

Project Name :

**a secure network design between two
bank branch using VPN**

Implemented by the engineer:

Alaa Al -Halabi

الهدف من المشروع:

شبكة الإنترنت ضرورة وأساس من أساسيات حياتنا اليومية، لكنها ليست شبكة آمنة، فالمتطفلين يستطيعون الوصول إلى بياناتنا الشخصية وخصوصاً السريّة منها، حيث لا نستطيع حماية هذه البيانات وبالتالي نكون قابليين للاختراق وعرضة لتتبع سلوكنا على هذه الشبكة.

وللتخلص من هذه المشكلة نلجأ لاستخدام تقنية VPN (الشبكة الخاصة الافتراضية) فهي وسيلة لحماية المعلومات التي يتم نقلها عبر الإنترنت، حيث نقوم بإنشاء "نفق" خاص افتراضي للدخول الآمن إلى شبكة داخلية، والوصول إلى الموارد والبيانات والاتصالات عبر شبكة غير آمنة مثل الإنترنت.

نقوم في هذا المشروع بربط فرع رئيسي لبنك يقع في لندن مع مكاتبه الفرعيين في كل من دبي وقطر. يمتلك البنك خادم تطبيق يستخدمه عملاؤه في جميع أنحاء العالم لإجراء المعاملات عبر الإنترنت ويقع في مقره الرئيسي. جميع الفروع بها اتصال إنترنت عالي السرعة. يوجد حوالي 100 مستخدم في كل من المكاتب الفرعية و 200 مستخدم في المكتب الرئيسي.

الهدف تمكين كل من الفرعين من التواصل مع المكتب الرئيسي بسرعة وبشكل آمن، لتقوم بعملها بأعلى كفاءة وجودة، لتحقيق ذلك نقوم بإنشاء أنفاق GRE بسيطة (غير محمية) وآمنة (مشفرة IPSec) بين كل مكتب فرعي مع الفرع الرئيسي مبنية على شبكة الإنترنت.

Abstract:

The internet can be a dangerous place. From companies harvesting data to hackers targeting personal information, it's easy to stumble into an unfortunate cyber accident. The consequences, however, can be extremely unfortunate. Using a Virtual Private Network (VPN) is one of the most essential precautions you can take while working online. Yes, even at home.

a VPN creates an encrypted tunnel between you and a remote server operated by a VPN service. All your internet traffic is routed through this tunnel, so your data is secure from prying eyes along the way. Because your traffic is exiting the VPN server, your computer appears to have the IP address of said server, masking your identity and location.

جدول الاختصارات العلميّة

| | |
|---------|---|
| ACL | Access List |
| AES | Advanced Encryption Standard |
| AH | Authentication Header |
| ASA | Adaptive Security Appliance |
| ASBR | Autonomous System Boundary Router |
| ATM | Asynchronous Transfer Mode |
| BGP | Border Gateway Protocol |
| CA | Certificate authority |
| CER | customer Edge Router |
| DES | Data Encryption Standard |
| DH | Diffie-Hellman |
| ESP | Encapsulating Security Payload |
| FEC | forwarding Equivalence Class |
| GRE | Generic Routing Encapsulation |
| HMAC | Hashed Message Authentication Codes |
| HTTPS | HypertText Transfer Protocol Secure |
| IKE | Internet Key Exchange |
| IPSec | Internet Protocol Security |
| ISAKMP | Internet Security Association and Key Management Protocol |
| L2TP | Layer 2 Tunneling Protocol |
| LAN | Local Area Network |
| LDP | Label Distribution Protocol |
| LER | Label Edge Router |
| LSP | Label-Switched Path |
| LSR | Label Switsh Router |
| M-D VPN | Multi-Domin Virtual Private Network |
| MD5 | Message Digest Algorithm |
| MPLS | Multiprotocol Label Switching |
| NAS | Network -Attached Storage |
| NAT | Network Address Translation |
| OSPF | Open shortest Path First |
| PAT | Port Address Translation |
| PER | Provider Edge Router |
| PPP | Point-To-Point Protocol |
| PPTP | Point-To-Point Tunneling Protocol |
| RSA | The Rivest-Shamir-Adleman Algorithm |
| RSVP | Resource Reservation Protocol |

| | |
|---------|------------------------------------|
| SA | Security Associations |
| S-D WAN | Software-Defined Wide Area Network |
| SHA | Secure Hash Algorithm |
| SSL | Secure Socket Layer |
| SSTP | Secure Socket Tunneling Protocol |
| TDM | Time-Division Multiplexing |
| TLS | Transport Layer Security |
| VLAN | Virtual Local Area Network |
| VLL | Virtual Leased Lines |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |

الفهرس

| | | |
|----|--|--|
| 10 | الفصل الأول: التعريف بالشبكة الخاصة الافتراضية | |
| 10 | 1.1 مقدمة | |
| 10 | 1.2 بيئة العمل | |
| 11 | 1.3 الشبكة الخاصة الافتراضية | |
| 12 | 1.4 أنماط تصنيف الشبكة الافتراضية الخاصة: | |
| 14 | 1.5 تقنيات VPN | |
| 15 | 1.5.1 Site-to- Site VPN | |
| 20 | 1.5.2 Remote Access VPN | |
| 23 | 1.6 آليات الأمن | |
| 24 | الفصل الثاني: التوجيه | |
| 24 | 2.1 VPN TUNNELLING | |
| 25 | 2.1.1 متطلبات اختيار VPN؟ | |
| 27 | 2.1.2 بروتوكولات الاتصال النفقية؟ | |
| 39 | الفصل الثالث: وظائف VPN | |
| 39 | 3.1 CONFIDENTIALITY | |
| 39 | 3.1.1 التشفير المتناظر | |
| 40 | 3.1.2 التشفير غير المتناظر | |
| 41 | 3.2 AUTHENTICATION | |
| 41 | 3.3 INTEGRITY: | |
| 42 | 3.3.1 خوارزمية التجزئة | |
| 45 | 3.3.2 خوارزميات المصادقة | |
| 46 | 3.4 ANTI-REPLAY | |
| 47 | الفصل الرابع: عمل IPSEC | |
| 47 | 4.1 أوضاع عمل IPSEC | |
| 47 | 4.1.1 وضع نفق IPSEC | |
| 49 | 4.1.2 وضع النقل IPSEC | |
| 50 | 4.2 إعداد IPSEC | |
| 50 | 4.2.1 ACL: Access List | |
| 52 | 4.2.2 ISAKMP | |
| 56 | 4.2.3 Crypto map | |

| | | |
|----------|---------------------------------------|-------|
| 58 | الفصل الخامس: تغليف التوجيه العام GRE | |
| 58 | مشاكل SITE-TO-SITE VPN | 5.1 |
| 58 | أنواع GRE | 5.2 |
| 59 | أوضاع GRE | 5.3 |
| 59 | GRE IPSEC TUNNEL | 5.3.1 |
| 61 | نمط GRE IPSEC Transport | 5.3.2 |
| 64 | الفصل السادس: التطبيق العملي | |
| 64 | خطوات العمل | 6.1 |
| 78 | النتائج | 6.2 |
| 78 | الصعوبات والتوصيات | 6.3 |
| 80 | الخاتمة | 7 |
| 81..... | المراجع | 8 |

فهرس الأشكال

| | | |
|----|---------------------------------------|-----------|
| 11 | VPN connectivity overview | الشكل 1-1 |
| 12 | أنماط VPN | الشكل 2-1 |
| 14 | تقنيات VPN | الشكل 3-1 |
| 15 | Site-to- Site VPN | الشكل 4-1 |
| 25 | VPN tunnelling | الشكل 1-2 |
| 26 | متطلبات VPN وفق الاستخدام | الشكل 2-2 |
| 32 | شكل IP Packet في AH | الشكل 3-2 |
| 34 | IP Packet in AH ,ESP | الشكل 4-2 |
| 38 | VPN Tunnelling Protocols | الشكل 5-2 |
| 47 | IPSec Tunnel Mode | الشكل 1-4 |
| 48 | IP Packet of IPSec Tunnel with ESP | الشكل 2-4 |
| 48 | IP Packet of IPSec Tunnel with AH | الشكل 3-4 |
| 49 | IPSEc Transport Mode | الشكل 4-4 |
| 50 | IP Packet of IPSec Transport with ESP | الشكل 5-4 |
| 50 | IP Packet of IPSec Transport with AH | الشكل 6-4 |
| 60 | GRE IPSec Tunnel | الشكل 1-5 |
| 62 | GRE IPSEC Transport | الشكل 2-5 |
| 64 | الشكل العام للشبكة | الشكل 1-6 |
| 74 | تنفيذ الأمر ping من L2 و PC3. | الشكل 2-6 |

| | | |
|----|--------------------------------|-----------|
| 75 | تنفيذ الأمر ping من PC3 إلى L2 | الشكل 3-6 |
| 76 | شكل الشبكة على GNS3 | الشكل 4-6 |
| 76 | تنفيذ الأمر ping من PC2 | الشكل 5-6 |
| 77 | تنفيذ الأمر ping من PC3 | الشكل 6-6 |

1 الفصل الأول :التعريف بالشبكة الخاصة الافتراضية

سنبتدى هذا الفصل بالمقدمة والحديث عن بيئة العمل المستخدمة ثم سنستعرض المعلومات التي توضح الشبكة الخاصة الافتراضية وأنواعها وتقنياتها.

1.1 مقدمة

يعيش العالم هذه الأيام ثورة في التطور والتقدم وخصوصاً في مجال التكنولوجيا. واعتمادنا على البيانات المحوسبة والحاجة لتبادلها إلكترونياً أصبحت الشبكة من الضروريات ولاسيما الشبكات الآمنة لحساسية البيانات المنقولة بين الفروع. بحيث يتم نقل بيانات الشبكات المحلية إلى الفروع البعيدة عبر الشبكة العامة بشكل آمن ومنخفض التكلفة مع قدرة أجهزة الشبكة إلى الوصول إلى الشبكة العامة في نفس الوقت.

في عالم اليوم المترابط ، من غير المنطقي الاعتقاد بأن نظام شبكة الكمبيوتر محصن من الهجمات أو اعتبارها صغيرة جداً بحيث لا يمكن أن تكون فريسة للدخلاء لكسب أي ميزة يحتاجونها. في بعض الأحيان ينخدع أصحاب الشركة من خلال التفكير في أن موارد الشركة ليست ذات قيمة عالية وبالتالي فهي لا تستحق أن تكون المستهدفة ، لكن في الحقيقة من الضروري للغاية أن تولى الشركات اهتماماً خاصاً لتشديد طبقاتها الأمنية لحماية الموارد وتجنب الوقوع ضحية للهجمات الإلكترونية العالمية.

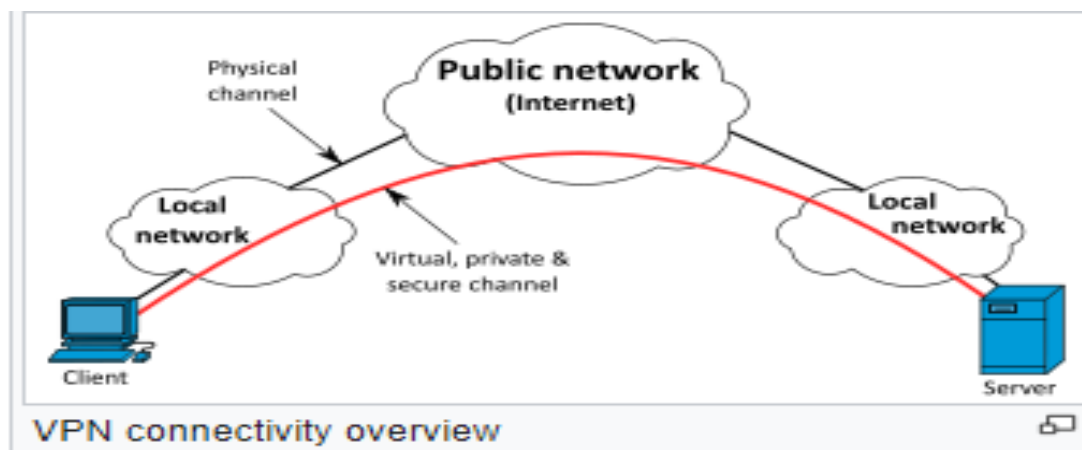
الغرض من هذا المشروع هو تصميم شبكة افتراضية خاصة (VPN) للبنك وتنفيذ تدابير أمنية لحماية موارد الشبكة وخدمات النظام. حيث توفر تقنية VPN (الشبكة الخاصة الافتراضية) وسيلة لحماية المعلومات التي يتم نقلها عبر الإنترنت، من خلال السماح للمستخدمين بإنشاء "نفق" خاص افتراضي للدخول الآمن إلى شبكة داخلية، والوصول إلى الموارد والبيانات والاتصالات عبر شبكة غير آمنة مثل الانترنت.

1.2 بيئة العمل

مع استمرار تطور أنظمة الشبكات في التعقيد ، تظهر مناهج وأدوات تعليمية جديدة لتسهيل التدريس والتعلم حول تكنولوجيا الشبكات. ضمن هذا الإطار ، تم تطوير برنامج التعلم الإلكتروني Cisco® Packet Tracer لمساعدة الطلاب على اكتساب مهارات تقنية الشبكات العملية في بيئة سريعة التغير. Packet Tracer عبارة عن أداة محاكاة مرئية عبر الأنظمة الأساسية تم تصميمها بواسطة Cisco Systems والتي تتيح للمستخدمين إنشاء هياكل الشبكة وتقليد شبكات الكمبيوتر

الحديثة. يسمح البرنامج للمستخدمين بمحاكاة تكوين موجهات Cisco والمحولات باستخدام واجهة سطر أوامر محاكاة (Graphical Network Simulator-3). اختصار إلى GNS3 هو محاكي برامج شبكة يسمح بدمج الأجهزة الافتراضية والحقيقية المستخدمة لمحاكاة الشبكات المعقدة.

1.3 الشبكة الخاصة الافتراضية



الشكل 1-1 VPN connectivity overview

أولاً: إنها شبكة، أي توفر اتصالاً متبادلاً لتبادل المعلومات بين مختلف الكيانات التي تنتمي إلى VPN.

ثانياً: كلمة "خاصة" تعني أن هناك خصوصية للبيانات ولا يطلع عليها إلا أطراف الاتصال.

ثالثاً: كلمة "افتراضية" تعني أن الاتصال الخاص يجري عبر قناة اتصال غير مادية يتم إنشاؤها وتأمينها عبر شبكة عامة خصيصاً لهذا الغرض.

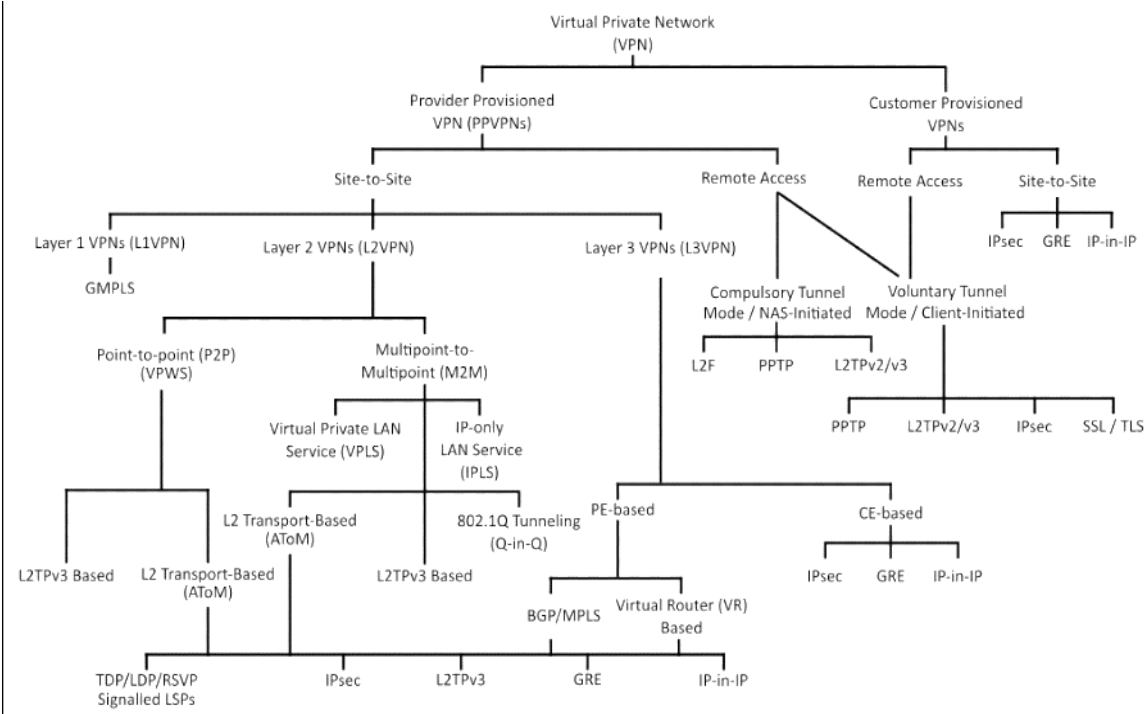
تقوم الشبكة الافتراضية الخاصة (VPN) بتوسيع شبكة خاصة عبر شبكة عامة، وتمكن المستخدمين من إرسال واستقبال البيانات عبر الشبكات المشتركة أو العامة كما لو كانت أجهزة الحوسبة الخاصة بهم متصلة مباشرة بالشبكة الخاصة.

تم تطوير تقنية VPN للسماح للمستخدمين عن بعد والمكاتب الفرعية بالوصول إلى تطبيقات الشركة ومواردها. لضمان الأمان، يتم تأسيس اتصال الشبكة الخاصة باستخدام بروتوكول نفق متعدد

الطبقات مشقّر، ويستخدم مستخدمو VPN طرق المصادقة، بما في ذلك كلمات المرور أو الشهادات، للوصول إلى VPN.

يتم إنشاء VPN عن طريق إنشاء اتصال افتراضي من نقطة إلى نقطة من خلال استخدام دوائر مخصصة أو مع بروتوكولات الاتصال النفقي عبر الشبكات الحالية.

1.4 أنماط تصنيف الشبكة الافتراضية الخاصة :



الشكل 1-2 أنماط VPN

● حسب طريقة الإدارة:

1. مدارة من قبل مزودات الخدمة:

مثل VPN باستعمال تبديل اللافئات متعدّدة البروتوكولات MPLS VPN وشبكة الموجه الافتراضي Virtual Router VPN.

2. مدارة من قبل العملاء:

مثل VPN باستعمال تغليف التوجيه العام GRE VPN و VPN باستعمال حزمة أمن بروتوكول الانترنت IPsec VPN.

