بدائل الحلول الأمنية التي توفرها الشبكة الافتراضية الخاصة VPN
أنموذج مقترح لاستخدام بدائل سيسكو ومايكروسوفت الامنية
في مصرف الرشيد / مكتب المندوب العام /المنطقة الشمالية

أ.م. رائد عبد القادر الدباغ
قسم نظم المعلومات الادارية/كلية الادارة والاقتصاد
جامعة الموصل
raiddabagh@yahoo.com

م.م.بشرى علي زينل
قسم ادارة الاعمال /كلية العلوم الادارية والمالية/
جامعة جيهان – اربيل /اربيل - العراق
Bushra.ali@cihanuniversity.edu.iq

تاريخ التقديم:2018/5/16
تاريخ القبول:2018/5/29

المستخلص

يسعى البحث الى توفير أنموذج مقترح لتطبيق الشبكة الافتراضية الخاصة بوصفها الاداة التي يتم بواسطتها حماية المعلومات المنقولة عبر نظام المعلومات المستند على الويب، وقد تضمن تصميم البحث استخدام منهج دراسة الحالة لغرض جمع البيانات عن مجال التطبيق (مصرف الرشيد) وتم استخدام برنامج visio لغرض تصميم ورسم مخططات النماذج المقترحة المستخدمة، اذ تم الاعتماد على البيانات التي تم جمعها من المقابلات الشخصية مع مسؤولي المصرف لغرض ايجاد حلول لمشكلة البحث ، ويعد البحث من انواع البحوث التطبيقية التي تستخدم اسلوب نمذجة البيانات modulation لغرض ايجاد حلول لمشكلة البحث.

وتكمن اهمية البحث في تناولها لاحد المواضيع الحيوية في الوقت الحالي، ألا وهي كيفية جعل البيانات المنقولة عبر انظمة المعلومات تتمتع بالامان، وتوفير وسائل الحماية والامان للمعلومات المنقولة من المركز الى الاطراف وبالعكس.

ولكي يتم تحقيق اهداف البحث بناء انموذج المقترح بأستخدام الشبكة الافتراضية الخاصة من خلال استخدام نماذج لاكثر الشركات ريادةً في مجال تكنولوجيا المعلومات والتي تتمثل بـ Cisco و Microsoft، وخرج البحث بجملة من الاستنتاجات اهمها انه يمكن اعتماد أحد النماذج المقترحة لاستخدام الشبكة الافتراضية الخاصة سواء كان النموذج المقدم من قبل سيسكو او من خلال تطبيق النموذج المقدم من قبل مايكروسوفت.

وعلى ضوء الاستنتاجات أُختُتم البحث بمجموعة من المقترحات اهمها، الأخذ بنموذج مايكروسوفت للشبكة الافتراضية الخاصة نظراً لسهولة تطبيقه باستخدام البنية التحتية للمصرف اذ لايحتاج الى معدات خاصة.

المصطلحات الرئيسة للبحث/ أمن المعلومات، أمن الشبكات، البروتوكولات، البنية التحتية للشبكة، الشبكة الأفتراضية الخاصة.

مقدمة البحث

تعد الشبكة الافتراضية الخاصة من ابرز الشبكات التي يتم منخلالها حماية المعلومات المنقولة، اذ تمتاز هذه الشبكة باستخدام البنية التحتية العامة مثل الانترنيت، بالاضافة الى استخدامها بروتوكولات خاصة بالامنية، و الميدان الابرز الذي تستخدم فيه هو المصارف نظراً لحساسية المعلومات التي يتم نقلها فيها، لكونها تتعلق بمعلومات خاصة بالزبائن والاموال الخاصة بالبنوك والارصدة، وقد تم توظيف هذا النوع من الشبكات لأقتراح انموذج يتم من خلاله تطبيق نظام ادارة بيانات الزبائن المستند على الويب، اذ اعتمد البحث منهج دراسة الحالة (Case Study)، وأختير مصرف الرشيد /مكتب المندوب العام للمنطقة الشمالية مجالاً للبحث.

اذ يمكن استخدام العديد من النماذج الخاصة باستخدام الشبكة الافتراضية الخاصة والتي تسهل على المنظمات وخصوصاً المصارف استخدام المعلومات ونقلها بشكل آمن والتي من اهمها شركة سيسكو والتي تعد من الشركات الرائدة في مجال تكنولوجيا المعلومات اذ تقدم العديد من تقنيات الحماية للمعلومات ومن ضمنها الشبكة الافتراضية الخاصة، بالاضافة الى توفيرها مكونات مادية تقوم بعملية تشفير البيانات وحمايتها مثل جدران النار وغيرها، فضلا عن شركة مايكروسوفت الغنية عن التعريف والتي تقدم حلول اخرى تعتمد على البرامجيات وانظمة التشغيل والتطبيقات على الاغلب.

المحور الاول/ منهجية البحث و الدراسات ذات العلاقة

أولاً- :دراسات ذات علاقة

يتضمن هذا المبحث عرضاً موجزاً لاهم الدراسات التي تمكن الباحثان من الاطلاع عليها، والتي تناولت مواضيع ذات علاقة بموضوع البحث الحالي، مع مناقشتها وبيان مجالات الاستفادة منها، وقد ارتأى الباحثان تبويب الدراسات السابقة على أساس دراسات تتعلق بالشبكة الافتراضية الخاصة وعلى وفق مايأتي:

أ- الدراسات ذات العلاقة بالشبكة الافراضية الخاصة

1- دراسة (Jaha, 2008)

عنوان الدراسة	Selecting and Implementing Proper Virtual Private Network (VPN) Solution for Libyan Industrial Sector اختيار وتطبيق حلول الشبكة الافتراضية المناسبة للقطاع الصناعي الليبي.
نوع البحث	بحث تطبيقي
مجال التطبيق	القطاع الصناعي الليبي
اساليب جمع البيانات	تم استخدام اسلوب دراسة الحالة استخدمت فيها النماذج المنطقية المستنبطة لتحديد الحلول المناسبة له .نتيجة لهذا، تم اقتراح النوع الذي يستخدم برنامج العميل المعتمد على الشبكة خاصة افتراضية
هدف البحث	- تقديم عرض لبروتوكولات الشبكة الافتراضية المختلفة، وتحديد الحلول المختلفة للشبكة الافتراضية الخاصة، بالاضافة الى تقديم نماذج منطقية للشبكات الافتراضية الخاصة، والتي تستخدم كأساس يساعد المؤسسة في اختيار حلول الشبكة الافتراضية الخاصة المناسبة، وتقديم الحل الامثل للشبكة الافتراضية الخاصة للقطاع الصناعي في ليبيا.
اهمية البحث	- يدرس البحث بعض حلول الشبكة الافتراضية الخاصة وتطوير نماذج منطقية يمكن ان تساعد في اختيار حلول الشبكة الافتراضية الخاصة المناسبة.
منهج البحث	- تم استخدام منهج دراسة الحالة وتطبيقه على القطاع الصناعي الليبي.
اهم االنتائج	- استخدام بروتوكولات PPTP للشبكة الافتراضية الخاصة تقلل من معدلات حزم البيانات المفقودة من خلال استخدام حلول Windows Server 2003.

2- دراسة (Hudson, 2002)

عنوان الدراسة	VyperNet – A Framework for Programmable Internet-Based Virtual Private Network فايبرنت- اطار عمل للشبكات الافتراضية الخاصة المستندة على الانترنيت
نوع البحث	بحث تطبيقي
مجال التطبيق	تم تطبيق اطار عمل VyperNet لبناء وتنظيم شبكات MPLS،
اساليب جمع البيانات	استخدام اساليب تشفير معقدة تعتمد استخدام برامج خاصة لبرمجة وتشفير الشبكة الافتراضية الخاصة، تم من خلالها جمع بيانات تم الاعتماد عليها فيما بعد للوصول لنتائج البحث .
هدف البحث	- تطوير تصميم معين يعمل من خلال اطار عمل يسمح للمسؤولين عن الشبكة بفتح شبكات تبديل لوحات البروتوكولات المتعددة MPLS، ليتم بنائها وتنظيمها من خلال اطراف خارجية.
اهمية البحث	- يقدم هذا البحث (VyperNet) وهو اطار عمل يمكن من بناء وانشاء شبكات افتراضية خاصة قابلة للبرمجة.
منهج البحث	- تم استخدام منهج برمجي يعتمد على تصميم اطار عمل يستخدم التشبيك الفعال للسماح بالبناء المرن لشبكات MPLS.
اهم النتائج	- اظهرت النتائج امكانية الوصول الى الطرف الاخر (المضيف) عبر انفاق مشفرة باستخدام الشبكة الافتراضية الخاصة.

ب- ملخص عن الدراسات ذات العلاقة

1- اكدت الدراسات ذات العلاقة بالشبكة الافتراضية الخاصة على عرض لبروتوكولات الشبكة الافتراضية المختلفة، وتحديد الحلول المختلفة للشبكة الافتراضية الخاصة، وتحديد المتطلبات المؤسسية، فضلا عن تقديم نماذج منطقية للشبكات الافتراضية الخاصة، والتي تستخدم كأساس يساعد المؤسسة في اختيار حلول الشبكة الافتراضية الخاصة المناسبة، وتحديد مواضع الضعف فيما يتعلق بالتهديدات الداخلية، وتحليل مدى معرفة المستفيد النهائي، وملىء الفجوة مابين البروتوكولات الامنية وامكانية تطبيقها على ارض الواقع.

ت- مجالات الأستفادة من الدراسات ذات العلاقة

1- المساهمة في صياغة منهجية البحث من خلال الاستفادة مما قدمته الدراسات السابقة في منهجياتها وجعلها اساس للبحث الحالي.

2- اسهام الدراسات السابقة في اعطاء الباحثان فكرة وتصور شامل وكامل لما يمكن الاستفادة منه من ادوات البحث المتوافرة، ولما يمكن ان يكون غير ذي فائدة في البحث الحالي من خلال توظيف ادوات ولغات البرمجة المناسبة، والتقانات ذات العلاقة بالنظام المصمم، والتي سبق ان تم استخدام ادوات مشابهة لها في مواضيع مماثلة.

3- اسهام الدراسات السابقة في التزويد بالمعارف اللازمة والتي كانت بمثابة اساس انطلق منه الباحثان للقيام بدراسة كافة الجوانب النظرية والميدانية لمشكلة البحث وايجاد الحلول اللازمة لها من خلال ادوات البحث وتحقيق الاهداف المرجوة منه.

ثانياً: منهجية البحث

يهدف هذا المبحث الى عرض المنهجية التي اعتمدها الباحثان في توضيح الاساس الفكري للبحث وعليه تضمن هذا المبحث الفقرات الآتية:

أ- مشكلة البحث

نظرا لاهمية المعلومات في العصر الحالي كونها مورداً من الموارد المهمة التي تعتمد عليها المنظمات، كان لابد من ايجاد طريقة يتم بها حماية هذه المعلومات اثناء انتقالها من حواسيب الزبون الى حاسوب الخادم وبالعكس والمعلومات غالباً تنقل عبر الانترنيت وهي شبكة سهلة الاختراق من قبل الجميع، ومن هنا يمكن التعبير عن مشكلة البحث من خلال التساؤلات البحثية الأتية:

1- هل يمتلك مصرف الرشيد/ مكتب المندوب العام / المنطقة الشمالية بنية تحتية كافية لتحقيق النقل الآمن للمعلومات الهامة عبر الانترنيت؟
2- هل سبق للمصرف ان استخدم تقانة الشبكة الافتراضية الخاصة او اي تقانة حماية مشابهة؟
3- هل يستوفي النظام المستخدم في كل شعبة من شعب المصرف كل متطلبات الزبائن المتمثلة بالسرعة والامان والدقة وعدم الوقوع في الاخطاء البشرية؟

ب- اهمية البحث

يمكن توضيح اهمية البحث الحالية من خلال النقاط الآتية:

1- يتوقع ان يسهم البحث في لفت الانتباه الى اهمية موضوع امن المعلومات المنقولة عبر انظمة المعلومات، وحمايتها من اي تعديل او تحريف.
2- بيان مدى أهمية استخدام الشبكة الافتراضية الخاصة بوصفها من التقانات الهامة التي تساهم في حماية المعلومات المصرفية.
3- تكمن اهمية البحث في تناوله لاحد المواضيع الحيوية في الوقت الحالي، ألا وهي كيفية جعل المعلومات المنقولة عبر انظمة المعلومات تتمتع بالامان، لانه لايمكن ان يتم استخدام انظمة المعلومات الموزعة في منظمات ذات معلومات حساسة مثل المصارف بدون توفير وسائل لحماية المعلومات اثناء انتقالها عبر الويب من الحاسوب الخادم الى الحاسوب الزبون وبالعكس.

د- اهداف البحث

يسعى هذه البحث الى تحقيق الاهداف الاتية:

1- توفير انموذج مقترح لتطبيق الشبكة الافتراضية الخاصة لكل من شركتي سيسكو ومايكروسوف يتضمن كل متضمنات الشبكة المحلية وكيفية بوصفها الاداة التي يتم بواسطتها حماية المعلومات المنقولة عبر نظام المعلومات الموزع.
2 - امكانية نقل معلومات تتمتع بالموثوقية والتكاملية والتوافرية مابين المركز والفروع بشكل آمن دون الخوف من امكانية اختراقها اثناء مرورها عبر الأنترنيت، من خلال أنفاق الشبكة الأفتراضية الخاصة.

