع نفسها من بين أكثر الشهادات الأمنية طلبًا والتي أعتبرها (رأي شخصي) المكان الأفضل لكي يبدأ أي شخص طريقة في أمن المعلومات مع مراعاة الأساسات العلمية، الشهادة لا تركز على أي منتج أو جهاز في العالم بل تركز في طريقة التفكير نفسه، كل تركيزها يتمحور حول الأمن العام للشركة بكل أشكاله، فهي مادة نظرية بامتياز وقد يزعجك هذا جدا في البداية وخصوصًا المهندسين الذين تعودوا على أوامر أو صور أو أي تطبيق عملي على الشيء الذي يتعلموه.

الشهادة أعتبرها مثل السهل الممتنع معقدة لكن تبني فيك الرجل الأمني المثالي القادر على السيطرة على أكثر الثغرات الأمنية ضيقًا، الازدياد هذا العام على شهادة الـ CISSP هو نتيجة تحول الكثير من الشركات إلى تقنية الـ Cloud ووجود خبراء CISSP سوف يزيد ويعزز من ضمان آمن هذه المعلومات هناك. الشهادة في قمة الاحترام ومن خلال متابعتي لمؤشر الرواتب العربي والغربي أجد أن الشهادة مؤشراتها دائمًا في ارتفاع لكن كما أقول دائما الاحترام والراتب العالي لأي شهادة يكون مبني على أمور تصعب توفرها. فعدا عن صعوبة دراسة تلك الشهادة سوف تجد المتطلبات القانونية تقف أمامك والتي أهمها هو وجود خبرة لاتقل عن الخمس سنوات في مجال أمن المعلومات وبضمان شخص يحمل نفس الشهادة.

ربما يتفجئ البعض من عدم وجود سيسكو على ساحة اكثر الشهادة طلبا لعام 2013 وهذه نتيجة طبيعية لأي متابع ميداني للواقع العملي والتي تحدثت عنه كثيرا، سيسكو لا أحد يعلوا عليها في ساحة الـ IT لكن عندما يزيد عدد الحاصلين على شهاداتها عن عدد الوظائف المتاحة سوف نجد أن الطب سوف يقل عليها . زد على ذلك دخول الكثير من الشركات التقنية مجال المنافسة مع سيسكو التى ظلت حتى 2004 تقريبا بدون منافس قوي وصريح لكن الآن هناك جونيبر وهواوي وافايا واتش بي وشركات أمنية بأعداد مهوولة، كل هذه الأمور أضعف من سوق سيسكو على الساحة العالمية، ولهذا السبب قررت الكتابة عن هذا الأمر وخصوصًا أني لاحظت أن لعام 2013 نكهة جديدة بدخول شهادات في مجال الكلاود والفيرتوال ساحة المنافسة. أتمنى أن تأخذوا هذه النصيحة بشكل إيجابي وأن لاتنسونا من دعواتكم ودمتم بود.

طريقك إلى عالم التكنولوجيا التخيلية

من خلال كتاباتي في المجلة والمدونة الخاصة تردني أسئلة كثيرة من المهتمين بالتكنولوجيا التخيليّة وأغلب الأسئلة تتعلق بكيفيّة الدّخول إلى هذا العالم الجديد وما هي الكورسات التي نحتاجها وترتيبها وشهادتها وأي منتج نقوم بدراسته وغيرها من الأسئلة.

لذلك سوف أخصص مقالي لعمل طريق وخطوات الدخول لهذه التكنولوجيا.
ولكني لن أقوم هنا بالتعريف بهذه التكنولوجيا لأنها أصبحت معروفة وإن لم تكن ملم بماهية هذه التكنولوجيا يجب عليك التعرف عليها أولاً .

أولاً : ما هي المتطلبات العلمية التي يجب أن تتوفر للشخص الذي يريد أن يدخل هذا المجال؟

يجب عليك إن أردت أن تدخل هذا المجال أن يكون لديك دراية بهذه التكنولوجيا بشكل جيد لأنك سوف تستخدمها في عملك وتعتمد عليها:

1 - IP Address
2 - DNS – DHCP
3 - Active Directory
4 - Network Infra
5 - Backup Solution
6 - Basic of Security

ثانيا: يوجد الكثير من الشركات تقدم تطبيقات لهذة التكنولوجيا مثل (VMware – Citrix – Microsoft) اتعلم أيهم ؟

الثلاثة يعملون فى هذا المجال وهم يتنافسون بشكل قوي فيما بينهم، لكن في السوق وفي الطلب على العمل يكون الطلب على المتخصصين فى تكنولوجيا الـ VMware لأنها أقواهم وتسبقهم في التكنولوجيا والدعم .
لكن لا تقلق عندما تكون متمكن من إحدى هذه المنتجات وتعمل عليها بشكل جيد يمكنك العمل على منتجات الشركات الأخرى بشكل معقول لأن الأفكار قريبة من بعضها أما الاختلاف فهو في الشكل والخطوات.

