LA SÉCURITÉ RÉSEAU AVEC IPSEC

(NETWORK SECURITY WITH IPSEC)

Ghislaine LABOURET

Hervé Schauer Consultants (HSC)
142, rue de Rivoli
75001 Paris
FRANCE

http://www.hsc.fr/

Résumé

IPsec est une norme qui définit une extension de sécurité pour le protocole Internet (IP) afin de permettre la sécurisation des réseaux basés sur ce protocole. Les services de sécurité fournis sont la confidentialité, l'authentification et l'intégrité des données, la protection contre le rejeu et le contrôle d'accès. Ces services sont basés sur des mécanismes cryptographiques qui leur confèrent un niveau de sécurité élevé lorsqu'ils sont utilisés avec des algorithmes forts. La sécurisation se faisant au niveau d'IP, IPsec peut être mis en œuvre sur tous les équipements du réseau et fournir un moyen de protection unique pour tous les échanges de données. De nombreux fournisseurs intègrent désormais IPsec dans leurs produits, ce qui facilite son déploiement à l'échelle d'un réseau d'entreprise. Des exemples d'utilisations typiques d'IPsec sont la création de réseaux privés virtuels, la sécurisation des accès distants à un intranet et la protection d'un serveur sensible.

Abstract

IPsec is a standard that defines an extension for the Internet protocol (IP) so as to secure the networks based on this protocol. The security services provided by IPsec are confidentiality, data origin authentication, data integrity, protection against replay and access control. These services are based on cryptographic mechanisms that give them a high security level when they are used with strong algorithms. As protection is applied at the IP layer, IPsec can be implemented on all the hardware that use the network and provide a single means of protection for all the data exchanges. Many providers now include IPsec in their products, which makes its deployment on a corporate network scale easier. Typical uses of IPsec are the creation of virtual private networks, the protection of remote access to an intranet and the protection of a sensitive server.

Version du 20 avril 1999

Table des matières

Introduction

Au cours de ces dernières années, l'utilisation du protocole Internet (*Internet Protocol, IP*) comme base des réseaux informatiques est devenue très importante, que ce soit par l'utilisation croissante de l'Internet ou dans le cadre de réseaux d'entreprises de type intranet. Si la flexibilité d'IP et sa simplicité ont su répondre aux besoins en matière de réseaux informatiques de ces dernières décennies, le but de ce protocole n'a jamais été d'assurer des communications sécurisées, d'où l'absence de fonctionnalités dans ce domaine. La facilité des attaques, le fait que la démocratisation de l'Internet les rende accessibles à beaucoup et la volonté croissante de pouvoir utiliser des réseaux IP pour des applications sensibles ont donc poussé au développement de diverses solutions de sécurité : gardes-barrières, routeurs filtrants, protocoles et applications sécurisées se sont multipliés. Devant les besoins grandissants dans ce domaine, et profitant de la définition du nouveau protocole IPv6, l'IAB (*Internet Architecture Board*) a donc décidé d'intégrer des services de sécurité dans le protocole IP lui-même, afin de pouvoir protéger les communications utilisant ce protocole. Le réseau IPv4 étant largement déployé et la migration complète vers IPv6 nécessitant encore beaucoup de temps, il est vite apparu intéressant de définir des mécanismes de sécurité qui soient communs à la fois à IPv4 et IPv6. Ces mécanismes sont couramment désignés par le terme IPsec pour *IP Security Protocol*.

IPsec se présente sous la forme d'une norme, développée par un groupe de travail du même nom à l'IETF (*Internet Engineering Task Force*) depuis 1992. Une première version basique de cette extension d'IP a paru, sous forme de RFC (*Request For Comment*), en 1995. Une seconde version, comportant en plus un système de gestion dynamique des paramètres de sécurité, a été publiée en novembre 1998. La maturité grandissante de la norme conduit désormais de nombreux fournisseurs à intégrer IPsec dans leurs produits, et l'on peut considérer que le marché commence à prendre de l'importance et sera bientôt un secteur incontournable de la sécurité réseau.