هـ- اسلوب اجراء البحث

اعتمد البحث الحالي منهج دراسة الحالة (Case Study) لكونه أحد مناهج البحث العلمي التي تتمتع بالتحليل الشامل والتفصيلي للمشكلة موضوع البحث، ويتضمن هذا المنهج اساليب عديدة لجمع المعلومات ذات العلاقة بمشكلة البحث وايجاد الحلول الناجعة لها، اذ يمكن أن يتضمن المقابلات الشخصية، والملاحظة، والاستفسار.
وعلى وفق ذلك سيتم تشخيص واقع المنظمة المبحوثة (مصرف الرشيد/ المندوب العام / المنطقة الشمالية) ومدى حاجتها لتوفير المتطلبات الأمنية اللازمة لنقل المعلومات الخاصة بزبائن المصرف عبر اطراف النظام الموزع كافة.

و- **حدود البحث** :تم تأطير البحث ضمن الحدود الزمانية والمكانية والبشرية وكما يأتي:

- الحدود الزمانية: امتدت مابين عامي (2012-2013) اعتماداً على البيانات ذات العلاقة بموضوع البحث.

- **الحدود المكانية: شملت الحدود المكانية اعتماد مصرف الرشيد / مكتب المندوب العام / المنطقة الشمالية كمجال للبحث.**
- **الحدود البشرية: اقتصرت الحدود البشرية على المقابلات الشخصية التي اجراها الباحثان مع المسؤولين في المصرف، وقسم الحاسبة الالكترونية ومتخصصي تكنولوجيا المعلومات والمبرمجين، وذوي الخبرة من العاملين في مصرف الرشيد.**

المحور الثاني/ الأطار النظري للبحث

اولاً: مفهوم الشبكة الافتراضية الخاصة

ان بيئات الاعمال الحديثة بدأت بالتغير بخطوات ثابتة منذ ظهور الانترنيت في التسعينيات، وفي الوقت الحالي اكثر من اي وقت آخر، حيث ان قادة المنظمات بدأوا يسألون انفسهم كيف يمكن الحصول على الكفاءآت من خلال جعل قوة العمل لديهم اكثر قدرة على التنقل وزيادة مجالات المبيعات وقنوات التوزيع مع الاستمرار بزيادة اقتصاديات المجال في استثمارات البنية التحتية للبيانات المتوافرة (Carmouche, 2006: 5).

يمكن ان تُطبق حلول الشبكة الافتراضية الخاصة على طبقات الشبكة المختلفة لمجموعة بروتوكولات نموذج نظام الاتصال المفتوح (OSI): مثل الطبقة الثالثة، الطبقة الثانية وربما ايضا الطبقة الاولى باستخدام بروتوكول الانترنيت عبر الوسائل الضوئية؛ اذ ان الطبقة الثانية التقليدية للشبكة الافتراضية الخاصة يتم نشرها من خلال معماريات تعاقب اطر البيانات frame relay ومعمارية نمط النقل غير المتزامن (ATM)، بينما الطبقة الثانية (المعاصرة او الحديثة) والطبقة الثالثة يتم بناؤها بالأعتماد على بروتوكول الانترنيت لشبكة العمود الفقري(BN)(Wood, 2005:2) .

واشار (Brooker, 2005: 3) الى ان اهم القضايا الاخلاقية المرتبطة بتصميم وتنفيذ الشبكات الافتراضية الخاصة تتمثل باستخدامها التشفير للحصول على الموثوقية والخصوصية؛ اذ ان استخدام التشفير يتضمن العديد من التطبيقات الاخلاقية والادبية والتي يجب اخذها بنظر الاعتبار قبل ان يتم تطوير النظام المستخدم لها.

قد اشار (Santos, 2007:12) الى ان المنظمات المختلفة تقوم بنشر الشبكات الافتراضية الخاصة من اجل التاكد من موثوقية الحزم المرسلة عبر شبكة غير محمية او عبر الانترنيت، اذ يتم تصميمها لتجنب امدادات (الاسلاك) غير الضرورية.

واشار(Garcia, 2008: 21) الى ان تقانة الشبكة الافتراضية الخاصة تقدم حلول مناسبة لتوزيع تدفق البيانات المنقولة من خلال نموذجين رئيسين هما:

- **الشبكات الافتراضية العامة (public): اذ تكون جميع تدفقات البيانات المنقولة عبر الشبكة الافتراضية الخاصة نفسها.**
- **الشبكات الافتراضية المستقلة(independent): اذ تنقل تدفقات البيانات المنقولة عبر العديد من الشبكات الافتراضية الخاصة.**

وقد تعددت مفاهيم الشبكة الافتراضية الخاصة تبعاً لانواعها والبروتوكولات المستخدمة فيها، واساليب بنائها والجدول(1) يستعرض آراء بعض الباحثين حول مفهوم الشبكة الافتراضية الخاصة.

الجدول(1)
مفهوم الشبكة الافتراضية الخاصة (VPN)

اسم الباحث، السنة: الصفحة	المفهـوم
(Nousiainen, 2010: 9)	هي شبكة مادية تربط مجموعة معينة من المواقع، والشبكة الافتراضية الخاصة عادة ما تتواجد في الطبقة الثانية، او الثالثة، والحلول من نوع خطوط الامدادات يمكن اعتبارها كشبكات افتراضية للطبقة الاولى.
(Bjornstand, 2007: 23)	وهي محاكاة لمعدات او (تسهيلات) شبكات المناطق الواسعة الخاصة، باستخدام تسهيلات بروتوكول الانترنيت.
(Lewis, 2006: 5)	تسمح الشبكة الافتراضية الخاصة بتوفير خدمات الشبكة الخاصة لمنظمة واحدة او لعدة منظمات عبر بنية تحتية عامة او مشتركة مثل شبكة الانترنيت.
(Paraskevaidis, 2006: 17)	يتم فيها محاكاة سلك أوخط (Wire) افتراضي يربط زبون الشبكة الافتراضية الخاصة مع المنزل او مع الانترانيت التعاوني، والتي يكون فيها فقط زبون الشبكة الافتراضية الخاصة وبوابة الشبكة الافتراضية الخاصة التي تربطه بمنزله، قادرين على فك تشفير البيانات المشفرة المتبادلة بينهم.
(Bless, 2006: 2)	تستفيد من البنية التحتية للاتصالات العامة من اجل الحفاظ على الخصوصية من خلال استخدام، بروتوكولات الانفاق والاجراءآت الأمنية.
(Chatziioannidis, 2004: 54)	وهي واحدة من التقانات المفيدة للمؤسسات التي يستعمل مستخدميها، و تتضمن الحواسيب المحمولة المرتبطة بهاتف نقال مع اي مضيف ضمن شبكة الانترانيت التعاونية، وتقوم بانشاء اتصالات آمنة من خلال تشفير البيانات المنقولة باستخدام بروتوكول الانفاق من نقطة الى نقطة، او بروتوكول الانفاق للطبقة الثانية.
(Wood, 2005, 3)	هي شبكات بيانات خاصة ومشتركة وتنشر عبر بنية تحتية عامة ومشتركة وتنفذ من خلال مدى واسع من التقانات، او بشكل ذاتي، او تدار من خلال مزود خدمة.
(Hudson, 2002:14)	هي شبكة خاصة تسمح للمواقع الموزعة بالارتباط ببعضها البعض من خلال شبكة واسعة النطاق (WAN) لها نفس خصائص الشبكات المحلية (LAN) المرتبطة بشكل مادي.
(Orgen, 2002: 4)	وهي اتصال الزبون الموزع على بنية تحتية مشتركة، باستخدام سياسات الشبكات الخاصة نفسها، وهذه البنية التحتية المشتركة ربما ترفع مستوى بروتوكول الانترنيت لمزود الخدمة وربما تفيد اوتستخدم شبكة الانترنيت العامة وربما لا تفيد.
(Kytola, 2002: 2)	وهي شبكة تربط الحواسيب المتواجدة عبر العالم، بشبكة افتراضية باستخدام الشبكات العامة، وسميت "بالشبكة الافتراضية " لانه يتم انشاء الروابط الخاصة بها فقط على اساس الحاجة.
(Klemetti,2001: 34)	وهي شبكة منطقية كبيرة تتكون من مجموعة من الشبكات المحلية الموزعة، ويمكن ان يتم توزيعها عبر الشبكات العامة وغير الآمنة، والتي يتم من خلالها تشفير وتوثيق البيانات المنقولة.
(Broman, 2001: 2)	وهي تسمح بنقل البيانات عبر انفاق من خلال قناة منطقية مشفرة، وهذا يسمح باستخدام البنية التحتية الشبكية الحالية، مع ضمان الخصوصية والامن.

المصدر: من اعداد الباحثان بالأعتماد على المصادر الواردة فيه.

مما سبق، يرى الباحثان ان الشبكة الافتراضية الخاصة تعد شبكة معتمدة على الانترنيت تستخدم بروتوكولات خاصة تعمل على تشفير الحزم وتغليفها لمنع اختراقها وتكوين انفاق تمر من خلالها المعلومات المهمة بحيث يتم تشفيرها عند جانب الارسال وفك تشفيرها عند جانب الاستقبال.

ثانياً: فوائد الشبكة الافتراضية الخاصة

اوضح كل من (Jaha, 2008: 1)، (Fisli, 2005: 3)، (Alchaal, 2005: 3) ان تقانة الشبكة الافتراضية الخاصة قد نشأت من حقيقة ان العديد من الشركات تمتلك العديد من التسهيلات المنتشرة عبر البلد الواحد او حول العالم، وبالاعتماد على الحلول التي يتم اختيارها فان الشركات تستفيد من الشبكة الافتراضية الخاصة من خلال الآتي:

1. تقليل الكلف: من خلال ربط الشبكات الداخلية، اذ ان الشبكات الداخلية والخارجية التي ترتبط من خلال حلول الشبكة الافتراضية الخاصة تقلل من كلف وتعقيد ادارة العديد من الشبكات، اذ تبطل الحاجة الى توظيف وتدريب اخصائيي الامن المهرة، او تحمل التكاليف التشغيلية العالية، وتنهي الشبكة الافتراضية الخاصة مشكلة تحمل الفواتير الشهرية الثابتة الخاصة بالخطوط المستأجرة، حيث ان الكلف تكون اعلى اذا كانت الخطوط قد تم شراؤها.
2. توسيع الاتصالات الجغرافية: ان الشبكة الافتراضية الخاصة تربط العاملين عن بعد بالموارد المركزية، بشكل افضل من القيام بتأسيس اتصالات موزعة مابين المركز والفروع، وهذا يسمح للشركات بمتابعة النشاط المحلي والعالمي، وربما لا يمكن الوصول الى الاتصالات العالمية بنفس مستوى استخدام الخطوط المستأجرة او التي يتم شراؤها، وحتى لو امكن استخدامها فان الكلف تكون ضخمة.
3. زيادة العائد على الاستثمار: اذ تقلل الحلول الامنية الفاعلة بشكل كبير من التهديدات، وتقلل ايضا من وقت التوقف، وخسائر الاعمال، فضلاً عن زيادة الارباح من خلال تحسين الانتاجية، وينتج التحسن في الانتاجية من القدرة على الوصول الى الموارد من اي مكان وفي اي وقت.
4. الامنية بشكل واضح: ان البيانات التي يتم ارسالها عبر الشبكة الافتراضية الخاصة تتمتع بالموثوقية، وتتطلب تخويل (Authentication) من اجل استلامها او ارسالها، فالمستخدمون يقومون بتوثيق الحزم، للتأكد من صلاحية المعلومات، ويكون تكامل البيانات في مثل هذه الحالة مضمون، والبيانات المنقولة اما ان يتم تشفيرها او ترسل بشكل غير مشفر وتمرر عبر شبكات موثوقة.
5. المرونة: ان المواقع والمستخدمين الجدد ضمن الشبكة الافتراضية الخاصة، يمكن ان يزيد من التعقيد وتستهلك الوقت، والمرونة هي شكل من اشكال توفير الكلف للمنظمة الصغيرة، ولكن مع نمو هذه المنظمة فان الاتصالات المترابطة بشكل متكامل ربما تكون مطلوبة ما بين المكاتب المختلفة، وتتجنب الشبكة الافتراضية الخاصة هذه المشكلة من خلال استخدام بنية تحتية متواجدة اصلاً.

بينما اشار (Murhammer et. al, 1999: 4) الى ان الشبكة الافتراضية الخاصة توصل المعلومات بأمان عبر الانترنيت الى المستخدمين عن بعد، والمكاتب الفرعية وشركاء الاعمال بشبكات تعاونية واسعة، وكما هو معلوم فان مزود خدمة الانترنيت يوفر امكانية الوصول بتكلفة منخفضة الى الانترنيت (من خلال الخطوط المباشرة، او ارقام الهواتف المحلية)، والتي تمكن الشركات من التخلص من ارقام الهواتف المجانية، وخطوط الامدادات الغالية الثمن، والمكالمات البعيدة المدى الحالية، وان اختيار حلول الشبكة الافتراضية الملائمة يجب ان يتم على وفق الاحتياجات مع الاخذ بنظر الاعتبار القضايا الآتية: (حاجات الأعمال، الأمان، والأداء).

ومما سبق يمكن القول ان اهم فوائد الشبكة الافتراضية الخاصة هي تقليلها للكلف، وامكانية استخدامها عبر مساحات جغرافية واسعة، وتميز المعلومات التي تنتقل من خلالها بالموثوقية، وسهولة تعديل هذه الشبكات بأضافة اطراف عديدة للاتصال، وتقليلها من وقت التوقف وخسائر الأعمال.