● حسب طبولوجية الشبكة:

1. شبكات الوصول البعادي :

تسمح للمستخدمين بالوصول إلى الموارد بشكل بعادي وتصنف حسب طريقة الإنشاء إلى:

(1) شبكات وصول بعادي تدعم النمط الإلزامي Compulsory mode : يقوم

المستخدم البعادي بإنشاء اتصال مع مزود الخدمة أو مع مخدّم نفاذ الشبكة (المزود)

NAS ويقوم المزود بإنشاء الاتصال مع الهدف ويحتفظ المستخدم بإمكانية ضبط

الخيارات الأمنية وهذا الاتصال مدار من قبل مزود الخدمة.

بروتوكول سيسكو للتوجيه على مستوى الطبقة الثانية L2F .

بروتوكول الأنفاق في الطبقة الثانية L2TP .

(2) شبكات الوصول البعادي التي تدعم النمط الاختياري Voluntary mode : يقوم

المستخدم البعادي بإنشاء اتصال مع الهدف البعيد مباشرة عبر الشبكة العامة وقد يكون

مدار بواسطة المزود أو العميل.

بروتوكول الأنفاق بين نقطتين PPTP .

بروتوكول الأنفاق في الطبقة الثانية L2TP .

2. شبكات بين المواقع:

تؤمن الاتصال بين موقعين أو أكثر متباعدين جغرافياً قد يتبعان لمؤسسة واحدة أو أكثر (شائع في

الطوبولوجيا التي ترتبط فيها قيادة شركة ما مع مكاتب فرعية عديدة لها). تصنف إلى :

(أ) حسب عدد المؤسسات التي تمتد على شبكاتها إلى:

1. داخلية Intranet : تصل بين عدة مواقع تتبع لنفس المؤسسة.

2. خارجية Extranet : تصل بين عدة مواقع تتبع لمؤسسات مختلفة.

ب) حسب إدراك المعدات فيها لوجود الأنفاق إلى:

1. مرتكزة على أجهزة العميل CE-Based VPN : تقوم أجهزة العميل بإنشاء الشبكة

الخاصة الافتراضية فيما بينها عبر شبكة مزود الخدمة ولكن أجهزة المزود ورغم مشاركتها

في توجيه البيانات تكون غير مدركة لوجود الشبكة الخاصة الافتراضية مثل IPSec

VPN و GRE VPN.

2. مرتكزة على أجهزة المزود PE-Based VPN: تقوم أجهزة المزود بإنشاء الشبكة

الخاصة الافتراضية فيما بينها وتدير عملية التوجيه عبرها وتكون معدات العميل معزولة عن

هذه الشبكة وتتصل مع أجهزة تخديم المزود (راوترات، سويتشات) لأجل تبادل البيانات

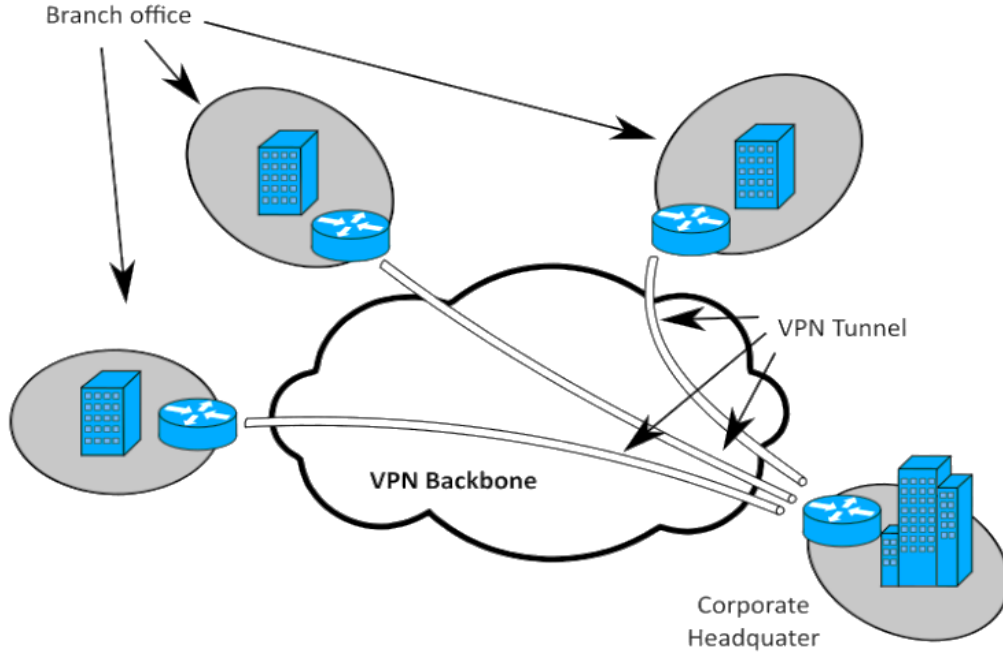
عبرها مثل L3MPLS VPN و Virtual router VPN.

1.5 تقنيات VPN

| Features | VPN Technology | | | | |
|--------------------------------|--|--|--|--|--|
| | Site-to-Site VPN | Remote Access VPN | SD-WAN VPN | Cloud VPN | Consumer VPN Business Plan |
| Ideal for | Connecting two or more networks (LANs) | Connecting devices to a single network | Connecting two or more networks (LANs) | Cloud-hosted infrastructure | Connecting office networks and remote workers to the internet securely |
| Ease of Deployment | Complex | Easy | Complex | Easy | Easy |
| Skill Level Required for Setup | Highly skilled technology experts | Skilled tech pros | Highly skilled technology experts | Skilled tech pros or skilled users with help | Skilled users with help from a skilled VPN support team |
| Performance | Excellent/best | Good to Very Good | Excellent | Very good | Good |
| Cost | Expensive | Moderate | Somewhat expensive | Moderate | Moderate |
| Target Market | Large Business | Any Size Business | Large Business | Any Size Business | Small to Medium Business |

الشكل 3-1 تقنيات VPN

:Site-to- Site VPN 1.5.1



الشكل 4-1 Site-to- Site VPN

ما هو VPN الموقع إلى الموقع؟

تتيح VPN الموقع من موقع إلى موقع تجاري لشركة لها مكاتب في مواقع متعددة إنشاء اتصالات آمنة بين شبكات LAN المختلفة في هذه المكاتب عبر الإنترنت. على سبيل المثال، قد تقوم الشبكة الظاهرية الخاصة من موقع إلى آخر بتوصيل شبكة LAN للمكاتب الفرعية بالشبكة الرئيسية في مقر الشركة.

وبالتالي، تعمل الشبكة الافتراضية الخاصة من موقع إلى آخر على توسيع شبكة الشركة، مما يجعل موارد الكمبيوتر في مكان واحد متاحة للموظفين في مواقع أخرى. هذه الإمكانية تجعل VPN من موقع إلى موقع خيار جذاب لشركة متنامية لها مكاتب فرعية في جميع أنحاء العالم.

الطريقتان الرئيسيتان لإنشاء شبكة اتصال VPN خاصة بالموقع هي:

- طريقة VPN الإنترنت.
- طريقة VPN لبروتوكولات تبديل الملصقات (MPLS).

يمكن الاختلاف بين الشبكات المستندة إلى الإنترنت و MPLS VPN في الاتصالات التي يستخدمونها، وما إذا كانت شبكة الشركة أو شبكة موثر VPN تقوم بإجراء التقق الافتراضي.

1.5.1.1 إنشاء VPN موقع على شبكة الإنترنت

تستخدم طريقة VPN على الإنترنت شبكة الشركة الحالية، إلى جانب البنية التحتية للإنترنت العامة. من أجل إعداد VPN موقع على شبكة الإنترنت بين موقعين، فإن بوابة VPN (جهاز التوجيه، أو جدار الحماية، أو مركز تركيز VPN، أو الأجهزة الأمنية) مثل Cisco Adaptive Security Appliance (ASA) مطلوبة في كلا الموقعين.

تقوم بوابة VPN بتغليف وتشفير كل حركة مرور البيانات الصادرة من موقع واحد، وإرسالها عبر نفق VPN عبر الإنترنت العام إلى بوابة VPN نظير في الموقع الثاني. عند استلام الإرسال، تقوم بوابة VPN التظيرة بفك تشفير المحتوى وتنقل البيانات إلى الشبكة المحلية لذلك المكتب.

1.5.1.2 إنشاء VPN موقع MPLS (Multiprotocol Label Switching)

على الرغم من وجود الشبكات الافتراضية الخاصة (VPN) من موقع إلى آخر عبر الإنترنت لسنوات عديدة، إلا أن MPLS هي طريقة جديدة نسبياً لإنشاء VPN موقع إلى آخر. في هذه الطريقة، يتم تأسيس اتصال VPN من خلال الاتصال بسحابة MPLS المقدمة من شركة الاتصالات، بدلاً من الاتصال بالإنترنت العام. وبالتالي، يستخدم MPLS VPN البنية التحتية الخاصة بموفر VPN، وليس الشركة التي تستخدم VPN. لتكوين MPLS VPN، يقوم مزود حلول أمان الأعمال بإنشاء اتصالات افتراضية بين مواقع مكاتب الشركة العميلة عبر شبكة MPLS الخاصة بالموفر.

تؤمن VPN نقل مشفر للبيانات عبر أنفاق خاصة بسريرة تامة. لكن بناء هذه الأنفاق في شبكات كبيرة سيكون مكلف بسبب الحاجة إلى الخطوط المستأجرة وإلى إعدادات خاصة وتجهيزات إضافية فكان الحل تقنية MPLS VPN التي تسمح بتنظيم الوصول إلى الأجزاء المختلفة والمستخدمين البعيدين عبر وصلة آمنة وبتكلفة مادية منخفضة لا تتضمن حجز لهذه الوصلات وإنما عبر بناء أنفاق خاصة مشفرة ضمن وصلات شبكة الإنترنت العامة.

أ) مميزات MPLS:

تحسن تقنية MPLS من أداء VPN حيث تتمتع بالمزايا التالية:

1-قابلية التوسع.

2-ضمان جودة الخدمة QoS.

3-الاستخدام الأفضل لعرض النطاق الترددي.

4-تقليل ازدحام الشبكة حيث تقوم بتحسين آلية التوجيه على مستوى الطبقة الثالثة وتأمين عزل واستقلالية البيانات عن طريق استخدام وسوم Label محددة الطول توسم بها رزم البيانات على مدخل شبكة MPLS محددة وجهتها دون أن تضطر بقيّة الموجهات الوسيطة الموجودة داخل البنية الداخلية للشبكة العامة إلى إشغال ذواكرها ومعالجتها بإعدادات جداول التوجيه في كل قفزة.

تعمل على شبكات المناطق الواسعة WAN لتحسين عمل شبكات مزودي خدمات الانترنت وتتميز بقدرتها على هندسة حركة البيانات .

الميزة الجوهرية لتقنية MPLS توافقيتها الكاملة مع بروتوكول الانترنت IP دون الحاجة إلى تغيير أي من مكونات الشبكة.

ب) عيوب MPLS

عيوب MPLS VPNs كانت دائماً التكلفة. تعتبر خدمات IP الخاصة مثل شبكات VPN الخاصة بموقع MPLS باهظة الثمن، خاصة بالنسبة للاتصالات الدولية.

ت) ملخص عمل تقنية MPLS :

تقوم على مبدأ تبديل قيم Label التي تم إلحاقها بكلّ رزمة بيانات في كلّ موجه عبر موجهات الشبكة إلى أن تصل إلى الوجهة المطلوبة حيث تنزع هذه القيمة.

لهذا الوسم صيغة ثابتة يتم إدخالها في بداية كلّ رزمة بيانات عند دخولها شبكة MPLS .

تسمى الموجّهات الخاصّة التي تتمّ فيها عمليّة تبديل الوسوم LSR "موجّهات وسيطيّة"، وتسمى الموجّهات التي تتمّ فيها عمليّة حذف أو إضافة الوسوم إلى رزمة ما LER "موجّهات طرفيّة".

عند مدخل الشبّكة يتمّ فحص وسم الرزمة لتحديد المسار الذي سيتمّ إرسالها فيه، والقيمة الجديدة التي ستستند إليه، وبما أن التّبديل بين الوسوم ثابت ← مسار الرزمة سيعتمد على القيمة البدائيّة له. كلّ الرزم التي يتمّ إرسالها عبر طريق واحد تدعى صفّ التّحويل المتكافئ FEC .

تسمى مسارات تبديل الوسوم LSP :وهي تسلسل من الوسوم عند كلّ عقدة على طول المسار من المنبع إلى الهدف. تخصّص إمّا قبل إرسال البيانات (قيادة متحكّم بها)، أو عند اكتشاف تدفق معيّن للبيانات (قيادة من قبل البيانات).

يتم توزيع الوسوم باستخدام أحد البروتوكولات التالية :

- LDP: بروتوكول توزيع الوسوم.
- RSVP
- OSPF
- تحمل على بروتوكولات توجيه مثل بروتوكول البوابة الخارجيّة BGP.

ث) مكوّنات شبّكة MPLS :

1- شبّكة العملاء C : هي الشبّكة التي يديرها المستخدم النهائيّ (العميل) ولها إمكانيّة الوصول إلى خدمات الطّبقّة الثّالثة في شبّكة MPLS VPN.

2- موجّه الحدّ لشبّكة العميل CER: بوّابة بين شبّكة العملاء وشبّكة ومزوّد الخدمة.
(LER)

3- موجّه الحدّ لشبّكة مزوّد الخدمة PER : يقدّم خدمات ل VPN ومسؤول عن عمليّة توصيل الخدمات.

4- موجّه مزوّد الخدمة P: يعمل بتقنيّة MPLS تكون موزّعة داخل شبّكة مزوّد الخدمة لكن لا تملك آليّة الارتباط الحدوديّ. (LSR)

5-موجّه النظام ذاتيّ الإدارة ASBR: يسمح بإمكانية الاتصال بين الأنظمة المتجاورة.

يعيّن كلّ من LSR, LER التسمية بشكل مستقل ويتم تبادل التسمية بواسطة LDP وبمجرّد إنشاء LDP وبناء كل راوتر جدول إعادة التوجيه MPLS خاصته، سيقوم كلّ من LSR, LER بتنفيذ إعادة التوجيه إمّا IP to label أو label to label أو label to IP .
لا يمكن إنشاء جدول إعادة التوجيه MPLS دون وجود جميع موجّهات MPLS التي تنشأ للتوجيه L3 (OSPF,BGP).

MPLS Label =32bit

| Label value | EXP | أسفل المكّس S | TTL |
|-------------|------|---------------|------|
| 20bit | 3bit | 1bit | 8bit |

S=0 ← ليس الإشعار الأخير بالمكّس.

S=1 ← الإشعار الأخير بالمكّس.

EXP=QOS جودة الخدمة.

(ج) أنواع MPLS VPN:

(1) Point to Point : تستخدم الخطوط المستأجرة الافتراضية VLL لتوفير الاتصال بين موقعين ويمكن تغليف إطارات TDM,Ethernet,ATM ضمن هذه الخطوط.

(2) L2 MPLS VPN : تقسم لنوعين :

1. معتمدة على BGP

2. معتمدة على LDP .

العميل الذي يدير التوجيه، يسمى خدمة VLAN ، توفر خدمة التبديل في السحاب.

(3) L3 MPLS VPN : يتم توجيه العملاء من قبل مزود الخدمة.

بعض العوامل الرئيسية التي يجب مراعاتها عند تحديد ما إذا كانت VPN من موقع إلى آخر مناسبة لشركتك هي:

- حجم العمل.
- عدد من المواقع.
- الانتشار الجغرافي (كم تبعد المواقع عن بعضها البعض).
- متطلبات تقاسم الموارد.

Remote Access VPN1.5.2

يمكن أن تكون الشبكات الافتراضية الخاصة للشركات إما من موقع إلى موقع (توصيل شبكتين محليتين أو أكثر في مواقع مختلفة) أو الوصول عن بعد (توصيل أجهزة الكمبيوتر الفردية بشبكة LAN).
تتيح شبكات VPN البعيدة الوصول للموظفين الوصول إلى الشبكة المحلية لشركتهم من المنزل أو في أي مكان في العالم.

من أجل إعداد VPN الوصول عن بعد ، يجب أن يكون لكل جهاز مستخدم برنامج عميل VPN مثبت ، أو يجب أن يكون لدى المستخدم وصول إلى عميل VPN على شبكة الإنترنت.
عندما يرسل جهاز المستخدم البيانات ، يقوم برنامج عميل VPN بتغليف وتشفير حركة المرور هذه ، ثم يرسلها عبر الإنترنت إلى بوابة VPN الخاصة بشبكة LAN الخاصة بالشركة.

عندما تستقبل عبارة VPN الإرسال المشفّر لأيّ مستخدم بعيد ، فإنّها تقوم بفكّ تشفير حركة المرور على شبكة LAN الخاصة بالشركة وترسلها ، تمامًا كما تفعل بوابة VPN من موقع إلى موقع. مقارنةً بتكوين VPN كامل من موقع إلى آخر ، ستشمل VPN الوصول عن بُعد بعض التنازلات في السرعة والأداء العام للشبكة. ومع ذلك ، بالنسبة للمنظمات الأصغر ، ستكون هذه المشكلات بسيطة للغاية ، وغالبًا لا تكون ملحوظة.

هناك مكوّنان مطلوبان في شبكة افتراضية خاصة للوصول عن بُعد:

- 1- خادم وصول إلى الشبكة (NAS)، يسمّى أيضًا بوابة وسائط أو خادم وصول بعيد.
- 2- برنامج العميل. بمعنى آخر، يحتاج الموظفون الذين يرغبون في استخدام VPN من أجهزة الكمبيوتر الخاصة بهم إلى برامج على أجهزة الكمبيوتر هذه التي يمكنها إنشاء اتّصال بالشبكة الظاهرية الخاصة والحفاظ عليه. تحتوي معظم أنظمة التشغيل اليوم على برنامج مدمج يمكنه الاتّصال بشبكات VPN ذات الوصول عن بُعد ، على الرغم من أنّ بعض شبكات VPN قد تتطلب من المستخدمين تثبيت تطبيق معين بدلاً من ذلك. يقوم برنامج العميل بإعداد الاتّصال التّفقيّ إلى NAS ، والذي يشير إليه المستخدم من خلال عنوان الإنترنت الخاصّ به. يدير البرنامج أيضًا التّشفير المطلوب للحفاظ على الاتّصال آمنًا.

1.5.2.1 SD-WAN VPN

في الماضي، كانت تُهج إدارة الشبكة مصمّمة حول الموظّفين الذين يستخدمون شبكات محلية منفصلة للفروع للوصول إلى التطبيقات المحلية. اليوم، يتمّ استضافة معظم تطبيقات الأعمال في السحابة. أدى هذا التّحوّل إلى SD-WAN VPN ، وهي تقنية VPN بديلة للأعمال وأكثر ديناميكية من VPN الوصول البعيد.

تعمل شبكة SD-WAN (الشبكة الواسعة المعرفة بالبرمجيات) على تبسيط إدارة شبكة WAN وتشغيلها عن طريق فصل أجهزة الشبكات عن آلية التّحكم الخاصة بها (البرمجيات). نظرًا لأنّ المنظمات أصبحت أكثر تفرّقًا جغرافيًا وتستخدم عددًا متزايدًا من التطبيقات المستندة إلى مجموعة النّظر، فإنّ شبكات WAN التقليديّة تكافح من أجل مواكبة كمية البيانات التي يتمّ إرسالها.

