Ministry Of Higher Education

Sebha University

College Of Information Technology

وزارة التعليم العالي

جامعة سبها

كلية تقنية المعلومات

قسم الشبكات و الإتصالات

بحث مقدم لإستكمال متطلبات نيل درجة البكالوريوس في الشبكات و الإتصالات

تحت عنوان

دراسة شاملة لتطوير نظام الخوادم لجامعة سبها

إعداد

المدني الكيلاني أبوبكر — **20170064**

فرج عبدالكريم علي — **20170049**

إشراف

د. حسن صالح القذافي

للعام الجامعي

خريف 2020

بِسْمِ اللهِ الرَّحْمَن الرَّحِيم

﴿يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنْكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ

وَاللَّهُ بِمَا تَعْمَلُونَ خَبِيرٌ﴾

صَدَقَ اللهُ العَظِيم

[سورة المجادلة الآية11]

الإهداء

إلى البلسم الذي يداوي جروحنا..

إلى من ربيانا صغيرا..

إلى من أحببنا ولن ننسى ...والدينا

إلى أشقائنا وشقيقاتنا الذين وقفوا بجانبنا طيلة السنين الماضية

إلى أصدقائنا الذين دعمونا وساندونا خلال دراستنا

إلى كل من له حق علينا...نهدي هذا العمل المتواضع

كلمة الشكر

قال رسول الله صلى الله عليه وسلم

"من لم يشكر الناس لم يشكر الله "

صدق رسول الله صلي الله عليه وسلم

الحمدلله على إحسانه والشكر له على امتنانه وتوفيقه لنا لبلوغ هذه المرحلة من الدراسة والعلم بعد شكره سبحانه وتعالى نتقدم بجزيل الشكر وخالص الامتنان إلي من شرفنا بإشرافه على هذا البحث الدكتور "حسن صالح القذافي" كذلك نتوجه بالشكر لجميع موظفي و مهندسين مركز تقنية المعلومات بجامعة سبها ، وعرفاناً بالجميل نتقدم بجزيل الشكر والتقدير إلي جميع أعضاء هيئة التدريس بكلية تقنية المعلومات ،والشكر والتقدير لكل من ساهم في أخراج البحث بالمستوي العلمي المنشود، ولكل من ساعدنا من قريب أو بعيد في إنجازه .

فهرس المحتويات

الإهداء II

كلمة الشكر III

الملخص IX

1. المقدمة 2

1.1 مشكلة البحث Research problem 4

2.1 حدود البحث Research Limits 4

3.1 أهمية البحث Significance of the Study : 4

4.1 أسئلة البحث Research Questions 5

5.1 أهداف البحث Research Objectives 5

6.1 النتائج المتوقعة Expected results 5

7.1 تنسيق البحث 5

2. الدراسات السابقة literature review 7

1.2 المناقشة Discussion 8

2.2 المحاكاة 9

3.2 بيئة النطاقdomain Environment 9

4.2 الدليل النشطActive Directory 10

1.4.2 مستخدمي و أجهزة الدليل النشط Active Directory Users and Computer (ADUC) 10

2.4.2 سياسات المجموعات Group Policy 11

5.2 نظام نطاق الأسماء(DNS) Domain Name System 12

6.2 خادم تكوين المضيف الديناميكي(DHCP) Dynamic Host Configuration Protocol 13

7.2 خادم الملفاتFile Server 13

8.2 خادم الطباعةPrinter Server 14

9.2 خادم الويبWeb Server 14
10.2 خدمة نشر ويندوز Windows deployment Services (WDS) 14
1.10.2 SETUP MGR TOOL..... 15
11.2 خدمة تحديثات ويندوز(Windows Server Update Services (WSUS 16
12.2 خادم سياسات الشبكة Network Policy Server (NPS)..... 16
13.2 جدار الحماية Firewall 19
1.13.2 Threat Management Gateway(TMG) 20
1.1.13.2 سياسات جدار الحماية TMG (TMG POLICIES)..... 22
2.1.13.2 TMG CLIENT 23
2.13.2 BANDWIDTH SPLITTER TOOL 24
3. منهجية البحث Research Methodology : 26
4. التطبيق العملي 31
1.4 عملية المحاكاة Simulation 31
2.4 إعداد و تهيئة خدمات الدليل النشطActive Directory..... 31
1.2.4 مستخدمي و أجهزة الدليل النشط Active Directory Users And Computers 32
2.2.4 تطبيق Group Policy..... 33
3.4 إعداد و تهيئة خادم نظام نطاق الأسماء DNS 35
4.4 إعداد و تهيئة خادم تكوين المضيف الديناميكي DHCP 37
5.4 إعداد و تهيئة خادم الملفات..... 38
6.4 إعداد و تهيئة خادم الطباعة 40
7.4 إعداد و تهيئة خادم الويب 41
8.4 إعداد و تهيئة خدمة نشر ويندوزWDS 43
1.8.4 Capture Image in WDS Server 44
9.4 إعداد و تهيئة خادم تحديثات ويندوزWSUS 45
10.4 إعداد و تهيئة خادم سياسات الشبكةNPS..... 48

11.4 إعداد و تهيئة جدار الحماية TMG 51

5. النتائج و المناقشة 58

1.5 الخلاصة 61

2.5 التوصيات و آفاق التطوير 62

3.5 المراجع 63

فهرس الأشكال

شكل (1.3) منهجية البحث 26
شكل (2.3) هيكلية البحث 29
شكل (1.4) الأجهزة والمستخدمين ضمن Domain 33
شكل (2.4) السجلات التي تم أنشائها على DNS 36
شكل (3.4) أعدادات خادم DHCP 38
شكل (4.4) الملفات التي تم انشائها ومشاركتها على خادم الملفات 39
شكل (5.4) تحديد مساحة الملفات بأستخدام File Server Resource Manager 40
شكل (6.4) ادارة الطابعات على الشبكة 41
شكل (7.4) أعدادات خادم الويب 42
شكل (8.4) عملية طلب الموقع من خادم الويب 42
شكل (9.4) أداة SETUPMGR و أعداداتها 44
شكل (10.4) أعدادات خادم WDS 45
شكل (11.4) التحديثات الي تم تحميلها على خادم WSUS 46
شكل (12.4) عملية طلب الأجهزة للتحديثات من خادم WSUS 47
شكل (13.4) عملية توزيع الأجهزة على المجموعات في خادم WSUS 48
شكل (14.4) ألية عمل خادم NPS 49
شكل (15.4) القيود المحددة من خادم NPS للاتصال بالشبكة 49
شكل (16.4) NAP Policies 50
شكل (17.4) ألية عمل جدار الحماية على الشبكة 51
شكل (18.4) أعدادات Intrusuion prevention System (IPS) 53
شكل (19.4) واجهة تطبيق TMG Client 54
شكل (20.4) عملية مراقبة المستخدمين عبر Bandwidth Splitter 55
شكل (21.4) أستهلاك ألمستخدم للحصة المخصصة له من عرض النطاق الترددي 56
شكل (1.5) التصميم النهائي للشبكة 60

فهرس الجداول

جدول (1.4) يوضح الصلاحيات التي تم تحديدها للمستخدمين داخل النطاق Domain 34
جدول (2.4) يوضح الصلاحيات المحددة للمستخدمين من خلال جدار الحماية TMG 52

الملخص

تهدف هذه الدراسة لتهيئة مجموعة من الخدمات الأساسية لتلبي متطلبات المستخدمين في شبكة جامعة سبها مع توفير الحماية لهذه الخدمات و الأمان للمستخدمين ضد التهديدات الداخلية و الخارجية لشبكة الجامعة ، حيث يعتبر عدم تكوين الخدمات بشكل صحيح و عدم تطبيق آليات الحماية و الأمان من أبرز المشكلات التي تواجهها الشبكات المعتمدة على بيئة النطاق Domain و نموذج الخادم–العميل (Client/Server) .

و في بيئة الشبكة الخاصة بجامعة سبها تمت دراسة حالة الخوادم المتواجدة في مركز تقنية المعلومات و ذلك لغرض معرفة أوجه القصور و معالجتها .

حيث أوضحت الدراسة عملية تهيئة الخوادم بأستخدام نظام تشغيل windows server 2012 عبر تقنية المحاكاة و تفعيل الخدمات عليها بهدف توفير أدارة مركزية عبر الخوادم لتلبي احتياجات المستخدمين ، بالأضافة إلى تهيئة عدة خدمات على هذه الشبكة من خلال النظام الجديد والتي لم تتوفر في الأنظمة القديمة و توفير الحماية لها عبر تهيئة خدمات الحماية والأمان المطلوبة و تفعيل أدوات المراقبة لتتبع أداء المستخدمين و كذلك وضع المستخدمين ضمن مجموعات وفق الجهات التي ينتمون إليها وتحديد صلاحيات كل مستخدم بناء على ذلك .

وقد حقق البحث نجاحاً بتوفيره للخدمات المطلوبة و رفعه لمستوى الحماية و الأمان على ما كان عليه سابقا .

الفصل الأول

مقدمة البحث

1. المقدمة

تعرف شبكات الحاسوب بأنها مجموعة من الأجهزة المتصلة مع بعضها البعض من خلال وسائط اتصال سلكية أو لاسلكية ، تسمح لأجهزة الحاسوب بالاتصال المباشر بين مستخدمي نفس الشبكة و مشاركة المعلومات و الموارد في ما بينهم.

و يوفر استخدام شبكات العديد من الميزات منها المشاركة في معدات و البرمجيات كما توفر إمكانية للتوسع و تدعم مركزية إدارة الشبكة مثل إدارة المستخدمين و الموارد الموجودة على الشبكة .

كما يجب أن تحقق شبكات الحاسوب ثلاث مفاهيم أساسية و هي الأداء و الموثوقية و الأمان حيث يقصد بالأداء فاعلية البرامج المستخدمة في الشبكة و فاعلية التوصيلات اما الموثوقية فيقصد بها إمكانية حدوث أخطاء و فشل في الاتصال حيث أن كلما زاد احتمال حدوث الأخطاء تقل موثوقية الشبكة أما المقصود بالأمان هي الإجراءات التي يمكن من خلالها توفير الحماية القصوى للبيانات في الشبكة من المخاطر التي تهددها .

و تمثل بيئة المجموعات (workgroup) و بيئة النطاق (domain) طرق مختلفة لربط أجهزة الحاسوب في الشبكات حيث يتمثل الاختلاف الرئيسي بينهم في كيفية إدارة أجهزة الحاسوب والموارد الأخرى الموجودة على الشبكة ، و في نموذج workgroup أو ما يعرف بشبكات الند للند (peer to peer) تكون جميع الأجهزة المتصلة على نفس المستوى من الصلاحيات التي تتشارك الموارد و مسؤوليات الشبكة فيما بينها ، أما في نموذج domain تكون موارد الشبكة متمركزة في جهاز واحد و هو الخادمserver و الأجهزة المتصلة بها Client مما يجعل الوصول إلى المعلومات أو الموارد المطلوبة أسهل بكثير مما لو كانت الموارد موزعه على أجهزة مختلفة كما يسهل أدارة البيانات و التحكم فيها .

و يعتبر الخادم جهاز أساسي في الشبكات و للبدء في إعداد الخادم يجب تنصيب نظام التشغيل عليه حيث يتم تخصيصه و تكوينه لأداء و ظيفة معينه أو مجموعة من الوظائف في نفس الوقت ، يوجد العديد من أنظمة التشغيل الخادم من أشهرها (Linux و Unix و Windows و FreeBSD و MacOS X) و يعتبر نظام تشغيل Windows Server هو الأكثر شيوعا .

و أصـــدرت شـــركة Microsoft مجموعـــة مـــن أنظمـــة التشـــغيل المخصصـــة للخـــادم منهـــا (windows server 2003,2003R2,2008,2008R2,2012,2012R2,2016,2019).

حيث وفرت أنظمة تشغيل Windows Server 2000&2003 الوظائف الأولية التي لا تزال قيد الاستخدام حتى اليوم و التي تشمل دعم The Extensible Markup Language (XML) كذلك استخدام الدليل النشط Active Directory للمصادقة بين المستخدم و الخادم ، في نسخة Windows Server 2003 R2 التي شملت تحسينات في خادم Active Directory و إضافة إمكانية تطبيق سياسات المجموعة Group Policy كذلك تمت تحسينات كبير في نظام Hyper-V من Microsoft مما ساعد مستخدمين Windows Server لإنشاء أجهزة افتراضية (VMs) و في نظام Window Server 2008 & 2008 R2 تم تضمين أدوات إدارة برامج جديدة تسمى Event Viewer و Server Manager منحت هذه الأدوات المساعدة للمسؤولين في الشبكة للتحكم في أنشطة الخادم كما شهد الإصدار 2008 R2 تحديثات إضافية لخدمة الدليل النشط Active Directory لدعم تنفيذ سياسة المجموعة Group Policy بشكل أفضل ، كما تمت إضافة بعض الخدمات الجديدة ، مثل Remote Desktop Services ، و في نسخة Windows Server 2012 تم إضافة ميزة العمل على السحابة Cloud كما تمت إضافة مجموعة من التحسينات التي ركزت على تحسين وظيفة Hyper-V ، إما Windows Server 2012 R2 كانت التغييرات عبارة عن تحسينات للوظائف اللازمة للتكامل مع الخدمات السحابية كما شهد هذا الإصدار المزيد من التحديثات في PowerShell ، و في Windows Server 2016 ، تمت إضافة خادم جديد يسمى Nano Server والذي كان تطبيق لخادم صغير الحجم مع واجهات محدودة ، مما يجعله أكثر أمانًا من الهجمات كما تمت إضافة Network Controller الذي ساعد على إدارة جميع أجهزة الشبكة ، سواء كانت فعلية أو افتراضية ، من مكان واحد كما تم تحسين Hyper-v عبر دعمه للتشفير ، و يعتبر Windows Server 2019 احدث إصدار من أنظمة تشغيل الخوادم و من أهم الإضافات عليه Windows Admin Center لتوفير إدارة مركزية للخادم.

1.1 مشكلة البحث Research problem

مع تزايد استخدام شبكات (Client/Server) و بيئة النطاق (Domain) و التقدم التقني الذي حدث في أنظمة تشغيل الخادم و الخدمات التي توفرها هذه الأنظمة ، و ضعف الخدمات التي توفرها الإصدارات القديمة ، كان لابد من مواكبة التطور الحاصل على هذه الأنظمة ، و لذلك فقد تم من خلال هذا البحث استخدام نظام تشغيل Windows Server 2012 بالإضافة إلى نظام تشغيل Windows Server 2008 r2 وذلك لبناء شبكة افتراضية خاصة بجامعة سبها تعمل بكفائة و توفر المستوى المطلوب من الحماية .

و من أبرز المشاكل التي تواجه الشبكة الحالية لجامعة سبها :-

1. وجود ضعف في بعض الخدمات التي تقدمها الشبكة الحالية لجامعة سبها .
2. القيود التي تم تطبيقها لا توفر المستوى المطلوب من الحماية مما يتسبب في ظهور تهديدات داخلية .
3. ضعف آليات و أساليب الحماية مما يقلل من الأمان للمستخدمين و يجعل الشبكة أكثر عرضه للتهديدات الخارجية .

2.1 حدود البحث Research Limits

يقتصر البحث على تهيئة مجموعة من الخدمات بأستخدام نظام التشغيل Windows Server 2008R2 & 2012 عبر تقنية المحاكاة نظرا لضعف الأمكانيات الموجودة للعمل على خوادم وتهيئتها و أعدادها ، حيث تم تفعيل مجموعة من الخدمات و أدوات المراقبة وكذلك تفعيل مجموعة من آليات الحماية و الأمان .

3.1 أهمية البحث Significance of the Study :

تتلخص أهمية الدراسة في التالي :

إعداد و تكوين مجموعة من الخوادم و الخدمات الأساسية تعمل بشكل متكامل مع بعضها لبعض بشكل افتراضي للحصول على خوادم تلبي متطلبات المستخدمين و تحقق أقصى قدر من الحماية و الأمان ضد تهديدات الداخلية و الخارجية ضمن شبكة جامعة سبها .

4.1 أسئلة البحث Research Questions

1. هل بالأمكان تكوين الخادم بطريقة صحيحة ليوفر المستوى المطلوب من الخدمات على شبكة جامعة سبها ؟
2. هل يمكن توفير المستوى المطلوب من الأمان للشبكة عبر وضع القيود على المستخدمين ؟
3. هل سيتم إعداد آليات الحماية بحيث توفر الأمان للمستخدمين من التهديدات الخارجية ؟

5.1 أهداف البحث Research Objectives

1. لتهيئة و إعداد الخوادم لتوفر الخدمات الأساسية لجامعة سبها .
2. لتحديد الصلاحيات و القيود لمستخدمي الشبكة وفق الفئات و المجموعات التي ينتمون إليها .
3. للتحكم في اتصال المستخدمين بالشبكات الخارجية وشبكة الانترنت .

6.1 النتائج المتوقعة Expected results

1. تقديم الخدمات المطلوبة عبر الشبكة بكفائة و بدون أي أخطاء .
2. الحصول على مستوى الحماية المطلوب للبيانات و الخدمات داخل الشبكة .
3. التقليل من إستهلاك عرض النطاق الترددي bandwidth و حماية الشبكة من التهديدات الخارجية .

7.1 تنسيق البحث

تناول الفصل الأول ملخص و مقدمة حول البحث و مناقشة لمشكلة البحث و أهميته كما تم طرح بعض الأسئلة حول البحث و تحديد الأهداف و النتائج المتوقعة .

و ناقش الفصل الثاني أهم الدراسات المتعلقة بالبحث و تعريف بالتقنيات المستخدمة .

كما ناقش الفصل الثالث تعريفاً بمنهجية دارسة الحالة و الخطوات المتبعة لتطبيق المنهجية و تحديد الهيكل العام للبحث .

و ناقش الفصل الرابع الخطوات العملية للتطبيق العملي و أهم أدوات و وسائل الحماية المستخدمة و في الفصل الخامس سيتم طرح نتائج البحث والخلاصة وآفاق التطوير للبحث .

الفصل الثانـي

الدراسات السابقة

2. الدراسات السابقة literature review

المحاكاة الافتراضية تكتسب زخماً في مجتمع تكنولوجيا المعلومات ، على الرغم من أن الأجهزة الافتراضية ليست مفهومًا جديدًا ، إلا أن التطورات الحديثة في تكنولوجيا الأجهزة والبرامج جعلت المحاكاة الافتراضية في طليعة إدارة تكنولوجيا المعلومات حيث أن أستقرارها و توفير التكاليف ، وسهولة الإدارة هي من بين أسباب الأرتفاع الأخير في استخدام الافتراضية ، و يمكن تصنيف الأجهزة الافتراضية لمحاكاة البرمجيات ونظام التشغيل منذ تحويل الخوادم المركزية الى أجهزة افتراضية مما تسبب في تطور الآلات الافتراضية حيث انها ستلعب دورًا كبيراً في إدارة الأنظمة [1].

يمكن دمج أكثر من خدمة على نفس الخادم حيث تسمح لك المحاكاة الافتراضية بدمج العديد من الخوادم في خادم افتراضي واحد مما يقلل من تكاليف الأجهزة والكهرباء والتبريد والتكاليف الإدارية ، و تعمل هذه الخوادم الظاهرية بشكل مستقل تمامًا عن بعضها البعض ، لذلك إذا تعطل أحدها ، فلن تتأثر باقي الخوادم ، و يعد التخطيط لعملية دمج الخادم وتنفيذها عملية معقدة ، كذلك ناقشة الدراسة عملية إنشاء شبكة افتراضية لتبادل المعلومات أو تقديم خدمة إلى أجهزة أو أجهزة حاسوب افتراضية أخرى و استخدم المحاكاة الافتراضية لدعم الوسائط القابلة للإزالة مثل الأقراص الضوئية للأقراص المضغوطة أو أقراص DVD لتقليل تكاليف الخادم ونفقات الإدارة والتعقيد [2] .

كما يعتبر الدليل النشط مكون أساسي للبنية التحتية للشبكة للعديد من الشبكات التنظيمية وهو مهم للأمن الداخلي للشبكة من خلال التخفيف من التهديدات الداخلية ومع ذلك ، فإن إدارتها غالبًا ما تكون مهمة معقدة وتستغرق وقتًا طويلاً ،كما يمكن أن تؤدي أخطاء التكوين إلى ثغرات أمنية خطيرة و تبحث المنظمات أمكانية معالجتها باستخدام أدوات لحل المشاكل الأمنية [3] .

و الدليل النشط يتم استخدامه عبر العديد من المؤسسات لمركزية التحكم في عمليات تسجيل دخول المستخدمين إلى موارد المؤسسة والشبكة ، والذي يتيح إدارة مركزية وآمنة للشبكة و تحتوي خوادم الدليل النشط على بعض نقاط الضعف و هناك العديد من الإرشادات الموصى بها لمعالجة مشكلات الأمان ويحتوي الدليل النشط على دعم مضمن لعناصر التحكم في الأمان ، كما هناك العديد من الطرق الممكنة لتعزيز أمان الدليل النشط والشبكة و يؤدي عدم تنفيذ الدليل النشط في المؤسسات

الكبيرة إلى فقدان السيطرة على موارد ومعلومات المستخدم مما قد يؤدي إلى تهديدات أمنية خطيرة [4] .

و يوفر نموذج (Client– server) أمكانية الربط بين المستخدم و الخادم لغرض تعزيز مشاركة المعلومات فيما بينهما ليسمح للعديد من المستخدمين بالوصول إلى نفس الخدمات في نفس الوقت ، و وفر نموذج Client– server بيئة مناسبه للتحكم المركزي في المستخدمين و تعزيز أمان الشبكة و إمكانية التوسع في الشبكة بسهولة مما يسمح بإضافة مستخدمين جدد و تفعيل خدمات جديدة ، يمثل المستخدم (Client) او العميل الذي يقوم بطلب عمليات المعاجلة بينما الخادم server هو مقدم الخدمة حيث يقوم بعمليات المعالجة ، يتم تنظيم طلبات المستخدمين وتحديد أولوياتها في نظام جدولة ، مما يساعد الخوادم على التعامل مع الطلبات في حالة تلقي الطلبات من العديد من المستخدمين في فترة زمنية قصيرة [5].