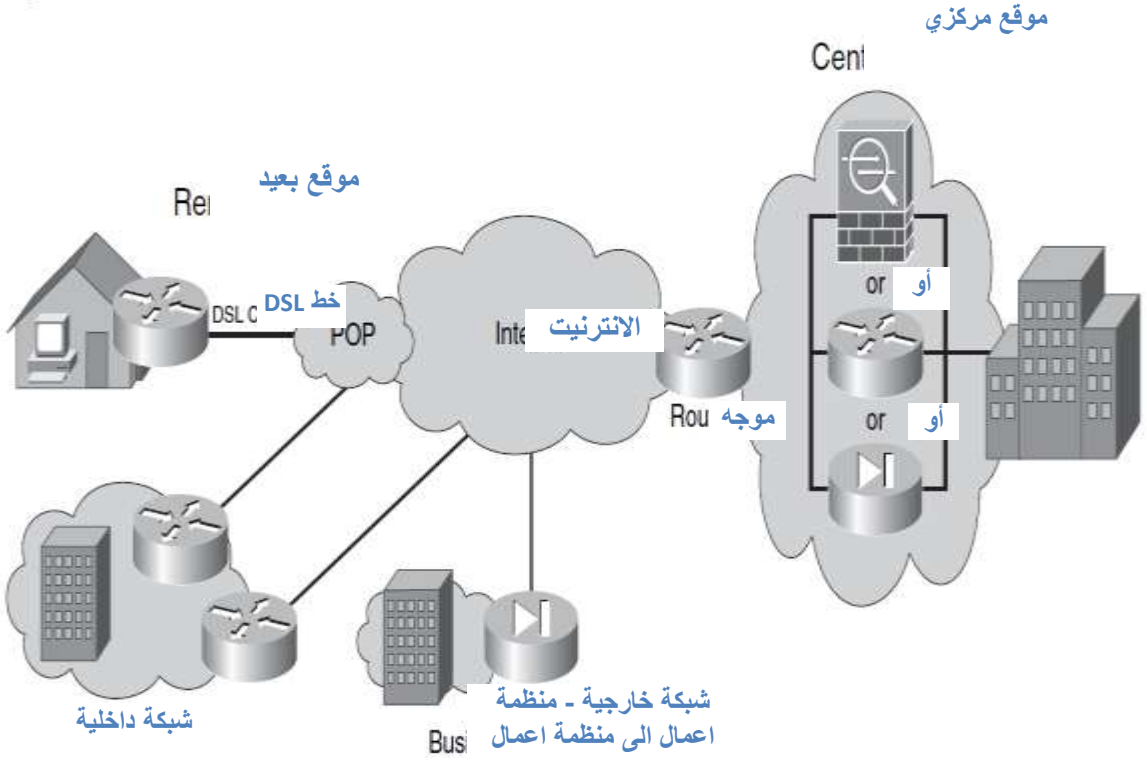
ثالثاً: انواع الشبكة الافتراضية الخاصة

تختلف انواع الشبكة الافتراضية الخاصة بحسب طبيعة الموقع الذي تطبق فيه اوالبروتوكولات المستخدمة في تطبيقها والاغراض التي يستفاد منها وبشكل عام هناك نوعان أساسيان من الشبكة الافتراضية الخاصة وكما يأتي: (Maquerry, 2008: 299)

1- الشبكة الافتراضية الخاصة نوع من - موقع - الى موقع.
2- الشبكة الافتراضية الخاصة للوصول عن بعد: ويتضمن هذا النوع نوعين من حلول الشبكة الافتراضية وهي:

- الشبكة الافتراضية الخاصة السهلة لـ Cisco.
- الشبكة الافتراضية الخاصة لبروتوكول الانترنيت الآمن (Cisco IOS): والتي تسمى أيضاً بالشبكة الافتراضية الخاصة بالويب.

ان الشبكة الافتراضية الخاصة نوع موقع- الى - موقع هي بمثابة امتداد لشبكات المناطق الواسعة الكلاسيكية، حيث تربط الشبكة الافتراضية الخاصة من موقع- الى - موقع جميع الشبكات مع بعضها البعض، على سبيل المثال يمكن ان تربط شبكة المكتب الفرعي بشبكة المكتب الرئيس للمنظمة، والشكل الآتي يظهر مثالاً للشبكة الافتراضية الخاصة نوع موقع- الى- موقع:



الشكل (1)
الشبكة الافتراضية الخاصة نوع من موقع الى موقع

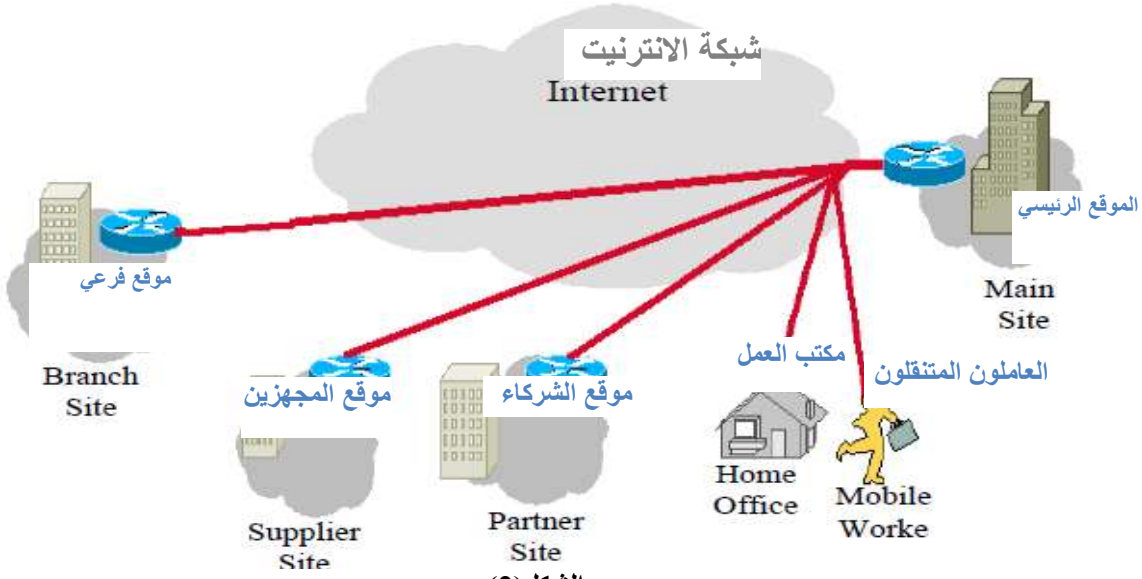
Source: Maquerry, Steven, (2008), Authorized Self-Study Guide Interconnecting: Cisco Network Devices, Part 2 (ICND2), 3rd Edition, Cisco Press, Indianapolis, USA, p.300.

في الشبكة الافتراضية الخاصة نوع موقع- الى- موقع فان خادم او مضيف برنامج زبون الشبكة الافتراضية الخاصة يمكن ان يكون من نوعCisco ، حيث ترسل وتستقبل البيانات المنقولة والخاصة ببروتوكول TCP/IP من خلال بوابة شبكة افترضية خاصة والتي يمكن ان تكون اما موجه (Router) او جدار ناري (Firewall) او مركز او مكثف (Concentrator) شبكة افتراضية خاصة من نوع Cisco.

ويمكن ان تقسم الشبكة الافتراضية الخاصة من نوع موقع- الى- موقع الى الشبكات الافتراضية الخاصة الداخلية والخارجية وكما يلي: (Jaha, 2008: 3).

- الشبكات الداخلية من موقع - الى - موقع: اذا كانت المؤسسة تملك واحداً او اكثر من المكاتب الفرعية فانها قد ترغب بربطها من خلال شبكة واحدة خاصة، من خلال تكوين الشبكة الافتراضية الخاصة الداخلية، حيث انه يعد من الحلول المنخفضة الكلفة بالمقارنة مع كلف صيانة خطوط الامدادات المتخصصة.
- الشبكات الخارجية من موقع الى موقع: عندما تستخدم المؤسسة علاقات مغلقة مع منظمات اخرى (على سبيل المثال شريك، او زبون، او مجهز)، فانها يمكن ان تبني شبكات افتراضية خارجية تربط الشبكات المحلية مع بعضها، ومن خلال ذلك فان المؤسسات الشريكة مع المنظمة يمكن ان تعمل ضمن بيئة مشتركة.

- **الشبكات الافتراضية الخاصة ضمن الشبكات الداخلية: يمكن ان تستفيد الشبكات الداخلية من تقانة الشبكة الافتراضية الخاصة من اجل تنفيذ "الوصول المسيطر عليه" (Controlled access) للشبكات الفرعية على الشبكات الخاصة، وعلى الرغم من ان الشبكات العامة لا تستخدم ضمن هذه الحالة، فان مزايا الامن (الموثوقية والتشفير) لتقانة الشبكة الافتراضية الخاصة الآمنة، ستحمي الاتصالات الداخلية الحساسة من الهجمات ضمن المنظمة.**

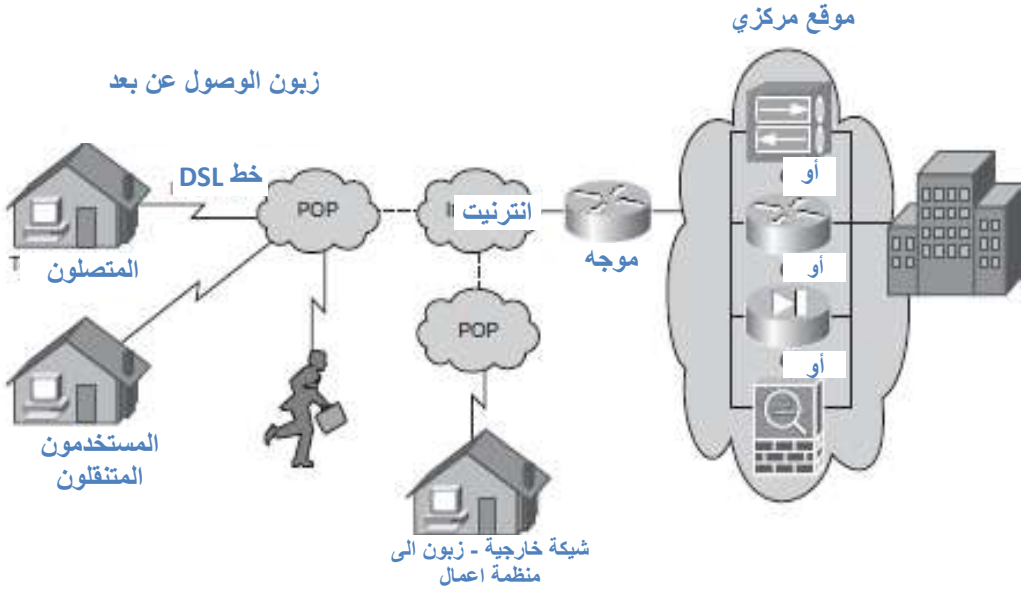


الشكل(2)

معمارية الشبكة الافتراضية الخاصة

Source: Jaha, Ahmed Abdulgader,(2008), Selecting and Implementing Proper PrivateNetwork (VPN) Solution for Libyan Industrial Sector, Master Thesis, The General Peoples Committee Secretary for Higher Education, The High Institute of Industry, Department of Electronic Engineering, Misurata, Libya, P.4.

اما الشبكة الافتراضية الخاصة من نوع الوصول عن بعد فتتضمن انشاء شبكات دوائر التحويل (Circuit Switching Netwok)، مثل خدمات الخطوط الهاتفية الاعتيادية Plain Old- Telephone Service (POTS) او (ISDN)؛ اذ ان الشبكة الافتراضية الخاصة من نوع الوصول عن بعد يمكن ان تدعم احتياجات المتصلين، والمستخدمين المتنقلين، والبيانات المنقولة عبر الشبكة الخارجية من المستهلكين الى الاعمال، وهذا النوع يقوم بربط حواسيب الخادم او المضيف المفردة بشكل يسمح بالوصول الى شبكة الشركة بشكل آمن، عبر الانترنيت والشكل يوضح نموذجاً للشبكة من نوع الوصول عن بعد (Maquerry , 2008: 299).



الشكل (3)
الشبكة الافتراضية الخاصة من نوع الوصول عن بعد

Source: Maquerry, Steven, (2008), "Authorized Self-Study Guide Interconnecting: Cisco Network Devices, Part 2 (ICND2)", 3rd Edition, Cisco Press, Indianapolis, USA, p.301.

ان الشبكة الافتراضية الخاصة يمكن ان تصنف الى نوعين آخرين، النوع الاول هو الشبكة الافتراضية المعتمدة على الزبون، والنوع الثاني الشبكة الافتراضية الخاصة المعتمدة على الويب وهي مدرجة كما يأتي: (Fisli, 2005: 13)

في بعض الاحيان فان ادوات الشبكة الافتراضية الخاصة والتي تنهي نفق الشبكة الافتراضية الخاصة، تكون عبارة عن برنامج يعمل على حاسوب شخصي - على سبيل المثال المستخدمون من المنزل- والتي تتضمن ادوات مكونات مادية معينة، تكون مكلفة بالنسبة للمستخدم، والشبكات التي تبنى بهذه الطريقة يطلق عليها (الشبكة الافتراضية الخاصة المعتمدة على الزبون).

