مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (30) العدد (3) 2008
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (30) No. (3) 2008

طريقة متكاملة لحماية الشبكة الحاسوبية

الدكتور تاج الدين جركس *
الدكتور عدنان معترماوي **
المهندس زياد الشر يقي***

(تاريخ الإيداع 7 / 4 / 2008. قُبِل للنشر في 2008/6/26)

□ الملخّص □

يعدّ موضوع أمن الشبكات من المواضيع المهمّة في مجال تقنيات المعلومات؛و لأنه الجوهر الحقيقي لأمن المعلومات،وبما أن هذه المعلومات هي العمود الفقري للمؤسسات والشركات, وأنّ كشفها المعلومات أو تغييرها قد يؤدي إلى انهيار المؤسسة. كما أن تصميم نظام آمن مطلق أمر مستحيل؛ لأن النظام الآمن الوحيد هو ذلك النظام الذي لا يتصل به أي شخص، وهو نظام غير مفيد ،ومع تطور وسائل الهجوم ومحاولات اختراق الشبكة كان لابد من بناء منظومة متكاملة لحمايتها من التهديدات الداخلية والخارجية و بالوقت نفسه تكون فعالة وقابلة للاستخدام.

الكلمات المفتاحية:أمن الشبكات–التهديدات–نهج المجموعة–الدليل النشط–الشبكة الخاصة الافتراضية.

* أستاذ– قسم هندسة الاتصالات و الإلكترونيات–كلية الهندسة الميكانيكية والكهربائية– جامعة تشرين–اللاذقية–سورية.
** مدرس– قسم هندسة الاتصالات و الإلكترونيات–كلية الهندسة الميكانيكية والكهربائية– جامعة تشرين–اللاذقية–سورية.
*** طالب دراسات عليا(ماجستير)– قسم هندسة الاتصالات و الإلكترونيات–كلية الهندسة الميكانيكية والكهربائية– جامعة تشرين–اللاذقية–سورية.

مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (30) العدد (3) 2008
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (30) No. (3) 2008

An Integrated Technique for protecting Computer Networks

Dr. Taje Din Jarkas*
Dr. Adnan Moatarmwi**
Ziad Alshreaky***

(Received 7 / 4 / 2008. Accepted 26 / 6 / 2008)

□ ABSTRACT □

Network security is considered an important subject in the information technology field, since it is crucial for information security. This information is the backbone of organizations and companies. Thus, giving away this information or changing it will break down the organization. In addition, designing an absolute safety network system is impossible because the only safe system available is the one that nobody can access; thus, it is not a useful system. With the development of offensive tools and attempts to hack the network system, it is necessary to build active and applicable integrated security systems to protect the network from internal and external threats.

Keywords: network security, threats, group policy, active directory, VPN

* **Professor, Department of Communication & Electronics Engineering, Faculty of Mechanical & Electrical Engineering, Tishreen University, Latakia, Syria.**
** **Assistant Professor, Department of Communication & Electronics Engineering, Faculty of Mechanical & Electrical Engineering, Tishreen University, Latakia, Syria.**
*** **Postgraduate student, Department of Communication & Electronics Engineering, Faculty of Mechanical & Electrical Engineering, Tishreen University, Latakia, Syria**

مقدمة :

شبكات الكمبيوتر هي التي تربط الأجهزة مع بعضها بعضاً محلياً ونطاقياً وعالمياً، والهدف منها هو التشارك بالموارد إلا أن المقايضة بين أمن الشبكات بما تعنيه هذه الكلمة من حماية للمعلومات من الأخطار الداخلية والخارجية وإمكانية الوصول إلى موارد الشبكة صعب جداً ؛ إذ كلما كانت الشبكة آمنة كلما كان الوصول إليها صعباً والعكس بالعكس؛ إذ كلما كان الوصول إليها سهلاً كلما كانت أقل أمان؛ لذلك من الضروري أن نتعرف على الأخطار التي تهدد الشبكة لابتكار آلية لحماية البيانات من هذه الأخطار من جهة وجعلها فعالة من جهة أخرى.

تم إجراء البحث في مختبرات كلية الهندسة الميكانيكية والكهربائية في جامعة تشرين و الشركة العامة لمرفأ اللاذقية في الفترة الواقعة بين 2007/8/1 و 2008/4/1.

هدف البحث وأهميته:

يقوم هذا البحث بتوصيف أهم التهديدات التي تتعرض لها الشبكات والآلية المستخدمة لبناء منظومة متكاملة لحماية الشبكة من التهديدات التي تتعرض لها، كذلك سوف نقوم بالمقارنة بين الشبكة المقترحة وبعض الشبكات الأخرى لإظهار ميزات الشبكة المقترحة.

طريقة البحث ومواده:

اعتمد هذا البحث بيئة windows server 2003 كنظام تشغيل ونهج المجموعة (group policy)[1,2] كسياسة داخلية ضمن الشبكة، وقد استخدم في الشبكة المقترحة الأدوات التالية:

1. نهج المجموعة(group policy) [1,2]: وهي آلية لإدارة السياسة الداخلية للشبكة؛ إذ نحدّد من خلالها شكل بيئة سطح المكتب، ومواضع التشكيل الجانبي للمستخدم وتوفر التطبيقات وإعدادات الأمان والبرامج وتسجيل الدخول والخروج.

2. المكتبة النشطة أو الدليل النشط (active directory) [1,2]:هو مخزن وخدمة كائن يستند إلى الشبكة، ويحدد ويدير الموارد، ويجعل هذه المستندات متاحة للمستخدمين والمجموعات المخولة.

3. مضاعفة المكتبة الفعالة(Replication active directory)[1,2]:وهو يقوم بعملية نسخ البيانات الموجودة في الـ active directory وأي تغير فيه سوف يؤدي إلى تغير في الـ replication active directory، وهو يستخدم من أجل موثوقية العمل واستمراريته.

4. نظام اسم المجال (DNS) [1,2]: خدمة قياسية تعمل مع شبكات TCP/IP، ويعدّ DNC خدمة اسم هرمية للحواسب المضيفة ويستخدم DNS كتكنولوجيا أساسية للدليل النشط ،يورد الـ DNS قائمة بأسماء المضيفين وعناوين IP.