ثالثا: ما هي الكورسات المطلوبة لكي تتعلم هذه التكنولوجيا؟

إجابة هذا السؤال تختلف بناءً على اختيار الشركة سوف تستخدم منتجاتها من الشركات الموجودة في السؤال السابق لأن كل شركة لها كورسات وشهادات خاصة بها.

لكننا هنا سوف نركز على الشركة الأهم وهي القائدة حتى الآن وهي VMware .
الكورس الأول لهذه الشركة هو VMware vSphere ESXi والذي يعطي أشهر شهادة عندهم وهي VCP.
الكورس في حد ذاته ليس طويل أو ضخم. هو عبارة عن 13 وحدة ومدته 40 ساعة فقط.
لكنه يعيطك المعلومات الكافية لكي تسطيع أن تبني مراكز بيانات كاملة عن طريق التكنولوجيا التخيلية.
يوجد تعديل جديد على هذه الشهادة تسمى VCP – Cloud وتعتبر هذه الشهادة جديدة وصدرت من عدة أشهر فقط
وهي عبارة عن نفس منهج الكورس السابق ويضاف عليه كورس آخر وهو VMware vCloud Director ويؤهلك لكي تعمل في الشركات التي تقدم السيرفرات المؤجرة للشركات الصغير، مثل شركات الـ ISP تقدم سيرفرات وهمية لكي تستأجرها شركات أخرى.
يوجد مستوى أعلى وكورسات وشهادات متقدمة وهي VCAP وهي المستوى المتقدم من المسؤولين عن مراكز الداتا سنتر الضخمة.
وهي تتكون من عدة كورسات لكني لا أرى لهذا المستوى داعي في عالمنا العربي الآن وأيضًا لا يوجد له كورسات في منطقتنا العربية .

يوجد مستوى أعلى وهي شهادة الـ VCDX وهي شهادة تعطى لخبراء تصميم مراكز الداتا الضخمة، وهذه الشهادة ليس لها كورسات إنما هي خبرة ومشاريع تقدم لشركة VMware هي شبية بشهادة CCIE عند شركة سيسكو
والحاصلين على هذه الشهادة في العالم لم يتعدوا المائة حتى الآن.
بالنسبة لمايكروسوفت لها شهادات جديدة للمتخصصين في هذه التكنولوجيا وهي شهادة تسمى MCSE Private Cloud

رابعًا: الإمتحانات والشهادات؟

الكثير يهتم بالشهادات وإن كانت ليست دلالة على فهمك للمعلومة، حتى الآن تشترط شركة VMware لكي تستطيع أن تمتحن وتحصل على شهادة يجب أن تكون قد حضرت الكورس الخاص بالامتحان في إحدى المراكز التعليمية المعتمدة منها.
أما بالنسبة للأسعار الأسعار فهي عالية نوعًا ما في هذه المراكز المعتمدة، ونصيحتي لك بأن لا تجعل الشهادة هي هدفك، بلاجعل هدفك هو أن تكون ملمًا بالتكنولوجيا والمنتج جيدًا ولك خبرة جيدة فيه.

خامسًا: هل هذه التكنولوجيا مطلوبة في سوق العمل في منطقتنا؟

بالتأكيد العمل رزق في الأول من عند الله – بالنسبة لمنطقتنا العربية هذه التكنولوجيا مازالت في بدايتها لكنها تنمو بشكل سريع والطلب يزداد عليها باستمرار فيجب أن تكونَ جاهزًا من الآن ولا تنتظر حتى لا تضيع عليك الفرصة.