تجمع شبكة SD-WAN VPN الجيدة بين مزايا التكلفة لشبكات VPN المستندة إلى موقع على شبكة الإنترنت مع الأداء وخفة الحركة في شبكات MPLS VPN. باستخدام SD-WAN ، يمكن للمؤسسات استبدال بعض دارات MPLS عالية الثمن على الأقل باتصالات إنترنت اقتصادية أكثر. تضمن إمكانيات التحسين والمسارات المتعددة لشبكة SD-WAN بقاء الأداء مرتفعاً بما يكفي لحجم عمل كل موقع، على الرغم من استخدام البنية التحتية العامة للإنترنت.

يمكن أن تكون منتجات SD-WAN عبارة عن أجهزة مادية أو أجهزة افتراضية. يتم وضعها في المكاتب البعيدة والفرعية، ومراكز بيانات الشركة، وعلى نحو متزايد، على المنصات السحابية.

1.5.2.2 Cloud VPN

تتيح الشبكة السحابية VPN للشركات الحفاظ على مواردها السحابية الخاصة وحمايتها من خلال تزويد الموظفين بإمكانية وصول VPN إلى تلك الموارد عبر الإنترنت.

كما يوحي الاسم، فإن Cloud VPN هي بنية تحتية قائمة على السحابة توفر خدمات VPN. تقوم العديد من الشركات بترحيل تطبيقات أعمالها إلى السحابة، ويعتمد الموظفون بشكل متزايد على أجهزتهم المحمولة وأجهزة الكمبيوتر المحمولة للوصول إلى هذه التطبيقات.

يوفر مزودو الخدمات السحابية للأعمال للشركات البنية التحتية للشبكة لتطبيقات المنازل وإتاحتها عن بُعد. ومع ذلك، فهي لا توفر الأمان لأجهزة الجوال والأجهزة المحمولة التي يستخدمها الموظفون (إحضار جهاز خاص بك أو BYOD). سحاب VPN يملأ هذه الفجوة من خلال تأمين أجهزة الموظفين.

تتضمن بعض فوائد شراء خطة VPN للأعمال من مزود VPN للمستهلك ما يلي:

- وظيفة VPN للوصول عن بُعد لتوصيل العمال بشبكة LAN.
- تحسين الأمان لأجهزة الموظفين.
- تشفير البيانات من طرف إلى طرف.
- الوصول الآمن إلى التطبيقات السحابية.

استنتاج

تُمكن الشبكات الافتراضية الخاصة (VPN) من موقع إلى المؤسسات: المؤسسات من الاتصال بشبكات LAN مفصولة جغرافياً بشكل آمن من أجل تزويد الموظفين في جميع المواقع بوصول آمن إلى موارد الشبكة.

1.6 آليات الأمن

لا يمكن لشبكات VPN أن تجعل الاتصالات عبر الإنترنت مجهولة تماماً، لكنها عادة ما تزيد من الخصوصية والأمان. لمنع الإفصاح عن المعلومات الخاصة، تسمح الشبكات الافتراضية الخاصة عادة بالوصول عن بعد المصادق عليه فقط باستخدام بروتوكولات الأنفاق وتقنيات التشفير.

ماذا يوفر نموذج أمان VPN:

1. سرية: بحيث أنه حتى إذا تم استنشاق حركة مرور الشبكة على مستوى الحزمة فإن المهاجم يرى البيانات المشفرة فقط.
2. مصادقة المرسل: لمنع المستخدمين غير المصرح لهم من الوصول إلى VPN.
3. تكامل الرسائل: للكشف عن أي حالات للعبث بالرسائل المرسل.

2 الفصل الثاني: التوجيه

يمكن أن تعمل بروتوكولات الأنفاق في طوبولوجيا شبكة من نقطة إلى نقطة لا يمكن اعتبارها نظرياً VPN لأنّ من المتوقَّع أن تدعم VPN حسب التعريف مجموعات عشوائية ومتغيّرة من عقد الشبكة. ولكن نظراً لأنّ معظم تطبيقات الموجه تدعم واجهة النفق المعرفة بواسطة البرامج، فإنّ شبكات VPN المزودة من قبل العملاء غالباً ما تكون أنفاقاً محدّدة ببساطة تعمل على بروتوكولات التوجيه التقليدية.

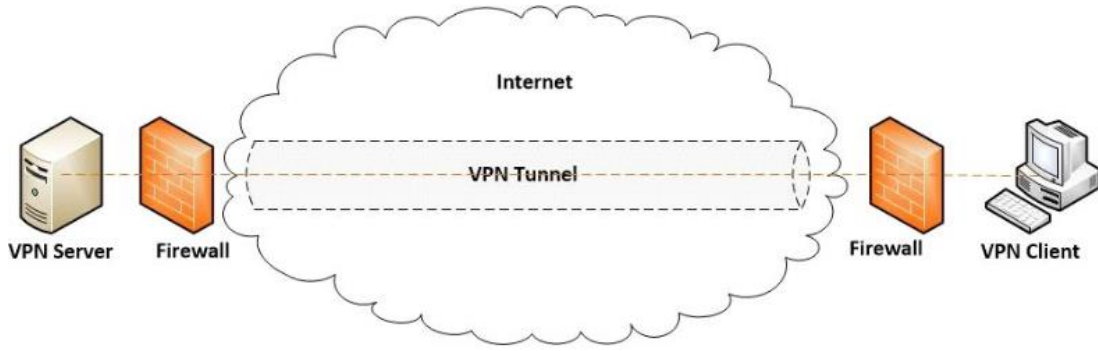
إنّ الشبكات الخاصة الافتراضية (VPN) تستخدم عملية تسمى "حفر الأنفاق" لتوسيع شبكة خاصة عبر شبكة عامة (الإنترنت). الأنفاق هي عملية تشفير البيانات وإبقائها منفصلة عن حركة المرور الأخرى على الإنترنت. إنّهُ يمكن VPN من حماية سرّيّة (تظلّ البيانات سرّيّة) وسلامة (تبقى البيانات دون تغيير) الرسائل أثناء انتقالها عبر الشبكة العامة.

سنقوم في هذا الفصل بشرح VPN tunnelling وأهم بروتوكولات الاتصال النفقية واستعراض ميزات وعيوب كل منها.

2.1 VPN Tunnelling

يصف مصطلح VPN tunnelling عملية يتمّ من خلالها نقل البيانات بأمان من جهاز أو شبكة إلى أخرى من خلال بيئة غير آمنة (مثل الإنترنت) دون المساس بالخصوصيّة. النفق ينطوي على حماية البيانات عن طريق إعادة تعبئتها في شكل مختلف.

في الواقع، لا يوجد نفق ماديّ، بالطبع؛ يجب أن تنتقل البيانات عبر نفس الأسلاك مثل أي بيانات أخرى تمر عبر الشبكة العامّة. بدلاً من ذلك، يستخدم نفق VPN المفاهيم المعروفة باسم تغليف البيانات وتشفيرها لنقل حركة البيانات بأمان عبر البيئة غير الآمنة. يعزل التغليف حزمة البيانات من البيانات الأخرى التي تنتقل عبر نفس الشبكة، في حين أن التشفير يجعل البيانات "غير مرئية" (غير مقروءة) حتّى لوكلاء المراقبة والجرائم الذين يتعرّفون عليها كمعلومات مشقّرة.



الشكل 1-2 VPN tunnelling

إنّ التّشفير يجعل بياناتنا المقروءة (نصّ عاديّ) غير قابلة للقراءة بالكامل (نصّ مشفّر) من قبل أيّ شخص يعترضها، في حين يلفّ التّغليف حزم البيانات بطبقاتٍ متتالية من معلومات التّحكّم بحيث لن يتمّ التّعرف عليها في معظم الحالات على أنّها مشفّرة. يستخدم نفق VPN هذه التّقنيّات لحجب بياناتنا من أجل الحفاظ على خصوصيّة أنشطة التّصفّح الخاصّة بنا وسريّتها.

2.1.1 متطلبات اختيار VPN؟

عند اختيار VPN، من المهمّ بالنّسبة لنا أن نفكّر في الكيفيّة التي ننوي استخدام الخدمة بها، وميّزات الأنفاق الأنسب لذلك الاستخدام.

| VPN use | Most important tunneling feature to have | Why is this important |
|---|---|--|
| Online streaming | Speed and ability to bypass blocking software | Minimize buffering and remove content access restrictions |
| Accessing banned websites | Security with strong encryption | Evade surveillance and bypass content restrictions (censorship) |
| Cloaking VoIP calls | Security with strong encryption | Evade surveillance |
| Public WiFi use | Security and privacy | Protect data that would otherwise be visible to any user of the shared network (WiFi networks are very poorly secured) |
| P2P file sharing | Security and privacy | Evade surveillance, especially tracking of data transmissions |
| Combating ISP bandwidth throttling | Speed | Minimize constant buffering |
| Mixed uses | Ease of switching between different protocols | Want to be able to choose the best protocol for each use |
| Multitasking, including local and remote uses | Split tunneling (detailed explanation below) | Simultaneous access to your local ISP and the VPN server without interruptions |

الشكل 2-2 متطلبات VPN وفق الاستخدام

هناك مميزات VPN متقدمة أخرى ضرورية لفعالية النفق، مثل مفتاح التوقف والنفق المقسم.

أ- مفتاح التوقف

هو إعداد آلية لرصد اتصّالنا بانتظام لأيّ تغييرات في الحالة. إذا لاحظ أيّ انقطاع عن خادم VPN الخاص بنا، فإنّه يقوم تلقائياً بإيقاف جهازنا أو إنهاء تطبيقات معيّنة من الاتّصال بالإنترنت من خلال مزود خدمة الإنترنت الخاص بنا بحيث لا تتعرّض بياناتنا ونشاطنا لعيون المتطفّلين.

هناك أوقات لا نحتاج فيها إلى كلّ حركة بياناتنا للدّهاب عبر نفق VPN الخاص بنا. وهنا يأتي دور مفهوم النفق المقسم.

ب- تقسيم الأنفاق

يمكننا تقسيم الأنفاق بشكل أساسي من توجيهِ بعض أنشطتنا عبر الإنترنت من خلال نفق VPN أثناء الوصول المباشر إلى الإنترنت من خلال موفر خدمة الإنترنت للآخرين. لماذا هذا مهم؟

تتمثل إحدى الوظائف الرئيسية للشبكة الافتراضية الخاصة في تزويدنا بقناة آمنة وخاصة لإرسال المعلومات وتلقيها بشكل مجهول. لكن الحقيقة هي: ليس كل ما نقوم به على الإنترنت يحتاج إلى المرور عبر نفق VPN. على سبيل المثال، هناك أوقات نريد فيها الوصول إلى الأفلام الأجنبية على خدمة بث مثل Netflix وفي نفس الوقت الوصول إلى خدمات الويب المحلية. عندما لا تكون هناك حاجة إلى حماية النفق، يمكن أن تكون الشبكة الظاهرية الخاصة (VPN) اختناقًا يبطئ اتصالننا.

أو نفترض أننا نريد القيام بأنشطة مصرفية عبر الإنترنت مع الحفاظ أيضًا على الوصول إلى خدمات الويب في البلدان الأخرى التي تتطلب استخدام VPN. يمكن وضع علامة على تغيير عنوان IP الخاص بنا (والموقع الظاهري) باستخدام VPN كنشاط مريب من قبل البنك الخاص بنا، مما قد يؤدي في الواقع إلى المزيد من غزوات خصوصيتنا.

في مثل هذه الحالات، يتيح لنا الاتصال التفتي المقسم إمكانية الوصول إلى خدمات الويب التي نريد أو نحتاج إلى حماية نفقها، دون فقدان الوصول المباشر إلى خدمات الويب المحلية. وإلا فسنجد أنفسنا متصلين باستمرار ونقطع اتصالننا بخدمة VPN. إلى جانب ذلك، سيساعدنا تقسيم الأنفاق في الحفاظ على الكثير من النطاق الترددي، حيث لا يلزم مرور حركة الإنترنت الخاصة بنا عبر خادم VPN.

2.1.2 بروتوكولات الاتصال التفتية؟

بروتوكول الاتصال التفتي هو بروتوكول اتصالات يسمح بنقل البيانات من شبكة إلى أخرى. يتضمن السماح بإرسال اتصالات الشبكة الخاصة عبر شبكة عامة (مثل الإنترنت) من خلال عملية تسمى التغليف.

نظرًا لأنّ التّفق ينطوي على إعادة تجميع بيانات حركة المرور في نموذج مختلف، ربّما باستخدام التّشفير كمعيار، فإنّه يمكن إخفاء طبيعة حركة المرور التي يتمّ تشغيلها عبر نفق.

يعمل بروتوكول الاتّصال التّفقيّ باستخدام جزء بيانات الحزمة (الحمولة النّافعة) لحمل الحزم التي توفّر الخدمة بالفعل. يستخدم Tunneling نموذج بروتوكول ذو طبقات مثل تلك الخاصّة بمجموعة بروتوكولات OSI أو TCP / IP ، ولكنّه ينتهك عادة الطّبقة عند استخدام الحمولة النّافعة لنقل خدمة لا تقدّمها الشّبكة عادةً. عادةً ما يعمل بروتوكول التّسليم بمستوى مساوٍ أو أعلى في نموذج الطّبقات من بروتوكول الحمولة النّافعة.

ما الذي نحتاج إلى معرفته عن بروتوكولات الأنفاق؟

يُمنح معظم مزوّد VPN المستخدمين خيارًا للاختيار من بين العديد من بروتوكولات الأنفاق. بروتوكول نفق VPN الذي نحدّده للاستخدام له آثار كبيرة على جودة وأداء التّفق الخاصّ بنا. تتضمّن بعض الأسئلة الرّئيسيّة التي يجب طرحها قبل اختيار بروتوكول نفق ما يلي:

- ما مدى سرعة ذلك؟
- ما مدى أمانها؟
- ما مدى سهولة عرض برنامج الحظر (تجاوز)؟
- ما مدى سهولة الوصول إليها واستخدامها؟

2.1.2.1 أنواع البروتوكولات التّفقيّة:

بروتوكول نفق VPN هو مجموعة من القواعد المتّفقّ عليها لنقل البيانات والتّشفير. تتضمّن بعض البروتوكولات الأكثر استخدامًا بروتوكول الاتّصال التّفقيّ من نقطة إلى نقطة (PPTP) ، بروتوكول نفق الطّبقة الثّانية (L2TP) ، أمان بروتوكول الإنترنت (IPSec) ، بروتوكول نفق مأخذ التّوصيل الآمن (SSTP) ، وفتح (SSL / TLS) VPN .

Point-to-Point Tunneling Protocol (PPTP) –1

تمّ تطوير PPTP بواسطة مجموعة من البائعين بقيادة Microsoft وتمّ تنفيذه في أنظمة تشغيل Microsoft منذ نظام التّشغيل Windows 95. يدعم PPTP موقع VPN بالإضافة إلى الوصول عن بعد عبر الإنترنت.

لذلك يعد PPTP أحد أقدم بروتوكولات نفق VPN وأسرعها وأكثرها استخدامًا وأسهل في الإعداد. من السهل تكوينها لأنها تتطلب اسم مستخدم وكلمة مرور وعنوان خادم فقط لإنشاء نفق إلى الخادم البعيد. إنه واحد من أسرع البروتوكولات بسبب انخفاض مستوى التشفير. لهذا السبب ، فإن PPTP مفيد للتطبيقات التي تكون فيها السرعة أكثر أهمية من الأمان الكامل.

مميزاته : سريع.

موجود مسبقاً على جهاز المستخدم.

سهل التثبيت.

عيوبه: مخترق من قبل وكالة الأمن القومي.

غير آمن.

2- Layer 2 Tunneling Protocol (L2TP)/Internet

Protocol Security (IPSec)

بروتوكول أنفاق الطبقة الثانية: بروتوكول نفقي يدعم VPN وجزء من خدمات التوصيل التي يقدمها مزود الخدمة. لا يدعم أي تشفير للبيانات ويعتمد على بروتوكول تشفير آخر لتأمين خصوصية البيانات مثل IPSec.

يطلب استخدام UDP port 500 (بورت سهل الحجب من قبل جدران الحماية NAT فرمًا تحتاج لعملية تحويل للبورت).

يعتبر امتداد لبروتوكول PPP الذي يدمج أفضل مميزات PPTP و L2F .

يقوم L2TP/IPSec بتغليف البيانات مرتين مما قد يبطئ الاتصال، ومع ذلك يوفر عملية تشفير \ فك تشفير في النواة ويسمح ب multithreading وهذا غير ممكن في OpenVPN .

مميزاته: آمن.

متاح على جميع الأجهزة وأنظمة التشغيل الحديثة.

سهل التثبيت.

عيوبه: أبطأ من OpenVPN

يمكن وجود مشاكل عند استخدامه مع جدران حماية.

يمكن أن يكون مخترق من قبل وكالة الأمن القومي.

3- Internet Key Exchange (IKEv2)/Internet Protocol Security (IPSec)

أحد البروتوكولات الأمنية للاتصالات عبر شبكات IP . يحقق الأهداف التالية:

سرية وصحة وسلامة البيانات المنقولة، كما يحقق التشفير وفك التشفير ومصادقة الحزم وتبادل المفاتيح الآمن وإدارتها.

المنفذ التي يعمل عليها:

UDP port 500 يسمح بإعادة توجيه ISAKMP عبر جدار الحماية.

IP port 50 and 51 : يسمحان بإعادة توجيه حركة مرور ESB and AH على التوالي.

ISAKMP : جمعية أمان الانترنت وبروتوكول إدارة المفاتيح هما مكونان أساسيان لشبكة IPSec VPN التي يجب أن تكون موجودة لتعمل بشكل طبيعي وحماية حركة المرور العامة التي يتم إعادة توجيهها بين العميل وخادم VPN أو خادم VPN إلى خادم VPN .

ESP : بروتوكول أمان التّغليف : يوفّر الحماية لبروتوكولات الطبقة العليا مع وجود منطقة موقّعة تشير إلى مكان توقيع حزمة بيانات محمية لأجل السّلامة، ومنطقة مشقّرة تشير إلى المعلومات المحمية بسريّة.

يحمي حمولة بيانات IP فقط وليس IP header إلى أن يتمّ نفق حزمة البيانات.

يستخدم لضمان السّريّة ومصادقة أصول البيانات وسلامة الاتّصال ودرجة ما من السّريّة على مستوى حركة المرور وخدمة anti-replay (عدم إعادة الإرسال).

يمكن تشفير ومصادقة البيانات أو أحدهما، للتّشفير يمكن اختيار أحد الخوارزميات التّالية : AES, DES, 3DES وهو معيار التّشفير المتقدّم يوفّر قدر أكبر من التّشغيل البيئي مع الأجهزة الأخرى بمفاتيح 128bit, 192bit, 256bit .