5. العنقود (cluster)[1,2]: مجموعة من الحواسب التي تتشارك في حمل العمل، وتؤدي تسامحاً فائضاً مع الخطأ وإذا فشل عضو فسوف يتكفل العضو الآخر بالعمل في عملية تدعى التعافي من الفشل.(fault tolerance system redundancy)

6. Raid array[3]: وهي مجموعة أقراص صلبة تخزن فيها البيانات (Data Base) تربط مع بعضها بعضاً بعدة تقنيات إما raid 0 وإما raid 1 أو raid 5.

7. الشبكة الخاصة الافتراضية(VPN)[4]: وهي عملية إنشاء قناة خاصة باستخدام الإنترنيت لربط موقعين في مكانين مختلفين باستخدام بروتوكولات معينة (L2TP, IPsec, PPTP)

8. Main data base[4]: وهو الجهاز الذي يتم عليه إنزال برامج ORACLE.

9. Redundancy data base[4]: وهو جهاز داعم يتم عليه أيضاً إنزال برامج ORACLE ويستخدم من أجل استمرارية العمل وسرعة الاستجابة.

10. شبكةLANالافتراضية (VLAN) [3]: هي مجموعة منطقية من محطات الشبكات والخدمات والأجهزة غير المقيدة بمقطع LAN المادي تقوم بتصفية البث والأمان وإدارة تدفق حركة المرور.

11. Application server[4,5]: واجهة برامج تطبيقية وسيطة تربط بين المستخدمين وأجهزة الـ Data Base تستخدم لمنع المستخدمين من العمل مباشرةً على أجهزة الـ Data Base والعبث فيها.

12. المبدل المركزي(Core Switch): جهاز شبكي يقوم بربط أجزاء الشبكة مع بعضها بعضاً، ويتم من خلاله إرسال الأطر بالاعتماد على عنوان وجهة كل إطار.

المبدل المركزي المستخدم في الشبكة المقترحة هو:

(Cisco 2950 Fast Ethernet switch 24 x 10/100 UTP) يدعم (VLAN, STP)

التهديدات التي تتعرض لها الشبكة:

التهديدات الأمنية للشبكات تشكل عائقاً تجاه السياسة الأمنية الموضوعة لحماية الشبكة، وهنالك أنواع مختلفة من التهديدات على سلامة الشبكة ويمكن تصنيفها في فئتين:

a. تهديدات خارجية (external threats)[6,7]

b. تهديدات داخلية (internal threats)[6,7]

a. التهديدات الخارجية:

1- خرق المطابقة للأفراد والبيانات(Authentication)

2- تزييف عنوان IP

3- هجمات نكران الخدمة (DoS)

4- فيروسات الكمبيوتر.

1- خرق المطابقة للأفراد والبيانات:كلمة المرور هي إجراء أمني مصمم لمنع الأشخاص غير المرخص لهم بالوصول إلى الشبكة من استخدام موارد الشبكة، وهي فعالة طالما أنها سرية، إلا أنه إذا عرف شخص ما اسم المستخدم وكلمة المرور لأحد المستخدمين يستطيع عندها ذلك الشخص الدخول إلى الشبكة واستخدام مواردها .

2- تزييف عنوان IP : عند تزييف IP يتم تغيير ترويسات الرسائل المرسلة فتظهر كأنها وردت من عنوان IP مختلف عن العنوان المرسل الحقيقي، وإذا كان هذا العنوان ثقة من قبل الشركة سيسمح لرزمة البيانات بالمرور.

3- هجمات نكران الخدمة (DoS):إن الهدف الرئيس من هجمات تشويه الخدمات والتسبب بإنكارها ليس للحصول على الولوج إلى التجهيزات أو المعلومات بل لمنع المستخدمين الشرعيين للخدمة من استعمالها، وإن هذا النوع من الهجمات يمكن أن يأتي بصور عديدة، فالمهاجمون قد يعمدون إلى إغراق النظام بكميات كبيرة من المعطيات غير الضرورية بهدف استنزاف مصادره أو التسبب بإبطاء أداء الشبكة في أوقات ضغط العمل عليها مما يسبب قلة ثقة زبائن الشبكة بأدائها، وفي حالات خاصة يعترضون المعلومات المنتقلة عبر الشبكة ويفكون تشفير المشفر منها ويعيدونها إلى أصحابها غير مشفرة مما ينسف الثقة بها تماماً .

4- فيروسات الكمبيوتر: وهي عبارة عن برمجيات ضارة تنتشر من كمبيوتر إلى آخر بنسخ شفراتها إلى ملفات أخرى مخزنة ضمن النظام من دون علم المستخدم وهي تهدف إلى تدمير النظام أو المعطيات مسببة خسائر بالملايين.

b. التهديدات الداخلية:

تعد التهديدات الداخلية واحدة من مناطق الاهتمام لدى العاملين في حقل أمن الشبكات؛ لوجود فرصة كبيرة ؛ إذ يحقق أشخاص من الداخل هجوماً على الشبكة لا يمكن تحقيقه من الخارج وفيما يلي نذكر بعض هذه الأخطار:

1- التجسس على الشركة .
2- الموظفون المتذمرون.
3- السياسة الداخلية.
4- الهندسة الاجتماعية.

1. التجسس على الشركات:تحاول الشركات المتنافسة التجسس على بعضها بعضاً؛ وذلك من خلال الوصول إلى الموظفين، وتقديم المكافآت لهم لقاء معلومات خاصة بالشركة التي يعملون فيها، وهذا النوع من أكثر أنواع التهديدات الداخلية تعقيداً وخطراً؛ إذ يمكن لشركة ناجحة أن تصبح بين ليلة وضحاها خاسرة نتيجة تسريب هذه المعلومات إلى الشركات المنافسة.

2.الموظفون المتذمرون : تقوم الشركة بتوجيه تنبيه لبعض الموظفين أو الاستغناء عن خدماتهم لسبب ما مما يولد حقداً لدى هؤلاء تجاه هذه الشركة يجعلهم يقومون بتخريب بياناتها أو محاولة تعطيل الشبكة من خلال نشر فيروسات ضمن شبكة الشركة وذلك بهدف الانتقام من دون الإحساس بالمسؤولية العامة .