سادسًا: ما هي الوظائف التي ممكن أن احصل عليها بعد تعلم هذه التكنولوجيا؟

حتى الآن لا يوجد اسم معين لوظيفة للمتخصصين في هذه التكنولوجيا لكن أقرب اسم هو System Engineer
حتى الان في عالمنا العربي لا يوجد شخص متخصص في هذه التكنولوجيا فقط أو يعملها فقط إلا في الشركات الضخمة جدًا أو شركات الـ ISP.
لأن غالبية أحجام الشركات في عالمنا العربي صغيرة إلى متوسطة، فالذي يدير هذه التكنولوجيا في الشركات هم System Engineer .

بالطبع عندما تتقدم هذه التكنولوجيا في منطقتنا وتكون الشركة ضخمة سوف يكون هناك متخصصين أكتر ويتم الفصل بين العاملين في هذه التكنولوجيا وبين الـ System Engineer ويكون لها مسمى وظيفي جديد.

هذه إجابات أغلب الأسئلة التي تردني للدخول لهذه التكنولوجيا
لكن يجب معرفة أنه يوجد عند كل شركة كورسات وامتحانات ومنتجات أخرى كثيرة لكني أردت أن أوضح لكم بداية الدخول لهذا العالم.

عشر طرق يمكن عملها لمنح مخدمك القديم حياة ثانية

مقدمة:

إذا كنت مسؤولاً عن شبكة، فربما قد لاحظت كيف يتم تطبيق قانون (مور) على المخدمات ، حيث أن مخدمك اليوم سوف يصبح مجرد كمبيوتر عادي قريبًا، ولذلك يجب الاهتمام دائمًا بالمخدمات لكي تبقى مجارية لمعايير الإنتاجية والآداء والتنافس، ولكن كثيرًا من المخدمات التي تحال إلى التقاعد مبكرًا يمكن أن تبقى تستخدم بشكل جيد. وأحيانا يمكن تحسين المخدمات القديمة بواسطة إضافة قرص صلب جديد و إضافة رامات جديدة. وبحسب طبيعة الشبكة يمكن أن تختار ما هو أفضل شيء يمكن عمله ولكنني في هذه المقالة سوف أعطيك عدة طرق يمكن أن تستخدم فيها مخدمك القديم :

كثير من مدراء الشبكات يعانون من الثّغرات الأمنية التي تكون موجودة في الشبكة لذلك يقومون بعمل Patch Management من أجل اكتشاف الثغرات الأمنية. فمثلا في بيئة مايكروسوفت يتم عمل patch)) لكل شي بشكل منتظم ابتداءً من الـ power point إلى الـ2003 windows server .

ولكننا أيضا نحتاج إلى عمل patch عند المستخدمين وليس من المعقول أن يتم عمل تحديث تلقائي لكل المستخدمين (حيث سيقومون بالدخول معًا إلى شبكة الانترنت وعمل تحميل لنفس الـ patches) وهذا يؤدي إلى استهلاك كبير لـ bandwidth ولن نستطيع أن نتحكم في الأشياء التي تحتاج أن نعمل لها patchوالأشياء التي يجب أن يتم معالجتها بشكل تلقائي. فنحن نحتاج إلى نظام تحكم مركزي .ولكن هكذا النظام بالنسبة إلى الشركات المتوسطة الحجم سوف يكلف ثمنًا كبيرًا، لذلك قامت مايكروسوفت بعمل خدمة (WSUS windows server update services) عن طريق هذه الخدمات يمكن لمخدم بمواصفات 1GHz للمعالج و1GB للرام أن يخدم حوالي 500 زبون (فبهذه الحالة يمكن جعل المخدم القديم لدينا يعمل كمخدم WSUS).

تشكل عملية التخزين الاحتياطي مشكلة أخرى لمديري الشبكات ولذلك يمكن الاستفادة من مخدمك القديم لحلها.

حيث يوجد العديد من البرامج القوية وذات السّعر المقبول والتي يمكن أن تجعل المخدم القديم يعمل كـ devices Network attach server(NAS).

حيث أننا باستخدام البرنامج NASLite-2 CDD يمكننا تحويل المخدم القديم إلى مخدم قوي جدًا في أمور النسخ الاحتياطي بواسطة إضافة بعض الـ

BIG Driver ويمكن إقلاع هذا البرنامج من cd أو من usb حيث يجعل الكمبيوتر ذو المواصفات القديمة يعمل بفعالية ولا يحتاج لتشغيله إلا لمجرد 8mb وهو يقلع مباشرة ضمن الـ ram ويحتاج إلى معالج Pentium وإلى 64 Mb للـRAM.