Cette présentation débutera par une description des composants d'IPsec, des principes sur lesquels repose la sécurisation et du fonctionnement du système. Dans un second temps, nous verrons dans quelles situations IPsec peut être utilisé et, en particulier, comment il peut être déployé et exploité, en pratique, à l'échelle d'un réseau d'entreprise.

1. Principe de fonctionnement

Cette partie présente les principales caractéristiques d'IPsec et notamment son principe de fonctionnement et les services de sécurité qu'il fournit.

1.1. La sécurisation des données échangées

La base d'IPsec est un ensemble de mécanismes de sécurisation des données circulant sur le réseau. Nous allons voir ici où interviennent ces mécanismes et quelle sécurité ils apportent.

Où intervient IPsec ?

IPsec s'insère, dans la pile de protocoles TCP/IP, au niveau d'IP. Cela signifie qu'il agit sur chaque paquet IP reçu ou émis et peut soit le laisser passer sans traitement particulier, soit le rejeter, soit lui appliquer un mécanisme de sécurisation.

Toutes les implémentations d'une pile de protocoles TCP/IP conformes à la version six d'IP doivent intégrer IPsec. En revanche, IPsec est optionnel pour la version actuelle d'IP, IPv4, et n'est pas encore fourni en standard sur la plupart des systèmes courants. Lorsque se sera le cas ou lorsque IPv6 sera en place, il sera possible à tout utilisateur désirant des fonctions de sécurité d'avoir recours à IPsec ; en attendant, il convient, pour utiliser IPsec, d'**acquérir un produit mettant en œuvre cette norme**.

Le placement d'IPsec au niveau IP, c'est-à-dire au niveau réseau, présente l'avantage de le rendre exploitable par les niveaux supérieurs, et, en particulier, d'offrir un moyen de **protection unique pour toutes les applications**. En d'autres termes, là où d'autres systèmes sécurisent les applications au cas par cas, IPsec, lui, sécurise le réseau sous-jacent. Cette approche n'est bien sûr pas exempte de contraintes, notamment des problèmes de performances et la difficulté de pouvoir distinguer les différents flux avec précision.

Du fait de son intégration dans la pile de protocoles, **IPsec peut être mis en œuvre sur tous les équipements utilisant le réseau** et assurer une protection soit **de bout en bout,** entre les tiers communicants, soit **lien par lien**, sur des segments de réseau. IPsec peut donc être utilisé dans de nombreuses situations : il peut offrir une protection aux applications qui utilisent le réseau, protéger l'accès d'un réseau en agissant comme un garde-barrière évolué, servir à mettre en place des réseaux privés virtuels, sécuriser les accès distants à un intranet...

Quels services de sécurité sont fournis ?

IPsec vise à prévenir les diverses attaques rendues possibles par le protocole IP, notamment empêcher un adversaire d'espionner les données circulant sur le réseau ou de se faire passer pour autrui afin d'accéder à des ressources ou données protégées.

Dans ce but, IPsec peut fournir, suivant les options sélectionnées, tout ou partie des services de sécurité suivants :

- **Confidentialité** des données et protection partielle contre l'analyse du trafic.

  Les données transportées ne peuvent être lues par un adversaire espionnant les communications. En particulier, aucun mot de passe, aucune information confidentielle ne circule en clair sur le réseau. Il est même possible, dans certains cas, de chiffrer les en-têtes des paquets IP et ainsi masquer, par exemple, les adresses source et destination réelles. On parle alors de protection contre l'analyse du trafic.

- **Authenticité** des données et **contrôle d'accès continu**.

  L'authenticité est composée de deux services, généralement fournis conjointement par un même mécanisme : l'authentification de l'origine des données et l'intégrité. L'authentification de l'origine des données garantit que les données reçues proviennent de l'expéditeur déclaré. L'intégrité garantit qu'elles n'ont pas été modifiées durant leur transfert.

