Journal of Engineering Sciences and Information Technology
Volume (5), Issue (3): 30 Sep 2021
P: 56 - 66

ISSN: 2522-3321

مجلة العلوم الهندسية وتكنولوجيا المعلومات
المجلد (5)، العدد (3): 30 سبتمبر 2021م
ص: 56 - 66

Build Encrypted Interconnection Networks by application of IP Security and Mac Address Filtering Authentication Methods

Jouma Ali AlMohamad

Faculty of Electrical and Electronic Engineering || Aleppo University || Syria

Abstract: To improve the security in data networks we use of IP Security and MAC Address Filtering authentication methods on network devices is very useful to be able to protect, verify and filter company data especially if data contain sensitive information like credit cards while using public data network. IP Security authentication provides integrity between connections, then Filtering MAC Address can help the router task to be able recognize users on the network, So that expected the combination between IP Security and Mac Address Filtering will provide security for every transfer and receive data from Headquarter to branch office, then the company doesn't have to worry about data package being robbed or manipulated by the unauthorized parties.

Keywords: Authentication, Interconnection, IP Security, Security, Mac Address Filtering.

بناء شبكات ربط مشفرة من خلال تطبيق أساليب مصادقة أمان IP وتصفية عنوان Mac

جمعه علي المحمد

كلية الهندسة الكهربائية والالكترونية || جامعة حلب || سورية

المستخلص: من اجل تعزيز الأمن في شبكات المعطيات فإننا نستخدم أساليب مصادقة أمان IP وتصفية عنوان MAC على أجهزة الشبكة مفيد جدًا للتمكن من حماية بيانات الشركة والتحقق منها وتصفيتها لاسيما إذا كانت البيانات تتضمن معلومات حساسة كبطاقات الائتمان عند استخدام شبكة معطيات عامة. تقدم مصادقة أمان IP السلامة بين الوصلات، بينما تساعد تصفية عنوان MAC مهمة جهاز التوجيه في التعرف على المستخدمين على الشبكة، لذلك من المتوقع أن يوفر الجمع بين أمان IP وتصفية عنوان MAC الأمان لكل عملية نقل واستلام البيانات من المقر الرئيسي للشركة إلى المكاتب الفرعية، فعندها فلن يكون هناك داع للقلق بشأن تعرض حزمة بيانات الشركة للسرقة أو التلاعب من قبل الأطراف غير المخولة.

الكلمات المفتاحية: المصادقة، الترابط، بروتوكول الإنترنت الأمن، الأمان، تصفية عنوان MAC.

1- المقدمة.

إن بروتوكول الإنترنت الأمن (IPSec) هو مجموعة بروتوكولات لتشفير البيانات المنقولة عبر الشبكة وهو طريقة للمساعدة في ضمان اتصالات خاصة وأمنة عبر شبكات بروتوكول الإنترنت (IP)من خلال استخدام خدمات الأمان بالتشفير [6]. يدعم IPSec سلامة البيانات على مستوى الشبكة، وسرية هذه البيانات، وكذلك مصادقة أصل البيانات، وحماية الرد [10]. ونظرًا لأن IPSec يعمل في طبقة الإنترنت (الطبقة 3) فإنه يوفر الأمان لجميع البروتوكولات تقريبًا في نموذج TCP/ IP، ولأن IPsec يتم تطبيقه بشفافية على التطبيقات، فهو يغني عن استخدام تقنيات الأمان الأخرى التي تعمل ضمن نموذج. [1] TCP/ IP

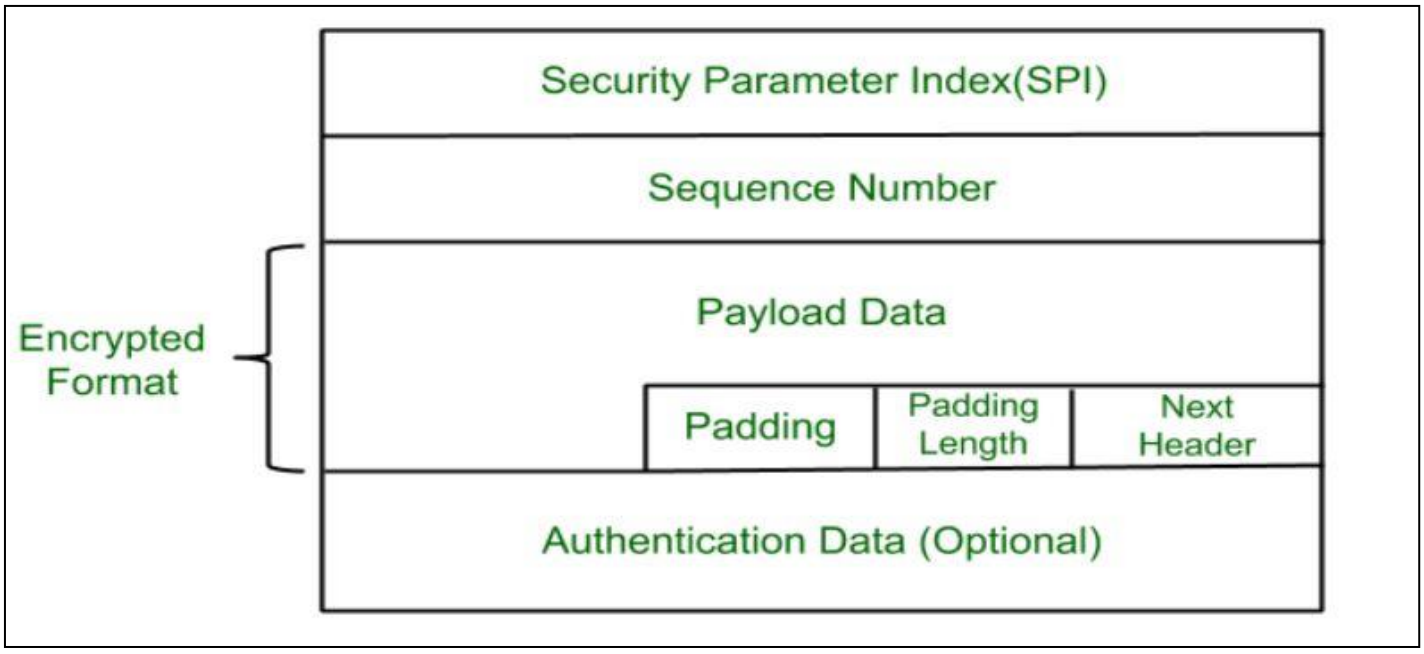
إن استخدام بروتوكول الانترنت الأمن IPsec يساعد على توفير دفاع عميق ضد:[11] [7]