AH رأس المصادقة : جزء من IPSec الذي يصادق أصول حزم IP ويضمن سلامة البيانات. يؤكّد على المصدر الأصليّ للترزمة ويضمن عدم تغيير محتوياتها (الرأس + الحمولة) منذ الإرسال.

تتمّ مصادقة الحزمة من خلال المجموع الاختباريّ المحسوب من خلال رمز مصادقة رسالة التّجزئة HMAC باستخدام مفتاح سريّ وخوارزميات تجزئة MD5 أو SHA .

MD5 ملخص الرّسالة: هي خوارزمية تنتج تجزئة 128bit من رسالة ذات طول عشوائيّ ومفتاح 16Byte.

SHA خوارزمية التّجزئة الآمنة: تنتج تجزئة 160bit من رسالة ذات طول عشوائيّ ومفتاح 20Byte ويعتبر أكثر أماناً من MD5 بسبب التّجزئات الأكبر التي ينتجها.

إذا تمّ إنشاء جلسة الأمان يمكن تكوين AH بشكل اختياريّ للدّفاع ضدّ هجمات anti-replay باستخدام تقنية التّأفدة المنزلة.

| | |
|-------------------------|----------------------|
| Clear-text user payload | ترويسة IP الطَّبيعية |
|-------------------------|----------------------|

| | | |
|-------------------------|-----------------|----------------------|
| Clear-text user payload | ترويسة المصادقة | ترويسة IP الطَّبيعية |
|-------------------------|-----------------|----------------------|



| | | |
|----|---|----|
| IC | S | S |
| V | N | PI |

الشكل 2-3 شكل IP Packet في AH

IKE: تبادل مفاتيح الانترنت : وظيفة هذا البروتوكول هي ضمان عملية توزيع مشاركة المفاتيح بين مستخدمي IPsec فهو بروتوكول التفاوض negotiation في نظام IPsec كما يؤكد على طريقة المصادقة والمفاتيح الواجب استخدامها ونوعها.

يعمل IPsec بأحد الوضعين:

1. التَّقْل: عادة يستخدم في LAN يطبق في الحالات التالية:
 - المحادثة بين الأجهزة في داخل أو نفس الشبكة الداخلية الخاصة Private LAN.
 - المحادثة بين جهازين لا يقطع بينهما firewall يعمل على NAT .
2. التَّفَق: يستخدم لتطبيق IPsec بين نقطتين عادة بين راوترين أي WAN يستخدم لتأمين البيانات فقط أثناء مرورها من مناطق غير آمنة كالإنترنت.

Note: طرفا النفق مضيفين ← يمكن استخدام الوضعين.

أحد طرفي النفق عبارة عن بوابة أمان مثل جدار الحماية ← يجب النفق.

يتكوّن نفق IPsec من زوج من SA أحادية الاتجاه (SA لكل اتجاه من النفق) يحدّده الذي يحدّد فهرس بارامترات الأمان SPI وعنوان الوجهة وبروتوكول الأمان AH أو ESP المستخدم.

SA اتفاق الأمان: اتّفاقيّة أحاديّة الاتجاه بين المشاركين في VPN فيما يتعلّق بالأساليب لاستخدامها في أمين قناة اتّصال من خلاله يمكن لنفق IPsec أن يوفّر:

-الخصوصيّة (خلال التّشفير).

-تكامل وسلامة المحتوى (خلال مصادقة البيانات).

-مصادقة المرسل وعدم الإنكار (خلال مصادقة مصدر البيانات).

وتجمع SA المكونات التّالية لتأمين الاتّصالات:

- خوارزميّات ومفاتيح الأمان.
- وضع البروتوكول إمّا نقل أو نفق.
- طريقة إدارة المفاتيح يدويّ أو Autokey.
- عمر SA.

| | AH | ESP | | | | | | | | | | | |
|-----|--|-----|------|-----------|-----------|--|---|-----------|-----------|------|-----------|------|-----------|
| نقل | <table><tr><td>IP</td><td>AH</td><td>TCP</td><td>data</td></tr></table> | IP | AH | TCP | data | <table><tr><td>IP</td><td>ESPheader</td><td>TCP</td><td>data</td><td>ESPtailer</td></tr></table> | IP | ESPheader | TCP | data | ESPtailer | | |
| IP | AH | TCP | data | | | | | | | | | | |
| IP | ESPheader | TCP | data | ESPtailer | | | | | | | | | |
| نفق | <table><tr><td>IP</td><td>AH</td><td>IP</td><td>TCP</td><td>data</td></tr></table> | IP | AH | IP | TCP | data | <table><tr><td>IP</td><td>ESPheader</td><td>IP</td><td>TCP</td><td>data</td><td>ESPtailer</td></tr></table> | IP | ESPheader | IP | TCP | data | ESPtailer |
| IP | AH | IP | TCP | data | | | | | | | | | |
| IP | ESPheader | IP | TCP | data | ESPtailer | | | | | | | | |

الشكل 4-2 IP Packet in AH ,ESP

ملخص لعمل IPSec:

- 1- يرسل جهاز A حزم بيانات عن طريق كابل على الشبكة لجهاز B.
 - 2- يقوم IPSec Driver على A بتحديد أنّ البيانات يجب أن تكون آمنة عند انتقالها من A إلى B.
 - 3- تتم عملية المباحثات negotiation بين الجهازين ويتفقان على استخدام المفتاح المشترك بينهما وعلى المفتاح السري الخاص بالتشفير عن طريق IKE حيث أنّ المفتاح المشترك يكون معلوماً من قبل الطرفين دون انتقاله للشبكة.
 - 4- يعمل IKE نوعين من الاتفاقيات بين الجهازين 2SA (روابط الأمن) :
- النوع الأول: يحدد كفاءة وثوق كلا الجهازين ببعضهما وكفاءة تأمين وحماية حزم البيانات الصادرة منهما.
- النوع الثاني: يحدد كفاءة حماية جزء ونوع محدد من اتصال التطبيق (البرنامج).

5- بعد اكتمال وإنهاء عملية المباحثة بواسطة IKE يتم تمرير مفتاح التشفير من A إلى IPsec Driver ثم يعمل هذا المحرك hash من حزم البيانات الصادرة للحفاظ على مصداقية المعلومة ويعمل على تشفير حزم البيانات للحفاظ على سلامة المعلومات.

6- جميع معدّات الشبكة الأخرى من راوترات وسيرفرات لا تحتاج تطبيق IPsec عليها حيث تتعامل مع حزم IPsec على أنّها حزم عادية وتمرّرها على الشبكة.

7- يفحص IPsec Driver الخاص بالجهاز B حزم البيانات للتأكد من مصداقيتها ويفكّ تشفير محتوياتها ثم يرسل البيانات إلى البرنامج المستقبل لها.

4. Secure Socket Tunneling Protocol (SSTP)

تمّ تطوير بروتوكول نفق مأخذ التوصيل الآمن (SSTP) من قبل Microsoft للمساعدة في حماية أنشطتنا عبر الإنترنت. وهي مدعومة بشكل افتراضي على أنظمة التشغيل Windows 7 و 8 و 10 ، مما يسهّل على مستخدمي Windows الإعداد. ينقل بيانات الإنترنت باستخدام طبقة المقابس الآمنة (SSL) - وهو نفس البروتوكول المستخدم لتشغيل اتصالات الويب الآمنة (HTTPS).

يستخدم SSTP إجراءات تشفير قوية ، مما يجعله بروتوكول VPN الأكثر أماناً المتاح افتراضياً في أنظمة تشغيل Windows ، ويمكن استخدامه بدلاً من PPTP أو IPsec / L2TP. ميزة SSTP عبر PPTP و L2TP هي أنّه لا يمكن حظره بسهولة ، حيث يتمّ نقل حركة المرور عبر اتصال ويب HTTPS الشهير.

5. TLS,SSL:Transport Layer Security,Secure Socket

Layer

بروتوكولات تشفير مصمّمة لتوفير أمان الاتصالات عبر شبكة الكمبيوتر. TLS هو بديل SSL لما يوفّره من أمان أعلى في التشفير حيث يستخدم HMAC.

تعتمد TLS في مبدأ عملها على مجموعة من الجهات الخارجية التي تعتبر مراجع مصدقة وموثوقة لإصدار شهادات الحماية وتسمى CA .

ملخص عمل TLS :

- (1) تبدأ العملية عندما يقوم العميل بالاتصال بالخادم وطلب تبادل البيانات عبر المنفذ الآمن خلال TLS في عملية "المصافحة" ويقوم العميل بإرسال قائمة بطرق التشفير التي يدعمها.
- (2) عندما يستلم الخادم الطلب يبحث في قائمة التشفير المرسلة له للعثور على أحد الطرق التي يدعمها هو أيضاً ويختار إحداها وإشعار العميل بها.
- (3) يقوم الخادم أيضاً بإرسال شهادة المفتاح العام للعميل وتحتوي على اسم الخادم واسم الجهة المصدقة CA على الشهادة المستخدمة والمفتاح العام للتشفير المستخدم.
- (4) عندما يستلم العميل هذه المعلومات يقوم بالمصادقة عليها والتأكد من صحة الشهادة المستخدمة وذلك بمقارنتها بما لديه من شهادات حماية قبل أن يبدأ الاتصال الآمن. وفي حال عدم مطابقتها يتم قطع الاتصال أو ظهور تحذير.
- (5) يولد العميل رقم عشوائي مشفر باستخدام المفتاح العام الذي ورده من الخادم (الذي لا يمكن فك تشفيره إلا باستخدام المفتاح الموجود على الخادم) ويرسله للخادم وذلك ليتم توليد مفتاح الجلسة الذي سيستخدم لتأمين الاتصال.
- (6) يستخدم الطرفان الرقم العشوائي لإنشاء مفتاح جلسة فريد للتشفير وفك تشفير البيانات المتبادلة خلال الجلسة حتى انتهاء الاتصال بينهما.

OpenVPN .6

تقنية مفتوحة المصدر تستخدم بروتوكولات SSL و TLS (على قناة التحكم) ومكتبة OpenSSL . يتطلب هذا البروتوكول درجة عالية من التهيئة ويعمل بشكل مثالي عبر UDP port ولكن يمكن تهيئته وضبطه ليعمل على أي بورت آخر ليجعل من الصعب حجبها. سريع للغاية ويقدم تشفير 256bit.

مكتبة OpenSSL : ميزة رائعة من مميزات هذا البروتوكول وتحتوي العديد من خوارزميات التشفير مثل 3DES, AES, Blowfish, Camellia ..

تعتبر خوارزميتا AES, Blowfish مستخدمتان بشكلٍ خصوصيٍّ من قبل مزوّديّ خدمة VPN . Blowfish تعتبر آمنة وتقدّم تشفير 128bit لكن لديها نقاط ضعف. AES أحدث التّقنيّات المتاحة تتعامل مع ملفّات أكبر حجماً من Blowfish بفضل حجم الحجب 128bit الذي تتمتّع به بينما حجم حجب 64bit Blowfish.

مميزاته: لديه القدرة على التّعامل مع أغلب جدران الحماية.

قابل للإعداد والتّهيئة المخصّصة.

يمكن معالجة عيوبه وثغراته كونه مفتوح المصدر.

متوافق مع العديد من خوارزميّات التّشفير.

آمن لدرجة كبيرة.

عيوبه: عمليات التّثبيت خادعة .

يتطلّب برنامج يعمل كطرف ثالث.

يحتاج بعض التّحسينات ليدعم على أجهزة المحمول.

يوضح الشكل 5-2 VPN Tunnelling Protocols مقارنة بين البروتوكولات النفقية

| VPN Tunneling Protocol | | | | | |
|------------------------|---------------------------------------|---------------------------------------|---|---|---|
| Features | PPTP | L2TP/IPSec | IKEv2/IPSec | SSTP | Open VPN |
| <i>Ease of setup</i> | Very easy | Easy | Easy | Easy | Tricky on its own, but easy if you use a good VPN |
| <i>Stability</i> | Struggles with most blocking software | Struggles with most blocking software | Struggles with some blocking software | Bypasses most blocking software | Bypasses most blocking software |
| <i>Encryption</i> | Basic | Strong | Very strong | Very strong | Very strong |
| <i>Speed</i> | Fast | A bit slow | Fast | Fast | Best performance |
| <i>Security</i> | Not secure | Secure but may be breakable | Very secure, but users are not free to access the codes to verify security claims | Very secure, but users are not free to access the codes to verify security claims | Very secure, and anyone is free to access the codes to verify security claims |
| <i>Compatibility</i> | Window, Mac OS, Linux, etc. | Window, Mac OS, Linux, etc. | Window, Mac OS, Linux, etc. | Windows only | Window, Mac OS, Linux, etc. |

الشكل 5-2 VPN Tunnelling Protocols

3 الفصل الثالث: وظائف VPN

تقدم تقنية VPN العديد من المزايا والوظائف المفيدة التي تؤمن سرية وسلامة البيانات المرسلة وتضمن عدم تعرضها للاختراق أو الكشف.

سنوضح في هذا الفصل الوظائف التي تقدمها تقنية VPN وما هي الخوارزميات والطرق التي تعتمد عليها في تحقيق تلك الوظائف.

Confidentiality 3.1

سرية البيانات يتم تحقيقها بخوارزميات التشفير والتي تقسم حسب نوع مفتاح التشفير وفك التشفير إلى نوعين: المتناظر وغير المتناظر، بالإضافة إلى نوع لا يحتاج إلى مفتاح تشفير وهو دالة هاش التشفيرية.

3.1.1 التشفير المتناظر

خوارزمية التشفير المتناظر تعني استخدام نفس المفتاح في التشفير وفك التشفير. يقوم نظام التعمية المتماثل symmetric systems باستخدام نفس المفتاح في التشفير وفك التشفير. من مزايا التشفير المتماثل أنه سهل الاستعمال وسريع ولكن لديه عيب مهم "خصوصاً حين يستخدم في الشبكات الكبيرة" وهو توزيع المفاتيح بين طرفي عملية التواصل على الشبكة اللذين يستخدمان عملية التشفير.

تعتمد قوة وفعالية التشفير على عاملين أساسيين:

أ) الخوارزمية.

ب) طول المفتاح مقدراً بالبت bit، كلما زاد البت، زادت نسبة الأمان وصعوبة فك الشيفرة.

من الأمثلة على الخوارزميات التي تستخدم التشفير المتناظر AES, 3DES, DES.

3.1.1.1 3DES

يستخدم Triple DES ثلاثة مفاتيح فردية مع 56 بت لكل منها، يضيف إجمالي طول المفتاح ما يصل إلى 168 بت.

كيف تتم عملية تشفير النصّ الواضح في Triple Des؟

- 1- تشفير كتل النصّ الواضح باستخدام (Single Des Block With key 56 bit (k1).
- 2- تشفير خرج (Output) العملية الأولى من جديد باستخدام (Single Des Block With key 56 bit (k2).
- 3- تشفير خرج العملية الثانية من جديد باستخدام (Single Des Block With key 56 bit (k3).
- 4- الخرج النهائي هو النصّ المشفّر (Ciphertext) .

3.1.1.2 Blowfish

السّمة المتفخخة هي خوارزمية أخرى مصمّمة لتحلّ محلّ DES ، يقوم هذا التّشفير المتماثل بتقسيم الرّسائل إلى كتل من 64 بت ويقوم بتشفيرها بشكلٍ فرديّ.

3.1.1.3 معيار التشفير المتقدم (AES)

هو خوارزمية موثوق بها كمعيار من قبل حكومة الولايات المتّحدة والعديد من المنظّمات. على الرّغم من أنّها فعّالة للغاية في شكل 128 بت، تستخدم AES أيضاً مفاتيح 192 و 256 بت لأغراض تشفير الخدمة الشّاقة. يُعتبر AES منيعاً إلى حدّ كبير لجميع الهجمات، باستثناء القوّة العاشمة، التي تحاول فكّ تشفير الرّسائل باستخدام جميع التّوليفات الممكنة في تشفير 128 أو 192 أو 256 بت،

3.1.2 التّشفير غير المتناظر

خوارزمية التّشفير غير المتناظر أو المفتاح العام يستخدم مفتاح للتّشفير وآخر لفكّ التّشفير، فهو يقوم بتوليد مفاتيح مختلفة ثم استخدامها في تشفير وفكّ تشفير زوجين من مفاتيح الحماية. وباستخدام هذين الزوجين من المفاتيح، أحدهما عام public والآخر خاصّ private ، يستطيع مفتاح واحد

منهما فقط أن يقوم بفك الشفرة التي ينشئها الآخر. ومن غير المرجح أن تؤدي معرفة مفتاح واحد فقط إلى تحديد المفتاح الآخر، ولهذا يتم استخدام نظام التعمية غير المتماثل في إنشاء التوقيعات الرقمية ونقل المفاتيح المتماثلة.

من الأمثلة على الخوارزميات التي تستخدم المفتاح المتناظر خوارزمية RSA.

3.1.2.1 RSA

RSA هي خوارزمية تشفير المفتاح العام ومعيّار تشفير البيانات المرسلة عبر الإنترنت، على عكس Triple DES، تعتبر RSA خوارزمية غير متماثلة نظراً لاستخدامها زوج من المفاتيح، لديك مفتاحك العام، وهو ما نستخدمه لتشفير رسالتنا، ومفتاح خاص لفك تشفيره، نتيجة تشفير RSA عبارة عن مجموعة ضخمة من mumbo jumbo والتي تستغرق المهاجمين وقتاً طويلاً وقدرة معالجة لاختراقها.

Note : لتحقيق الأداء الجيد مع الأمان نستخدم :

← المفتاح يشفر ب asymmetric.

← البيانات تشفر ب symmetric.

3.2 Authentication

لدينا طريقتين للتحكم :

Pre-shared key : نضع للأجهزة نفس المفتاح من أجل المصادقة ونقوم بتغييره كل فترة.

public key infrastructure : نقوم بوضع مفتاح المصادقة في وثيقة الأمان ونرسله للأجهزة وذلك لتسهيل الأمر.

3.3 Integrity:

أي صحة البيانات وعدم تعرضها للتلاعب .

3.3.1 خوارزمية التجزئة

هدف خوارزمية التجزئة هو إنشاء تجزئة آمنة؛ ولكن ما هي التجزئة؟ التجزئة هي قيمة محسوبة من رقم إدخال أساسي باستخدام دالة التجزئة. إنها خوارزمية رياضية تعين البيانات ذات الحجم التعسفي إلى تجزئة بحجم ثابت. تم تصميمه ليكون وظيفة أحادية الاتجاه، غير قابلة للتحويل. ومع ذلك، في السنوات الأخيرة تم اختراق العديد من خوارزميات التجزئة. حدث هذا ل MD5.

