الفصل السادس

6 أمن بروتوكول الإنترنت

محتويات الفصل:

"إذا قام جاسوس بإفشاء سر قبل أوانه، فلابد من تنفيذ حكم الإعدام فيه وفيمن أُفشى إليه ذلك السر."

— من كتاب فن الحرب، لصن تزو.

النقاط الرئيسة

- أمن بروتوكول الإنترنت (IPSec) هو إمكانيات يمكن إضافتها إلى أيٍّ من نسخ بروتوكول الإنترنت الحالية (IPv4 أو IPv6) بواسطة ترويسات إضافية.
- يشمل أمن بروتوكول الإنترنت IPSec ثلاثة مجالات وظيفية: التوثيق، والسرية، وإدارة المفاتيح.
- يستخدم التوثيق كود HMAC للتحقّق من الرسالة. ولتوثيق رسالة، يمكن تطبيق عملية التوثيق على رزمة بروتوكول الإنترنت الأصلية كاملةً (نمط النفق) أوعلى كل الرزمة باستثناء ترويسة بروتوكول الإنترنت (نمط النقل).
- يتم توفير السرية عن طريق صيغة تشفير تُعرف باسم "التغليف الأمني للحمولة". يمكن استيعاب كلٍّ من نمطي النفق والنقل.
- يحدّد أمن بروتوكول الإنترنت (IPSec) عدداً من أساليب إدارة المفاتيح.

لقد طوَّر مجتمع الإنترنت آليات أمن خاصة بتطبيقات معينة في عدد من مجالات التطبيق، بما في ذلك البريد الإلكتروني (S/MIME, PGP)، نظم زبون/خادم (Kerberos)، نظم الوصول إلى شبكة الويب (طبقة المقابس الآمنة SSL)، وغيرها. ومع ذلك فلدى المُستخدِمين بعض المخاوف الأمنية فيما يتعلق بكل طبقات البروتوكول. فعلى سبيل المثال، تستطيع مؤسسة ما تشغيل شبكة TCP/IP خاصة وآمنة من خلال حظر روابط المواقع غير الموثوق بها، وتشفير الرزم المغادرة لحدود المؤسسة، وتوثيق (authenticating) الرزم التي تدخل حدود المؤسسة. وهكذا فمن خلال تنفيذ الأمن على مستوى بروتوكول الإنترنت (IP)، يمكن لمؤسسة أن

تضمن أمن شبكاتها ليس فقط للتطبيقات التي تمتلك آليات أمنية ولكن أيضا بالنسبة للكثير من التطبيقات التي لا تمتلك تلك الآليات.

يشمل الأمن على مستوى بروتوكول الإنترنت (IP) ثلاث وظائف أساسية: التوثيق (authentication)، والسرية (confidentiality)، وإدارة المفاتيح (key management). تضمن آلية التوثيق أن الرزمة المُستلمة قد أُرسِلت فعلاً من قِبَل الطرف المعرّف كمصدر لها في ترويسة الرزمة. بالإضافة لذلك، تضمن تلك الآلية أن الرزمة لم يتم تغييرها أثناء انتقالها. أما وظيفة السرية فتتيح لطرفي الاتصال تشفير رسائلهم المتبادلة لمنع تنصت أي طرف ثالث، بينما تختص وظيفة إدارة المفاتيح بعملية التبادل الآمن للمفاتيح.

نبدأ هذا الفصل بلمحة عامة عن أمن بروتوكول الإنترنت (IPSec) ومقدمة لبنية ذلك البروتوكول. بعد ذلك نلقي نظرةً تفصيليةً على مجالات كلٍّ من الوظائف الأساسية الثلاث. ويتضمن ملحق هذا الفصل مراجعةً لبروتوكولات الإنترنت.

1-6 لمحة عامة عن أمن بروتوكول الإنترنت

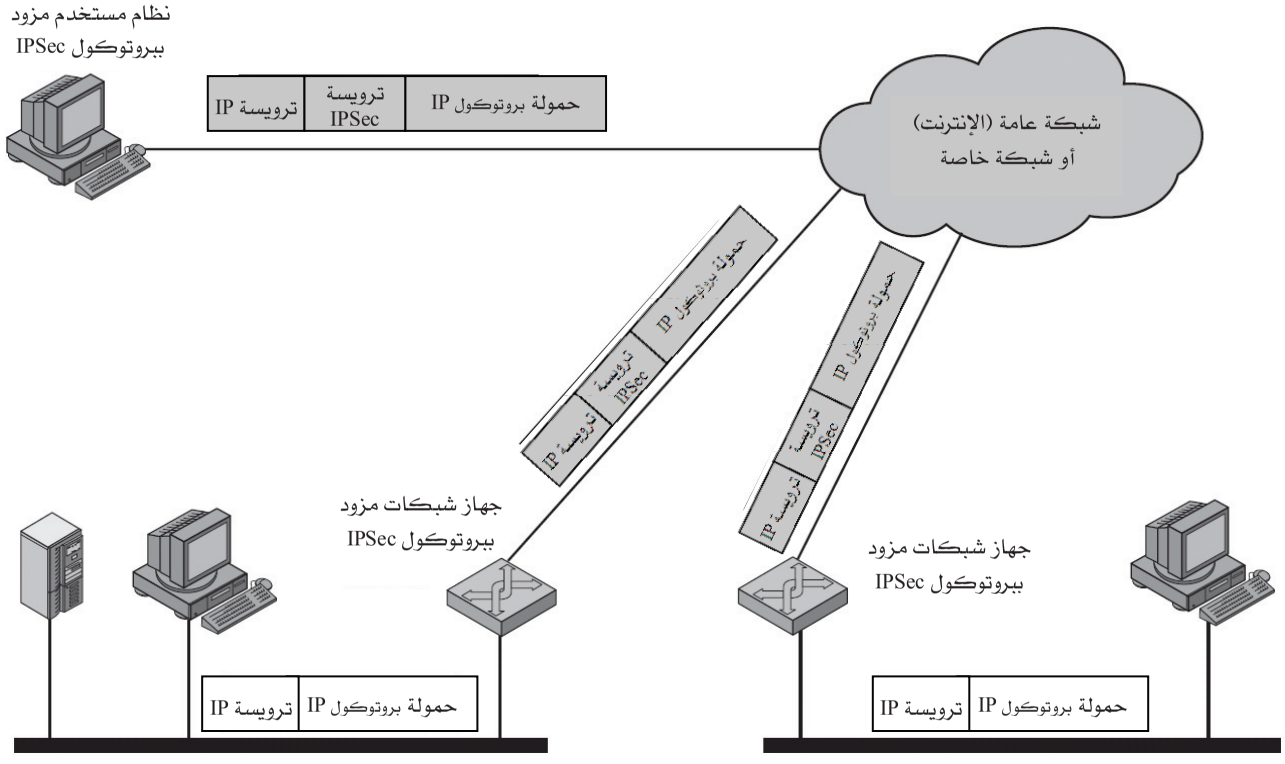
استجابةً لتلك القضايا، قام مجلس البنية المعمارية للإنترنت (IAB) بإدراج التوثيق والتشفير كسِمات أمن ضرورية في الجيل المقبل من بروتوكول الإنترنت، والذي صدَر باسم IPv6. ولحسن الحظ، فقد صُممت تلك الإمكانات الأمنية بحيث يمكن استخدامها مع كلٍّ من إصدار IPv4 الحالي وإصدار IPv6 المستقبلي. وهذا يعني أن منتجي البرمجيات يمكنهم البدء بتوفير تلك الميزات من الآن، وقد قام كثيرٌ منهم بالفعل بتضمين تلك الإمكانات الأمنية (IPSec) في منتجاتهم.

1-1-6 تطبيقات أمن بروتوكول الإنترنت (IPSec)

يوفر أمن بروتوكول الإنترنت (IPSec) إمكانية تأمين الاتصالات عبر الشبكات المحلية والشبكات الواسعة سواءً كانت عامة أو خاصة، وكذلك عبر الإنترنت. ومن أمثلة تلك الاستخدامات ما يأتي:

- تأمين الاتصال بمكتب فرعي عبر الإنترنت: يمكن لشركة إنشاء شبكة خاصة افتراضية ((virtual private network (VPN آمنة عبر الإنترنت أو عبر شبكة واسعة عامة (WAN). وبهذه الطريقة يمكن للشركات الاعتماد بشكلٍ كبير على شبكة الإنترنت ومن ثم تقليل احتياجاتها من الشبكات الخاصة، مما يوفر عليها كثيراً من التكاليف وأعباء إدارة الشبكة.
- الوصول الآمن عن بُعد عبر الإنترنت: يمكن لمستخدمٍ طريفٍ مزوّد ببروتوكولات أمن الإنترنت (IP security protocols) إجراء مكالمة محلية لموفر خدمة الإنترنت (ISP) والوصول من خلالها بشكلٍ آمن إلى شبكة الشركة، مما يقلل من تكاليف سفر عدد من الموظفين وانتقالهم إلى موقع الشركة يومياً.
- إنشاء توصيلات إكسترانت وإنترانت مشتركة مع الشركاء: يمكن أن يُستخدم بروتوكول IPSec لتأمين الاتصال مع المؤسسات الأخرى، بما يضمن الموثوقية والسرية ويوفر آلية لتبادل المفاتيح.
- تعزيز أمن التجارة الإلكترونية: رغم أن بعض تطبيقات الويب وبعض تطبيقات التجارة الإلكترونية مزودة ببروتوكولات أمنية مبيّتة كجزءٍ منها، فإن استخدام IPSec يعزز من هذا الأمن.

تكمن الميزة الرئيسة لبروتوكول IPSec – التي تمكنه من دعم تلك التشكيلة الكبيرة من التطبيقات المتنوعة – في أنه يمكنه تشفير و/أو توثيق كل حركة مرور للبيانات على مستوى بروتوكول الإنترنت (IP). ولذا، فإنه يمكن تأمين كافة التطبيقات الموزعة، بما في ذلك الوصول عن بُعد (remote logon)، وتطبيقات زبون/خادم، والبريد الإلكتروني، ونقل الملفات، والوصول إلى شبكة الويب، وهلم جرا.



الشكل 6-1: أحد سيناريوهات بروتوكول IP.

يوضّح الشكل 6-1 مثالاً لأحد السيناريوهات النمطية لاستخدام بروتوكول IPSec. تمتلك مؤسسة عدة شبكات محلية في مواقع متفرقة. يُستخدم بروتوكول الإنترنت IP غير الآمن على كلٍّ من تلك الشبكات المحلية. أمَّا حركة البيانات بعيداً عن مواقع المؤسسة فتستخدم بروتوكول IPSec عبر شبكة واسعة (WAN) عامة أو خاصة، حيث يجري تنفيذ تلك البروتوكولات في أجهزة الشبكات، كالموجّهات (routers) أو جدران الحماية النارية (firewalls)، والتي تربط كلاً من الشبكات المحلية بالعالم الخارجي. تقوم أجهزة بروتوكول IPSec تلك على الشبكة في العادة بتشفير (encrypt) وضغط (compress) كل البيانات التي تمر من الشبكة المحلية إلى الشبكة الواسعة العامة، وكذلك إزالة تشفير (decrypt) وفك ضغط (decompress) كل البيانات التي تمر من الشبكة الواسعة إلى الشبكة المحلية. ويلاحظ أن تلك العمليات تكون شفافة بالنسبة لمحطات العمل والخادمات على الشبكة المحلية. يمكن أيضاً تأمين نقلٍ آمن للبيانات لأفراد المُستخدِمين الذين يتصلون بالشبكة الواسعة (WAN) عن طريق وصلة مودم هاتفي. ينبغي أن تقوم محطات العمل التي يستعملها هؤلاء المُستخدِمين بتنفيذ بروتوكولات IPSec لتوفير الأمن لهم.

6-1-2 فوائد أمن بروتوكول الإنترنت

عدّد [MARK97] المزايا الآتية لبروتوكول IPSec:

- عند تنفيذ بروتوكول IPSec في جدار حماية (firewall) أو موجّه (router)، فإنه يوفر أمناً قوياً يمكن تطبيقه على كل حركة مرور البيانات التي تعبر حدود شبكة المؤسسة في كلا الاتجاهين. أما داخل نطاق المؤسسة أو مجموعة العمل فلن تعاني حركة المرور من الأعباء الإضافية الناجمة عن المعالجة الأمنية التي يتطلبها بروتوكول IPSec.
- عند تنفيذ بروتوكول IPSec في جدار حماية فإنه يقاوم محاولات التجاوز إذا تعيّن على كل حركة المرور الواردة من الخارج استخدام بروتوكول

الإنترنت (IP) وكان جدار الحماية هو المعبر الوحيد لدخول البيانات من الإنترنت إلى المؤسسة.

- نظراً لوجود بروتوكول IPSec أسفل طبقة النقل (TCP، UDP) فإنه يكون شفافاً بالنسبة للتطبيقات، لذا فلا حاجة لتغيير أي برمجيات على نظام لمستخدم ولا على نظام لخادم إذا ما كان IPSec مُنفَّذاً في الجدار الناري أو الموجّهات. وحتى في حالة تنفيذ IPSec على الأنظمة الطرفية، فإن برمجيات الطبقة العليا (بما في ذلك التطبيقات) لن تتأثر.
- يمكن أن يكون بروتوكول IPSec شفافاً للمستخدمين الطرفيين، ولذا فلا حاجة لتدريب المُستخدِمين على آليات الأمن، ولا لإصدار مفاتيح خاصة لكل مستخدم أو إلغاء تلك المفاتيح عندما يترك المُستخدِم العمل.
- يمكن أن يوفر بروتوكول IPSec الأمن لأفراد المُستخدِمين إذا لزم الأمر، وهذا أمر مفيد للعاملين الذين يبعدون عن موقع العمل وكذلك لإقامة شبكة فرعية افتراضية آمنة داخل المؤسسة للتطبيقات الحساسة.

6-1-3 تطبيقات التوجيه

بالإضافة إلى دعم المُستخدِمين الطرفيين وحماية أنظمة المؤسسة وشبكاتها، يمكن لبروتوكول IPSec أن يؤدي دوراً حيوياً في بنية التوجيه المُستخدَمة لتوصيل الشبكات مع بعضها. ويعدّد المرجع [HUIT98] الأمثلة الآتية لاستخدام بروتوكول IPSec في التأكد مما يأتي:

- أن الإعلان عن موجّه (أي موجّه جديد يعلن عن نفسه) يأتي من موجّه موثوق.
- أن الإعلان عن جار (أي موجّه يسعى إلى إنشاء أو الحفاظ على علاقة جوار مع موجّه في مجال توجيه آخر) يأتي من موجّه موثوق.
- أن رسالة إعادة التوجيه تأتي من الموجّه الذي تم إرسال الرزمة الأولية إليه.
- أن عملية تحديث جداول التوجيه (routing update) غير مزيفة.

بدون هذه التدابير الأمنية يمكن للخَصْم عرقلة الاتصالات أو تحويل اتجاه بعض حركة المرور. ينبغي أن تعمل بروتوكولات التوجيه – مثل بروتوكول OSPF – فوق الارتباطات الأمنية بين الموجّهات ويتم تعريفها بواسطة بروتوكول IPSec.

2-6 البنية الأمنية لبروتوكول الإنترنت (IP)

لقد أصبحت مواصفات بروتوكول IPSec معقدةً للغاية. وللتعرف على البنية العامة لهذا البروتوكول سنبدأ باستعراض الوثائق التي تُعرِّف البروتوكول، ثم نناقش خدمات IPSec ونتناول مفهوم ارتباطات الأمن (security association).

1-2-6 وثائق أمن بروتوكول الإنترنت

تتكون مواصفات أمن بروتوكول الإنترنت من عدد من الوثائق، أهمها ما صدر في نوفمبر عام 1998 وتشمل طلبات التعليقات (RFC) أرقام 2401، 2402، 2406، 2408:

- طلب التعليقات 2401: لمحة عامة عن البنية الأمنية لـ IPSec .
- طلب التعليقات 2402: وصف لتوثيق الرزمة كامتداد لـ IPv4 وIPv6.
- طلب التعليقات 2406: وصف لتشفير الرزمة كامتداد لـ IPv4 وIPv6.
- طلب التعليقات 2408: مواصفات الإمكانات الخاصة بإدارة المفاتيح.

يُعدُّ دعم هذه السمات إلزامياً لـ IPv6 واختيارياً لـ IPv4. في كلتا الحالتين، يتم تنفيذ السمات الأمنية كترويسات مُلحقة تتبع ترويسة بروتوكول الإنترنت (IP) الرئيسة. وتُعرف الترويسة المُلحقة للتوثيق بترويسة التوثيق والترويسة المُلحقة للتشفير بترويسة حمولة الأمن المغلّفة (Encapsulating Security Payload (ESP)).

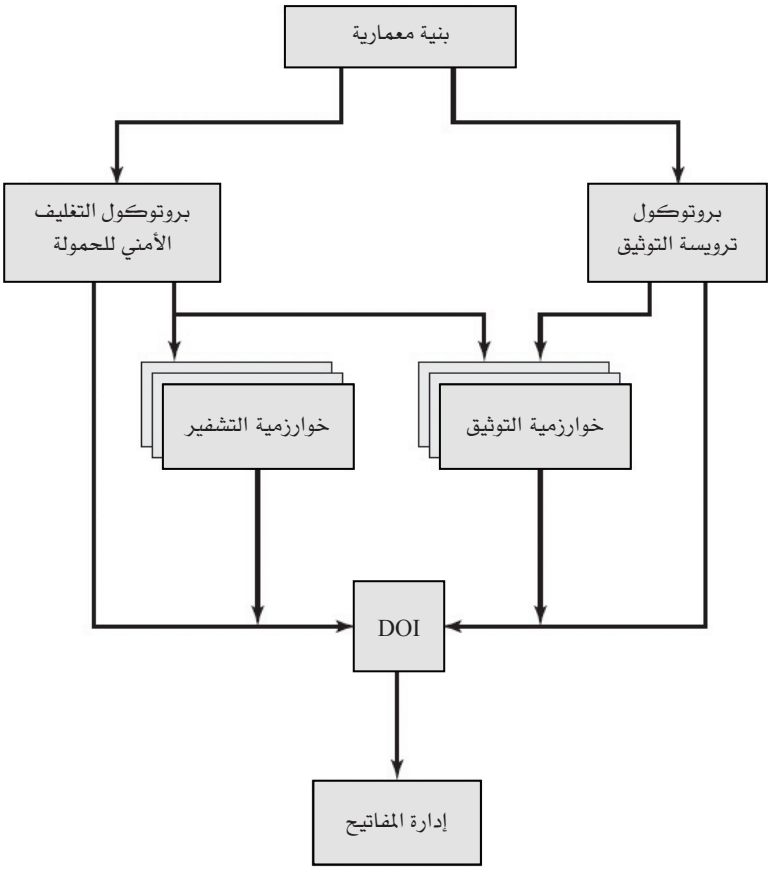
بالإضافة إلى الوثائق الأربع المذكورة، فقد تم نشر عدد من المسودات الإضافية بواسطة مجموعة عمل بروتوكول أمن الإنترنت (IP Security Protocol

(Working Group من قِبَل فريق مهام هندسة الإنترنت (IETF). وتقسم الوثائق إلى سبع مجموعات، كما هو مبين في الشكل 6-2 (طلب التعليقات 2401):

- البنية: تتناول المفاهيم العامة، والمتطلبات الأمنية، والتعريفات، وآليات تقنية IPSec.
- حمولة الأمن المغلّفة (ESP): تغطي صيغة الرزمة (format) والأمور العامة المتصلة باستخدام ESP لتشفير الرزمة وكذلك توثيقها (إن لزم الأمر).
- ترويسة التوثيق ((Authentication Header (AH): تغطي صيغة الرزمة والأمور العامة التي تتعلق باستخدام AH لتوثيق الرزمة.
- خوارزمية التشفير: مجموعة من الوثائق التي تصف كيفية استخدام خوارزميات تشفير مختلفة لـ ESP.
- خوارزمية التوثيق: مجموعة من الوثائق التي تصف كيفية استخدام خوارزميات التوثيق المختلفة لـ AH ولخيار التوثيق في ESP.
- إدارة المفاتيح: الوثائق التي تصف أنظمة إدارة المفاتيح.
- نطاق التفسير: يتضمن القيم المطلوبة للوثائق الأخرى حتى يمكن ربط الوثائق بعضها ببعض. ويشمل ذلك أسماء خوارزميات التشفير والتوثيق المصرح بها، وكذلك قيم مُعامِلات التشغيل كأعمار المفاتيح.

6-2-2 خدمات أمن بروتوكول الإنترنت (IPSec)

يقدم بروتوكول IPSec خدمات أمنية لطبقة بروتوكول الإنترنت (IP) من خلال تمكين النظام من اختيار البروتوكولات الأمنية المطلوبة، وتحديد خوارزميات الخدمات، وحفظ مفاتيح التشفير اللازمة لتفعيل الخدمات المطلوبة. ولتوفير الأمن يستخدم IPSec بروتوكولين: الأول عبارة عن بروتوكول توثيق يتم تحديده بواسطة ترويسة البروتوكول – أي ترويسة التوثيق (AH) – أما الثاني فبروتوكول مشترك للتشفير والتوثيق يتم تحديده من قِبَل صيغة (format) رزمة هذا البروتوكول؛ حمولة الأمن المغلفة (ESP). يقدم IPSec الخدمات الأمنية الآتية:



الشكل 6-2: عرض عام لوثائق بروتوكول IPSec.

الجدول 6-1 خدمات بروتوكول IPSEC.