ان الاختلاف الاساسي مابين هذين النوعين من الشبكات، هو ان الشبكة الافتراضية المعتمدة على الزبون تتطلب تحميل برنامج الزبون على كل حاسوب مضيف يرتبط عن بعد بالشبكة التعاونية، في حين يعتمد النوع الثاني منها على طبقة مآخذ التوصيل الآمنة Secure Socket Layer (SSL) والمستخدمة في المستعرضات الخاصة بالويب لذلك يطلق عليها الشبكة الافتراضية المعتمدة على الويب.

ان الشبكة الافتراضية المعتمدة على الزبون تستخدم كوسيلة لحماية اتصالات البيانات الحاصلة مابين موقع وموقع كبديل اقل تكلفة لاستخدام الشبكات الافتراضية الخاصة الموثوقة.

في حين بيّن (Jaha, 2008: 38) الى ان تقانة الشبكة الافتراضية الخاصة يمكن ان تصنف تبعاً لطريقة تنفيذها الى مايأتي:

1- الشبكة الافتراضية المعتمدة على المكونات المادية

ان الشبكات الافتراضية المعتمدة على المكونات المادية عادة ما تستخدم موجهات التشفير والتي تشفر البيانات المرسلة وتفك تشفير البيانات القادمة، حيث انها تصمم لتعمل فور ربطها (plug & play)، وهذا يجمع مابين الامنية وسهولة الاستخدام، واكبر الاضافات التي تقدمها تتضمن توفير اعلى للبيانات الشبكية لكل نظم الشبكة الافتراضية الخاصة، وهذا التوزيع الايجابي غالبا ما يترافق مع زيادة التكاليف مما يجعلها اكثر انواع حلول الشبكة الافتراضية كلفة، وهنالك نقطة سلبية اخرى تتمثل بكونها اقل مرونة من الحلول المعتمدة على البرامجيات.

2- الشبكات الافتراضية المعتمدة على البرامجيات

في الاوضاع الاعتيادية تكون الشبكات الافتراضية الخاصة المعتمدة على البرامجيات مناسبة لبيئات العمل التي تربط نهاية نقطتي اتصالات شبكة افتراضية خاصة وغير مسيطر عليها من قبل نفس المنظمة، ويمكن ان يتم استخدام سيناريو آخر في الشبكات الافتراضية المعتمدة على البرامجيات في حالة كون المنظمة تمتلك جدران نار مختلفة ضمن المنظمة نفسها، اذ انه من الطبيعي ان تقوم البرامجيات بتغيير نفسها بما يناسب بيئات التشغيل المختلفة، وتواجه هذه النظم انخفاض الاداء اكثر من المعتمدة على المكونات المادية، ولغرض تنفيد هذا النوع يتطلب وجود كادر تقانة معلومات على علم بنظم تشغيل المضيف، والتطبيق، وآلية الامان المناسبة (مثل بروتوكول بناء الانفاق من- نقطة - الى نقطة، بروتوكول الانترنيت الآمن وغيرها).

اما(Roman et.al, 2005: 185-192) فقد اشار الى ان الشبكة الافتراضية الخاصة يمكن تصنيفها,وفقاً لمعمارياتها الى ثلاثة اصناف وكما يلي:

1- الشبكة الافتراضية الخاصة الآمنة

تمر حزم البيانات من خلال الشبكة باستخدام حماية مشفرة، اذ ان الشبكة الافتراضية الخاصة تكون ضمن المنظمة او الشركة، ويقوم طاقم الموظفين بادارة سياسة الامن الداخلي، والتقنيات المستخدمة في هذا النوع من الشبكة الافتراضية الخاصة هي IPsec وSSL.

2-الشبكة الافتراضية الخاصة الموثوقة

تمر حزم البيانات من خلال الشبكة عبر مسارات محمية ومعرَّفة بشكل مسبق، ومن خلال هذه المعمارية فان مهام الادارة تعتمد على مزود الخدمة، وهنالك العديد من التقانات التي تستخدم لتوفير هذا النوع من خدمات الشبكة الافتراضية الخاصة،منها (MPLS و ATM Circuits وFrame Relay).

3- الشبكة الافتراضية الخاصة الهجينة

هذه المعمارية تجمع مابين الخصائص الخاصة بالشبكة الافتراضية الخاصة الآمنة، والشبكة الافتراضية الخاصة الموثوقة.

خامساً: بروتوكولات الشبكة الافتراضية الخاصة

تم تطوير العديد من البروتوكولات الأمنية خلال السنوات القليلة الماضية، نذكر منها:

1. بروتوكول الانترنيت الآمن IPsec

يبدأ تاريخ بروتوكول الانترنيت الآمن في عام 1995 عندما تم تحديد مواصفات المسودة الاولى لبروتوكول الانترنيت، وفي نهاية عام 1998 تم طرح النسخة الرسمية الاولى منه، ليجعل النسخة السابقة تقترب من الزوال، والتي يطلق عليه بروتوكول الانترنيت الآمن الاصدار الاول، وبعد سبع سنوات من ذلك في العام 2005، ظهر الاصدار الثاني لبروتوكول الانترنيت الآمن وتم اجراء العديد من التعديلات على هذا البروتوكول لتسهيله وتعديله ليناسب حقول الممارسة، وقد تطور حتى الوصول في الوقت الحالي الى بروتوكول الانترنيت الاصدار السادس (IPv6) (Barylski, 2010: 30).

ان بروتوكول الأنترنيت الآمن وهو معيار لحماية اتصالات بروتوكول الانترنيت من خلال تشفير او توثيق كل حزم بروتوكول الانترنيت، اذ انه يوفر الامان لطبقة الشبكة، ويمكن استخدامه لبناء الشبكات الافتراضية الخاصة والذي يعد من أكثر استخداماته شيوعا(Yang, 2006: 1).

يقوم بروتوكول الانترنيت الآمن بتغليف البيانات من خلال رأس (Header)، عبر نفق يربط مابين مضيفين، او بوابتين امنيتين، او مضيف وبوابة أمنية و غالباً مايكون موجه او جدار ناري، اذ ان المرونة المتوافرة في النقاط النهائية للاتصال تعني ان هذا البروتوكول هو الاختيار الشائع الاستخدام لانشاء انفاق الشبكة الافتراضية الخاصة الديناميكية والآمنة (Hudson, 2002: 18).

ان وثائق بروتوكول الانترنيت الآمن المقدمة من قبل IETF تهتم بثلاث مجالات رئيسة ذات علاقة بأمن بروتوكول الانترنيت (IP Securing) وهي خوارزميات التشفير، وخوارزميات الموثوقية (التخويل) وادارة المفاتيح، ان الفائدة الرئيسة المستحصل عليها من بروتوكول الانترنيت الآمن، تتمثل بزيادة توافقها مع منتجات IPsec الاخرى والتوافق يعد حاجة ضرورية في عالم اليوم، اذ يتوقع من العديد من المنتجات والخدمات ان تتصل مع بعضها البعض بشكل آمن (Scott et.al, 1999: 28).

بينما اشار (Faineza & Amso, 2008: 15) الى ان بروتوكول الانترنيت الآمن يتكون من العديد من المكونات تتمثل بالآتي:

1- الروابط الامنية Security Association (SA).
2- قاعدة بيانات السياسات الأمنية Security Policy Database (SDB).
3- بروتوكولين خاصين بالأمنية وهما Authentication Header (AH) , Encapsulated Security Payload (ESP).
4- يمتلك هذا البروتوكول صيغتين؛ صيغة النقل وصيغة بناء الانفاق.
5-خوارزميات التشفير التي تستخدم لتوفير الموثوقية (التخويل)، والتشفير.
6-ادارة المفاتيح والتي تتم من خلال بروتوكول استبدال مفتاح الانترنيت، او تبديل المفاتيح اليدوي.

بينما اوضح (Mohan, 2005: 5) بان بروتوكول الانترنيت الآمن قد تم تطويره لتوفير الامان ضد الهجمات المتواجدة اصلاً في بروتوكول الانترنيت من خلال تعريف آلية أمنية مرنة لارسال البيانات عبر وسط غير آمن، ويمتلك بروتوكول الانترنيت الآمن القدرة على توفير مدى غير محدود من الخدمات الأمنية المعرفة بواسطة سياسة أمنية، حيث تعرف السياسة الأمنية خدمات أمنية محددة لكل حزمة وذلك حسب خصائص هذه الحزمة (مثل عناوين المصدر، وعناوين الارسال).

وتعد صيغ الأنفاق وصيغ النقل من الصيغ الأكثر أستخداماً في هذا البروتوكول والتي يمكن توضيحها من خلال الآتي: (Kilecrease, 2009 :9).

- صيغة الانفاق: تقوم بتغليف حزم IP كاملة وتحويلها الى حزمة جديدة وارسال الحزمة الجديدة الى نقطتها النهائية، وهذا يساهم في حماية العناوين الخاصة بكل من المرسل والمستقبل، وكل البيانات الوسطية (Meta Data) او المعلومات الوسطية، التي تعرف بيانات اخرى موجودة في الحزمة، ويمكن ان تمثل حقائق او معطيات، او مجموعة من البيانات.
- صيغة النقل: في صيغة النقل يتم تشفير كمية البيانات وتغليفها، وهذا يقلل بشكل واضح من النفقات، ولكن المهاجمين يمكن ان يقوموا بسهولة بقراءة البيانات الوسطية واكتشاف من يقوم بالاتصال، على الرغم من ان البيانات قد تم تشفيرها وحمايتها.

<u>2- بروتوكول الانفاق من نقطة - الى – نقطة (PPTP)</u>

ان بروتوكول الانفاق من نقطة- الى- نقطة، يستخدم اسم مستخدم وكلمة مرور من اجل توفير اتصالات موثوقة (مخولة)، ومشفرة مابين حاسوب زبون وبوابة، او ما بين بوابتين، حيث يستخدم رابط بروتوكول السيطرة على النقل(TCP)، من اجل الحفاظ على النفق، وبروتوكول تغليف التوجيه العام General Routing Encapsulation (GRE) من اجل تغليف اطارات PPP بالنسبة للبيانات المنقولة عبر الانفاق، اذ ان احمال البيانات الاساسية (Payloads) لاطارات PPP المغلفة يمكن تشفيرها او ضغطها من خلال اسلوب مايكروسوفت للتشفير من نقطة الى نقطة Microsoft's - Point to Point Encryption (MPPM) (Wong, 2003: 43).

يعد هذا البروتوكول امتداداً لمعيار بروتوكول من نقطة- الى- نقطة (PPP)، اذ ان خدمات الانفاق التي يوفرها بروتوكول PPTP تحاول ان تتفوق على طبقة بروتوكول الانترنيت، بينما يخضع بروتوكول PPP التقليدي لبروتوكول الانترنيت، وبشكل مثالي فان بروتوكول PPP ملائم لاغراض التعديل والتحديث، لان وظيفته الاساسية تقوم بتقليد سلوك ما تحتاجه الشبكة الافتراضية الخاصة والذي يتمثل بنفق من نقطة- الى- نقطة، وكل ما نحتاجه بهذه الحالة هو الامان، اما PPTP يكون اقرب الى اتصالات آمنة من مضيف - الى - مضيف اكثر من كونه اقرب الى شبكة محلية - الى - شبكة محلية وعلى الرغم من انه يمكن توجيه مرور البيانات المنقولة (Traffic) عبر قناة PPTP، فان حلول بروتوكول الانترنيت الآمن تكون مناسبة بشكل افضل لهذا النوع من التطبيقات (Scott et.al, 1999: 31) .

أما عن أهم المزايا والعيوب لبروتوكول الأنفاق من نقطة - الى- نقطة (PPTP) فيمكن ذكرها بالآتي: (Akbar & Shahzad, 2009: 21)

أ- المزايا:

- يقوم بتقليل النفقات.
- لاتوجد حاجة لاستخدام البنية التحتية للمفتاح العام.(Public Key Infrastructure (PKI.
- يقوم بدعم العديد من روابط بروتوكول الانفاق من نقطة - الى - نقطة في خادم الشبكة الافتراضية الخاصة.
- تقوم بالدعم الكامل لترجمة عناوين الشبكة (Network Address Translation (NAT.

ب- العيوب:

- يتضمن هذا البروتوكول مشاكل أمنية ومشاكل لجدران النار.
- يستطيع البروتوكول فقط دعم استخدام نفق واحد في كل مرة من قبل احد المستخدمين.
- لا يزود بتخويلات (موثوقية) اضافية.
- السيطرة على الوصول لبروتوكول الانفاق من نقطة - الى - نقطة مبني على فلترة وتصفية الحزم.

3- بروتوكول الانفاق للطبقة الثانية Layer 2 Tunneling Protocol (L2TP)

ان هذا البروتوكول يغلف اطارات PPP ليتم ارسالها عبر مدى واسع من الاتصالات، مثل شبكات IP و Frame relay و ATM، وعندما يبنى لاستخدام بروتوكول الانترنيت كوسط للنقل فان هذا البروتوكول يستخدم لبناء الانفاق عبر الانترنيت (Wong, 2003: 43).

ويزود هذا البروتوكول بتقانة بناء روابط انفاق من نقطة - الى- نقطة، والتي بدلاً من ان يتم انهاؤها عند اقرب بروتوكول مكتب بريد(POP) متواجد في اقرب مزود خدمة انترنيت فانه يتم توسيعه ليصل الى ابعد بوابة وصول للانترانيت التعاونية، ويتم انشاء الانفاق اما من خلال المضيف البعيد، اومن خلال مزود خدمة الانترنيت لبوابة الوصول(Murhammer et.al, 1999: 23) .