يجب أن تكون الخوارزمية سريعة لحساب قيمة التجزئة لأي نوع من البيانات؛ يجب أن يكون من المستحيل تحديد رسالة من قيمة التجزئة (هجوم القوة الغاشمة كخيار وحيد)؛ يجب أن يتجنب تصادم التجزئة، كل رسالة لها تجزئة خاصة بها؛ كل تغيير للرسالة، حتى أصغرها، يجب أن يغير قيمة التجزئة. يجب أن يكون مختلفاً تماماً. يمكننا استخدامها للتوقيعات الرقمية ورموز مصادقة الرسائل (MACs) وأشكال أخرى من المصادقة. يمكننا أيضاً استخدامها لفهرسة البيانات في جداول التجزئة، وبصمات الأصابع وتحديد الملفات، والكشف عن التكرارات أو كمجموع اختباري.

كيف تعمل؟

قبل إرسال ملف، يستخدم المستخدم 1 خوارزمية التجزئة لإنشاء المجموع الاختباري للملف. ثم يرسله مع الملف نفسه. يتلقى المستخدم 2 كلاً من الملف والمجموع الاختباري. يمكنه الآن استخدام خوارزمية التجزئة نفسها في الملف المستلم.

أشهر خوارزميات التجزئة: دالة هاش التشفيرية .

3.3.1.1 دالة هاش التشفيرية

هي دالة تأخذ أي عدد من قطع البيانات وتعيد سلسلة ثابتة الطول من البتات تسمى قيمة هاش التشفيرية، بحيث أن أي تغيير في البيانات الأصلية (عرضياً أو متعمداً) سوف يؤدي إلى تغيير كبير في قيمة هاش التشفيرية (باحتمال كبير جداً). عادة تسمى البيانات المشفرة "الرسالة" ومقدار هاش التشفيري يسمى الخلاصة. (Digest)

هذا النوع من الخوارزميات لا يحتاج إلى مفتاح تشفير لأنه لا يستخدم لتشفير النصوص وإنما للتأكد من أن محتوى الرسالة موثوق ولم يتم التعديل عليه. وذلك بمقارنة الخلاصة المرسلّة مع الخلاصة المولدة من الرسالة المطلوب التأكد من صحّة محتواها.

من الأمثلة على دالة هاش التشفيرية خوارزميات MD5, SHA1, SHA2..

MD5 3.3.1.1.1

تعالج خوارزمية تجزئة رسالة MD5 البيانات في كتل 512 بت، مقسمة إلى 16 كلمة تتكوّن من 32 بت لكل منها. الإخراج من MD5 هو قيمة تلخيص رسالة 128 بت بسبب الثغرات الواسعة، فقد تمّ اختراقه.

يتمّ حساب قيمة ملخص MD5 في مراحل منفصلة تعالج كل كتلة 512 بت من البيانات جنباً إلى جنب مع القيمة المحسوبة في المرحلة السابقة. تبدأ المرحلة الأولى بقيم ملخص الرسالة التي تمت تهيئتها باستخدام القيم العددية السداسية المتتالية. تتضمن كل مرحلة أربعة تمريرات ملخص الرسائل التي تتعامل مع القيم الموجودة في كتلة البيانات الحالية والقيم التي تتم معالجتها من الكتلة السابقة. تصبح القيمة النهائية المحسوبة من الكتلة الأخيرة هضم MD5 لتلك الكتلة.

الهدف من أي وظيفة ملخص الرسالة هو إنتاج ملخصات تبدو عشوائية. لكي يتم اعتبارها آمنة تشفيرياً، يجب أن تستوفي وظيفة التجزئة متطلّين: أولاً، أنه من المستحيل على المهاجم إنشاء رسالة تطابق قيمة تجزئة معينة؛ وثانياً، أنه من المستحيل على المهاجم إنشاء رسالتين تنتجان نفس قيمة التجزئة.

SHA-family 3.3.1.1.2

خوارزمية التجزئة الآمنة هي وظيفة تجزئة مشفرة تمّ تصميمها بواسطة وكالة الأمن القومي الأمريكية. تمّ تصميم خوارزمية التجزئة المشفرة لتوفير تعيين عشوائي من سلسلة بيانات ثنائية إلى "ملخص الرسالة" ذي الحجم الثابت وتحقيق خصائص أمان معينة. يمكن استخدام خوارزميات التجزئة للتوقيعات الرقمية

ورمز مصادقة الرسائل ووظائف الاشتقاق الرئيسية والوظائف العشوائية الزائفة والعديد من تطبيقات الأمان الأخرى.

تم اختراق SHA-0 منذ سنوات عديدة. ينتج SHA-1 قيمة تجزئة 160 بت (20 بايت). يتم تقديمه عادةً على شكل رقم سداسي عشري يتكوّن من 40 رقماً. تم اختراقه في عام 2005 ولكن "موته" الحقيقي حدث في عام 2010 عندما بدأت العديد من المنظّمات في التوصية باستبدالها.

حالياً تعتبر SHA-2 أكثر أماناً. تتضمن SHA-2 عدّة تغييرات مهمّة.

لدى عائلتها ستّ وظائف تجزئة مع ملحّصات SHA-224 : ، SHA-256 أو 512 بت SHA-224 : ، SHA-256 ، SHA-384 ، SHA-512 ، SHA-512/224 ، SHA-512/256. ،

إنّ SHA-2 أكثر تعقيداً بكثير ولا تزال تعتبر آمنة. ومع ذلك، تشترك SHA-2 في نفس الهيكل والعمليات الرياضيّة مثل سابقتها (SHA-1).

SHA-3

أسرع بشكل ملحوظ من SHA-2 (من 25% إلى 80% ، اعتماداً على التنفيذ). يستخدم بناء الإسفنج. يتمّ امتصاص البيانات أولاً في "الإسفنج" والنتيجة هي "الضّغط".

اقترح مؤلّفو SHA-3 ميزات إضافية مثل نظام التّشفير المصدّق ونظام تجزئة الأشجار، لكن لم يتمّ توحيدها بعد. مع ذلك، إنّها خوارزمية التّجزئة الأكثر أماناً في الوقت الحاليّ.

يعتبر SHA-3 مثاليّاً لتأمين الأنظمة الفرعية المضمّنة وأجهزة الاستشعار والأجهزة الإلكترونيّة الاستهلاكيّة والأنظمة الأخرى التي تستخدم أكواد مصادقة الرسائل القائمة على المفاتيح المتماثلة (MACs). كما أنّ الخوارزمية أسرع من سابقتها.

يوفّر SHA-3 وظيفة آمنة أحاديّة الاتجاه. هذا يعني أنّه لا يمكننا إعادة بناء بيانات الإدخال من

إخراج التجزئة، ولا يمكننا تغيير بيانات الإدخال دون تغيير التجزئة. لن نجد أيضاً أي بيانات أخرى بنفس التجزئة أو أي مجموعتين من البيانات بنفس التجزئة.

3.3.2 خوارزميات المصادقة

تتحقق خوارزميات المصادقة من تكامل البيانات وصحة الرسالة. يدعم برنامج Firewall ثلاث خوارزميات مصادقة HMAC-MD5 و HMAC-SHA1 و HMAC-SHA2 (وهي اختصار لـ "رمز مصادقة الرسالة استناداً على التجزئة ذات المفتاح أو رمز مصادقة الرسالة استناداً على التجزئة هاش) هي نوع معين من رمز مصادقة الرسالة (MAC) متضمنة لدالة التجزئة التشفيرية ومفتاح تشفير سري.

كما هو الحال مع أي رمز مصادقة الرسالة (MAC) يمكن استخدامه للتحقق من سلامة البيانات ومن صحة الرسالة في الوقت ذاته.

يمكن استخدام أية دالة تجزئة تشفيرية كـ (SHA-256 أو SHA-3 في حساب HMAC (رمز مصادقة الرسالة استناداً على التجزئة .

وتسمى خوارزمية MAC الناتجة HMAC-X ، حيث أن X تعبر عن دالة التجزئة المستخدمة) مثال HMAC-SHA256 أو HMAC-SHA3

تعتمد قوة التشفير في ال HMAC على قوة تشفير دالة التجزئة المستخدمة، وعلى حجم خرج التجزئة، وعلى حجم ونوعية المفتاح.

يستخدم HMAC مرورين (دورتين) في حساب التجزئة. أولاً يستخدم المفتاح السري ليتم اشتقاق مفتاحين منه – أحدهما داخلي والآخر خارجي.

وهكذا توفر الخوارزمية حصانة أفضل ضدّ هجمات تمديد الطول (length extension attacks).

تجزأ دالة التجزئة التكرارية الرسالة إلى عدّة كتل ذات حجم ثابت وتكرر عليهم بوساطة دالة ضغط على سبيل المثال: يعمل SHA-256 على كتل 512-بت.

حجم خرج ال HMAC يساوي حجم دالة التجزئة المستخدمة . مثال: 256 و 1600 بت في حالة SHA-256 و SHA-3 على التوالي، على الرغم من أنّه يمكن اقتطاعه عند الرغبة. ال HMAC لا يقوم بتشفير الرسالة. عوضاً عن ذلك، يجب إرسال الرسالة (سواء كانت مشفرة أم لا) إلى جانب تجزئة/هاش ال HMAC.

ستقوم الأطراف التي تحتوي على المفتاح السري بتجزئة الرسالة مرة أخرى بأنفسهم، وإذا كانت الرسالة أصلية، فستطابق التجزئتان المستلمة والمحسوبة.

Anti-replay 3.4

عدم قبول إعادة إرسال البيانات أي منع الدخول في جلسة الاتصال حيث يكون لكل جلسة رقم تسلسلي مختلف.

4 الفصل الرابع: عمل IPSec

بروتوكول IPSec من البروتوكولات الأمنية للاتصالات عبر شبكات IP الذي يضمن سرية وسلامة البيانات حيث يقوم بتشفير كل البيانات المنقولة بالتالي يضمن عدم تعرضها للاختراق. يوضح هذا الفصل أوضاع عمل IPSec والخطوات المتبعة في إعدادة على أجهزة التوجيه في الشبكة.

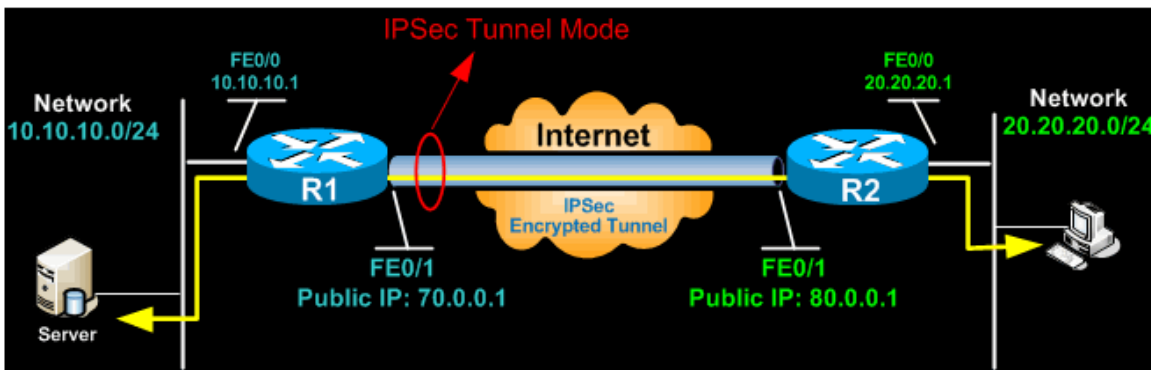
4.1 أوضاع عمل IPSec

يعمل IPSec بأحد الوضعين: وضع النفق ، وضع النقل.

4.1.1 وضع نفق IPSEC

وضع نفق IPSec هو الوضع الافتراضي. باستخدام وضع التّفق، تتم حماية حزمة IP الأصلية بالكامل بواسطة IPSec. وهذا يعني أن IPSec يغلف الحزمة الأصلية، ويشفرها، ويضيف رأس IP جديداً ويرسلها إلى الجانب الآخر من نفق VPN (نظير IPSec).

يتم استخدام وضع التّفق بشكل شائع بين البوابات (موجهات Cisco أو جدران الحماية ASA)، أو في المحطة الطرفية للبوابة حيث تعمل البوابة كوكيل للمضيفين خلفها.

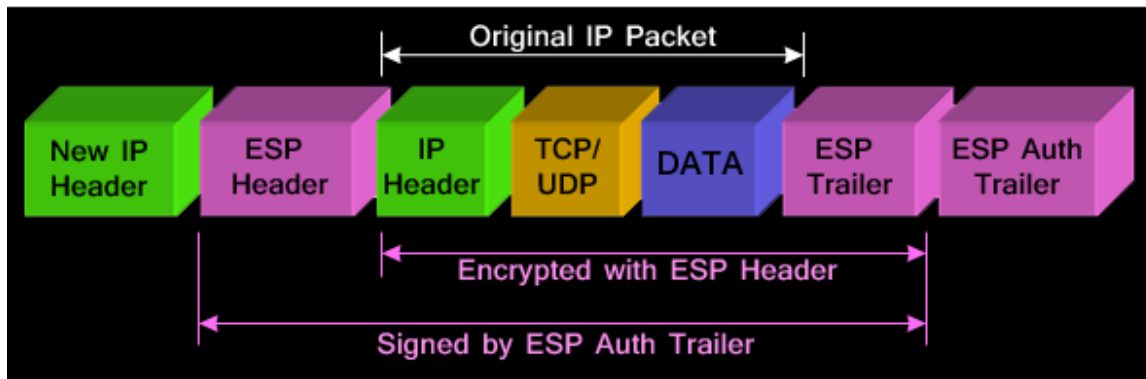


الشكل 4-1 IPSec Tunnel Mode

مثال على وضع النفق هو نفق IPsec بين عميل VPN Cisco و بوابة IPsec (مثل ASA5510 أو PIX Firewall). يتصل العميل ببوابة IPsec. يتم تشفير حركة المرور من العميل وتغليفها داخل حزمة IP جديدة وإرسالها إلى الطرف الآخر. بمجرد فك تشفير جهاز الجدار الناري، يتم إرسال حزمة IP الأصلية للعميل إلى الشبكة المحلية.

في وضع النفق ، يتم إدراج رأس IPsec (رأس AH أو ESP) بين رأس IP وبروتوكول الطبقة العليا. بين AH و ESP ، يُستخدم ESP بشكل شائع في تكوين IPsec VPN Tunnel.

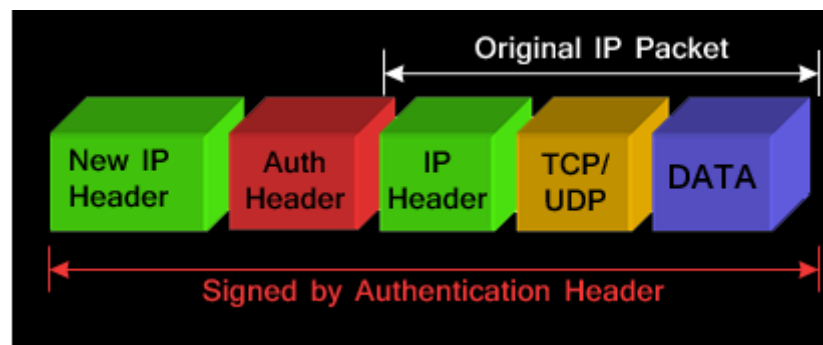
يوضح الشكل 2-4 IP Packet of IPsec Tunnel with ESP للحزمة أدناه وضع نفق IPsec برأس ESP



الشكل 2-4 IP Packet of IPsec Tunnel with ESP

يتم تعريف ESP في رأس IP الجديد بمعرف بروتوكول IP 50.

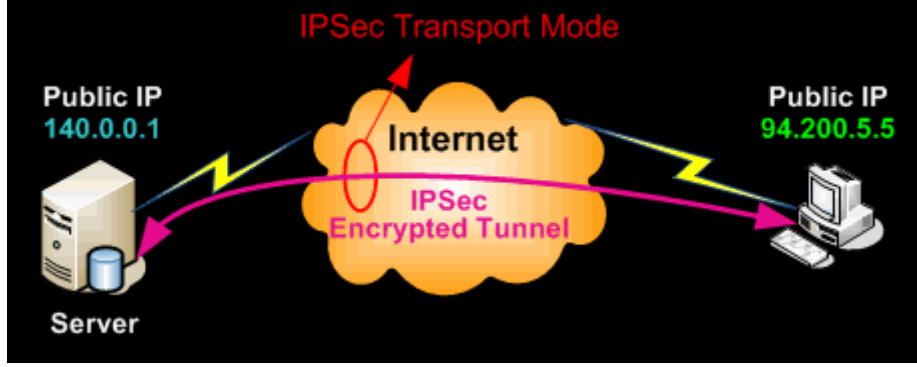
يوضح الشكل 3-4 IP Packet of IPsec Tunnel with AH للحزمة أدناه وضع نفق IPsec برأس AH:



الشكل 3-4 IP Packet of IPsec Tunnel with AH

4.1.2 وضع النقل IPSEC

يتم استخدام وضع النقل IPsec للاتصالات من طرف إلى طرف، على سبيل المثال، للاتصال بين العميل والخادم أو بين محطة العمل والبوابة (إذا كانت البوابة تُعامل كمضيف). من الأمثلة الجيدة على ذلك جلسة Telnet أو Remote Desktop المشفرة من محطة عمل إلى خادم.

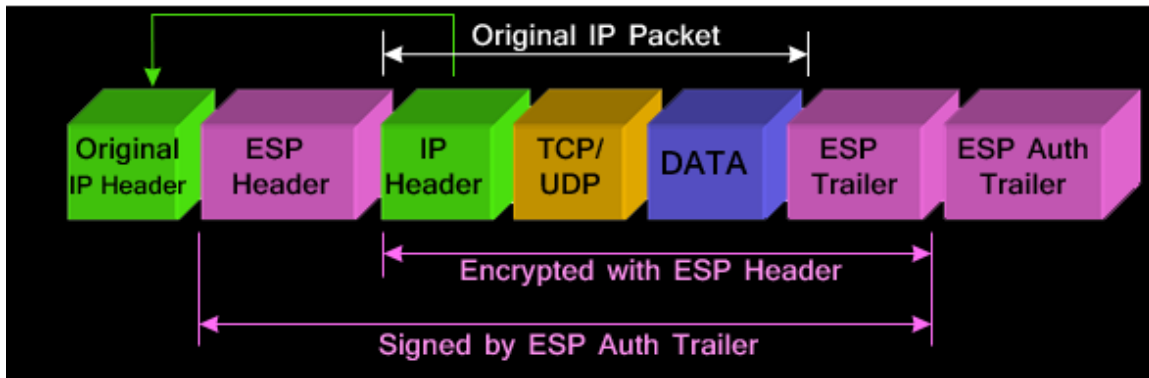


الشكل 4-4 IPsec Transport Mode

يوفر وضع النقل حماية لبياناتنا، والمعروفة أيضاً باسم IP Payload ، ويتكوّن من رأس TCP / UDP + البيانات ، من خلال رأس AH أو ESP. يتم تغليف الحمولة بواسطة رؤوس ومقطورات IPsec. تظلّ رؤوس IP الأصلية كما هي، باستثناء أنّه تمّ تغيير حقل بروتوكول IP إلى ESP (50) أو AH (51)، ويتم حفظ قيمة البروتوكول الأصلي في مقطع دعائيّ IPsec ليتمّ استعادته عند فكّ تشفير الحزمة.