3.السياسة الداخلية:إن المنافسة الشريفة بين الزملاء العاملين في الشركة نفسها يؤدي إلى تطور العمل، إلا أنه إذا تحولت هذه المنافسة إلى غيرة وحسد بين الزملاء بحيث يصبح هذا الموظف مستعداً للقيام بأي شيء ليتقدم على زميله كتخريب العمل الذي يقوم به أو الوصول إلى بريده الإلكتروني وإتلاف ملفات ورسائل خاصة بالعمل مما يعود بالضرر على الشركة ككل.

4.الهندسة الاجتماعية: وهي تعتمد على استغلال العلاقات الاجتماعية بين الأشخاص داخل الشركة أو خارجها من أجل اختراق الشبكة كأن يقوم شخص بزيارة صديق له ضمن الشركة ويستطيع بطريقة ما أن يحصل على اسم المستخدم وكلمة المرور لهذا الصديق أو يتصل شخص ما ضمن الشركة بأحد الموظفين ويوهمه بأنه من قسم الـ (IT) ويطلب منه اسم المستخدم وكلمة المرور الخاصة به.

إدارة أمن الشبكة الحاسوبية وتصميمه:

عند تصميم نظام أمني جيد وموثوق يجب أن نأخذ بعين الاعتبار جميع الاحتمالات الممكنة لمنع حدوث خرق لهذا النظام، فقد يكون الأمر مدبراً أو قد يكون غير متعمد "خطأ ناتج عن سوء الاستخدام" ومن أهم مراحل التصميم نذكر مايلي:[1,3,4]

1. الوقاية: وتعدّ من أهم مراحل تصميم النظام الأمني؛ إذ إنه كلما قمنا بإجراءات وقاية لحماية الشبكة كلما منعنا المخربين من الوصول إليها، إلا أن هذا يتطلب تجهيزات كثيرة وبالتالي تكلفة كبيرة.

2. الكشف: ويقصد به كشف المخربين، وهو جزء من الوقاية في النظام الأمني بحيث يتمكن هذا النظام من منع الأشخاص غير المصرح لهم بالدخول كما يسجل محاولات الدخول الفاشلة لكشف نوع النشاطات التخريبية والأشخاص القائمين بهذه النشاطات.

3. الردع: يجب توفر الردع المناسب للنشاطات التخريبية؛ لأن ذلك يؤدي لخوف المخربين من اكتشاف أمرهم ومحاسبتهم ، وهذا راجع للقوانين والدساتير في كل دولة.

4. توفر الحماية من التهديدات الخارجية: ويقصد بها أن يتوفر في النظام الوسائل المناسبة لحماية الشبكة من الأخطار الخارجية التي تم ذكرها من قبل.

5. توفر الحماية من التهديدات الداخلية : ويقصد بها أن يطبق ضمن الشبكة سياسة معينة تؤمن الحماية من الأخطار الداخلية التي تم ذكرها من قبل.

6. استمرارية العمل: ويقصد بها وجود أجهزة مساعدة تقوم بالعمل ريثما يتم إصلاح الجزء المعطل من الشبكة بحيث لا يؤثر في أداء الشبكة ولا يؤدي إلى ضياع البيانات خلال هذه الفترة .

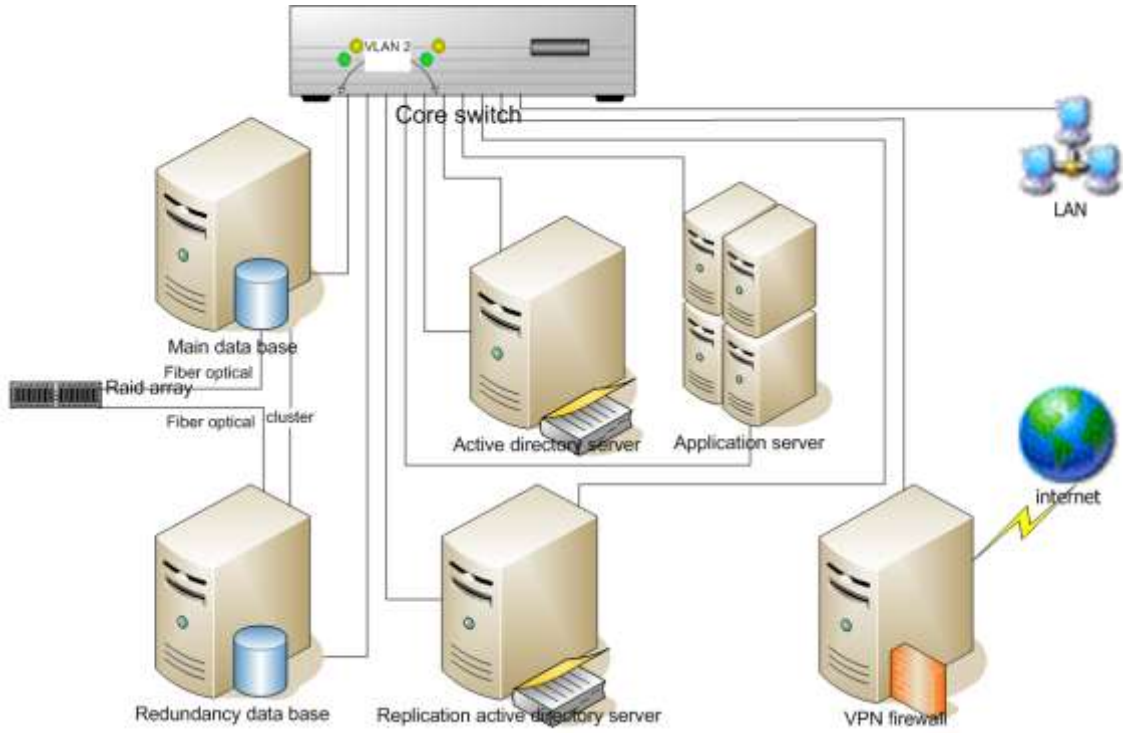
7. قابلية هذا النظام الأمني للعمل من دون أن يؤثر في أداء الشبكة.

8. تصحيح النظام: ويقصد بها اكتشاف نقاط الضعف في هذا النظام وتصحيحها بشكل مستمر.