تشكّل عمليّة نسخ الأقراص وأخذ صور لها (ghost images) توفير الوقت والجهد. حيث نشعر بذلك عند حدوث مشكلة ما، ولذلك تشكّل عملية إيجاد مكان لتخزين الصور الكبيرة عائقًا بالنسبة لمديري الشّبكات ، لذلك يمكن استخدام المخدمات القديمة لهذا الغرض حيث نستفيد من قدرتها التخزينية على تخزين النسخ وعندما يحتاج الزبون لأي صورة يمكن نسخ الصورة إلى محرك أقراص قابل للإزالة وأخذ الصورة منه.

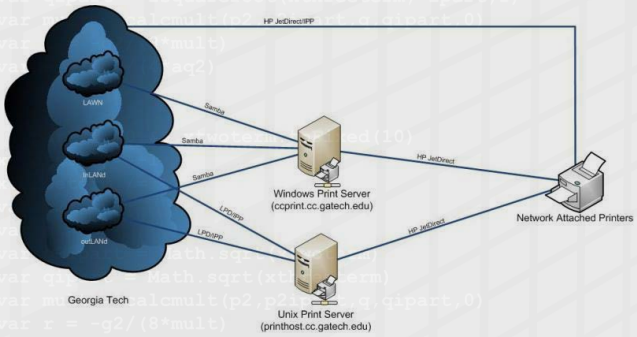
حيث نقوم بجعل المخدم القديم يعمل كجدار ناري في حال لم تكفي الـ access list للقيام بعمل جيد وأيضًا في حال لم يكن لدينا الميزانية المناسبة لشراء عتاد مادي خاص بالجدار الناري أو لشراء برمجيات خاصة بالجدار الناري.

حيث يمكن استخدام العديد من الـ open source firewall والتي تعطينا عديد من الخيارات ولمزيد من المعلومات حول هذه البرمجيات يمكن الذهاب إلى الرابط التالي:
/http://www.smoothwall.org

لأننا لا نحتاج إلى مواصفات كبيرة من أجل الاختبار حيث يمكن إجراء اختبار بمواصفات قليلة وهذا أفضل، حيث قد نحتاج فقط إلى إضافة بعض الرامات لتحسين أدائه ، ويمكن استخدامه لاختبار التطبيقات الجديدة أو للتدريب على أنظمة تشغيل بديلة .
ويمكن أيضًا أن ننصّب جهاز كمبيوتر أو مخدم افتراضي عليه بواسطة استخدام برامج خاصة لذلك مثل VMware والتي يمكن أن تجد نسخ مجانية منها.

يمكن استخدام المخدّم القديم كمخدّم للطباعة ومخدم للملفات، وبذلك نخفّف العبء عن المخدم الأساسي الذي يعمل للطباعة وللملفات .
وكذلك فإن عمليّة تنصيب الـ file server هي سهلة كثيرًا. ولمزيد من المعلومات حول الـ windows server 2003 print server يمكنك قراءة المقالة التالية :

http://www.microsoft.com/windowsserver2003/techinfo/overview/print.mspx



إذا أردت أن تجرب قدرات الـ terminal server service يمكنك أن تستخدم مخدمك القديم لذلك، فقط تحتاج لإضافة بعض الرّامات. وللمزيد من المعلومات حول windows server 2003 terminal service قم بتحميل هذا الملف: www.microsoft.com/windowsserver2003/techinfo/overview/termserv.mspx

حيث يمكن استخدامه كمخدم إضافي للـ DHCP نجعله يعمل على SUBNET أخرى.

أكبر خطأ قد يرتكبه المدير عندما يستمع إلى جماعة اللينكس هو بالتخلي عن Exchange Server الخاص بمايكروسوفت.

فربما قد يرغب هو وباقي أعضاء الإدارة بجميع خصائص هذا البرنامج بشكل مجاني ولكن للأسف هذا الأمر غير متاح ولكن يوجد منتج مفتوح المصدر يدعى Zimbra لم اختبره شخصيًا ولكنه يبدو فعالاً للشركات المتوسطة والصغيرة للمزيد من المعلومات حول هذا البرنامج ننصحك بالذهاب إلى:
http://www.zimbra.com/community/documentation.html.
-http://techrepublic.com.com/2415-92919-11_1035.html

أما بالنّسبة لمتطلبات هذا البرنامج فهو يتطلب معالج 1.5 GHZ و 1 GB من الرام و 5 غيغا من المساحة التخزينية للقرص مخصصة للبرنامج ومساحة إضافية لتخزين البريد.