- الهجمات ضمن الشبكة من أجهزة كمبيوتر غير موثوق بها، وكذلك الهجمات التي يمكن أن تؤدي إلى رفض خدمة التطبيقات.
- تلف البيانات.
- سرقة البيانات.
- سرقة بيانات اعتماد المستخدم.
- القيام برقابة على الخوادم وأجهزة الكمبيوتر الأخرى والشبكة.

يمكن استخدام IPsec للدفاع ضد الهجمات على الشبكة من خلال مجموعة من عمليات تصفية حزم IPsec لدى حواسيب المضيف وفرض الاتصالات الموثوقة فقط. ويمكن تنفيذ سياسات IPSec لتلبية متطلبات الأمان للعديد من أنواع المؤسسات المختلفة. [2]

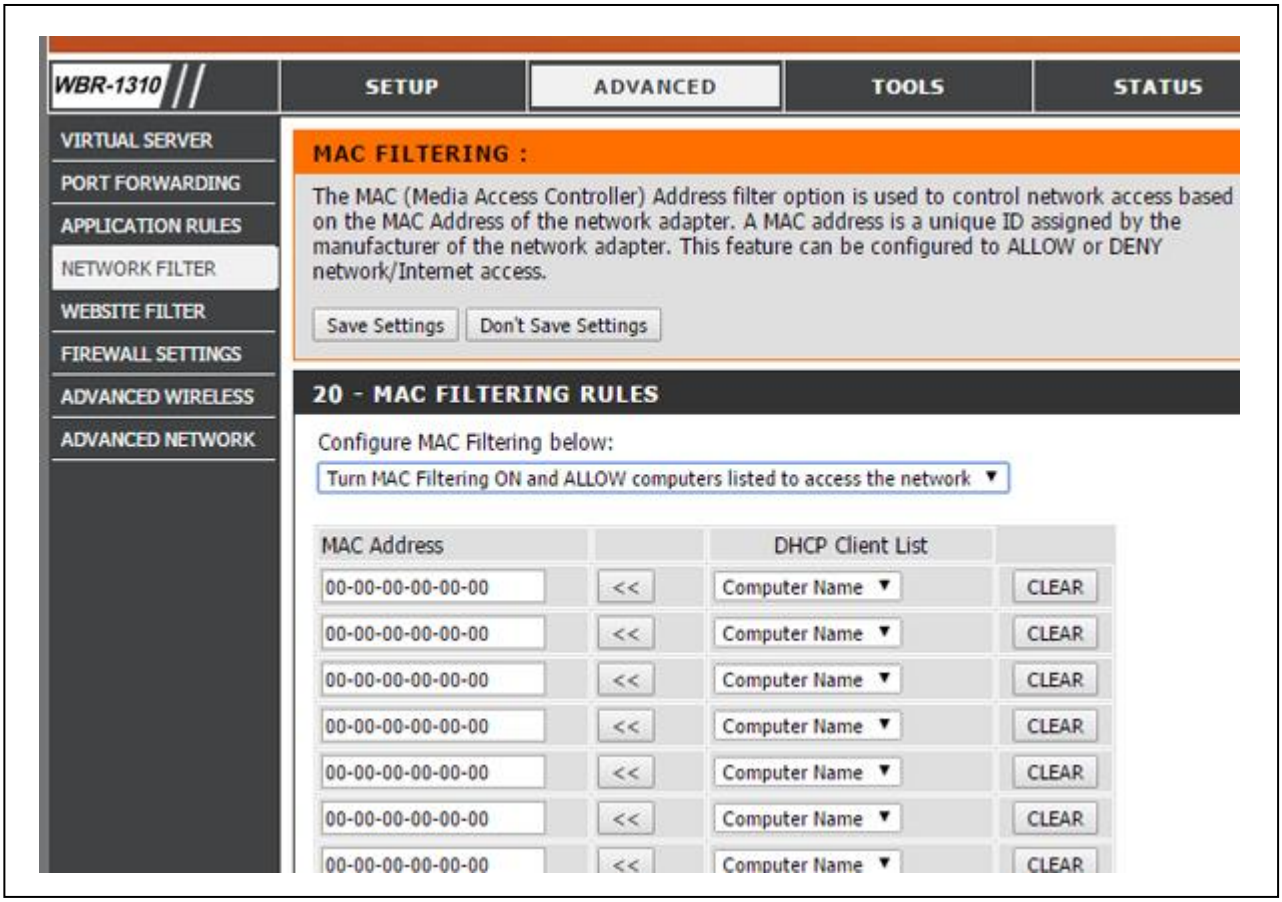
إن إرسال البيانات وتخزينها عبر الوسائط الإلكترونية يحتاج عمليات يجب أن تضمن أمن وسلامة البيانات المرسلة [8]. وبالتالي فإن أمان الشبكة يجب أن يضمن حماية البيانات الموجودة في الأجهزة والبرامج وأنظمة الشبكة، وعدم إتلافها، وعدم تغييرها لأي سبب من الأسباب، وأن النظام يعمل بشكل مستمر دون أي انقطاع في الخدمة [4]. ويجب أن تظل البيانات سرية أثناء الإرسال والاستقبال، ولتحقيق ذلك، يتم تنفيذ عملية التشفير (وفك التشفير) للبيانات المراد إرسالها. يتم التشفير أثناء التسليم عن طريق تغيير البيانات الأصلية إلى بيانات سرية بينما يتم فك التشفير أثناء الاستلام عن طريق تغيير البيانات السرية إلى بيانات أصلية [3]. لذا فإن البيانات المرسلة أثناء عملية الإرسال هي بيانات سرية، بحيث لا يمكن معرفة البيانات الأصلية من قبل جهات غير مخولة. ولا يمكن معرفة البيانات الأصلية إلا من قبل الأطراف المخولة.[9]