كما أن اختيار واختبار وبناء خادم نشر الشبكة الهجين الذي يجب أن يكون قادرًا على تثبيت أنظمة التشغيل المستندة إلى نظام تشغيل Windows و Linux تم تصميم الخادم لمساعدة مسؤولي النظام في جامعة ميكيلي للعلوم التطبيقية ، ركزت الدراسة على نظام التشغيل Windows ، لأنه كان نظام التشغيل الأساسي المستخدم في الجامعة ، في البداية تم تصنيف الطرق المختلفة حسب المواصفات الفنية ثم اختبارها لإثبات قابليتها للاستخدام يتم تنفيذ عمليات نشر Windows باستخدام مجموعة أدوات النشر من Microsoft ومجموعة أدوات التقييم والنشر لـ Windows الاستراتيجيات المختارة هي High–Touch و Low–Volume و Lite–Touch و High–Volume ، يتم نشر أنظمة التشغيل المستندة إلى Linux مع حزمة Syslinux المثبتة في Windows Deployment Server أظهرت نتائج الدراسة أن نشر الشبكات لأنظمة التشغيل يوفر قدرًا كبيراً من الوقت على المدى الطويل وليس من الصعب إعداده ، و توضح الدراسة نقاط الاهتمام التي يجب الاهتمام بها أثناء التنفيذ العملي و الخطوات لازم إتباعها [6] .

1.2 المناقشة Discussion

أوضحت الدراسات السابقة أهمية استخدام نموذج (Client/Server) و الميزات التي يقدمها مثل مركزية التحكم كما يعزز الجوانب الأمنية للشبكة و دعم لتوسع الشبكة بشكل أكبر كما أوضحت الدراسات السابقة أهمية المحاكاة الافتراضية و تأثيرها في تطورات مجال تكنولوجيا المعلومات كما

أنها توفر التكاليف و القدرة على الإدارة كذلك توفر المحاكاة الافتراضية عملية دمج أكثر من خادم في خادم افتراضي واحد و التي توفر بدورها في عدد الأجهزة التي يتم إنشائها افتراضيا و عدم تأثيرها على بعضها في حالة حدوث عطل في احدها ، كذلك ناقشة الدراسات جانبا مهم و هو دليل النشط (Active directory) حيث يعتبر من الخدمات الأساسية و مهم للأمن الداخلي للشبكة و التحكم في المستخدمين ، و يؤدي عدم تنفيذ الدليل النشط إلى فقدان السيطرة على موارد الشبكة و معلومات المستخدم مما يؤدي إلى مشاكل أمنية خطيرة ، كما ناقشة الدراسات السابقة أخطاء التكوين التي ينتج عنها ثغرات أمنيه خطيرة و التي يتم البحث عن طرق لمعالجتها باستخدام أدوات تساعد في حلول المشاكل الأمنية .

2.2 المحاكاة

تتيح لك المحاكاة الافتراضية العمل على أجهزة وهمية غير حقيقية على الجهاز الحقيقي و تمكنك من تنصيب أنظمة تشغيل لتعمل و كأنها أنظمة منفصلة قائمة بذاتها لا تربطها علاقة بنظام التشغيل المخصص للجهاز الحقيقي ، حيث تتيح لك أستخدام أكثر من نظام تشغيل في نفس الوقت مما يوفر سهوله في التحكم بهذه الأنظمة إذ أنها توجد داخل ملفات محدده المسار فلكل نظام ملف خاص به ، كما توفر المحاكاة الوقت و الجهد و المال بأستخدام أنظمة افتراضية بدل من أجهزة حقيقية مكلفة الثمن [7] .

3.2 بيئة النطاق domain Environment

تعرف هذه طريقة باسم Client/Server و فيها يتم تثبيت الدليل النشط Active Director على الخادم و هذه الخدمة تسمى Domain Controller أي المتحكم في Domain و يتحكم في جميع صلاحيات الأجهزه و مستخدميها على شبكة أي أن التحكم يكون بشكل مركزي من خلال خدمة Domain Controller ، كما أن أستخدام بيئة النطاق Domain يزيد من الأمان و الحماية داخل الشبكة و سهولة إدارتها و التحكم في مواردها [8].

يوفر نظام تشغيل windows server حزمة من البرامج الأساسية التي تسمح للخادم بأداء وظيفة معينه بعد التثبيت و التكوين الصحيح التي تسمى Roles و هي الخدمات الأساسية في النظام مثل (DNS,DHCP,WSUS,WEB Server) وعند تكوين هذه الخدمات يطلب منك إضافة بعض الخصائص تسمى features من اجل عمل الخادم بشكل أفضل [8].

4.2 الدليل النشط Active Directory

هو عبارة عن خدمة تقوم بإنشاء قاعدة بيانات تجمع بيانات كل مستخدمين أو العملاء Client و يضم أيضا خدمات و موارد النظام وذلك لتمكين التحكم المركزي بالأجهزة داخل الشبكة من خلال وضع صلاحيات معينه لكل جهاز بشبكة [8].

يتضمن الدليل النشط active director الأتي :

- The schemaمجموعة من القواعد التي تحدد فئات الكائنات و السمات الموجودة في الدليل النشط و القيود المفروضة على الكائنات و تنسيق أسمائها .
- A global catalog يحتوي على معلومات حول كل كائن و يسمح للمستخدمين و مسؤولي النظام بالوصول لهذه المعلومات و الولوج إليها .
- A query and index mechanism بحيث يتيح لمستخدمي الشبكة لاستعلام عن الكائنات و خصائصها في الشبكة .
- A replication service تحتوي على نسخه كاملة من كافة معلومات active director و يتم تحديث المعلومات في حال حدوث أي تعديل بشكل دوري .

يوفر Active Directory عدة خدمات لإدارة المستخدمين و أجهزتهم التي تم تسجيلها في النطاق Domain [8].

1.4.2 مستخدمي و أجهزة الدليل النشط Active Directory Users and Computer (ADUC)

هي وحدة إدارية تمكنك من إدارة الكائنات (المستخدمون و أجهزتهم) داخل النظام و من مهامها :

- إضافة و حذف و المستخدمين .

- إنشاء وحدة تنظيمية جديدة Organizational Unit – OU لتنظيم كائنات الدليل النشط و نقلها الى وحدات تنظيمية مختلفة بغرض ترتيبها .
- إدارة Group police و وضع الصلاحيات .
- البحث عن الكائنات داخل قاعدة بيانات الدليل النشط Active Directory
- يمكن من خلالها أنشاء حساب المستخدم بداخل (Organizational Unit – OU) و يتم تحديد الاسم الخاص بها بناء على المكان الموجود به المستخدمون أو الوظيفة التي يقومون بها ، حيث يتم تطبيق Group Policy عليها وتحديد صلاحيات المستخدمين [8] .

يتم تحديد عدد من الخصائص لكل مستخدم منها :

First name : الاسم الأول من أسم المستخدم

Last name : الاسم الأخير من أسم المستخدم

Initials : يمثل الحرف الأول من أسم المستخدم الأوسط

Full name : يتم ملئ هذه الخانة بشكل تلقائي

User logon name :يمثل أسم المستخدم لتسجيل الدخول إلى أجهزة النطاق Domain عن طريق الاسم الأول و الأخير للمستخدم

Password :كلمة المرور و يتم إعادة تعينها من قبل المستخدم عند أجراء تسجيل دخول للنظام لأول مره.[8] .

2.4.2 سياسات المجموعات Group Policy

هي مجموعة من السياسات التي توضع بهدف التحكم بكيفية عمل مستخدم أو جهاز واحد و صلاحياته أو مجموعة من المستخدمين أو الأجهزة و صلاحياتهم ضمن وحدة تنظيم Organizational Unit – OU أو ضمن مجال معين Domain أو موقع Site ، حيث تستخدم لضبط أداء المستخدم من خلال تطبيق سياسات تحدد صلاحياتهم و مدى الحرية المسموح بها فيما يتعلق باستخدام البرامج و أجهزة الحاسوب و موارد شبكة [8].

ويتم تطبيق الصلاحيات على مستويين :

المستوى الأول خاص بأجهزة الحاسوب Configuration Computer بحيث نحدد مجموعة من السياسات المطبقة على جهاز الحاسوب بصرف النظر عن المستخدم الذي يقوم بالعمل عليه و هذه سياسات يتم تطبيقها أثناء عملية Booting .

المستوى الثاني و هو المستخدمين User Configuration و فيه تحدد السياسات الخاصة بالمستخدم بصرف النظر عن الجهاز الذي يقوم بالعمل عليه و يتم تطبيق هذه السياسات بعد أن يقوم المستخدم بعملية الدخول login فور كتابة أسم المستخدم و كلمة المرور يتم تطبيق السياسات على المستخدم.

5.2 نظام نطاق الأسماء (DNS) Domain Name System

هو نظام يقوم بتخزين المعلومات المتعلقة بأسماء النطاقات (Domain Name) الموجودة فى قاعدة البيانات الموزّعة على الإنترنت و يقوم (DNS) بربط المعلومات و العناوين بأسماء النطاقات المرتبطة و يعمل DNS على إنشاء قاعدة بيانات تحتوي على سجلّات تربط عناوين (IP) بأسماء النطاقات ، عندما تريد الوصول إلى أحد المواقع مثلا "www.google.com" يرسل المتصفح استعلاماً لمعرفة عنوان IP إلى خادم "DNS" المُعرّف على جهازك (سيسمى الخادم المحلي) يبحث DNS عن IP إذا كان مخزّناً لديه في قاعدة البيانات المحلية فإذا وجده يرسل ردا إلى الجهاز المُستعلِم [8] .

كما يحتوي DNS على ما يعرف بالذاكرة المؤقتة (Cash) التي تحتوي على العناوين التي سبق للخادم أنْ استعلم عنها و يقوم بالاحتفاظ بها لفترة محدودة، ليقوم بالرجوع إليها مباشرة إذا طلبت منه مرة أخرى دون الحاجة إلى إعادة الاستعلام [9].

و يتكون(DNS) من الأتي :

1 مجال الأسماء (Domain Name Space) :

يحتوي مجال الأسماء على جميع عناصر النطاق، حيث يتم إلحاق أسماء عناصر النطاق به، ويمكن إعتباره قاعدة بيانات النظام.

2 خدمات الأسماء (Name Servers or Services) :

يحتوي خادم "DNS" على معلومات عن عناوين الحواسيب الموجودة على الشبكة وعناوين الـ IP الموافقة لها حيث تقدم هذه المعلومات إلى المستخدمين الذين يقومون بإرسال الطلبات "Requests" من أجل الحصول على مثل هذه المعلومات وفي حال لم يكن الخادم قادراً على تقديم المعلومات لسبب أو لآخر، فإنّ الطلب يمكن أنْ يمرر إلى خادم آخر .

3 أجهزة العملاء على الشبكة (Resolvers or Clients) :

وهم مستخدمي الشبكة الذين يقومون بتقديم طلبات تحويل أسم معطى إلى عنوان IP الموافق والضروري من أجل تحقيق الاتصال عبر الشبكة.[8] .

6.2 خادم تكوين المضيف الديناميكي Dynamic Host Configuration Protocol (DHCP)

خادم DHCP هو خادم شبكة يوفر عناوين IP والبوابات الافتراضية Gateway ومعاملات الشبكة الأخرى بشكل تلقائي ويقوم بتعيينها إلى أجهزة العميل ، و يعتمد على البروتوكول القياسي المعروف باسم بروتوكول التكوين الديناميكي للمضيف أو DHCP للرد على طلبات العملاء.

يرسل خادم DHCP تلقائيًا معاملات الشبكة المطلوبة للعملاء للتواصل بشكل صحيح على الشبكة و بدونها يتعين على مسؤول الشبكة إعداد كل جهاز ينضم إلى الشبكة يدويًا ، الأمر الذي قد يكون مرهقًا خاصة في الشبكات الكبيرة ، و عادة ما تعين خوادم DHCP لكل عميل عنوان IP لا يتكرر، والذي يتغير عندما تنتهي فترة أستخدام العميل لعنوان IP .[8]

7.2 خادم الملفات File Server

خادم الملفات هو خادم مركزي في شبكة يوفر أنظمة ملفات أو أجزاء من نظام ملفات للعملاء المتصلين بشبكة لذلك توفر خوادم الملفات للمستخدمين مكان تخزين مركزي للملفات الموجودة على وسائط البيانات الداخلية ، والتي يمكن لجميع العملاء المصرح لهم الوصول إليها ، يحدد مسؤول الشبكة قواعد صارمة فيما يتعلق بالمستخدمين الذين لديهم حقوق الوصول على سبيل المثال ، يمكن المسؤول من تعيين الملفات التي يمكن رؤيتها وفتحها بواسطة مستخدم معين أو مجموعة من

المستخدمين ، و ما إذا كان يمكن عرض البيانات فقط أو إضافتها أو تحريرها أو حذفها أيضًا من قبل المستخدم [10].

8.2 خادم الطباعة Printer Server

خادم الطباعة هو مكون شبكة نشط يتلقى مهام الطباعة من المستخدمين المتصلين او مجموعات المستخدمين داخل الشبكة و تعيد توجيهها إلى الطابعات أو الأجهزة الطرفية الأخرى داخل الشبكة ، يوفر لك خادم الطباعة أداء عالي و معدلات نقل البيانات عالية و خيارات إدارة متنوعة و دعما شاملا للأنظمة و بروتوكولات التشغيل ، حيث توفر عملية نقل الملفات من جهاز حاسوب إلى أخر قبل طباعه من مزايا استخدام خادم الطباعة انه يسمح لعدة مستخدمين بمشاركة نفس الطابعة و تجنب الأضرار من نقل الملفات من جهاز حاسوب إلى أخر [11].

9.2 خادم الويب Web Server

خادم الويب هو نظام معلومات موزع قائم على الانترنت يمكن لأي شخص لديه جهاز كمبيوتر متصل بالانترنت إسترداد المعلومات بسهولة عن طريق إعطاء عنوان ويب ، يعد الويب طريقة ممتازة لنشر المعلومات و إتاحتها عل مدار الساعة طوال أيام الأسبوع يمكن أيضا جمع المعلومات من مستخدمي الويب و العملاء من خلال نماذج عبر الانترنت .

الهدف الأساسي لخادم الويب هو معالجة و إرسال صفحات الويب للمستخدمين ، يتم إجراء هذا الاتصال الداخلي باستخدام بروتوكول نقل النص التشعبي (Hypertext Transfer Protocol HTTP) تحتوي صفحات الويب في الغالب على محتوى ثابت يتضمن مستندات HTML و الصور و ملف CSS و ما إلى ذلك يدعم الخادم أيضا بروتوكول SMTP بروتوكول نقل البريد البسيط لإرسال البريد الالكتروني و بروتوكولFTP برتوكول نقل الملفات والذي يعمل على نقل الملفات [12] .

10.2 خدمة نشر ويندوز Windows deployment Services (WDS)

يمكن استخدام (WDS) لتثبيت نظام التشغيل على الأجهزة من خلال الشبكة بحيث لا يقوم مسؤول النظام بتثبيت النظام على كل جهاز بشكل فردي ، حيث يتم وضع نسخه من نظام التشغيل على خادم WDS و تنصيبها على أجهزة الشبكة عن طريق استخدام تقنية إرسال البث المتعدد Multicast مما

يعني أن أجهزة حاسوب متعددة تتلقى نفس نسخة نظام التشغيل مع تقليل استهلاك النطاق الترددي عبر الشبكة ، كما يمكن (WDS) الإرسال بشكل أحادي Unicast بمعنى تنصيب نظام تشغيل بشكل منفصل لكل جهاز ، ويعمل خادم (WDS) مع أنظمة التشغيل من خلال ما يسمى صور (image) والتي يقوم مسؤول النظام بإضافتها ، و يمكن من خلال خدمات إدارة الصور managing image التي يوفرها خادم WDS إدارة صور لأنظمة التشغيل كاملة أو لنسخة نظام التشغيل[13].

يستخدم WDS أربع أنواع من الصور image :

1 Boot image : تمثل صورة خاصة تمكن الحاسوب من الإقلاع والبدء في تثبيت نظام التشغيل حيث توجد صورة تمهيديه افتراضية تسمى Boot.wim في مجلد الملفات الخاصة بأنظمة التشغيل Windows .

2Install image : تحتوي هذه النسخة على نظام التشغيل بالإضافة إلى تحديثات البرامج والتطبيقات الإضافية توجد صورة تثبيت افتراضية تسمى Install.wim في مجلد الملفات الخاصة بأنظمة التشغيل Windows .

3 Discover image : تعتبر نسخه خاصة للأجهزة التي لا يمكنها تحميل برامج التشغيل المناسبة لبدء جلسة مع خادم WDS .

4 Capture image : يمكِّن هذا النوع من أخد نسخة أو صورة لنظام تشغيل من جهاز على الشبكة و استخدامها كصورة لتثبيت نظام تشغيل على الأجهزة الأخرى [14].

1.10.2 SETUP MGR TOOL

هي أداة تستخدم لتجهيز و تهيئة أي نظام تشغيل ليتم تثبيته على الأجهزة ، حيث أن هذه الأداة تعمل على إدخال البيانات المطلوبة عند تحميل نظام التشغيل وتجهيز النسخة ليتم تثبيتها ، و يمكن من خلالها تجهيز نظام التشغيل ببيانات مثل اسم الجهاز ومعلومات النطاق Domain وكذلك الرقم التسلسلي لتفعيل نظام التشغيل في حال وجوده كما يمكن من خلالها تجهيز النظام بأسم مستخدم وكلمة مرور وكذلك تحديد لغة النظام والوقت، وعند إدخال هذه البيانات يمكن أخذ نسخة من هذا النظام وتثبيتها على أي جهاز أخر .

11.2 خدمة تحديثات ويندوز Windows Server Update Services (WSUS)

هو إحدى خدمات مايكروسوفت التي تمكن المسؤولين من إدارة توزيع التحديثات والإصلاحات العاجلة التي تصدر لمنتجات Microsoft الموجودة على أجهزة الكمبيوتر في الخادم يتم تحميل هذه التحديثات من موقع مايكروسوفت ومن ثم توزيعها على أجهزة الكمبيوتر على الشبكة بهدف توفيرها عبر الشبكة حيث يتم تحميل التحديثات مرة واحدة فقط عن طريق الخادم وأيضا ضمان عدم تنزيل أى تحديثات لم يختبرها و يوافق عليها مدير أو مسؤول الشبكة ، كما يتيح Wsus عدة خصائص من أهمها تحسين موارد الشبكة ، التحميل التلقائي للتحديثات ، التحميل المستهدف للتحديثات لجهاز حاسوب معين أو مجموعات من أجهزة الحاسوب ، و تحميل التحديثات الأمنية و التعريفات عبر الشبكة [14].

12.2 خادم سياسات الشبكة Network Policy Server (NPS)

خادم سياسات الشبكة أو ما يعرف ب NPS SERVER والذي يعتبر من أهم الخوادم المستخدمة في الجانب الأمني للشبكة ، حيث أن هذا الخادم يعمل على إنشاء مجموعة من السياسات POLICY التي تحتوي على قيود أو شروط بحيث لا يستطيع أي جهاز COMPUTER أو مستخدم USER أن يتصل بالشبكة إلا في حال تحقيق هذه الشروط [14].

يجبر خادم NPS المستخدمين والأجهزة على اختبار كل السياسات POLICIES الموجودة عليه وذلك بأستخدام عدة آليات أو خدمات والتي يتم تهيئة و إعداد NPS للعمل معها ، والتي من المفترض لأي مستخدم أو جهاز يرغب بالاتصال بالشبكة أن يتعامل مع هذه الخدمات (أي أن عملية التحقق AUTHINTICATION تتم من خلال هذه الخدمات) ، وهذه الخدمات عادة ما تكون على أجهزة أخرى أو خوادم تسمى RADIUS CLIENT ، حيث أن خادم NPS لابد من أن يكون له عميل CLIENT يؤدي الخدمة المحددة لكي تستطيع الأجهزة الوصول إليه [14] ، ويقدم NPS الخدمات التالية :-

1. RADIUS SERVER FOR DIAL UP AND VPN
2. RADIUS SERVER FOR 802.1X WIRELESS OR WIRED CONNICTION
3. NETWORK ACCESS PROTECTION (NAP)

كل الخدمات السابقة تشترك في أنها تعمل على منع أي مستخدم أو جهاز لم يحقق كل القيود المحددة من الاتصال بالشبكة ، ولكنها تختلف من حيث آلية عملها .

- RADIUS SERVER FOR DIAL UP AND VPN

في حال تم تهيئة خادم NPS لتقديم هذه الخدمة فأن عملية التحقق AUTHINTICATION ستتم من خلال هذا الخادم والذي يسمى في هذه الحالة RADIUS SERVER ، وبالتالي فأن أي جهاز يريد الاتصال بالشبكة عبر تقنيات DIAL-UP أو من خلال الشبكات الافتراضية الخاصة VPN يجب عليه تحقيق POLICY التي تسمح له بالاتصال بالشبكة ومن ثم يسمح له خادم NPS بالاتصال وفق ما تم وضعه من قيود عليه [14] .

- RADIUS SERVER FOR 802.1X WIRELESS OR WIRED

تختلف هذه الخدمة عن الخدمة السابقة (VPN & DIAL-UP) بأنها تعمل وفقا لنوع الاتصال الذي يستخدمه CLIENT (سلكي أو لا سلكي) و ما إذا كان هذا الاتصال موثوق أو لا ، و هذه الخدمة تمر بنفس المراحل التي تمر بها خدمة (VPN & DIAL-UP) [14].

- NETWORK ACCESS PROTECTION (NAP)

يتم تهيئة خادم NPS ليعمل مع NAP Service والذي يعمل على التحقق من أن الجهاز الذي يريد الاتصال بالشبكة يملك كل المتطلبات المحددة ، هذه المتطلبات يتم التحقق منها بواسطة SECURITY HEALTH VALIDATOR (SHV) ، حيث يتم تنفيذ خدمة SHV بواسطة خادم NPS ، كما أن NAP يتطلب تفعيل خدمة أخرى على أجهزة الشبكة وهي SECURITY HEALTH AGENT(SHA) حتى يتمكن من العمل على الشبكة [14].

