حماية الشبكة الافتراضية (vpn)

مفهوم IPSec Protocol:

الIPSec هو طريقه وليس بروتوكول حيث يوجد لIPSec بروتوكولان رئيسيان هما :

أولا: AH : Authentication Header

يستخدم الAH في توقيع الرسائل والبيانات Sign ولا يعمل على تشفيرها Encryption ، حيث يحافظ فقط على ما يلي للمستخدم :

1. موثوقية البيانات Data authenticity :اي ان البيانات المرسله من هذا المستخدم هي منه وليست مزوره او مدسوسه على الشبكه .

2. صحة البيانات Integrity Data : اي ان البيانات المرسله لم يتم تعديلها على الطريق (اثناء مرورها على الاسلاك) .

3. عدم اعادة الارسال Anti-Replay : وهذه الطريقه التي استخدمها المخترقون حيث يقومون بسرقة الباسوورد وهي مشفره ويقومون باعادة ارسالها في وقت اخر للسيرفر وهي مشفره وطبعا يفك السيرفر التشفير ويدخل المستخدم على اساس انه شخص اخر،، فالIPSec يقدم حلولا لمنع هذه العمليه من الحدوث.

ثانيا: ESP : Encapsulating Security Payload

يوفر هذا البروتوكول التشفير والتوقيع للبيانات معا Encryption and Signing ، ومن البديهي اذا ان يستخدم هذا البروتوكول في كون المعلومات سريه Confidential او Secret ،، او عند ارسال المعلومات عن طريق Public Network مثل الانترنت ،

يوفر الESP المزايا التاليه:

1. Source authentication : وهي مصداقية المرسل .
2. التشفير للبيانات Data Encryption : حبث يوفر التشفير للبيانات لحمايتها من التعديل او التغيير او القراءه .

3. Anti-Replay : عدم إعادة الإرسال.

ثالثا : Exchange IKE : Internet Key

الوظيفة الاساسيه لهذا البروتوكول هي ضمان الكيفيه وعملية توزيع ومشاركة المفاتيح Keys بين مستخدمي الIPSec ، فهو بروتوكول الnegotiation اي النقاش في نظام الIPSec كما انه يعمل على تاكيد طريقة

الموثوقيه Authentication والمفاتيح الواجب استخدامها ونوعها (حيث ان الIPSec يستخدم التشفير DES3 وهو عباره عن زوج من المفاتيح ذاتها يتولد عشوائيا بطرق حسابيه معقده ويتم اعطاءه فقط للجهة الثانيه ويمنع توزيعه وهو من نوع Symmetric Encryption اي التشفير المتوازي ويستخدم تقنية الPrivate Key .

طرق الIPSec التي تستخدمها في الشبكه (IPSec modes).

ينقسم الIPSec الى نظامين او نوعين وهما :

1. نظام النقل Mode Transport

2. نظام النفق Tunnel Mode .

اولا : Transport Mode

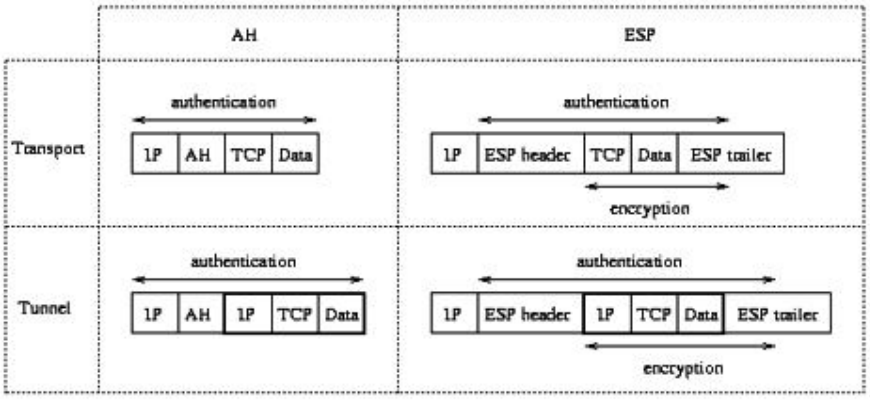
يستخدم هذا النظام عادة داخل الشبكه المحليه LAN : Local Area Network حيث يقدم خدمات التشفير للبيانات التي تتطابق والسياسه المتبعه في الIPSec بين اي جهازين في الشبكه اي يوفر Endpoint-to-Endpoint Encryption فمثلا اذا قمت بضبط سياسة الIPSec على تشفير جميع الحركه التي تتم على بورت 23 وهو بورت الTelnet (حيث ان الTelnet ترسل كل شيء مثلما هو دون تشفير Text Plain) فاذا تمت محادثه بين السيرفر والمستخدم على هذا البورت فان الIPSec يقوم بتشفير كل البيانات المرسله من لحظة خروجها من جهاز المستخدم الى لحظة وصولها الى السيرفر.