  La garantie de l'authenticité de chaque paquet reçu permet de mettre en œuvre un contrôle d'accès fort tout au long d'une communication, contrairement à un contrôle d'accès simple à l'ouverture de la connexion, qui n'empêche pas un adversaire de récupérer une communication à son compte. Ce service permet en particulier de protéger l'accès à des ressources ou données privées.

- Protection contre le **rejeu**

  La protection contre le rejeu permet de détecter une tentative d'attaque consistant à envoyer de nouveau un paquet valide intercepté précédemment sur le réseau.

Ces services sont basés sur des **mécanismes cryptographiques** modernes qui leur confèrent un **niveau de sécurité élevé** lorsqu'ils sont utilisés avec des algorithmes forts.

Comment sont fournis ces services ?

Les services de sécurité mentionnés ci-dessus sont fournis au moyen de **deux extensions du protocole IP** appelées AH (*Authentication Header*) et ESP (*Encapsulating Security Payload*) :

- **AH** est conçu pour assurer **l'authenticité** des datagrammes IP sans chiffrement des données (i.e. sans confidentialité).

  Le principe d'AH est d'adjoindre au datagramme IP classique un champ supplémentaire permettant à la réception de vérifier l'authenticité des données incluses dans le datagramme. Un numéro de séquence permet de détecter les tentatives de rejeu.

- **ESP** a pour rôle premier d'assurer la **confidentialité** mais peut aussi assurer l'**authenticité** des données.

  Le principe d'ESP est de générer, à partir d'un datagramme IP classique, un nouveau datagramme dans lequel les données et éventuellement l'en-tête original, sont chiffrés. ESP peut également assurer l'authenticité des données par ajout d'un bloc d'authentification et la protection contre le rejeu par le biais d'un numéro de séquence.

Ces deux extensions peuvent être utilisées séparément ou combinées pour obtenir les services de sécurité requis.

AH et ESP sont basés sur l'utilisation d'algorithmes cryptographiques et ne sont pas restreints à un algorithme particulier : ils sont **utilisables avec de nombreux algorithmes**. Chaque produit comportant IPsec sera donc livré avec un ensemble d'algorithmes, parmi lesquels l'utilisateur ou l'administrateur du réseau pourront choisir. Cette façon de procéder permet notamment, pour se conformer à des contraintes législatives par exemple, de limiter les algorithmes de chiffrement fournis à une longueur de clef donnée voire de fournir uniquement des algorithmes d'authentification, sans possibilité de chiffrement. IPsec comporte une liste d'algorithmes proposés pour être utilisés avec IPsec et dont l'utilisation est négociable en ligne par le biais d'un protocole appelé IKE. À l'heure où ce document est rédigé, cette liste contient notamment les algorithmes de chiffrement NULL (pas de chiffrement), CAST-128 (clef de 40 à 128 bits), Blowfish (40-448 bits), RC5 (40-2040 bits), DES (56 bits) et DES triple (clef de 168 bits mais de force équivalente à 112 bits). Pour garantir l'interopérabilité entre les équipements, la norme IPsec rend certains de ces algorithmes obligatoires. Actuellement, DES-CBC et 3DES-CBC sont obligatoires pour le

chiffrement ; pour l'authentification, HMAC-MD5 et HMAC-SHA-1 doivent être présents dans toute implémentation conforme d'IPsec.

D'autre part, **deux modes** de protection existent :

- Le mode **transport** protège uniquement le contenu du paquet IP sans toucher à l'en-tête ; ce mode n'est utilisable que sur les équipements terminaux (postes clients, serveurs).
- Le mode **tunnel** permet la création de tunnels par "encapsulation" de chaque paquet IP dans un nouveau paquet. Ainsi, la protection porte sur tous les champs des paquets IP arrivant à l'entrée d'un tunnel, y compris sur les champs des en-têtes (adresses source et destination par exemple). Ce mode est celui utilisé par les équipements réseau (routeurs, gardes-barrières...).