يحتوي SHV على مجموعة من المتطلبات و هي :-

FIREWALLSETTINGS - ANTIVIRUS SITTINGS - SPYWARE SITTINGS- AUTOMATIC UPDATE SETTINGS – SECURITY SETTINGS

يجب على أي جهاز يرغب بالاتصال بالشبكة أن يكون به خصائص تطابق ما تم وضعه في SHV .

ويمكن تطبيق NAP مع الخدمات التالية :-

DHCP –VPN – REMOTE DESKTOP GATEWAY – IEEE 802.1X WIRED – IEEE 802.1X WIRELESS – IPSEC WITH HEALTH REGISTERATION AUTHORITY [15] .

NPS SERVER يحتوي على ثلاث أنواع من PLOICY والتي يعتمد عليها أي مستخدم أو جهاز في اتصاله بالشبكة وهي :-

1. CONNECTION REQUEST POLICIES

تعتبر أول POLICY يتم اختبارها ويتم فيها تحديد نوع الاتصال كما يتم وفقها تحديد ما إذا كان مسموح لأي جهاز بالدخول للشبكة أو لا و ما إذا كان طلبه للأتصال بالشبكة مقبول أو مرفوض ، كما يتم تحديد المكان الذي سيتم معالجة طلبات الاتصال عليه على هذا الخادم أو على خادم أخر، وما هي القيود التي تم تحديدها ليتم الأتصال بالشبكة [14]

يوجد العديد من القيود التي يمكن تحديدها ضمن هذا النوع من POLICY من أهمها :-

Day and Time Restrictions

Access Client IPv4 Address

Access Client IPv6 Address

2. NETWORK POLICIES

يتم فحص و معالجة هذه Policy في حال تمكن الجهاز من تحقيق الشروط المحددة في CONNECTION REQUEST POLICIES وهي أيضا تتحكم في اتصال أي جهاز بالشبكة إما مسموح ACCESS أو ممنوع DENY والقيود التي يتم الأتصال وفقها ، وتحديد نوع الوصول للشبكة في حال تحقيق أي CLIENT لهذه POLICY (وصول كامل – وصول كامل لفترة زمنية محددة – وصول محدود) و في حالة الوصول المحدود يتم تحديد الأجهزة التي يمكنه الأتصال بها أو ما يعرف بمنطقة العزل Remediation Area [14].

من اهم القيود ضمن هذا النوع من POLICY :-

Windows Groups – Day and Time Restrictions – Machine Groups

User Groups – Health Policy

- Health Policy

نوع من القيود يتم استخدامه مع NETWORK ACCESS PROTECTION (NAP) حيث يتم تحديد الآلية التي سيتم وفقها السماح للجهاز بالأتصال بالشبكة أو منعه وفقا لما تم وضعه من متطلبات للاتصال بالشبكة ضمن SHV (SECURITY HEALTH VALIDATOR) ، وهي تعمل مع كل من CONNECTION REQUEST POLICY و NETWORK POLICY وتحتوي HEALTH POLICY على العديد من الآليات للتحقق من حالة الجهاز وهي :-

Client Passes All SHV Checks

Client Fails All SHV Checks

Client Passes One Or More SHV Checks

Client Fails One Or More SHV Checks

Client Reported AS Transitional By One Or More SHVs

Client Reported As Infected By One Or More SHVs

Client Reported As Unknown By One Or More SHVs

ويمكن وضع HEALTH POLICY كأحد القيود في NETWORK POLICY في حال تحقق أي من هذه الآليات فأنه يقوم إما بمنع الأتصال أو السماح به وذلك وفقا لما تم تحديده في NETWORK POLICY [14] .

13.2 جدار الحماية Firewall

جدار الحماية هو جهاز أمان للشبكة يراقب حركة مرور بيانات الشبكة الواردة والصادرة ويقرر ما إذا كان يجب السماح بحركة مرور معينة أو حظرها بناءً على مجموعة محددة من قواعد الأمان.

تعتبر جدران الحماية خط الدفاع الأول في أمان الشبكات حيث إنها تشكل حاجزًا بين الشبكات الداخلية الأمنة والمتحكم بها و الموثوقة والشبكات الخارجية غير الموثوقة مثل الإنترنت ،حيث أن كل اتصالات الشبكة الواردة والصادرة يجب ان تمر من خلال جدار الحماية ليتم فحصها والتأكد من انها

لا تحتوي على أي برمجيات خبيثة أو فيروسات والسماح بمرور هذه الأتصالات أو منعها بواسطة القواعد التي يحددها جدار الحماية [16] .

يمكن أن يكون جدار الحماية من الأجهزة HARDWARE أو البرامج SOFTWARE .

من أمثلة Hardware Firewall :-

. Fortinet FortiGate. - Juniper Firewall - Zyxel ZyWALL

و من أمثلة Software Firewall :-

Microsoft Fofront Threat Mangment Gateway(TMG 2010) وهو جدار حماية وفرته شركة Microsoft .

1.13.2 Threat Management Gateway(TMG)

TMG هو جدار حماية بأمكانه التعامل مع البيانات أو الأتصالات بين الشبكات المختلفة والتحكم بها من حيث السماح بالأتصال بشبكة أو جهاز ضمن الشبكة او منعه ، كما أن TMG لديه القدرة على التعامل مع التطبيقات و كذلك مكافحة البرامج الضارة و التصدي للعديد من التهديدات التي تواجه الشبكات الحديثة.

كما يعتبر تطوير لـ Microsoft ISA Server و يتضمن جميع وظائف ISA Server ، كما تم أجراء العديد من التحسينات على الخدمات القديمة و إضافة بعض الخدمات الجديدة منها ما يتعلق بالأمن وبعضها يتعلق بأستكشاف الأخطاء وإصلاحها [17].

خلافا للجيل الأول لجدران الحماية (Packet Filtering) و الجيل الثاني (Circuit-Level) والذي كانت خدماتها محدودة وتقتصر على السماح او منع الأتصالات بين الشبكات ، ومراقبة هذه الأتصالات وتدفق البيانات بين الشبكات ، فأن جدار الحماية TMG يعتمد على تقنية تسمى UTM أو UNIFIED THREAT MANAGEMENT ، و عكس أنظمة ال Firewall القديمة والتي كانت توفر مهام Routing والمهام المتعلقة بالFirewall فأن الأنظمة التي تعتمد على تقنية UTM تقوم بتنفيذ عدد من الوظائف بالأضافة الى الوظائف السابقة وهي :-

- FIREWALL :- بأماكانه إنشاء قواعد RULES للسماح او لمنع الأتصالات او البيانات من المرور عبره ، وكذلك مراقبة حركة البيانات [17].
- ROUTING :- حيث أن TMG يستطيع الربط بين الشبكات المختلفة (ROUTE) وذلك من خلال خدمات ROUTING التي يتم إعدادها من خلال TMG كما ان TMG يستطيع التعامل مع تقنية ترجمة عنوان الشبكة (Network Address Translation (NAT ، حيث ان TMG يقوم بأعداد هذه الخدمات بين الشبكات بشكل تلقائي بعد أن يتم تهيئته [17].
- ANTI-VIRSUS :- يستطيع TMG من خلاله التعامل مع الملفات او البرامج الخبيثة او الفيروسات ومنعها من الدخول الى الشبكة ، حيث ان أي بيانات او ملفات يتم ارسالها بين الشبكات تمر عبره وبالتالي يستطيع فحصها والتأكد منها [17].
- ANTI-SPAM :- يقصد ب SPAM الرسائل المزعجة او الرسائل الغير مرغوبة (مثل رسائل الأعلانات) يتم من خلال هذه الخدمة فحص الرسائل التي يتم ارسالها الى الشبكة (في حال وجود MAIL SERVER في الشبكة) ويتم حظر هذه الرسائل في حال تم تصنيفها بانها SPAM كما يمكن من خلالها منع استقبال أي رسائل او السماح بأستقبالها بناء على بعض القواعد مثل محتوى الرسالة او عنوان الرسالة او عنوان IP للمرسل وغيرها [17].
- IPS Intrusion Prevention System :- مجموعة من القواعد الأمنية التي يتم تحديدها بواسطة TMG للتعامل مع أي عمليات او هجمات تشكل خطر على الخدمات الموجودة في الشبكة مثل تكرار عملية ping على الشبكة بشكل كبير او ما يعرف ب ping to death او DNS ATTACKs ، وبالتالي يتم السماح او منع الجهاز المسؤول عن هذه العملية وفقا للقواعد التي تم تحديدها في IPS [17].
- WEB OR URL FILTERING :- يتم من خلالها تحديد العمليات التي يستطيع أي جهاز القيام بها عند اتصاله بشبكة الأنترنت مثل تحديد المواقع التي يستطيع الوصول اليها وكذلك تحديد البروتوكولات المستخدمة في الأتصال وذلك بأستخدام سياسات POLICIES يتم انشائها والتي نستطيع من خلالها اما السماح بالوصول لما تم تحديده من مواقع وخدمات او منعه ، كما نستطيع تحديد البيانات او الملفات والمحتوى الذي يمكن عرضه او تحميله من الأنترنت [17].

بالأضافة الى ان TMG عندما يتم تهيئته ضمن الشبكة فأنه يعمل على تقسيم الشبكة الى خمسة أقسام هي :-

1. Local Host :- هذه الشبكة الموجود بها TMG فقط .
2. INTERNAL :- الشبكة الداخلية ويقصد بها شبكة LAN .
3. EXTERNAL :- الشبكة الخارجية تتضمن كل الأتصالات من خارج شبكة LAN مثل الأتصالات عبر الأنترنت .
4. VPN :- تتضمن المستخدمين و الأجهزة المتصلين بالشبكة من خلال خدمات VPN .
5. VPN Quarantined :- هذه الشبكة يتم فيها حجز أي مستخدم او جهاز لا يتطابق مع الشروط او القيود المحددة للاتصال عبر خدمات VPN [17].

1.1.13.2 سياسات جدار الحماية TMG (TMG POLICIES)

عندما يتم تهيئة TMG فأنه يقوم بإنشاء POLICY تعمل على إقفال كل الأتصالات بين الشبكات ولذلك لن يستطيع أي مستخدم ضمن أي شبكة من الأتصال بمستخدم او الوصول لخدمة ضمن شبكة أخرى ، وللسماح بالأتصالات بين هذه الشبكات يتم إنشاء POLICIES تعمل على فتح الاتصالات بين الشبكات وذلك وفقا للقيود المحددة والخدمات المسموح بها ، ويحتوي TMG على عدة POLICIES :-

- SYSTEM POLICIES :- وهذه POLICY خاصة بال TMG حيث تعمل على فتح الأتصالات بين شبكة LOCAL HOST الخاصة بالTMG وباقي الشبكات .
- ACCESS POLICY :- وهي POLICIES المسؤولة عن فتح الاتصالات بين مختلف الشبكات الموجودة على TMG .
- PUBLISH POLICY :- يتم إنشائها للسماح للمستخدمين خارج شبكة LAN بالوصول للخدمات داخل الشبكة مثل خدمات الويب أو البريد الإلكتروني Mail وغيرها [17] .

و في ما يلي أكثر البروتوكولات استخداما من خلال Policies التي يوفرها TMG :-

1. بروتوكول نقل النص التشعبي Hyper Text Transfer Protocol (http)

تعتمد جميع مواقع الويب على هذا البروتوكول و يستخدم لإدارة الاتصالات بين متصفحات الويب وخوادم الويب .

2. بروتوكول نقل النص التشعبي الآمن Hypertext Transfer Protocol Secure(https)

نسخة أكثر أمانا من بروتوكول HTTP تعتمد على استخدام طبقة الاتصال الأمن Secure Socket Layer (SSL) لتأمين الاتصال .

3. بروتوكول نقل الملفات File Transfer Protocol FTP

يتيح هذا البروتوكول عملية نقل ومعالجة الملفات بين جهازين أو أكثر .

4. نظام أسماء النطاقات Domain Name Service (DNS)

تعمل على ربط الأسماء للمواقع و الأجهزة بعناوين IP .

5. بروتوكول نقل البريد Simple Mail Transfer Protocol (SMTP)

يستخدم هذا البروتوكول لنقل البريد الالكتروني بين الأجهزة .

6. بروتوكول مكتب البريد Post Office Protocol (POP)

يسمح هذا البروتوكول للمستخدمين بإستقبال البريد وتخزينه على الأجهزة الخاصة بهم [18].

TMG CLIENT 2.1.13.2

حتى يتمكن TMG من مراقبة و التحكم في الأتصالات بين الشبكات فلابد من أن تمر كل الأتصالات عبره ، وليتم ذلك يجب أن يتم إعداد الأجهزة ضمن الشبكة لتتعرف على TMG وتقوم بالأتصال بالشبكات والأجهزة الأخرى من خلاله ، ويوجد ثلاث طرق يمكن استخدامها لأعداد TMG CLIENT :-

1. WEB Proxy Client :- في هذه الطريقة يتم تهيئة TMG ليكون خادم Proxy ثم يتم إضافة عنوان IP الخاص بالTMG لي إعدادات Proxy الخاصة بالعميل CLIENT .
2. SecureNET :- في هذه الطريقة يتم إضافة ip الخاص بال TMG ليكون Gateway ضمن إعدادات كرت الشبكة الخاص بجهاز المستخدم.

3. Forefront TMG CLIENT :- في هذه الطريقة يتم تثبيت تطبيق TMG CLIENT على الأجهزة يقوم بالتعرف على TMG و يسمح بالأتصالات من خلاله وذلك إما عن طريق ACTIVE DIRECTORY أو عن طريق DHCP أو عن طريق DNS [17] .

وتختلف هذه الطرق من حيث درجة الأمان و الخدمات التي توفرها كل طريقة ،حيث يوفر Forefront TMG CLIENT اتصالات اكثر امانا بين TMG و الأجهزة مقارنة مع الأنواع الأخرى ، وكذلك تختلف الطرق السابقة من حيث دعمها للبروتوكولات المختلفة و المستخدمة في الأتصال ، ولذلك لابد من تحديد الألية المناسبة للعمل بها وذلك وفقا لمتطلبات و أحتياجات الشبكة.

2.13.2 BANDWIDTH SPLITTER TOOL

هي أحدى الأدوات المستخدمة للتحكم في حركة البيانات عبر الشبكة ، حيث يمكن من خلالها التحكم و مراقبة اتصالات وكذلك تحديد سرعة اتصال المستخدمين عبر شبكة الانترنت .

وتوفر هذه الأداة نوعين من القواعد Rules والتي يتم تحديدها للمستخدمين أو أجهزتهم :-

1. قواعد سرعة الأتصال Shaping Rule :- وهي قواعد يتم من خلالها تحديد سرعة التحميل Download والرفع Upload للمستخدمين أو الأجهزة .
2. قواعد الحصص أو السعة Quota Rules :- وهي قواعد يتم من خلالها تحديد حصة أو سعة معينة من عرض النطاق الترددي Bandwidth لكل مستخدم أو جهاز ، وتعمل هذه القواعد على منع المستخدمين و الأجهزة من الأتصال بالأنترنت عند استهلاك حصصهم .

من مميزات BANDWIDTH SPLITTER :-

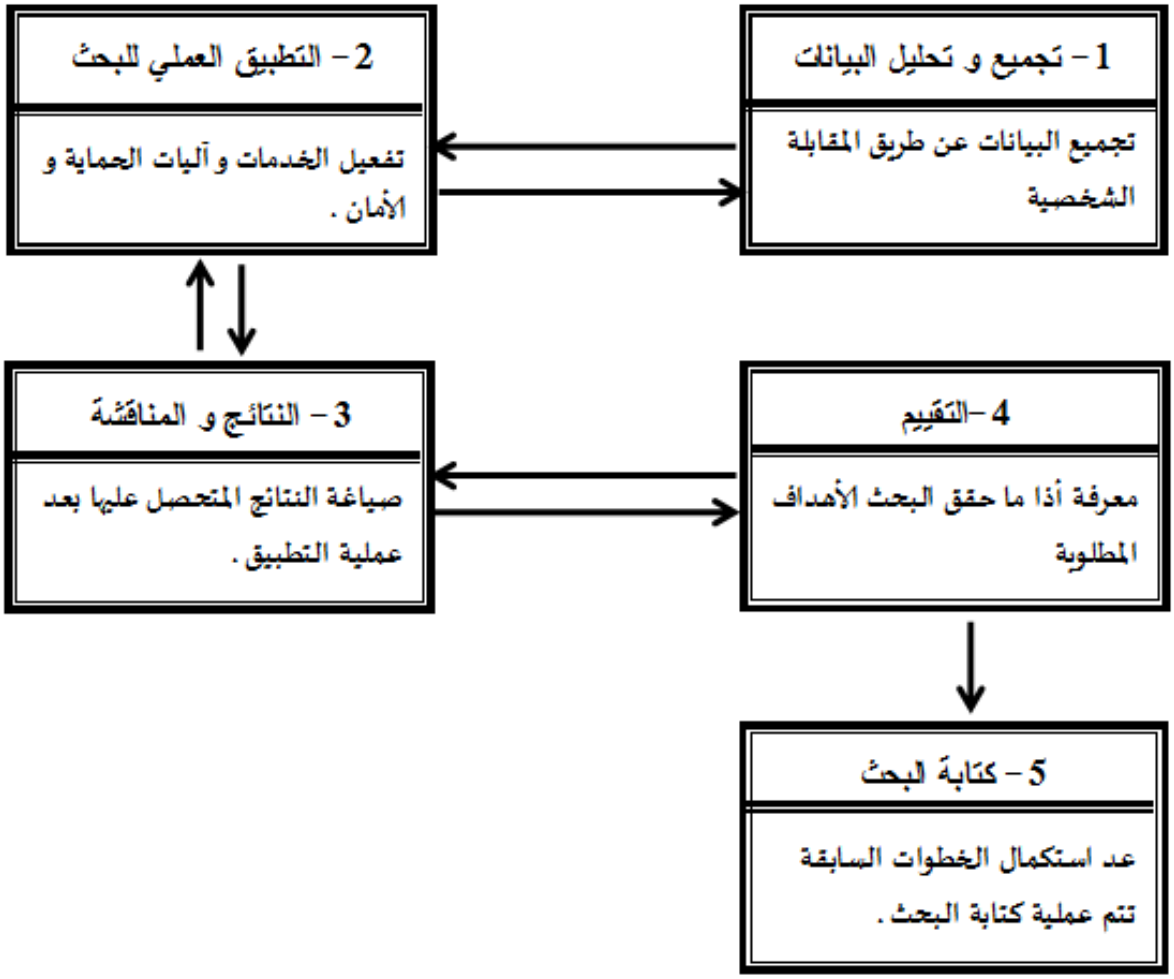
1. التحكم في استخدام عرض النطاق الترددي .
2. تحديد سعة Quota من النطاق الترددي لكل مستخدم .
3. مراقبة الأتصالات في الوقت الحقيقي .

الفصل الثالث

منهجية البحث

3. منهجية البحث Research Methodology :

المنهجية التي تم إتباعها في هذه الدراسة هي Case Study و المنهجية المتبعة تدرس حالة خادم في الشبكة والتي تعتمد على أيجاد مشكلة أو ضعف في دراسات سابقة ومحاولة حلها بعد التعمق في دراستها و الخطوات التي تعتمد عليها, و سيتم الأعتماد على هذه المنهجية لدراسة حالة الخادم الحالي و معرفة الأخطاء ناتجة عن تكوينات نظام التشغيل و معالجتها في الخادم الجديد ، وهي طريقة لدراسة وحدة معينه مثل منشأة صناعية أو دراسة حالة جهاز في شبكة أو دراسة وظيفة معينه حيث تتناول جميع الأجزاء الكلية و معاملة جزئيات من حيث علاقاتها البنائية و الوظيفية بكل ما يتضمنها من مكونات تعتمد هذه الدراسة على التحقيق أو الاطلاع على دراسات سابقة وكذلك الاطلاع على نتائجها ومحاولة أيجاد ضعف أو المشاكل في هذه الدراسات ، و يوضح **شكل 3-1** خطوات المنهجية التي تم أتباعها :



شكل(1.3) منهجية البحث

و يتم إتباع منهجية دراسة الحالة للوصول إلى النتائج المطلوبة و تتلخص خطوات المنهجية في النقاط التالية :

1. تجميع و تحليل البيانات Data analysis

تمت عملية تجميع البيانات عن طريق المقابله الشخصية و ذلك لغرض معرفة العيوب و القصور في بيئة نظام الحالي .

كما تمت عملية المقابلة الشخصية مع مهندسين و موظفين مركز تقنية المعلومات جامعة سبها و طرح الأسئلة التالية :-

ما هي الخدمات التي لا يوفرها النظام الحالي ؟
ما هي الخدمات التي يجب توفيرها ؟
هل استهلاك النطاق الترددي يمثل مشكلة ؟
ما هي القيود لتي يجب وضعها على المستخدمين ؟
ما هي التصنيفات التي يجب اتبعها لتنظيم المستخدمين ضمن مجموعات معينه ؟

حيث تم الحصول على مجموعة من الأجوبة بالخدمات الغير موجودة على النظام الحالي و الخدمات التي يلزم توفيرها للحصول على نظام يعمل بشكل أفضل كما أن استهلاك النطاق الترددي bandwidth المخصص للاتصال بالانترنت يمثل مشكلة كبيرة و لابد من وضع آليات لتقليل استهلاكه ، كما تم تحديد تصنيفات المستخدمين و التعرف على أهم القيود التي يجب أن يتم تطبيقها و بناء على الإجابات التي تم الحصول عليها من المقابلة الشخصية يتم البدء في مرحلة التطبيق العملي .