	التغليف الأمني للحمولة (تشفير مع توثيق)	التغليف الأمني للحمولة (تشفير فقط)	ترويسة التوثيق
التحكم في الوصول	✓	✓	✓
السلامة اللاتوصيلية	✓		✓
توثيق منشأ البيانات	✓		✓
رفض الرزم المعاد إرسالها	✓	✓	✓
السرية	✓	✓	
سرية محدودة لتدفق حركة المرور	✓	✓	

- التحكم في الوصول (Access control).
- السلامة اللاتوصيلية (Connectionless integrity).
- توثيق منشأ البيانات (Data origin authentication).
- رفض الرزم المعاد إرسالها (Rejection of replayed packets) (شكل من أشكال سلامة التسلسل الجزئي).
- السرية (Confidentiality).
- سرية محدودة لتدفق حركة المرور (Limited traffic flow confidentiality).

يبيّن الجدول 6-1 الخدمات التي يوفرها بروتوكولا AH وESP. هناك حالتان لبروتوكول ESP؛ مع وبدون خيار التوثيق. و يُعدُّ كلٌّ من AH وESP وسيلة للتحكم في الوصول مبنية على أساس توزيع مفاتيح التشفير وإدارة تدفق حركة المرور بالنسبة لتلك البروتوكولات الأمنية.

6-2-3 الارتباطات الأمنية

يُعدُّ الارتباط الأمني (security association (SA)) مفهوماً أساسياً في آليات كلٍّ من التوثيق والسرية لبروتوكول الإنترنت (IP). ويُعَرَّف الارتباط بأنه علاقة في اتجاه واحد بين مرسل ومستقبِل توفر خدماتٍ أمنية لحركة المرور على هذه العلاقة. عند الحاجة لإقامة علاقة أقران (peer relationship) لتبادل المعلومات بطريقة أمنة في كِلا الاتجاهين، فإنه ينبغي استخدام ارتباطين أمنيين. وتُقَدم الخدمات الأمنية لارتباط أمنى للاستخدام إما من قِبَل AH أو ESP ، ولكن ليس كليهما.

ويحدّد الارتباط الأمني تماماً بمعرفة ثلاثة مُعامِلات:

- مؤشر المُعامِلات الأمنية (Security Parameters Index (SPI)): سلسلة من البتات تخصص لهذا الارتباط الأمني وتكون ذات دلالة محلية. ويتم نقل SPI في ترويسات AH وESP لتمكين نظام المستقبِل من اختيار الارتباط الأمني الذي تتم على أساسه معالجة الرزمة المستلَمة.

- عنوان IP للوجهة: هذا هو عنوان الوِجهة للارتباط الأمني، والذي يمكن أن يكون نظاماً طرفياً أو أحد أنظمة الشبكة كجدارٍ ناري مثلاً أو موجّه. وفي الوقت الحالي، يُسمح فقط بالعناوين أحادية الإرسال (unicast).
- معرِّف بروتوكول الأمن: يبيّن ما إذا كان هذا الارتباط ارتباطاً أمنياً خاصاً بـ AH أو ESP.

لذلك، ففي أي رزمة IP [1]، يُعَرَّف الارتباط الأمني بواسطة عنوان الوِجهة في ترويسة IPv4 أو IPv6 بالإضافة إلى مؤشر المُعامِلات الأمنية (SPI) في ترويسة الامتداد المُلحقة (AH أو ESP).

❖ مُعامِلات الارتباط الأمني:

في كل تنفيذ لبروتوكول IPSec، توجد قاعدة بيانات أساسية [2] للارتباطات الأمنية تحدّد المُعامِلات الخاصة بكل ارتباط أمني. وعادةً ما يُعَرَّف الارتباط الأمني بالمُعامِلات الآتية:

- عدّاد الرقم التسلسلي: بقيمة طولها 32 بتاً، ويستخدم في توليد حقل الرقم التسلسلي في ترويسة AH أو ESP، كما سيوضّح في الجزء 3-6 (لازم لجميع التنفيذات).
- فيض الرقم التسلسلي: مؤشر يدل على ما إذا كان فيض عداد الرقم التسلسلي ينبغي أن يؤدي إلى حدث يتطلب التدقيق وإلى منع انتقال المزيد من الرزم على هذا الارتباط الأمني أم لا (لازم لجميع التنفيذات).
- النافذة المضادة لإعادة الإرسال: تُستخدم لتحديد ما إذا كانت رزمة AH أو ESP الواصلة قد أعيد إرسالها، كما سيوضّح بالجزء 3-6 (لازمة لجميع التنفيذات).

---

[1] في هذا الفصل تشير رزمة IP إلى وحدة بيانات IPV4 أو رزمة بيانات IPV6.

[2] أساسية بمعنى أن الوظائف التي توفرها قاعدة بيانات الارتباط الأمني يجب أن تكون موجودة في أي تنفيذ لـ IPSec، ولكن الطريقة التي يتم بها توفير تلك الوظائف ترجع إلى المنفّذ.

- معلومات AH: وتشمل خوارزمية التوثيق،والمفاتيح، وأعمار المفاتيح، والمتغيرات ذات الصلة المستخدمة مع AH (لازمة لتنفيذات AH).
- معلومات (ESP): وتشمل خوارزمية التشفير والتوثيق، ومفاتيحها، وقيم التهيئة الخاصة بها، وأعمار المفاتيح، والمتغيرات ذات الصلة المستخدمة مع ESP (لازمة لتنفيذات ESP).
- عمر هذا الارتباط الأمني: وهو الفترة الزمنية أو عدد البايتات التي يجب بعدها إما استبدال الارتباط الأمني بآخر جديد (ومُعامِل أمني SPI جديد) أو إنهاؤه، بالإضافة إلى مؤشر للدلالة على أيٍّ من هذين الإجراءين ينبغي اتخاذه (لازم لجميع التنفيذات).
- نمط بروتوكول IPSec: ويشمل نمط النفق (Tunnel)، ونمط النقل (Transport)، ونمط الرمز العام (Wildcard) (لازم لجميع التنفيذات). وستتم مناقشة هذه الأنماط لاحقاً في هذا الجزء.
- MTU [3] للمسار: وهي أقصى وحدة إرسال مُلاحَظَة للمسار والمتغيرات التي طالت فترة تواجدها (لازمة لجميع التنفيذات).

تُقرَن آلية إدارة المفاتيح التي يتم استخدامها لتوزيع المفاتيح بآليات التوثيق والخصوصية عن طريق المُعامِل الأمني فقط. ومن ثَمَّ يتم تحديد التوثيق والخصوصية بشكلٍ مستقل عن أي آلية محدّدة لإدارة المفاتيح.

[3] MTU = Maximum Transmission Unit : الوحدة القصوى للإرسال، وهو أقصى حجم ممكن لرزمة بحيث يمكن إرسالها من دون تجزئة

❖ مُعامِلات اختيار الارتباط الأمني (SA Selectors):

يوفر بروتوكول IPSec للمستخدم قدرا كبيرا من المرونة من حيث طريقة تطبيق خدمات IPSec على حركة مرور بروتوكول الإنترنت (IP). وكما سنرى لاحقا، يمكننا الجمع بين عدة ارتباطات أمنية بأكثر من طريقة للحصول على التشكيلة المطلوبة للمُستخدِم. وعلاوةً على ذلك، يتميز IPSec بقدرة عالية على الفرز والتمييز بين حركة المرور المحميّة بـ IPSec والأخرى المسموح لها بتجاوز قيود IPSec، وفي الحالة الأولى الربط بين حركة مرور IP والارتباطات الأمنية الخاصة بها.

يتم الربط بين حركة مرور IP وارتباطات أمنية معينة (أوبدون أي ارتباطات أمنية في حالة حركة المرور المسموح لها بتجاوز IPSec) بواسطة قاعدة بيانات السياسة الأمنية ((Security Policy Database (SPD). في أبسط أشكالها، تحتوي قاعدة بيانات السياسة الأمنية على مُدخَلات يُعَرِّفُ كلٌّ منها مجموعةً فرعيةً من حركة مرور IP ويشير إلى الارتباط الأمني الخاص بها. أما في بيئات أكثر تعقيداً، فقد يوجد عدة مُدخَلات تربط بين نفس المجموعة الفرعية من حركة مرور IP وعدة ارتباطات أمنية أو بين ارتباط أمني واحد وعدة مجموعات فرعية من حركة مرور IP. ويمكن للقارئ الاطلاع على وثائق IPSec ذات الصلة للحصول على تفاصيل أكثر.

ويُعرَّف كل مُدخل لقاعدة البيانات SPD بمجموعة من قيم حقول بروتوكول الإنترنت (IP) وبروتوكولات الطبقة العليا، تسمى مُعامِلات الاختيار (selectors). وفي الواقع، تُستخدَم تلك المُعامِلات لتصفية حركة المرور الصادرة لربطها بارتباط أمني معين. وتعالَج كل رزمة IP صادرة كما يأتي:

1. قارن قيم حقول مُعامِلات الاختيار في الرزمة بقاعدة بيانات السياسة الأمنية (SPD) لإيجاد مُدخل مطابق، والذي قد يشير إلى صفر أو عدد أكبر من الارتباطات أمنية.
2. حدّد الارتباطات الأمنية لتلك الرزمة، إن وجدت، بالإضافة إلى مؤشر المُعامِلات الأمنية (SPI) لها.
3. قم بمعالجة IPSec المطلوبة (أي معالجة AH أوESP).

ويتحدّد مُدخل قاعدة بيانات السياسة الأمنية بمُعامِلات الاختيار الآتية:

- عناوين IP للوِجهة: والتي قد تكون عنواناً واحداً، أو قائمة تضم عناوين محدّدة، أو مدى متصلاً من العناوين، أوعنوان قناع (mask) برمز عام (wildcard). والصنفان الأخيران مطلوبان لدعم عددٍ من أنظمة الوِجهة لها نفس الارتباط الأمني (كأن تكون مثلاً خلف نفس جدار الحماية الناري).
- عناوين IP للمصدر: والتي قد تكون عنواناً واحداً، أو قائمة تضم عناوين محدّدة، أو مدى متصلاً من العناوين، أوعنوان قناع برمز عام (wildcard). الصنفان الأخيران مطلوبان لدعم عددٍ من أنظمة المصدر لها نفس الارتباط الأمني (كأن تكون مثلاً خلف نفس جدار الحماية الناري).

- هوية المستخدم (UserID): مُعَرِّف للمستخدم من نظام التشغيل. ليس هذا حقلاً في بروتوكول الإنترنت IP ولا في ترويسات الطبقات العليا ولكنه يكون متاحاً إذا ما كان IPSec يعمل على نفس نظام تشغيل المُستخدِم.
- مستوى حساسية البيانات: يُستخدم للأنظمة التي تقوم بتأمين تدفق المعلومات (مثلاً سرِّي (secret) أو غير سرِّي (unclassified)).
- بروتوكول طبقة النقل: يتم الحصول عليه من حقل "الترويسة التالية" (Next Header) لبروتوكول IPv4 أو IPv6. وقد يكون ذلك رقم بروتوكول واحد، أو قائمة بأرقام بروتوكولات محدّدة، أو مدى متصل من أرقام البروتوكولات.
- منافذ المصدر والوِجهة: وقد تكون قيمة منفذ TCP أو UDP واحد، أو قائمة بتلك المنافذ، أومنفذ بالرمز العام (wildcard).

4-2-6 نمط النقل ونمط النفق

يدعم كلٌّ من AH وESP نمطين للاستخدام هما نمط النقل ونمط النفق. ويمكن فهم هذين النمطين بشكلٍ أفضل في سياق وصف AH وESP، كما سيتم في الجزأين 6-3 و6-4 على التوالي. أما هنا فنكتفي بلمحة موجزة.

❖ نمط النقل:

يوفر نمط النقل الحماية لبروتوكولات الطبقة العليا في المقام الأول، بمعنى أن حماية نمط النقل تمتد إلى الحمولة لرزمة بروتوكول الإنترنت (IP). ومن الأمثلة على ذلك قطعة TCP أو UDP أو رزمة ICMP، وجميعها تعمل مباشرة فوق بروتوكول الإنترنت في رصة بروتوكول المضيف. وعادةً ما يُستخدم نمط النقل في الاتصالات من طرف إلى طرف بين مضيفين (على سبيل المثال، عميل وخادم، أو محطتي عمل). وعندما يقوم مضيف بتشغيل AH أو ESP على IPv4، تكون الحمولة هي البيانات التي عادةً ما تتبع ترويسة بروتوكول الإنترنت (IP). أما في حالة IPv6، فتكون الحمولة هي البيانات التي تتبع عادةً كلاً من ترويسة بروتوكول الإنترنت (IP) وأيّاً من ترويسات امتدادات IPv6 المُستخدَمة، مع احتمال استثناء ترويسة خيارات الوِجهة التي يمكن أن تُضَمَّن في الحماية.

يقوم ESP في نمط النقل بتشفير الحمولة لبروتوكول الإنترنت (IP) وتوثيقه اختياريا ولا يتم ذلك مع ترويسة بروتوكول الإنترنت (IP). أما AH فيقوم في نمط النقل بتوثيق الحمولة لبروتوكول الإنترنت (IP) وأجزاء مختارة من ترويسة بروتوكول الإنترنت (IP).

❖ نمط النفق:

يوفر نمط النفق الحماية لرزمة بروتوكول الإنترنت (IP) بكاملها. ولتحقيق ذلك، تُضاف حقول AH أو ESP إلى رزمة بروتوكول الإنترنت، ثم تُعامَل الرزمة بأسرها بالإضافة إلى الحقول الأمنية على أنها الحمولة لرزمة IP "خارجية" جديدة بترويسة IP خارجية جديدة. وتسير الرزمة الأصلية (أو الداخلية) بأكملها عبر "نفق"

من نقطة على شبكة بروتوكول الإنترنت (IP) إلى النقطة التي تليها، ولا يمكن لأيٍّ من الموجّهات على طول المسار فحص ترويسة بروتوكول الإنترنت الداخلية. ولأن الرزمة الأصلية مغلّفة، فإن الرزمة الأحدث والأكبر قد يكون لها عنواني مصدر ووِجهة مختلفين تماما مما يرفع من مستوى الأمن. ويُستخدَم نمط النفق عندما يكون أحد طرفي الارتباط الأمني أو كلاهما بوابة أمنية تُطبّق IPSec كجدار حماية ناري أو موجّه.

وفي نمط النفق، يستطيع عددٌ من المضيفين على شبكات خلف جدران نارية الاتصال الآمن مع بعضهم بعضاً دون تنفيذ IPSec. وتُنقل الرزم غير المحمية الصادرة عن المضيفين في مثل هذا الاتصال بنمط النفق عبر نفق خلال الشبكات الخارجية باستخدام الارتباطات الأمنية المثبَّتة عن طريق برمجيات IPSec في الجدران النارية أو الموجّهات الآمنة على حدود الشبكة المحلية.

فيما يأتي مثالٌ على كيفية عمل نمط النفق ببروتوكول IPSec. يُرسِل المضيف A رزمة IP على الشبكة بعنوان وِجهة للمضيف B على شبكة أخرى. تُوجَّه هذه الرزمة من المضيف الأصلي (المُرسِل) إلى جدار الحماية أو إلى موجّه آمن على حدود شبكة المضيف A، يقوم جدار الحماية بتصفية جميع الرزم الصادرة لتحديد مدى الحاجة لمعالجة IPSec. إذا كانت تلك الرزمة من المضيف A إلى المضيف B تتطلب IPSec، يقوم جدار الحماية بمعالجتها تبعاً لـ IPSec وتغليفها بترويسة IP خارجية. ويكون عنوان IP للمصدر لتلك الرزمة الخارجية هو عنوان جدار الحماية ذاك، أما عنوان الوِجهة فيمكن أن يكون عنوان جدار الحماية الذي يشكِّل حدود الشبكة المحلية للمضيف B. وتُوجَّه تلك الرزمة إلى جدار حماية المضيف B. تقوم موجّهات المسار بتفحُّص ترويسة IP الخارجية فقط. وعند جدار حماية المضيف B، تُنزع ترويسة بروتوكول الإنترنت الخارجية ويتم تسليم الرزمة الداخلية للمضيف B.

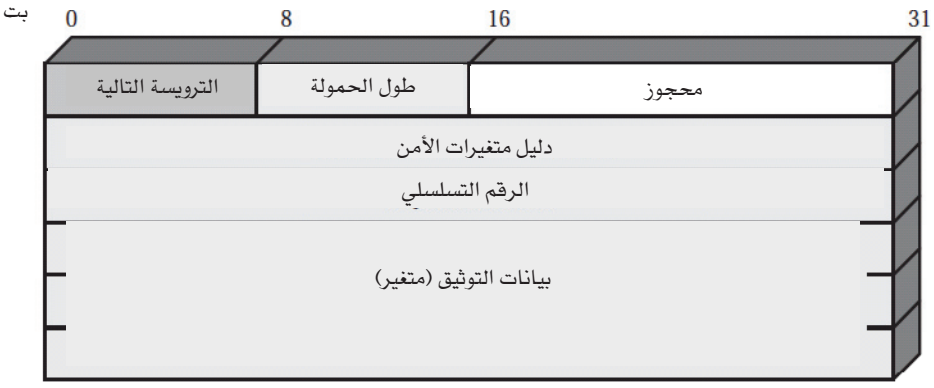
يقوم ESP في نمط النفق بتشفير رزمة بروتوكول الإنترنت الداخلية كاملةً وتوثيقها اختياريا، بما في ذلك ترويسة IP الداخلية. يقوم AH في نمط النقل بتوثيق رزمة بروتوكول الإنترنت الداخلية كاملةً وأجزاء مختارة من ترويسة IP الخارجية.
ويلخص الجدول 6-2 طريقة عمل نمطي النقل والنفق.

3-6 ترويسة التوثيق

توفّر ترويسة التوثيق دعماً لسلامة بيانات رزم بروتوكول الإنترنت (IP) وتوثيقها. تضمن ميزة سلامة البيانات استحالة أن تمر أي تغيّرات في محتوى الرزمة خلال مسارها بدون اكتشاف. أما عملية التوثيق فتُمكّن أيّ نظام طرفي أو جهاز على الشبكة من توثيق المستخدم أو التطبيق، ثم تقوم بتصفية حركة المرور بناءً على ذلك، كما تمنع هجمات تزييف العنوان (spoofing) المنتشرة حالياً على الإنترنت. تحمي ترويسة التوثيق أيضاً ضد هجوم إعادة الإرسال (replay attack) الذي سيتم وصفه لاحقاً في هذا الجزء.

الجدول 6-2 وظائف نمطي النفق والنقل.

	ارتباط أمني بنمط النقل	ارتباط أمني بنمط النفق
ترويسة التوثيق	توثيق حمولة بروتوكول IP وأجزاء محدّدة من ترويسة التوثيق، وترويسات IPv6 ملحقة	توثيق ترويسة بروتوكول IP الداخلية كاملةً (الترويسة الداخلية + حمولة بروتوكول IP) + أجزاء محدّدة من ترويسة بروتوكول IP الخارجية وترويسات IPv6 الملحقة الخارجية
التغليف الآمني للحمولة	تشفير حمولة بروتوكول IP بالإضافة إلى أيٍّ من ترويسات IPv6 الملحقة والتي تلي ترويسة التغليف الآمن للحمولة	تشفير رزمة بروتوكول IP الداخلية كاملةً
التغليف الأمني للحمولة مع التوثيق	تشفير حمولة بروتوكول IP بالإضافة إلى أيٍّ من ترويسات IPv6 الملحقة والتي تلي ترويسة التغليف الآمن للحمولة. توثيق حمولة بروتوكول IP ولكن ليس ترويسة بروتوكول IP.	تشفير حمولة بروتوكول IP الداخلية كاملةً. توثيق حمولة بروتوكول IP الداخلية كاملةً



الشكل 6-3: ترويسة التوثيق لبروتوكول IPSec.

يعتمد التوثيق على استعمال كود التحقق من الرسالة (ماك) (Message Authentication Code (MAC))، وكما هو موضّح في الفصل الثالث، يجب أن يشترك كلا الطرفين في المفتاح السري.

تتكون ترويسة التوثيق من الحقول الآتية (الشكل 6-3):

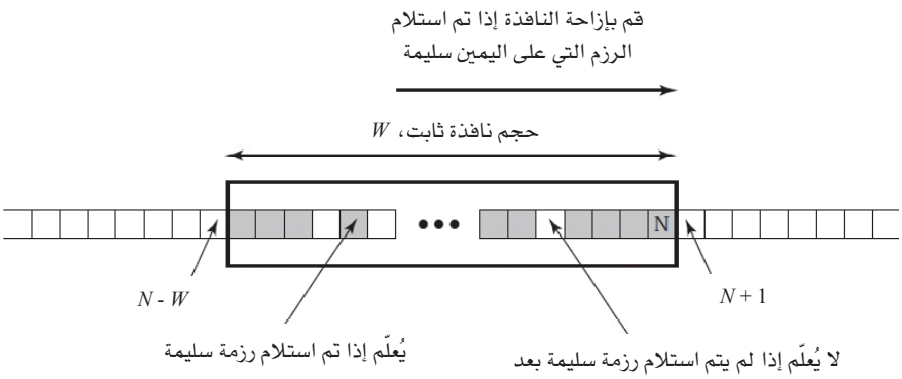
- الترويسة التالية (Next Header) (8 بتات): وتحدّد نوع الترويسة اللاحقة مباشرةً لهذه الترويسة.
- طول الحمولة (Payload Length) (8 بتات): وهو طول ترويسة التوثيق (مُقاساً بعدد الكلمات بطول 32 بتاً) ناقص 2. وعلى سبيل المثال، الطول المفترَض لحقل بيانات التوثيق هو 96 بتاً، أي ثلاث كلمات كلٌّ منها 32 بتاً). وبإضافة ثلاث كلمات هي طول الترويسة الثابتة، يكون طول الترويسة الكلي هو ستّ كلمات، ففي هذه الحالة يحتوي حقل طول الحمولة على القيمة 4 (أي 6 - 2 = 4).
- محجوز (Reserved) (16 بتاً): للاستخدام في المستقبل.
- مؤشر المُعامِلات الأمنية (Security Parameters Index): (32 بتاً): ويحدّد الارتباط الأمني.