1.2. La gestion des paramètres de sécurisation

Les mécanismes mentionnés ci-dessus font appel à la cryptographie et utilisent donc un certain nombre de paramètres (algorithmes utilisés, clefs, mécanismes sélectionnés...). Afin d'échanger des données de façon sécurisée, il est donc nécessaire, dans un premier temps, de se mettre d'accord sur les paramètres à utiliser, et notamment d'échanger des clefs de façon sûre.

L'approche la plus simple pour cet échange préalable est la **gestion manuelle**, qui consiste à laisser l'administrateur configurer manuellement chaque équipement utilisant IPsec avec les paramètres appropriés. Si cette approche s'avère relativement pratique dans un environnement statique et de petite taille, elle ne convient plus pour un réseau de taille importante. De plus, elle implique une définition totalement statique des paramètres et un non-renouvellement des clefs. La première version d'IPsec, parue en 1995, se basait sur cette méthode manuelle pour la configuration des équipements.

La seconde approche est la **gestion automatique** au moyen d'un protocole approprié. Les développements dans ce domaine ont abouti à un protocole de gestion des paramètres relatifs à IPsec connu sous le nom de **IKE** (*Internet Key Exchange*). Bien que ce nom insiste sur le rôle d'échange de clefs, IKE se charge en réalité de la gestion (négociation, mise à jour, suppression) de tous les paramètres relatifs à la sécurisation des échanges. Contrairement aux mécanismes AH et ESP qui agissent directement sur les données à sécuriser, IKE est un protocole de plus haut niveau, dont le rôle est l'ouverture et la gestion d'une pseudo-connexion au-dessus d'IP. En particulier, IKE inclut, au début de la négociation, une **authentification mutuelle des tiers communicants** qui peut se baser soit sur un **secret partagé préalable** soit sur des **clefs publiques**. L'échange des clefs publiques utilisées par IKE peut se faire soit manuellement, soit directement dans le cadre d'IKE par un échange de certificats en ligne, soit par le biais d'une infrastructure à clefs publiques (*Public Key Infrastructure, PKI*) extérieure.

Afin de stocker et de manipuler facilement l'ensemble des paramètres gérés par IKE et utilisés par les mécanismes de sécurisation, IPsec a recours à la notion d'association de sécurité (*Security Association, SA*). **Une association de sécurité est une structure de données qui regroupe l'ensemble des paramètres de sécurité associés à une communication donnée**. Pour stocker l'ensemble des associations de sécurité actives, on utilise une "base de données des associations de sécurité" (*Security Association Database, SAD*). Les éléments stockés dans cette base de données sont créés et modifiés par IKE puis consultés par la couche IPsec pour savoir comment traiter chaque paquet reçu ou à émettre.

1.3. La configuration

Les protections offertes par IPsec sont basées sur des choix définis par l'administrateur du réseau par le biais de **politiques de sécurité**. Ces politiques sont généralement stockées dans une "base de données de politique de sécurité" (*Security Policy Database, SPD*) et se présentent sous forme

d'une liste ordonnée de règles, chaque règle comportant un certain nombre de critères qui permettent de déterminer quelle partie du trafic est concernée. La consultation de la base de donnée des politiques de sécurité **permet de décider, pour chaque paquet, s'il se verra apporter des services de sécurité, sera autorisé à passer outre ou sera rejeté**. C'est également cette base qui **indique à IKE quelles associations de sécurité il doit négocier**, et, en particulier, quels tunnels sécurisés il doit établir.

Pour le moment, la configuration des équipements IPsec passe par la configuration manuelle des politiques de sécurité sur chaque équipement. Des systèmes de gestion centralisée et dynamique de ces politiques sont en cours d'élaboration.

1.4. Synthèse

Le schéma ci-dessous représente les différents composants d'IPsec et leurs interactions. On y retrouve notamment :

- AH et ESP, les **mécanismes de sécurisation** au niveau IP qui protègent les données transférées. Les paramètres relatifs à l'utilisation de ces mécanismes sont stockés dans des **associations de sécurité**.
- **IKE**, le protocole orienté connexion utilisé par les équipements IPsec pour gérer les associations de sécurité. Une configuration manuelle des associations de sécurité est également possible.
- Un ensemble de **politiques de sécurité**, qui sont les règles à appliquer au trafic traversant un équipement donné. C'est par elles que l'administrateur du réseau configure IPsec et notamment indique à IKE quels sont les tunnels sécurisés à créer.