2. التطبيق العملي للبحث Applying study

تمثل هذه المرحلة تطبيق عملي للبحث حيث تم العمل بشكل افتراضي ابتداء من تنصيب نظام تشغيل (windows server 2012 & 2008R2) و تكوين الخدمات بشكل صحيح كما تمت عملية تحديد الصلاحيات للمستخدمين و تفعيل أدوات و وسائل الأمان ، وتم تكوين الخدمات التالية

Active directory , Domain name system , Dynamic host configuration protocol ,Windows Deployment Service, windows server update Service , Web Server, Printer Server, File Server , NPS Server .

كما تم وضع مجموعة من القيود و الشروط (group policy) على كل مستخدم ضمن المجموعة التي ينتمي إليها و استخدام TMG Firewall لحماية الشبكة من تهديدات الخارجية .

3. النتائج و المناقشة

بناء على ما تم الوصول إليه في التطبيق العملي للبحث يمكن صياغة النتائج المتحصل عليها من التطبيق الفعلي و مناقشة الإضافة التي توفرها كل خدمة تم تفعيلها على الخادم و هل تم توفير المستوى المطلوب من الحماية و الأمان للمستخدمين .

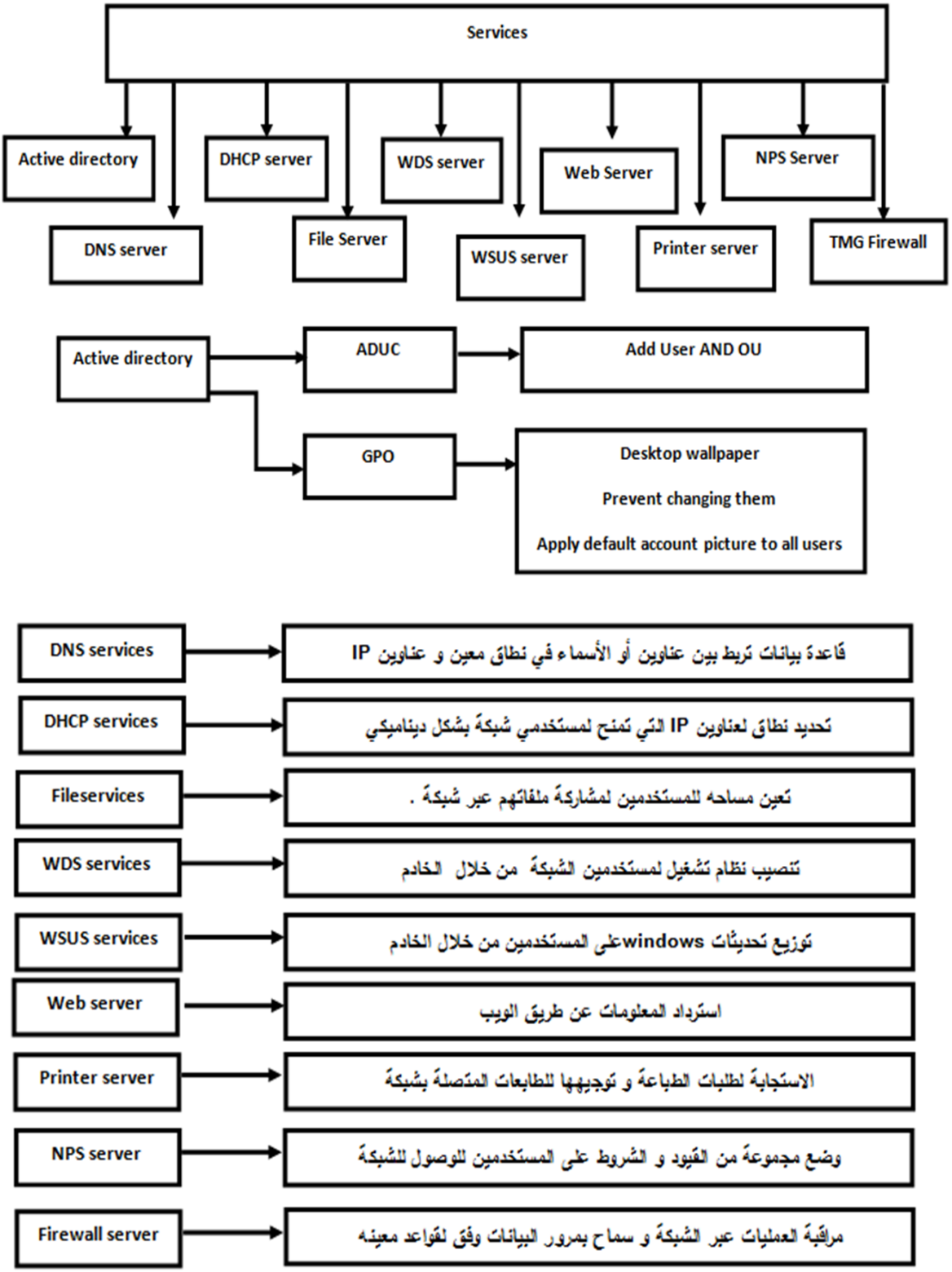
4. التقييم

يتم تقييم البحث بناء على النتائج التي تم الوصول إليها و تحديد إذا ما كانت هناك إضافة فعليه كرفع لمستوى الحماية و الأمان و تكوين الخدمات بشكل صحيح دون حدوث ثغرات أم لا .

5. كتابة البحث

بعد الحصول على نتائج و التأكد من صحتها و الإنتهاء من عمل التقييم يتم البدء في كتابة البحث .

ويوضح **الشكل 3-2** الخدمات التي تناولها البحث (هيكلية البحث) :-



شكل (2.3)هيكلية البحث

الفصل الرابع

التطبيق العملي للبحث

4. التطبيق العملي

1.4 عملية المحاكاة Simulation

تم استخدام بيئة VMWare لمحاكاة و بناء شبكة افتراضية لجامعة سبها حيث تم استخدام الإصدار 15 من بيئة VMWare WorkStation PRO وذلك لإنشاء و أعداد و تهيئة خوادم افتراضية تعمل بأنظمة تشغيل Windows server 2008 R2 و Windows Server 2012 ، حيث توفر بيئة VMWare العديد من المزايا مثل أمكانية تشغيل مختلف التطبيقات عليها ، و أمكانية أجراء الاختبارات بسهولة واسترداد البيانات في حال حصول أي ضرر ، وكذلك توفر بيئة VMWare شبكات افتراضية والتي تعرف بأسم VM Network (VMnet) ،حيث تم استخدام أحد الشبكات التي توفرها هذه البيئة وهي VMnet 2 وذلك لمحاكاة عملية الأتصال بالأنترنت من خلال جدار الحماية ، كما تم توصيل الخوادم ببعضها من خلال الخاصية Bridged التي توفرها بيئة VMWare والتي تسمح للخوادم بالأتصال من خلال كرت الشبكة الخاص بالجهاز المستضيف لبيئة المحاكاة VMWare .

2.4 إعداد و تهيئة خدمات الدليل النشط Active Directory

بما أن لبيئة النطاق Domain التي تقدمها أنظمة التشغيل Windows العديد من المزايا التي ساعدت على تسهيل إدارة الشبكة و من خلال العديد من الخدمات التي توفرها وكذلك تفوقها على شبكات Workgroup سواء في ما يتعلق بالبنية التحتية للشبكة أو بالجانب الخدمي والأمني للشبكة فقد تم تصميم وتهيئة هذه الشبكة بأستخدام نظام Windows Server 2012 و الأستفادة من بيئة النطاق Domain وخدمات Domain Controller التي يوفرها هذا النظام وذلك لبناء شبكة لجامعة سبها والتي تم تسميتها **ITC.COM** .

حيث أن الجهاز الرئيسي والذي يقوم بدور Domain Controller و يسمى Primary Server هو المتحكم في خدمات Domain ، كما أن الأجهزة أو الخوادم الرئيسية في الشبكة عادة ما يتم تهيئتها بأستخدام عنوان ثابت Static IP وذلك لأن استخدام العناوين الديناميكية أو المتغيرة Dynamic IP يتطلب تغيير الإعدادات الخاصة بالشبكة حتى تتمكن الأجهزة الأخرى من معرفة العنوان الجديد وكذلك لتتمكن من التسجيل داخل النطاق Doamin و الأستفادة من خدماته .

ويعمل الجهاز الرئيسي Domain Controller على التحكم بالأجهزة ومستخدمي الشبكة من خلال خدمات يقدمها والتي يتم تهيئتها و إعدادها من خلاله .

1.2.4 مستخدمي و أجهزة الدليل النشط Active Directory Users And Computers

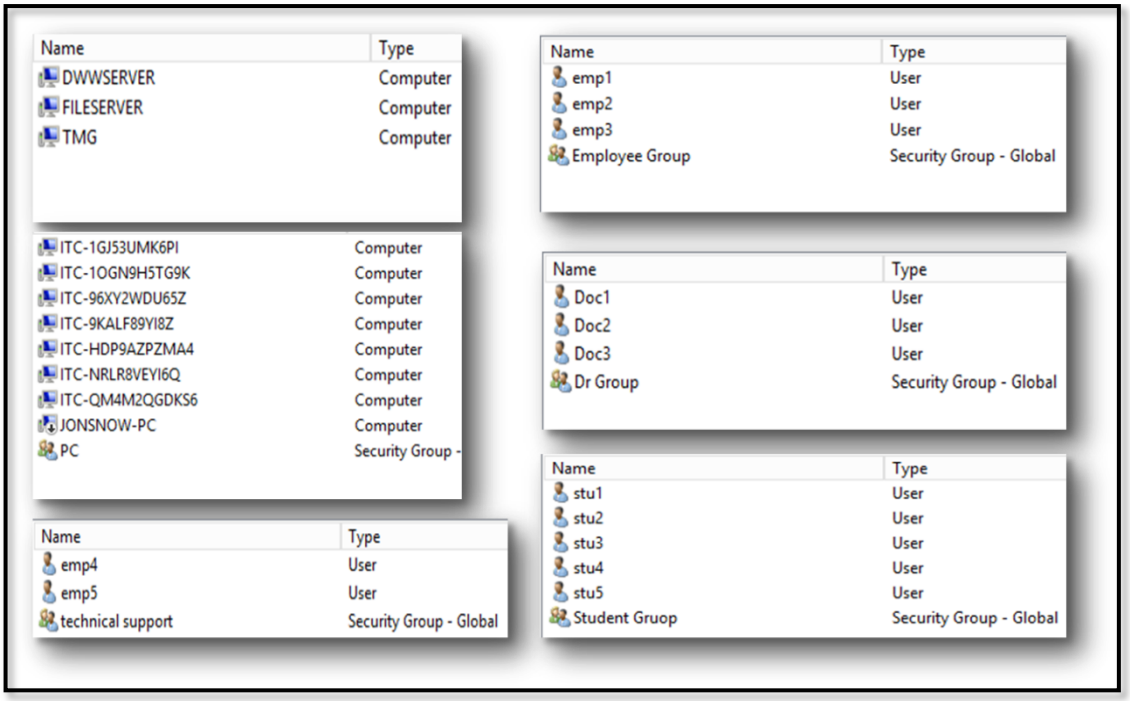
من خلال خدمات المستخدمين والأجهزة على Domain Controller تم إضافة مجموعة من الأجهزة و الخوادم إلى النطاق Domain والتي يتم وضعها بشكل تلقائي ضمن ما يسمى حاوية Container خاصة بالأجهزة التي يتم إضافتها ضمن Domain ، كما تم إنشاء وحدات تنظيمية Organizational Unit (OU) رئيسية تسمى ITC تحتوي على كل الأجهزة والمستخدمين ضمن Domain ،حيث تم إنشاء OU خاصة بالطلبة STUDENTS الموجودين على Domain ، وكذلك OU للأجهزة التي يتم إضافتها ضمن Domain بحيث يتم نقل الأجهزة من موقعها الأفتراضي إلى OU خاصة بهم .

وكذلك تم إنشاء OU خاصة بالموظفين Employee وأخرى خاصة بالمدرسين كما تم إنشاء OU خاصة بالفنيين Technical Support ، و تم منح كل OU منها صلاحيات خاصة وذلك حسب إحتياجات كل مستخدم .

كما تم إنشاء مجموعة خاصة لكل فئة من المستخدمين مما يسهل التعامل معهم من خلال خدمات Domain من حيث إدارة المستخدمين وكذلك تسهل عملية تحديد الصلاحيات للمستخدمين حسب مجموعاتهم .

ومن خلال إعدادات الأمان أو Security التي توفرها هذه الخدمة فقد تم منع المستخدمين من إضافة الأجهزة أو تسجيلها ضمن domain والذي كان مسوح لهم ضمن الإعدادات الأفتراضية حيث تم السماح للفنيين Technical Support و المسؤول Admin فقط بالقيام بهذه العملية .

ويوضح **الشكل 4-1** المستخدمين و الأجهزة الذين تم إنشائهم من خلال خدمات المستخدمين والأجهزة Users And Computers التي يوفرها Domain .



شكل(1.4) الأجهزة والمستخدمين ضمن Domain

2.2.4 تطبيق Group Policy

من خلال Group policy تم تحديد الصلاحيات لكل ORGANIZATIONAL UNIT (OU) ، حيث يتم تحديد الصلاحيات على مستوى كل من المستخدمين والأجهزة .

وبشكل افتراضي فأن Group Policy تقوم بتطبيق اثنان من Policy هما :-

1. Default Domain Policy:- وهي يتم تطبيقها على Domain بالكامل وتحتوي على صلاحيات خاصة بإنشاء كلمات المرور مثل درجة التعقيد Complexity وطول كلمة المرور .
2. Domain Controller Policy :- حيث تحتوي على الصلاحيات التي يتم تطبيقها على الجهاز الرئيسي .

بالإضافة إلى policy السابقة فقد تم تحديد صلاحيات خاصة لكل OU تم إنشائها ضمن Domain ويوضح الجدول 4-1 هذه الصلاحيات.

جدول(1.4) يوضح الصلاحيات التي تم تحديدها للمستخدمين داخل النطاق **Domain** .

اسم POLICY	وظيفتها	تم تطبيقها على
Control Panel Policy	• تعمل على تحديد صورة الافتراضية لكل حساب على الجهاز .	ITC
DHCP NAP POLICY	• Policy خاصة بخادم NPS تعمل على تفعيل عملية الحجز عبر خادم DHCP وكذلك تفعيل Security Center على أجهزة المستخدمين .	ITC
Firewall Policy	• تعمل على السماح بعملية Ping من خلال بروتوكول ICMP على كل الأجهزة التي تم تسجيلها في Domain	ITC
Remote Desktop Policy	• تسمح بالاتصال بالأجهزة من خلال خدمات الاتصال عن بعد .	ITC
TMG CLIENT Policy	• تقوم بتثبيت التطبيق الخاص ب TMG والذي يعمل على توصيل الأجهزة ب TMG Firewall .	ITC
University Background Policy	• تقوم بتغيير صورة الخلفية لكل أجهزة الشبكة إلى صورة خاصة بالجامعة .	ITC
Disable CMD And Registry Policy	• تعمل على منع الوصول إلى كل من موجه الأوامر CMD و خدمات Registry .	Employee FOS Student
TMG Client Settings Policy	• تمنع تغيير إعدادات الاتصال بين الأجهزة و Firewall	Employee FOS Student
User Control Panel And Start Menu Taskbar and Personalization	• تمنع الدخول إلى لوحة التحكم . • تمنع تعديل على سطح المكتب الخاص بالأجهزة . • تمنع التعديل على قائمة Start وكذلك إزالة أي برامج تم تثبيتها عليها .	Employee FOS Student

Student Data and Share File Policy	• تعمل على مشاركة الملفات الموجودة على File Server من خلال Script يتم تنفيذه عند تسجيل دخول أي مستخدم على الجهاز .	FOS Student
WSUS Policy	• تعمل على تفعيل Windows update على أجهزة الشبكة . • تعمل على تحديد عنوان Windows Update server الذي سيتم تحميل التحديثات منه والذي سيكون في هذه الحالة عنوان Wsus Server الموجود على الشبكة	ITC PC Domain Controller
Printer Policy	• تعمل على مشاركة الطابعات مع أجهزة الشبكة عبر خادم الطباعة .	Domain
WinXp Wsus Targeting Policy	• تعمل على تنظيم الأجهزة عند استقبالها للتحديثات ضمن Containers وهذه policy خاصة بالأجهزة التي تستقبل تحديثات Windows_XP .	ITC PC
Win2012 Wsus Targeting Policy	• تعمل على تنظيم الأجهزة عند استقبالها للتحديثات ضمن Containers وهذه policy خاصة بالخوادم التي تستقبل تحديثات Windows Server 2012	Domain Controller
Removable Devices Policy	• تعمل على منع الأجهزة والمستخدمين من استخدام أي وسائط اتصال USB أو محركات الأقراص .	STUDENTS

3.4 إعداد و تهيئة خادم نظام نطاق الأسماء DNS

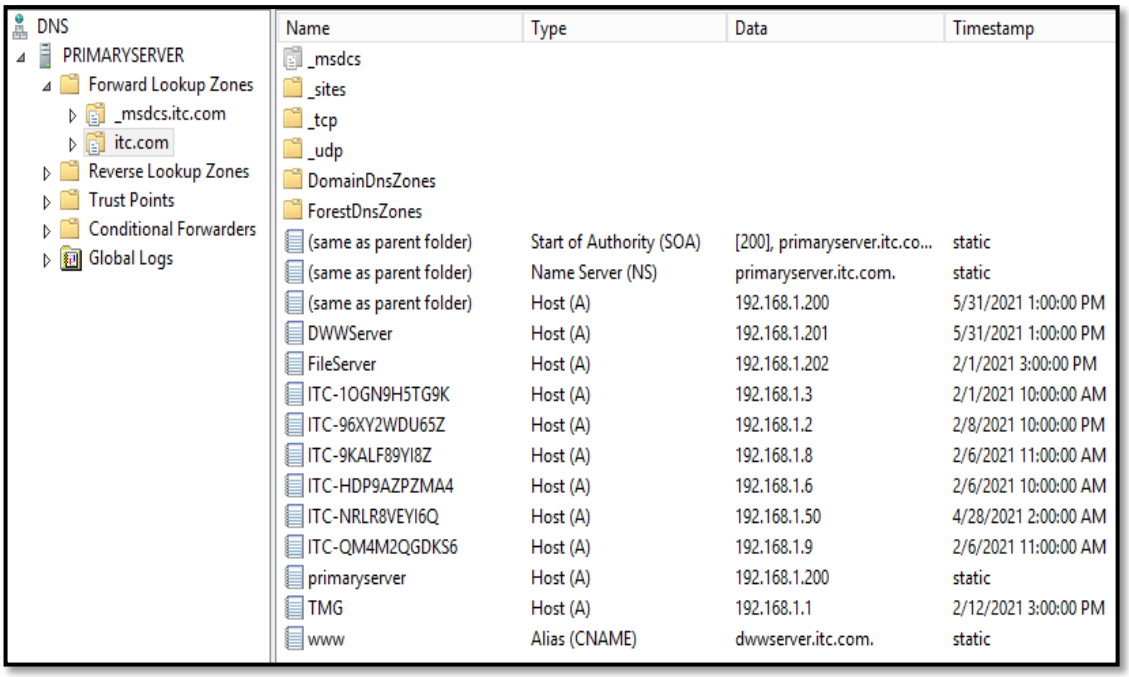
من ضمن متطلبات تهيئة وإعداد الجهاز الرئيسي Domain Controller هو تهيئة خادم DNS حيث أن أي جهاز بعد أضافته أو تسجيله ضمن Domain فأنه يتم تسجيله في سجل تم إنشائه داخل خادم DNS ، و يحتوي كل سجل على عنوان الجهاز في الشبكة و كذلك اسم الجهاز حتى تتمكن الأجهزة من الأتصال ببعضها عن طريق اسم الجهاز .

وبالتالي فأن كل الأجهزة ضمن الشبكة ستستخدم عنوان الجهاز الرئيسي Domain Controller كعنوان DNS في إعدادات الشبكة الخاصة وذلك لأن خدمة DNS موجودة على الجهاز الرئيسي ، وبذلك تتمكن كل أجهزة الشبكة من الأتصال ببعضها بأستخدام أسماء الأجهزة عن طريق هذا العنوان.

السجلات التي تم إنشائها داخل خادم Dns كالتالي :-

1. سجل الجهاز الرئيسي بأسم PrimaryServer للعنوان 192.168.1.200 .
2. سجل لخادم الملفات File Server باسم FileServer للعنوان 192.168.1.202 .
3. سجل لأجهزة Printer, WEB , NPS (NAP) , WSUS , WDS والتي تم تهيئتها ضمن نفس الخادم بأسم DWWServer للعنوان 192.168.1.201 .
4. سجل TMG SERVER (سجل لمنفذ TMG Server المتصل بشبكة الداخلية) بأسم TMG للعنوان 192.168.1.1 .
5. كما تم انشاء Alias(CNAME) بمعنى اسم أخر للجهاز DWWServer بأسم www وهذا السجل خاص بخادم الويب .

و يوضح **الشكل 4-2** السجلات التي تم إنشائها على خادم DNS :-



شكل(2.4) السجلات التي تم أنشائها على DNS

4.4 إعداد و تهيئة خادم تكوين المضيف الديناميكي DHCP

تم تهيئة خادم DHCP ضمن الشبكة بحيث يقوم بتوزيع أعدادات الشبكة على الأجهزة وذلك من خلال إنشاء Scope أو نطاق داخل DHCP و الذي يسمى Network 1 ، يعمل النطاق على توزيع إعدادات الخاصة بالشبكة على أي جهاز يتصل بها حتى يتمكن من الأتصال بالجهاز الرئيسي Domain Controller والتسجيل في Domain .

حيث انه تم إنشاء حاوية للعناوين(Pool) والتي تعتبر من ضمن إعدادات النطاق والتي يتم فيها تحديد مجال العناوين التي سيتم توزيعها (أي تحديد أول و أخر عنوان) وكذلك يتم فيها تحديد العناوين التي سيتم إستثنائها من عملية التوزيع عبر DHCP وذلك لمنع توزيع أي عناوين ثابتة Static IP خاصة بالأجهزة أو الخوادم في الشبكة .

حيث أن مجال او نطاق العناوين الذي تم تحديده هو :- 192.168.1.1 - 192.168.1.254 .