يتم استخدام وضع النقل IPsec عادةً عند استخدام بروتوكول نفق آخر (مثل GRE) لتغليف حزمة بيانات IP أولاً، ثمّ يتم استخدام IPsec لحماية حزم نفق GRE.

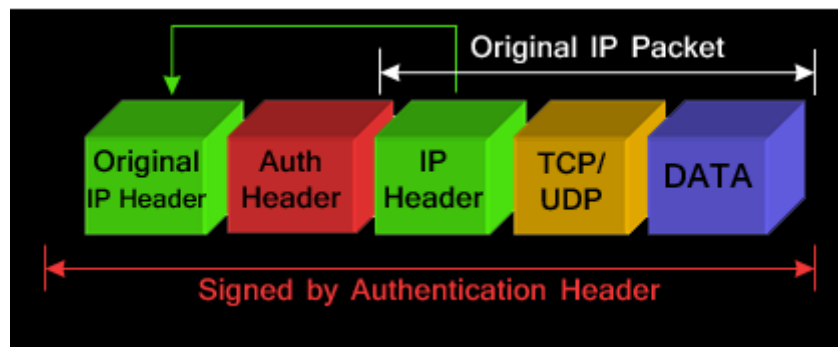
يوضّح الشكل 5-4 للحزمة أدناه وضع النقل IPsec برأس ESP:



الشكل 5-4 IP Packet of IPsec Transport with ESP

لاحظ أنه تم نقل رأس IP الأصلي إلى الأمام. يثبت وضع رأس IP الخاص بالمرسل في المقدمة (مع تغييرات طفيفة في معرف البروتوكول) أن وضع النقل لا يوفر الحماية أو التشفير لرأس IP الأصلي ويتم التعرف على ESP في رأس IP الجديد بمعرف بروتوكول IP 50.

يوضح الشكل 6-4 للحزمة أدناه وضع النقل IPsec برأس AH:



الشكل 6-4 IP Packet of IPsec Transport with AH

4.2 إعداد IPsec

لإعداد IPsec يجب اتباع الخطوات التالية:

4.2.1 ACL: Access List

هي من أبسط أدوات الحماية وتستخدم للتحكم بمنع أو السماح بمرور البيانات (Traffics) من وإلى أجهزة الشبكة كال Routers و Firewalls بناءً على مجموعة من المعايير لتحقيق شرط توافق

ال IP المرسل أو توافيقها مع إغلاق أو السماح ل Port معين، أو تطبيق المنع والسماح ضمن أوقات معينة خلال الأسبوع.

يقوم الموجه بتجاهل وفترة حزم البيانات حسب مجموعة من المعايير التي يحددها مدير الشبكة.

1. معايير ACL :

- منع القراصنة من الدخول للشبكة.
- وعدم السماح للموظفين من استخدام بعض أجزاء النظام وغيرها.

يمكن استخدام ال ACL ضمن ال Firewall Router الذي يقع بين الشبكة الداخلية والشبكة الخارجية التي يمكن أن تكون الإنترنت أو يمكن استخدامها ضمن ال Router الموجود بين طرفي شبكتين داخليتين للتحكم بمرور ال Traffic لأجزاء معينة من هاتين الشبكتين.

2. أنواع ACL :

لإنشاء ال ACL فسطر الأوامر يبدأ ب access-list وتتبعها إما كلمة السماح (Permit) (تعني السماح بمرور البيانات بدون فترة) أو المنع (Deny) تعني فترة البيانات قبل عبورها جهاز الموجه. مع كتابة رقم يدل على نوع access-list. حيث له نوعان:

- *Standard* يستخدم في تقييمه لل Packet عنوان الجهاز المرسل بالتالي يعمل فقط على المستوى الثالث من الطبقات السبعة وهو ال Network Layer وله مجالين من 1 ولغاية 99 أو من 1300 ولغاية 1999.
- *Extended* النوع الثاني يستخدم في تقييمه لل Packet العديد من الأمور، مثل: عنوان المرسل، عنوان المستقبل، نوع بروتوكول معين في المستوى الرابع أو Transport Layer، رقم Port للجهاز المرسل، رقم البورت للجهاز المستقبل بالتالي يتحكم بمستويين من مستويات الطبقات السبعة وهما The Network Layer و The Transport Layer ، وأيضاً له مجالين من 100 ولغاية 199 أو المجال من 2000 ولغاية 2699.

```
R1(config)#access-list 100 permit ip 192.168.1.0
0.0.0.255 192.168.3.0. 0.0.0.255
```

ISAKMP4.2.2

تحدّد ISAKMP الإجراءات وتنسيقات الحزم لإنشاء اقترانات الأمان والتفاوض عليها وتعديلها وحذفها. تحتوي SA على كافة المعلومات المطلوبة لتنفيذ خدمات أمان الشبكة المختلفة، مثل خدمات طبقة IP (مثل مصادقة الرأس وتغليف الحمولة) أو خدمات طبقة النقل أو التطبيق أو الحماية الذاتية لحركة التفاوض. تحدّد ISAKMP الحمولات لتبادل بيانات إنشاء المفاتيح والمصادقة. توفر هذه التّنسيقات إطار عمل متسق لنقل بيانات المفتاح والمصادقة بشكل مستقلّ عن تقنية إنشاء المفاتيح وخوارزمية التّشفير وآلية المصادقة. تستخدم ISAKMP عادةً IKE لتبادل المفاتيح. يتمّ تشكيل SA الأولي باستخدام هذا البروتوكول. يمكن أن يكون لدينا أكثر من سياسة على جهاز التوجيه الخاص بنا. قد نحتاج إلى القيام بذلك إذا كان جهاز التوجيه الخاص بنا يحتوي على نظراء متعدّدين ولدى كلّ نظير قدرات مختلفة أو تكوينات سياسة.

4.2.2.1 IKE Phase1

ينشئ زميلان ISAKMP قناة آمنة ومصدّق عليها. تُعرف هذه القناة ISAKMP SA.

لتكوين IKE المرحلة الأولى، تحتاج إلى تكوين سياسات ISAKMP.

يحتوي نهج ISAKMP / IKE واحد على المعلومات التالية: تحديد الأولويات أو رقم التسلسل وخوارزمية التّشفير ووظيفة التجزئة وطريقة المصادقة ومجموعة مفاتيح DH وعمر الاتصال.

إنشاء سياسة:

1. رقم الأولوية:

قد تحتاج إلى عدّة سياسات ISAKMP. يتمّ تعيين رقم أولوية فريد لكل سياسة ISAKMP بين 1 و 10000. تعتبر السياسة ذات الأولوية رقم 1 هي السياسة ذات الأولوية القصوى. يبدأ التفاوض بشأن السياسة برقم الوثيقة الأقرب إلى 1. من الشائع بدء ترقيم السياسة عند 10.

R1(config)# crypto isakmp policy 10

2. خوارزمية التشفير.

R1(config-isakmp)# encryption [aes | aes-192 | aes-256 |
des | 3des]

3. معلمة المصادقة:

يُدعم IOS ثلاثة توقيعات RSA للمصادقة، RSA nonces ومفاتيح مشتركة مسبقاً.

- يؤدي استخدام توقيعات RSA للمصادقة إلى تكوين الموجه لاستخدام المصادقة المستندة إلى شهادة X.509. هذا هو الخيار الأكثر أماناً، ولكنه يتطلب نشر وإدارة خادم مرجع مصدق.
- يمكن أيضاً استخدام RSA nonces هو رقم عشوائي يتم إنشاؤه بواسطة بادئ IKE، مشفراً بالمفتاح العام للمستلم. الجانب الإيجابي في استخدام nonces RSA هو أنها آمنة للغاية، كما أنها لا تتطلب خادم مرجع مصدق. الجانب السلبي هو أن التظير يحتاج إلى المفاتيح العامة لجميع النظراء الآخرين الذين يتواصل معهم. وهذا يعني وجود درجة من تكلفة العمالة في استخدام هذه الطريقة.
- الخيار الأخير هو المفاتيح المشتركة مسبقاً. تُستخدم المفاتيح المشتركة مسبقاً لدعم الشبكات الافتراضية الخاصة من موقع إلى موقع ومن عميل إلى موقع، في حين يتم استخدام الخيارين السابقين بدقة لتكوينات الهيكلية من موقع إلى موقع. على الرغم من أن المفاتيح المشتركة مسبقاً هي الطريقة الأقل أماناً، إلا أنها أيضاً الأكثر استخداماً لمصادقة أقران البوابة هذا لأنه سريع وسهل الإعداد.

في تكوين عميل IPsec، تتم إدارة المفاتيح المشتركة مسبقاً باستخدام المصادقة الموسعة IKE (Xauth)، وهي طريقة مصادقة ثنائية باستخدام مستخدم وكلمة مرور مجموعة للمصادقة. تعمل كلمة مرور المجموعة بشكل أساسي كمفتاح مشترك مسبقاً، وهي قيمة مشتركة يستخدمها جميع العملاء والبوابة، بينما تكون كلمة مرور المستخدم فريدة فقط للعميل المحدد.

R1(config-isakmp)# authentication [pre-share | crack |
rsa-sig]

4. معامل (Diffie-Hellman (DH)

خوارزمية تبادل المفاتيح هي طريقة لتبادل مفاتيح التشفير بأمان عبر قناة اتصالات عامة. لا يتم تبادل المفاتيح في الواقع - يتم اشتقاقها بشكل مشترك.

في حين أن تبادل مفاتيح Diffie-Hellman قد يبدو معقدًا، إلا أنه جزء أساسي من تبادل البيانات بأمان عبر الإنترنت. طالما تم تنفيذه جنباً إلى جنب مع طريقة المصادقة المناسبة وتم اختيار الأرقام بشكل صحيح، فإنها لا تعتبر عرضة للهجوم.

يوجد عدة تعريفات (مجموعات)، تُستخدم مجموعات Diffie-Hellman لتحديد قوة المفتاح المستخدم في عملية تبادل مفاتيح Diffie-Hellman. تعتبر أرقام مجموعة Diffie-Hellman الأعلى أكثر أماناً، ولكن تتطلب مجموعات Diffie-Hellman الأعلى موارد معالجة إضافية لحساب المفتاح.

- 1: Diffie-Hellman group 1 (768 bit)
- 2: Diffie-Hellman group 2 (1024 bit)
- 5: Diffie-Hellman group 5 (1536 bit)
- 14: Diffie-Hellman group 14 (2048 bit)
- 15: Diffie-Hellman group 15 (3072 bit)
- 16: Diffie-Hellman group 16 (4096 bit)
- 19: Diffie-Hellman group 19 (256-bit ECP)

20: Diffie-Hellman group 20 (384-bit ECP)

21: Diffie-Hellman group 21 (521-bit ECP)

24: Diffie-Hellman group 24 (2048 bit, 256-bit subgroup)

- R1(config-isakmp)# **group 5**
- R1(config-isakmp)# **exit**

5. عنوان IP

يمكن استخدام عنوان IP لمواجهة الاسترجاع عندما تكون هناك مسارات متعددة للوصول إلى عنوان IP الخاص بالتطبيق

```
R1(config)# crypto isakmp key secretkey address  
192.168.300.1
```

4.2.2.2 :IKE Phase 2

يتمّ التفاوض على SAs نيابة عن خدمات مثل IPSec التي تحتاج إلى مواد أساسية. تسمى هذه المرحلة الوضع السريع.

لتكوين المرحلة 2، نحتاج إلى تحديد مجموعة التحويل، التي تحدّد التجزئة، وبروتوكول الأمان، والتشفير المستخدم للمرحلة 2:

On Both Routers:

```
Rx(config)# crypto ipsec transform-set TSET esp-3des  
esp-md5-hmac
```

```
Rx(cfg-config-trans)# exit
```

Crypto map4.2.3

في الخطوة الأخيرة، يتم تكوين خريطة التشفير لتحديد التطير، و ACL التشفير ومجموعة التحويل. هناك ثلاثة خيارات عند تكوين خريطة التشفير .

- IPsec-ISAKMP هذا هو الخيار الأفضل ينصّ على أننا نستخدم ISAKMP لتشفير المفتاح وفكّ تشفيره.
- دليل IPsec: هذا هو الخيار الأسوأ. هذا يعني أنّه يجب إدخال المفتاح يدوياً. (هل يمكنك تحيّل إدخال مفتاح 512 بت يدوياً؟)
- GDOI: يُستخدم هذا الاختيار لتكوين GETVPN. وهو يشير إلى مجال التفسير الجماعي.

- On R1:
- R1(config)# **crypto map TST 10 ipsec-isakmp**

ستظلّ خريطة التشفير الجديدة هذه معطّلة حتّى يتمّ تكوين نظير وقائمة وصول صالحة.

```
R1(config-crypto-map)# set peer 209.165.200.1
```

```
R1(config-crypto-map)# match address 100
```

```
R1(config-crypto-map)# set transform-set TSET
```

```
R1(config-crypto-map)# exit
```

تطبّق الخطوة الأخيرة خريطة التشفير على الواجهة التي تواجه النظير الآخر:

On R1:

```
R1(config)# interface GigabitEthernet0/0
```

```
R1(config-if)# crypto map TST
```


%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

أ- كيف يتم تطبيق خريطة التشفير؟

- يمكن تطبيق خريطة تشفير واحدة على واجهة.
- يمكن تطبيق خريطة التشفير نفسها على واجهات متعددة.
- لاستيعاب العديد من الأنفاق يتم استخدام إدخالات خريطة التشفير. يمكن أن تحتوي خريطة تشفير واحدة على إدخالات متعددة يتم تحديدها برقم.

ب- أنواع خرائط التشفير: يوجد نوعين من خرائط التشفير:

- خريطة تشفير ثابتة - تحدد النظر وحركة المرور ليطم تشفيرها بشكل صريح، تستخدم عادةً لاستيعاب عدد قليل من الأنفاق مع ملفات تعريف وخصائص مختلفة (شركاء ومواقع وموقع مختلف).
- خريطة التشفير الديناميكية - هي إحدى الطرق لاستيعاب النظراء الذين يشاركون نفس الخصائص (على سبيل المثال، مكاتب متعددة الفروع تشترك في نفس التكوين) أو أقران لديهم عنوان IP ديناميكي (DHCP, etc.)

يجب أن يتطابق إدخال خريطة التشفير crypto map مع حركة المرور المحددة بواسطة قائمة الوصول access-list 100 وتنفيذ المعلومات المحددة في ملف تعريف ISAKMP.

5 الفصل الخامس: تغليف التوجيه العام GRE

GRE هو بروتوكول نفق تم تطويره بواسطة Cisco ويسمح بتغليف مجموعة كبيرة من بروتوكولات طبقة الشبكة داخل الارتباطات من نقطة إلى نقطة. تم استخدامه في هذا المشروع للتغلب على المشاكل الممكنة، وهذا ما نستعرضه في هذا الفصل، حيث نوضح فيه المشاكل التي تواجهها في site-to-site VPN والفوائد التي يقدمها GRE وأنواعه.

5.1 مشاكل site-to-site VPN :

يحتاج كل فرع من الفروع إلى وضع إعداداته لوحده في الفرع الرئيسي بالتالي يؤثر على موارد الراوتر، تم حل هذه المشكلة من خلال DM-VPN حيث نقوم بإعدادات الفرع الرئيسي مرة واحدة فقط. رغم أمان IPsec إلا أنه لا ينقل جميع أنواع البيانات مثل البث العام والمتعدد الصوت. لحل هذه المشكلة نستخدم GRE فهي تنقل جميع أنواع البيانات لكنها غير آمنة وبذلك نرى أن عملهما معاً يجنبنا المشاكل.

5.2 أنواع GRE :

لديه نوعان:

1. IPsec over GRE

أولاً نطبق GRE لنقل جميع أنواع البيانات ويتم تطبيق IPsec على البيانات المهمة فقط بالتالي هو اتصال ضعيف نسبياً حيث بعض الأمور تحتاج إلى تشفير بصورة مستقلة. لكننا نضطر لاستخدام هذا النوع عندما تمنع البنية التحتية استخدام IPsec.

2. GRE over IPsec

هو النوع الأفضل وتكون جميع البيانات مشفرة، له عدة أنواع: Hub and spoke هو الأكثر شيوعاً.

partial mesh- أكبر سيئاته أنه يجب أن يستخدم static ip public ولا تنقل بروتوكولات التوجيه

full mesh- سيئته يجب أن يستخدم static ip public ولا تنقل بروتوكولات التوجيه

5.3 أوضاع GRE :

كما هو الحال مع IPsec، عند تكوين GRE مع IPsec، هناك وضعان يمكن فيهما تكوين GRE IPsec، وضع التفق GRE IPsec ووضع النقل GRE IPsec.

5.3.1 GRE IPSEC TUNNEL

مع وضع نفق GRE IPsec، يتم تغليف حزمة GRE بأكملها (التي تتضمن حزمة رأس IP الأصلية) وتشفيرها وحمايتها داخل حزمة IPsec. يوفر GRE عبر وضع نفق IPsec أماناً إضافياً لأنه لا يتم الكشف عن أي جزء من نفق GRE، ومع ذلك، هناك زيادة في الحمل تضاف إلى الحزمة. يقلل هذا الحمل الإضافي المساحة الحرة القابلة للاستخدام لحملنا (حزمة IP الأصلية)، مما يعني احتمال حدوث مزيد من التجزئة عند إرسال البيانات عبر GRE IPsec Tunnel VPN.

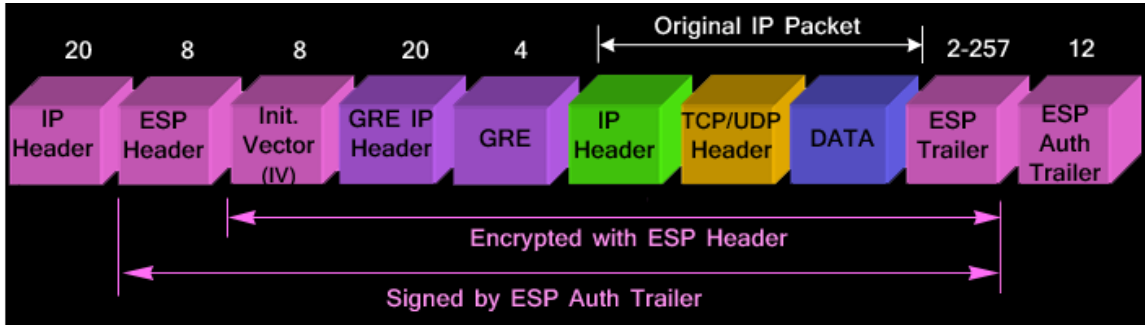
وضع نفق IPsec هو خيار التكوين الافتراضي لكل من شبكات VPN GRE وغير GRE IPsec. عند تكوين مجموعة تحويل IPsec، لا توجد أوامر تكوين أخرى مطلوبة لتمكين وضع التفق:

```
R1(config)# crypto ipsec transform-set TS esp-3des  
esp-md5-hmac
```

حساب وضع نفق GRE IPSEC في الخارج

سيساعدنا حساب المصروفات الزائدة في فهم مقدار المساحة الإضافية التي يتطلبها GRE عبر IPsec في وضع التفق ومساحتنا الفعالة القابلة للاستخدام.