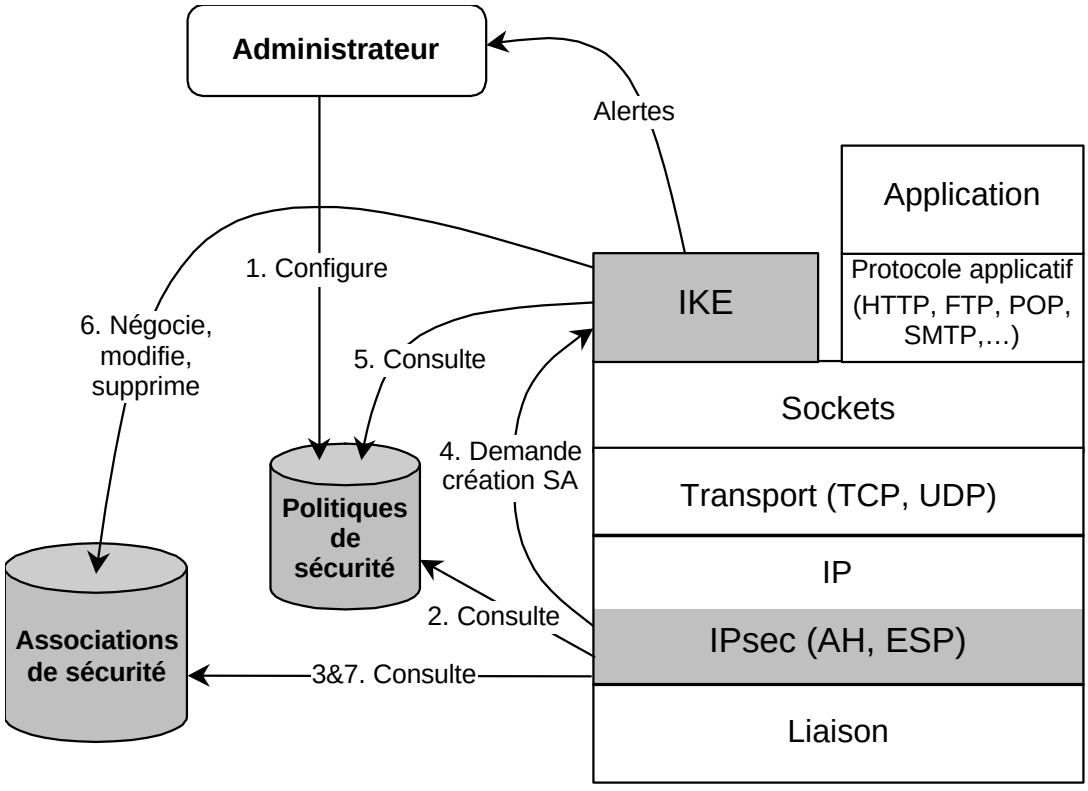

Figure 1. Composants d'IPsec et actions à l'émission de données

SA = *Security Association* = Association de sécurité

2. Déploiement et utilisations pratiques

Cette partie aborde les différents aspects du déploiement d'IPsec sur un réseau d'entreprise.

2.1. Où trouver IPsec

IPsec ne nécessite **aucune modification des applications utilisées**, il est totalement transparent. **La seule chose à acquérir est un système mettant en œuvre IPsec**, et éventuellement une infrastructure à clefs publiques si l'on désire y avoir recours pour faciliter un déploiement à grande échelle.