العناوين التي تم إستثنائها من عملية التوزيع عبر DHCP :-

1. العنوان 192.168.1.1 وهو عنوان البوابة Gateway التي تصل الأجهزة بجدار الحماية حتى تتمكن من الاتصال عبر الانترنت .
2. مجال العناوين 192.168.1.200 - 192.168.1.210 حيث أن هذه العناوين مخصصة لأجهزة الخوادم على الشبكة .

العناوين الثابتة Static IP التي تم منحها لأجهزة الخوادم في الشبكة :-

1. عنوان الجهاز الرئيسي Domain Controller :- 192.168.1.200 .
2. عنوان File Server :- 192.168.1.202 .
3. عنوان خوادم Printer, WEB , (NAP) NPS , WSUS , WDS :- 192.168.1.201
4. عنوان البوابة Gateway (عنوان منفذ جدار الحماية TMG المتصل بشبكة الداخلية) :- 192.168.1.1 .

الإعدادات الخاصة بالنطاق Scope والتي يتم توزيعها على الأجهزة :-

1. عنوان Gateway :- 192.168.1.1 .
2. عنوان DNS Server :- 192.168.1.200 .
3. اسم Domain (DNS Domain Name) :- ITC.com .
4. أعدادات PXE Client (عملية الأتصال عن بعد بخادم WDS) .

ويوضح **الشكل 4-3** الإعدادات الخاصة بخادم DHCP .

Start IP Address	End IP Address	Description
192.168.1.1	192.168.1.254	Address range for distribution
192.168.1.1	192.168.1.1	IP Addresses excluded from distribution
192.168.1.200	192.168.1.210	IP Addresses excluded from distribution

Option Name	Vendor	Value	Policy Name
003 Router	Standard	192.168.1.1	None
006 DNS Servers	Standard	192.168.1.200	None
015 DNS Domain Name	Standard	itc.com	None
060 PXEClient	Standard	PXEClient	None

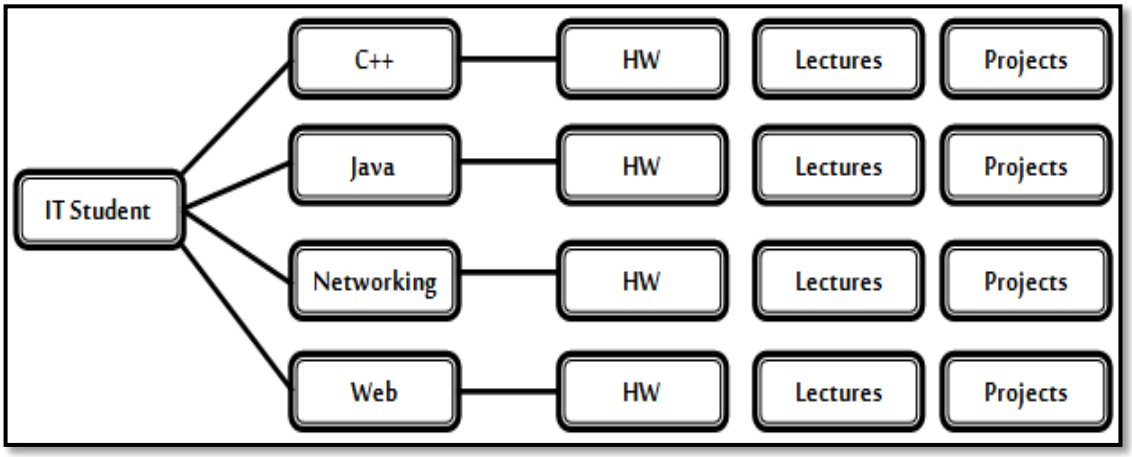
شكل(3.4) أعدادات خادم DHCP

5.4 إعداد و تهيئة خادم الملفات

تعتبر خدمات الملفات من الخدمات الأساسية والتي لابد أن توفرها أي شبكة ضمن البنية التحتية الخاصة بها والموجودة ضمن مختلف المؤسسات ، حيث ان هذه الخدمات مسؤولة عن أدارة الملفات التي يتم تخزينها أو مشاركتها مع أجهزة الشبكة من خلال هذه الخدمات .

وبما أن خدمات الملفات توفر تحكما مركزيا للملفات أو البيانات التي يتم مشاركتها عبر الشبكة من الجانبين الخدمي والأمني فقد تم تهيئة وإعداد هذه الخدمات بحيث تسمح بمشاركة المستخدمين لملفاتهم وبياناتهم عبر هذه الشبكة بشكل امن وبما يوفر الأمان لبياناتهم.

حيث تم إنشاء ملف تخزين على خادم الملفات المركزي بأسم IT Student بحيث يسمح للمستخدمين بمشاركة الملفات المطلوبة عليه وذلك وفقا للصلاحيات التي تم منحها لكل مستخدم (طالب – مدرس – موظف – فني) ، فقد تم إنشاء هذا الملف بحيث يسمح لكل من الطالب والمدرس بمشاركة أي ملفات مطلوبة بينهم مثل المحاضرات أو المشاريع وغيرها بحيث لن يسمح لأي طالب بالإطلاع على ملفات الطلبة الأخرين ولا التعديل عليها ، ولكن يسمح للمدرسين بالإطلاع والتعديل وحذف أي من هذه الملفات وذلك وفقا للصلاحيات التي يتم منحها لكل من الطالب و المدرس ،ويوضح **الشكل 4-4** الملفات التي تم إنشائها على خادم الملفات.



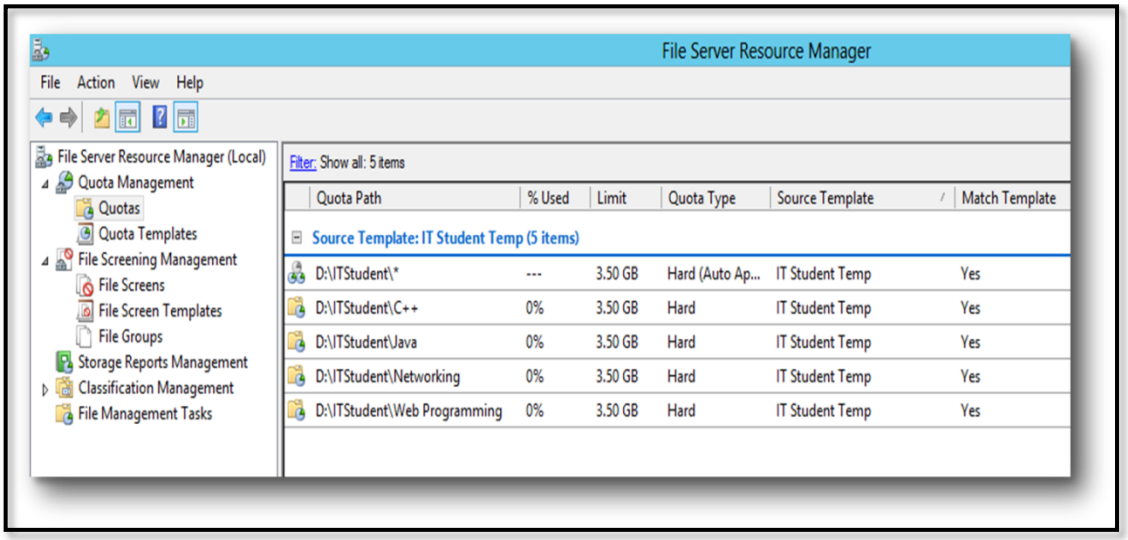
شكل(4.4) الملفات التي تم انشائها ومشاركتها على خادم الملفات

ولتسهيل الوصول الى الملفات التي تم مشاركتها عبر خادم الملفات المركزي للمستخدمين المخولين بالوصول اليها فقد تم استخدام Script يعمل على انشاء Network Drive وهو قرص يتم انشائه على جهاز الكمبيوتر ويحتوي على الملفات والبيانات التي تم تحديدها لمشاركتها ، ويحتوي هذا Script على الأمر التالي :-

. **net use s: \\FileServer\ITStudent**

ولتنفيذ Script على كل المستخدمين المحددين فقد تم استخدام Group policy لتنفيذه على المستخدمين عند تسجيل الدخول إلى حساباتهم ، وبالتالي عند دخول أحد المستخدمين المحددين إلى حسابه سيتم تطبيق Script عليه وسيظهر الملف الذي تم مشاركته على شكل قرص تخزين في جهاز الكمبيوتر .

بالإضافة إلى ما سبق فقد تم تهيئة خدمة File Server Resource Manager والتي تسمح بتحديد انواع الملفات التي يمكن تخزينها وكذلك تحديد مساحة تحزين لكل مستخدم Quota ، حيث تم إعداد هذه الخدمة بحيث تمنع تخزين ملفات الوسائط المختلفة (الصوت – الصور – الفيديو) وكذلك ملفات البريد الألكتروني والملفات التنفيذية وملفات النسخ الأحتياطي Backup كما تم تحديد مساحة 3.50 GB لكل ملف من الملفات التي تم مشاركتها يمكن من خلال هذه الخدمة إنشاء تقارير توضح العمليات التي تم تنفيذها على الملفات وكذلك مساحة التخزين المستخدمة ، ويوضح **الشكل4-5** عملية تحديد مساحة الملفات بأستخدامFile Server Resource Manager .



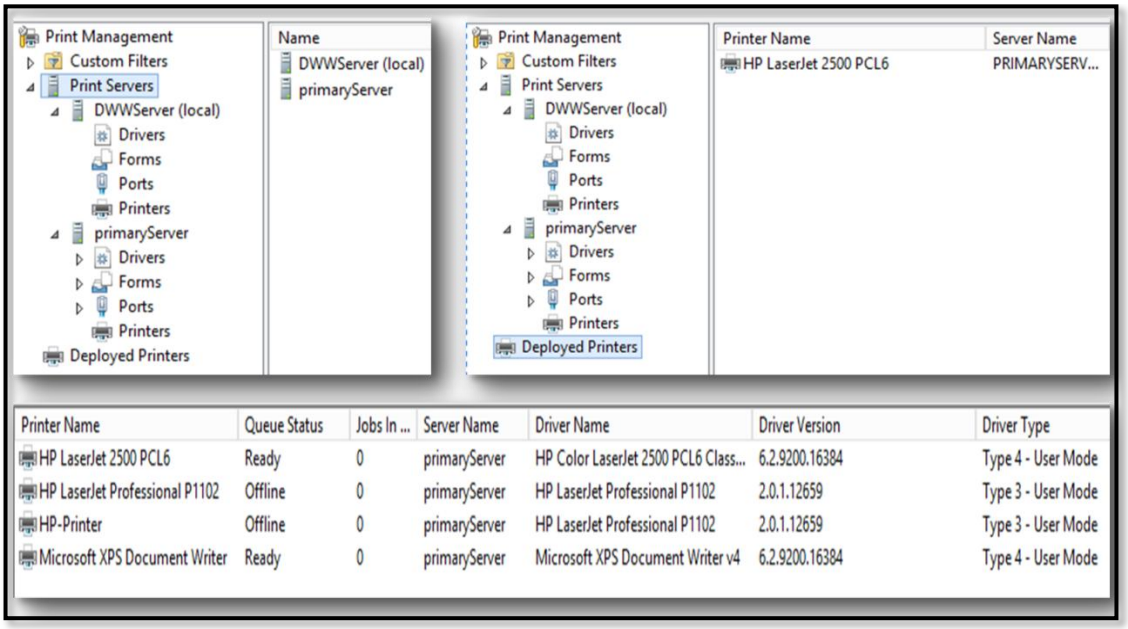
شكل(5.4) تحديد مساحة الملفات بأستخدام File Server Resource Manager

6.4 إعداد و تهيئة خادم الطباعة

يعتبر خادم الطباعة من الخدمات الأساسية التي يجب تهيئتها و توفيرها في أي شبكة ،لذلك فأنه من الضروري تهيئة وإعداد جهاز مركزي يكون مسؤول عن إدارة الطابعات الموجودة على الشبكة و التحكم في عمليات الطباعة و كذلك تحديد مجموعة من الصلاحيات ذات العلاقة بعملية الطباعة و تحديد المستخدمين المخولين بأجراء هذه العملية .

و بالتالي فقد تم تهيئة هذا الخادم بحيث يمكن من خلاله التحكم بالطابعات المتصلة بالشبكة وكذلك تحديد التعريفات الخاصة بالطابعات حتى تتمكن من الأتصال بالأجهزة ، كما تم إضافة الطابعات إلى أجهزة الشبكة وذلك من خلال نشرها أو مشاركتها عبر Group Policy التي يوفرها الجهاز الرئيسي Domain controller و دون الحاجة إلى تهيئتها على كل جهاز في الشبكة بشكل منفصل

، أي أن هذا الخادم يوفر تحكم كامل لكل الطابعات الموجودة على الشبكة ويوضح **الشكل 4-6** عملية إدارة الطابعات المتصلة بالشبكة من خلال خادم الطباعة .



شكل(6.4) ادارة الطابعات على الشبكة

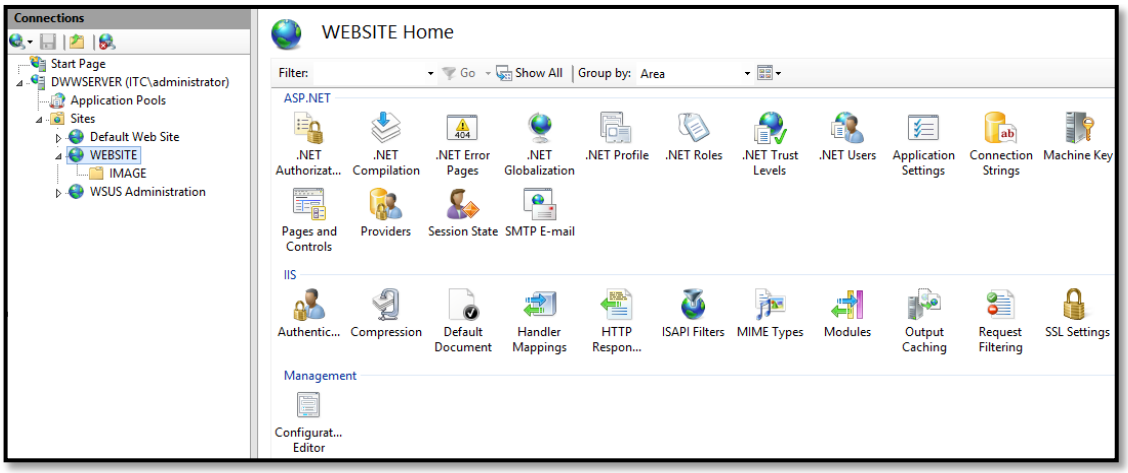
7.4 إعداد و تهيئة خادم الويب

أن كل مؤسسة حاليا تحتاج إلى موقع الكتروني خاص بها على الشبكة ، و حتى يتمكن المستخدمين أو العملاء من الوصول لهذا الموقع فأنه لابد لها من تهيئة خادم ويب لرفع أو أستضافة موقعها حتى يتمكن المستخدمين من الوصول للموقع من خلال الشبكة ، ولذلك فقد تم تهيئة خادم ويب ضمن هذه الشبكة بحيث يمكن من خلاله الوصول إلى أي موقع تم نشره أو مشاركته ، حيث تم تصميم صفحة لموقع الكتروني وهي عبارة عن صفحة لتسجيل الدخول والتي تم تصميمها بأستخدام لغة HTML و CSS وذلك لأختبار عمل هذا الخادم ، والتحقق من أمكانية وصول المستخدمين للموقع بشكل داخلي (داخل المؤسسة) ، وذلك نظرا لعدم توفر عنوان عام Public IP حتى يمكن للمستخدمين الوصول اليه من خلال الأنترنت .

كما تم تحديد اسم أخر Alias(CNAME) من خلال خادم DNS للجهاز الذي تم تهيئة خادم الويب عليه كالتالي www حتى يتمكن المستخدمين من الوصول الى الموقع من خلال هذا الأسم ، وتم تحديد بيانات الوصول للموقع كالتالي :-

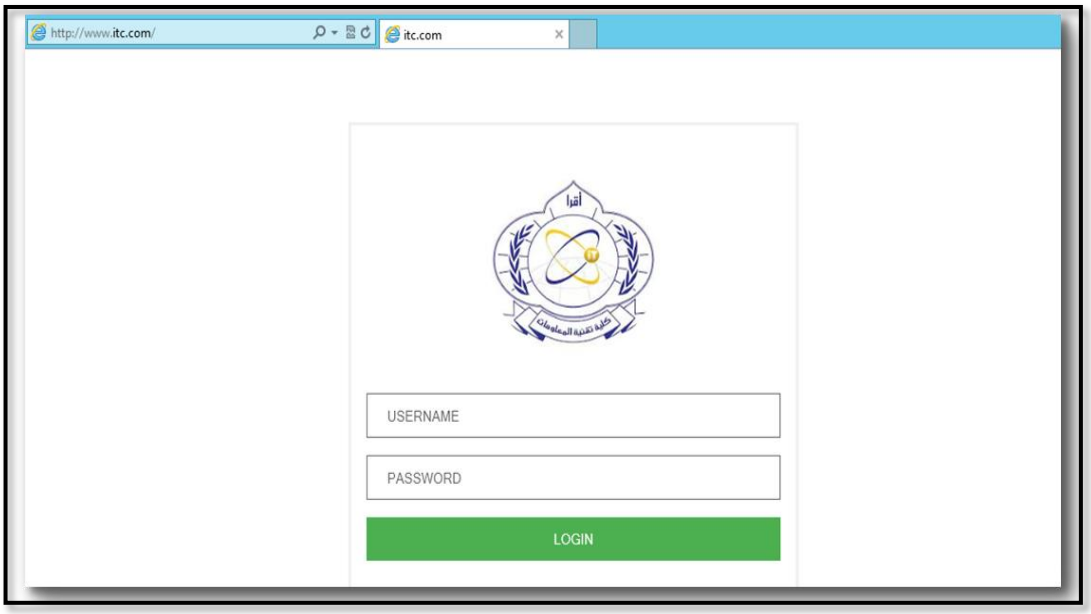
1. تهيئة الموقع بأستخدام بروتروكول HTTP .
2. اسم الموقع Host Name :- www.itc.com .
3. يعمل من خلال المنفذ port 80 .
4. عنوان IP الخاص بالجهاز المستضيف للموقع 192.168.1.201 .

و يوضح **الشكل 4-7** أعدادات خادم الويب.



شكل(7.4) أعدادات خادم الويب

و يوضح **الشكل 4-8** عملية طلب احد المستخدمين للموقع .



شكل(8.4) عملية طلب الموقع من خادم الويب

8.4 إعداد و تهيئة خدمة نشر ويندوز WDS

من خلال عملية أعداد خادم WDS تم تهيئة هذا الخادم بحيث يسمح للأجهزة المتصلة بالشبكة بتحميل أنظمة التشغيل عن طريق الشبكة ، حيث أن أنظمة التشغيل يتم أعدادها على شكل صور Images ، وتقوم الأجهزة بالوصول الى الصور Images الخاصة بأنظمة التشغيل من خلال عملية الأقلاع Boot عبر كرت الشبكة بعد حصولها على عنوان IP من خادمDHCP ، حيث تم استخدام نسخة Windows XP و أنشاء صورة IMAGE من النسخة ضمن ملف Install Image الموجود على الخادم ، كما تم أنشاء صورة Image لملف الأقلاع BOOT والتي تكون موجودة ضمن ملف BOOT Images على الخادم حتى تتمكن الأجهزة من الوصول الى نسخة Windows XP او أي نظام تشغيل أخر يوفره الخادم بعد حصولها على عنوان IP .

كما تم انشاء Option او اعدادات خاصة بخادم WDSعلى خادم DHCP ، حيث ان هذه الأعدادات يتم توزيعها على الأجهزة حتى تتمكن من الأتصال بخادم WDS ، وهي أعدادات خاصة بـ(PXE) Preboot execution Environment وتعرف في DHCP ب Pxe Client ، حيث أن PXE يعمل من خلال كرت الشبكة وهو الذي يسمح للجهاز بعملية الأقلاع Booting عبر كرت الشبكة و كذلك عملية الأتصال وتحميل أنظمة التشغيل عن بعد .

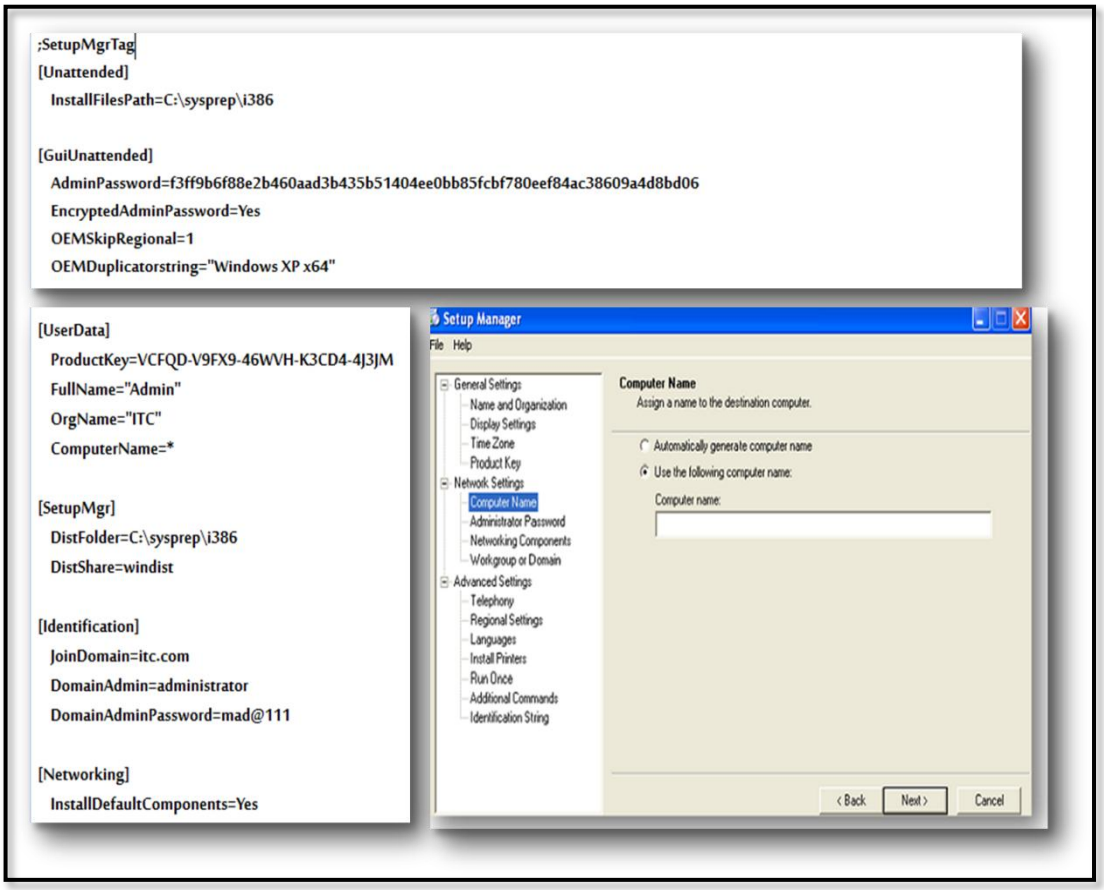
وكذلك تم تحديد المستخدمين المسموح لهم بعملية تحميل الأنظمة عبر خادم WDS ، حيث تم أعطاء هذه الصلاحية للفنين او قسم الدعم الفني (Technical Support) ، وتم منع كل المستخدمين في Domain من الوصول الى أنظمة التشغيل على الخادم و تحميلها (Administrator يسمح له بالوصول بشكل أفتراضي) .