- الرقم التسلسلي (Sequence Number) (32 بتاً): قيمة متزايدة لعدّاد، سيُناقَش لاحقاً.
- بيانات التوثيق (Authentication Data) (بطول متغيِّر): حقل متغير الطول (يجب أن يكون عدداً صحيحاً من كلمات 32- بت) ويتضمّن قيمة التحقق من السلامة (Integrity Check Value (ICV))، أو كود التحقق من الرسالة (ماك)، لهذه الرزمة، سيُناقَش لاحقاً.

6-3-1 الخدمة المضادة لإعادة الإرسال (Anti-Replay Service)

في هجوم إعادة الإرسال يحصل المهاجم على نسخة من الرزمة الموثّقة ثم يرسلها لاحقاً إلى الوِجهة المقصودة. وقد يؤدي استلام نسخ مكرّرة وموثقة من رزم بروتوكول الإنترنت (IP) إلى إرباك الخدمة بشكلٍ أو بآخر، أو إلى عواقب وخيمةٍ أخرى. وقد صُمِّم حقل الرقم التسلسلي لإحباط مثل تلك الهجمات. ولفهم ذلك سنناقش أولاً عملية توليد الرقم التسلسلي من قِبَل المُرسِل، ثم ننظر في الكيفية التي تتم بها معالجة هذا الرقم عند المُستلِم.

عندما يتم تأسيس ارتباط أمني جديد، يضع المُرسِل القيمة (0) في عداد الرقم التسلسلي. وفي كل مرة يتم فيها إرسال رزمة على هذا الارتباط الأمني، يقوم المُرسِل بزيادة قيمة العداد بواحد ويسجّل تلك القيمة في حقل الرقم التسلسلي. ومن ثَمَّ، فإن أول قيمة تُستخدم تكون 1. إذا كانت الخدمة المضادة لإعادة الإرسال مفعَّلة (وهو المُفترض أساساً) فينبغي ألا يسمح المُرسِل للرقم التسلسلي بالعودة من أقصى قيمة للعد (2^{32}-1) إلى نقطة الصفر حتى لا يسمح بوجود عدة رزم شرعية لها نفس الرقم التسلسلي. لذا فعند وصول العداد إلى القيمة (2^{32}-1) يجب على المُرسِل إنهاء ذلك الارتباط الأمني والتفاوض على ارتباط أمني جديد بمفتاح جديد.



الشـــكل 6-4: الآلية المضادة لإعادة الإرسال.

ونظراً لأن بروتوكول الإنترنت هوخدمة لاتوصيلية وغير موثوقة، فإن البروتوكول لا يضمن أن الرزم سيتم تسليمها بالترتيب ولا يضمن حتى أن كافة الرزم سيتم تسليمها. ولذلك فإن وثيقة IPSec الخاصة بالتوثيق تفرض على المتلقي أن يُنشئ نافذةً بحجم W، (بقيمة مُفترضة $W = 64$). ويُمثِّل أعلى رقم تسلسلي، N، ورد حتى الآن من الرزم الصالحة الحافة اليمنى للنافذة. يتم وضع علامة بالشريحة (fragment) المناظـرة في تلك النافذة (الشـكل 6-4) لأي رزمـة برقـم تسلسلي في النطـاق من $N - W + 1$ إلى N وتم استلامها بشكلٍ صحيح (أي موثّقة بشكلٍ مناسب). وعند استلام رزمة يتم معالجتها لدى المُستلم على النحو الآتي:

1. إذا وقعت الرزمة المستلَمة ضمن النافذة وكانت جديدة، يتم التحقق من كود ماك، فإذا كانت الرزمة موثّقة توضع علامة بالشريحة المناظرة في النافذة.
2. إذا كانت الرزمة المستلَمة على يمين النافذة وكانت جديدة، يتم التحقق من كود ماك، فإذا كانت الرزمة موثّقة يتم تقديم النافذة إلى اليمين فيكون الرقم التسلسلي هذا هو الحافة اليمنى للنافذة كما يتم وضع علامة بالشريحة المناظرة في النافذة.

3. إذا كانت الرزمة المستلَمة على يسار النافذة، أو في حالة فشل توثيقها، يتم تجاهل تلك الرزمة وتدوين هذا الحدث للمراجعة.

6-3-2 قيمة التحقق من السلامة (Integrity Check Value (ICV))

يحمل حقل بيانات التوثيق قيمة تُعرف بقيمة التحقق من السلامة (ICV). وهذه القيمة هي رمز توثيق الرسالة أو نسخة مبتورة (truncated) من الكود الناتج من خوارزمية ماك. وتنص المواصفات الحالية على ضرورة الالتزام بدعم ما يأتي:

- HMAC-MD5-96
- HMAC-SHA-1-96

وكلاهما يستخدم خوارزمية HMAC، الأولى مع خوارزمية خلاصة الرسائل MD5، والثانية مع كود التحوير الآمن SHA-1 (سبق مناقشة كلٍّ من تلك الخوارزميات في الفصل الثالث). في كلتا الحالتين يتم حساب القيمة الكاملة لـ HMAC ولكن بعد ذلك يتم بترها واستخدام الـ 96 بتاً الأولى فقط، والتي هي قيمة الطول المُفترَض لحقل بيانات التوثيق.

ويتم حساب كود التحقق من الرسالة (الماك) على:

- حقول ترويسة IP التي لا تتغير أثناء الانتقال (ثابتة) أو تلك التي يمكن التنبؤ بقيمتها عند وصولها إلى نقطة النهاية لهذا الارتباط الأمني لترويسة التوثيق. أما الحقول التي قد تتغير أثناء الانتقال، أو التي لا يمكن التنبؤ بقيمتها عند وصولها فيتم تعيين 0 كقيمة مبدئية لها بكلٍّ من المصدر والوِجهة لأغراض حسابية.
- ترويسة التوثيق AH فيما عدا حقل بيانات التوثيق. يتم تعيين 0 كقيمة مبدئية لحقل بيانات التوثيق بكلٍّ من المصدر والوِجهة لأغراض حسابية.
- بيانات بروتوكول المستوى الأعلى بأكملها، والتي يُفترَض أن تكون غير قابلة للتغيير أثناء الانتقال (على سبيل المثال، قطعة TCP أو رزمة IP داخلية في نمط النفق).

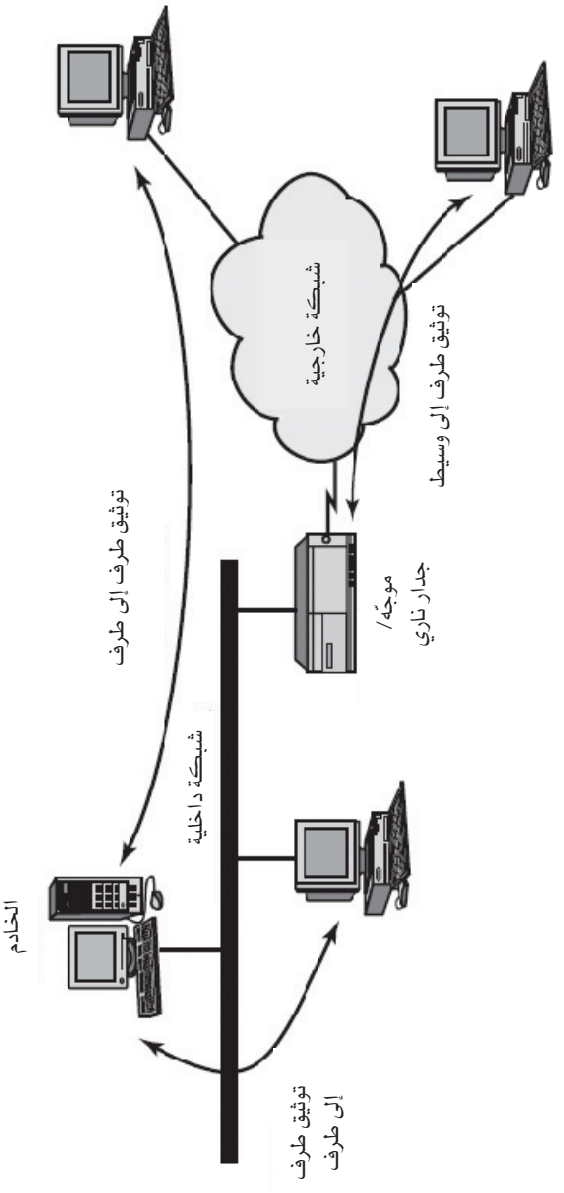
وكأمثلة على الحقول الثابتة في بروتوكول IPv4، هناك طول ترويسة الإنترنت وعنوان المصدر. ويعد عنوان الوِجهة (سواءً كان توجيه المصدر صارماً أو فضفاضاً) مثالاً على حقل قابل للتغيُّر ولكن يمكن التنبؤ به. أما أمثلة الحقول القابلة للتغيير ويتم تصفيرها قبل حساب ICV فتضم العُمر الافتراضي وحقول المجموع التدقيقي للترويسة. لاحظ أن كلاً من حقل عنوان المصدر وحقل عنوان الوِجهة محميّان، مما يمنع تزييف العناوين أو انتحالها.

بالنسبة لبروتوكول IPv6، فمن الأمثلة في الترويسة الرئيسة: رقم الإصدار (حقل ثابت)، وعنوان الوِجهة (حقل قابل للتغيُّر ولكن يمكن التنبؤ به)، ووسمة التدفق (قابل للتغير، ويُصفَّر لأغراض حسابية).

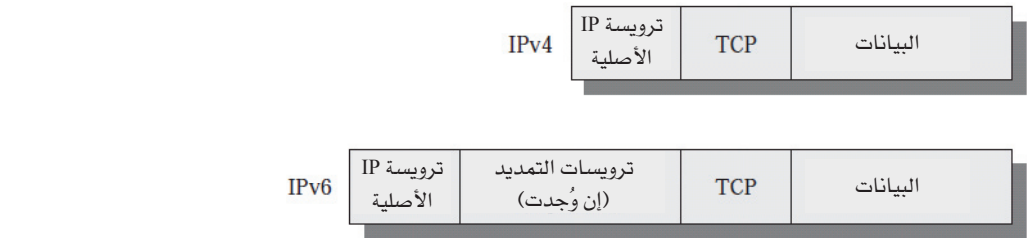
6-3-3 نمطا النقل والنفق

يوضّح الشكل 6-5 أسلوبين يُمكن من خلالهما استخدام خدمة توثيق IPSec. في الأسلوب الأول، يتم توفير خدمة التوثيق مباشرةً بين الخادم ومحطات عمل الزبون؛ ويمكن أن تكون محطات العمل تلك على نفس شبكة الخادم أو على شبكة خارجية. وطالما أن محطة العمل والخادم يشتركان في مفتاحٍ سريٍ محمي فإن عملية التوثيق تكون آمنة، يستخدم هذا الأسلوب الارتباط الأمني في نمط النقل. في الأسلوب الآخر، تُوثّق محطة العمل البعيدة نفسها للجدار الناري للمؤسسة، إما للنفاذ إلى الشبكة الداخلية بأكملها أو لأن الخادم المطلوب لا يدعم ميزة التوثيق، يستخدم هذا الأسلوب الارتباط الأمني في نمط النفق.

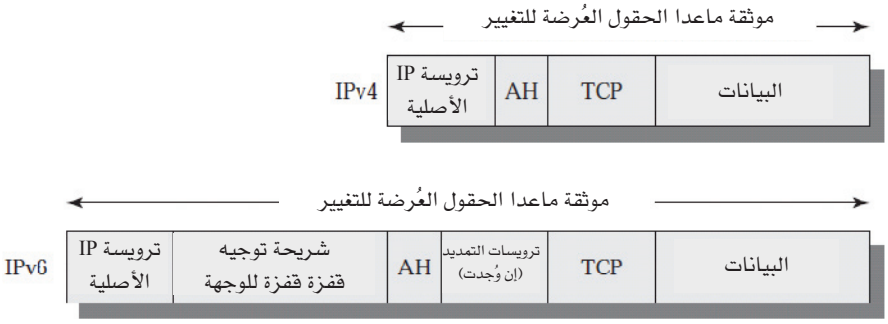
في هذا الجزء الفرعي سنتناول مجال التوثيق الذي توفره AH وموقع ترويسة التوثيق في كلا الأسلوبين، علماً بأن الاعتبارات مختلفةٌ بعض الشيء بالنسبة لـ IPv4 وIPv6. ويبيّن الشكل 6-6 (a) رزم IPv4 وIPv6 النمطية. في هذه الحالة، يكون حمل IP الآجر هو قطعة TCP، كما يمكن أيضا أن تكون وحدة بيانات لأي بروتوكول آخر يستخدم بروتوكول IP، كبروتوكول ICMP أو UDP.



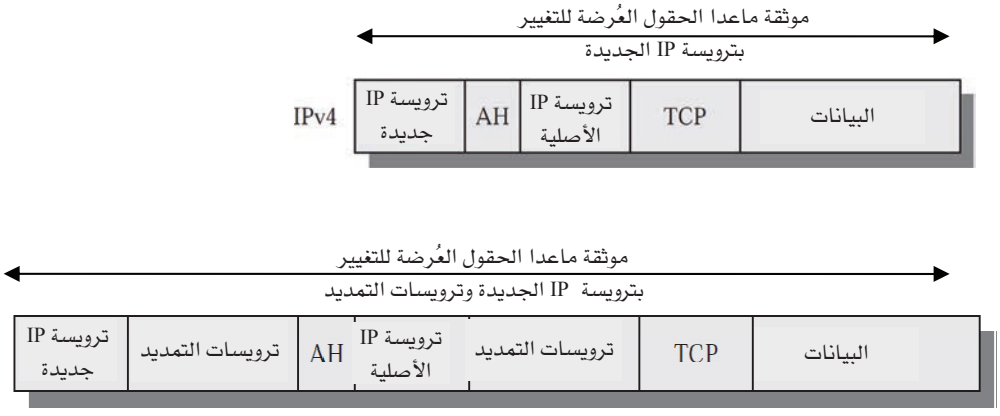
الشكل 6-5: التوثيق من طرف إلى طرف في مقابل التوثيق من طرف إلى وسيط.



(a) قبل إدراج ترويسة التوثيق



(b) نمط النقل



(c) نمط النفق

الشكل 6-6: مجالات التوثيق بترويسة AH.

بالنسبة لترويسة التوثيق بنمط النقل باستخدام IPv4، يتم إدراج ترويسة التوثيق بعد ترويسة بروتوكول الإنترنت الأصلية وقبل حمل IP الآجر (مثلاً قطعة TCP)، كما هو مُبيّن في الجزء العلوي من الشكل 6-6 (b). يغطي التوثيق الرزمة بأكملها، باستثناء الحقول القابلة للتغيير في ترويسة IPv4 والتي يتم تصفيرها لحساب كود التحقق من الرسالة (ماك).

وفي سياق IPv6، يُنظر إلى ترويسة التوثيق (AH) على أنها حمولة من طرفٍ إلى طرف، بمعنى أنها لا تُفحص أو تُعالج من قِبَل الموجّهات الوسيطة. وعليه تظهر ترويسة التوثيق بعد ترويسة الأساس لـ IPv6 وترويسات القفزة - بقفزة، والتوجيه، والترويسات الجزئية الملحقة. ويمكن أن تظهر ترويسة خيارات الوِجهة الملحقة قبل أو بعد ترويسة AH تبعاً للدلالات المرغوبة. ومرةً أخرى يشمل التوثيق الرزمة بأكملها، باستثناء القابلة للتغيُّر والتي يتم تصفيرها لحساب كود التحقق من الرسالة (ماك).

بالنسبة لترويسة التوثيق بنمط النفق، يتم توثيق رزمة بروتوكول IP الأصلية بأكملها، ويتم إدراج ترويسة التوثيق بين ترويسة IP الأصلية وترويسة IP خارجية جديدة (الشكل 6-6 (c)). وتحمل ترويسة IP الداخلية عناوين المصدر الأصلي الأساسي والوِجهة النهائية، بينما قد تتضمّن ترويسة IP الخارجية عناوين IP مختلفة (على سبيل المثال، عناوين جدران نارية أو بوابات أمنية أخرى).

في نمط النفق يتم حماية رزمة IP الداخلية بأكملها، بما في ذلك ترويسة IP الداخلية كلها، بواسطة ترويسة التوثيق. ويتم حماية ترويسة IP الخارجية (وفي حالة IPv6، الترويسات الملحقة الخارجية) باستثناء الحقول القابلة للتغيير، والتي لا يمكن التنبؤ بها.

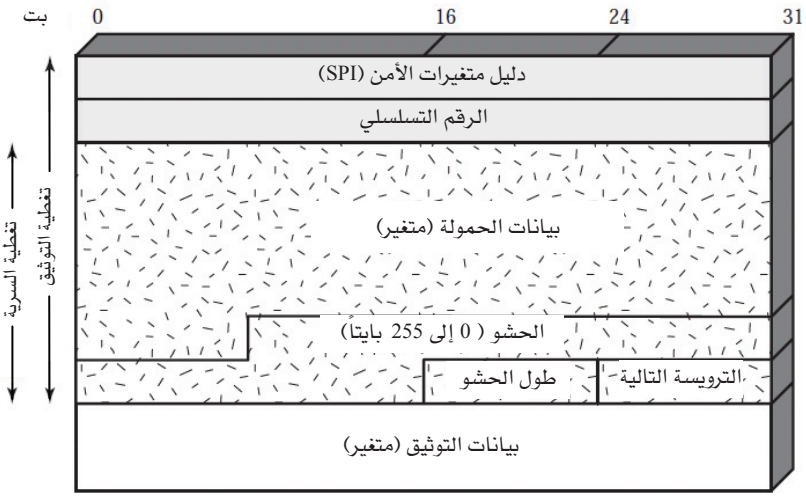
4-6 التغليف الأمني للحمولة (Encapsulating Security Payload (ESP))

يوفّر التغليف الأمني للحمولة (ESP) خدماتٍ للسرية، بما في ذلك سرية محتويات الرسالة وسرية محدودة لتدفق حركة المرور. كما يُمكن أيضاً للتغليف الأمني للحمولة توفير خدمة التوثيق كميزة اختيارية.

6-4-1 صيغة التغليف الأمني للحمولة

يوضّح الشكل 6-7 صيغة رزمة التغليف الأمني للحمولة (ESP)، والتي تتضمّن الحقول الآتية:

- مؤشر مُعامِلات الأمن (Security Parameters Index) (32 بتاً): يُعرِّف ارتباط أمن.
- الرقم التسلسلي (Sequence Number) (32 بتاً): قيمة متزايدة لعدّاد، ويستغل لاكتشاف إعادة الإرسال كما نوقش في ترويسة التوثيق.
- بيانات الحمولة (Payload Data) (بطول متغيِّر): وهي قطعة بمستوى النقل (في نمط النقل) أو رزمة IP (في نمط النفق) محميّة بالتشفير.
- الحشوة (Padding) (من 0 إلى 255 بايت): سنتناول الغرض من هذا الحقل لاحقاً.
- طول الحشوة (Pad Length) (8 بتات): ويُمثل عدد بايتات الحشوة.
- الترويسة التالية (Next Header) (8 بتات): وتحدّد نوع البيانات الواردة في حقل بيانات الحمولة عن طريق تحديد الترويسة الأولى في ذلك الحِمل (على سبيل المثال، ترويسة مُلحقة في IPv6 أو بروتوكول طبقة أعلى كـ TCP).
- بيانات التوثيق (Authentication Data) (بطول متغير): حقل بطول متغيّر (يجب أن يكون عدداً صحيحاً من كلمات 32-بت) يتضمّن قيمة تحقق السلامة (ICV) محسوبةً على رزمة التغليف الأمني للحمولة (ESP) ناقصةً حقل بيانات التوثيق.



الشكل 6-7: صيغة التغليف الأمني للحمولةِ في IPSec.

6-4-2 خوارزميات التشفير والتوثيق

تقوم خدمة التغليف الأمني للحمولةِ بتشفير الحقول الآتية: بيانات الحمل الآجر، والحشوة، وطول الحشوة، والترويسة التالية. إذا كانت الخوارزمية المستخدمة لتشفير الحمل الآجر تتطلب بيانات تزامن للتشفير، كمتجه التهيئة (IV)، فإنه يمكن إدراج تلك البيانات صراحةً في بداية حقل بيانات الحمولة. وإذا أُدرجت، فإن متجه التهيئة عادةً ما يكون غير مُشفَّر، رغم أنه كثيراً ما يُذكر على أنه جزء من النص المُشفَّر.