ونظرًا للحاجة إلى تحسين الأمان في الشبكة، فإن بروتوكول IPsec قادر على زيادة هذا الأمان. وهو عبارة عن مجموعة من البروتوكولات المستخدمة لتأمين اتصال بروتوكول الإنترنت IP مع المصادقة والتشفير على كل حزم بيانات IP وله الشكل التالي: [5]



الشكل(1)بنية IPsec

كما أن عنوان Mac هو عنوان جهاز فريد يحدد هوية الجهاز على الشبكة فكل عنوان mac يختلف عن العناوين الأخرى لأنه تم تنظيمه للاستخدام من قبل IEEE، من خلال تخصيص عناوين Mac إلى 48 بت بالنظام الست عشري. تمثل أول 24 بت رمزًا خاصًا بالشركة، بينما تمثل الـ 24 بت المتبقية رقم البطاقة [14]. مثال على عنوان mac هو كما يلي: D2-FC-C8-65-1F-6C.



الشكل (2) تصفية عناوين MAC

إن التصفية هي طريقة لتحديد عناوين الأجهزة المسموح لها أو المحظورة من القيام بتنفيذ عمليات معينة كما هو مبين بالشكل أعلاه [12]. لذلك سيقوم جهاز التوجيه بإجراء مسح لكل عميل ليتمكن من تحديد عنوان mac الذي يمكنه الوصول إلى الخادم [13].

إن هذه المقاربة غاية في الأهمية لدى الشركات التي لديها معلومات حساسة وتخشى عليها من الافتضاح لاسيما شركات الحوالات المالية التي تستخدم شبكات معطيات عامة.

2. مشكلة البحث:

يعد هذا البحث مهمًا لتعزيز أمان الشبكات ويمكن صياغة مشكلة الدراسة في النقاط التالية:

1- إمكانية ربط فروع الشركة بشكل آمن.
2- إجراء تطبيق عملي حول ذلك.

3. فرضيات البحث: تفترض الدراسة تطبيق كل من:

1- تطبيقات IPsec.

2- تصفية عناوين MAC.

4. أهمية البحث:

لقد أصبحت القضايا الأمنية مهمة للغاية في هذا الوقت، خاصة بالنسبة للشركات التي لديها العديد من الفروع في مواقع مختلفة والتي تتطلب أنظمة أمان عالية الأداء، للحفاظ على سرية المعلومات بين المكتب الرئيسي والمكاتب الفرعية للشركة.

5. مصطلحات البحث:

1. IPsec (IP Security) بروتوكول الإنترنت الأمن: هو مجموعة بروتوكولات لتشفير البيانات المنقولة عبر الشبكة.
2. MAC(Media Access Control) عنوان التحكم بالوصول للوسط: هو عنوان جهاز فريد يحدد هوية الجهاز على الشبكة.
3. PDN (Public Data Network) شبكة المعطيات العامة: وهي الشبكة التي يتم من خلالها ربط شبكات معظم المؤسسات والشركات في المدن كافة.
4. WAN (Wide Area Network) شبكة واسعة النطاق: وهي الشبكة التي تغطي رقعة جغرافية واسعة.
5. LAN (Local Area Network) شبكة محلية: وهي شبكة ضمن حيز جغرافي صغير (احد فروع شركة مثلا).
6. VPN (Virtual Private Network) شبكة خاصة افتراضية: وهي شبكة تخيلية يتم انشاؤها ضمن الشبكة العامة لنقل البيانات بشكل أمن.

6. منهجية البحث:

أ- طرائق البحث:

ب- النتائج والمناقشة:

ج- اختبار بناء النظام:

7. هيكلة البحث:

تم تحليل الاحتياجات وشرح طبولوجيا التصميم لشبكة أي شركة مرتبطة بالشبكة العامة للمعطيات وإجراء الاعدادات للأجهزة لكل من المقر الرئيسي والمقرات الفرعية للشركة.