Pour utiliser IPsec, l'entreprise doit donc vérifier que ses systèmes (matériel ou logiciel) intègrent ces fonctions étendues. En effet, IPsec est avant tout une norme développée par l'IETF ; si son intégration obligatoire dans toute pile IPv6 signifie qu'il sera livré en standard avec des systèmes comportant IPv6, pour qu'il soit utilisable sur un système IPv4 donné, il faut qu'un fournisseur choisisse de l'implémenter dans son produit. Jusqu'à très récemment, l'absence de maturité de la norme avait pour conséquence un faible nombre d'implémentations. La parution d'une nouvelle version très complète en novembre 1998 et la mode grandissante des réseaux privés virtuels ont conduit, aux États-Unis, à une explosion du marché. La France réagit pour le moment de façon plus modérée, mais l'apparition de plusieurs produits français ou disponibles dans l'Hexagone indique que le marché français dans ce domaine est loin d'être inactif.

IPsec faisant partie intégrante de la pile de protocoles TCP/IP, il **peut être mis en œuvre sur tout équipement utilisant le réseau**. On distingue cependant deux types d'équipements différents : les passerelles de sécurité et les hôtes finaux.

Passerelles de sécurité

Une passerelle de sécurité est un équipement placé à la frontière entre deux réseaux ou deux sous-réseaux et qui met en œuvre des fonctions de sécurité. Ce terme englobe en particulier les produits **gardes-barrières**, les **routeurs** lorsqu'ils jouent un rôle dans la sécurité du réseau et les **boîtiers** dédiés pour la création de réseaux privés virtuels.

Comme exemple d'implémentations IPsec sur ces équipements, on peut citer le logiciel garde-barrière Firewall-1 de Check Point (à partir de la version 4.0), le système d'exploitation pour routeurs Cisco IOS (à partir de la version 11.3.(3)T), les modules KAME pour FreeBSD et FreeS/WAN pour Linux, l'implémentation native dans OpenBSD, l'implémentation dans AIX 4.3 de Bull SA...

Dans les routeurs, IPsec est principalement utilisé pour la création de réseaux privés virtuels. Intégré dans un garde-barrière, il représente une évolution par rapport aux simples filtres - IPsec permet des fonctionnalités supplémentaires et une amélioration de la sécurité - mais ne remplace pas nécessairement les relais applicatifs. Enfin, intégré dans des systèmes d'exploitation généralistes, il peut être exploité sur des machines tenant lieu de passerelle de sécurité comme de serveur.

Hôtes finaux

Les hôtes finaux sont des machines situées à l'extrémité d'une communication. Ce terme englobe en particulier les **serveurs** applicatifs ou de données et les **postes utilisateurs** (station de travail, ordinateur portable...).

Dans ces cas, les implémentations modifient ou s'interfacent avec la pile TCP/IP du système. Cela peut aller d'une implémentation native dans le système d'exploitation (comme pour OpenBSD) à un simple module à ajouter sur la machine (c'est le cas pour beaucoup d'implémentations clientes pour

Windows) en passant par une recompilation du noyau du système (KAME pour FreeBSD et FreeS/WAN pour Linux).

Une machine, qui possède un système d'exploitation comprenant IPsec ou un module IPsec s'interfaçant avec sa pile réseau, est alors en mesure d'utiliser ce protocole pour protéger ses échanges avec d'autres équipements "compatibles IPsec", que ce soient d'autres hôtes finaux ou des passerelles de sécurité. Lorsque IPsec est installé sur un serveur sensible, il peut être utilisé pour protéger l'accès à ce serveur. Installé sur une machine utilisateur, il permet d'accéder aux serveurs ou aux réseaux protégés par IPsec.