تتطلّب المواصفات الحالية أن تلتزم التنفيذات الممتثلة بدعم معيار تشفير البيانات (DES) في نمط تسلسل كتلة الشفرة (CBC) (نوقش في الفصل الثاني). وهناك عدد من الخوارزميات الأخرى التي تم تخصيص محدّدات لها في وثيقة نطاق التفسير (Domain of Interpretation (DOI)) ولذا يمكن استخدامها للتشفير بسهولة، بما في ذلك:

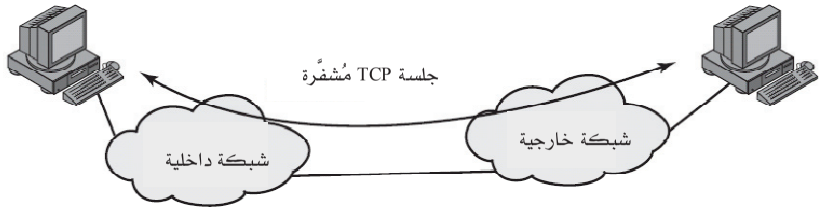
- معيار DES ثلاثي المفاتيح.
- RC5.
- IDEA.
- معيار IDEA ثلاثي المفاتيح.
- CAST.
- Blowfish.

وكما هوالحال مع ترويسة التوثيق، يدعم التغليف الأمني للحمولة استخدام كود التحقّق من الرسالة (ماك) بطول مُفترض يبلغ 96 بتاً. وأيضا كما هوالحال مع ترويسة التوثيق، تنص المواصفات الحالية على أن التنفيذات الممتثلة لابد أن تدعم HMAC-MD5-96 وHMAC-SHA-1-96.

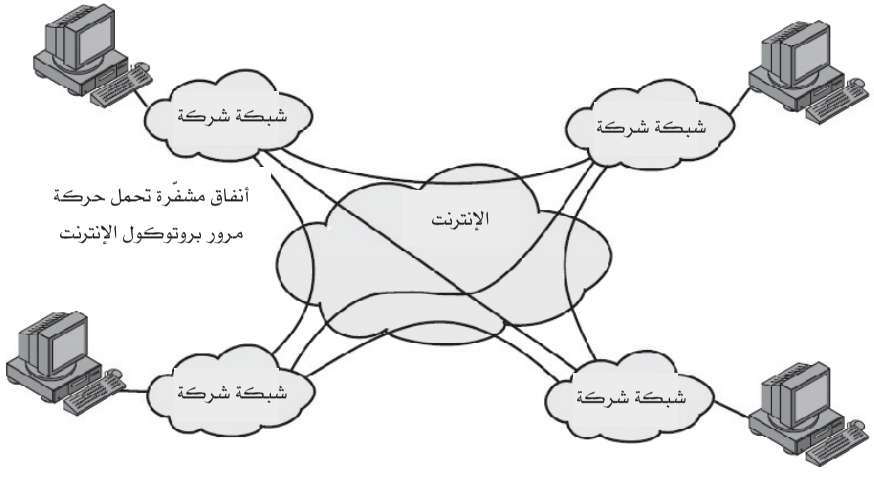
6-4-3 الحشو

يخدم حقل الحشوة عدة أغراض:

- إذا كانت خوارزمية التشفير تتطلب أن يكون النص الأصلي عدداً معيّناً من البايتات (على سبيل المثال، عدداً صحيحاً من الكتل لأحد شفرات الكتلة) يُستخدَم حقل الحشو لتوسيع النص الأصلي (والذي يتألف من حقول بيانات الحمولة، والحشوة، وطول الحشوة، والترويسة التالية) إلى الطول المطلوب.
- تتطلب صيغةُ التغليف الأمني للحمولة أن تكون حقول طول الحشوة والترويسة التالية منحازة يميناً داخل كلمة مؤلَّفة من 32 بتاً. وفي المقابل، يجب أن يكون النص المُشفَّر عدداً صحيحاً من الكلمات. ويُستخدَم حقل الحشو لتحقيق تلك المحاذاة.
- قد يضاف المزيد من الحشو لتوفير سريّة جزئيةٍ لتدفق حركة المرور عن طريق إخفاء الطول الفعلي للحمل الآجر.



(a) أمن مستوى النقل



(b) شبكة خاصة افتراضية بنمط النفق

الشكل 6-8: التشفير بنمط النقل مقابل التشفير بنمط النفق.

6-4-4 نمطا النقل والنفق

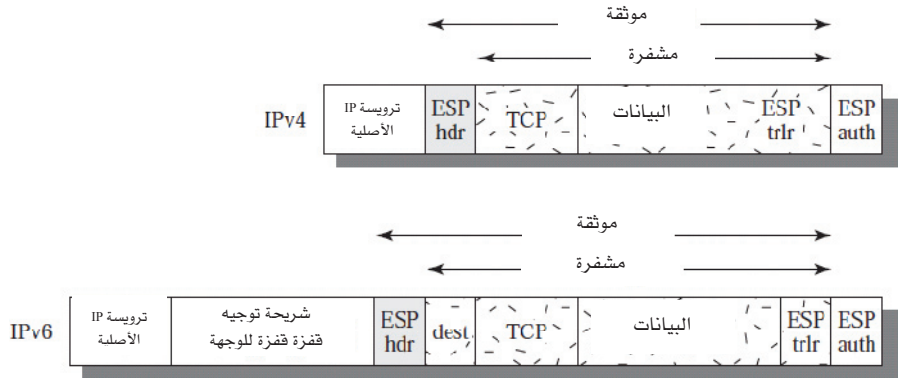
يبيّن الشكل 6-8 أسلوبين لاستخدام خدمة التغليف الأمني للحمولة في بروتوكول IPSec. في الجزء العلوي من الشكل (6-8 (a))، يتم توفير التشفير (والتوثيق اختيارياً) بين المضيفين مباشرة. ويبيّن الشكل 6-8 (b) كيفية استخدام عملية نمط النفق لإنشاء شبكة خاصة افتراضية. وفي هذا المثال، تمتلك منظمة أربع شبكات خاصة مرتبطة عبر الإنترنت. ويستخدم المضيفون على الشبكات الداخلية شبكة الإنترنت لنقل البيانات ولكنهم لا يتفاعلون مع غيرهم من مضيفي الإنترنت. وبإنهاء الأنفاق عند بوابة الأمن لكل شبكة داخلية، يسمح هذا الترتيب للمضيفين بتجنب تنفيذ الإمكانات الأمنية. ويتم دعم الأسلوب السابق بواسطة ارتباط أمني بنمط النقل، في حين أن الأسلوب الأخير يستخدم ارتباطاً أمنياً بنمط النفق.

في هذا الجزء، سنلقي نظرةً على مجالات التغليف الأمني للحمولة لكلا النمطين، مع ملاحظة أن الاعتبارات مختلفة بعض الشيء بالنسبة لـ IPv4 وIPv6. وكما كان الحال في مناقشتنا عن مجالات ترويسة التوثيق، سوف نستخدم صيغة الرزمة بالشكل 6-6 (a) كنقطة انطلاق.

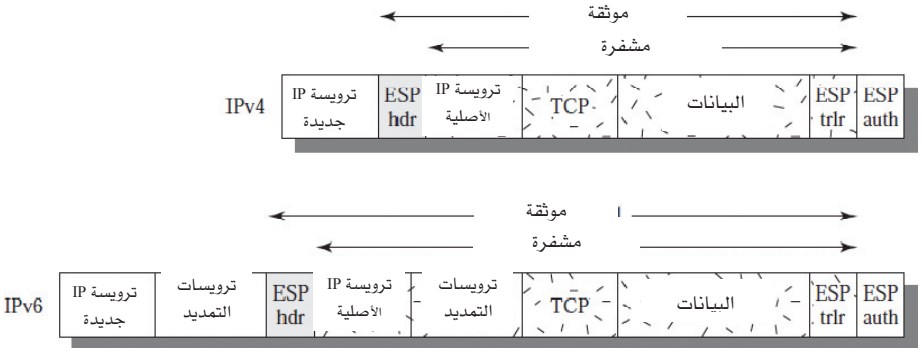
❖ التغليف الأمني للحمولة بنمط النقل:

يستخدم التغليف الأمني للحمولة بنمط النقل للتشفير والتوثيق الاختياري للبيانات التي يحملها بروتوكول الإنترنت (على سبيل المثال، قطعة TCP) كما هو مبيّن في الشكل 6-9 (a). وبالنسبة لـ IPv4 يتم في هذا النمط إدخال ترويسة التغليف الأمني للحمولة في رزمة IP مباشرةً قبل ترويسة طبقة النقل (على سبيل المثال: UDP، TCP، ICMP) ويتم وضع تذييل للتغليف الأمني للحمولة (حقول الحشوة، طول الحشوة، والترويسة التالية) بعد رزمة IP، في حال اختيار التوثيق، يتم إضافة حقل بيانات توثيق التغليف الأمني للحمولة بعد تذييل التغليف الأمني للحمولة. ثم يتم

تشفير القطعة بمستوى النقل كاملةً بالإضافة إلى التذييل. ويشمل التوثيق كل النص المُشفَّر بالإضافة إلى ترويسة التغليف الأمني للحمولة.



(a) نمط النقل



(b) نمط النفق

الشكل 6-9: مجال التشفير والتوثيق للتَّغليف الأمني للحمولة.

في سياق IPv6 يُنظر للتغليف الأمني للحمولة على أنه حمولة من طرفٍ إلى طرف، بمعنى أنه لا يُفحص أو يُعالج من قِبَل الموجّهات الوسيطة. وعليه تظهر

ترويسة التوثيق بعد ترويسة الأساس الـ IPv6 وترويسات القفزة - بقفزة، والتوجيه، والترويسات الجزئية الملحقة. ويمكن أن تظهر ترويسة خيارات الوِجهة الملحقة قبل ترويسة التغليف الأمني للحمولة أو بعدها تبعاً للدلالات المرغوبة. وبالنسبة لـ IPv6، يغطي التشفير قطعة مستوى النقل كاملةً بالإضافة إلى تذييل التغليف الأمني للحمولةِ وترويسة خيارات الوِجهة الملحقة في حال وقوعها بعد ترويسة التغليف الأمني للحمولة. ومرةً أخرى، يشمل التوثيق النص المُشفَّر كاملا بالإضافة إلى ترويسة التغليف الأمني للحمولة.

يمكن تلخيص عمل نمط النقل على النحو الآتي:

1. عند المصدر، يتم تشفير كتلة البيانات التي تتكون من تذييل التغليف الأمني للحمولة بالإضافة إلى كل قطعة طبقة النقل، كما يتم استبدال النص الأصلي لتلك الكتلة بالنص المُشفَّر لتشكيل رزمة IP بغرض النقل. ويتم إضافة التوثيق إذا استخدم هذا الخيار.
2. يتم بعد ذلك توجيه الرزمة للوِجهة المطلوبة. ويقوم كل موجّه وسيط بفحص ومعالجة ترويسة IP بالإضافة إلى أي ترويسات IP ملحقة بالنص الأصلي، ولكنه لا يحتاج إلى فحص النص المُشفَّر.
3. تقوم عقدة الوِجهة بفحص ومعالجة ترويسة IP، بالإضافة إلى أي ترويسات IP ملحقة بالنص الأصلي. ثم تقوم بفك تشفير ما تبقى من الرزمة لاسترداد النص الأصلي بقطعة طبقة النقل، وذلك بناءً على مؤشر المُعامِلات الأمنية (SPI).

يوفر نمط النقل السرية لأي تطبيق يستخدم هذا النمط، ومن ثَمَّ لا يحتاج إلى تنفيذ السرية في كل تطبيق على حدة. كما يتميز أيضاً بدرجة معقولة من الكفاءة، حيث إنه لا يؤدي إلا إلى زيادة طفيفة في الطول الإجمالي لرزمة IP. ولكن من عيوب هذا النمط إمكانية القيام بتحليل لحركة مرور الرزم المُرسَلة بواسطته.

❖ التغليف الأمني للحمولة بنمط النفق:

يُستخدم التغليف الأمني للحمولة بنمط النفق لتشفير رزم IP بكاملها (الشكل 9-6 (b)). في هذا النمط، تُثبَّت ترويسة التغليف الأمني للحمولة في مُقدِّمة الرزمة ثم يتم تشفير الرزمة بالإضافة إلى تذييل التغليف الأمني للحمولة. ويمكن استخدام هذه الطريقة لإحباط محاولات تحليل حركة المرور.

نظراً لأن ترويسة IP تتضمّن عنوان الوِجهة وربما أيضاً تعليمات توجيه المصدر ومعلومات خيار القفزة - بقفزة، فلن يكون بالإمكان نقل رزم IP المُشفَّرة مع ترويسة التغليف الأمني للحمولةِ المثبتة في مقدمتها– حيث لن تستطيع الموجّهات الوسيطة معالجة تلك الرزم. ولذا فمن الضروري تغليف الكتلة بأكملها (ترويسة التغليف الأمني للحمولة، بالإضافة إلى النص المُشفَّر، وبيانات التوثيق إن وجدت) مع ترويسة IP جديدة والتي سوف تتضمّن معلومات كافية للتوجيه ولكن ليس لتحليل حركة المرور.

في حين يُعدُّ نمط النقل مناسباً لحماية الاتصالات بين الأنظمة المضيفة التي تدعم ميزة التغليف الأمني للحمولة، يُعدُّ نمط النفق مفيداً في التشكيلات التي بها جدار حماية أو أي نوع آخر من البوابات الأمنية التي تحمي شبكة موثوق بها من شبكات خارجية. وفي تلك الحالة الأخيرة يحدث التشفير فقط بين مضيف خارجي وبوابة أمنية أو بين اثنتين من البوابات الأمنية. وهذا يعفي الأنظمة المضيفة على الشبكة الداخلية من عبء معالجة التشفير ويبسِّط عملية توزيع المفاتيح عن طريق خفض عدد المفاتيح المطلوبة. بالإضافة إلى ذلك فإنه يحبط محاولات تحليل حركة المرور على أساس الوِجهة النهائية.

لنأخذ بعين الاعتبار حالة مضيف خارجي يرغب في الاتصال مع مضيف على شبكة داخلية محميّة بواسطة جدار حماية، علماً بأن التغليف الأمني للحمولة مُنفَّذ بالمضيف الخارجي وبجدران الحماية. ويتم اتباع الخطوات الآتية لنقل قطعة من طبقة النقل من المضيف الخارجي إلى المضيف الداخلي:

1. يقوم المصدر بإعداد رزمة IP داخلية عنوان الوِجهة فيها هو عنوان المضيف الداخلي المستهدف. تُثبَّت ترويسة التغليف الأمني للحمولة في مقدمة تلك الرزمة، ثم يتم تشفير الرزمة مع تذييل التغليف الأمني للحمولة، كما

يمكن إضافة بيانات التوثيق. يتم تغليف الكتلة الناتجة بترويسة IP جديدة (ترويسة الأساس مع ملحقات اختيارية كخيارات التوجيه والقفزة - بقفزة لـ IPv6) والتي يكون عنوان الوِجهة فيها هو عنوان جدار الحماية، وبهذا يتم تشكيل رزمة IP الخارجية.

2. يتم توجيه الرزمة الخارجية إلى جدار الحماية. يقوم كل موجّه وسيط بفحص ومعالجة ترويسة IP الخارجية بالإضافة إلى أيٍّ من ترويسات IP الملحقة الخارجية، وبدون حاجة لفحص النص المُشفَّر.
3. يقوم جدار الحماية المقصود بفحص ومعالجة ترويسة IP الخارجية بالإضافة إلى أيٍّ من ترويسات IP الملحقة الخارجية. ثم تعمل عقدة الوِجهة على فك تشفير ما تبقى من الرزمة على أساس مؤشر مُعامِلات الأمن (SPI) بترويسة التغليف الأمني للحمولة لاسترداد النص الأصلي لرزمة IP الداخلية. بعد ذلك تُنقل هذه الرزمة عبر الشبكة الداخلية.
4. يتم توجيه الرزمة الداخلية بعد ذلك عبر عدد من الموجّهات بالشبكة الداخلية لتصل إلى المضيف المقصود.

5-6 الجمع بين الارتباطات الأمنية

يمكن لارتباط أمني واحد استخدام ترويسة التوثيق (AH) أو التغليف الأمني للحمولةِ (ESP) ولكن ليس كلاهما معاً. وفي بعض الأحيان يتطلب تدفق معيّن لحركة المرور استخدام الخدمات التي تقدمها ترويسة التوثيق والتغليف الأمني للحمولة. كما قد يتطلب تدفق معيّن خدمات أمن IPSec بين الأنظمة المضيفة، وفي نفس الوقت قد يتطلب هذا التدفق نفسه خدمات أخرى بين البوابات الأمنية، كجدران الحماية. في جميع هذه الحالات ينبغي استخدام عدة ارتباطات أمنية لتحقيق خدمات IPSec المنشودة لنفس تدفق حركة المرور. يُمثل مصطلح "رزمة الارتباطات الأمنية (security association bundle) سلسلة من الارتباطات الأمنية التي يتم معالجة حركة المرور من خلالها لتوفير المجموعة المطلوبة من خدمات أمن IPSec. هذا وقد تنتهي الارتباطات الأمنية برزمةٍ ما في نقاط نهاية مختلفة أو في نفس النقطة النهاية.

ويمكن الجمع بين الارتباطات الأمنية في رزم بطريقتين:

- جوار النقل: ويشير إلى تطبيق أكثر من بروتوكول أمني على نفس رزمة IP، دون الاستعانة بنفق. تسمح هذه الطريقة للجمع ما بين ترويسة التوثيق والتغليف الأمني للحمولة بمستوى واحد فقط من هذا الجمع؛ لأن تراكبها (nesting) لا يُؤدي أي فائدة إضافية لكون المعالجة تتم في موقع أمن IPSec واحد، ألا وهي الوِجهة النهائية.
- النفق المتكرر: ويشير إلى تطبيق طبقات متعددة من البروتوكولات الأمنية تنفّذ من خلال نفق بروتوكول IP. وتتيح هذه الطريقة استخدام مستويات متعددة من التراكب (nesting)، لأن كل نفق يمكن إنشاؤه أو إنهاؤه في مواقع IPSec مختلفة على طول المسار.

ويمكن الجمع بين النهجين، على سبيل المثال بجعل ارتباط أمني بنمط النقل يربط بين أنظمة مضيفة وينتقل في جزء من مساره بين البوابات الأمنية خلال ارتباط أمني بنمط النفق.

ومن قضايا رزم الارتباط الأمني الشائقة قضية الترتيب الذي تتم به عمليات التوثيق والتشفير بين زوج معيّن من النقاط الطرفية وسبل تحقيق ذلك. وسوف نتناول هذه المسألة فيما يلي، ثم ننظر إلى ترتيبات الارتباطات الأمنية التي تتضمّن نفقاً واحداً على الأقل.

1-5-6 التوثيق بالإضافة إلى السرية

يمكن الجمع بين التشفير والتوثيق بغية نقل رزمة IP بخاصيتي التوثيق والسرية بين أنظمة مضيفة. وسوف ننظر إلى عدة سبل لتحقيق ذلك.

❖ خيار التوثيق مع التغليف الأمني للحمولة:

يوضّح الشكل 6-9 هذه الطريقة، حيث يُطبّق المستخدم أولاً التغليف الأمني للحمولة على البيانات التي يتعين حمايتها ثم يلحق بها حقل بيانات التوثيق. وهناك في الواقع حالتان فرعيتان:

- التغليف الأمني للحمولة بنمط النقل: يُطبّق كلٌّ من التوثيق والتشفير على حمولة IP التي يتم تسليمها إلى المضيف، أما الترويسة (IP) فلا يتم حمايتها.
- التغليف الأمني للحمولةِ بنمط النفق: يُطبّق التوثيق على رزمة IP بالكامل والتي يتم تسليمها إلى عنوان IP للوِجهة الخارجية (على سبيل المثال، جدار الحماية)، ويتم التوثيق عند تلك الوِجهة. كما يتم حماية رزمة IP الداخلية بكاملها بموجب آليات الخصوصية، وذلك لتسليمها إلى عنوان IP للوِجهة الداخلية.

وفي كلتا الحالتين، يُطبّق التوثيق على النص المُشفَّر وليس النص الأصلي.

❖ تجاور النقل:

هناك طريقة أخرى لتطبيق التوثيق بعد التشفير باستخدام رزمة مكوَّنة من ارتباطين أمنيين بنمط النقل، حيث يكون الداخلي منهما ارتباطاً أمنياً مع تغليف أمني للحمولة والخارجي ارتباطاً أمنياً مع ترويسة التوثيق. وفي هذه الحالة يتم استخدام التغليف الأمني للحمولة بدون خيار التوثيق. ولأن الارتباط الأمني الداخلي بنمط النقل، فإنه يتم تشفير حمولة IP. وتتألف الرزمة الناتجة من ترويسة IP (وربما ترويسات IPv6 ملحقة) يليها التغليف الأمني للحمولة. بعدها يتم تطبيق ترويسة التوثيق بنمط النقل، بحيث يغطي التوثيق التغليف الأمني للحمولة مع ترويسة IP الأصلية (وملحقاتها) باستثناء الحقول القابلة للتغيير. وتمتاز هذه الطريقة على مجرد استخدام ارتباط أمني واحد مع التغليف الأمني للحمولةِ بخيار التوثيق بأن التوثيق يشمل المزيد من الحقول، بما في ذلك عناوين IP للمصدر والوِجهة. أما عيب هذه الطريقة فهو زيادة العبء الإضافي نتيجة استخدام ارتباطين أمنيّين بدلاً من ارتباطٍ واحد.