قل عني مؤمن بالخرافات ولكنّي أحب أن أبقي مخدماتي نظيفة و نقية ومخصصة لتعمل مهامها الخاصة. لذا ولكوني مدير شبكة WAN فأنا بحاجة لبرامج تنصت sniff و ping لتتفحص وتخبرني حول حالة الشبكة .ولكني لا أحب أن يتم تنصيب مثل هذه البرمجيات في متحكم الدومين domain controller الخاص بي أو أي خدمة أخرى تقوم بالعمل على هدف معين مخصصة له .
لهذا أنا استعملت المخدم الأول القديم لأداء هذه المهمة النبيلة .

حيث أعطيت هذا العمل لـ Spice works IT Desktop وبذلك يصبح سطح المكتب الخاص بالـ IT هو مجاني سهل الاستعمال ومبني على المتصفح .

يمكن أن تصدق مايقال في الموقع بأن هذا المنتج يستغرق أقل من 5 دقائق للإقلاع والعمل فهو مصمّم لتنظيم أقل من 250 جهاز على الشبكة .

من متطلباته هو ويندوز xp أو 2003 مخدم ، مع معالج 700 MHz وذاكرة 512.

كما يمكنك أن تضع The Dude للعمل فهو يقوم بعمل جيد بمطابقة شبكتك ويمكن استعماله لعملية ping , port probes, and outage notifications.

الأثر الاقتصادي لـ CLOUD وسيناريوهات الاستخدام

Identification
غسان محمد ابو جسار
الجنسية : الأردن
حاصل على دبلوم هندسة اتصالات وبكالوريوس علم حاسوب مبرمج بلغة الجافا فني اتصالات لاسلكية وفني شبكات حاسوب
ghajassar@gmail.com
JORDAN

تمكِّن البنى التّحتية للحوْسبة السحابية CLOUD COMPUTING الشركات من زيادة الاستثمار في مجال تقنية المعلومات والتّطوير في مجال البرامج والأجهزة .

أصبح التوجه الآن عزيزي القارئ إلى أتمتة مجموعات إدارية مختلفة الأنظمة والتخصّصات كأنها كيان واحد يكون على عاتق شركة حواسيب متخصّصة في هذا الأمر. وكما نعلم أن CLOUD COMPUTING عبارة عن نظام افتراضي VIRTUAL SYSTEM وهو تطور طبيعي لمراكز المعلومات DATA CENTER والاتصالات الذي يوظف النظم الإدارية المأتمتة وتحقيق توازن في حجم العمل وتمثيل افتراضي للتكنولوجيا .

وبنية الـ CLOUD يمكن أن تكون نموذجًا فعّالا للتّوفير في الكلفة لتقديم خدمات المعلومات والحد من تعقيدات إدارة تكنولوجيا المعلومات وتشجيع الابتكار والاستجابة في الوقت الحقيقي RESPONSE THROUGH REAL TIME وتحقيق التوازن في توزيع عبئ العمل الـ CLOUDS تجعل من إطلاق تطبيقات الـ WEB أمرًا سهلاً وتعمل على زيادة وتوسيع نطاق استخدامها لتدعم عدة تطبيقات برمجية مختلفة مثل برامج الجافا التقليدية وأنظمة تشغيل لينوكس وأباتشي وقواعد بيانات MYSQL وبرمجيات PHP .

شركة GOOGLE FILE SYSTEM و IBM وHP وغيرها توفر وسيلة لآلاف التطبيقات عبر السرفرات الموجودة في شركاتها للقيام بعمليات برمجية لشركات مختلفة في أنحاء العالم لحظيًا.

كمية كبيرة من COMPUTER RESOURCES على شكل XEN VIRTUAL MACHINES يمكن توفيرها في الـ CLOUD وإتاحتها تطبيقات جديدة في دقائق معدودة بدلاً من الانتظار لأيام وأسابيع لمواءمة هذه الأجهزة لتستطيع العمل على هذه التطبيقات الجديدة. ومطوروا هذه التطبيقات ومستخدموها يستطيعون استخدام هذه RECOURSES بشكل مباشر وحصري لهم ولاتنسى قدراتها بالاحتفاظ بحق الملكية لأصحاب هذه التطبيقات وسريتها.