الطريقة المقترحة لحماية الشبكة:

تم تصميم هذه الشبكة لحماية البيانات من الاعتداءات الداخلية والخارجية، بالإضافة إلى أدائها العالي وموثوقيتها وذلك من خلال مجموعة من الإجراءات المبينة في الشكل(1) حيث تم تركيب core switch تدعم الـVLAN بالإضافة إلىactive directory serverالذي تم فيه استخدام الـ windows server 2003 كنظام تشغيل وتم تفعيل الـ (Active Directory و Domain Controller وDNS و DHCP) أما Replication active directory server فقد تم استخدام الـwindows server 2003 كنظام تشغيل وتمت الإشارة في أثناء عملية تنزيل (Active Directory وDomain Controller و DNS و DHCP) بأنه يوجد نظام تشغيل أساسي وأن هذا النظام هو نظام مساعد يقوم بعملية المطابقة كل نصف ساعة بشكل افتراضي مع النظام الأساسي بحيث إذا توقف الـactive directory server عن العمل لسبب ما فإن الـ Replication Active Directory server الذي يكون في مرحلة الـ stand by سوف يعمل مباشرة ولن يحدث انقطاع في الشبكة ، كما تم تقسيم المستخدمين ضمن المؤسسة إلى مجموعات وتم تطبيق الـ group policy على هذه المجموعات بحيث يحصل كل مستخدم على صلاحيات تتناسب مع طبيعة العمل المسندة له.من جهة أخرى تم تطبيق الـ cluster بين

(Main Data Base و Redundancy Data Base) بحيث إذا توقف الـ Main Data Base عن العمل لسبب ما يعمل الـRedundancy Data Base مباشرة من دون توقف بحيث لا يضيع أي جزء من البيانات وتخزن البيانات في الـ Raid Array ، كما تم تفعيل ميزة الـ VLAN على عدد من بوابات ال Core Switch وهي VLAN2 وتم وصل كرتي الشبكة لكل من الـ(Main Data Base و Redundancy Data Base) إلى الـ VLAN2 في حين تم توصيل أحد كرتي شبكة لكل من الـ (active directory server و active directory server) (Replication على الـ VLAN2 بينما الكرت الآخر تم توصيله إلى بوابات الـ Core Switch التي لا تنتمي إلى الـ VLAN2، وتم وصل هذه الشبكة مع الـ Internet عن طريق الـ VPN firewall وتم استخدام الـ Application server؛ ليصل المستخدم إلى Web Site الشركة من دون العمل على الـ (Main Data Base أو Redundancy Data Base) بشكل مباشر.



الشكل (1) بنية الشبكة المقترحة

إذا حاول أحد العاملين بالشركة الوصول إلى الـ Data Base، وهو ليس مخوّلاً فإنه سوف لن يصل؛ لأنه لا ينتمي إلى مجموعة الـ Administrator ؛ وبالتالي لا يملك صلاحيات مدير الشبكة (اسم المستخدم وكلمة المرور) في الوصول إلى الـ Data Base وإن حصل على اسم المستخدم وكلمة المرور لمدير الشبكة لسبب من الأسباب فإنه سوف لن يصل؛ لأن مأخذ الشبكة التي يعمل عليها لا ينتمي إلى الـ VLAN2 .

أما إذا حاول شخص من خارج الشركة الوصول إلى الـ Data Base فإنه لن يصل؛ لأنه لا يوجد قناة VPN بينه وبين الشركة وإن حاول اختراق القناة ونجح في ذلك، فإنه لن يصل أيضاً إلى الـ Data Base؛ لأن بوابة الـ Core Switch الموصولة مع الـ internet لا تنتمي إلى الـ VLAN2؛ وبذلك فإن هذه الشبكة تكون قد حققت المطلوب بأداء وفاعلية عاليين جداً.

مخطط عمل الشبكة:

يحاول شخص الدخول إلى الشبكة هنا نميز حالتين:

الأولى:إذا أراد الدخول إلى الـ Domain

الثاني:إذا أراد الدخول إلى الـ Data Base

في الحالة الأولى كما هو مبين في الشكل(2)نميز حالتين:

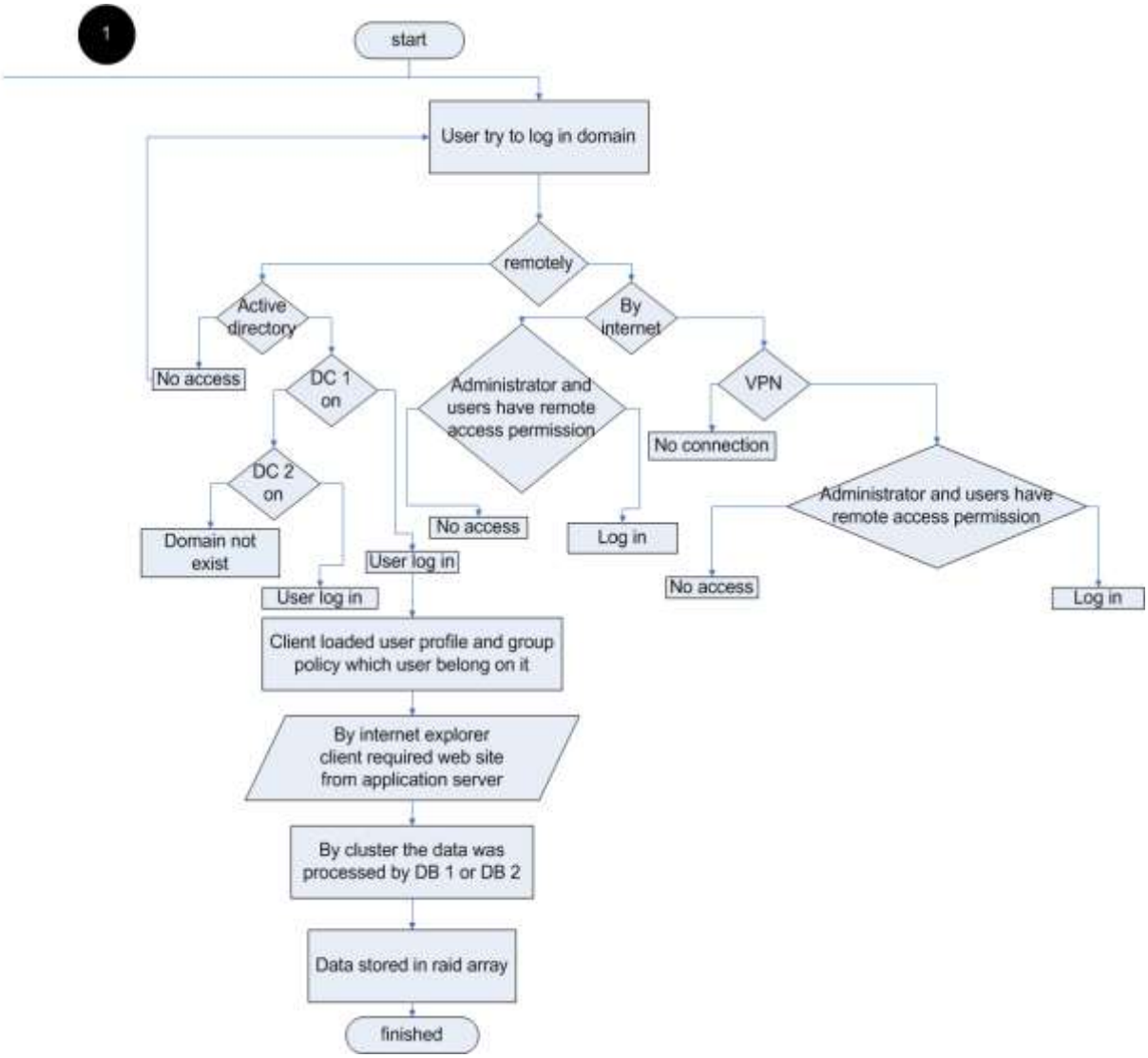
1.إذا كان الشخص ضمن المؤسسة، و يملك صلاحيات الدخول إلى الشبكة (اسم المستخدم وكلمة المرور)، فإنه سوف يدخل إلى الشبكة ويتم تحميل الـ user profile له حسب الـ group policy التي ينتمي إليها، ومن ثم عن طريق الـ internet explorer يدخل إلى web site المؤسسة أما إذا كان الشخص لا يملك اسم المستخدم وكلمة المرور فإنه لا يستطيع الدخول إلى الشبكة .

2.اتصال الشخص عن بعد(remotely)، إذا كان الشخص ضمن المؤسسة ومدير الشبكة أو يملك صلاحيات الاتصال عن بعد فسوف يسمح له بالدخول إلى الـ domain وإلاّ فلن يسمح له بالدخول، أما إذا كان الشخص المتصل خارج المؤسسة (فرع آخر للشركة)، و مدير الشبكة أو يملك صلاحيات الاتصال عن بعد بواسطة الـ VPN وكان المنشأ بين هذين الفرعين VPN فإنه سوف يدخل الـ domain وإلا فإنه لن يدخل إليه.

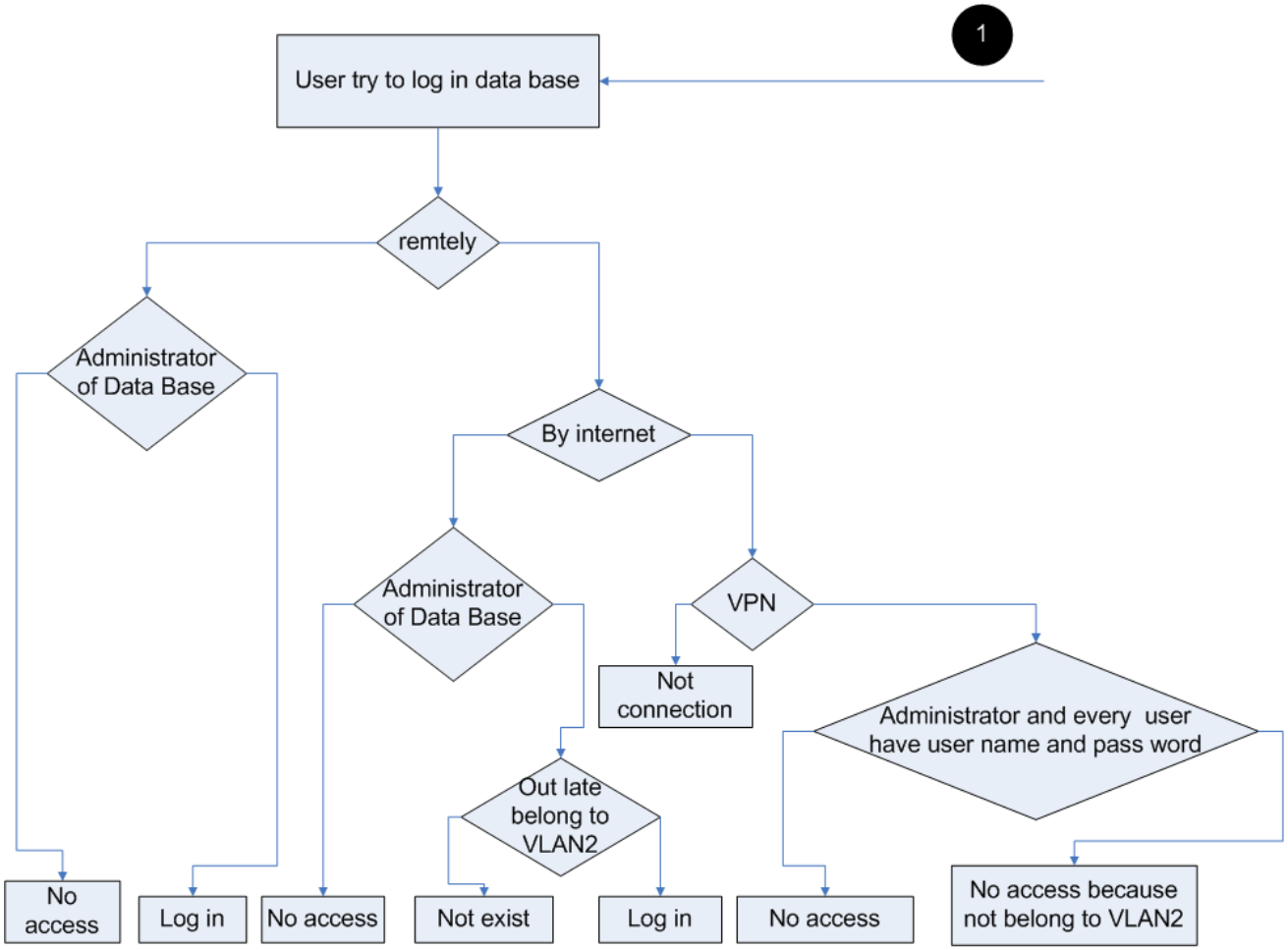
الحالة الثانية إذا أراد الدخول إلى الـ Data Base كما هو مبين في الشكل (3) نميز حالتين:

1.إذا كان الشخص ضمن المؤسسة، وكان المدير المسوؤل عن الـ Data Base فسوف يسمح له بالدخول إلى الـ Data Base وغير ذلك لن يسمح لأحد بالدخول.

2.يتصل الشخص عن بعد(remotely)، وهو ضمن المؤسسة و المدير المسوؤل عن الـ Data Base وإذا كان المأخذ الذي يتصل به ينتمي إلى الـ VLAN2 سوف يسمح له بالدخول إلى الـ Data Base وغير ذلك لن يسمح لأحد بالدخول إليها، وأي مستخدم من خارج المؤسسة لن يسمح له بالوصول إليها.



الشكل(2) الجزء الأول من مخطط عمل الشبكة



ملاحظة:
DC1: active directory server
DC2: replication active directory server
VPN: virtual private network
Lan: local area network
VLAN: virtual local area network

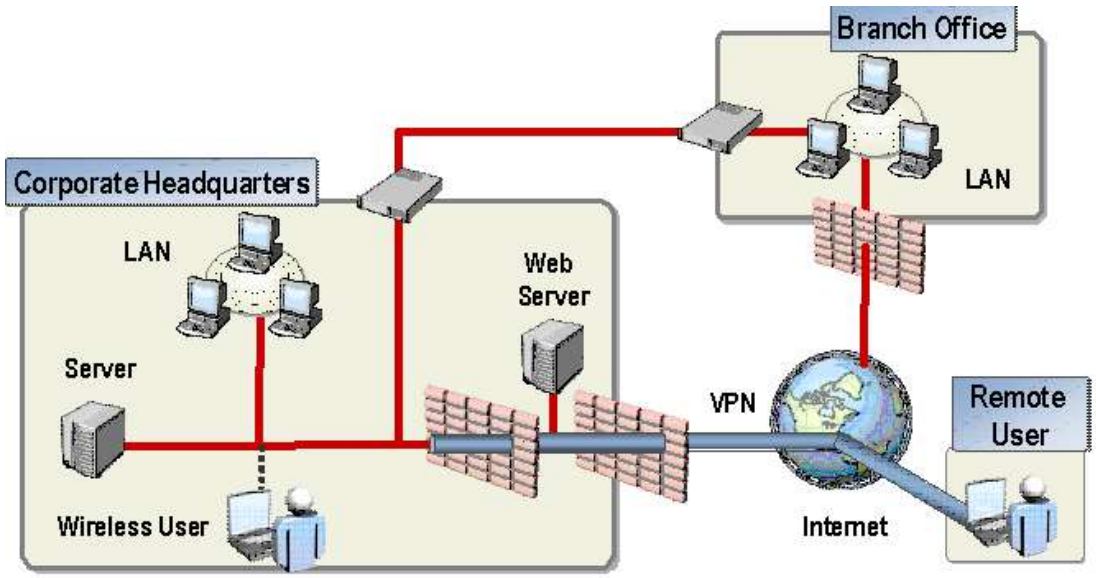
الشكل(3) الجزء الثاني من مخطط عمل الشبكة

النتائج والمناقشة:

مقارنة بين الشبكة المقترحة و *بعض الطرق المتاحة من مايكروسوفت لحماية الشبكة*:

تمت المقارنة بين الشبكة المقترحة وشبكات مايكروسوفت على مبدأ الأمان و أداء الشبكة واستمراريتها في حال حصول عطل في الشبكة، بالإضافة إلى التكلفة من الناحية النظرية (إذ تختلف التكلفة باختلاف حجم الشركة وعدد المستخدمين فيها)

1- الطريقة الأولى:[2]



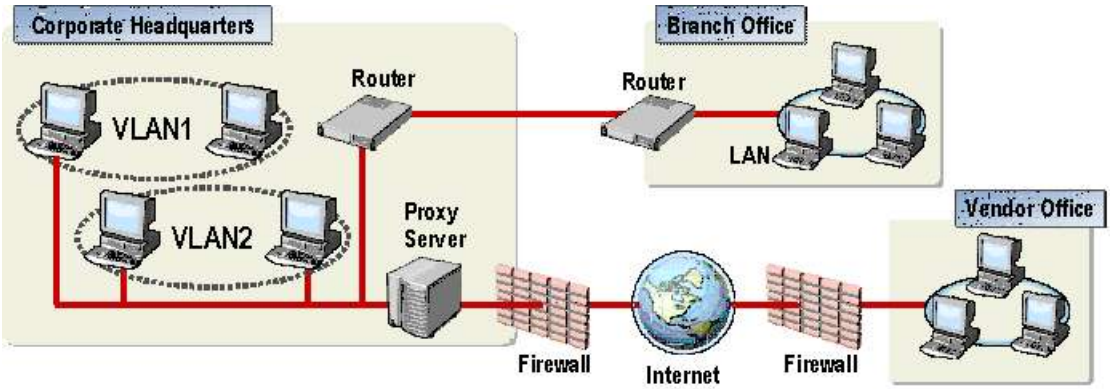
الشكل(4) أحد طرق حماية الشبكة من مايكروسوفت