بالأضافة الى انه قد تم انشاء نسخة من نظام التشغيل تدعم التحميل عبر تقنية MULTICAST والتي تعتبر أفضل من حيث سرعة التحميل مقارنة بالتحميل عبر تقنية UNICAST في حالة طلب النسخة من عدد كبير من الأجهزة ، كما تم تحديد عدد الأجهزة المطلوبة لكي يبدأ الخادم عملية التحميل عند العدد 2 (أي جهازين) ، وبالتالي فأن الخادم لن يقوم بأرسال بيانات و ملفات نظام التشغيل الى الأجهزة حتى تصل الأجهزة الى العدد المطلوب .

Capture Image in WDS Server 1.8.4

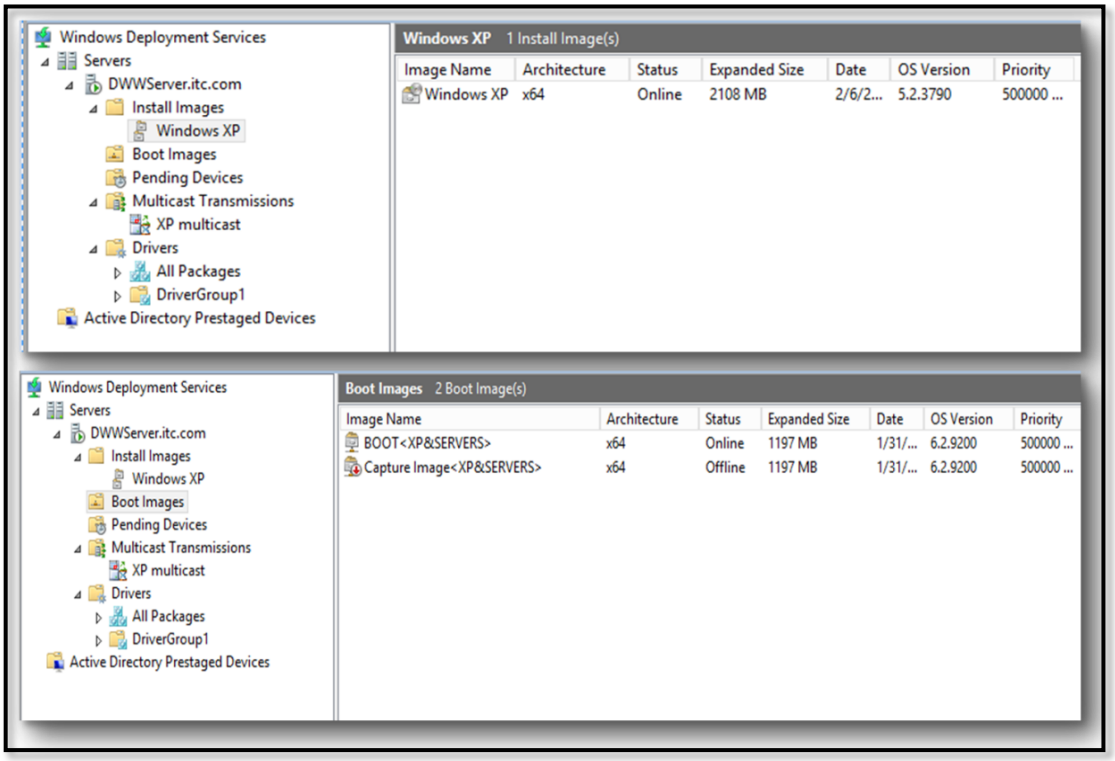
من خلال خدمات تصوير أنظمة التشغيل Capure Image التي يوفرها WDS Sevrer و التي تقوم بأخذ نسخ من أنظمة تشغيل الأجهزة التي تتصل بالخادم تم إنشاء نسخة جاهزة لنظام التشغيل (Windows XP) حيث تحتوي هذه النسخة على البرامج و التعريفات المطلوبة ، وبالتالي فأن الأجهزة لن تحتاج الى تثبيت أي برامج أو تعريفات عند الأنتهاء من تحميل نظام التشغيل من خادم WDS.

كما تم التعديل على هذه النسخة بحيث يتم إضافة الجهاز الذي يقوم بتحميل النسخة الى النطاق Domain وتسجيله في الجهاز الرئيسي Domain Controller و إنشاء أو توليد Generate اسم جديد لكل جهاز يقوم بتحميل النسخة حتى لا تتشابه أسماء الأجهزة التي يتم تسجيلها في Domain ، حيث تم استخدام أداة (SetUP Manager) SETUPMGR في إجراء هذه التعديلات ، و يوضح **الشكل 4-9** كل من أداة SETUPMGR والأعدادات الخاصة بها .



شكل(9.4) أداة SETUPMGR و أعداداتها

و يوضح **الشكل 4-10** اعدادات خادم WDS :-



شكل(10.4) أعدادات خادم WDS

9.4 إعداد و تهيئة خادم تحديثات ويندوز WSUS

على الرغم من أن عملية التحقق من التحديثات وتثبيتها تعتبر من العمليات المهمة والضرورية والتي تقوم بها الأجهزة الموجودة في الشبكة والتي تتحقق الأجهزة من خلالها إذا ما كان هناك أي تحديثات مهمة وخاصة في الجانب الأمني ألا أن هذه العملية تتطلب استهلاك مقدار كبير من عرض النطاق Bandwidth المخصص للشبكة وخاصة انه سيكون لدينا عدد كبير من الأجهزة والخوادم التي تحتاج للتحقق من التحديثات يوميا ، وبالتالي فأن هذه العملية ستسبب بطئ في ألأتصال عبر شبكة الأنترنت ، ولحل هذه المشكلة تم تهيئة خادم WSUS حتى يكون هو فقط المسؤول عن تحميل أي تحديثات تحتاجها الأجهزة ، ثم يقوم هذا الخادم بتوزيع هذه التحديثات على الأجهزة .

حيث تم استخدام قاعدة بيانات داخلية Windwos Internal Database (WID) لتخزين التحديثات التي يقوم الخادم بتحميلها وذلك من بعد أن يقوم بعملية المزامنة مع خادم التحديثات Update Server الخاص بمايكروسوفت .

كما تم تحديد فئات (Classes) التحديثات المطلوبة التي سيقوم الخادم بتحميلها ، وكذلك تم تحديد المنتجات Products التي سيتم تحميل التحديثات الخاصة بها .

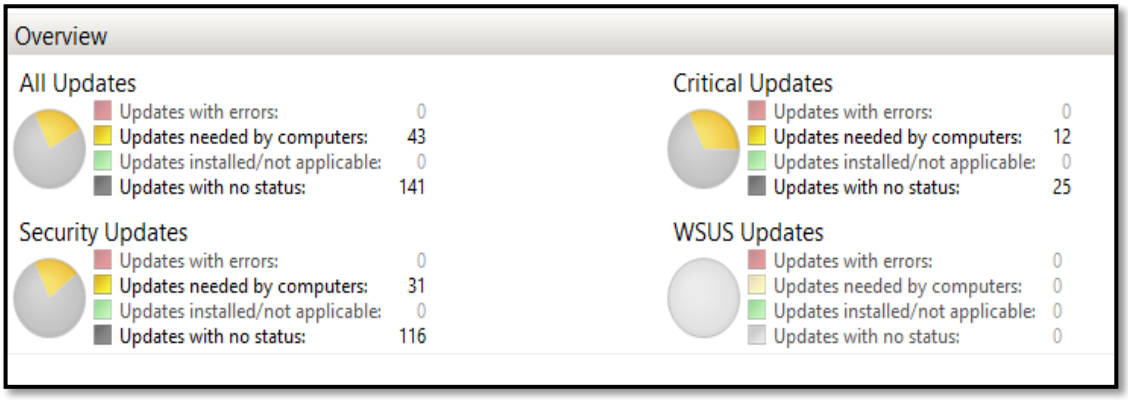
المنتجات أو Products التي تم تحديدها لتحميل التحديثات لها :-

1. Windows Server 2012 .
2. Windows XP .

الفئات Classes التي تم تحديدها لتحميل التحديثات لها :-

1. Critical Updates .
2. Definition Updates .
3. Security Updates .

و يوضح **الشكل 4-11** التحديثات الي تم تحميلها على خادم WSUS :-



شكل (11.4) التحديثات الي تم تحميلها على خادم WSUS

وحتى تتمكن الأجهزة المتصلة بالشبكة من الوصول الى التحديثات فقد تم استخدام Group Policy التي يوفرها Domain وذلك لتحديد العنوان الخاص بالخادم الذي سيتم تحميل التحديثات منه وهو عنوان خادم WSUS ،حيث تم تحديد عنوان خادم التحديثات WSUS للأجهزة كالتالي :-

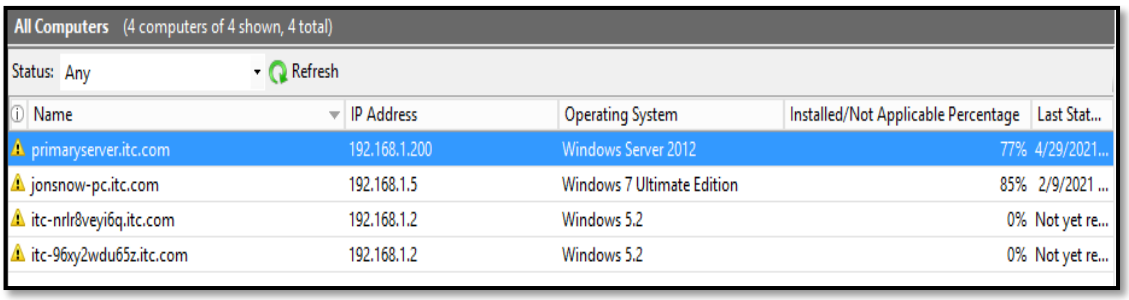
http://DWWServer:8530 .

حيث أن DWWSERVER هو اسم الخادم الذي تم تهيئة WSUS عليه ، و 8530 هو رقم المنفذ Port الخاص بخادم WSUS .

وبأستخدام Group Policy تم التعديل على إعدادات التحديثات الخاصة بالأجهزة حتى تقوم بتحميل التحديثات من WSUS ولكن لا تقوم بتثبيتها على الأجهزة حتى يقوم المستخدم بذلك ، حيث تم تحديد ذلك بتحديد الأعدادات على Policy كالتالي :-

Download the updates automatically and notify when they are ready to be installed

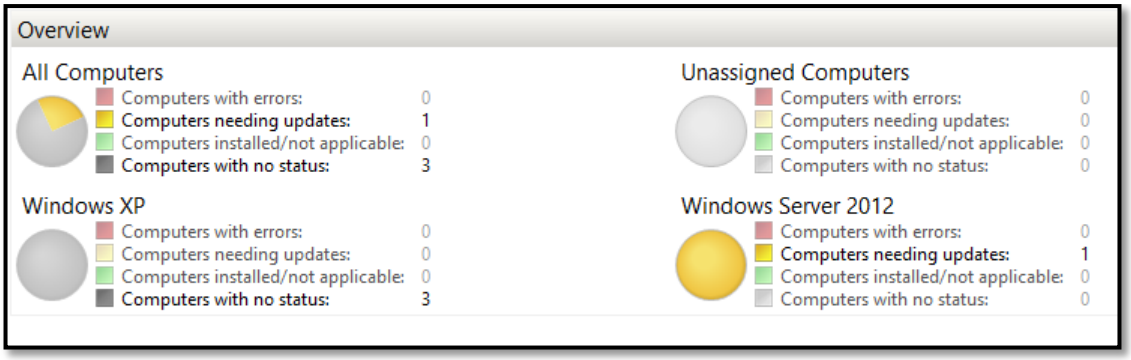
وبالتالي فأن أي جهاز سيقوم بطلب التحديثات سيتم تسجيله على خادم WSUS، ويوضح **الشكل 4-12** الأجهزة التي تقوم بطلب التحديثات من خادم Wsus .



شكل (12.4) عملية طلب الأجهزة للتحديثات من خادم WSUS

و حتى يتمكن WSUS من تصنيف وتنظيم كل الأجهزة التي تقوم بطلب التحديثات منه ضمن مجموعات فقد تم استخدام Group Policy على الأجهزة بحيث يتم تنظيمها في مجموعات يتم انشائها على WSUS Server عن طريق تفعيل (Client Side Targeting) على هذه الأجهزة وذلك من خلال Group Policy .

حيث يتم إضافة جهاز Domain Controller إلى مجموعة بأسم Windows server 2012 ، بينما يتم إضافة الأجهزة الأخرى إلى مجموعة بأسم Windows XP ، وذلك وفقا لما تم تحديده في السياسات Policy ، و حسب مكان تواجد هذه الأجهزة على OU الموجودة في Active Directory والتي تم تطبيق policy عليها (أي أنه سيتم توزيع الأجهزة على مجموعات في WSUS حسب ترتيب ومكان الأجهزة علىActive directory user and computer) ، مما يسهل من عملية إدارة وتوزيع التحديثات على الأجهزة ويوضح **الشكل 4-13** هذه العملية .



شكل(13.4) عملية توزيع الأجهزة على المجموعات في خادم WSUS

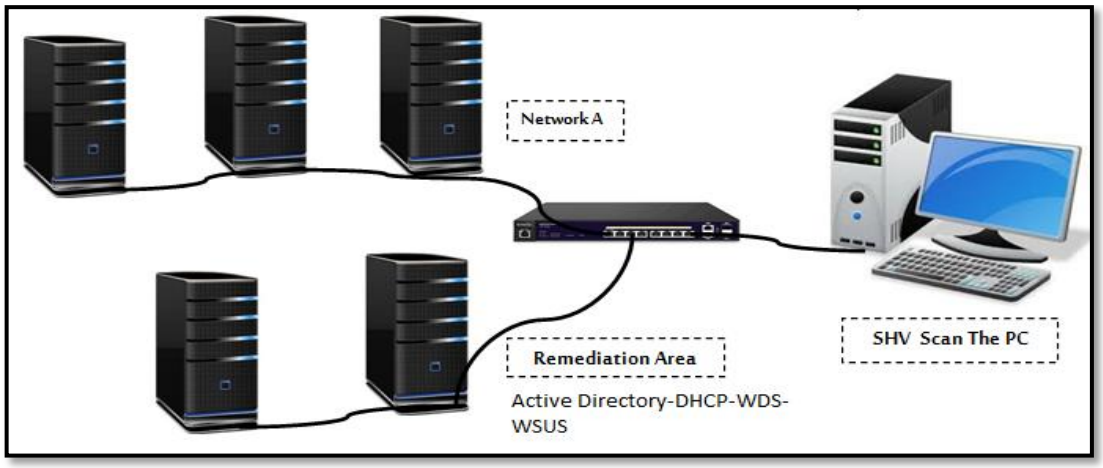
10.4 إعداد و تهيئة خادم سياسات الشبكة NPS

بما أن أمان الأجهزة المتصلة بالشبكة وخلوها من أي فيروسات يعتبر جزء لا يتجزء من أمان الشبكة فلابد من التأكد من أن هذه الأجهزة ليس عليها أي فيروسات أو برامج يمكنها التأثير على أمن الشبكة ، وبالتالي فقد تم إعداد هذه الشبكة لفحص الأجهزة قبل الأتصال بها وذلك من خلال الخدمات التي يوفرها خادم NPS.

تم إعداد هذه الخدمة لتقوم بفحص أي جهاز يريد الأتصال بالشبكة والتأكد من تحقيقه للشروط او القيود التي تم وضعها لكي تتمكن من الأتصال ، حيث يتم تنفيذ هذه الخدمة من خلال خدمة Network Access Protection (NAP) التي يوفرها هذا الخادم والتي تعمل من خلال خادم DHCP حيث أن أي جهاز يريد الحصول على IP يمكنه من الأتصال بالشبكة لابد له من تحقيق الشروط التي تم تحديدها ضمن مدقق الأمان SHV ليتمكن من الأتصال بكل الأجهزة و الخوادم الموجودة في الشبكة وفي حال عدم تحقيقه لأحد الشروط فأنه يستطيع الأتصال بالخوادم التي تم وضعها ضمن منطقة العزل Remediation Area وهي :-

1. Active Directory
2. DHCP
3. Windows Deployment Server
4. Windows Update Server

الشكل 4-14 يوضح الية عمل NPS .



شكل(14.4) ألية عمل خادم NPS

من القيود التي تم تحديدها على الأجهزة لكي تستطيع الأتصال بالشبكة والموضحة في **الشكل4-15**

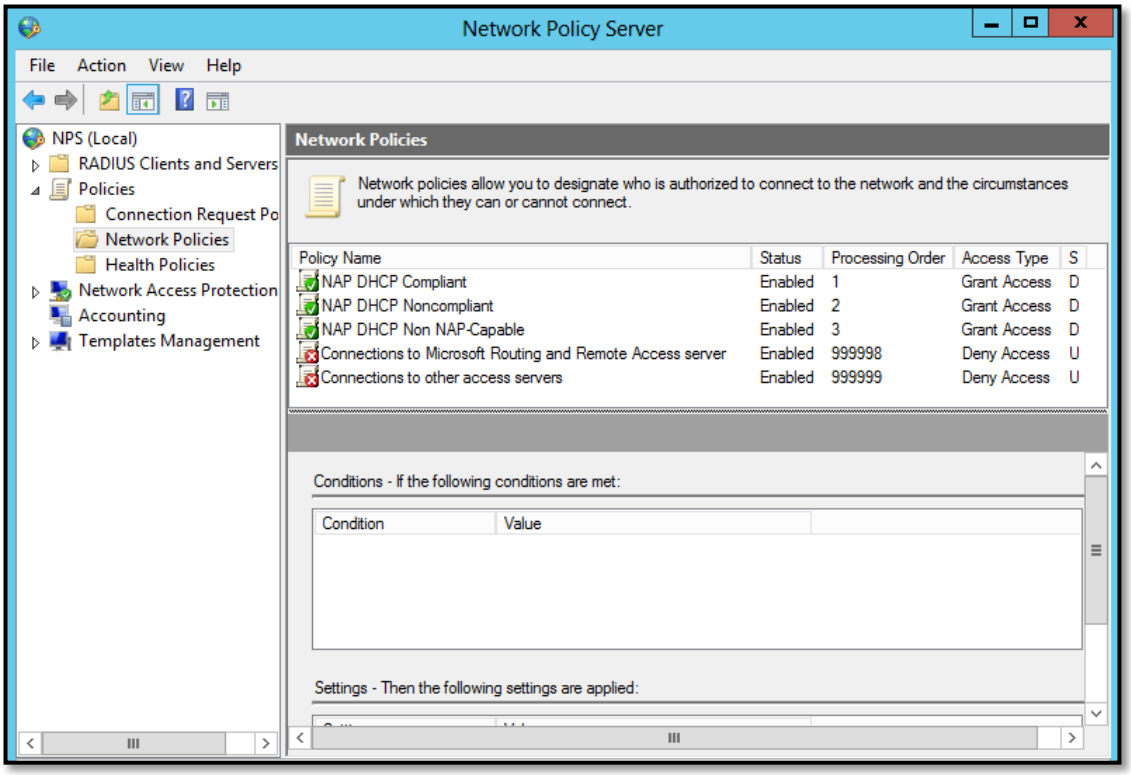
1. أن يكون جدار الحماية Firewall مفعل على الأجهزة .
2. أن تحتوي الأجهزة على برنامج حماية من الفيروسات Anti Virus .
3. أن تحتوي الأجهزة على برامج حماية من التجسس Anti Spyware .

شكل(15.4) القيود المحددة من خادم NPS للاتصال بالشبكة

كما يمكن اضافة قيود اخرى مثل ان يكون الجهاز بأخر تحديثاته وذلك بأن يكون متصل بشكل اوتوماتيكي بسيرفر مايكروسوفت لتحميل التحديثات ولكن نظرا لأستخدام خادم خاص بالتحديثات Windows Server Update Service في الشبكة لم يتم تفعيل automatic Update .

كما تم تطبيق Policies خاصة بخدمة Network Access Protection على أجهزة الشبكة من خلال Group Policy التي يوفرها Domain Controller لكي تستطيع الأجهزة التعامل مع هذه الخدمات ، حيث تم استخدام Group Policy لتفعيل Nap Service على أجهزة الشبكة لكي تستطيع التعامل مع خدماتها ، كما تم تفعيل خدمات حجز الأجهزة من خلال DHCP (DHCP Quarantine Enforcement) وكذلك Security Center على أجهزة الشبكة وذلك لتنبيه المستخدمين بأن أجهزتهم لم تحقق شروط الأتصال بالشبكة وانه قد تم عزل أجهزتهم في منطقة العزل Remediation Area .