سيناريوهات الاستخدام

CLOUD COMPUTING أصبحت تلعب دورًا مهمًا في مجالاتٍ شتّى، مثل شركات الطيران والابتكارات والعوالم الافتراضية والتجارة الإلكترونية والشبكات الاجتماعية.

الابتكارات

عندما يقوم المبتكرون بطلب الموارد عبر الانترنت من خلال واجهة ويب بسيطة ويقوموا بتحديد تاريخ معين لبداية تجاربهم ونهايتها وإعلام الـ CLOUD RESOURCE ADMINISTRATORS بذلك ليقوم بالموافقة أو رفض هذه الطلبات. وبناءً على موافقة مسبقة من CLOUD RESOURCE ADMINISTRATORS FOR CLOUD SERVER يقوموا بتوفير الموارد RECOURSES للمطورين في دقائق أو ساعات بناءً على نوع الموارد التي تم طلبها.

العوالم الافتراضيية

العوالم الافتراضية أو VIRTUAL WORDS تحتاج لتسخير كميات ضخمة من قدرات الحواسيب خصوصًا الـ VIRTUAL SPACES التي تطورت بشكل كبير وأصبحت أكثر استخدامًا من خلال الشبكة ومن أهم تطبيقات الـ VIRTUAL WORDS الـ MMPOG MASSIVELY MULTIPLAYER ONLINE GAMES وأكثرها استخدامًا أصبحت الـ VIRTUAL WORDS التجارية. آلاف من السيرفرات لتقوم بخدمة عشرات الملايين من المستخدمين المسجلين في هذه العوالم الافتراضية والشركات التي تستضيف هذه البيئات الافتراضية تحتوي على أجهزة للمراقبة في الوقت الحقيقي REAL TIME MONITORS لإظهار مستوى الاستخدام للبنية التحتية للـ RESOURCES وحساب زمن الاستجابة للعملاء ووجود الـ REALMS الفرعية داخل العالم الافتراضي التي تدعم مجموعة معينة من الناس أو مجموعة فرعية من العالم سهّلت الأمر. فعلى سبيل المثال تكتشف الشركة أن القطاع REALM A لديه زيادة كبيرة في الاستخدام وأوقات الاستخدام بينما القطاع S Zg انخفض الاستخدام فيها فتقوم الشركة بإعادة توزيع للمصادر مثلا بسحب 10 سيرفرات من كلا القطاعيين S Zg وعمل توفير هذه السيرفرات للقطاع A وبدقائق معدودة دون انقطاع عن أي مستخدم في أي قطاع كان، وبعد ذلك يعود معدل وقت الاستجابة للقطاع A إلى مستويات مقبولة.

وبذلك تقوم الشركة بتوفير تكاليف عالية بإعادة استخدام معدات غير مستغلة، وحافظت على رضا العملاء بمعدل استجابة أسرع وتجنب شكاوي الزبائن لطلب المساعدة عند سوء الخدمة وهذا كله بدقائق معدودة الذي كان يتطلب تطبيقه في السابق أسابيع وأشهر لإعادة تحسين الخدمة كسابق عهدها.

في الأعمال التجارية الإلكترونية

التطور والتوسع يمكن تحقيقه بتوفير سيرفرات جديدة عند الحاجة لها، على سبيل المثال خلال ذروة موسم التسوق يمكن توفير المزيد من السيرفرات الافتراضية لتلبية المتطلبات التي يحتاجها التسوق الالكتروني وفي مثال أخر قد تواجه الشركة أعباء عمل إضافية في عطلة نهاية الأسبوع أو في المساء فإذا كانت الشركة تمتلك CLOUD كبيرة الحجم فإنه من الممكن جدولة COMPUTER RESOURCES حتى يتم توفيرها في كل مساء أو في عطلة نهاية الأسبوع أو خلال موسم الذروة . وفي ذلك يتم تحقيق استغلال أمثل للـCLOUD بدلا من حجزها على مدار الأسبوع دون الحاجة لها

جانب آخر من هذا السيناريو ينطوي على توظيف السياسات التجارية لتحديد التطبيقات ذات الأولوية والتي تحتاج . COMPUTING RESOURCES .

أكثر التطبيقات المدرّة للمال تصنف بأولوية أعلى من تطبيقات البحوث والتطوير والابتكار ولهذا البنية التحتية للشركات التي تقدم الـ CLOUD تعدل COMPUTER RESOURCES بشكل مناسب وتلقائي فيما يتلاءم مع السياسيات التجارية.