في هذه الشبكة تم استخدام أكثر من fire wall وهذا يبطئ من أداء الشبكة، بالإضافة إلى صعوبة إدارتها، واستخدام 2 servers الأول web server لإدارة موقع الشركة على الإنترنيت، والـ server الآخر لإدارة عدة عمليات (DNS-AD-DB)، وبالتالي أي عطل في هذا الـ server يؤدي إلى توقف الشبكة، وكذلك تكون معالجة البيانات بطيئة، كما أن البيانات في هذه الشبكة غير محمية من المخربين الداخليين في حين أنها محمية من قبل المعتدين الخارجيين عن طريق الـ VPN ، بينما أقمنا في الشبكة المقترحة جهازين هما: active directory، وجهازين Data Base إذا إن أي عطل في أحد الجهازين (AD or DB) يؤدي إلى عمل الجهاز الآخر أتوماتيكياً، وهذا يجعلها أكثر موثوقية وسرعة، كما أن البيانات في هذه الشبكة محمية من المخربين الداخليين بواسطة الـ VLAN2و الـ group policy والخارجيين بواسطة الـ VPN و الـ VLAN2 . نلخص عملية المقارنة بالجدول رقم (1)

الجدول1 () مقارنة بين الشبكة المقترحة وشبكة الحماية من مايكروسوفت

الميزات	الشبكة المقترحة	شبكة الحماية من قبل مايكروسوفت
1- إدارة أمن الشبكة	سهلة	صعبة
2- الاتصال عن بعد	VPN	VPN and fire wall
3- عدد ال fire wall	1	3
4- الموثوقية	عالية جداً	قليلة
5- عدد أجهزة ال server	5	2
6- حماية البيانات من الاعتداءات الخارجية	متوفرة	متوفرة
7- حماية البيانات من الاعتداءات الداخلية	متوفرة	غير متوفرة
8- الأداء	سريع	بطيئ
9- استمرارية العمل	متاحة	غير متاحة
10- الكلفة	قليلة	عالية

2- الطريقة الثانية:[6]



الشكل(5) طريقة ثانية لحماية الشبكة من مايكروسوفت

تم فصل الشبكة إلى أقسام بواسطة الـ VLANs و باستخدام VLAN1، وهي بشكل عام لا ينصح باستخدامها؛ لأنها VLANالافتراضية ضمن الـ (switch or router)، وبالتالي تتعرض لهجمات كثيرة من قبل المخربين، وهي نقطة ضعف للشبكة، بالإضافة إلى أن عملية الاتصال بين هذه الأقسام سيصبح بطيئاً وصعباً ويتطلب (router or switch) من الأنواع ذات التكلفة العالية، كما تم استخدام server واحد لإدارة مهام الشبكة من الداخل -DNS-AD

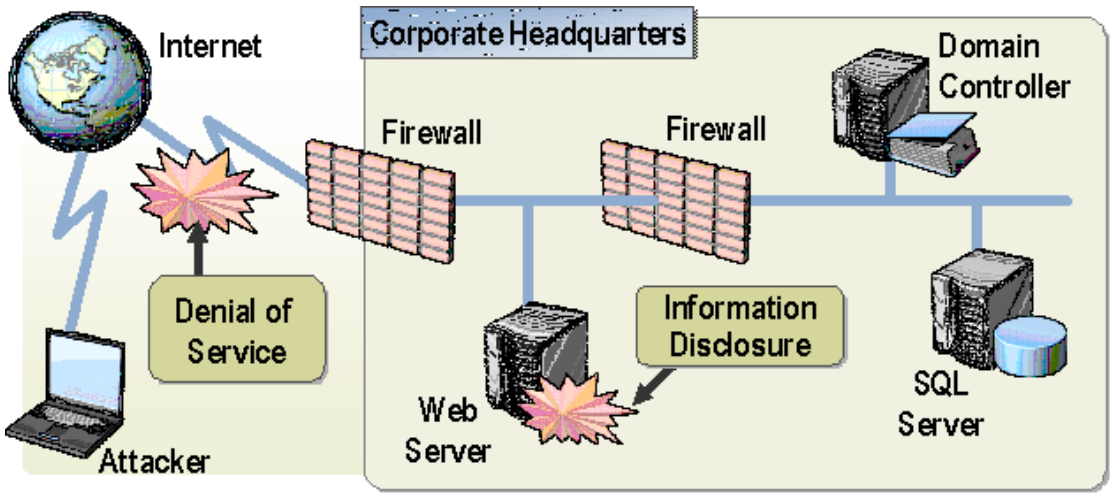
(DB) كما تم استخدام الـ server كـ proxy server نفسه وهذا يؤدي إلى بطء في الشبكة بشكل كبير، كما يزيد من مخاطر تعرض بيانات الشبكة للسرقة، بالإضافة إلى أن أي عطل في الـ server يؤدي إلى توقف الشبكة في حين أن الشبكة المقترحة لم نستخدم فيها VLAN1 وإنما استخدمنا VLAN 2 لحماية الـ Data Base من الاعتداءات الداخلية والخارجية، كما استخدمنا الـ group policy لتحديد المهام والإستراتجيات المتبعة ضمن الشركة، بالإضافة إلى أنه تم فصل الـserver الذي يقوم بإدارة الشبكة من الداخل عن الـ server الذي يقوم بعملية الحماية من الاعتداءات الخارجيةfirewall VPN كما أنه في الشبكة المقترحة أقمنا جهازين من Active Directoryوجهازين من Base Data بحيث أي عطل في أحد الجهازين (AD or DB) يؤدي إلى عمل الجهاز الآخر أوتوماتيكيا وهذا يجعلها أكثر موثوقية وسرعة.

نلخص عملية المقارنة بالجدول رقم (2)

الجدول2 () مقارنة بين الشبكة المقترحة و الطريقة الثانية لحماية الشبكة من مايكروسوفت

الميزات	الشبكة المقترحة	شبكة الحماية من قبل مايكروسوفت
1- إدارة أمن الشبكة	سهلة	صعبة
2- الاتصال عن بعد	VPN	Fire wall and proxy server
3- عدد ال fire wall	1	2
4- الموثوقية	عالية جداً	قليلة
5- عدد أجهزة ال server	5	1
6- حماية البيانات من الاعتداءات الخارجية	متوفرة	متوفرة ولكن بفعالية قليلة
7- حماية البيانات من الاعتداءات الداخلية	متوفرة	غير متوفرة
8- الأداء	سريع	بطيئ
9- استمرارية العمل	متاحة	غير متاحة
10- الكلفة	قليلة	عالية

3- الطريقة الثالثة:[2]