1- تحليل الاحتياجات:

أجرى الباحثون تحليلًا لأنواع مختلفة من الأجهزة المطلوبة وتكوين عنوان IP لكل جهاز كما هو موضح في الجدول 1 والجدول 2. في موجه عنوان IP الخاص بشبكة WAN، أستخدم IP العام وليس لحماية خصوصية IP العام التي يجب أن نقوم بها، لإجراء الاختبار، لا يزال من الممكن إجراؤها باستخدام عنوان IP الفعلي مع عدد قليل من عناوين IP المخفية.

الجدول (1) مواصفات الأجهزة

NO	Hardware	Component	Type	Quantity
1	Devices	Router	Mikrotik RB951G-2HnD	2 pcs
		Switch	TP link LS1008G	2 pcs

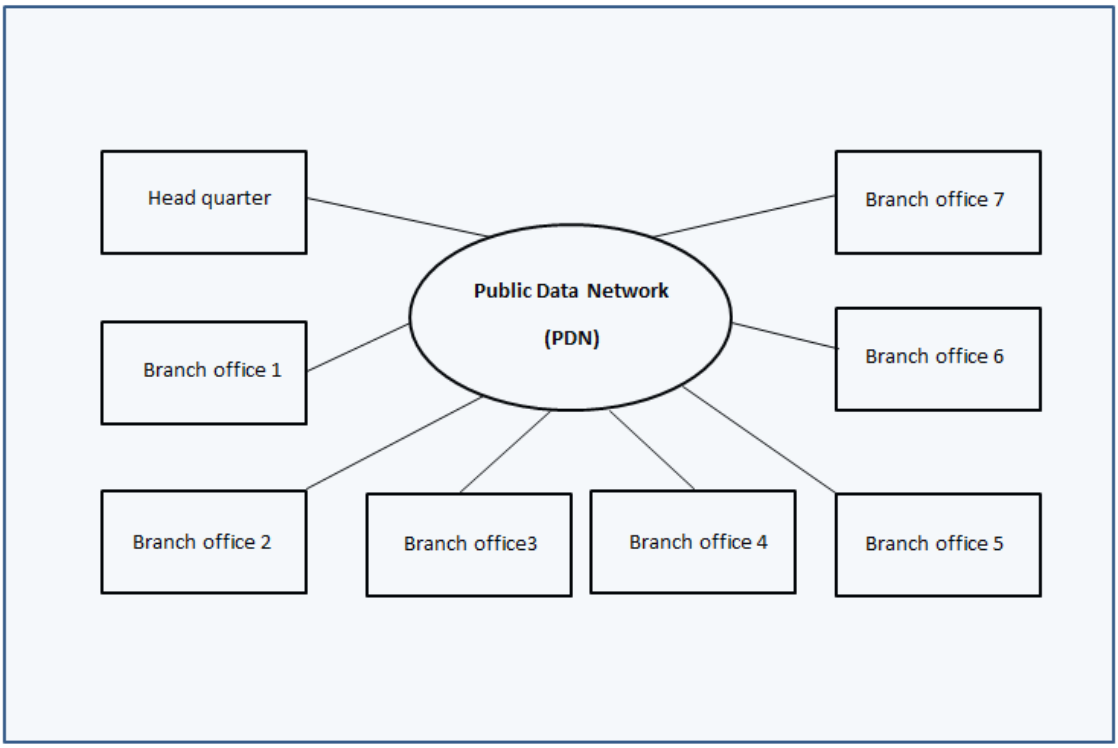
NO	Hardware	Component	Type	Quantity
		Access Point	D-Link DAP1360	2 pcs
2	Pc Server	Processor	Xeon	2 pcs
		RAM	16 GB	2 pcs
		Hard disk	1 TB	2 pcs
3	Pc Client	Processor	Intel Core i7 , Windows 10	2 pcs
		RAM	8 GB	2 pcs
		Hard disk	1 TB	2 pcs
4	Laptop Client	Processor	Intel Core i7 ,Windows 10	2 pcs
		RAM	8 GB	2 pcs
		Hard disk	1 TB	2 pcs
5	Tools	Crimping	Port RJ-45	1 pcs
		UTP Cable	Cat 6	100 Meter

الجدول(2) عناوين IP

No	Device	Interface	IP Address	Gateway	Location
1	Mikrotik	WAN	155.155.155.2/30	155.155.155.1/30	Headquarter
		LAN	192.168.1.1/24		
2	Access Point	LAN (Bridge Mode)	192.168.1.2/24	192.168.1.1/24	
3	PC Server	EthO	192.168.1.254/24	192.168.1.1/24	
4	PC Client	EthO	192.168.1.3/24	192.168.1.1/24	
5	Laptop Client	WLAN Card	192.168.1.4/24	192.168.1.1/24	
6	Mikrotik Router	WAN	156.156.156.2/30	156.156.156.1/30	Branch Office
		LAN	192.168.0.1/24		
7	Access Point	LAN (Bridge Mode)	192.168.0.2/24	192.168.0.1/24	
8	PC Server	EthO	192.168.0.254/24	192.168.0.1/24	
9	PC Client	EthO	192.168.0.10/24	192.168.0.1/24	
10	Laptop Client	WLAN Card	192.168.0.11/24	192.168.0.1/24	

2- طبولوجيا التصميم:

قمنا بتصميم الهيكل الموضح في الشكل 3 أدناه، وبعمل مخطط للشبكة لكل من المكتب الرئيسي والمكاتب الفرعية والتي هي جميعا ترسل بياناتها من خلال شبكة المعطيات العامة.