Fonctionnalités fournies et restrictions légales

Nous avons mentionné dans la première partie le fait que chaque produit comportant IPsec est livré avec un ensemble d'algorithmes, parmi lesquels l'utilisateur ou l'administrateur du réseau pourront choisir. Cette façon de procéder permet de se **conformer à des contraintes législatives** en fournissant des **versions ne comportant que certains algorithmes** ou ne rendant possible l'utilisation que de certaines longueurs de clef. En France, la réglementation sur les moyens et prestations de cryptologie contrôle les opérations de fourniture, d'importation, d'exportation et d'utilisation ; elle prévoit, suivant les cas, trois procédures : demande d'autorisation, déclaration préalable ou dispense de formalités. L'importation et l'utilisation de moyens de chiffrement utilisant des clefs d'une taille inférieure ou égale à 40 bits sont totalement libres, seule la fourniture requiert une déclaration préalable ; cette taille de clef est cependant largement insuffisante de nos jours. Entre 40 et 128 bits, l'importation et l'utilisation ont été libéralisées par un décret le 17 mars 1999, à condition pour les entreprises utilisatrices que le produit ait fait l'objet d'une déclaration préalable par son fournisseur ou par un importateur. Cela devrait conduire à l'apparition sur le marché français de produits qui, parce qu'ils ont fait l'objet d'une déclaration de la part de leur fournisseur, pourront être utilisés sans formalités par les entreprises. Dans le cas où le fournisseur n'aurait pas fait les démarches nécessaires auprès du SCSSI, l'entreprise qui désire néanmoins importer et/ou utiliser un tel produit peut le faire, moyennant une déclaration préalable de sa part. Au-delà de 128 bits, une demande d'autorisation est pour le moment toujours nécessaire.

D'une manière générale, il convient, lors de l'acquisition d'un produit IPsec, de vérifier la **liste des fonctionnalités fournies** par ce produit. En effet, de nombreux fournisseurs proposent différentes versions de leurs produits, avec différents niveaux de fonctionnalités. En particulier, on trouve encore beaucoup de produits qui ne comportent que du chiffrement faible (40 bits, DES simple), lequel est à proscrire dès que des données confidentielles sont à protéger. On notera cependant que l'utilisation d'IPsec pour de l'authentification seule apporte déjà un service de sécurité considérable. D'autre part, la gestion dynamique des clefs pour IPsec étant relativement récente, certains produits ne proposent qu'une gestion manuelle des clefs ou n'incluent pas la possibilité d'authentification mutuelle au moyen de clefs publiques mais seulement par secret partagé.

2.2. Déployer IPsec : planification, installation et configuration

Les étapes du déploiement

IPsec s'insérant au cœur même du réseau, son déploiement requiert avant tout une étape d'identification des besoins. Il convient tout d'abord d'établir le plan du réseau et d'**identifier les communications à sécuriser**. Dans ce but, l'établissement d'une cartographie des flux peut s'avérer nécessaire. Une fois les communications à sécuriser identifiées, il convient de choisir le type de sécurisation souhaitée : chiffrement et/ou authentification des données, mode d'authentification des tiers, niveau de granularité souhaité, algorithmes à utiliser...

Une fois ces choix globaux établis, on peut passer à une seconde phase qui consiste à identifier les équipements concernés par la mise en œuvre de la politique de sécurité retenue et à **calculer les règles à faire appliquer par chaque équipement**. C'est également à cette étape qu'interviendra éventuellement le choix et la mise en œuvre de l'infrastructure à clefs publiques à laquelle auront recours les équipements IPsec.

Il ne reste alors plus qu'à installer et configurer IPsec sur l'ensemble des équipements précédemment identifiés.

Installation d'IPsec sur une machine

L'installation d'IPsec sur un équipement donné varie en fonction de la façon dont se présente IPsec pour cet équipement : intégré dans le produit ou module à ajouter (avec ou sans recompilation du noyau).

Lorsque IPsec est intégré dans un produit, l'installation se résume souvent à une mise à jour du produit et ne nécessite pas de compétences supplémentaires.

Lorsque IPsec s'intègre dans un système d'exploitation, la mise à jour du système peut s'avérer délicate et nécessiter un arrêt prolongé de la machine concernée. Il sera donc préférable de tester l'installation sur une machine hors production au préalable. Les implémentations actuelles pour les systèmes Unix sont généralement très complètes en terme de fonctionnalités fournies mais peu conviviales. Elles nécessitent de bien connaître le système. À l'opposé, les modules à ajouter à un système propriétaire comme Windows ne fournissent, en général que des fonctionnalités réduites mais sont très simples à installer.