يُظهر الشكل 1-5 هيكل الحزمة مثلاً على GRE عبر IPsec في وضع النفق:



الشكل 1-5 GRE IPsec Tunnel

نقطتان مهمتان يجب مراعاتهما عند حساب المصروفات الزائدة:

اعتماداً على خوارزمية التشفير المستخدمة في مجموعة تحويل التشفير، يمكن أن يبلغ طول ناقل التهيئة (IV) المعروض 8 أو 16 بايت. على سبيل المثال، يقدم DES أو DES3 حقل IV 8 بايت، حيث يقدم AES حقل IV 16 بايت. في مثالنا، نحن نستخدم تشفير DES3، وبالتالي ننتج حقل IV 8 بايت.

يختلف حجم مقطوعة ESP عادةً. وتتمثل مهمتها في التأكد من محاذاة حقل طول اللوحة والرأس التالي (كلاهما بطول 1 بايت ومضمّن في مقطوعة ESP) ومصادقة ESP للمقطوعة على حد 4 بايت. هذا يعني أنّ إجمالي عدد البايت، عند إضافة الحقول الثلاثة معاً، يجب أن يكون مضاعفاً لـ 4.

فيما يلي التكاليف العامة المحسوبة:

$$\text{حجم ESP: } 20 (\text{IP Hdr}) + 8 (\text{ESP Hdr}) + 8 (\text{IV}) + 4 (\text{ESP Trailer}) + 12 (\text{ESP Auth}) = 52 \text{ بايت}$$

Note: تمّ حساب مقطوعة ESP على أنّها 4 بايت حسب الملاحظة أعلاه.

حمل GRE: 20 (GRE IP Hdr) + 4 (GRE) = 24 بايت

إجماليّ المصروفات: 52 + 24 = 76 بايت.

5.3.2 غط GRE IPSEC Transport

مع وضع النقل GRE IPsec، يتمّ تغليف حزمة GRE وتشفيرها داخل حزمة IPsec، ومع ذلك، يتمّ وضع رأس IP GRE في المقدمة. هذا يكشف بفعاليّة رأس GRE IP لأنّه غير مشفر بنفس الطريقة التي يتمّ بها في وضع النفق.

لا يتمّ استخدام وضع النقل IPsec بواسطة التكوين الافتراضيّ ويجب تكوينه باستخدام الأمر التالي ضمن مجموعة تحويل IPsec:

```
R1(config)# crypto ipsec transform-set TS esp-3des
```

```
esp-md5-hmac
```

```
R1(cfg-crypto-trans)# mode transport
```

وضع النقل GRE IPsec له بعض قيود التنفيذ. لا يمكن استخدام وضع النقل GRE IPsec إذا كان نفق التشفير يعبر جهازاً باستخدام ترجمة عنوان الشبكة (NAT) أو ترجمة عنوان المنفذ (PAT). في مثل هذه الحالات، يجب استخدام وضع النفق.

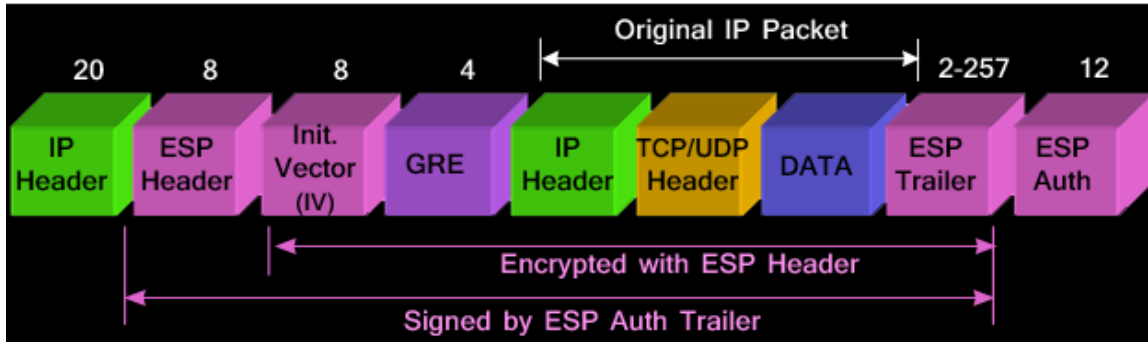
أخيراً، إذا كانت نقاط نهاية نفق GRE ونقاط نهاية نفق التشفير مختلفة، فلا يمكن استخدام وضع النقل GRE IPsec.

تقيّد هذه القيود بشكلٍ خطيرٍ استخدام وتنفيذ وضع النقل في بيئة شبكة WAN.

حساب وضع نقل GRE IPSEC في الخارج:

سيساعدنا حساب المصروفات الزائدة في فهم مقدار مساحة GRE عبر IPsec في استخدامات وضع النقل ومساحتنا الفعّالة القابلة للاستخدام.

يُظهر الشكل 2-5 هيكل الحزمة أدناه مثلاً على GRE عبر IPsec في وضع النقل:



الشكل 2-5 GRE IPSEC Transport

مرة أخرى، نقطتان مهمتان يجب مراعاتهما عند حساب المصروفات الزائدة:

اعتماداً على خوارزمية التشفير المستخدمة في مجموعة تحويل التشفير، يمكن أن يبلغ طول ناقل التهيئة (IV) المعروض 8 أو 16 بايت. على سبيل المثال، يقدم DES أو DES3 حقل 8 IV بايت، حيث يقدم AES حقل 16 IV بايت. في مثالنا، نحن نستخدم تشفير DES3، وبالتالي نتج حقل 8 IV بايت.

يختلف حجم مقطورة ESP عادةً. وتتمثل مهمتها في التأكد من محاذاة حقلي طول اللوحة والرأس التالي (كلاهما بطول 1 بايت ومضمّن في مقطورة ESP) ومصادقة ESP للمقطورة على حد 4 بايت. هذا يعني أنّ إجمالي عدد البايت، عند إضافة الحقول الثلاثة معاً، يجب أن يكون مضاعفاً لـ 4.

فيما يلي التكاليف العامة المحسوبة:

$$\text{ESP: } 20 (\text{IP Hrd}) + 8 (\text{ESP Hdr}) + 8 (\text{IV}) + 4 (\text{ESP Trailer}) \text{ حمل} \\ = 52 (\text{ESP Auth}) + 12 \text{ بايت}$$

Note: تمّ حساب مقطوعة ESP على أنّها 4 بايت حسب الملاحظة أعلاه.

حمل 4 (GRE) = 4 GRE: بايت.

إجماليّ المصروفات: 56 = 4 + 52 بايت.

من الواضح أن وضع النقل GRE IPSec يوفر 20 بايت تقريباً لكلّ حزمة زائدة. قد يوفر هذا كميّة معتدلة من النطاق التردديّ على ارتباط WAN، ومع ذلك، لا توجد زيادة كبيرة في أداء وحدة المعالجة المركزيّة باستخدام هذا الوضع.

6 الفصل السادس: التطبيق العملي

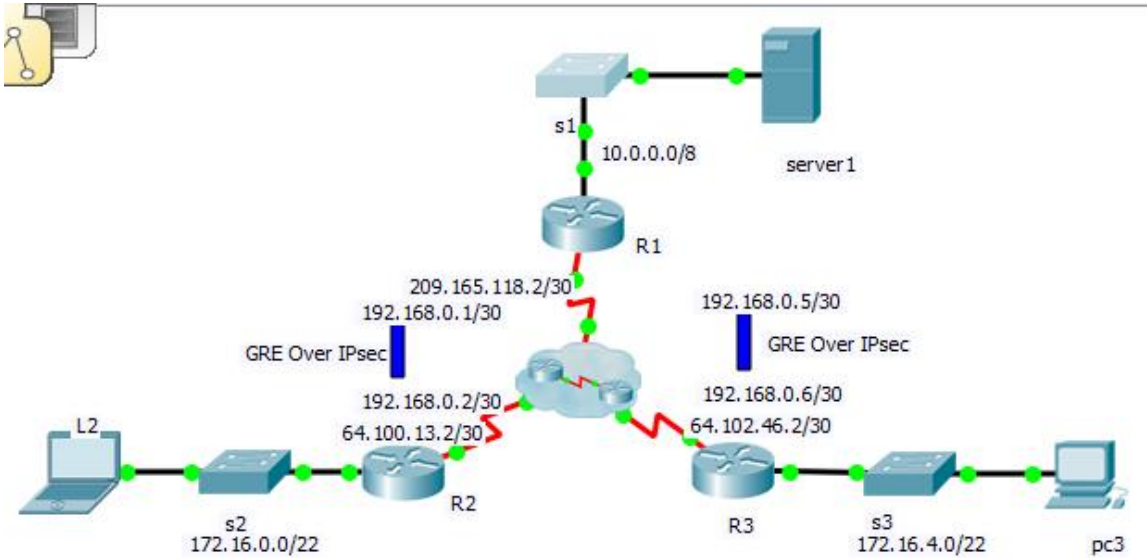
لدينا بنك فيه مكتب رئيسي يقع في لندن ولديه مكتبان فرعيان يقعان في دبي وقطر. يمتلك البنك خادم تطبيق يستخدمه عملاؤه في جميع أنحاء العالم لإجراء المعاملات عبر الإنترنت ويقع في مقره الرئيسي. جميع الفروع بها اتصال إنترنت عالي السرعة. يوجد حوالي 100 مستخدم في كل من المكاتب الفرعية و 200 مستخدم في المكتب الرئيسي.

تريد كل من الفروع التواصل مع المكتب الرئيسي بسرعة وبشكل آمن، لتقوم بعملها بأعلى كفاءة وجودة، لتحقيق ذلك نقوم بإنشاء أنفاق GRE بسيطة (غير محمية) وأمنة (مشفرة IPsec) بين كل مكتب فرعي مع الرئيسي مبنية على شبكة الإنترنت.

نستخدم في تنفيذ هذا التطبيق بيئتي العمل Packet Tracer و GNS3.

حيث نستخدم سويتشات في كل مقر لربط أجهزته، بالإضافة لراوتر لنصل إلى الشبكة العامة.

6.1 خطوات العمل



الشكل 1-6 الشكل العام للشبكة

يظهر الشكل 6-1 طريقة ربط الأجهزة لتكوين الشكل العام لفروع البنك.

أولاً: جدول العناوين

| Device | Interface | IP Address | Subnet Mask | Default Gateway |
|---------|-----------|---------------|-----------------|-----------------|
| R1 | G0/0 | 10.0.0.1 | 255.0.0.0 | N/A |
| | S0/0/0 | 209.165.118.2 | 255.255.255.252 | N/A |
| | Tunnel 0 | 192.168.0.1 | 255.255.255.252 | N/A |
| | Tunnel 1 | 192.168.0.5 | 255.255.255.252 | N/A |
| R2 | G0/0 | 172.16.0.1 | 255.255.252.0 | N/A |
| | S0/0/0 | 64.100.13.2 | 255.255.255.252 | N/A |
| | Tunnel 0 | 192.168.0.2 | 255.255.255.252 | N/A |
| R3 | G0/0 | 172.16.4.1 | 255.255.252.0 | N/A |
| | S0/0/0 | 64.102.46.2 | 255.255.255.252 | N/A |
| | Tunnel 0 | 192.168.0.6 | 255.255.255.252 | N/A |
| Server1 | NIC | 10.0.0.2 | 255.0.0.0 | 10.0.0.1 |
| L2 | NIC | 172.16.0.2 | 255.255.252.0 | 172.16.0.1 |
| PC3 | NIC | 172.16.4.2 | 255.255.252.0 | 172.16.4.1 |

جدول العناوين Table 1

ثانياً: نقوم بالخطوات التالية:

1. نتحقق من اتصال جهاز التوجيه

الخطوة 1: Ping R2 و R3 من R1.

أ. من R1 ، نقوم باختبار اتصال عنوان IP الخاص بـ S0 / 0/0 على R2.

ب. من R1 ، نقوم باختبار اتصال عنوان IP الخاص بـ S0 / 0/0 على R3.

الخطوة 2: Ping Server1 من L2 و PC3.

أجرينا محاولة تنفيذ الأمر ping على عنوان IP الخاص بالخادم 1 من L2.

الخطوة 3: Ping PC3 من L2.

أجرينا محاولة تنفيذ الأمر ping على عنوان IP الخاص بـ PC3 من L2.

Note: الخطوة 2 و 3 فشلتنا بسبب عدم وجود طريق إلى الوجهة.

2. تمكين مميزات الأمان

الخطوة 1: تنشيط وحدة securityk9.

أ- نقوم بإصدار الأمر show version في المستخدم EXEC أو وضع EXEC

ذي الامتيازات للتحقق من تنشيط ترخيص حزمة تقنية الأمان.

| Technology | Technology-package | Technology-package |
|------------|--------------------|--------------------|
|------------|--------------------|--------------------|

| Current | Type | Next reboot |
|---------|------|-------------|
|---------|------|-------------|

| | | | |
|----------|----------|-----------|----------|
| ipbase | ipbasek9 | Permanent | ipbasek9 |
| security | None | None | None |
| uc | None | None | None |
| data | None | None | None |

ب- إذا لم يكن الأمر كذلك، نقوم بتنشيط الوحدة النمطية securityk9 للتمهيد التالي للموجه، وقبول الترخيص، وحفظ التكوين، وإعادة التشغيل .

```
R1(config)# license boot module c2900 technology-  
package securityk9
```

```
<Accept the License>
```

```
R1(config)# end
```

```
R1# copy running-config startup-config
```

```
R1# reload
```

ج. بعد اكتمال إعادة التحميل، نقوم بإصدار إصدار العرض مرة أخرى للتحقق من تنشيط ترخيص حزمة تقنية الأمان.

معلومات ترخيص حزمة التكنولوجيا للوحدة النمطية: 'c2900'

| ----- | | | |
|------------|--------------------|--------------------|-------------|
| ----- | | | |
| Technology | Technology-package | Technology-package | |
| | Current | Type | Next reboot |
| ----- | | | |
| ----- | | | |
| ipbase | ipbasek9 | Permanent | ipbasek9 |
| security | securityk9 | Evaluation | securityk9 |
| uc | None | None | None |
| data | None | None | None |

د. نكرّر الخطوات من 1 أ إلى 1 ج مع R2 و R3.

3. Configure IPsec Parameters

الخطوة 1: تحديد حركة المرور المثيرة للاهتمام على R1.

أ. نقوم بتكوين ACL 101 لتحديد حركة المرور من LAN على R1 إلى LAN على R2 و R3 على أنّها مثيرة للاهتمام. ستؤدّي هذه الحركة المثيرة للاهتمام إلى تنفيذ IPsec VPN كلّما كان هناك حركة مرور بين شبكات LAN R1 و R2 - R3. لن يتمّ تشفير جميع حركات المرور الأخرى التي يتمّ الحصول عليها من شبكات LAN. يجب أن نتذكّر أنّه بسبب رفض أي ضمني، ليست هناك حاجة لإضافة العبارة إلى القائمة.

```
R1(config)# access-list 101 permit ip 10.0.0.0 0.255.255.255  
172.16.0.0 0.0.3.255
```

ب. نكرّر الخطوة 1 أ لتكوين ACL 101 لتحديد حركة المرور على شبكة LAN الخاصة بـ R3 على أنّها مثيرة للاهتمام.

```
R1(config)# access-list 101 permit ip 10.0.0.0  
0.255.255.255 172.16.4.0 0.0.3.255
```

الخطوة 2: تكوين خصائص ISAKMP المرحلة 1 على R1.

أ. تكوين خصائص سياسة التشفير ISAKMP 101 على R1 مع سيسكو مفتاح التشفير المشترك. لا يجب تكوين القيم الافتراضية، لذلك يجب فقط تكوين التشفير وطريقة تبادل المفاتيح وطريقة DH.

```
R1(config)# crypto isakmp policy 101  
R1(config-isakmp)# encryption aes
```

```
R1(config-isakmp)# authentication pre-share
```

```
R1(config-isakmp)# group 5
```

```
R1(config-isakmp)# exit
```

ب. إنشاء مفاتيح isakmp لكلٍ نظير R1.

```
R1(config)# crypto isakmp key cisco address 64.100.13.2
```

```
R1(config)# crypto isakmp key cisco address 64.102.46.2
```

الخطوة 3 : تكوين خصائص ISAKMP المرحلة 2 على R1.

أ. ننشئ مجموعة VPN-SET المحولة لاستخدام esp-aes و esp-sha-hmac. ثمّ

نقوم بإنشاء خريطة التشفير VPN-MAP التي تربط جميع معلمات المرحلة 2 معاً.

نستخدم الرقم التسلسلي 101 وحدّده كخريطة ipsec-isakmp.

```
R1(config)# crypto ipsec transform-set R1_Set esp-aes  
esp-sha-hmac
```

```
R1(config)# crypto map R1_Map 101 ipsec-isakmp
```

```
R1(config-crypto-map)# set peer 64.100.13.2
```

```
R1(config-crypto-map)# set peer 64.102.46.2
```

```
R1(config-crypto-map)# set transform-set R1_Set
```

```
R1(config-crypto-map)# match address 101
```

```
R1(config-crypto-map)# exit
```

الخطوة 4: تكوين خريطة التشفير على الواجهة الصّادرة.

أخيراً، نربط خريطة تشفير R1_Map بواجهة Serial 0/0/0 الصّادرة.

```
R1(config)# interface S0/0/0
```

```
R1(config-if)# crypto map R1_Map
```

الخطوة 5: تكوين معلمات IPsec على R2 و R3

نكرّر الخطوات من 1-4 على R2 و R3. نقوم بتعديل المجموعة، وأسماء الخريطة من R1 إلى R2 و R3. نستخدم نفس رقم ACL الموسع، 101. نلاحظ أنّ كلّ جهاز توجيه يحتاج فقط إلى اتّصال مشفّر واحد إلى R1. لا يوجد اتّصال مشفّر بين R2 و R3.