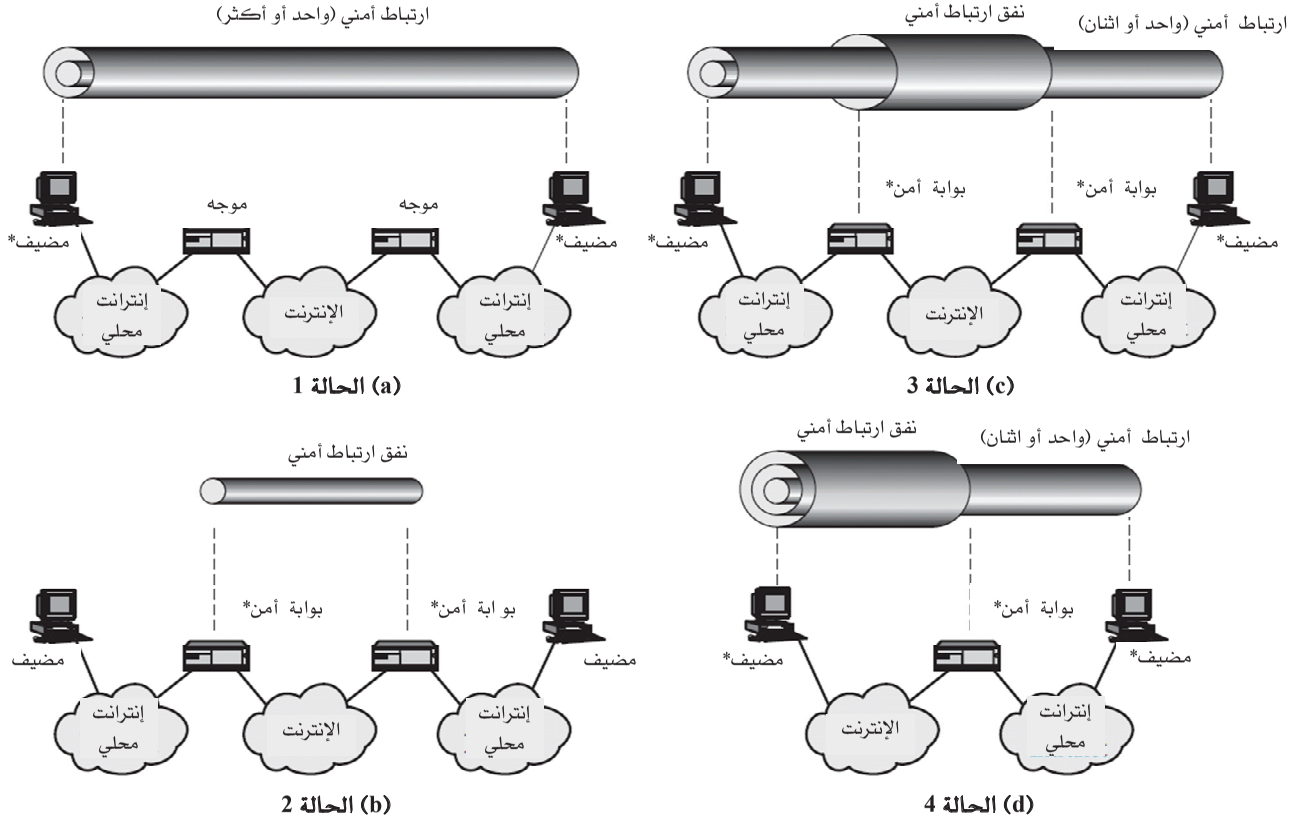
❖ رزمة النقل - النفق:

قد يكون من الأفضل استخدام التوثيق قبل التشفير لعدة أسباب. أولها: أن بيانات التوثيق تكون محمية بواسطة التشفير، ومن ثَمَّ سيكون من المستحيل على أي شخص اعتراض الرسالة وتغيير بيانات التوثيق بها دون أن يتم اكتشاف ذلك، وثانيها، قد يكون من المستحسن تخزين معلومات التوثيق مع الرسالة عند المُستلِم للرجوع إليها إذا ما دعت الحاجة لذلك لاحقاً. ويُعدُّ ذلك أكثر ملاءمة إذا كانت معلومات التوثيق تُطبّق على الرسالة غير المُشفَّرة؛ وإلا فإن الرسالة يجب أن يتم إعادة تشفيرها للتحقق من معلومات التوثيق.

تتلخص إحدى طرق تطبيق التوثيق قبل التشفير بين نظامين مضيفين في استخدام رزمة تتألف من ارتباطين، داخلي بترويسة توثيق بنمط النقل وخارجي بالتغليف الأمني للحمولةِ بنمط النفق. وفي هذه الحالة، يتم تطبيق التوثيق على حمولة IP بالإضافة إلى ترويسة IP (وملحقاتها) باستثناء الحقول القابلة للتغيير. ويتم بعد ذلك معالجة رزمة IP الناتجة في نمط النفق بواسطة التغليف الأمني للحمولة، والنتيجة هي تشفير الرزمة الداخلية الموثقة كاملةً وإضافة ترويسة IP خارجية جديدة (وملحقاتها).

2-5-6 التوليفات الأساسية للارتباطات الأمنية

تتضمن وثيقة بنية IPSec أربعة أمثلة على توليفات للارتباطات الأمنية التي يتعيّن على الأنظمة المضيفة المتوافقة مع IPSec (كمحطات العمل، والخادمات) أو بوابات الأمن (كجدران الحماية، والموجّهات) دعمها، كما هو موضح بالشكل 6-10. ويمثل الجزء السفلي من الشكل التوصيل المادي للعناصر ؛ بينما يمثل الجزء العلوي التوصيل المنطقي عن طريق ارتباط أمني واحد أو عدة ارتباطات أمنية متراكبة (nested). يمكن أن يكون كل ارتباط أمني ترويسة توثيق أو تغليفاً أمنياً للحمولة. ويمكن أن تكون الارتباطات الأمنية من مضيف إلى مضيف إما بنمط النقل أو نمط النفق، وإلا فإنه يتعيّن أن يكون الارتباط بنمط النفق.



الشكل 6-10: التوليفات الأساسية للارتباطات الأمنية (* = تطبق بروتوكول أمن الانترنت).

في الحالة 1، يتم توفير كل إجراءات الأمن بين الأنظمة الطرفية التي تنفذ أمن بروتوكول IPSec. للاتصال بين نظامين طرفيّين عبر الارتباط الأمني لابد أن يشتركا في المفاتيح السرية المناسبة. ومن بين التوليفات الممكنة:

1. ترويسة التوثيق بنمط النقل.
2. التغليف الأمني للحمولة بنمط النقل.
3. التغليف الأمني للحمولة متبوعاً بترويسة توثيق بنمط النقل (ارتباط أمني بالتغليف الأمني للحمولة داخل ارتباط أمني بترويسة التوثيق).
4. أيٍّ من الحالات السابقة (1، أو 2، أو 3) داخل ترويسة التوثيق أو داخل التغليف الأمني للحمولة بنمط النفق.

ناقشنا حتى الآن كيف يمكن استخدام تلك التوليفات المختلفة لدعم التوثيق، والتشفير، والتوثيق قبل التشفير، والتوثيق بعد التشفير.

في الحالة 2، يتم توفير الأمن بين البوابات الأمنية فقط (الموجّهات، جدران الحماية، الخ) ولا تقوم الأنظمة المضيفة بتنفيذ بروتوكول IPSec. وتوضح هذه الحالة الدعم للشبكات الخاصة الافتراضية (VPN) البسيطة. وتنص وثيقة بنية الأمن على أن المطلوب لهذه الحالة هو ارتباط أمني بنفق واحد فقط. ويمكن للنفق دعم ترويسة توثيق أو التغليف الأمني للحمولة أو التغليف الأمني للحمولة مع خيار التوثيق. لا يحتاج الأمر هنا إلى أنفاق متراكبة لأن خدمات IPSec تُطبّق على الرزمة الداخلية برمتها.

الحالة 3 مبنية على الحالة 2 وذلك بإضافة نظام أمن من طرف إلى طرف. يُسمح هنا بنفس التوليفات التي تمت مناقشتها في الحالتين 1 و2. ويوفّر نفق البوابة إلى بوابة التوثيق أو السرية أو كليهما لكامل حركة المرور بين الأنظمة الطرفية. عندما يتبع نفق البوابة إلى بوابة نظام التغليف الأمني للحمولة، فإنه يوفر أيضاً شكلاً محدوداً من سرية حركة المرور. ويمكن للمضيفين كلٍ على حدة تنفيذ أي خدمات IPSec إضافية تكون مطلوبة لتطبيقات معينة، أو لمستخدمين معيّنين عن طريق ارتباطات أمنية من طرفٍ إلى طرف.

توفر الحالة 4 الدعم لمضيف بعيد يستخدم الإنترنت للوصول إلى جدار الحماية للمؤسسة ومن ثم الوصول إلى خادم أو محطة العمل خلف جدار الحماية. المطلوب هنا فقط هو نمط النفق بين المضيف البعيد وجدار الحماية. وكما في الحالة رقم 1، يمكن استخدام ارتباط أمني واحد أو ارتباطين بين المضيف البعيد والمضيف المحلي.

6-6 إدارة المفاتيح

يتضمّن الجزء الخاص بإدارة المفاتيح في IPSec تحديد المفاتيح السرية وتوزيعها. ويحتاج الأمر عادةً إلى أربعة مفاتيح للاتصال بين تطبيقين: زوج مفاتيح (مفتاح للإرسال وآخر للاستقبال) لكلٍّ من ترويسة التوثيق والتغليف الأمني للحمولة. وتتطلب وثيقة بنية IPSec دعم نوعين من أساليب إدارة المفاتيح:

- يدوي: يقوم مسئول النظام يدوياً بتهيئة كل نظام مع المفاتيح الخاصة به والمفاتيح الخاصة بالأنظمة الأخرى المُتصلة. ويُعدُّ هذا الأسلوب عملياً أكثر في البيئات الصغيرة الثابتة نسبيا.
- آلي: حيث يمكن استحداث مفاتيح جديدة للارتباطات الأمنية آلياً حسب الطلب، ويسهِّل عملية استخدام المفاتيح في نظام مُوزَّع كبير دائم التطور.

يُعرف بروتوكول إدارة المفاتيح الآلي المفترض في بروتوكول IPSec بـ (ISAKMP/Oakley)، ويتألف من العناصر الآتية:

- بروتوكول أوكلي لتعيين المفاتيح (Oakley Key Determination Protocol): أوكلي هو بروتوكول لتبادل المفاتيح يستند إلى خوارزمية ديفي- هيلمان مع توفير أمن إضافي. يُعدُّ أوكلي بروتوكولاً عاما لا يتطلب صيغاً بعينها.
- بروتوكول ارتباط أمن الإنترنت وإدارة المفاتيح (Internet Security Association and Key Management Protocol (ISAKMP)): يوفر بروتوكول ارتباط أمن الإنترنت وإدارة المفاتيح (ISAKMP) إطاراً لإدارة مفاتيح الإنترنت، كما يوفر الدعم المحدّد للبروتوكول، بما في ذلك الصيغ، للتفاوض على السمات الأمنية.

ولا يُملي ISAKMP خوارزمية محدّدة لتبادل المفاتيح؛ ولكنه يتكون من مجموعة من أنواع الرسائل تسمح باستخدام مجموعة متنوعة من خوارزميات تبادل المفاتيح. حدّد الإصدار الأوليّ من بروتوكول ISAKMP أوكلي كخوارزمية تبادل المفاتيح المعتمدة.

نبدأ هذا الجزء بلمحة عامة عن بروتوكول أوكلي، ثم نتناول بعد ذلك بروتوكول ISAKMP.

1-6-6 بروتوكول أوكلي لتعيين المفاتيح

يمكن اعتبار بروتوكول أوكلي تنقيحاً لخوارزمية ديفي- هيلمان لتبادل المفاتيح. تذكّر أن خوارزمية ديفي- هيلمان تتضمّن التبادلات التالية والتي تتم بين المستخدمين A و B. ولإتمام تلك التبادلات لابد من وجود اتفاق مسبق على متغيرين عامَّين: q وهوعدد أوَّلي كبير؛ وα وهو جذر بدائي للعدد الأوَّلي q. حيث يختار A عدداً صحيحاً عشوائياً (X_A) كمفتاحٍ خاصٍ به، ويرسل إلى B مفتاحه العام ($Y_A = \alpha^{X_A} \bmod q$). وبنفس الطريقة، يختار B عدداً صحيحاً عشوائياً X_B كمفتاحٍ خاصٍ به، ويرسل إلى A مفتاحه العام ($Y_B = \alpha^{X_B} \bmod q$). عندها يمكن لكل جانب حساب مفتاح الجلسة السري من:

وتتمتع خوارزمية ديفي - هيلمان بميزتين مهمتين:

- يتم إنشاء المفاتيح السرية عند الحاجة فقط. ولذا فلا حاجة لتخزين المفاتيح السرية لفترة طويلة من الزمن والذي قد يشكّل تهديداً أمنياً.
- لا يتطلب التبادل وجود بنية تحتيَّة فيما عدا الاتفاق على المتغيرين العامَّين.

ومع ذلك، فهناك عدد من نقاط الضعف في خوارزمية ديفي - هيلمان كما ورد في [HUIT98]:

- أنها لا تقدم أي معلومات عن هوية الأطراف.

- أنها عُرضةٌ لهجوم "رجل في الوسط"، والذي يقوم فيه طرف ثالث C بالاتصال مع الطرف A متقمصاً شخصية الطرف B وكذلك الاتصال مع الطرف B متقمصاً شخصية الطرف A. يؤدي ذلك في النهاية إلى أنَّ كلاً من A وB يقومان بالفعل بالتفاوض على المفتاح مع الطرف C وليس مع بعضهما بعضاً، مما يمكّن C بعد ذلك من التنصت على حركة المرور وتمريرها. يمضي هجوم "رجلٌ في الوسط" على النحو الآتي:

1. يرسل الطرف B مفتاحه العام Y_B في رسالة موجهة إلى الطرف A (انظر الشكل 3-11).
2. يقوم الخَصْم E باعتراض تلك الرسالة، ويحفظ المفتاح العام للطرف B ثم يقوم بإرسال رسالةٍ إلى الطرف A بهوية (User ID) الخاصة بالطرف B ولكن مع المفتاح العام للخَصْم E. تُرسَل هذه الرسالة بهذه الطريقة حتى تبدو كما لوكانت قد أُرسلت من النظام المضيف للطرف B. باستلام هذه الرسالة من الخَصْم E يقوم الطرف A بحفظ المفتاح العام للخَصْم E مع هوية الطرف B. وبالمثل، يرسِل الخَصْم E رسالة إلى الطرف B مع المفتاح العام للخَصْم E، والتي تزعم أنها من الطرف A.
3. يقوم B بحساب مفتاح سري K_1 بناءً على المفتاح الخاص للطرف B وY_E. ويقوم A بحساب مفتاح سري K_2 بناءً على المفتاح الخاص للطرف A وY_E. يقوم الخَصْم E بحساب K_1 مستخدماً مفتاح E السري X_E وY_B وحساب K_2 مستخدماً X_E وY_A.
4. من الآن فصاعداً يصبح الخَصْم E قادراً على توصيل الرسائل من الطرف A إلى الطرف B ومن الطرف B إلى الطرف A، وتغيير تشفيرهما كما يريد دون أن يدري الطرف A ولا الطرف B أن الخَصْم E يشاركهما اتصالاتهما.

- تُعدُّ الخوارزمية عالية الكلفة حسابياً حيث تتطلب عمليات حسابية مُكثّفة وتستغرق وقتاً طويلاً، مما يعرضها لهجمات العرقلة (clogging attacks)، حيث يطلب الخَصْم عدداً كبيراً من المفاتيح، ويستهلك الضحية لذلك موارد معالجة ضخمة للقيام بعمليات الرفع الأسّي المقاسي (modular exponentiation) بدون طائل بدلاً من القيام بعمل مفيد.

$I \rightarrow R$: $CKY_I, OK\_KEYX, GRP, g^x, EHAO, NIDP, ID_I, ID_R, N_I, S_{KI}[ID_I \| ID_R \| N_I \| GRP \| g^x \| EHAO]$

$R \rightarrow I$: $CKY_R, CKY_I, OK\_KEYX, GRP, g^y, EHAS, NIDP, ID_R, ID_I, N_R, N_I, S_{KR}[ID_R \| ID_I \| N_R \| N_I \| GRP \| g^y \| g^x \| EHAS]$

$I \rightarrow R$: $CKY_I, CKY_R, OK\_KEYX, GRP, g^x, EHAS, NIDP, ID_I, ID_R, N_I, N_R, S_{KI}[ID_I \| ID_R \| N_I \| N_R \| GRP \| g^x \| g^y \| EHAS]$

الرموز:

I = المنشئ (البادئ)

R = المستجيب

CKY_I, CKY_R = كوكيز البادئ والمستجيب

OK_KEYX = نوع رسالة تبادل المفاتيح

GRP = اسم مجموعة ديفي – هيلمان لهذا التبادل

g^x, g^y = المفتاحان العامان للبادئ والمستجيب؛ g^{xy} = مفتاح الجلسة نتيجة هذا التبادل

EHAO, EHAS = وظيفة التشفير والتوثيق بالهاش التي تم عرضها واختيارها

NIDP = تدل على عدم استخدام التشفير لبقية هذه الرسالة

ID_I, ID_R = مُعرِّفا البادئ والمستجيب

N_I, N_R = عددان عشوائيان يستخدمان لمرة واحدة (nonce) يوفرهما البادئ والمستجيب لهذا التبادل

$S_{KI}[X], S_{KR}[X]$ = ترمزان للتوقيعين على X باستخدام المفتاح الخاص (مفتاح التوقيع) للبادئ والمستجيب

الشكل 6-11: مثال أوكلي للتبادل الاعتسافي للمفاتيح.

يهدف بروتوكول أوكلي إلى الحفاظ على مزايا خوارزمية ديفي- هيلمان وفي نفس الوقت تلافي نقاط الضعف فيها.

❖ خصائص بروتوكول أوكلي:

يتميز بروتوكول أوكلي بخمس خصائص مهمة:

1. تستخدم آلية تُعرف باسم الكوكيز (cookies) لإحباط هجمات العرقلة.
2. تمكِّن الطرفين من التفاوض على مجموعة (group)؛ ومن ثم تحديد المتغيرين العامَّين لخوارزمية ديفي - هيلمان لتبادل المفاتيح.
3. تستعمل أعدد الاستخدام لمرة واحدة فقط (nonces) للحماية ضد هجمات إعادة الإرسال.
4. تُتيح تبادل قيم مفاتيح ديفي - هيلمان العامة.
5. تقوم بتوثيق تبادلات ديفي - هيلمان لإحباط هجمات "رجل في الوسط".

بعد أن ناقشنا خوارزمية ديفي - هيلمان، لنلقِ نظرةَ على ما تبقى من تلك الخصائص بالترتيب. ننظر أولاً إلى مشكلة هجمات العرقلة. في هذا الهجوم يزيِّف الخَصْم عنوان المصدر لمستخدم شرعي ويرسل مفتاح ديفي - هيلمان عمومي إلى الضحية. ينفِّذ الضحية عمليات الرفع الأسّي المقاسي (modular exponentiation) لحساب المفتاح السري. وبتكرار رسائل من هذا النوع يمكن عرقلة نظام الضحية بحسابات وعمليات غير مُجدية. ويتطلب تبادل الكوكي أن يرسل كل جانب عدداً شِبه عشوائي، أي الكوكي، في الرسالة الأوليّة، والتي يقر الجانب الآخر بتلقّيها. وينبغي تكرار هذا الإقرار في الرسالة الأولى لتبادل مفاتيح ديفي - هيلمان، وإذا كان عنوان المصدر مزوراً لا يحصل الخَصْم على أي جواب. ومن ثَمَّ، يمكن للخَصْم جعل المستخدم يولّد إشعارات استلام فقط وليس القيام بحسابات ديفي - هيلمان المعقّدة.

يتطلب بروتوكول ISAKMP أن يلبي توليد الكوكيز المتطلبات الثلاث الأساسية الآتية:

1. يجب أن يعتمد الكوكي على الأطراف المعنية. وبهذا يُمنَع المهاجِم من الحصول على الكوكي باستخدام عنوان IP ومنفذ UDP حقيقين ثم استعمال ذلك الكوكي لإغراق الضحية بالطلبات المقدّمة من عناوين IP أو منافذ تم اختيارها عشوائياً.
2. يجب ألا يكون بإمكان أي شخص آخر غير الجهة المُصدرة توليد كوكيز تكون مقبولة لدى تلك الجهة. ويعني ذلك ضمناً أن الجهة المُصدرة ستَستخدم معلومات سرية محلية في توليد الكوكي والتحقق منه لاحقاً. ويجب أن لا يكون بالإمكان استخلاص تلك المعلومات السرية من أي كوكي. والهدف من هذا الشرط هو أن الجهة المُصدرة لن تحتاج إلى حفظ نسخ من الكوكيز الخاصة بها مما قد يجعلها أكثر عرضة للانكشاف، ولكن سيمكنها التحقق من أي إشعار استلام لكوكي عندما تحتاج إلى ذلك.
3. يجب أن تكون أساليب توليد الكوكي والتحقق منه سريعة لإحباط الهجمات التي تهدف إلى استهلال موارد المعالج.

يتلخص الأسلوب الموصى به لإنشاء كوكي في استخدام دالة من دوال التحوير (hashing) السريعة (على سبيل المثال: MD5) على عناوين IP للمصدر والوِجهة، ومنافذ UDP للمصدر والوِجهة، وقيمة سريّة مولّدة محليا.