الشكل (3) طبولوجيا شبكة المعطيات العام والمواقع الرئيسة والفروع المرتبطة بها

تحتاج المؤسسات والشركات إلى بناء شبكات اتصالات معطيات لربط فروعها ببعضها من خلال قنوات اتصال خاصة تؤمن تبادل البيانات فيما بينها بموثوقية وأمان. ولكن بالنظر إلى الكفاءة المرجوة من إنشاء مثل هذه الشبكات الخاصة، يظهر بأنها غير مناسبة للتطبيق بشكل مطلق لأسباب تتعلق بالتكلفة المادية وتباعد مواقع الشركة أو كثرتها أحيانًا. وللتغلب على مثل هذه الصعوبات مع المحافظة على الخصوصية برزت فكرة استخدام الشبكات العامة المتاحة (Public Data Networks) لربط الفروع والأطراف مع إضافة الحماية اللازمة للمعلومات أثناء انتقالها في تلك الشبكات العامة مما يمنع الآخرين من الاطلاع عليها.

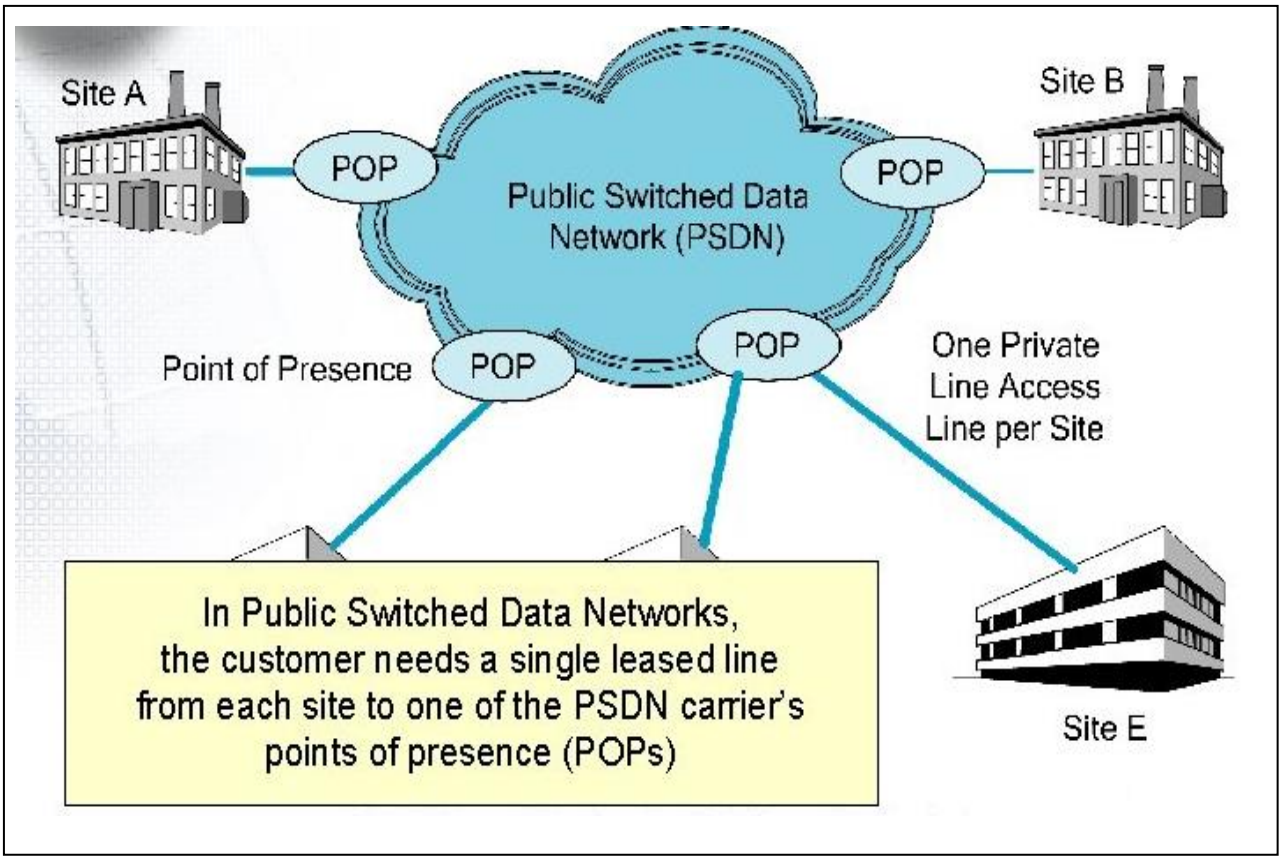
إن استخدام الشبكات الخاصة الافتراضية VPN يوفر عدة مميزات، من أهمها قلة التكلفة اللازمة لإنشائها، حيث أن كل ما يلزم هو استخدام الشبكة القائمة والمتاحة مسبقًا بالإضافة إلى بعض البرمجيات للحماية دون الحاجة إلى مد توصيلات سلكية. كما أنها تتميز بسرعة إعدادها وإتاحة ميزة حرية التنقل للمستخدم دون عناء نقل أي عتاد. ومن الأمثلة العملية على ذلك الصلاحيات التي تعطى لبعض الموظفين حيث يتمكنون من إنجاز أعمالهم من مواقع خارج مقر العمل عن طريق الارتباط بشبكة المؤسسة أو الشركة من خلال شبكة افتراضية.

ولتنفيذ شبكة خاصة افتراضية لشركة ما يتم حجز نطاق خاص بالشركة Domain ويمنح رقم فريد ضمن شبكة الـ WAN التي تربط منظومة اتصالات الإنترنت في الدولة والمعروفة باسم الـ PDN (Public Data Network) حيث تستخدم كما تم الذكر أعلاه كبنية تحتية لتنفيذ الشبكة الخاصة الافتراضية.