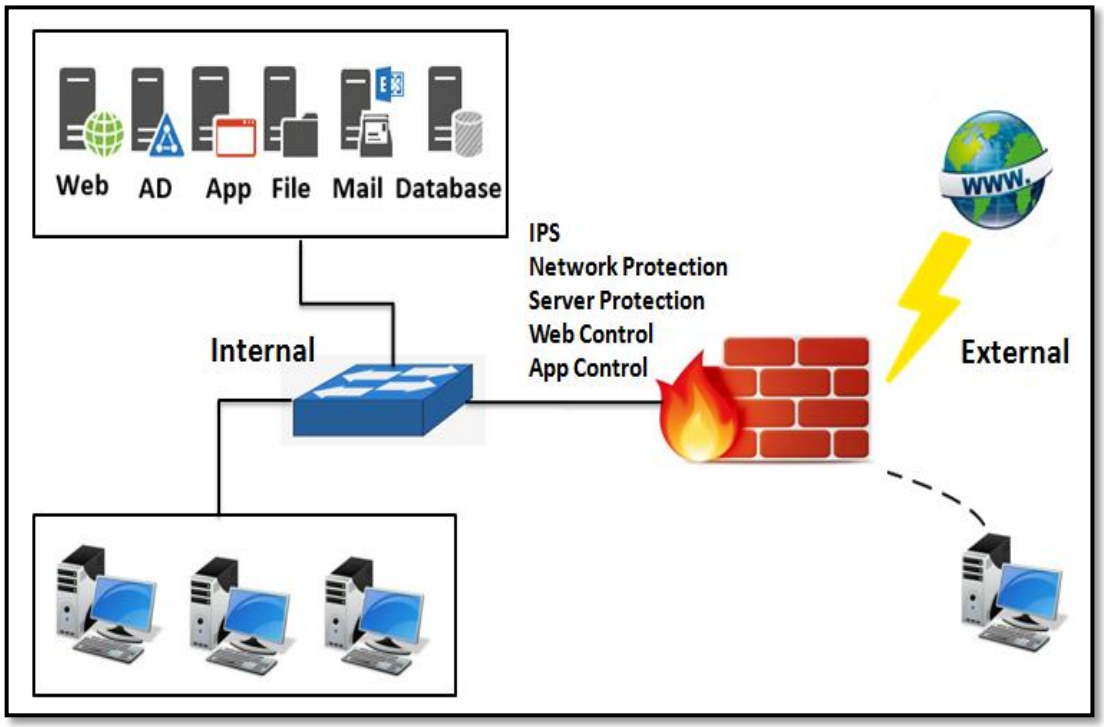
الشكل 4-16 يوضح NAP Policies :-



شكل(16.4) NAP Policies

11.4 إعداد و تهيئة جدار الحماية TMG

من المهم لكل شبكة أن يتم تصميمها وإعدادها بحيث تستطيع مراقبة اتصالاتها مع الشبكات الخارجية (مثل شبكة الانترنت) والتحكم بها ، عادة ما تتم هذه العملية من خلال جدران الحماية Firewalls (سواء كانت Hardware أو Software) والتي تعتبر من الخدمات المهمة و الأساسية التي يتم إعدادها ضمن أي شبكة ، حيث توفر Firewalls العديد من الخدمات التي يمكنها مراقبة والتحكم في اتصالات أي شبكة مع الشبكات الأخرى، وقد تم في هذه الشبكة تهيئة و إعداد TMG للعمل كجدار حماية Firewall ومراقبة الاتصالات بين مختلف الشبكات ، و يوضح **الشكل 4-17** آلية عمل Firewall في الشبكة :-



شكل(17.4) ألية عمل جدار الحماية على الشبكة

وبما أن TMG عند دخوله للشبكة يقوم بتقسيمها إلى خمسة أقسام (Local Host – Internal – External – VPN – VPN Quarantined) فأنه لابد من أن يتم ربط هذه الشبكات مع بعضها حتى تتمكن من الاتصال من خلال TMG ، ويتم ذلك من خلال خدمات Routing و NAT التي يوفرها TMG.

كما انه قد تم تحديد المستخدمين المخولين بالوصول إلى شبكة الانترنت (طلبة – موظفين– مدرسين – فنيين) و كذلك تحديد البروتوكولات التي يستطيعون استخدامها عبر الشبكة والتي من خلالها يمكن تحديد الخدمات التي يمكنهم استخدامها أو الوصول إليها عبر الشبكة .

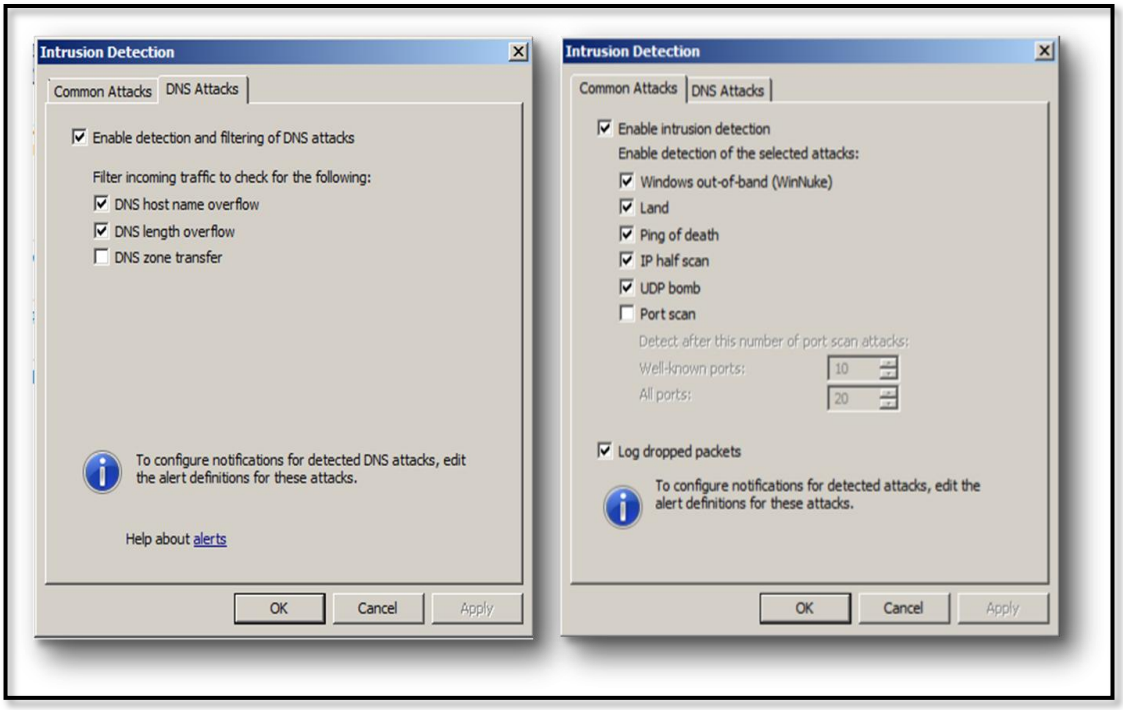
الجدول 2-4 يوضح الصلاحيات والبروتوكولات التي تم منحها إلى المستخدمين من خلال TMG :-

جدول (2.4) يوضح الصلاحيات المحددة للمستخدمين من خلال جدار الحماية TMG

Destination	Source	ACTION	PROTOCOLS	USERS
EXTERNAL	INTERNAL	ALLOW	DNS Server – DNS – FTP Over Http – FTP Server – FTP – HTTP – HTTPS – HTTP Server – HTTPs Server POP3 Server – POP3 – POP3S Server SMTP – SMTP Server – SMTPS Server	STUDENTS FOS
EXTERNAL	INTERNAL	DENY	DNS Server – DNS – FTP Over Http – FTP Server – FTP – HTTP – HTTPS – HTTP Server – HTTPs Server POP3 Server – POP3 – POP3S Server SMTP – SMTP Server – SMTPS Server	EMPLOYEES
EXTERNAL	INTERNAL	ALLOW	DNS Server – DNS – FTP Over Http – FTP Server – FTP – HTTP – HTTPS – HTTP Server – HTTPs Server POP3 Server – POP3 – POP3S Server SMTP – SMTP Server – SMTPS Server	Technical Support
EXTERNAL	DWWServer	ALLOW	ALL Outbound TRAFFIC	ALL Users
EXTERNAL	INTERNAL	ALLOW	ALL Outbound TRAFFIC	domain admin

بالإضافة إلى POLICY أخرى يقوم TMG بإنشائها بشكل تلقائي عند تهيئته والتي تعمل على أقفال أو منع كل الاتصالات بين الشبكات المختلفة التي يقوم TMG بإنشائها .

كما تم إعداد و تهيئة خدمة URL Filtering التي يوفرها TMG وذلك لمنع الوصول إلى أي مواقع غير ضرورية والتي يمكن أن تكون سببا في إستهلاك موارد الشبكة وكذلك Bandwidth مما يسبب بطئ في الاتصالات للمستخدمين ، كما تم تفعيل خدمات IPS أو ما يعرف بنظام منع التجسس (Intrusoin Prevention System) والتي تستطيع من خلالها منع الوصول لأي مستخدم يحاول تنفيذ أي عملية قد تشكل خطرا على الشبكة مثل استخدامه لخدمة اختبار الاتصال Ping بشكل كبير أو ما يعرف Ping of Death والتي قد تعتبرها هذه الخدمة كهجوم على الشبكة ، كما تم تفعيل خدمات للحماية من برامج التجسس بحيث أن أي شخص يحاول الأتصال بهذه الشبكة مستخدما هذه البرامج أو يحاول إرسال بيانات لا يستطيع TMG التعرف عليها سيتم منعه من الأتصال ، ويوضح **الشكل 4-18** أعدادات IPS :-



شكل (18.4) أعدادات Intrusuion prevention System (IPS)

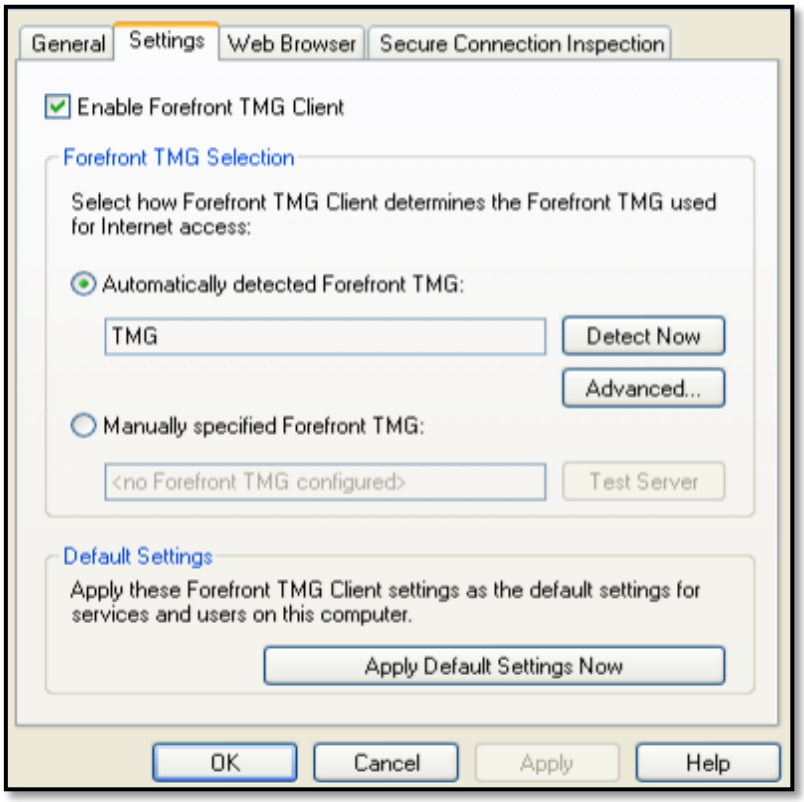
عندما يتم الأنتهاء من تهيئة و إعداد TMG Firewall فأن الأجهزة الموجودة في الشبكة لن تستطيع الأتصال من خلال TMG ولابد من ان يتم تهيئة الأتصال بينها وبين TMG حتى تستطيع الوصول إلى شبكة الأنترنت والشبكات الأخرى ، وبما أن TMG يوفر ثلاث طرق للأجهزة للتمكن من

الأتصال به (Proxy – SecureNAT – TMG Client) وبعد الدراسة لمزايا وعيوب كل طريقة من الطرق السابقة فقد تم استخدام TMG Client ليسمح للأجهزة بالأتصال من خلاله .

TMG Client يوفر العديد من المزايا مثل امكانية التعامل مع حسابات المستخدمين والأجهزة التي يتم تسجيلها في Active Directory وأن يسمح أو يمنع الأتصال بين الشبكات بناء على حسابات المستخدمين أو أجهزتهم (عناوين IP) ، وبما ان TMG Client يستخدم عدة طرق للسماح بالأتصال عبر (Active Directory – DHCP –DNS) فقد تم إعداد الأتصال ليتم من خلال Active Directory وذلك بتفعيل خدمة ADconfig على Domain ومن ثم كتابة الأمر التالي :-

TMG adconfig add –default –type winsock –url http://tmg.itc.com:80/wspad.dat

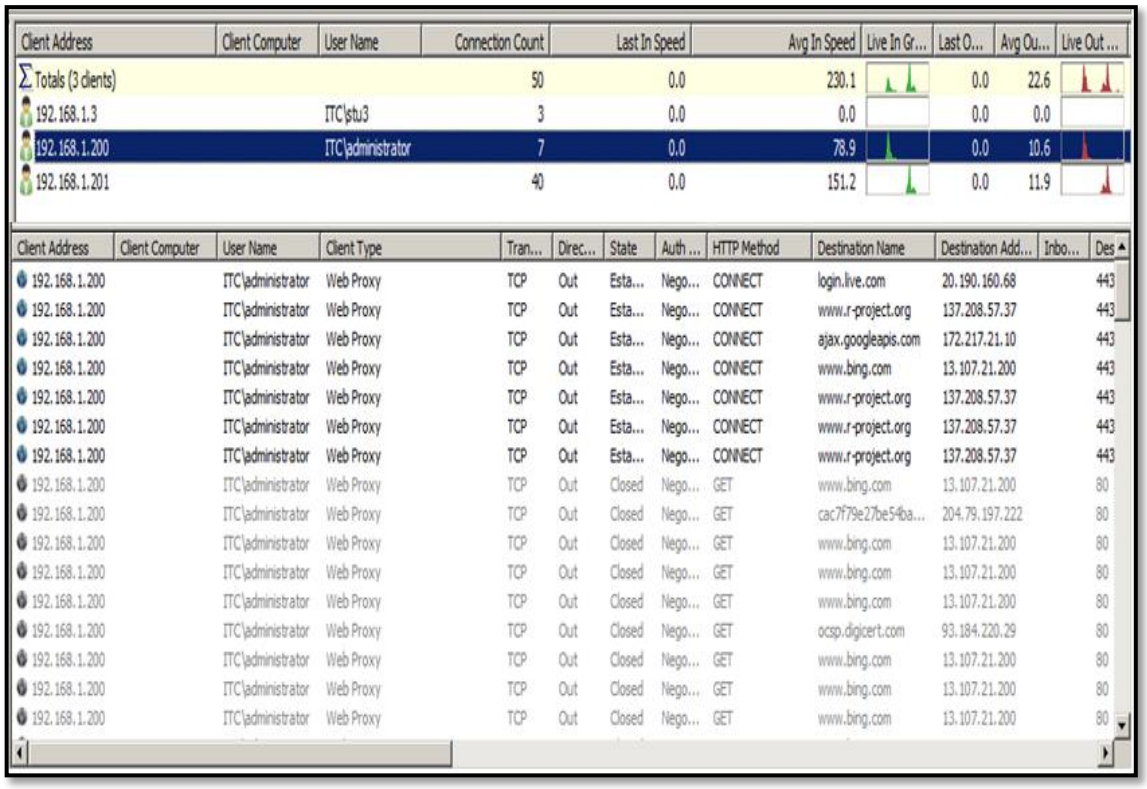
بعد ان تم تنفيذ الأمر السابق على Domain سيقوم بأرسال إعدادت TMG الى الأجهزة وذلك من خلال تطبيق TMG Client الذي تم تثبيته على أجهزة الشبكة من خلال Group Policy حتى تتمكن كل الأجهزة من فحص الشبكة والوصول الى TMG والحصول على الأعدادات من خلال هذا التطبيق ،و يوضح **الشكل 4-19** واجهة التطبيق TMG Client :-



شكل(19.4) واجهة تطبيق TMG Client

كما أنه تم استخدام أداة Bandwidth Splitter من خلال TMG للمراقبة و التحكم في عرض النطاق Bandwidth المستخدم من قبل المستخدمين على الشبكة حيث تم أعداد هذه الأداة لتقوم بالتالي :-

1. تحديد سرعة التحميل Download والرفع Upload لحسابات الطلبة ب 800 kbps وذلك عبر قواعد تحديد السرعة Shaping Rule .
2. تحديد حصة Quota من Bandwidth ب 10Mb لحسابات الطلبة وذلك عبر قواعد الحصص Quota Rule .
3. أنشاء قواعد Rules لمراقبة استهلاك كل من Administrator و خادم التحديثات Wsus للنطاق الترددي Bandwidth المخصص للشبكة ، و يوضح **الشكل 4-20** عملية مراقبة المستخدمين عبر أداة Bandwidth Splitter .

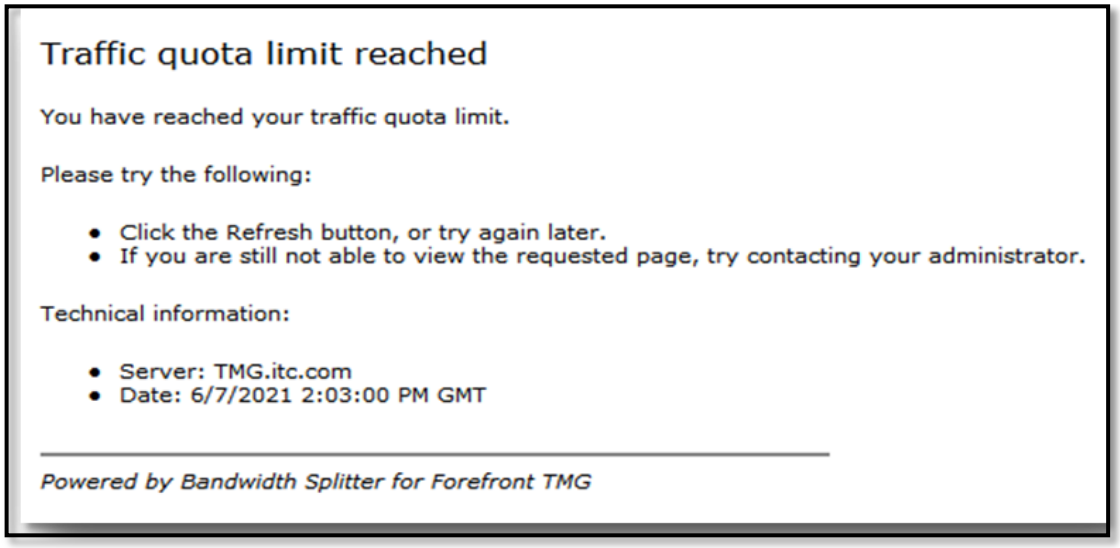


Client Address	Client Computer	User Name	Connection Count	Last In Speed	Avg In Speed	Live In Gr...	Last O...	Avg Ou...	Live Out ...
Σ Totals (3 clients)			50	0.0	230.1		0.0	22.6	
192.168.1.3		ITC\stu3	3	0.0	0.0		0.0	0.0	
192.168.1.200		ITC\administrator	7	0.0	78.9		0.0	10.6	
192.168.1.201			40	0.0	151.2		0.0	11.9	

Client Address	Client Computer	User Name	Client Type	Tran...	Direc...	State	Auth ...	HTTP Method	Destination Name	Destination Add...	Inbo...	Des
192.168.1.200		ITC\administrator	Web Proxy	TCP	Out	Esta...	Nego...	CONNECT	login.live.com	20.190.160.68		443
192.168.1.200		ITC\administrator	Web Proxy	TCP	Out	Esta...	Nego...	CONNECT	www.r-project.org	137.208.57.37		443
192.168.1.200		ITC\administrator	Web Proxy	TCP	Out	Esta...	Nego...	CONNECT	ajax.googleapis.com	172.217.21.10		443
192.168.1.200		ITC\administrator	Web Proxy	TCP	Out	Esta...	Nego...	CONNECT	www.bing.com	13.107.21.200		443
192.168.1.200		ITC\administrator	Web Proxy	TCP	Out	Esta...	Nego...	CONNECT	www.r-project.org	137.208.57.37		443
192.168.1.200		ITC\administrator	Web Proxy	TCP	Out	Esta...	Nego...	CONNECT	www.r-project.org	137.208.57.37		443
192.168.1.200		ITC\administrator	Web Proxy	TCP	Out	Esta...	Nego...	CONNECT	www.r-project.org	137.208.57.37		443
192.168.1.200		ITC\administrator	Web Proxy	TCP	Out	Closed	Nego...	GET	www.bing.com	13.107.21.200		80
192.168.1.200		ITC\administrator	Web Proxy	TCP	Out	Closed	Nego...	GET	cac7f79e27be54ba...	204.79.197.222		80
192.168.1.200		ITC\administrator	Web Proxy	TCP	Out	Closed	Nego...	GET	www.bing.com	13.107.21.200		80
192.168.1.200		ITC\administrator	Web Proxy	TCP	Out	Closed	Nego...	GET	www.bing.com	13.107.21.200		80
192.168.1.200		ITC\administrator	Web Proxy	TCP	Out	Closed	Nego...	GET	www.bing.com	13.107.21.200		80
192.168.1.200		ITC\administrator	Web Proxy	TCP	Out	Closed	Nego...	GET	ocsp.digicert.com	93.184.220.29		80
192.168.1.200		ITC\administrator	Web Proxy	TCP	Out	Closed	Nego...	GET	www.bing.com	13.107.21.200		80
192.168.1.200		ITC\administrator	Web Proxy	TCP	Out	Closed	Nego...	GET	www.bing.com	13.107.21.200		80
192.168.1.200		ITC\administrator	Web Proxy	TCP	Out	Closed	Nego...	GET	www.bing.com	13.107.21.200		80

شكل(20.4) عملية مراقبة المستخدمين عبر Bandwidth Splitter

و يوضح **الشكل 4-21** عملية منع مستخدم من الاتصال بالأنترنت عند أستهلاكه للحصة Quota المخصصة له .