4- بروتوكول من نقطة- الى- نقطة Point- To- Point Protocol PPP

ان بروتوكول من نقطة - الى - نقطة (PPP) حقيقة ليس بروتوكول تشفير وانما هو بروتوكول تغليف، حيث انه لايحتاج الى انهاء الاطارات الحالية برموز رأسية خاصة او نهايات خاصة والتي عادة مايتم ازالتها في جانب الاستقبال، وبدلاً من ذلك فانه يسمح بنقل بيانات بروتوكول TCP/IP عبر وسط تمَ تطويره لنقل البيانات الصوتية الهاتفية، ويستخدم هذا البروتوكول لتغليف الرسائل ونقلها عبر خطوط تسلسلية، لذلك فانه يسمح لبروتوكول TCP/IP وغيره من البروتوكولات ان يتم نقله عبر خطوط الاتصالات، يستخدم بروتوكول PPP لانشاء روابط الاتصالات مابين الموجهات، من المستخدم الى الموجه، ومن الموجه الى الموجه، وكذلك يوظف لانشاء روابط الانترنيت مابين الحواسيب ونقطة التواجد على الانترنيت Point Of Presence (POP) والتي عادة ماتكون مجموعة من المودمات وخوادم الوصول في موقع مزود خدمة انترنيت معين، ان المستخدم يطلب نقطة التواجد POP عبر خطوط الاتصالات ويتم تبادل الاتصال عبر بروتوكول PPP (Harris, 2008: 611).

ويتم تصميم بروتوكول PPP لارسال البيانات من خلال خطوط الطلب الهاتفي، او من خلال روابط متخصصة من نقطة - الى - نقطة، وبالنسبة لبروتوكول الانترنيت فان PPP يقوم بتغليف الحزم من خلال اطارات PPP وبعد ذلك تنقل حزم PPP المغلفة عبر رابط من نقطة- الى- نقطة، وبذلك عُرف هذا البروتوكول بأنه البروتوكول الذي ينشيء الاتصالات ما بين الزبون البعيد وشبكة المنظمة من خلال خادم الوصول عن بعد Remote Access Server (RAS) (Jaha, 2008: 10)، والشكل(9) يوضح معمارية بروتوكول نقطة- الى- نقطة (PPP).

الشكل (4)
معمارية بروتوكول نقطة-الى- نقطة PPP

Source: Jaha, Ahmed Abdulgader, (2008), Selecting and Implementing Proper Private Network (VPN) Solution for Libyan Industrial Sector, Master Thesis, The General Peoples Committee Secretary for Higher Education, The High Institute of Industry, Department of Electronic Engineering, Misurata, Libya, P.10.

ويستخدم بروتوكول PPP لنقل البيانات عبر روابط من نقطة - الى - نقطة بشكل متعدد البروتوكولات، اذ يوفر PPP طريقة لتغليف البيانات مع بروتوكولات السيطرة على الرابط (LCP) Link- Control Protocol، لانشاء اتصالات طبقة ربط البيانات، مع بناء وتدقيق مجموعة من بروتوكولات السيطرة على الشبكة Network Control Protocol (NCP) لبناء وانشاء بروتوكولات طبقة الشبكة المختلفة (Paraskividis, 2006: 28).

ومما سبق يستخلص الباحثان ان الشبكات الافتراضية الخاصة تستخدم العديد من البروتوكولات، كل منها يتميز بمميزات خاصة به، فمثلاً بروتوكول الانترنيت الآمن، تم تطويره لتوفير الامان ضد الهجمات المتواجدة اصلاً في بروتوكول الانترنيت، اما بروتوكول PPP فهو بروتوكول تغليف اذ يقوم بتغليف الحزم من خلال اطارات PPP وبعد ذلك تنقل حزم PPP المغلفة عبر رابط من نقطة- الى- نقطة، في حين ان بروتوكول L2TP يستخدم لبناء الانفاق عبر الانترنيت.

المحور الثالث الجانب العملي/ بدائل الحلول الامنية التي توفرها الشبكة الافتراضية الخاصة

اولاً : وصف المنظمة المبحوثة

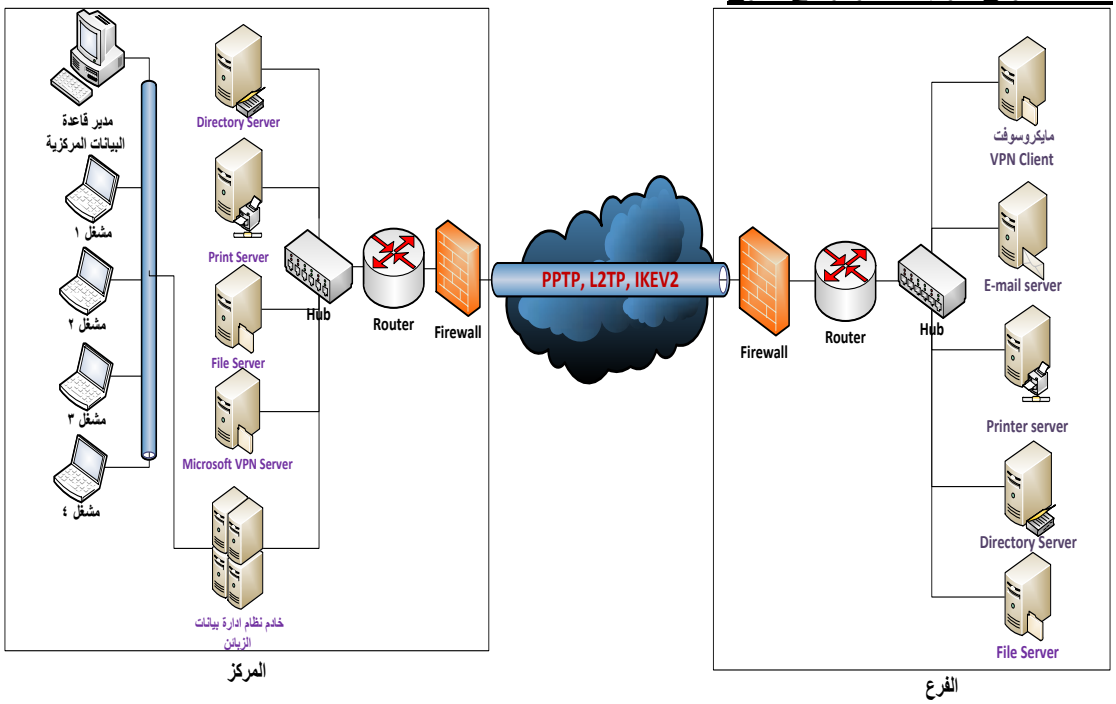
تأسّس مصرف الرشيد (المنظمة المبحوثة) في عام 1988، ويضم المصرف (163) فرعاً و(27) مكتباً إداريا والإدارة العامة للمصرف تتشكل من (13) قسماً و(56) شعبة وفي كل محافظة يضم مصرف الرشيد عدداً من الفروع ففي محافظة نينوى يضم المصرف (8) فروع، وهي الموصل /3، خالد بن الوليد، الدواسة، سنجار، حي الزهور، أبي تمام، الجزيرة، مخمور، وقد حقق مصرف الرشيد نمو في مختلف أوجه العمل ، ويحتوي كل فرع من فروع المصرف يحتوي على مجموعة من الشعب الادارية والتي تمثل المستويات الادراية الدنيا ، اما عن المتطلبات المادية التي يمتلكها المصرف قيد البحث، فالمصرف يمتلك مجموعة من الحواسيب في كل شعبة من شعبه مع وجود حاسوب واحد فقط مرتبط بالانترنت ضمن كل شعبة، فضلا عن العديد من المكونات المادية المتمثلة بالطابعات الاعتيادية والنقطية، كما تم ملاحظة انه لا ترتبط شعب المصرف مع بعضها البعض عن طريق شبكة داخلية، اذ ان كل شعبة من شعب المصرف تمتلك برامجيات خاصة بها تعمل بشكل مستقل عن شعب المصرف الاخرى، كما يفتقر المصرف ايضاً الى وجود الشبكات ومن ثم فأن كل حاسوب في المصرف يعمل بشكل مستقل اما الهيكل التنظيمي فهو نفسه في جميع المصارف او الفروع ولكن بدون وجود ربط في العمل بين كل منها وهذا ما يؤدي الى الهدر في الوقت والجهد والكلفة.

ان كل شعبة من شعب المصرف تمتلك خطي عمل احدهما يدوي والاخر الكتروني، وكل شعبة تمتلك برنامج خاص بها مكتوب بلغة Foxpro Under DOS والقسم الاخر مكتوب بلغة Fox plus، بأستثناء التوقيفات التقاعدية تكون مكتوبة بلغة Visual FoxPro Under DOS وهذا البرنامج خاص بأعداد خلاصة خدمة للموظفين من أجل التسريح، يعد الحاسوب خط عمل ثانوي بالنسبة للمصرف، على الرغم من وجود قسم خاص بالحاسوب، الا ان عملهم يقتصر على تقديم الدعم الفني للحواسيب ضمن المصرف اذ يتم استخدام الحواسيب لحفظ العمل بعد ان يتم توثيقه ورقياً، وان الزبون لا يتعامل بشكل مباشر مع الحاسوب في انجاز عملياته المصرفية ويكون تعامله مع الموظف الذي يتعامل مع النظام ويقدم له المعلومات المطلوبة.

ومن خلال البحث سيتم تزويد المصرف بحلول وبدائل امنية تحمي المعلومات الزبائن اثناء نقلها نظراً لكون النظام موضوع على شبكة عامة مثل الانترنيت، وافضل طريقة مقترحة لحماية المعلومات اثناء نقلها تتمثل بالشبكة الافتراضية الخاصة، نظراً لكونها شبكة تعمل على تشفير المعلومات قبل الارسال بواسطة بروتوكولات خاصة للاغراض الامنية، ويتم نقل المعلومات عبر انفاق شديدة الحماية غير قابلة للأختراق، بحيث تصبح المعلومات المشفرة غير مفهومة من قبل المخترقين ومن ثم يتم فك التشفير في جانب الاستقبال بحيث تصل المعلومات المطلوبة بكل شفافية الى الجانب الآخر، وهناك العديد من حلول الشبكة الأفتراضية واشهرها الحلول المقدمة من قبل شركة سيسكو Cisco والحلول المقدمة من قبل شركة مايكروسوفت Microsoft، وسنعرض كلاً من البديلين في الفقرات القادمة.

1- البدائل الأمنية لمايكروسوفت من خلال الشبكة الافتراضية الخاصة

الحالة الاولى: ارتباط المركز مع الفرع



الشكل (5) انموذج مقترح لربط فروع المصرف مع المركز باستخدام حلول مايكروسوفت

المصدر : من اعداد الباحثان بتصرف استناداً الى ماورد في:

Thomas, Orin 2011, Windows Server 2008 R2 Secrets, John Willey & Sons, Inc. , USA, P. 468

(الموقع الرسمي http://technet.microsoft.com/en-us/library/cc958037.aspx لمايكروسوفت)

يتضح من خلال الشكل (5) ارتباط المركز بفرع من الفروع المنتشرة في العراق، اذ يرتبط المركز عادة داخلياً من خلال شبكة محلية تربط مجموعة من الخوادم، منها خادم النظام المقترح لادارة بيانات الزبائن، خادم الدليل Directory Server، خادم طابعة الشبكة، خادم الملفات، خادم البريد الالكتروني، فضلا عن خادم مايكروسوفت للشبكة الافتراضية الخاصة، والذي يرتبط بدوره بحاسوب المدير الذي يوجد في المركز والذي يملك كافة الصلاحيات للوصول الى بيانات الزبائن التي يحتاجها في الفروع، فاذا اراد احد الفروع معلومات عن زبون معين يوجد في الفرع الخاص به سيتم ذلك بشكل آمن من خلال الشبكة الافتراضية الخاصة وبروتوكولاتها، ولابد من وجود موجه وجدار ناري في المركز مرتبطين بالشبكة المحلية في المركز لتسهيل عملية نقل البيانات وزيادة الامان اثناء النقل عبر الانترنيت، ومن خلال نفق الشبكة الافتراضية الآمن.

اما بالنسبة للفرع الذي يتصل بالمركز، فتربطه ايضاً شبكة متكونة من خادم مايكروسوفت للشبكة الافتراضية الخاصة والذي يصبح حاسوب زبون في حالة الأرتباط مع المركز وطلب معلومات زبون معين، وخادم الملفات، وخادم طابعة الشبكة، وخادم الدليل Directory، وخادم البريد الألكتروني، وترتبط كل من هذه الخوادم مع بعضها عن طريق شبكة محلية توجد في الفرع، والتي ترتبط بدورها عن طريق موجه وجدار ناري بنفق الشبكة الافتراضية الخاصة الذي ينقل المعلومات المطلوبة من قبل حواسيب مدير الفرع، والمشغلين في الفرع، فمثلاً قد يطلب مدير الفرع معلومات عن اعداد الحسابات في الفرع، فيتصل بقاعدة البيانات المتواجدة بالمركز عن طريق زبون الشبكة الافتراضية الخاصة، فسيتم تشفير طلبه عبر بروتوكولات الشبكة الافتراضية ليصنع نفق بالمعلومات المشفرة الى المركز فتدخل المعلومات عبر الجدار الناري والموجه، لينقل عبر الشبكة المحلية الموجودة في المركز ثم يصل الى خادم الشبكة الافتراضية الخاصة الذي يفك تشفير المعلومات المطلوبة من قبل الفرع، ليأخذ المعلومات المطلوبة من قبل الفرع من خادم نظام ادارة بيانات الزبائن بحسب البيانات التي يمتلك الفرع صلاحية الوصول اليها، وتعاد النتيجة بعد ذلك عبر الشبكة المحلية للمركز، لتنتقل عبر نفق الشبكة الافتراضية الخاصة الذي بدوره يشفر المعلومات المنقولة عبر الانترنيت ليصل للجدار الناري المتواجد في الفرع، والمتصل بزبون الشبكة الافتراضية الخاصة الطالب للمعلومات ليرسلها بعد ذلك الى مدير الفرع والمشغلين العاملين في الفرع.