تدعم خوارزمية أوكلي استخدام مجموعات مختلفة من مفاتيح تبادل ديفي-هيلمان، حيث تضم كل مجموعة تعريف المتغيرين العامّين وهوية الخوارزمية. وتشمل المواصفات الحالية المجموعات الآتية:

- الرفع الأسّي المقاسي مع مُعامِل من 768 بتاً:

$q = 2^{768} - 2^{704} - 1 + 2^{64} \times (\lfloor 2^{638} \times \pi \rfloor + 149686)$

$\alpha = 2$

- الرفع الأسّي المقاسي مع مُعامِل من 1024 بتاً:

$q = 2^{1024} - 2^{960} - 1 + 2^{64} \times (\lfloor 2^{894} \times \pi \rfloor + 129093)$

$\alpha = 2$

- الرفع الأسّي المقاسي مع مُعامِل من 1536 بتاً:
  - سيتم تحديد المتغيرات.
- مجموعة المنحنى الإهليلجي (Elliptic curve group) على 2^{155}:
  - المولد (الست عشري): X=7B, Y=1C8.
  - متغيرات المنحنى الإهليلجي (الست عشرية): A=0, Y= 7338F.
- مجموعة المنحنى الإهليلجي (Elliptic curve group) على 2^{185}:
  - المولد (الست عشري): X=18, Y=D.
  - متغيرات المنحنى الإهليلجي (الست عشرية): A=0, Y= 1EE9.

المجموعات الثلاث الأُوَل هي خوارزمية ديفي - هيلمان التقليدية باستخدام الرفع الأسّي المقاسي. تستخدم المجموعتان الأخريان المنحنى الإهليلجي المناظر لديفي- هيلمان.

تستعمل خوارزمية أوكلي الأعداد التي تُستخدم لمرة واحدة فقط للحماية ضد هجمات إعادة الإرسال. ويتم توليد كل عدد من تلك الأعداد محلياً كعدد شبه عشوائي. تظهر تلك الأعداد في الردود ويتم تشفيرها أثناء بعض الإجراءات في عملية التبادل لأغراض الحماية.

يمكن استخدام ثلاثة أساليب مختلفة للتوثيق مع خوارزمية أوكلي:

- التواقيع الرقمية: يتم توثيق عملية التبادل عبر توقيع ناتج دالة تحوير (هاش) يمكن الحصول عليه بصورة متبادلة؛ ويقوم كل طرف بتشفير الهاش مع المفتاح الخاص به. ويتم توليد الهاش على المتغيرات المهمة؛ كهويات المستخدمين والأعداد التي تُستخدم لمرة واحدة فقط.
- التشفير بالمفاتيح العامة: يتم توثيق عملية التبادل عبر تشفير المتغيرات كهوية المُستخدِمين والأعداد التي تُستخدم لمرة واحدة فقط، وذلك بواسطة المفتاح الخاص بالمرسل.
- التشفير بالمفاتيح المتماثلة: يمكن استخدام مفتاح مستمد من آلية خارج النطاق لتوثيق التبادل بواسطة التشفير المتماثل لمتغيرات عملية التبادل.

❖ مثال لتبادل أوكلي:

تتضمن مواصفات بروتوكول أوكلي عدداً من الأمثلة لعمليات التبادل التي يُسمح بها بموجب البروتوكول. ولإعطاء نكهة لحديثنا عن أوكلي، نورد هنا مثالاً واحداً، يطلق عليه في المواصفات عملية اعتساف تبادل المفاتيح، نظراً لأن التبادل يتم باستخدام ثلاثة رسائل فقط.

يوضّح الشكل 6-11 بروتوكول اعتساف تبادل المفاتيح (aggressive key exchange protocol). في الخطوة الأولى، ينقل البادئ I كوكي، والمجموعة التي ستُستخدَم، ومفتاح ديفي - هيلمان الخاص بـ I لهذا التبادل. كما يشير I أيضاً إلى الخوارزميات التي ستستخدم في هذا التبادل للتشفير بالمفاتيح العامة، وتوليد دالة التحوير (هاش)، والتوثيق. كما تتضمن الرسالة أيضا معرِّفي البادئ I والمستجيب R والعدد الذي سيستخدمه I لمرة واحدة فقط في هذا التبادل. وأخيراً، وباستخدام

المفتاح الخاص بـ I، يُذيِّل I الرسالة بتوقيعه على هويتي I وR، والعدد المستخدم لمرة واحدة، والمجموعة، والمفتاح العام لديفي - هيلمان، والخوارزميات المعروضة للاستخدام.

عندما يتلقى R الرسالة يتحقق من التوقيع باستخدام مفتاح توقيع I العام. ويرسل R إشعاراً بالاستلام وذلك بإعادة إرسال الكوكي الخاص بـ I، ومعرِّفه، وعدده المستخدم مرة واحدة، وأيضاً المجموعة. كما يُدرج R أيضا في الرسالة كوكي، ومفتاحه العام لديفي - هيلمان، والخوارزميات المختارة (والتي يجب أن تكون ضمن الخوارزميات المعروضة)، ومعرِّف R، والعدد الذي يستخدمه R لمرة واحدة في هذا التبادل. وأخيراً، يُذيِّل R الرسالة بتوقيعه باستخدام المفتاح الخاص به على المعرِّفين، والعددين المستخدمين لمرة واحدة، والمجموعة، والمفتاحين العامين لديفي - هيلمان، والخوارزميات المختارة.

عندما يتلقى I الرسالة الثانية يتحقق من التوقيع باستخدام المفتاح العام لـ R. تضمن قيم الأعداد المستخدمة لمرة واحدة أن هذه الرسالة ليست تكراراً لرسالة قديمة. ولإتمام عملية التبادل، لا بد أن يرسل I رسالة إلى R ليؤكد لـ R أنه قد استلم المفتاح العام لـ R.

2-6-6 بروتوكول أمن الإنترنت وإدارة المفاتيح (ISAKMP)

يحدّد بروتوكول أمن الإنترنت وإدارة المفاتيح (ISAKMP) الإجراءات وصيغ الرزم اللازمة لإنشاء الارتباطات الأمنية والتفاوض عليها وتعديلها وإلغائها. وكجزء من عملية إنشاء ارتباط أمني جديد، يحدّد ISAKMP الأحمال الآجرة اللازمة لتبادل بيانات توليد المفاتيح وبيانات التوثيق. وتوفر صيغ الحمولة هذه إطاراً متوافقاً ومستقلاً لبروتوكول تبادل المفاتيح، وخوارزميات التشفير، وآليات التوثيق.

❖ صيغة ترويسة بروتوكول ISAKMP:

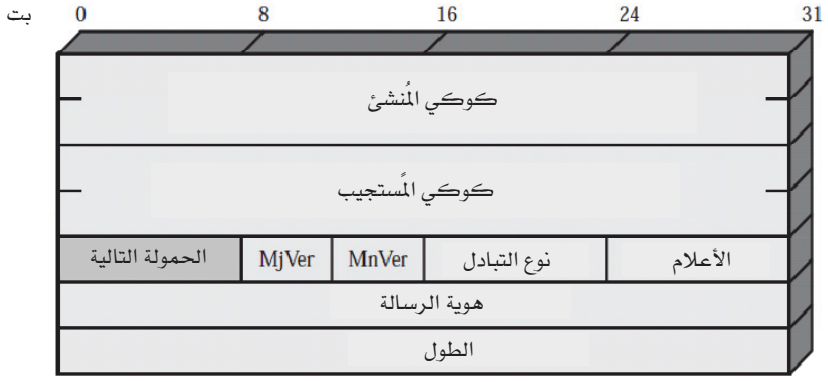
تتكون رسالة ISAKMP من ترويسة ISAKMP يليها حمل آجر واحد أو أكثر، وتنقل كلها ضمن بروتوكول النقل. وتتطلب المواصفات أن تدعم التنفيذات استخدام UDP كبروتوكول للنقل.

يوضّح الشكل 6-12 (a) صيغة الترويسة لرسالة ISAKMP، والتي تتكون من الحقول الآتية:

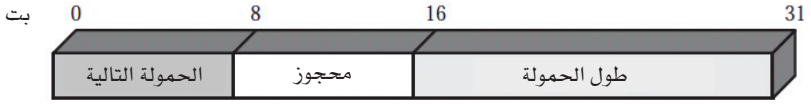
- كوكي البادئ (Initiator Cookie) (64 بتاً): كوكي الجهة التي بادرت بإنشاء الارتباط الأمني، أو الإخطار بالارتباط الأمني، أو إلغاء الارتباط الأمني.
- كوكي المجيب (Responder Cookie) (64 بتاً): كوكي الجهة المجيبة؛ يكون هذا الحقل خالياً في الرسالة الأولى من البادئ.
- الحمولة التالية (Next Payload) (8 بتات): يبيّن نوع الحمولة الأولى في الرسالة؛ سيتم مناقشة الحمولات في الجزء التالي.
- رقم الإصدار الرئيس (Major Version) (4 بتات): يبيّن رقم الإصدار الرئيس لبروتوكول ISAKMP المُستخدَم.
- رقم الإصدار الثانوي (Minor Version) (4 بتات): يبيّن رقم الإصدار الثانوي لبروتوكول ISAKMP المُستخدَم.
- نوع التبادل (Exchange Type) (8 بتات): يبيّن نوع التبادل، سيناقش لاحقاً في هذا الجزء.
- الأعلام (Flags) (8 بتات): تُبين الخيارات المحدّدة لتبادل بروتوكول ISAKMP. وقد تم تحديد اثنين من تلك البتات حتى الآن هما بت التشفير (Encryption) وبت الارتباط (Commit). وتأخذ بت التشفير القيمة 1 إذا كانت جميع الأحمال الآجرة التالية للترويسة قد تم تشفيرها باستخدام خوارزمية التشفير الخاصة بهذا الارتباط الأمني. أما بت الارتباط فيستخدم

لضمان أن المادة المُشفَّرة لا يتم استلامها قبل الانتهاء من إنشاء الارتباط الأمني.

- هوية الرسالة (Message ID) (32 بتاً): هوية فريدة لهذه الرسالة.
- الطول (Length) (32 بتاً): الطول الكلي للرسالة (الترويسة بالإضافة إلى الحمولات) بالبايتات.



(a) ترويسة ISAKMP



(b) ترويسة حمولة عامة

الشكل 6-12: صيغة ISAKMP.

❖ أنواع الحمولة في بروتوكول ISAKMP:

تبدأ جميع أنواع الحمولة في بروتوكول ISAKMP بنفس ترويسة الحمولة العامة المبينة في الشكل 6-12 (b). وتكون قيمة حقل الحمولة التالية صفراً فقط إذا كانت تلك هي الحمولة الأخيرة في الرسالة؛ وإلا فإن قيمتها تحدّد نوع الحمولة

المقبلة. ويدل حقل طول الحمولة على حجم هذه الحمولة بالبايتات بما في ذلك ترويسة الحمولة العامة.

يلخص الجدول 6-3 أنواع الحمولة المحدّدة لبروتوكول ISAKMP، كما يسرد الحقول أو المتغيرات التي تشكّل جزءاً من كل حمولة. وتُستخدم حمولة الارتباط الأمني (SA payload) للبدء في إنشاء الارتباط الأمني. في هذه الحمولة، قيمة متغير نطاق التفسير (DOI) تُحدّد نطاق التفسير الذي تتم المفاوضات في إطاره. ويُعدُّ IPSec أحد الأمثلة لقيم DOI، ولكن يمكن استخدام ISAKMP في سياقات أخرى. أما مُعامِل الحالة (Situation parameter) فيحدّد السياسة الأمنية لتلك المفاوضات، وبشكلٍ أساسي يتم من خلاله تحديد المستويات الأمنية اللازمة للتشفير والسرية (على سبيل المثال، مستوى الحساسية، وحجرة الأمن (security compartment)).

تتضمّن حمولة الاقتراح (Proposal payload) معلومات تُستخدم أثناء التفاوض بخصوص الارتباط الأمني. وتُبيّن الحمولة بروتوكول هذا الارتباط الأمني (إما ترويسة التوثيق أو التغليف الأمني للحمولة) والذي من أجله يتم التفاوض على الخدمات والآليات. كما تتضمّن الحمولة أيضاً المُعامِل الأمني (SPI) للجهة المُرسِلة وعدد التحويلات (transforms). وجديرٌ بالذكر أن كلّ تحويل يوضع في حمولة من حمولات التحويل. يوفّر استخدام عدة حمولات تحويل للبادئ عدة بدائل، والتي يتعيّن على المجيب اختيار أحدها أو رفض العرض كله.

يُحدّد حقل حمولة التحويل (Transform payload) أحد التحويلات الأمنية لاستخدامه في تأمين قناة الاتصالات للبروتوكول المحدّد. ويُستخدم متغيّر رقم التحويل لتحديد تلك الحمولة بحيث يمكن للمجيب استخدامه كإشارة إلى قبوله لذلك التحويل. ويحدّد حقل هوية التحويل (Transform-ID) وحقل الخصائص (Attributes) تحويلاً بعينه (مثلاً، 3DES للتغليف الأمني للحمولة، و-HMAC-SHA-96-1 لترويسة التوثيق) مع الخصائص الخاصة به (مثلاً، طول كود التحوير (الهاش)).

الجدول 6-3 أنواع حمولات ISAKMP.

النوع	المتغيرات	الوصف
الارتباط الأمني (SA)	مجال التفسير (DOI)، الحالة	يُستخدم للتفاوض حول الخواص الأمنية، يحدّد DOI والحالة التي ينعقد التفاوض في ظلها
المقترح (P)	رقم المقترح، هوية البروتوكول، حجم مؤشر المُعامِلات الأمنية، عدد التحويلات، مؤشر المُعامِلات الأمنية.	يُستخدم أثناء التفاوض حول ارتباط أمني؛ يُحدّد البروتوكول المُستخدم وعدد التحويلات
التحويل (T)	رقم التحويل، هوية التحويل، خواص الارتباط الأمني	يُستخدم أثناء التفاوض حول ارتباط أمني، يُحدّد التحويل وخواص الارتباط الأمني ذات الصلة
تبادل المفاتيح (KE)	بيانات تبادل المفاتيح	يدعم عدة أساليب لتبادل المفاتيح
التعريف (ID)	نوع التعريف، بيانات التعريف	يُستخدم لتبادل معلومات التعريف
الشهادة (CERT)	تكويد الشهادة، بيانات الشهادة	يُستخدم لنقل الشهادات والبيانات الأخرى المتعلقة بها
طلب الشهادة (CR)	أرقام أنواع الشهادات، أنواع الشهادات، أرقام جهات إصدار الشهادات، جهات إصدار الشهادات.	يُستخدم لطلب الشهادات؛ يُحدّد أنواع الشهادات المطلوبة والجهات المقبولة لإصدار الشهادات
الهاش (HASH)	بيانات الهاش	يتضمّن بيانات مولّدة من وظيفة الهاش
التوقيع (SIG)	بيانات التوقيع	يتضمّن بيانات مولّدة من وظيفة التوقيع الرقمي
العدد الذي يستخدم لمرة واحدة فقط (NONCE)	بيانات العدد الذي يستخدم لمرة واحدة فقط	يتضمّن عدداً يستخدم لمرة واحدة فقط
الإخطار (N)	DOI، هوية البروتوكول، حجم مؤشر المُعامِلات الأمنية، نوع رسالة الإخطار، مؤشر المُعامِلات الأمنية، بيانات الإخطار	يُستخدم لنقل بيانات الإخطار، كحالة خطأ ما
الحذف (D)	DOI، هوية البروتوكول، حجم مؤشر المُعامِلات الأمنية، عدد مؤشرات المُعامِلات الأمنية، مؤشرات المُعامِلات الأمنية (واحد أو أكثر)	يُحدّد ارتباطاً أمنياً لم يعد صالحاً

يمكن استخدام حمولة تبادل المفاتيح (Key Exchange payload) لمجموعة متنوعة من أساليب تبادل المفاتيح، بما في ذلك أوكلي، وديفي - هيلمان، وتبادل المفاتيح المبني على RSA المُستخدَم من قِبَل PGP. ويتضمّن حقل بيانات تبادل المفاتيح البيانات المطلوبة لتوليد مفتاح الجلسة ويعتمد على الخوارزمية المُستخدَمة لتبادل المفاتيح.

يُستخدم حقل حمولة التعريف (Identification payload) لتحديد هوية النظراء المتواصلين، ويمكن استخدامه أيضاً لتحديد موثوقية المعلومات. وعادةً ما يحتوي حقل بيانات الهوية (ID Data field) على عنوان IPv4 أو IPv6.

تنقل حمولة الشهادة (Certificate payload) شهادة مفتاح عام. ويبيّن حقل ترميز الشهادة (Certificate Encoding field) نوع الشهادة أو المعلومات ذات الصلة بالشهادة، والتي قد تشمل ما يأتي:

- شهادة X.509 المُغلَّفة بـ PKCS #7.
- شهادة PGP.
- مفتاح DNS المُوقَّع.
- شهادة X.509 للتوقيع.
- شهادة X.509 لتبادل مفاتيح.
- علامات كيربيروس (Kerberos tokens).
- قوائم إلغاء الشهادات (CRL).
- قوائم إلغاء الهيئات (ARL).
- شهادة SPKI.

في أي مرحلة من مراحل تبادلات بروتوكول ISAKMP يستطيع المرسل أن يُرفِق حمولة طلب شهادة (Certificate Request) لطلب شهادة الطرف الآخر المُتّصَل به. وقد تسرد الحمولة أكثر من نوع من الشهادات المقبولة، وأيضاً أكثر من جهة مقبولة لإصدار الشهادات.

يحتوي حقل حمولة الهاش (Hash payload) على البيانات المولّدة بواسطة دوال التحوير المطبَّقة على جزء من الرسالة و/أو حالة بروتوكول ISAKMP. وقد تُستخدم هذه الحمولة للتحقق من سلامة البيانات في رسالةٍ ما أو لتوثيق الجهات المتفاوضة.

يحتوي حقل حمولة التوقيع (Signature payload) على البيانات المولدة بواسطة التوقيع الرقمي على جزءٍ من الرسالة و/أو حالة بروتوكول ISAKMP. وتستخدم هذه الحمولة للتحقق من سلامة البيانات في الرسالة، كما يمكن استخدامها أيضاً لخدمات دحض الإنكار.

يحتوي حقل حمولة العدد الذي يستخدم لمرة واحدة فقط (Nonce payload) على بيانات عشوائية تُستخدم لضمان الحيوية (liveness) خلال عملية التبادل وتوفير الحماية ضد هجمات إعادة الإرسال.

يحتوي حقل حمولة الإخطار (Notification payload) على معلومات عن الخطأ أو معلومات عن حالة ذلك الارتباط الأمني أو حالة مفاوضاته. وقد تم تعريف رسائل أخطاء بروتوكول ISAKMP كما يأتي:

نوع الحمولة غير صحيح	لم يتم اختيار أي مقترح
هوية البروتوكول غير صحيحة	بيانات الهاش غير صحيحة
تكويد الشهادة غير صحيح	الإصدار الثانوي غير صحيح
DOI غير مدعوم	تركيب المقترح غير صالح
مؤشر المُعامِلات الأمنية (SPI) غير صحيح	فشل التوثيق
الشهادة غير صحيحة	نوع التبادل غير صحيح
الحالة غير مدعومة	الحمولة مشوَّهة
هوية التحويل غير صحيحة	التوقيع غير صحيح
تركيب طلب الشهادة غير صالح	الأعلام (Flags) غير صحيحة
الكوكي غير صحيح	بيانات المفتاح غير صحيحة
الخواص غير مدعومة	إخطار بالعنوان
جهة إصدار الشهادة غير صحيحة	هوية الرسالة غير صحيحة
الإصدار الرئيسي غير صحيح	

حتى الآن تم تعريف رسالة حالة بروتوكول ISAKMP واحدة فقط وهي "متصلة". وبالإضافة إلى إخطارات بروتوكول ISAKMP تلك، تُستخدم أيضاً إخطارات خاصة بـ DOI. وفيما يتعلق ببروتوكول IPSec فقد تم تعريف الرسائل الإضافية الآتية للحالة:

- فترة العمر للمُجيب (Responder-Lifetime): لبيان فترة العمر للارتباط الأمني الذي تم اختياره من قِبَل المُجيب.
- حالة إعادة الإرسال (Replay-Status): وتُستخدم للتأكيد الإيجابي على رغبة (أو عدم رغبة) المُجيب في تفعيل إمكانية اكتشاف الخدمة المضادة لإعادة الإرسال.
- الاتصال الأوّليّ (Initial-Contact): لإبلاغ الطرف الآخر أن هذا هو أول ارتباط أمني يجري إنشاؤه مع النظام البعيد. ويمكن لمتلقي هذا الإشعار بعد ذلك حذف أي ارتباط أمني لديه للنظام المُرسِل مُفترضاً أن النظام المُرسِل قد تم بدء إعادة تشغيله من جديد، ولذا لم يعد لديه إمكانية الوصول إلى تلك الارتباطات الأمنية.

ويشير حقل حمولة الحذف (Delete payload) إلى الارتباطات الأمنية التي قام المُرسِل بحذفها من قاعدة بياناته، ومن ثَمَّ لم تعد سارية المفعول.

❖ تبادلات بروتوكول ISAKMP:

يوفِّر بروتوكول ISAKMP إطاراً لتبادل الرسائل، حيث تُستخدم أنواع الحمولات كلبنات بناء. وتُحدّد المواصفات خمسة أنواع للتبادلات ينبغي دعمها، والتي يلخِّصها الجدول 6-4. تشير SA في الجدول إلى حمولة ارتباط أمني مع ما يرتبط بها من حمولات البروتوكول وحمولات التحويل.