ويتم الربط الفيزيائي لفروع الشركة باستخدام الدارات النحاسية أو الضوئية التي تربط المقر الرئيس للشركة أو أحد الفروع بأقرب مركز نفاذ إلى منظومة الـ PDN والتي عادة توجد ضمن أقرب مركز هاتفي.

يتطلب كل فرع من فروع الشركة تجهيزات طرفية أو ما يعرف بالـ Router وإلى إعدادات برمجية خاصة لربط الفرع عبر الشبكة المخصصة للشركة وتتضمن: اسم المستخدم User name وكلمة المرور Password وعنوان الشبكة الداخلية Network IP.

ويتم تنظيم الإعدادات البرمجية لكافة الشبكات الخاصة باستخدام سيرفر مخصص لهذا الغرض حيث يقوم بربط بارامترات الاتصال الخاصة لكل فرع (اسم المستخدم وكلمة المرور وعنوان الشبكة الداخلية) بالنطاق المخصص للشركة.

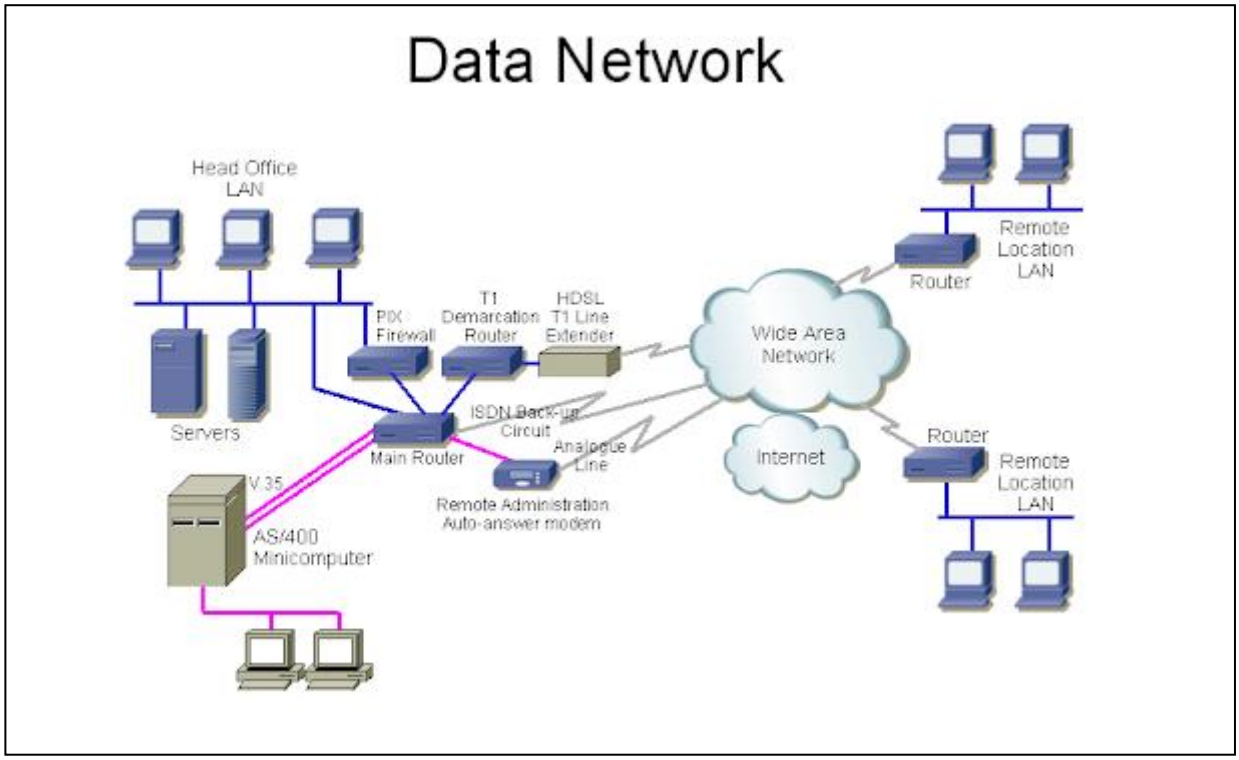


الشكل (4) ربط مقار الشركات ببعضها من خلال شبكة تبديل المعطيات العامة

وبعد إنشاء كافة الحسابات المطلوبة لربط فروع الشركة وربطها بالنطاق الخاص الممنوح للشركة يتم كمرحلة أخيرة لاستكمال الإعدادات البرمجية للخدمة بإضافة النطاق ضمن إعدادات الراوتر الموسع ضمن مركز النفاذ الأقرب لكل فرع لكي يتمكن فرع الشركة من الولوج إلى الشبكة الموسعة WAN المستخدمة لتنفيذ الشبكة الافتراضية الخاصة بالشركة وبذلك تكون الخدمة جاهزة من قبل مزود الخدمة وبدوره يقوم كل فرع بإدخال الإعدادات البرمجية على الطرفية الخاصة به (اسم المستخدم وكلمة المرور وعنوان الشبكة الداخلية) لتصبح الخدمة فعالة لديه.

إن ربط مقار الشركات والمؤسسات ببعضها من خلال شبكة المعطيات العامة والتي تعرف احيانا بشبكة تبديل المعطيات العامة (Public Switched Data Network) PSDN يتم من خلال خطوط مؤجرة leased line قد تكون كوابل نحاسية أو ضوئية وفق نقل البيانات المطلوبة من مقر الشركة إلى أقرب نقطة توضع POP (Point Of Presence) والتي تربط بين مقار الشركات والشبكة العامة كما هو موضع في الشكل أعلاه (4).