اما الاختيار ما بين برتوكولات الانفاق المختلفة المستخدمة في ويندوز بضمنها نسخة Windows 2008 فانه يتم بناءاً على احتياجات المؤسسة وابرز انواع البروتوكولات المستخدمة لهذا الغرض برتوكول PPTP و L2TP.

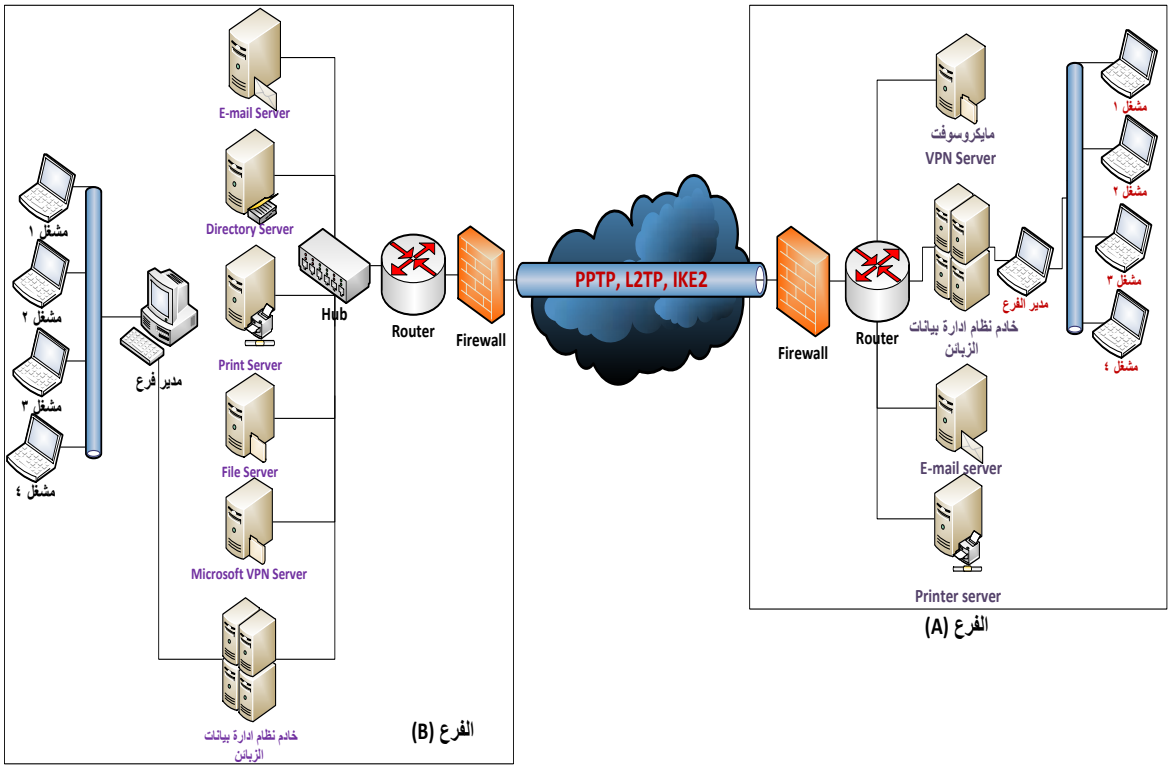
الجدول (2) المقارنة بين برتوكولات النقل PPTP وL2TP

معيار المقارنة	PPTP	L2TP
نوع نظام تشغيل حاسوب الزبون	تدعم الحواسيب التي تستخدم انظمة التشغيل، ويندوزXP، ويندوزسيرفر2003، ويندوزNT ، ويندوز مليينيوم.	تدعم انظمة حواسيب الزبون التي تعمل بانظمة التشغيل، ويندوز 2000، ويندوزXP وويندوز سيرفر 2003.
الأمن	يوفر موثوقية البيانات، اي ان البيانات التي يتم التقاطها لايمكن تفسير معناها بدون مفتاح التشفير الاصلي. كما انها لاتوفر التكاملية، اي البيانات لم يتم تعديلها اثناء النقل، او التأكد من تخويل أصل البيانات (التأكد من ان البيانات قد ارسلت من قبل المستخدم المخول).	توفر اعلى درجات الامان من خلال توفير موثوقية البيانات وتكاملية البيانات، والتحقق من أصل البيانات.
الاداء	يدعم خادم الشبكة الافتراضية الخاصة روابط برتوكولPPTP اكثر من روابط L2TP/IPSec.	بسبب ان التشفير باستخدام برتوكول يتطلب قوة معالجة كبيرة، فان خادم الشبكة الافتراضية الخاصة يدعم عمل روابط L2TP بشكل اقل، ولدعم روابط L2TP فانه يتطلب زيادة قوة المعالجة لوحدة المعالجة المركزية.

المصدر: الجدول من اعداد الباحثان بالاعتماد على المعلومات الواردة في الموقع الرسمي لمايكروسوفت
http://www.windowsecurity.com/articles/vpn-options.html

الحالة الثانية: ارتباط فرع مع فرع من خلال الشبكة الافتراضية الخاصة

يمكن ان يتم استخدام اسلوب من موقع الى موقع في حالة ارتباط فرع مع فرع من خلال حلول ويندوز الامنية باستخدام الشبكة الافتراضية الخاصة، ولمصرف الرشيد العديد من الفروع المتواجدة في كافة انحاء العراق ففي الانبار مثلا تتواجد فروع الرمادي، القائم، هيت ، ناحية العامرية، المجمع الكمركي، راوة، الكرمة، فرع الرحمن، جامعة الانبار، الشركة العامة لصناعة الحراريات، ولغرض اتصال اي فرع من الفروع لابد من توفير آلية معينة تظهر من خلال الشكل(6).



الشكل(6) انموذج مقترح لربط فروع المصرف مع بعضها بأستخدام حلول مايكروسوفت

المصدر : من اعداد الباحثان بتصرف استناداً الى ماورد في:

Thomas, Orin, 2011, Windows Server 2008 R2 Secrets, John Willey & Sons, Inc. , USA, P. 468

http://technet.microsoft.com/en-us/library/cc958037.aspx (الموقع الرسمي لمايكروسوفت)

اذ يظهر الشكل انه لابد من وجود المكونات الاساسية الآتية في كل فرع:

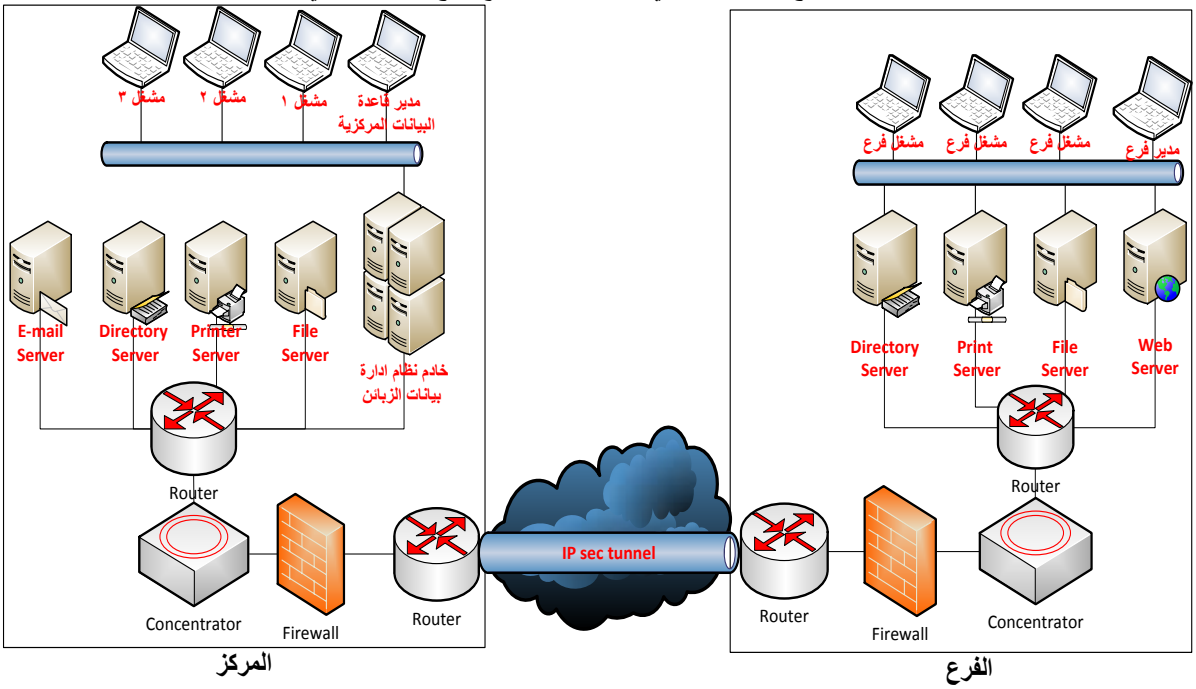
- جدار ناري و يمثل الوسيلة الدفاعية الاولى لحماية النظام ومعلومات الفرع.
- موجه و يكون ضرورياً لربط الشبكة وتوجيه حزم البيانات الى وجهتها النهائية.
- شبكة محلية تربط حواسيب الفرع كافة، بضمنها الحواسيب الخاصة بشعب المصرف كافة، فضلا عن الارتباط بحاسوب مدير الفرع والمشغلين العاملين في الفرع، اذ ان لكل منهم صلاحيات معينة للوصول لمعلومات زبائن المصرف والمعطاة لهم من المدير في المركز.

- تحتوي الشبكة المحلية على مجموعة من الخوادم كما اسلفنا سابقاً تتضمن خادم البريد الالكتروني، خادم الملفات، خادم طابعة الشبكة، خادم الدليل Directory وغيرها، واهم انواع هذه الخوادم يتمثل بخادم الشبكة الافتراضية الخاصة الذي يمكن الحصول عليه من خلال ويندوز بأستخدام ويندوز سيرفر او ويندوز 7 او اي اصدار اخر حسب نوع البرتوكول واستخدامه، ففي حالة طلب فرع معلومات من فرع آخر سيصبح هذا الحاسوب الذي يحتوي نظام التشغيل ويندوز حاسوب زبون فيطلب المعلومات من خادم الشبكة الافتراضية الخاصة المتواجد في الفرع الآخر.
- اهم مكونات الشبكة المتواجدة في الفرع تتضمن خادم نظام ادارة بيانات الزبائن، ويعد السبب الاساسي لاستخدام الشبكة الافتراضية الخاصة مابين الفروع، فليس من الممكن ان يتم استخدام نظام مستند على الويب ويستخدم الانترنيت كقاعدة اساسية في مصرف ضخم مثل مصرف الرشيد يحتوي بيانات حساسة خاصة بالزبائن من دون توفير الحماية الكافية لها، وتوفرها انفاق الشبكة الافتراضية.

2- البدائل الامنية لسيسكو من خلال الشبكة الافتراضية الخاصة

الحالة الاولى: من المركز الى الفرع

توفر سيسكو كأحدى الشركات الرائدة في مجال صناعة المكونات المادية والبرمجية للشبكات العديد من الحلول التي يمكن من خلالها حماية المعلومات اثناء نقلها عبر الشبكات العامة وخاصة الانترنيت، فقد توفر حلول برامجية باستخدام برامجيات معينة تستخدم اسلوب الخادم الزبون، او قد تستعيض عن ذلك باستخدام المكونات المادية كجدارن نار الشبكة الافتراضية الخاصة، او موزعات الشبكة الافتراضية الخاصة او بوابات الشبكة الافتراضية الخاصة، وسنأخذ احد النماذج المعتمدة من قبل سيسكو بوصفه مثالاً على ارتباط المركز الذي سنفترض وجود خادم نظام ادارة بيانات الزبائن فيه ومابين احد فروع المصرف المنتشرة في العراق من خلال اسلوب الوصول عن بعد، وارتباط فرع معين يوجد في محافظة معينة مع فرع اخر يوجد في المحافظة نفسها.



الشكل (7) انموذج مقترح لربط فروع المصرف مع المركز باستخدام حلول سيسكو

المصدر: الانموذج من اعداد الباحثان بتصرف استناداً الى:

Chamouche, James Henrey, 2006, IPsec Virtual Private Network Fundementals, Cisco Press, P.156.