يسمح التبادل الأساسي (Base Exchange) بنقل مواد تبادل المفاتيح وبيانات التوثيق معاً، مما يقلل من عدد التبادلات على حساب حماية الهوية. وتقوم أول رسالتين بتوفير الكوكيز وإنشاء ارتباط أمني باستخدام البروتوكول والتحويلات

المتفق عليها، ويستخدم كلا الجانبين عدداً يُستعمل لمرة واحدة فقط للحماية ضد هجمات إعادة الإرسال. وتقوم الرسالتان الأخيرتان بتبادل بيانات المفتاح وهوية المُستخدِم بآلية التوثيق المُستخدمة لتوثيق المفاتيح والهويات والأعداد التي تُستعمل لمرة واحدة فقط من أول رسالتين.

يقوم تبادل حماية الهوية (Identity Protection Exchange) بتوسيع التبادل الأساسي لحماية هويات المُستخدِمين، حيث تقوم أول رسالتين بإنشاء الارتباط الأمني. وتقوم الرسالتان التاليتان بعملية تبادل المفاتيح، مع الأعداد التي تُستخدَم لمرة واحدة للحماية ضد هجمات إعادة الإرسال. وبمجرد حساب مفتاح الجلسة، يتبادل الطرفان الرسائل المُشفَّرة التي تحتوي على بيانات التوثيق كالتوقيعات الرقمية وكذلك شهادات توثيق المفاتيح العامة بشكلٍ اختياري.

ويُستخدم تبادل التوثيق فقط (Authentication Only Exchange) للقيام بتوثيقٍ متبادَل بدون تبادل للمفاتيح، حيث تقوم أول رسالتين بإنشاء الارتباط الأمني. بالإضافة إلى ذلك يستخدم المُجيب الرسالة الثانية لبيان هويته مستخدماً التوثيق لحماية الرسالة. ويقوم البادئ بإرسال رسالة ثالثة للتعريف بهويته الموثّقة.

يُقلل التبادل الاعتسافي (Aggressive Exchange) عدد التبادلات من ناحية ولكنه - من ناحية أخرى - لا يوفر حمايةً للهوية. في الرسالة الأولى يقترح البادئ ارتباطاً أمنياً مع البروتوكول المصاحب له بالإضافة إلى خيارات التحويل. كما يقوم أيضاً ببدء عملية تبادل المفاتيح ويرسل هويته. في الرسالة الثانية يشير المُجيب إلى قبوله لذلك الارتباط الأمني مع بروتوكول وتحويل معينين، كما يقوم باستكمال عملية تبادل المفاتيح وتوثيق المعلومات المُرسَلة. وفي الرسالة الثالثة ينقل البادئ نتيجة توثيق تشمل البيانات السابقة مُشفَّرةً بواسطة المفتاح االسري المُشترك للجلسة.

يُستخدم التبادل الإخطاري (Informational Exchange) لنقل المعلومات باتجاه واحد بهدف إدارة الارتباط الأمني.

الجدول 6-4 أنواع تبادلات ISAKMP.

التبادل	ملاحظات
(a) التبادل الأساسي	
(1) **I → R:** SA; NONCE	بدأ التفاوض على ارتباط أمني- بروتوكول ISAKMP
(2) **R → I:** SA; NONCE	الاتفاق على الارتباط الأمني الأساسي
(3) **I → R:** KE; ID_I; AUTH	توليد المفتاح، يتحقق المستجيب من هويّة البادئ
(4) **R → I:** KE; ID_R; AUTH	يتحقق البادئ من هويّة المستجيب، توليد المفاتيح، يتم إنشاء الارتباط الأمني
(b) تبادل حماية الهوية	
(1) **I → R:** SA	بدأ التفاوض على ارتباط أمني- بروتوكول ISAKMP
(2) **R → I:** SA	الاتفاق على الارتباط الأمني الأساسي
(3) **I → R:** KE; NONCE	توليد المفتاح
(4) **R → I:** KE; NONCE	توليد المفتاح
(5)* **I → R:** ID_I; AUTH	يتحقق المستجيب من هويّة البادئ
(6)* **R → I:** ID_R; AUTH	يتحقق البادئ من هويّة المستجيب، يتم إنشاء الارتباط الأمني
(c) تبادل التوثيق فقط	
(1) **I → R:** SA; NONCE	بدأ التفاوض على ارتباط أمني- بروتوكول ISAKMP
(2) **R → I:** SA; NONCE; ID_R; AUTH	الاتفاق على الارتباط الأمني الأساسي، يتحقق المستجيب من هويّة البادئ
(3) **I → R:** ID_I; AUTH	يتحقق البادئ من هويّة المستجيب، يتم إنشاء الارتباط الأمني
(d) تبادل اعتسافي	
(1) **I → R:** SA; KE; NONCE; ID_I	بدأ التفاوض على ارتباط أمني- بروتوكول ISAKMP وتبادل المفاتيح
(2) **R → I:** SA; KE; NONCE; ID_R; AUTH	يتحقق المستجيب من هويّة البادئ، توليد المفتاح، الاتفاق على الارتباط الأمني الأساسي
(3)* **I → R:** AUTH	يتحقق البادئ من هويّة المستجيب، يتم إنشاء الارتباط الأمني
(e) تبادل إخطاري	
(1)* **I → R:** N/D	إخطار بخطأ أو بحالة، أو إلغاء

مفتاح:

I = البادئ

R = المستجيب

* = تمثل تشفير حمولة بعد ترويسة بروتوكول ISAKMP

AUTH = آلية التوثيق المستخدمة

7-6 توصيات للمطالعة

تم تغطية IPv6 وIPv4 بتفصيل أكبر في [STAL04]، ويتضمن [CHEN98] مناقشةً جيدة لتصميم بروتوكول IPSec. أما [FRAN01] و[DORA99] فيقدمان معالجة شاملة لبروتوكول IPSec.

[CHEN98] Cheng, P., et al. "A Security Architecture for the Internet Protocol," *IBM Systems Journal,* Number 1, 1998.

[DORA03] Doraswamy, N., and Harkins, D. *IPSec.* Upper Saddle River, NJ: Prentice Hall, 2003.

[FRAN01] Frankel, S. *Demystifying the IPSec Puzzle.* Boston: Artech House, 2001.

[STAL04] Stallings, W. *Computer Networking with Internet Protocols and Technology.* Upper Saddle River, NJ: Prentice Hall, 2004.

8-6 مصادر للمعلومات على الويب

مشروع المعهد الوطني للمعايير والتكنولوجيا (NIST) الخاص ببروتوكول IPSec: يتضمن أوراقاً بحثية وعروضاً وتنفيذات مرجعية.

9-6 مصطلحات رئيسة

Anti-replay service	خدمة مضادة لإعادة الإرسال
Authentication header (AH)	ترويسة التوثيق
Encapsulating security payload (ESP)	التغليف الأمني للحمولة
Internet Security Association and Key Management Protocol (ISAKMP)	جمعية أمن الإنترنت وبروتوكول إدارةِ المفاتيح
IP Security (IPSec)	بروتوكول أمن الإنترنت
Oakley key determination protocol	بروتوكول أوكلي لتعيين المفاتيح
Replay attack	هجوم إعادة الإرسال
Security Association (SA)	الارتباط الأمني
Transport mode	نمط النقل
Tunnel mode	نمط النفق

10-6 أسئلة للمراجعة ومسائل

1-10-6 أسئلة للمراجعة

1-6 أعط أمثلة لتطبيقات بروتوكول IPSec.

2-6 ما الخدمات التي يقدمها بروتوكول IPSec؟

3-6 ما المتغيرات التي تُعرّف الارتباط الأمني وما المتغيرات التي تصف طبيعة ارتباطٍ أمنيٍّ معين؟

4-6 ما الفرق بين نمط النقل ونمط النفق؟

5-6 ما المقصود بهجوم إعادة الإرسال؟

6-6 لماذا يشتمل التغليف الأمني للحمولة على حقل الحشو؟

7-6 ما الطرق الأساسية لتجميع الارتباطات الأمنية؟

8-6 ما دور بروتوكول أوكلي لتعيين المفاتيح ودور بروتوكول أمن الإنترنت وإدارة المفاتيح ISAKMP في بروتوكول أمن الإنترنت IPSec؟

2-10-6 مسائل

1-6 أثناء مناقشة معالجة ترويسة التوثيق، أشير إلى أن حساب كود التحقق من الرسالة (MAC) لا يشمل كل الحقول في ترويسة التوثيق:

a. لكل واحد من الحقول في ترويسة IPv4، بيِّن ما إذا كان الحقل غيرَ قابل للتغيير، أو قابلاً للتغيير ولكنه تغييرٌ مُتوقع، أو قابلاً للتغيير (يُصفّر قبل حساب ICV).

b. قم بنفس الشيء بالنسبة لترويسة IPv6.

c. قم بنفس الشيء بالنسبة لترويسات IPv6 الملحقة. وفي كل حالة على حدة، برر قرارك لكل حقل.

2-6 عند استخدام نمط النفق، يتم إنشاء ترويسة بروتوكول إنترنت خارجية. لكلٍّ من IPv4 وIPv6، وَضِّح العلاقة بين كل حقل في ترويسة بروتوكول IP الخارجية وكل ترويسة مُلحقة في الرزمة الخارجية مع الحقل المناظر أو الترويسة المُلحقة المناظرة لرزمة بروتوكول IP الداخلية. أي وَضِّح أيّ قيم الترويسة الخارجية يتم استنتاجها من قيم الترويسة الداخلية وأيّ منها يتم تحديده بشكلٍ مستقل عن قيم الترويسة الداخلية.

3-6 مطلوب القيام بالتوثيق والتشفير من طرفٍ إلى طرف بين مضيفين. ارسم أشكالاً مشابهة للشكلين 6-6 و6-9. تُوضح:

a. جوار النقل، مع تطبيق التشفير قبل التوثيق.

b. ارتباطاً أمنياً بنمط النقل مجمّعاً داخل ارتباط أمني بنمط النفق، مع تطبيق التشفير قبل التوثيق.

c. ارتباطاً أمنياً بنمط النقل مجمّعاً داخل ارتباط أمني بنمط النفق، مع تطبيق التوثيق قبل التشفير.

4-6 تنص بنية أمن بروتوكول الإنترنت IPSec على أنه عند تجميع ارتباطين أمنيين بنمط النقل ليتسنى استخدام كلٍّ من بروتوكول ترويسة التوثيق وبروتوكول التغليف الأمني للحمولة من العمل على نفس التدفق من طرف إلى طرف، فإن ترتيباً واحداً فقط للبروتوكولات الأمنية يكون مناسباً: القيام ببروتوكول التغليف الأمني للحمولة قبل بروتوكول ترويسة التوثيق. وضّح أسباب كون ذلك هو النهج الموصى به بدلاً من التوثيق قبل التشفير.

5-6 a. أيّ أنواع تبادل بروتوكول ISAKMP (الجدول 6-4) يُناظر تبادل أوكلي الاعتسافي للمفاتيح (الشكل 6-11) ؟

b. في تبادل أوكلي الاعتسافي للمفاتيح، وضِّح نوع حمولة بروتوكول ISAKMP المناظر لكل متغير بكل رسالة.

الملحق A-6

التشبيك البيني وبروتوكول الإنترنت

يعطي هذا الملحق لمحةً عامّةً عن بروتوكولات الإنترنت، حيث نبدأ بنبذةٍ مختصرةٍ عن دور بروتوكول الإنترنتِ في توفير التشبيك البيني (internetworking) ونتبع ذلك بعرض بروتوكولي الإنترنت الرئيسين IPv4 وIPv6 .

دور بروتوكول الإنترنت

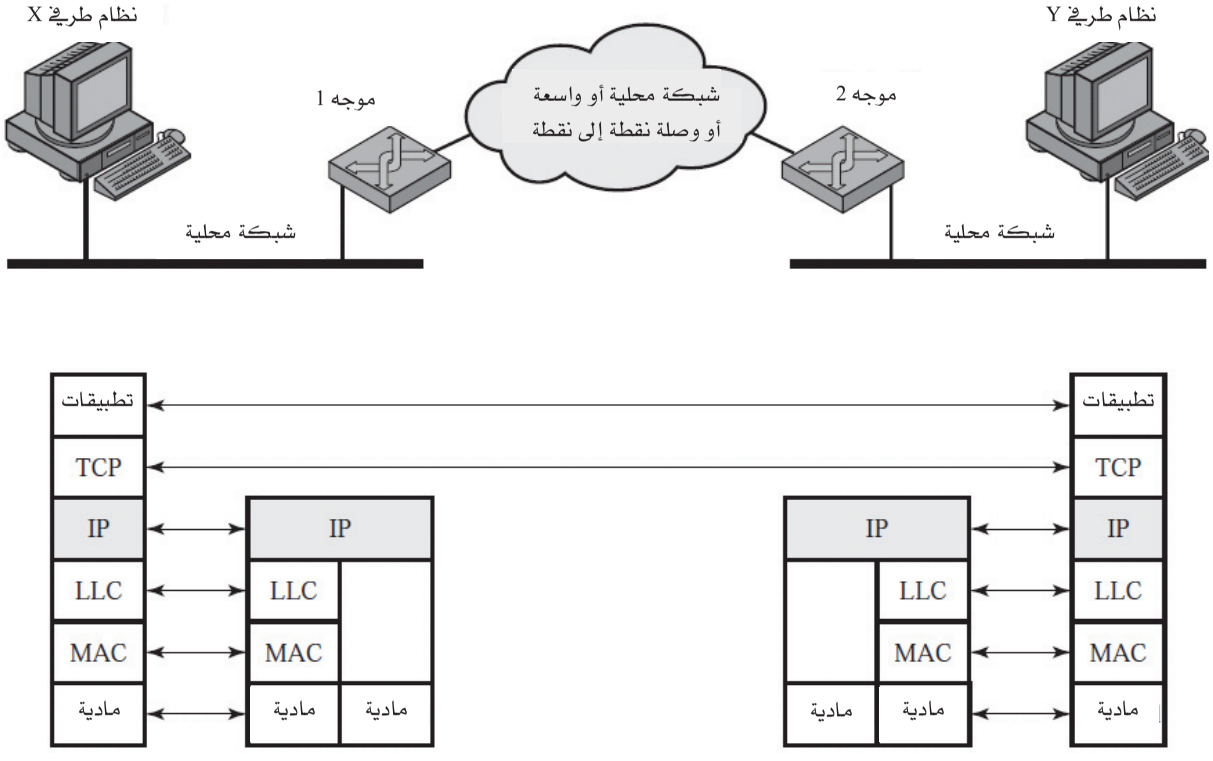
يوفر بروتوكول الإنترنت (IP) الوظائف المطلوبة لربط أنظمةٍ طرفية عبر عدة شبكات. لهذا الغرض فإن IP يُستخدم في كل الأنظمة الطرفيةِ وفي الموجّهات، أي الأجهزة التي تُوفر الاتصالات بين الشبكات. وتُغَلَّف البيانات عالية المستوى في نظام طرفي مصدري في وحدة بيانات بروتوكول IP ((Protocol Data Unit (PDU) تمهيداً لإرسالها. وتُمرّر PDU عبر شبكة أو أكثر من خلال الموجّهات الوسيطة حتى تصل إلى النظام الطرفي المُستهدف.

يجبُ على الموجّه أن يكون قادراً على العمل مع وجود عدة اختلافات بين الشبكات، منها:

- أساليب العنونة: قد تستخدم الشبكات أساليب مختلفةً لتخصيص العناوين للأجهزة على الشبكة. فعلى سبيل المثال؛ تستخدم شبكة اتصالات محلية (LAN) من طراز IEEE 802 عناوين بطول 16 بتاً أو بطول 48 بتاً لكل جهاز متصل بالشبكة. أمّا شبكة تحويل الرزم العامة من طراز X.25 فتستخدم عناوين بطول 12 خانة عشرية (Decimal Digit) بواقع 4 بتّات لكل خانة بمجموع 48 بتاً. وعليه فلابد من توفير أسلوب عالمي لعنونة الشبكات، وكذلك توفير خدمة للدليل (Directory Service).

- الحجم الأقصى للرزم: قد يتطلب الأمر تقسيم الرزم المرسلة من شبكةٍ معينة إلى قطعٍ أصغر لإرسالها إلى شبكةٍ أخرى، وتُعرف هذه العملية بالتجزيء (fragmentation). فعلى سبيل المثال، الحجم الأقصى للرزمة في شبكة إيثرنت هو 15,000 بايت بينما الحجم الشائع في شبكات X.25 هو 1000 بايت فقط. فعلى الموجّه الذي يستلم رزمةً مُرسَلةً من نظام إيثرنت لإرسالها عبر شبكة X.25 تجزئة الرزمة القادمة إلى رزمتين أصغر حجماً.
- الواجهات (Interfaces): تختلفُ وجهات البرمجيات (software) والأجهزة (hardware) للشبكات المختلفة. لذا فإن مفهوم عمل الموجّه ينبغي ألا يعتمد على تلك الاختلافات.
- الاعتمادية (Reliability): بوسع الخدمات المختلفة المتوفرة على الشبكة توفير أيّ شيءٍ بدءاً من دائرة افتراضية موثوقة من طرف إلى طرف (end-to-end) وانتهاءً بخدمة عديمة الموثوقية. لذا فلا ينبغي أن يعتمد الموجّه في عمله على فرضيّة موثوقية الشبكة.

كما يوضّح الشكل 6-13، يعتمد الموجّه في عمله على بروتوكول الإنترنت، في هذا المثال، يقوم بروتوكول الإنترنت (IP) ضمن مجموعة بروتوكولات TCP/IP بتأدية تلك المهمة. ولا بد من تنفيذ بروتوكول IP في جميع الأنظمة الطرفية، وعلى جميع الشبكات، وكذلك في الموجّهات. وعلاوة على ذلك ينبغي أن تكون البروتوكولات الأعلى من بروتوكول IP على كل نظام طرفي متوافقة لنجاح عمليات الاتصال. تحتاج الموجّهات الوسيطة لبروتوكولات حتى IP فقط.



الشكل 6-13: مثال لتهيئة نظام TCP/IP.

خذ في الاعتبار نقل كتلة بيانات من النظام الطرفي X إلى النظامِ الطرفي Y في الشكل 6-13. تستقبل طبقة IP على X كتل البيانات المطلوب إرسالها إلى Y من بروتوكول TCP على X، وتقوم طبقة IP بإلحاق ترويسة تحدّد عنوان الإنترنت العالمي لنظام الوِجهة الطرفي Y. يتكون هذا العنوان من جزأين: معرِّف شبكة ومعرّف نظامٍ طرفي، وسنشير هنا إلى هذه الكتلةِ كرزمة IP. بعد ذلك يُدرك بروتوكول IP أن مضيف الوِجهة Y يوجد على شبكةٍ فرعيةٍ أخرى. ولذا تكون الخطوة الأولى هي إرسال تلك الرزمة إلى موجّه، في هذا المثال الموجّه 1. للقيام بذلك، يُسلِّم IP وحدة بياناته إلى طبقة LLC مرفقةً بمعلومات العنونة الملائمة. وتقوم LLC بتكوين وحدة بيانات LLC تُسلِّمها إلى طبقة الماك أسفلها والتي تقوم بدورها بتكوين رزمة ماك تتضمّن ترويستها عنوان الموجّه 1.

بعد ذلك تنتقل الرزمة على الشبكة المحلية (LAN) إلى الموجّه 1 والذي يقوم بنزع ترويسات الرزمة وترويسة LLC والتذييلات ثم تحليل ترويسة IP لتحديد العنوان النهائيّ للبيانات (في هذه الحالة Y) حيث ينبغي على الموجّه الآن اتخاذ قرارٍ يتعلق بتوجيه مسار البيانات. هناك احتمالان:

1. النظام الطرفي المستهدف Y متصلٌ مباشرةً بإحدى الشبكات الفرعية المتصلة بالموجّه.
2. للوصول للنظام الطرفي المستهدف Y ينبغي المرور عبر موجّه آخر أو أكثر.

في هذا المثال لا بد للرزمة من المرور عبر موجّه 2 لبلوغ غايتها النهائية. وعليه يقوم موجّه 1 بتمرير رزمة IP إلى موجّه 2 عن طريق شبكات وسيطة، وفي هذا يستخدم الموجِّه بروتوكولات تلك الشبكة الوسيطة. فمثلاً، إذا كانت الشبكة الوسيطة من نوع X.25 فإن وحدة بيانات IP تُغلَّف مع معلومات العنونة الملائمة ضمن رزمة X.25 حتى تصل إلى موجّه 2. عندما تصل تلك الرزمة إلى موجّه 2 يقوم الموجّه بنزع ترويسة الرزمة ويكتشف الموجّه أنَّ الوِجهة النهائية

لرزمة IP هي النظام الطرفي Y والموصّل مباشرةً على شبكة فرعية متصلة بالموجّه. ومن ثَمَّ يُنشئ الموجّه رزمةً معنونةً إلى Y ويُرسلها على الشبكة المحلية (LAN). وأخيراً تصل البيانات إلى Y حيث تُزال ترويسات الرزمة وLLC والإنترنت وكذلك التذييلات.