كما انه وبغية استمرارية عمل شبكات الشركات المرتبطة بشبكة المعطيات العامة وعدم توقفها فإننا نقوم بتأمين ربط آخر احتياطي (back up) كما هو موضح بالشكل التالي (5).



الشكل (5) تأمين دارات ربط احتياطية لضمان عدم توقف شبكات المكاتب الرئيسة للشركات المرتبطة بشبكة المعطيات

ولتعزيز أمن المعلومات في شبكات تبادل المعطيات المذكورة أعلاه يقدم الباحثون مقاربة جديدة تتلخص بتطبيق كل من بروتوكول أمان الأنترنت IPsec وتصفية عناوين MAC وبذلك يتم الوصول إلى مستوى عال من الأمن.

3- إعداد الأجهزة

بعد إجراء تصميم هيكل الشبكة حسب الحاجة، فإن الخطوة التالية هي تكوين Mikrotik راوتر.

1. Mikrotik Headquarter Configuration Stage
   a) Wan Interface Configuration is on the menu:
   New terminal –> add command:

```
#ip address add address= 155.155.155.2/ 30 network= 155.155.155.0 interface= ether1-WAN
```

   b) Lan Interface Configuration is on the menu:
   New terminal –> add command:

```
#ip address add address= 192.168.1.1/ 24 network= 192.168.1.0 interface= ether5-LAN
```

   c) Configuration L2TP Server. It's on the menu: PPP-> Interface Tab
   –> L2TP Server. with Secret IP: C0nn3ctS3rv3r
   d) Create a Secret User. It's on the Menu: PPP-> Secret.
   Select the Secret Tab-> Click Add [+] With Password: 5erverL2TP
   e) IP Security configuration. there on the menu: IP-> IPSec.

Select IPSec Proposal Tab-> Click Add

2. Branch Office Mikrotik Configuration Stage

a) WAN Interface Configuration is on the menu:

New terminal-> add command:

```
#ip address add address= 156.156.156.2/ 30 network= 156.156.156.0 interface= ether1-WAN
```

b) LAN Interface Configuration is on the menu:

New terminal-> add command:

```
#ip address add address= 192.168.0.1/ 24 network= 192.168.0.0 interface= ether5-LAN
```

c) Headquarter

d) IP Security configuration must be adjusted to the IPSec Server configuration. The configuration is on the menu:

IP-> IPSec-> IPSec Proposal tab –> Click Add.

3. Configuration Static Routing for Router HQ. in the new terminal menu:

add command:

```
#ip route add gateway= 50.50.50.2 dst-address= 192.168.0.0/24 check-gateway= ping type= unicast distance= 1 scope= 30 target – scope= 10
```

Then add routing for Branch Office. The same menu as the add command:

```
#ip route add gateway= 50.50.50.1 dst – address – 192.168.1.0/24 check – gateway= ping type= unicast distance= 1 scope= 30 target – scope= 10
```

4. Configuration MAC-Address filtering for Router HQ and Branch Office. is on the IP menu-> Firewall

- يمكننا أيضا" إدخال الأمر في محطة الوكيل عن طريق كتابة:

```
#ip firewall filter add chain= forward out-interface= "l2tp-connectsrv" src-mac-address= 8C:EC:4B:90:77:C5 action= accept.
```

- ثم بالنسبة إلى عنوان mac، أدخل عنوان mac المسموح له بالوصول إلى خادم البيانات على vpn، ثم نقوم بحظر جميع المستخدمين غير المصرح لهم عن طريق إدخال الأمر:

```
# ip firewall filter add chain = forward out-interface = "l2tp-connectsvr" action =
```

ثم نقوم بتكوين وكيل المكتب الفرعي، بنفس الطريقة، يمكنه الدخول من خلال المحطة على الوكيل ثم اكتب الأمر:

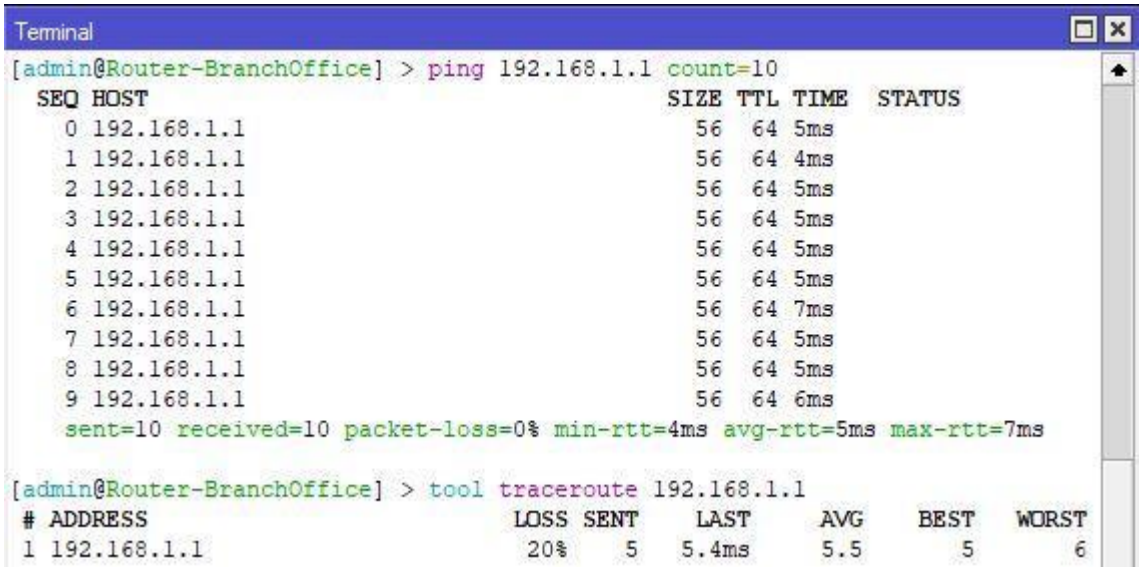
```
# ip firewall filter add chain = forward out-interface = "Connect To HQ" src-mac-
address = 00: 06: 19: 08: 00: 2D action = accept.
```