نلاحظ من خلال الشكل (7) ان المركز يرتبط عادة من خلال شبكة محلية LAN تربط كافة حواسيب المصرف بمجموعة من الخوادم، منها خادم الايميل، خادم الملفات، خادم طابعة الشبكة، خادم الدليل Directory واخيراً خادم نظام ادارة بيانات الزبائن الذي يحوي بيانات عن زبائن كافة الفروع ومعلوماتهم الشخصية والمصرفية والخاصة، ويرتبط هذا الخادم عادة داخل المركز مع مجموعة من حواسيب الزبون التي يسمح من خلالها لعدد من المشغلين بالتعامل مع النظام حسب الصلاحيات المعطاة لهم من قبل مدير قاعدة البيانات المركزية، وكأي شبكة محلية تحتوي على خوادم لابد من وجود موجه يرتبط بها ويوجه حزم البيانات المنتقلة عبر الشبكة المحلية، والذي يرتبط عادة بمكثف شبكة افتراضية خاصة من نوع سيسكو والذي يرتبط بدوره بجدار ناري ومن ثم موجه من نوع سيسكو مبرمج بأسلوب معين يسمح بتشكيل انفاق الشبكة الافتراضية الخاصة والذي يربط المركز بالنفق المشفر الذي يصنعه بروتوكول الشبكة الافتراضية الخاصة، ويكون هنا من نوع IPsec باستخدام معدات سيسكو للشبكة الافتراضية الخاصة وسنركز هنا على نوعين من المعدات وهما زبون الشبكة الافتراضية الخاصة والمكثفات وكما يلي:

- زبون الشبكة الافتراضية الخاصة يمكن ان يكون مستند على المكونات المادية، او المكونات البرمجية، تقدم سيسكو موجه الشبكة الافتراضية الخاصة 827 او زبون الشبكة الافتراضية الخاصة المستند على المكونات المادية 3002 المتناسب مع حلول الشبكات الافتراضية الخاصة للوصول عن بعد ، اذ ان زبون الشبكة الافتراضية الخاصة المستند على البرامجيات، يمكن ان يعمل على حواسيب الزبون المتنقلة والبعيدة، ويعمل مع جميع انظمة التشغيل كالويندوز واللينيكس والماكنتوش، وغيرها، فضلا عن انه لا يحتاج الى اضافة تطبيقات الشبكة الافتراضية على الحواسيب او محطات العمل، ويجمع مابين خصائص الزبون البرمجي Software client والتي تتضمن المرونة وسهولة التوزيع والثبات، ومابين امكانية الاعتماد عليها بشكل كبير بالنسبة الى الزبون المادي.
- مكثفات الشبكة الافتراضية الخاصة: تستخدم لانهاء روابط الشبكة الافتراضية الخاصة القادمة من حواسيب زبون الشبكة الافتراضية الخاصة، وعادة ما تصمم مكثفات الشبكة الافتراضية الخاصة لانهاء اعداد كبيرة من روابط برتوكول الانترنيت الآمن القادمة من زبون الشبكة الافتراضية الخاصة من خلال حلول سيسكو للوصول عن بعد.

من خلال نفق الشبكة الافتراضية الخاصة الذي تكوّنه برتوكولات الشبكة الافتراضية الخاصة (في حالة نموذج سيسكو المستخدم تم استخدام برتوكول IPsec)، ومن خلال ارتباط المركز مع الفرع تنقل المعلومات المطلوبة مثلاً من مدير الفرع الى المركز بعد ان يتم تشفيرها، والتي ترتبط بدورها بالموجه المتواجد في الفرع، و يكون ايضاً من نوع سيسكو كما ذكرنا والذي يرتبط بدوره بجدار ناري ومكثف الشبكة الافتراضية الخاصة الذي ينهي روابط الشبكة الافتراضية القادمة وينقلها عبر موجه الشبكة المحلية التي تربط الفرع وخوادمه اذ ترتبط الشبكة المحلية المتواجدة في الفرع بمدير الفرع وحواسيب المشغلين الذين يكون لهم الصلاحية بادخال البيانات فضلا عن الحصول على بعض التقارير التي تقع ضمن نطاق صلاحياتهم.

وبذلك تكون مكونات نموذج سيسكو في جانب المركز والفرع مايأتي:

- شبكة محلية تتكون من مجموعة من الخوادم، بضمنها خادم نظام ادارة بيانات الزبائن لمصرف الرشيد الادارة العامة.
- زبون شبكة افتراضية خاصة على شكل موجه سيسكو 827.
- مكثف الشبكة الافتراضية الخاصة Concentrator.
- جدار ناري Firewall.
- نفق الشبكة الافتراضية الخاصة المستخدم لبرتوكول IPsec.

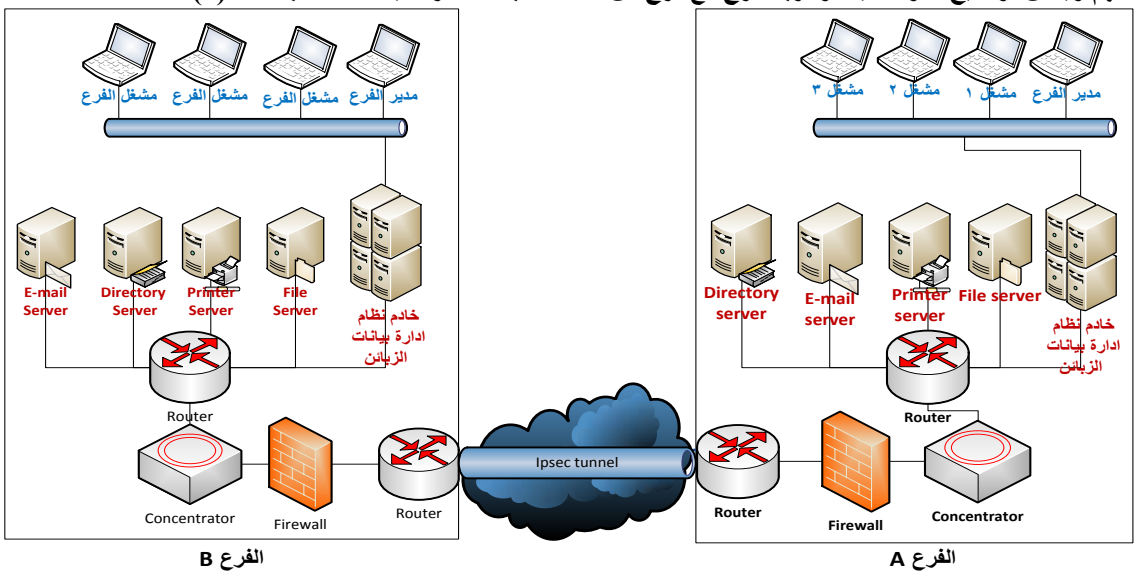
الحالة الثانية: ارتباط فرع مع فرع

عند ارتباط فرع مع فرع فيتواجد عادة في كل فرع شبكة محلية تربط كافة معدات وحواسيب المصرف مع بعضها، بضمنها خادم نظام ادارة بيانات الزبائن الذي من اجله يتم استخدام الشبكة الافتراضية، اذ ان المعلومات المصرفية تعد معلومات حساسة وعرضة للاختراق والتعديل فلا يمكن ان يتم نقلها بدون توفير الحماية الكافية التي توفرها انفاق الشبكة الافتراضية الخاصة والتي تصنعها معدات سيسكو عالية الجودة وشديدة الحماية وذلك في نموذجنا المستخدم بالاعتماد على بروتوكول IPsec.

وعندما يرغب فرع معين بالحصول على معلومة عن زبون معين لديه حساب في فرع اخر فيمكنه من خلال صلاحية المستخدم (مدير فرع، مشغل فرع) والوصول الى المعلومات المطلوبة في خادم نظام ادارة بيانات الزبائن الموجود في الفرع المقابل الذي تخزن فيه كافة معلومات الزبون الشخصية والمصرفية والخاصة ضمن الفرع المحدد فقط، ففي حالة وجود حساب الزبون في فرع آخر لن نحتاج الى التكرار في معلومات الزبون، واستهلاك الجهد والوقت في اعادة ادخال معلومات الزبون فمن خلال نظام ادارة بيانات الزبائن يمكن تشخيص وجود معلومات سابقة للزبون وحالة الحسابات الخاصة به في الفروع.

تتضمن المعدات المتواجدة في فرع معين استخدام شبكة محلية كما اسلفنا تربط حواسيب المصرف مع مدير الفرع والمشغلين، فضلا عن كافة شعب المصرف التي كانت كل منها مستقلة سابقاً وغير مرتبطة بشبكة تضمن تناسق العمل وتناغمه مابين كافة الشعب وعدم حاجة الزبون الى فتح حساب جديد له في كل شعبة من شعب المصرف، وقد تم مليء هذه الفجوة من خلال النظام الموحد المقترح الذي يسمى ادارة بيانات الزبائن لمصرف الرشيد.

فضلا عن ضرورة وجود موجه يربط ويوجه حزم البيانات عبر الشبكة، والذي يرتبط بدوره بمكثف الشبكة الافتراضية الخاصة وهو عبارة عن معدات خاصة بسيسكو تضمن تجميع كافة حزم البيانات القادمة من الشبكة وتركيزها وتوجيهها عبر الجدار الناري PIX؛ وهو اختصار لـ Private Internet Exchange وهو عبارة عن جدار ناري لبروتوكول الانترنيت و مترجم عناوين الشبكة NAT، ويرتبط بدوره بموجه الشبكة الافتراضية الخاصة المبرمج باسلوب معين، بحيث يصنع انفاق آمنة للبيانات لتعبر من خلالها عبر الويب لحين وصولها الى الفرع الآخر المطلوب ارسال البيانات اليه، ويحتوي ايضاً على هذا النوع من الموجهات، فضلا عن الجدار الناري PIX الخاص بحزمIP، وترتبط ايضاً هذه المعدة بدورها بمكثف الشبكة الافتراضية الخاصة المرتبط بموجه اعتيادي يوجه حزم البيانات القادمة من الفروع الى اجزاء الشبكة المحلية المتواجدة في الفرع، وذلك بحسب المعلومات المطلوبة والصلاحية الخاصة بكل منهم ويمكن توضيح حلول سيسكو لربط فرع مع فرع من خلال الشبكة الافتراضية الخاصة بالشكل (8).



الشكل (8) انموذج مقترح لربط فروع المصرف باستخدام حلول سيسكو

المصدر: الانموذج من اعداد الباحثان بتصرف استناداً الى:

Chamouche, James Henrey, 2006, IPsec Virtual Private Network Fundamentals, Cisco Press, P.156.

ومما سبق فانه يمكن المقارنة مابين حلول Cisco وحلول مايكروسوفت من خلال الجدول (3) الآتي:

الجدول (3)

المقارنة مابين الحلول الامنية لشركة سيسكو والحلول الأمنية لشركة مايكروسوفت

معيار المقارنة	الشبكة الافتراضية الخاصة لسيسكو	الشبكة الافتراضية الخاصة لمايكروسوفت
الكلفة	عالية الكلفة لاعتمادها على معدات خاصة.	منخفضة الكلفة بالمقارنة مع سيسكو.
نوع المنصات المعتمدة عليها	تعتمد على المكونات المادية المبرمجة لتعمل كشبكة افتراضية خاصة مثل جدار النار والموزعات والبوابات وغيرها.	لاتحتاج الى معدات خاصة بل تعتمد على برمجيات معينة تُنصّب في كل من طرفي الاتصال الخادم والزبون مثل ويندوز سيرفر وغيرها من اصدارات ويندوز.
انظمة التشغيل	تعمل مع جميع انظمة التشغيل كويندوز وماكنتوش ولينكس وغيرها.	تعمل فقط مع انظمة تشغيل ويندوز.
من حيث البساطة والتعقيد	لكونها تحتاج معدات خاصة فانها تكون معقدة بعض الشيء لحاجة كل مكون الى اعدادات خاصة به.	تمتاز بسهولة ربطها فهي تحتاج فقط الى تنصيب البرمجية الخاصة بالشبكة الافتراضية على جهتي الخادم والزبون.
من حيث المرونة	تكون اقل مرونة لانها تتطلب توافق المكونات الشبكة مع معدات سيسكو الخاصة بالشبكة الافتراضية مما يجعلها اقل مرونة.	تعمل مع كافة انواع المكونات المادية سواء كانت لسيسكو او غيرها لذا تكون اكثر مرونة.
من حيث الاعتمادية	اكثر اعتمادية	اقل اعتمادية
من حيث الحاجة الى تدريب العاملين	ضرورة تدريب العاملين لاستخدام المكونات المادية للشبكات الافتراضية الخاصة من نوع سيسكو التي قد تكون غريبة بالنسبة لغير المتخصصين في هذا المجال.	لاتحتاج الى تدريب العاملين فبرامجياتها تنصب على بيئات الويندوز التي تعد مألوفة من قبل الجميع.

المصدر: الجدول من اعداد الباحثان.

ويرى الباحثان انه وفقاً للبنية التحتية الحالية للمصرف فأن اعتماد حلول مايكروسوفت يكون اقل تكلفة نظراً لكونه يعتمد على وجود برنامج (VPN) على حاسوبي الخادم والزبون، فضلاً عن كونه سهل الاستخدام ويتطلب خطوات تنصيب بسيطة للحصول على الشبكة الافتراضية الخاصة من خلاله، بعكس حلول سيسكو التي تكون بجودة اعلى، الا انها تكون اعلى كلفة واكثر تعقيداً لحاجتها لمعدات خاصة وخبرات متخصصة للعمل بها.