R2:

```
R2(config)# access-list 101 permit ip 172.16.0.0 0.0.3.255  
10.0.0.0 0.255.255.255
```

```
R2(config)# crypto isakmp policy 101
```

```
R2(config-isakmp)# encryption aes
```

```
R2(config-isakmp)# authentication pre-share
```

```
R2(config-isakmp)# group 5
```

```
R2(config-isakmp)# exit
```

```
R2(config)# crypto isakmp key cisco address 209.165.118.2
```

```
R2(config)# crypto ipsec transform-set R2_Set  
esp-aes esp-sha- hmac
```

```
R2(config)# crypto map R2_Map 101 ipsec-isakmp
```

```
R2(config-crypto-map)# set peer 209.165.118.2
```

```
R2(config-crypto-map)# set transform-set R2_Set
```

```
R2(config-crypto-map)# match address 101
```

```
R2(config-crypto-map)# exit
```

```
R2(config)# interface S0/0/0
```

```
R2(config-if)# crypto map R2_Map
```

R3:

```
R3(config)# access-list 101 permit ip 172.16.4.0 0.0.3.255  
10.0.0.0 0.255.255.255
```

```
R3(config)# crypto isakmp policy 101
```

```

R3(config-isakmp)# encryption aes
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 5
R3(config-isakmp)# exit
R3(config)# crypto isakmp key cisco address 209.165.118.2
R3(config)# crypto ipsec transform-set R3_Set
esp-aes esp-sha- hmac
R3(config)# crypto map R3_Map 101 ipsec-isakmp
R3(config-crypto-map)# set peer 209.165.118.2
R3(config-crypto-map)# set transform-set R3_Set
R3(config-crypto-map)# match address 101
R3(config-crypto-map)# exit
R3(config)# interface S0/0/0
R3(config-if)# crypto map R3_Map

```

4. تكوين أنفاق GRE عبر IPSec

الخطوة 1: تكوين واجهات التتفق R1.

ندخل إلى وضع التكوين للتتفق 0 R1.

```

R1(config)# interface tunnel 0

```

نقوم بتعيين عنوان IP كما هو موضح في جدول العنوان.

```

R1(config-if)# ip address 192.168.0.1
255.255.255.252

```

تعيين المصدر والوجهة لنقاط نهاية التتفق.

```

R1(config-if)# tunnel source s0/0/0

```

```
R1(config-if)# tunnel destination 64.100.13.2
```

تكوين النفق 0 لنقل حركة مرور IP عبر GRE.

```
R1(config-if)# tunnel mode gre ip
```

يجب أن تكون واجهة Tunnel 0 نشطة بالفعل. في حالة عدم وجودها ، نتعامل معها مثل أي واجهة أخرى.

نكرر الخطوات من a-f1 لإنشاء واجهة Tunnel 1 إلى R3.

```
R1(config)# interface tunnel 0
```

```
R1(config-if)# ip address 192.168.0.5
```

```
255.255.255.252
```

```
R1(config-if)# tunnel source s0/0/0
```

```
R1(config-if)# tunnel destination 64.102.46.2
```

```
R1(config-if)# tunnel mode gre ip
```

الخطوة 2: تكوين واجهة النفق R2 و R3.

أ. نكرر الخطوات من e1 - a مع R2.

```
R2(config)# interface tunnel 0
```

```
R2(config-if)# ip address 192.168.0.2
```

```
255.255.255.252
```

```
R2(config-if)# tunnel source s0/0/0
```

```
R2(config-if)# tunnel destination 209.165.118.2
```

```
R2(config-if)# tunnel mode gre ip
```

ب. نكرر الخطوات من e1 - a مع R3.

```
R3(config)# interface tunnel 0
```



```
R3(config-if)# ip address 192.168.0.6  
255.255.255.252
```

```
R3(config-if)# tunnel source s0/0/0
```

```
R3(config-if)# tunnel destination 209.165.118.2
```

```
R3(config-if)# tunnel mode gre ip
```

الخطوة 3: تكوين مسار لحركة مرور IP الخاصة.

أ. نحدد مساراً من R1 إلى الشبكات 172.16.0.0 و 172.16.4.0 باستخدام عنوان المرحلة التالية لواجهة التّفق.

```
R1(config)# ip route 172.16.0.0 255.255.252.0 192.168.0.2
```

```
R1(config)# ip route 172.16.4.0 255.255.252.0 192.168.0.6
```

ب. نحدد مساراً من R2 و R3 إلى شبكة 10.0.0.0 باستخدام عنوان المرحلة التالية لواجهة التّفق.

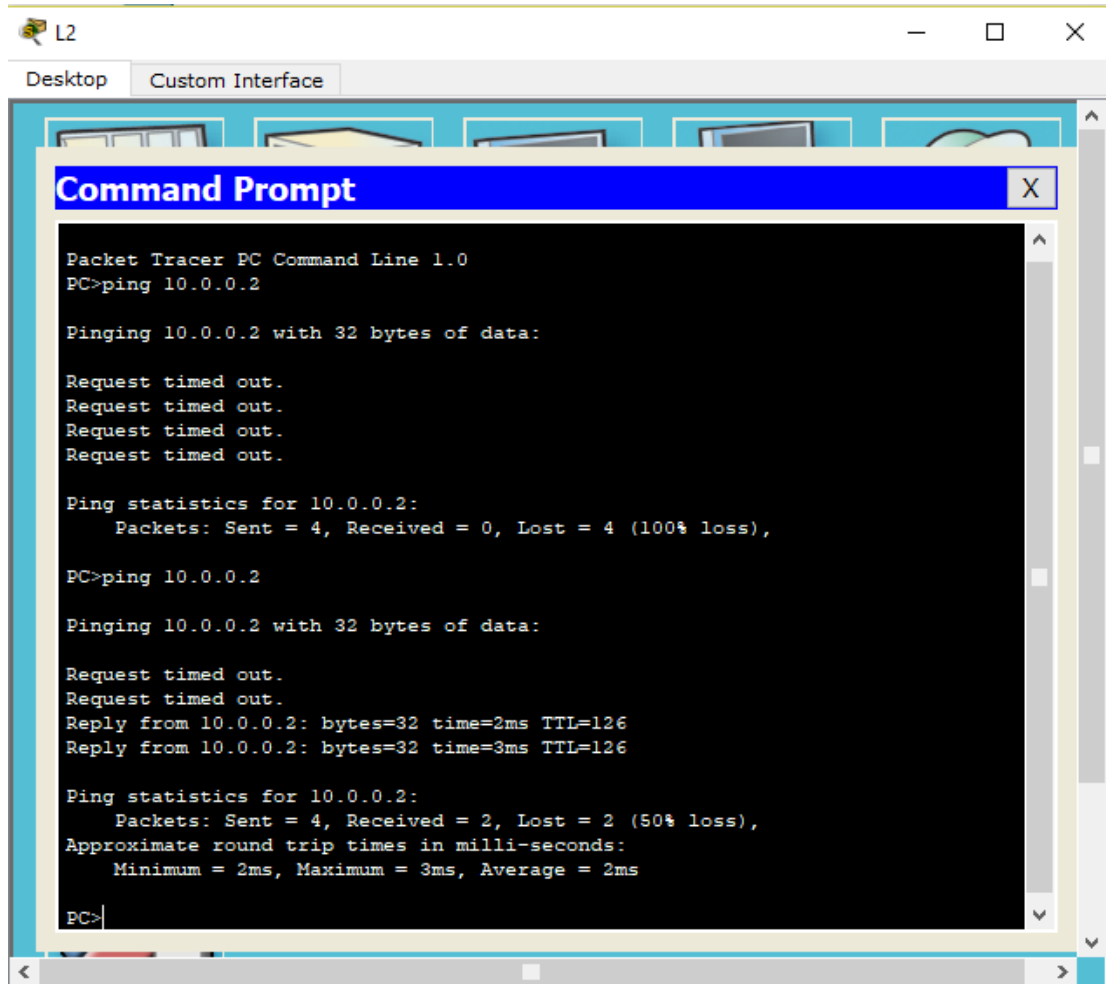
```
R2(config)# ip route 10.0.0.0 255.0.0.0 192.168.0.1
```

```
R3(config)# ip route 10.0.0.0 255.0.0.0 192.168.0.5
```

5. تحقق من الاتصال

الخطوة 1: Ping Server1 من L2 و PC3.

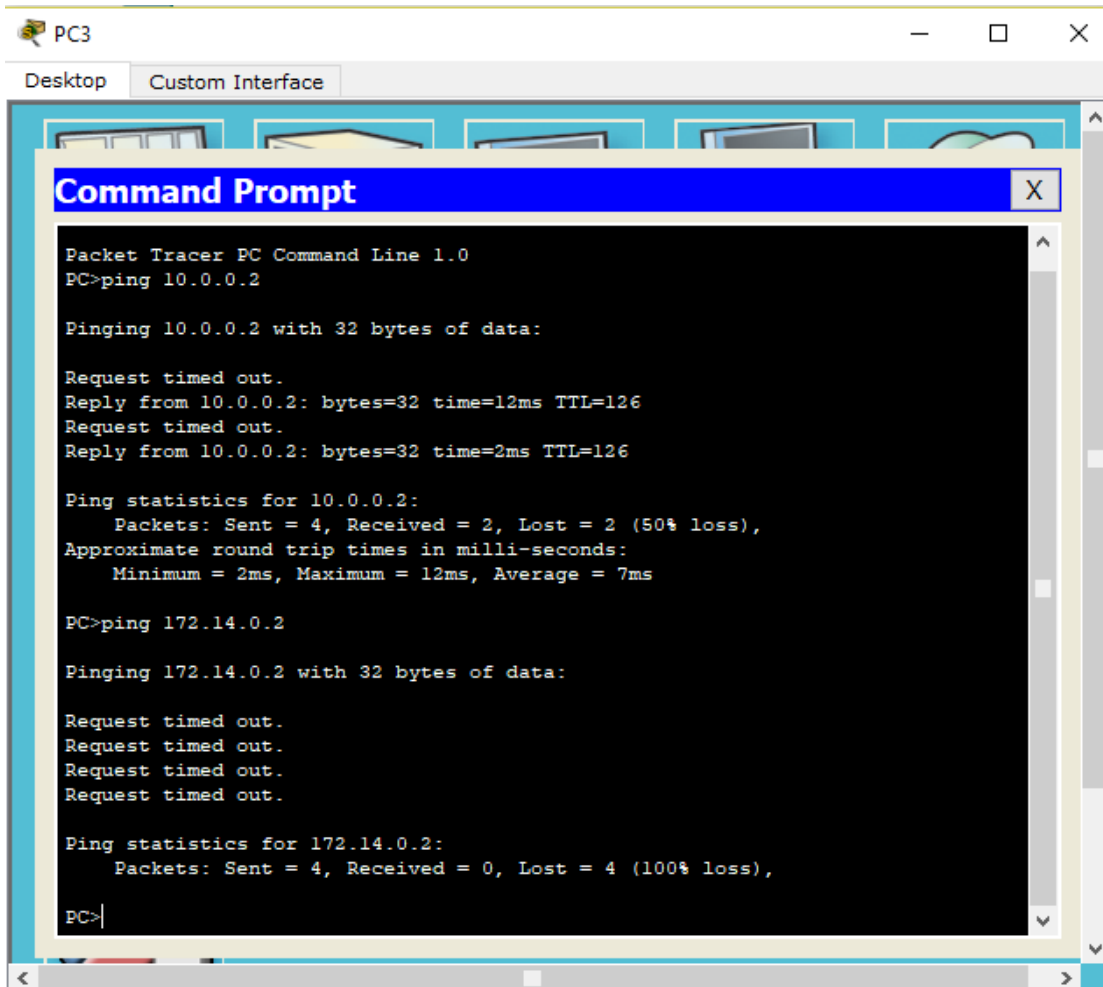
جرت محاولة تنفيذ الأمر ping على عنوان IP الملقم 1 من L2.



الشكل 2-6 تنفيذ الأمر ping من L2 و PC3.

نلاحظ من الشكل 2-6 أن الأمر ping ناجحاً وذلك لوجود نفق بين المقر الفرعي الذي يحتوي على الجهاز L2 والمقر الرئيسي الذي يحتوي المخدم.

جرت محاولة تنفيذ الأمر ping على عنوان IP لـ L2 من PC3.



```
Packet Tracer PC Command Line 1.0
PC>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Request timed out.
Reply from 10.0.0.2: bytes=32 time=12ms TTL=126
Request timed out.
Reply from 10.0.0.2: bytes=32 time=2ms TTL=126

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 12ms, Average = 7ms

PC>ping 172.14.0.2

Pinging 172.14.0.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

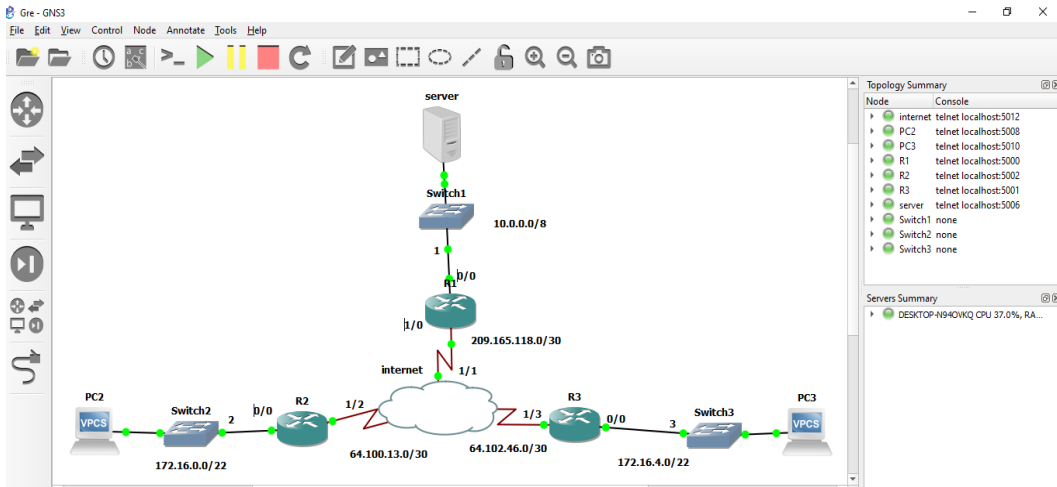
Ping statistics for 172.14.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

الشكل 3-6 تنفيذ الأمر ping من PC3 إلى L2

نلاحظ من الشكل 3-6 أن الاختبار فشل بسبب عدم وجود نفق بين الشبكتين المتمثلتين بالمكتب الفرعي من خلال الحاسب PC3 والمكتب الفرعي الآخر المتمثل بـ L2.

إجراء التجربة السابقة نفسها على GNS3 وتم تمثيلها كما يظهر الشكل 4-6 التالي:



الشكل 4-6 شكل الشبكة على GNS3

نتائج التنفيذ:

القيام بالأمر ping على عنوان IP مملق 1 من PC 2.

```

Welcome to Virtual PC Simulator, version 0.6.2
Dedicated to Daling.
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

Checking for duplicate address...
PC1 : 172.16.0.2 255.255.252.0 gateway 172.16.0.1

PC2> ping 10.0.0.2
10.0.0.2 icmp_seq=1 timeout
10.0.0.2 icmp_seq=2 timeout
84 bytes from 10.0.0.2 icmp_seq=3 ttl=62 time=54.033 ms
84 bytes from 10.0.0.2 icmp_seq=4 ttl=62 time=52.520 ms
84 bytes from 10.0.0.2 icmp_seq=5 ttl=62 time=61.857 ms

PC2>

```

الشكل 5-6 تنفيذ الأمر ping من PC2

نلاحظ من الشكل 5-6 أن الأمر ping تم بنجاح. وهذا يفسر وجود نفق بين المكتب الرئيسي الذي يحتوي على المخدم وبين المكتب الفرعي الذي يحتوي الجهاز PC2.

تنفيذ الأمر ping على عنوان ال IP للمخدم من الجهاز PC3.

```

Dedicated to Daling.
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

Checking for duplicate address...
PC1 : 172.16.4.2 255.255.252.0 gateway 172.16.4.1

PC3> ping 10.0.0.2
*172.16.4.1 icmp_seq=1 ttl=255 time=31.472 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.4.1 icmp_seq=2 ttl=255 time=10.562 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.4.1 icmp_seq=3 ttl=255 time=17.775 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.4.1 icmp_seq=4 ttl=255 time=8.976 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.4.1 icmp_seq=5 ttl=255 time=9.962 ms (ICMP type:3, code:1, Destination host unreachable)

PC3> ping 10.0.0.2
*172.16.4.1 icmp_seq=1 ttl=255 time=8.934 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.4.1 icmp_seq=2 ttl=255 time=16.420 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.4.1 icmp_seq=3 ttl=255 time=17.621 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.4.1 icmp_seq=4 ttl=255 time=8.006 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.4.1 icmp_seq=5 ttl=255 time=14.215 ms (ICMP type:3, code:1, Destination host unreachable)

PC3> ping 10.0.0.2
10.0.0.2 icmp_seq=1 timeout
84 bytes from 10.0.0.2 icmp_seq=2 ttl=62 time=54.847 ms
84 bytes from 10.0.0.2 icmp_seq=3 ttl=62 time=51.745 ms
84 bytes from 10.0.0.2 icmp_seq=4 ttl=62 time=64.570 ms
84 bytes from 10.0.0.2 icmp_seq=5 ttl=62 time=42.530 ms

```

الشكل 6-6 تنفيذ الأمر ping من PC3

من الشكل 6-6 نلاحظ أنَّ النفق بين المكتب الرئيسي والمكتب الفرعي الآخر الذي يحتوي الجهاز PC3 قائم وذلك بسبب نجاح الأمر ping بينهما.

6.2 النتائج

- عند مقارنة GRE عبر نفق IPSec و GRE عبر وضع النقل IPSec، هناك اختلافات كبيرة لا يمكن تجاهلها.
- إذا كانت أنفاق GRE ونقاط نهاية التشفير ليست هي نفسها (عنوان IP الحكيم)، فإن وضع النقل ليس بالتأكيد خياراً.
- إذا اجتازت الحزم جهازاً (جهاز توجيه) حيث يتم استخدام NAT أو PAT مرة أخرى، فلا يمكن استخدام وضع النقل.
- من ناحية أخرى، يبدو أن وضع النفق يسدّد حمله الإضافي 20 بايت من خلال كونه مرناً بما يكفي لاستخدامه في أي نوع من بيئة WAN وتقديم حماية متزايدة من خلال تشفير GRE IP Header داخل حزمة ESP.
- مع الأخذ في الاعتبار الحمل الإضافي الصغير لوحدة المعالجة المركزية التي ينتجها وضع النفق والمزايا التي يقدمها، لا نعتقد أنه من قبيل المصادفة أن Cisco حدّدت هذا الوضع في التكوين الافتراضي لـ IPSec.

6.3 الصعوبات والتوصيات

- مشكلة IPSec أنه لا ينقل بروتوكولات توجيه لوحده لأنها معتمدة على البث العام والبث المتعدد، ولا ينقل الصوت أيضاً لأنه يعتمد على البث المتعدد لذلك من الضروري الاستعانة بطريقة ثانية مثل GRE لتحل هذه المشكلة حيث أن GRE تنقل كل أنواع البيانات.
- مشكلة GRE غير آمنة فمن الضروري إنشاء اتصال IPSec أولاً.
- عند استخدام GRE over IPSec يفضل استخدام IP summarization لتقليل حجم جداول التوجيه ومساحة الذواكر المستخدمة وتسهيل إعدادات IPsec.

Idea and implementation of :

Eng. Alaa Al –Halabi

All intellectual property rights are reserved and affiliated with the owner of the project