يتم تطبيق هذا النظام Transport Mode في الحالة التاليه وهي:
المحادثه التى تتم بين الاجهزه في داخل او نفس الشبكه الداخليه الخاصه Private LAN .

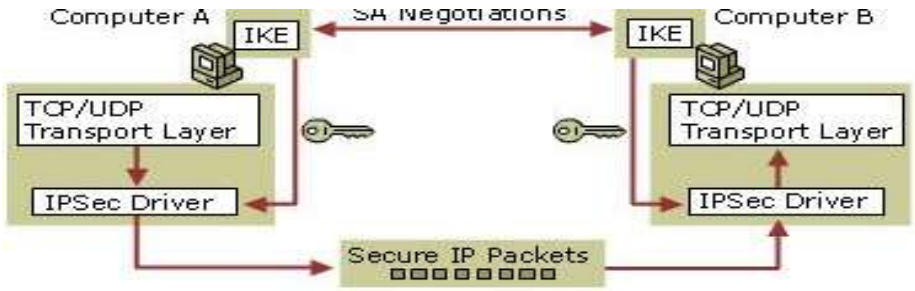
ثانيا: Tunnel Mode

يتم استخدام هذا النظام لتطبيق الIPSec بين نقطتين تكون بالعاده بين راوترين 2 Routers ، اذا يتم استخدام هذا النظام بين نقطتين بعيدتين جغرافيا اي سيتم قطع الانترنت في طريقها الى الطرف الثاني ، مثل الاتصالات التي تحدث بين الشبكات المتباعده جغرافيا WAN : Wide Area Network ، يستخدم هذا النظام فقط عند الحاجة لتأمين البيانات فقط اثناء مرورها من مناطق غير امنه كالانترنت ، فمثلا اذا أراد فرعين لشركه ان يقوم بتشفير جميع البيانات التي يتم ارسالها فيما بينهم على بروتوكول FTP: File Transfere Protocol فيتم اعداد الIPSec على اساس الTunneling Mode .

مخطط لكل من الPackets في الESP AH في كلتا النظامين Tunnel and Transport Modes .



طريقة حماية الشبكة الافتراضية عن طريق IPsec



يعمل الIPSec على الشبكه بسبع خطوات رئيسيه :
سيتم شرح طريقة حماية الشبكة الافتراضية عن طريق IPsec من خلال الصورة السابقة :

1. يقوم الجهاز A بارسال حزم بيانات عن طريق الكوابل على الشبكه الى الجهاز B .

2. يقوم IPSec Driver على الجهاز A بتحديد ان البيانات يجب ان تكون امنه عند انتقالها من كمبيوتر A الى B .

3. تتم عملية المباحثات بين الجهازين Negotiations فيتباحثان ويتفقان على استخدام المفتاح المشترك بينهما Shared Key وعلى المفتاح السري الخاص بالتشفير Secret Key ، وكله عن طريق بروتوكول IKE - Internet Key Exchange . مع الملاحظه بان المفتاح المشترك Shared Key يكون معلوما من قبل الطرفين دون انتقاله على الشبكه.

4. يقوم الIKE بعمل نوعين من الاتفاقيات بين الجهازين Two types of Agreements ، تسمى Security Associations SA او روابط الامن ، بين الجهازين. النوع الاول يحدد كيفية وثوق كلا الجهازين ببعضهما البعض وكيفية تأمين وحماية حزم البيانات الصادره عنهما، والنوع الثاني يحدد كيفية حماية جزء ونوع محدد من

اتصال التطبيق (البرنامج) .
5. بعد اكتمال وانتهاء عملية المباحثه بواسطه IKE ، يتم تمرير مفتاح التشفير من الجهاز A الى IPSec Driver ثم يعمل هذا المحرك IPSec Driver على عمل هاش Hashes من حزم البيانات الصادره للحفاظ على مصداقية المعلومه Data Integrity ، وممكن أن يقوم بتشفير حزم البيانات للحفاظ على سرية المعلومات Data confidentiality .

6. جميع معدات الشبكه الاخرى مثل الراوترات والسيرفرات لا تحتاج لتطبيق الIPSec عليها، حيث تتعامل مع حزم الIPSec على انها حزم عاديه وتقوم بتمريرها على الشبكه.
7. يقوم الIPSec Driver الخاص بالجهاز B بفحص حزم البيانات للتأكد من مصداقيتها Integrity وممكن ان يقوم بفك تشفير محتوياتها ، ومن ثم يعمل على ارسال البيانات الى البرنامج او التطبيق المستقبل لها.