المحور الرابع /الأستنتاجات والتوصيات

أولاً: الأستنتاجات

يهدف هذا المحور بصورة اساسية الى تقديم خلاصة لما توصل اليه البحث من استنتاجات نظرية ومن ثم التطرق الى الاستنتاجات الخاصة بالجانب العملي وكما يلي:

1- يمكن توفير الامان والحماية من خلال القيام بتحليل نقاط الضعف وتوفير الادوات التي تمنع التهديدات بالاعتماد على العديد من الادوات والتقانات كجدران النار ونظم كشف الاختراق فضلاً عن الشبكات الافتراضية الخاصة.

2- تعد الشبكة الافتراضية الخاصة من ابرز الحلول الامنية لتوفير الحماية للمعلومات المنقولة عبر انظمة المعلومات المستندة على الويب لكون مبدأ عملها يعتمد على وجود بنية تحتية عامة مثل الانترنيت، فضلاً عن كونها تستخدم بروتوكولات خاصة تقوم بصنع انفاق تُشفر المعلومات وتُغلفها لمنع اختراقها، ويوجد العديد من انواع الشبكة الافتراضية بحيث تتناسب مع البيئات المختلفة، الى جانب كونها توفر الامان وتزيد الارباح وتتمتع بالمرونة من خلال امكانية اضافة اطراف جديدة للاتصال وهذا ما يتناسب مع طبيعة انظمة المعلومات المستندة على الويب التي تتطلب امكانية الوصول اليها من قبل الجميع.

3- تستخدم الشبكة الافتراضية الخاصة العديد من البروتوكولات واكثرها شيوعاً في الاستخدام، بروتوكول الأنترنيت الآمن والذي له القدرة على القيام بالتشفير والتغليف لتوفير الحماية من الهجمات المتواجدة اصلاً في برتوكول الانترنيت، فضلا عن بروتوكول الانفاق من نقطة الى نقطة والذي يتميز بتقليله النفقات لكونه يدعم العديد من الروابط في خادم الشبكة الافتراضية.

4- يمكن الأخذ بأحد النماذج المقترحة لاستخدام الشبكة الافتراضية الخاصة سواء كان النموذج المقدم من قبل سيسكو بوصفه يوفر الكفاءة في الحماية واكثر اعتمادية على الرغم من ارتفاع تكاليف معداته، او من خلال تطبيق النموذج المقدم من قبل مايكروسوفت بوصفه نموذج يوفر السهولة في الاستخدام وعدم الحاجة الى معدات خاصة او الى خبرات متخصصة لتطبيقه، كبدائل للحلول الامنية من اجل وضع معلومات زبائن المصرف على الشبكة من دون القلق حول امكانية التعديل او اختراقها من قبل المخترقين.

ثانياً: التوصيات

استناداً الى الاستنتاجات التي توصل اليها الباحثان، فانه يمكن صياغة مجموعة من المقترحات التي من شأنها ان تدعم ادارة المصرف (بيئة التطبيق) وكما يلي:

1- يوصي الباحثان الأخذ بنموذج الشبكة الافتراضية الخاصة لمايكروسوفت نظراً لسهولة تطبيقه بالتوافق مع البنية التحتية للمصرف اذ لا يحتاج الى معدات خاصة سوى البرمجيات المنصبة على حواسيب الخادم والزبون في طرفي الاتصال مثل مايكروسوفت سيرفر.

2- ضرورة التخلي عن العمل التقليدي وجعل خط العمل المعتمد على الحاسوب اساسياً للعمل وليس مجرد خط عمل ثانوي يدعم خط العمل التقليدي.

3- تطوير البنية التحتية للمصرف بتوفير حواسيب حديثة تعمل بانظمة حديثة تدعم استخدام البرمجيات المعتمدة على الويب في انظمة شعب المصرف كافة.

4- يوصي الباحثان توفير معدات الشبكة الافتراضية الخاصة لغرض توفير امنية اكبر للبيانات الخاصة بالزبائن والتي يتم نقلها عبر شعب وفروع المصرف المختلفة.

5- تخصيص وتوفير الموازنات المالية للعمل بالنظام والنماذج المقترحة لغرض شراء النسخ الاصلية من المعدات والبرامجيات اللازمة لتطبيق النظام المقترح بشكل يحقق النفع والتقدم للادارة العامة لمصرف الرشيد.

6- ضرورة تعريف الكادر الوظيفي في المصرف بأهمية الاخذ بالنظام المقترح من خلال الندوات التعريفية، والذي يصب في مصلحة نجاح تطبيق النظام المقترح وتجنب مقاومة التغيير من قبل مناصري الابقاء على اسلوب العمل التقليدي.

المصادر

1- **Akbar & Shahzad, 2009, Security in Private Branch IP-Telephony Network with QoS Demands, Technical Report, School of Information Science, Computer and Electrical Engineering, Halmstad University**
http://hh.diva-portal.org/smash/get/diva2:239748/FULLTEXT01.
2- **Barylski, Marcin Adam, 2010, Performance And Security Testing For Improving Quality of Distributed Applications Working In Public/Private Network Environments, PHD's Dissertation, Faculty of Electronics, Telecommunications & Informatics, Gdansk University of Technology**
3- **Bjornstad, Torstein, (2007), Using GSM SIM Authentication in VPNs, Master Thesis, Department of Telematics, Norwegian University of Science and Technology**
http://wifo5-03.informatik.unimannheim.de/bizer/pub/
4- **Bless, Patrik, (2006), Security Policy Compliance at VPN Sites, Master Thesis,School of Computer & Communications Sciences, Swiss federal Institute of Technology, Zurich, Switzerland.**
http://www.open.ch/tl_files/OpenSystems/_img/13_high_re_org/SecurityPolicyCompliance_bless.pdf
5- **Brooker,Marc, 2005, An IPsec Gateway Based on the Intel IXP2400 Network Processor.**
http://www.rrsg.ee.uct.ac.za/theses/ug_projects/brooker_ugthesis.pdf..
6- **Broman, David, 2001, Lossless Data Compression Methods for Achieving Better Performance in a Wireless VPN, Master Thesis, Linkoping institute of technology, Stockholm, Sweden.**
http://www.bromans.com/david/publ/lossless_data_compression.pdf
7- **Carmouche, James Henry, 2006, IPsec Virtual Private Network Fundamentals, Cisco Press.**
8- **Chatziioannidis, Ioannis, 2004, High Speed Internet Access Using Cellular Infrastructure, Master thesis, Naval Postgraduate School, Monterey, California, USA.http://www.dtic.mil/dtic/tr/fulltext/u2/a427298.pdf**
9- **Faienza & Amso, 2008, IPsec Intrusion Detection Analysis: Using data from an Ericsson Ethernet Interface Board, Master Thesis Report *KTH* Royal Institute of Technology, Stockholm, Sweden.**
(http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/080618-Julian_Amso_and_Achille_Faienza-report-public_version.pdf
10- **Fisli, Rezan,(2005), Secure Corporate Communications over VPN-Based WANs, Master Thesis, Department of Numerical Analysis and Computer Science, Royal Institute of Technology, Stockholm, Sweden**
(http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.131.5170&rep=rep1&type=pdf

11- **Garcia, Gabriela Limon,(2008), IPSec performance analysis for large-scale Radio Access Networks, Master Thesis, Faculty of Information and Natural Sciences, Department of Computer Science and Engineering, Helsinki University of Technology.**
(http://nordsecmob.tkk.fi/Thesisworks/Thesis_GabrielaLimon_TKK.pdf).
12- **Harris, Shun, 2008, all In One -CISSP- Exam Guide, 4th Edition, The McGraw-Hill.**
13- **Hudson, Adam, (2002), VyperNet – A Framework for Programmable Internet-Based Virtual Private Networks, Master Thesis, School of Information Technologies, University of Sydney,**
(http://sydney.edu.au/engineering/it/~ahudson/document.cgi?doc=adam_hudson_honours_thesis&ext=pdf).
14- **Harris, Shun, 2008, all In One -CISSP- Exam Guide, 4th Edition, The McGraw-Hill.**
15- **Jaha, Ahmed Abdulgader,(2008), Selecting and Implementing Proper Virtual Private Network (VPN) Solution for Libyan Industrial Sector, Master Thesis, The High Institute of Industry, Department of Electronic Engineering.**
http://www.misurata.com.ly/doc/Binder1.pdf.
16- **Kilcrease, Patrick N., 2009, Employing A Secure Virtual Private Network (VPN) Infrastructure as a Global Command And Control Gateway To Dynamically Connect And Disconnect Diverse Forces On a Task –Force – By – Task -Force Basis, Master Thesis, Naval Postgraguate. School, Monterey, California.**
http://www.dtic.mil/cgi\bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf
17- **Klemetti, Kari, 2001, Authentication in Extranets, Master Thesis, Helsinki, Department of Computer Science, Telecommunications Software and Multimedia Laboratory, University of Technology.**
http://siteseerx.ist.psu.edu
18- **Kytola, Olli, 2002, Wireless Technologies in E-Business Services, Security and Management, Master Thesis, Department of Industrial Engineering and Management, International Operations and Marketing, Lappeenranta University Of Technology. http://www.tbrc.fi/pubfilet/TBRC_2002828233535.pdf**
19- **Mohan, Raj, 2002, XML Based Adaptive IPSEC Policy Management_In A Trust Management Context, Master Thesis, Naval Postgrguate School, Monterey, California.**
http://www.cisr.us/downloads/theses/02thesis_mohan.pdf
20- **Nousiainen, Jukka, 2010, Management of Carrier Grade Intra-Domain Ethernet, School of Science and Technology, Faculty of Electronics, Communications and Automation, Department of Communications and Networking, Aalto University., http://lib.tkk.fi/Dipl/2010/urn100187.pdf**

21- **Orgen, Niklas, 2002, Selecting /Realizing of Virtual Private Networks with Multi Protocol Label Switching or Virtual Local Area Networks, Master Thesis, KTH Royal Institute of Technology, Stockholm, Sweden, http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/020609-Niklas-Ogren.pdf**

22- **Paraskevaidis, Dimitris C.,2006, Services Architecture on Top of the Peer-to-Peer Wireless Network Confederation, Master Thesis, Department of Informatics, Athens University Of Economics And Business, Greek. (http://www.mm.aueb.gr/master_theses/polyzos/2006_paraskevaidis.pdf.)**

23- **Wong, Jenne, 2003, Performance Investigation Of Secure 802.11 Wireless LANs: Raising the Security Bar to Which Level, Master Thesis, University of Canterbury. http://www.cosc.canterbury.ac.nz/research/reports/MastTheses/2003/mast_0301.pdf**

24- **Yang, Yanyan, 2006, IPSEC/VPN Security Policy Engineering: Automatic Generation And Conflict Detection, Dissertation, University Of California. (http://www.cs.ucdavis.edu/research/tech-reports/2007/CSE-2007-16.pdf.)**

25- **Roman, Rodrigo & Lopez, Javier & Zhou, Jianying, 2005, Casual Virtual Private network, International Journal of Computer Systems, Science & Engineering, CRL Publishing Ltd. http://www.lcc.uma.es/~roman/files/roman-j-csse07.pdf**

26- **Lewis, Mark, 2006, Comparing, Designing, and Deploying VPNs, Cisco Press, USA.**

27- **Maquerry, Steve,2008, Authorized Self - Study Guide Interconnecting Cisco Network Devices, 3rd Edition, Cisco Press,,Indeiana,USA.**

28- **Murhammer, Martin W, Bourne, Tim & Gaidosch, Tamas & Kunzinger, Charles & Rademacher, Laura & Weinfurteret.al, Andreas, 1999, a Comprehensive Guide to Virtual Private Networks, Vol. 2, IBM Red Books.**

29- **Santos, Omar, 2007, End –To- End Network Security, Security– In – Depth, 2008, Cisco Press, USA.**

30- **Scott, Charlie & Erwin, Mike & Wolfe, Paul, 1999, Virtual Private Networks, Second Edition, O'Reilly, 2nd Edition.**

31- **Thomas, Orin, 2011, Windows Server 2008 R2 Secrets, John Willey & Sons, Inc., USA.**

32- **Wood, Robert, 2005, Next Generation Network Services, 2006, Cisco Systems, Inc., Cisco Press, USA.**

Alternative security solutions offered by virtual private network vpn model proposal to use alternatives to Cisco and Microsoft security in al-rasheed bank-delegate general office- northern region

Abstract

The study aimes to provide a Suggested model for the application of Virtual Private Network as tool that used to protect the transmitted data through the Web based information system, and the research included using case study methodology in order to collect the data about the research area (Al-rasheed Bank) by using Visio to desig and draw the diagrams of the suggested models, and adopting the data that have been collected by the interviews with the bank's employees, and the research used the modulation of data in order to find solutions for the research's problem.

The importance of the study Lies in dealing with one of the vital topics at the moment, namely, how to make the information transmitted via information systems celebrating safety, which is missed by many organizations, despite its importance, and providing the means for the protection and safety of the information transmitted from the center to the branches and back again to the center.

In order to achieve the goals of the study we build the suggested model, by using the Virtual Private Network through Cisco and Microsoft suggested models, The study concludes a set of conclusions, the most important, adopt a proposed model to use virtual Private Network, whether the model presented by Cisco or through the application form provided by Microsoft.

In light of the findings the study concluded a set of including, adopting the model of Microsoft Virtual Private Network due to the easy to apply using the infrastructure of the bank as tubeless to special equipment.

Keywords/ virtual private network, information security, network security, network infrastructure.