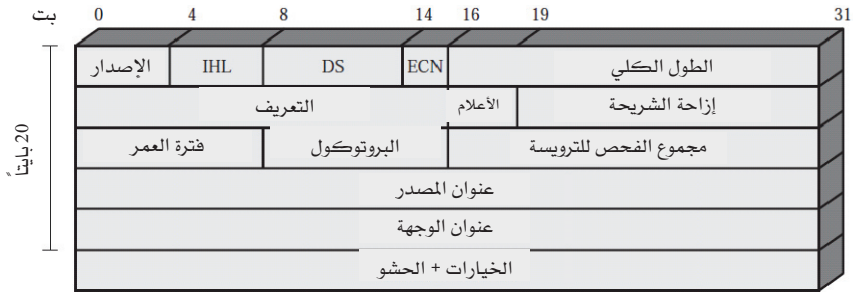
هذه الخدمة المقدّمة من IP غير موثوقة، حيث إن بروتوكول IP لا يضمن وصول البيانات كلّها ولا وصولها بالترتيب السليم إلى وِجهتها. وتناط بالطبقة في المستوى الأعلى (هنا بروتوكول TCP) مسئولية التعافي من أية أخطاء قد تحدُث. ويوفر هذا النهج قدراً كبيراً من المرونة. نظراً لأن تسليم البيانات غير مضمون، فلا توجد أيَّة متطلبات معيّنة للموثوقية على أيٍّ من الشبكات الفرعية. وعليه، فإن البروتوكول يمكنه العمل مع أي توليفة من الأنواع المختلفة من الشبكات الفرعية. وبما أن ضمان وصول البيانات بنفس ترتيب إرسالها غير مطلوب، فإنَّ الرزم المتتالية يمكنها أن تتبع مساراتٍ مختلفة عبر الإنترنت. ويسمح ذلك للبروتوكول بالاستجابة لحالات الازدحام والتعطل في الشبكة وذلك بتغيير المسارات.

الإصدار الرابع لبروتوكول الإنترنت (IPv4)

لعقودٍ مضت، بقى الإصدار الرابع من بروتوكول الإنترنت (IPv4) بمثابة حجر الزاوية لبنية بروتوكول TCP/IP.

يوضّح الشكل 6-14 (a) صيغة ترويسة IP والتي تتكون من 20 بايتاً أو 160 بتاً. وتتضمن الحقول الآتية:

- الإصدار (Version) (4 بتات): ويحدّد رقم الإصدار للسماح بتطور البروتوكول؛ القيمة 4.
- طول ترويسة الإنترنت ((Internet Header Length (IHL)) (4 بتات): طول الترويسة مقاساً بكلمات مؤلَّفة من 32 بتاً، الحد الأدنى 5 كلمات أي 20 بايتاً.



(a) ترويسة IPv4.

(b) ترويسة IPv6.

الشكل 6-14: ترويسات IP.

- DS/ECN (8 بتات): حيث تعني DS الخدمات التفاضلية (Differentiated Services)، وتعني ECN الإخطار الصريح بالازدحام (Explicit Congestion Notification). قبل استحداث الخدمات التفاضلية، كان يُطلق على هذا الحقل "نوع الخدمة" (Type of Service (TOS))

ويُستخدم لتحديد قيم متغيرات الموثوقية والأولوية والتأخير والطاقة الإنتاجية لنقل البيانات. حالياً يقُسّم الحقلُ إلى 6 بتّات للخدمات التفاضلية (DS) وبتّين للإخطار الصريح بالازدحام (ECN).

- الطول الكلي (Total Length) (16 بتاً): طول رزمة IP الكلي بالبايتات.
- المعرِّف (Identification) (16 بتاً): رقم تسلسلي يُكوِّن، مع عنواني المصدر والوِجهة ومع بروتوكول المُستخدِم، تعريفاً حصرياً لرزمةٍ ما. لذا يجب أن يكون هذا الرقم فريداً للرزمة لتمييزها عن أخرى تشاركها نفس عنواني المصدر والوِجهة ونفس بروتوكول المُستخدِم، وذلك طوال فترة بقاء الرزمة في الإنترنت.
- أعلام (Flags) (3 بتات): تم تعريف اثنين فقط من البتات الثلاث. في حالة تجزيء الرزمة، تُبيّن البت الأولى (المزيد More) ما إذا كان هذا الجزء هو الجزء الأخير من الرزمة الأصلية أو لا. أما البت الثانية (لا تجزّيء Don't Fragment) فتمنع التجزيء عندما تكون قيمتها "1". وتُستخدم تلك البت عندما لاتتوافر لدى النظام الطرفي المستهدف إمكانية إعادة تجميع الرزم المجزّأة. حيث يتم في هذه الحالة إهمال تلك الرزمة إذا تجاوز حجمها الحجم الأقصى للرزمة على أي شبكة فرعية على المسار. لذا فعندما تكون تلك البت لها القيمة 1 يستحسن استخدام توجيه مصدري (source routing) لتفادي الشبكات الفرعية التي لها قيم صغيرة للحجم الأقصى للرزمة.
- قيمة الإزاحة لهذا الجزء (Fragment Offset) (13 بتاً): يحدّد موضع هذا الجزء في الرزمة الأصلية، والتي تقاس بوحدة طولها 64 بتاً. وهذا يعني

أن أي جزء من أجزاء الرزمة – عدا الجزء الأخير – لا بد أن يكون طول حقل بياناته من مضاعفات 64 بتاً.

- العُمرُ الافتراضي ((Time to Live (TTL) (8 بتّات): يحدّد أقصى فترة بالثواني يُسمح لرزمة بأن تظل بالإنترنت. ويجب أن يقوم كل موجّه بإنقاص العمر الافتراضي لكل الرزم التي تمر به بواحد على الأقل. لذا فإن العمر الافتراضي يشبه إلى حدٍّ ما عدد القفزات.

- البروتوكول (8 بتات): يحدّد هذا الحقل بروتوكول الطبقة الأعلى مباشرةً التي ستتسلّم حقل البيانات عند الوِجهة، وعليه فإن هذا الحقل يحدّد نوع الترويسة التالية في الرزمة بعد ترويسة IP.

- المجموع التدقيقي للترويسة (Header Checksum) (16 بتاً): يتم تطبيق كود اكتشاف الأخطاء (error-detection code) على الترويسة فقط. ونظراً لأن بعض حقول الترويسة يمكن أن تتغير أثناء النقل (كحقل العمر الافتراضي أو الحقول المتعلقة بعملية تجزيء البيانات (segmentation)) فإن هذه العملية تُكرر ويُتحقق منها عند كل موجّه. قيمة حقل المجموع التدقيقي هي مكمل الواحد (1's complement) للمجموع بطول 16 بتاً لمكمل الواحد لكل كلمة بطول 16 بتاً من كلمات الترويسة. ولأغراض الحساب يتم تصفير حقل المجموع التدقيقي نفسه في البداية.

- عنوان المصدر (Source Address) (32 بتاً): يُكوّد هذا الحقل ليسمح بتخصيص عدد متغير من البتات لتحديد الشبكة والنظام الطرفي الموصّل بها (7 و24 بتاً، أو 14 و16 بتاً، أو 21 و8 بتات).

- عنوان الوِجهة (Destination Address) (32 بتاً): وله نفس خصائص عنوان المصدر.
- الخيارات (Options) (متغيرة): يُكوّد هذا الحقل لتمثيل الخيارات المطلوبة من المُرسِل والتي قد تشمل: وسمة الأمن (security label)، أو توجيه المصدر (source routing)، أو توجيه السِّجِل (record routing)، أو خاتم الوقت (time-stamping).
- الحشو (Padding) (متغير): يُستخدم لجعل طول ترويسة الرزمة من مضاعفات 32 بتاً.

الإصدار السادس لبروتوكول الإنترنت (IPv6)

في عام 1995 أصدر فريق مهام هندسة الإنترنت (IETF) – وهو الفريق الذي يضع معايير بروتوكولات الإنترنت – مواصفات الجيل التالي لبروتوكول الإنترنت، والذي عرف آنذاك بـ IPng. تحولت تلك المواصفات إلى مواصفات قياسية في عام 1996 وعُرِفت باسم IPv6.

يوفّر IPv6 عدداً من التحسينات الوظيفية مقارنةً بـ IPv4، حيث صُمِّم لاستيعاب السرعات العالية المتوفرة للشبكات الحديثة وكذلك الأنواع المختلفة من البيانات المُتدفقة عبر تلك الشبكات، بما في ذلك الصور والصوت والفيديو التي أصبحت شائعة الانتشار. ولكن القوة الدافعة وراء تطوير البروتوكول الجديد كانت الحاجة لمزيد من العناوين. يستخدم IPv4 عناوين بطول 32 بتاً لتحديد المصدر والوِجهة. مع النمو الهائل لشبكة الإنترنت والشبكات الخاصة المتصلة بها، أصبح طول هذا العنوان غير كاف لتعريف جميع الأنظمة التي تحتاج إلى عناوين. ويوضّح الشكل 6-14(b) أن حقل عناوين المصدر والوِجهة في IPv6 يتكون من 128 بتاً. في نهاية المطاف، من المتوقع ترحيل جميع المنشآت

التي تستخدم TCP/IP من بروتوكول الإنترنت الحالي إلى IPv6، ولكن هذه العملية سوف تستغرق عدة سنوات، أو ربما عقود.

❖ ترويسة IPv6

لترويسة IPv6 طولٌ ثابتٌ يبلغ 40 بتاً وتتضمن الحقول الآتية (الشكل 6-14(b)):

- الإصدار (Version) (4 بتات): ويحدّد رقم الإصدار لبروتوكول الإنترنت؛ القيمة 6.
- DS/ECN (8 بتات): حيث DS تعني الخدمات التفاضلية (Differentiated Services)، وتعني ECN الإخطار الصريح بالازدحام (Explicit Congestion Notification). قبل استحداث الخدمات التفاضلية، كان يُطلق على هذا الحقل "فئة المرور" (Traffic Class)، وتُرك محجوزاً للاستخدام من قِبَل الأطراف البادئة و/أو الموجّهات المُمَرِّرة لتحديد الفئات والأوليات المختلفة لرزم IPv6 والتمييز بينها. يشار حالياً لأول 6 بتات من حقل فئة المرور بالخدمات التفاضلية (Differentiated Services). أما البتان المتبقيتان فمحجوزتان لحقل الإخطار الصريح بالازدحام (Explicit Congestion Notification).
- وسمة التدفق (Flow Label) (20 بتاً) يمكن استخدام هذا الحقل من قِبَل المُضيف لبيان تلك الرزم التي تتطلب معاملة خاصة من قِبَل الموجّهات داخل الشبكة، حيث يمكن لوسمة التدفق المساعدة في عملية حجز الموارد والمعالجة الآنية لحركة مرور البيانات.
- طول الحمولة (Payload Length) (16 بتاً) طول الجزء المتبقى من رزمة IPv6 بعد الترويسة بالبايتات. وبعبارة أخرى، هو الطول الإجمالي لجميع

الترويسات الملحقة بالإضافة إلى طول وحدة بيانات بروتوكول النقل (Transport PDU).

- الترويسة التالية (Next Header) (8 بتات) يحدّد نوعية الترويسة التي تلي ترويسة IPv6 مباشرةً ؛ وهذه إما أن تكون ترويسة IPv6 ملحقة أو ترويسة طبقة أعلى، مثل TCP أو UDP.
- حد عدد القفزات (Hop Limit) (8 بتات) العدد المتبقي من القفزات المسموح به لهذه الرزمة. يقوم المصدر بتحديد هذه القيمة. وتقوم كل عقدة تمرّر هذه الرزمة بطرح 1 من قيمة هذا الحقل. تُهمل هذه الرزمة عندما تصل هذه القيمة إلى الصفر.
- عنوان المصدر (Source Address) (128 بتاً): عنوان مُنشئ الرزمة.
- عنوان الوِجهة (Destination Address) (128 بتاً): عنوان المستلِم المقصود لهذه الرزمة. في الواقع قد لا يكون هذا هو عنوان الوِجهة النهائية في حالة وجود ترويسة تمرير كما سنوضّح لاحقاً.

رغم أن ترويسة IPv6 أطول من الجزء الإلزامي لترويسة IPv4 (40 بايتاً مقابل 20 بايتاً)،فإنها تتضمن عدداً أقل من الحقول (8 حقول مقابل 12). ولهذا فإن العمليات التي تقوم بها الموجّهات أقل لكل ترويسة، مما يُسرع من عملية التوجيه.

❖ ترويسات IPv6 الملحقة

تشمل رزمة IPv6 ترويسة IPv6 التي نوقشت أعلاه، كما قد تشمل عدداً من الترويسات الملحقة. تم تعريف الترويسات الملحقة الآتية خارج نطاق IPSec:

- ترويسة خيارات القفزة - بقفزة (Hop-by-Hop Options Header): تُعرِّف الخيارات الخاصة التي تتطلب معالجة بكل قفزة.

- ترويسة التوجيه (Routing Header): توفّر توجيهاً ممتداً يماثل التوجيه المصدري في IPv4.
- ترويسة التجزيء: تتضمّن معلومات التجزيء وإعادة التجميع.
- ترويسة التوثيق: توفر سلامة الرزمة وتوثيقها.
- ترويسة التغليف الأمني للحمولة: توفر الخصوصية.
- ترويسة خيارات الوِجهة: تتضمن معلومات اختيارية تُفحص من قِبَل عقدة الوِجهة.

عند استخدام عدة ترويسات ملحقة، يوصي معيار IPv6 بترتيب ترويسات IPV6 على النحو الآتي:

1. ترويسة IPv6: يتعيّن إلزاميا أن تكون دائماً في المقدمة
2. ترويسة خيارات القفزة – بقفزة
3. ترويسة خيارات الوِجهة: للخيارات التي سيتم معالجتها من قِبَل أول وِجهة والتي تظهر في حقل عنوان IPv6 للوِجهة ـ بالإضافة إلى الوجهات التالية المتضمّنة في ترويسة التوجيه
4. ترويسة التوجيه
5. ترويسة التجزيء
6. ترويسة التوثيق
7. ترويسة التغليف الأمني للحمولة
8. ترويسة خيارات الوِجهة: للخيارات التي ينبغي معالجتها فقط من قِبَل الوِجهة النهائية للرزمة.

يوضّح الشكل 6-15 مثالاً لرزمة IPv6 التي تتضمن أمثلة لكل الترويسات غير الأمنية. لاحظ أن ترويسة IPv6 وكل ترويسة ملحقة تتضمن حقل الترويسة

التالية والذي يعرِّف نوعية الترويسة التالية مباشرةً. إذا كانت الترويسة التالية ترويسةً ملحقة فعندئذٍ يتضمّن ذلك الحقل مُعرِّف النوعية (type identifier) لتلك الترويسة. وإلا فإن ذلك الحقل يتضمّن معرِّف بروتوكول الطبقة الأعلى التي تستخدم IPv6 (عادةً ما يكون بروتوكول نقل)، بنفس القيم المستعملة بحقل البروتوكول في IPv4. في الشكل 6-15، طبقة البروتوكول الأعلى هي TCP، لذا فإن بيانات الطبقة الأعلى التي تحملها رزمة IPv6 تتكون من ترويسة TCP تليها كتلة بيانات التطبيق.

الشكل 6-15: رزمة IPv6 مع ترويسات ملحقة (تحتوي على قطعة TCP).

تحمل ترويسة خيارات القفزة - بقفزة معلومات اختيارية والتي، إن وُجدت، فإنه ينبغي فحصها بكل موجّه على المسار. تتألف الترويسة من الحقول الآتية:

- الترويسة التالية (Next Header) (8 بتات): يعرِّف نوع الترويسة التي تلي هذه الترويسة مباشرةً
- طول امتداد الترويسة (Header Extension Length) (8 بتات): طول هذه الترويسة بوحدات طولها 64 بتاً، ولا يشمل ذلك أول 64 بت.
- الخيارات (Options): تتضمّن خياراً واحداً أو أكثر. يحتوي كل خيار على ثلاثة حقول فرعية هي: مؤشر لبيان نوع الخيار، والطول، والقيمة.

تم حتى الآن تعريف خيار واحد هو خيار الحمولة الفائقة (Jumbo Payload Option) والذي يُستخدم لإرسال رزم IPv6 بحمولات تزيد على 2^{16}-1 65535 =بايتاً. حقل خيار البيانات لهذا الخيار طوله 32 بتاً ويعطي طول الرزمة بالبايت باستثناء ترويسة IPv6.

لمثل تلك الرزم، ينبغي أن يكون حقل طول الحمولة في ترويسة IPv6 صفراً، ويجب أن لا يكون هناك ترويسة تجزيء. مع هذا الخيار، يستطيع IPv6 دعم رزم يصل طولها إلى أكثر من 4 بلايين بايت، مما يسهل نقل رزم الفيديو الكبيرة ويمكّن IPv6 من تحقيق الاستفادة القصوى من سعات الإرسال المتاحة على أي وسائط إرسال.

تتضمّن ترويسة التوجيه قائمة العُقَد الوسيطة (عقدة واحدة أو أكثر) والتي ينبغي أن تُزار خلال المسار إلى وِجهة الرزمة. تبدأ جميع ترويسات التوجيه بكتلة طولها 32 بتاً تحتوي على أربعة حقول طول كلٍّ منها 8 بتات، ويتبع هذه الكتلة بيانات التوجيه المتعلقة بنوعٍ معينٍ من التوجيه. الحقول الأربعة بطول 8 بتات لكلٍّ منها هي: الترويسة التالية، وطول امتداد الترويسة بالإضافة إلى:

- نوع التوجيه (Routing Type): ويُعَرِّف نوعية معيّنة من ترويسات التوجيه. إذا لم يتعرف الموجّه على قيمة نوع التوجيه، فيتعيّن عليه إهمال الرزمة.
- قطع المسار المتبقية (Segments Left): عدد العقد الوسيطة المنصوص عليها صراحةً والتي يجب زيارتها قبل الوصول إلى الوِجهة النهائية.

بالإضافة إلى هذا التعريف العام لترويسة التوجيه، تعرّف مواصفات IPv6 ترويسة التوجيه من النوع الصفري (Type 0). عند استخدام ترويسة التوجيه من النوع الصفري فإن عقدة المصدر لا تضع عنوان الوِجهة النهائية في ترويسة IPv6. وبدلا من ذلك، يوضع هذا العنوان كآخر عنوان مسجل بترويسة التوجيه، أما ترويسة IPv6 فيكون عنوان الوِجهة بها هو أول موجّه مطلوب على المسار. ولا يتم فحص ترويسة التوجيه حتى تصل الرزمة إلى العقدة المعرّفة بترويسة IPv6، وعندها يتم تحديث محتويات ترويسة IPv6 وترويسة التوجيه ثم تمرّر الرزمة. وتشمل عملية التحديث وضع العنوان التالي الذي سوف تتم زيارته في ترويسة IPv6 وإنقاص حقل "قطع المسار المتبقية" في ترويسة التوجيه.

يتطلب بروتوكول IPv6 أن تقوم عقدة IPv6 بعكس المسارات المبينة في رزمة تحتوي على ترويسة توجيه، كي تعيد الرزمة إلى المُرسِل.

تستخدم عقدة المصدر ترويسة التجزيء (Fragment Header) عند الحاجة إلى التجزيء. وفقاً لـ IPv6، يُسمَح للعقد المصدرية فقط القيام بعملية التجزيء، ولا يجوز ذلك للموجّهات الواقعة على مسار انتقال الرزمة. ولتحقيق الاستفادة القصوى من بيئة تربيط الشبكات، لا بد للعقدة من استخدام خوارزمية لاكتشاف المسار (path discovery algorithm) لتحديد أصغر قيمة لوحدات الإرسال القصوى (MTU) التي تدعمها الشبكات الفرعية على المسار. بعبارة أخرى، تحدّد خوارزمية اكتشاف المسار قيمة (MTU) للشبكة الفرعية على المسار والتي تمثل عنق الزجاجة. بناءً على ذلك،تقوم عقدة المصدر بعملية

التجزيء حسب المطلوب لكلَ من عناوين الوِجهة، وإلا فإنه سيتعيّن على المصدر تحديد حجم كل الرزم بـ 1280 بايتاً، وهو الحد الأدنى لوحدة الإرسال القصوى (MTU) التي يجب أن تدعمها أي شبكة فرعية.

بالإضافة إلى حقل الترويسة التالية، تتضمّن ترويسة التجزيء الحقول الآتية:

- قيمة الإزاحة لهذا الجزء (Fragment Offset) (13 بتاً): يحدّد موضع هذا الجزء في الرزمة الأصلية، ويُقاس بوحدات طول كلٍّ منها 64 بتاً. وهذا يعني أن أي جزء من أجزاء الرزمة – عدا الجزء الأخير – لابد أن يكون طول حقل بياناته من مضاعفات 64 بتاً.
- محجوز (Res) (بتان) مخصّص للاستخدام في المستقبل.
- علامة المزيد (More (M) Flag) (بت واحد): 1= مزيد من الأجزاء (Fragments)، 0 = الجزء الأخير.
- المعرِّف (Identification) (32 بتاً): للتعريف الحصري بالرزمة الأصلية. ويجب أن يكون المُعرِّف فريداً لعنوان مصدر الرزمة وعنوان وِجهة الرزمة طوال فترة تواجد الرزمة بالإنترنت. يتم تجميع كل الأجزاء التي تحمل نفس المُعَرِّف ونفس عنوان المصدر ونفس عنوان الوِجهة لإعادة تكوين الرزمة الأصلية.

تحمل ترويسة خيارات الوِجهة (Destinations Options Header) معلومات اختيارية، في حال وجودها يتم فحصها من قِبَل عقدة وِجهة الرزمة فقط. صيغة هذه الترويسة هي نفس صيغة ترويسة خيارات القفزة – بقفزة.