ثم نقوم بحظر جميع المستخدمين غير المصرح لهم عن طريق إدخال الأمر:

```
# ip firewall filter add chain = forward out-interface = "Connect To HQ" action =
```

4- اختبار الاتصالات بين المكاتب:

في هذا الاختبار، سيتم إجراء الاختبار على كل جهاز توجيه لمعرفة ما إذا كانت الاتصالات بين أجهزة التوجيه المكتبية متصلة أم لا، باستخدام أدوات PING و TRACEROUTE على جهاز التوجيه.



الشكل (6) PING و Traceroute في فرع Router Office إلى Router-HQ

في الشكل 6، يمكن استنتاج أن الاتصالات بين المكاتب متصلة بالفعل لأنها قادرة على تبادل ping و traceroute المرسلين من كل جهاز توجيه.

8. الخلاصة والتوصيات:

في هذا البحث بينا أن أمن المعلومات مهم جدًا لأي شركة لا سيما تلك الشركات التي طبيعة عملها تتطلب نقل معلومات هامة كالبنوك المصارف وشركات الحوالات المالية التي تستخدم شبكات المعطيات العامة (Public Data Networks)لذلك اصبح من الأهمية بمكان تطبيق طريقة تصفية عنوان MAC وأمن IP على شبكات اتصالات البيانات، الذي له تأثير فعال جدا للتمكن من تقليل حدوث الهجمات من قبل الأطراف غير المخولة وبالتالي الحد من قدرتها على الوصول أو التلاعب بالبيانات على الشبكة، فمن ناحية يقوم جهاز التوجيه بتسجيل عنوان MAC الخاص بالمستخدم حتى يتمكن هذا المستخدم من الوصول إلى البيانات على الخادم وبذلك يتم منع الأطراف غير المخولة من ارسال أية بيانات وطبعا هذا يحتاج إلى تحديث قاعدة بيانات الأجهزة المسموح لها بالإرسال وذلك بشكل دوري، كما أننا باستخدام IP Sec نجعل البيانات المنقولة بين المرسل والمستقبل مشفرة وبذلك نضمن أن الطرف الذي لديه

مفتاح التشفير فقط هو الوحيد الذي يمكنه الوصول إلى هذه المعلومات. إننا باستخدام كل من IPsecو MAC Filtering معا حققنا سوية عالية في أمن المعلومات لدى الشركات والمؤسسات التي تستخدم شبكة معطيات عامة في نقل المعلومات بين مقراتها الرئيسية وفروعها.

9. قائمة المراجع.

[1] M. Babu, "Performance analysis of IPSec VPN over VoIP networks using OPNET," International Journal of Advanced Research in Computer Science and Software Engineering, 2012. DOI: 10.5815/ijcnis.2015.12.01.

[2] S. E. Frankel, et al., "Guide to IPsec VPNs: Recommendations of the national institute of standards and technology," NIST Special Publication, Special Publication (NIST SP)-800-77, 2005.

[3] P. Jokela, J. Melen, and R. Moskowitz, Using the Encapsulating Security Payload (ESP) Transport Format with the Host Identity Protocol (HIP), RFC 7402, 2015.

[4] S. Kent, IP Authentication Header, RFC 2402, 2005.

[5] S. Kent, R. Atkinson, IP Authentication Header, RFC 2402, 1998.

[6] S. Kent, IP Encapsulating Security Payload (ESP05), RFC 4303, 2005.

[7] J. Klaue, and A. Hess, "On the impact of ipsec on interactive communications," in Proceedings of 19th IEEE International Parallel and Distributed Processing Symposium, 2005.

[8] A. Mazalek, Z. Vranova, and E. Stankova, "Analysis of the impact of IPSec on performance characteristics of VoIP networks and voice quality," in International Conference on Military Technologies (ICMT'15), 2015.

[9] V. Nikov, "A DoS Attack Against the Integrity-Less ESP (IPSec)", International Conference on Security and Cryptograph, 2006.

[10] J.P. Degabriele, K.G. Paterson, "Attacking the IPsec Standards in Encryption-only Configurations" IEEE Symposium on Security and Privacy 2007, pp. 335 – 349, 2007.

[11] S. Kent, K. Seo, "Security Architecture for the Internet Protocol", IETF, RFC 4301, 2005.

[12] IEEE 802.1AE-2006, "IEEE Standard for Local and Metropolitan Area Networks – Media Access Control (MAC) Security", 2006.

[13] Mochamad Akbar Fajar Hidayat Putra, Ucuk Darusalam, Andri Aningsih "Application of IP Security and MAC Filtering Authentication Methods to Build Encrypted Interconnection Networks", Journal Mantik, Volume 1, 2020, pp 343-353.

[14] Wikipedia, "MAC address," 6 July 2017. [Online]. Available: https://id.wikipedia.org/wiki/MAC_address. [Accessed 22 August 2017].