الهوايات الشخصية

لم يعد مفهوم الابتكار والاختراع أمرًا محصورًا على الشركات والمؤسسات التجارية، لا بل أصبح الابتكار والاختراع على المستوى الفردي أكثر وأوسع خصوصًا أن الـ CLOUD أصبحت توفر RESOURCE لأي مخترع ومبتكر على المستوى الفردي.

اليوم في هذا السوق التنافسي العالمي يجب على الشركات الحصول على موارد أكثر لتحقيق النجاح هذا يتطلب تمكين موظفيها، والشركاء التجاريين والمستخدمين من استخدام أدوات ومنصات تعزّز الابتكار و CLOUD COMPUTING INFRASTRUCTURES هي الجيل القادم الموفّر لهذه الأدوات والمنصّات التي ستعزز من نجاح الشّركات في أي مجال كانت ومهما كان حجمها.

كلمة مهندسي نتوورك ست

NetWork Set First Arabic Magazine For Networks

أحمد خير الدين

«كانت مجرد زيارة لرابط في غوغل ليس أكثر، إلا أن نتوورك ست و ضعت نقطة.
و البداية من اول السطر في عالم الشبكات.
نتورك ست قدّمت معلومة صحيحة سهلة، بسيطة، ممتعة و باللغة العربية.
أحرص دائمًا على رفع القبعة لرئيس التحرير، المهندس أيمن النعيمي.»

شريف مجدي

« هناك فرق بين شخص يفهم موضوع معين وآخر تجاوز مرحلة الفهم لينهمك في شرحه ببساطة ووضوح للآخرين ,ولن تصل إلى تلك المرحلة إلا عن طريق محاولة الكتابة بنفسك ,والتي قد يستفيد منها غيرك ولكن المستفيد الأكبر والحقيقى من تلك التجربة سيكون أنت , هذا هو أهم مبدأ تعلمته من خلال تجربة الكتابة فى نتورك ست »

أحمد سلطان

مجلة نتورك ست بمثابة كنز مجاني متاح للجميع لا يعرف قيمته سوى من تعب وتحمل مشقة الوصول إليه»
المجلة تضع بين يديك خلاصة خبرات مهندسي الشبكات في مختلف أنحاء الوطن العربي وكل ما عليك هو أن: «تأخذ من كل بستان زهرة حتى تكوّن أنت بستانك الخاص»

أحمد هيكل

كان لي الشرف بالانضمام لهذا الفريق الكبير فى المجلة ونيل شرف إيصال المعلومات إلى كل من يريد أن يستزيد من المعلومات المتوفرة على الانترنت وهنا لابد من التوجه بالشكر إلى كل اعضاء المجله الكرام وقرائها من العالم العربي وخاصة المهندس أيمن النعيمي على هذا المجهود الرائع والأفكار الأروع وإن شاء الله إلى الأمام دائمًا.

رضا عبد الرحمن أحمد:

مع أن مقالي الأول كان على وشك أن لا يرى النور لكنني تفاجأت أيما مفاجأة ، مزيدًا من النجاحات التى تحلق بكم فى سماء الشبكات إخواني الأعزاء فأنتم من سوف تفتحون أبواب المعرفة لكل من هو هائم على رصيف المتصفحات يرجو علمًا ينفع الناس به وينتفع هو به ويزيد مما اعطاه الله إياه .
2012 كانت سنة مميزة لهذه المجلة العملاقة ولكنني أتوقع 2013 أنها ستحدث صدىً عالٍ في أعداد هذه المجلة وسيكون الإقبال عليها فوق التوقعات .

أسامة كامل

أول مجلة عربية متخصصة بالشبكات . هذه الكلمة تكفي ليتعلم الناس التميز والمنافسة الشريفة.
انتظروا المزيد من الجديد.

أيمن النعيمي

عندما بدأت كنت وحيدا, أكتب أصمم أدقق, أفعل كل شيئ بنفسي والآن والحمد لله أحيانا لا أجد لنفسي مكان أنشر فيه مقالاتي. مرة زمن طويل كنت ولا زلت اطمح إلى المزيد من التطور للمجلة والتى تكتمل بأن تشاركونا خبرتكم وعلمكم, شاركونا وكونوا السباقين وتذكروا أن مشاركة العلم هي واجب على الجميع.


NetWork Set
First Arabic Magazine For Networks