الشكل(6) طريقة ثالثة لحماية الشبكة من مايكروسوفت

في هذه الشبكة تم تقسيم مهام الشبكة على عدة servers حيث أن الـ domain controller server لإدارة (AD-DNS) والـSQL server لمعالجة البيانات و الـ web server لإدارة موقع الشركة على الإنترنيت كما تم استخدام fire wall لحماية الشبكة من الاعتداءات الخارجية و fire wall آخر لمنع المستخدمين ضمن الشبكة غير المسموح لهم بإرسال البيانات أو استقبالها عن طريق الإنترنيت من الوصول إلى الإنترنيت، إلا أن هذه الطريقة لم تراعِ حماية البيانات من الاعتداءات الداخلية، كما أن أي عطل في الـ domain controller server سيؤدي إلى منع المستخدمين من الدخول إلى الشبكة، ولا يوجد هنا بديل يقوم بالعمل حتى يتم إصلاح domain controller serverكما أنه إذا وجد عدد كبير من المستخدمين الذين يريدون الدخول إلى الشبكة في الوقت نفسه فسيؤدي ذلك إلى بطء في الشبكة؛ وذلك لأن user profile لكل المستخدمين موجودة في domain controller server، كما أن مطابقة اسم المستخدم وكلمة المرور تتم هناك.

بينما توقف الـ SQL server سيؤدي إلى توقف عمل الـ soft ware المحمل ضمن الشبكة، ويتوقف تخزين البيانات، وتضيع جميع العمليات المنفذة خلال فترة توقف الـ SQL server؛ وذلك لأنه لا يوجد بديل يقوم بالعمل حتى يتم إصلاحه، وكذلك لا يوجد وسيط بين الـ SQL server والـ user وهو الـApplication Server مما يعرض الـ Data Base إلى خطر كبير، بينما في الشبكة المقترحة استخدمنا وسيطاً بين الـ user و الـ Data Base وأيضاً VPN لحماية البيانات من الاعتداءات الخارجية و2 VLAN لحماية البيانات من الاعتداءات الداخلية، كما استخدمنا الـ group policy لتحديد المستخدمين الذين يحق لهم فقط العمل على الإنترنيت، وأيضاً في الشبكة المقترحة أقمنا جهازين هما Active Directoryوجهازين هما Data Base إذ إن أي عطل في أحد الجهازين(AD or DB) يؤدي إلى عمل الجهاز الآخر أتوماتيكياً، وهذا يجعلها أكثر موثوقية وسرعة، بالإضافة إلى الـApplication Server الذي يقوم بدور الوسيط بين المستخدم والـ Data Base . نلخص عملية المقارنة بالجدول رقم (3)

الجدول3 () مقارنة بين الشبكة المقترحة و الطريقة الثالثة لحماية الشبكة من مايكروسوفت

الميزات	الشبكة المقترحة	شبكة الحماية من قبل مايكروسوفت
1- إدارة أمن الشبكة	سهلة	صعبة قليلاً
2- الاتصال عن بعد	VPN	Fire wall
3- عدد ال fire wall	1	2
4- الموثوقية	عالية جداً	قليلة
5- عدد أجهزة ال server	5	3
6- حماية البيانات من الاعتداءات الخارجية	متوفرة	متوفرة ولكن بفعالية قليلة
7- حماية البيانات من الاعتداءات الداخلية	متوفرة	غير متوفرة
8- الأداء	سريع	متوسط السرعة
9- استمرارية العمل	متاحة	متاحة ولكن بفعالية أقل
10- الكلفة	قليلة	عالية

الاستنتاجات والتوصيات:

إن البيانات والمعلومات الموجودة ضمن الشبكة هي عصب الشركة، فتخريب هذه البيانات يؤثر سلباً في صناعة القرار ضمن الشركة، ويؤدي إلى تدميرها مع مرور الوقت، وفكرة تحول المعلومات السرية أو الخاصة إلى عامة في متناول الجميع فكرة مرفوضة بالنسبة إلى معظم الشركات الرسمية وغير الرسمية، وقد تناولنا في هذا البحث طريقة مبتكرة لحماية هذه البيانات ونتيجة المقارنة مع بعض الشبكات الأخرى هنالك بعض التوصيات يجب مراعاتها في أثناء بناء شبكة آمنة وهي:

1. عدم استخدام VLAN1 لأي غرض.
2. إغلاق كل البوابات غير المستخدمة في الـ Switch.
3. عدم استخدام أكثر من fire wall لأنه يبطئ أداء الشبكة.
4. تأمين حماية للشبكة من التهديدات الداخلية والخارجية.
5. تأمين استمرارية العمل من خلال تأمين أجهزة مساعدة(back up server).
6. عدم استخدام الـ Server لأكثر من غرض(DNS-AD-DB).

جدول الاختصارات:

LAN	Local area network
DNS	Domain name system
VLAN	virtual Local area network
IP	Internet protocol
L2TP	Layer 2 tunnelling protocol
PPTP	Point to point tunnelling protocol
DB	Data base
IPsec	IP security
RAID	Redundant array of independent disk
AD	Active directory
STP	Spanning tree protocol
VPN	Virtual private network
IT	Information technology

المراجع:

1- REIMER,S.;MULCARE,M.*Active directory for Microsoft windows server 2003*,Microsoft press,USA,2003,480.

2-FERGUSON,B.;HUGGINS,D.*MSCE Designing a Microsoft windows server2003active directory and network Infrastructure,* Microsoft press,USA,2003,512.

3-DELATE,G.;SCHAUWERS,G.*Network security fundamentals,*
Cisco press,USA,2004,480.

4-SMITH,B.;KOMAR,B.*Microsoft windows security resource kit,second edition,* Microsoft press,USA,2005,716.

5- معمو ،محمـــد شـــيخو ؛الطويل،هالة.*Windows server2003 دليـــل مـــدير النظـــام*،شـــعاع للنشـــر والعلوم،1096،2005.

6-Microsoft corporation, *Fundamentals of net work security,* Microsoft press,USA,2003,440.

7- شايندر ،ديبرا ليتلجون؛أماتو ،فيتو.*أساسيات شبكات الكمبيوتر*،الدار العربية للعلوم،2003،646.