Traffic quota limit reached

You have reached your traffic quota limit.

Please try the following:

- Click the Refresh button, or try again later.
- If you are still not able to view the requested page, try contacting your administrator.

Technical information:

- Server: TMG.itc.com
- Date: 6/7/2021 2:03:00 PM GMT

Powered by Bandwidth Splitter for Forefront TMG

شكل(21.4) أستهلاك ألمستخدم للحصة المخصصة له من عرض النطاق الترددي

الفصل الخامس

النتائج و التوصيات

5. النتائج و المناقشة

مـــن خـــلال اســـتخدام بيئـــة النطـــاق أو المجـــال (Domain) التـــي يوفرهـــا نظـــام التشـــغيل Window Server 2012 لبناء شبكة لجامعة سبها نستنتج أن بيئة النطاق توفر مستوى أعلى من الخدمات مقارنة ببيئة المجموعات Workgroup من حيث توفيرها لتحكم مركزي لمختلف الخدمات على الشبكة ، بالإضافة لتوفير درجة أعلى من الأمان من خلال الخدمات و التقنيات المختصة بالجانب الأمني و التي توفرها هذه البيئة في نظام Windows Server 2012 و الغير موجودة فـــي الأنظمـــة القديمـــة ، حيـــث أن خـــدمات المســـتخدمين و الأجهـــزة أو مـــا يعـــرف بخـــدمات Active Directory Users And Computers جعلت من عملية أدارة حسابات المستخدمين التي يتم إنشائها و الأجهزة التي يتم تسجيلها في النطاق عملية مركزية (أي يمكن إدارة كل هذه الحسابات والأجهزة من الخادم المركزي) ، كما أن تحديد الصلاحيات بأستخدام Group Policy لتعريف و ربط الأجهزة بالخدمات التي تم أعدادها و تهيئتها على الشبكة وكذلك تحديد صلاحيات المستخدمين و الأجهزة كان له دور كبير في تحسين الجانبين الأمني و الخدمي لهذه الشبكة ، حيث أنها تضمن اتصال الأجهزة بالخدمات عند تشغيلها وكذلك عدم تجاوز المستخدمين او الأجهزة لصلاحياتهم ، بالأضافة إلى أن هذه البيئة جعلت من تسجيل بيانات الأجهزة في خادم DNS و أنشاء سجلات لهم عملية غير معقدة ،وذلك لأنه يتم أنشاء سجل لأي جهاز يتم تسجيله في النطاق داخل خادم DNS تلقائيا بدل إنشائه بشكل يدوي ، كما أن عملية توزيع العناوين عبر خادم DHCP على أجهزة الشبكة أصبحت أكثر أمانا ، وذلك لأن بيئة النطاق جعلت من اتصال خادم DHCP موثوق وبالتالي يمنع توزيع عناوين IP من أي خادم DHCP غير موثوق .

بالإضافة إلى أن تهيئة خادم ويب على الشبكة الخاصة بجامعة سبها سيوفر أمكانية استضافة المواقع داخل المؤسسة بدل من أستضافتها لدى شركات أو مؤسسات أخرى تقدم خدمات استضافة المواقع بمقابل مادي .

كما أن تهيئة خادم ملفات مركزي سهل من عملية أدارة الملفات وتحديد صلاحيات كل مستخدم من حيث الوصول للملفات أو التعديل عليها وحذفها مما يوفر الخصوصية لبيانات كل مستخدم ، بالإضافة إلى أن تحديد مساحة تخزين معينه لكل مستخدم و منعه من تخزين ملفات الوسائط كالصور والموسيقى والفيديو وغيرها ستوفر في مساحة التخزين على خادم الملفات بشكل كبير،

و يوفر خادم الملفات حماية للملفات أو البيانات الموجودة عليه عبر منع تخزين أي ملفات قد تشكل خطر على هذه البيانات ، و سيقوم بعرض بيانات أي مستخدم يحاول القيام بأي عملية غير مسموح بها أو تخزين أي ملف بأمتداد غير مسموح به من خلال Event Viewer التي يوفرها النظام وذلك لأتخاذ الأجراء المناسب له ، كما بسط خادم الطباعة من عملية أدارة الطابعات المتصلة بالشبكة وكذلك عملية مشاركتاها عبر الشبكة من خلال Group Policy بدلا من إضافة الطابعات لكل جهاز وكذلك مشاركتها من كل جهاز للأجهزة الأخرى .

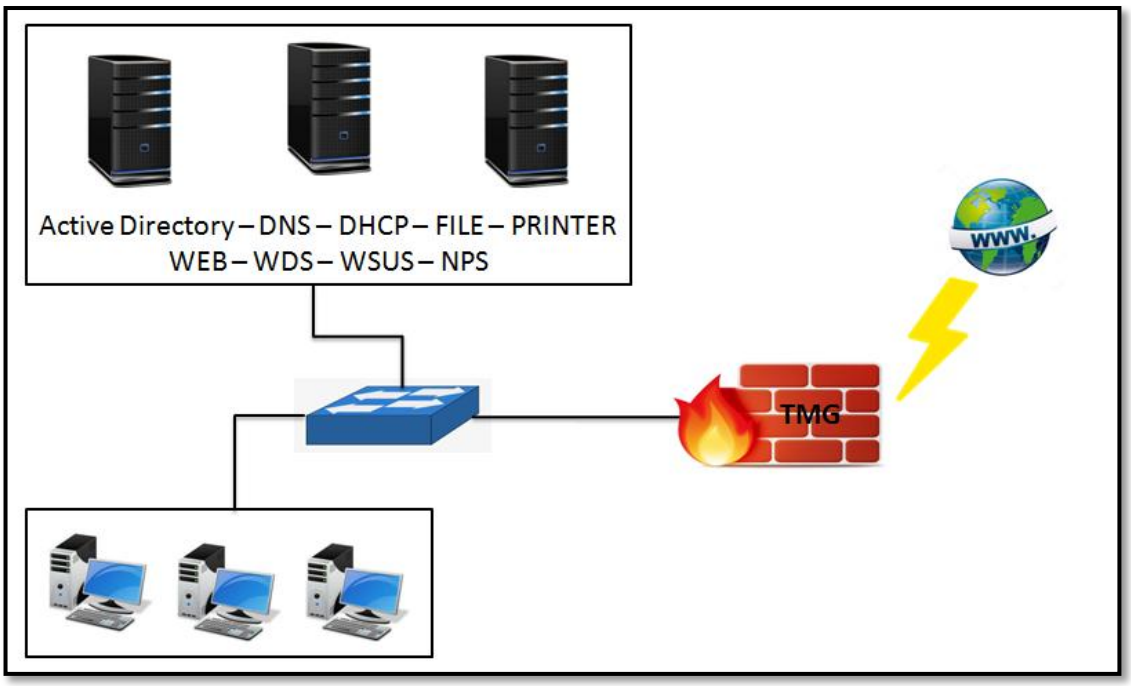
ومن خلال تهيئة خادم WDS فقد عملنا على توفير خادم مركزي لإدارة عملية تحميل أنظمة التشغيل عن بعد لأجهزة الشبكة و تحديد المستخدمين المخولين بالوصول إليها مما سيوفر الجهد و كذلك الوقت المستغرق لتحميل الأنظمة ، حيث أنه يمكن للأجهزة الوصول للخادم عن طريق الشبكة بدلا من نقل الأجهزة من المكان التي تتواجد فيه والذي سيتطلب بذل جهد كبير ، كما أن تحميل نظام التشغيل على الأجهزة سيستغرق وقت أقل مقارنة بالوقت المستغرق عند استخدام الوسائل التقليدية مثل DVD والذي يتطلب إدخاله في كل جهاز بشكل منفصل للحصول على النسخة ، كما أنه من خلال خادم WSUS عملنا على توفير التحديثات لأنظمة التشغيل على الخادم وبالتالي فأن الأجهزة لن تحتاج لاستخدام الانترنت للحصول على التحديثات بل ستقوم بالاتصال بخادم WSUS وتحميل التحديثات الجديدة مما قلل من استهلاك عرض النطاق الترددي Bandwidth المخصص للاتصال بشبكة الانترنت .

وقد وفر خادم NPS مستوى جيد من الحماية للشبكة الداخلية من خلال عزل أي جهاز في حال عدم تحقيقه لمتطلبات الاتصال الأمن عبر خدمة Network Access Protection (NAP) و وضعه في منطقة العزل Remediation Area وبالتالي سنضمن عدم أتصال أي جهاز قد يشكل خطرا على الشبكة بأي خوادم تحتوي على بيانات ومعلومات مهمة .

ومن خلال تهيئة جدار الحماية TMG Firewall للعمل في هذه الشبكة فقد حققنا حماية للاتصالات التي تتم بين الشبكة الداخلية والشبكات الأخرى وذلك عبر مراقبة حركة بيانات المستخدمين Traffic و منع أي عمليات مشبوهة يمكن أن تشكل خطراً على أجهزة و خوادم الشبكة الداخلية ، كما قل إستهلاك عرض النطاق الترددي المخصص للاتصال بالانترنت نتيجة للقواعد Rules التي تم وضعها عبر أداة Bandwidth Splitter من خلال TMG ، وبالتالي فأن تقليل إستهلاك عرض

النطاق الترددي سينتج عنه أيضا تقليل التكاليف المدفوعة لمزود الخدمة ، وعلى الرغم من أن TMG يوفر أمكانية التحكم في الوصول إلى المواقع أو منعها عبر خدمة URL Filtring ألا انه لا يؤدي هذه الخدمة بشكل جيد فقد يتمكن المستخدم من الوصول إلى موقع قد تم منع الوصول إليه .

وبالتالي فقد تم تهيئة خوادم الشبكة لتقدم مجموعة من الخدمات الأساسية عبر الشبكة وتوفير أدارة مركزية لها، وكذلك حماية الخوادم وبياناتها عبر خدمات و تقنيات الأمان التي تم تهيئتها على الشبكة ، بالإضافة إلى توفير تحكم في عرض النطاق الترددي Bandwidth عبر خدمات جدار الحماية مما يقلل من استهلاكه و يوضح **الشكل1.5** التصميم النهائي للشبكة .



شكل(1.5) التصميم النهائي للشبكة

1.5 الخلاصة

تم في هذا البحث دراسة الخوادم الموجودة في مركز تقنية المعلومات وذلك لمعرفة القصور في خدماتها والمشاكل التي تواجهها لمعالجتها والرفع من مستوى خدماتها، حيث تم بناء شبكة لجامعة سبها باستخدام بيئة النطاق Domain التي يوفرها نظام التشغيل Windwos server ، كما تم استخدام نظام التشغيل Windows server 2012 لتهيئة أجهزة الخوادم و إعدادها لتقدم خدماتها على الشبكة ، فقد تم توفير أدارة لحسابات المستخدمين و الأجهزة عبر خدمات أدارة حسابات المستخدمين والأجهزة التي يوفرها الدليل النشط ، بالإضافة إلى توفيرها لخدمة DNS حتى تتمكن أجهزة الشبكة من الاتصال ببعضها عن طريق الأسماء وكذلك خدمة DHCP لتوزيع العناوين على الأجهزة الموجودة على الشبكة ، كما وفرت هذه الشبكة أمكانية إستضافة المواقع من خلال خادم الويب ، و نتيجة لاستخدام بيئة النطاق Domain في هذه الشبكة فقد تم توفير أدارة مركزية لملفات المستخدمين والطابعات المتصلة بالشبكة عبر خادم الملفات و خادم الطابعات التي تم تهيئتهما على الشبكة ، كما وفر خادم WDS أمكانية تحميل أنظمة التشغيل عن بعد عبر الشبكة بالإضافة إلى توفير التحديثات لهذه الأنظمة من خلال خادم WSUS ، و من خلال تهيئة خادم NPS و أعداده لتقديم خدمة NAP تم توفير الحماية لخوادم و أجهزة الشبكة وذلك عبر منع اتصال أي جهاز لم يحقق متطلبات الاتصال الأمن و تحويله لمنطقة العزل Remediation Area ، وكذلك منع أي عمليات مشبوهة من الشبكات الخارجية عبر خدمات التي يوفرها جدار الحماية TMG من خلال مراقبته وتحكمه في اتصالات وحركة بيانات المستخدمين والذي سمح أيضا بالتحكم في عرض النطاق الترددي Bandwidth لكل مستخدم وتقليل استهلاكه عبر الخدمات التي يوفرها جدار الحماية ، وبهذا فقد تحصلنا على شبكة تلبي إحتياجات المستخدمين كما توفر أكبر قدر ممكن من الحماية والأمان لخوادمها .

2.5 التوصيات و آفاق التطوير

من خلال ما تحصلنا عليه من نتائج نوصي بما يلي :-

1. مراقبة حالة الاتصال بين الجهاز الرئيسي Domain Controller و أجهزة الشبكة ، حيث أن اتصال الأجهزة مع الجهاز الرئيسي قد يصبح اتصال غير موثوق نتيجة لعدم استخدام الأجهزة لوقت طويل وبالتالي فأن المستخدمين لن يسمح لهم بتسجيل الدخول عبر حساباتهم مما يتطلب أعادة تسجيل الجهاز داخل النطاق Domain .
2. استخدام برامج المراقبة Monitoring لمراقبة أجهزة ومكونات الشبكة ،حيث يمكن لهذه البرامج مراقبة أداء أجهزة الشبكة وتنبيه مدير الشبكة في حال حدوث أي مشاكل لمعالجتها مما سيوفر شبكة تعمل بكفائة عالية .
3. دراسة إمكانية استخدام جدار حماية مادي Hardware Firewall بدلا من جدار حماية برمجي Software Firewall مثل TMG في شبكة جامعة سبها ، وذلك نظرا لضعف الخدمات التي يقدمها جدار الحماية البرمجي .
4. دراسة إمكانية استخدام تقنية الشبكات الافتراضية الخاصة Virtual Private Network (VPN) في شبكة جامعة سبها .

3.5 المراجع

1 Daniels, J.: ‘Server virtualization architecture and implementation’, XRDS: Crossroads, The ACM Magazine for Students, 2009, 16, (1), pp. 8-12

2 Kansal, A., Zhao, F., Liu, J., Kothari, N., and Bhattacharya, A.A.: ‘Virtual machine power metering and provisioning’, in Editor (Ed.)^(Eds.): ‘Book Virtual machine power metering and provisioning’ (2010, edn.), pp. 39-50

3 Tankard, C.: ‘Taking the management pain out of Active Directory’, Network Security, 2012, 2012, (4), pp. 8-11

4 Binduf, A., Alamoudi, H.O ,.Balahmar, H., Alshamrani, S., Al-Omar, H., and Nagy, N.: ‘Active Directory and Related Aspects of Security’, in Editor (Ed.)^(Eds.): ‘Book Active Directory and Related Aspects of Security’ (IEEE, 2018, edn.), pp. 4474-4479

5 Oluwatosin, H.S.: ‘Client-server model’, IOSRJ Comput. Eng, 2014, 16, (1), pp. 2278-8727

6 Sharapov, V.: ‘Implementing a hybrid network deployment server for Windows and Linux’, 2016

7 Chowdhury, N.M.K., and Boutaba, R.: ‘Network virtualization: state of the art and research challenges’, IEEE Communications magazine, 2009, 47, (7), pp. 20-26

8 Zacker, C.: ‘<Exam Ref 70-410 Installing and Configuring Windows Server 2012 R2 (PDFDrive.com).pdf>’ (Microsoft, 2014. 2014)

9 Mockapetris, P., and Dunlap, K.J.: ‘Development of the domain name system’, in Editor (Ed.)^(Eds.): ‘Book Development of the domain name system’ (1988, edn.), pp. 123-133

10 Henrick, K., and Thornton, J.M.: ‘PQS: a protein quaternary structure file server’, Trends in biochemical sciences, 1998, 23, (9), pp. 358-361

11 >‘DP-311U_PS Admin User's Manual.pdf>’, 1997

12 Filibeli, M.C., Ozkasap, O., and Civanlar, M.R.: ‘Embedded web server-based home appliance networks’, Journal of Network and Computer Applications, 2007, 30, (2), pp. 499-514

13 Ahonen, A.: ‘Windows Deployment Services: Esiasennuspalvelin’, 2010

14 Russel, C.: ‘<Administering Windows Server 2012 R2 (PDFDrive.com).pdf>’ (Microsoft Press, 2014. 2014)

15 Sood, A.: ‘Network access control’, Rivier Academic Journal, 2007, 3, pp. 1-12

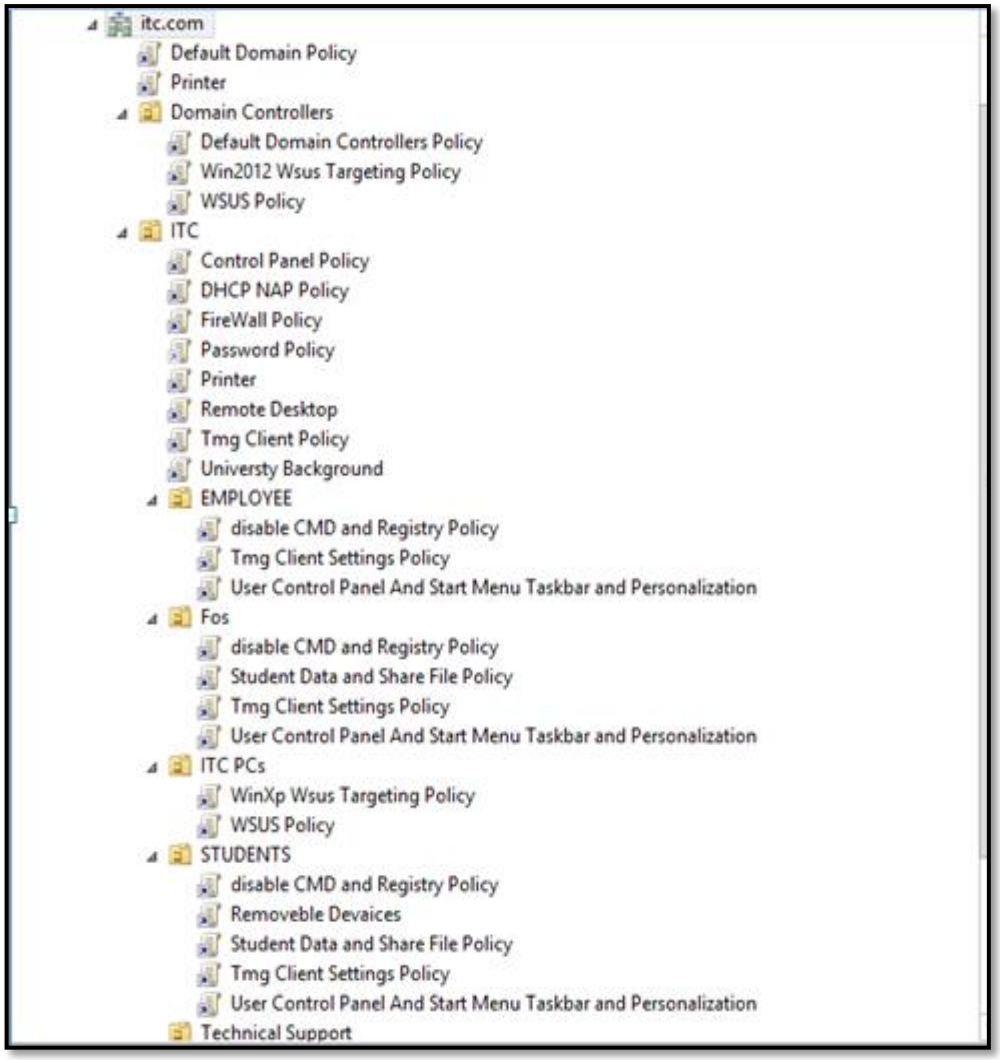
16 Gouda, M.G., and Liu ,A.X.: ‘Structured firewall design’, Computer networks, 2007, 51, (4), pp. 1106-1120

17 Harrison, J., Diogenes, Y., and Saxena, M.: ‘Microsoft Forefront Threat Management Gateway (TMG) Administrator's Companion (Pro-Administrator's Campanion)’

18 Kozierok, C.M.: ‘The TCP/IP guide: a comprehensive, illustrated Internet protocols reference’ (No Starch Press, 2005. 2005)

الملاحق

ملحق أ :- صورة توضح Group Policy التي تم تحديدها للمستخدمين والأجهزة على الشبكة.



ملحق ب :- صور توضح الصلاحيات (Policy) التي تم أعدادها على جدار الحماية .

All Firewall Policy

Search... Examples

Order	Name	Action	Protocols	From / Listener	To	Condition	Description	Policy
1	FOS	Allow	DNS Server DNS FTP Over HTTP FTP Server FTP HTTP HTTPS Server HTTPS POP3 Server POP3 ...	Internal	External	FOS Student		Array
2	Empolyee	Deny	DNS Server DNS FTP Over HTTP FTP Server FTP HTTP HTTPS Server HTTPS POP3 Server POP3 ...	Internal	External FaceBook youtube	Employees		Array
3	Technical Support	Allow	DNS Server DNS FTP Over HTTP FTP Server FTP HTTP HTTPS Server	Internal	External FaceBook youtube	Technical Sup...		Array

3	Technical Support	Allow	DNS Server DNS FTP Over HTTP FTP Server FTP HTTP HTTPS Server HTTPS POP3 Server POP3 ...	Internal	External FaceBook youtube	Technical Sup...		Array
4	Allow User to Con...	Allow	All Outbound Traffic	Internal	External	Domain Admin		Array
Last	Default rule	Deny	All Traffic	All Networks (...	All Networks (...	All Users	Predefined acces...	Array