Configuration d'IPsec

L'interface et la méthode de configuration d'IPsec **varient fortement d'un produit à l'autre** ; en particulier, tous les fournisseurs ne font pas de distinction claire entre les politiques de sécurité et les associations de sécurité telles qu'elles ont été présentées dans la partie 1, ce qui peut prêter à confusion. Pour chaque équipement, il faut donc consulter la documentation et apprendre les commandes correspondantes. L'utilisateur est généralement aidé par le fait que de nombreux paramètres sont positionnés par défaut sur des valeurs classiques.

Un point important à retenir est que, **pour que deux équipements puissent s'entendre, ils doivent être configurés avec des paramètres similaires** ; cela nécessite une concertation dans le cas où les deux équipements à faire dialoguer ne seraient pas sous la responsabilité de la même personne.

Il n'existe **pas encore de produit de configuration globale**, même si des initiatives commencent à apparaître du côté des fournisseurs et si des réflexions en ce sens ont débuté dans le groupe de travail IPsec.

2.3. Exemples de déploiements : réseaux privés virtuels, extranet, serveurs protégés...

Ce paragraphe présente trois exemples typiques d'utilisation d'IPsec dans un réseau d'entreprise. Il va de soi que, dans la pratique, ces trois cas peuvent être combinés et déclinés en de nombreuses variantes.

Exemple 1 : réseaux privés virtuels

Une première utilisation possible d'IPsec est la création de réseaux privés virtuels entre différents réseaux privés séparés par un réseau non fiable comme l'Internet. Les matériels impliqués sont les passerelles de sécurités en entrée/sortie des différents réseaux (routeurs, gardes-barrières, boîtiers

dédiés). Cette configuration nécessite donc l'installation et la configuration d'IPsec sur chacun de ces équipements afin de **protéger les échanges de données entre les différents sites**.

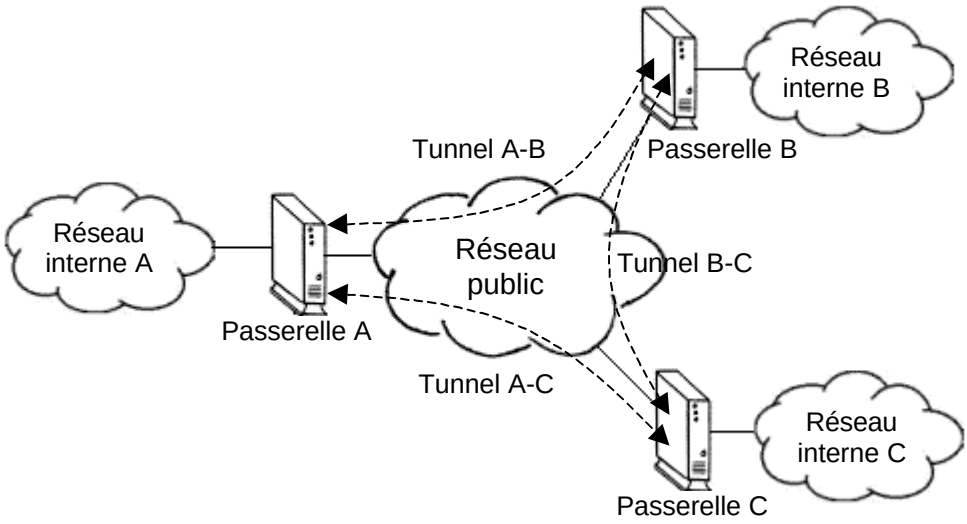

Figure 2. Réseaux privés virtuels

Cet usage d'IPsec présente un certain nombre de limites :

- Si beaucoup de communications doivent être chiffrées, des problèmes de performances peuvent apparaître.
- La configuration des équipements IPsec se faisant souvent manuellement et statiquement, l'utilisation d'une telle configuration avec un nombre élevé de sites et de tunnels est pour le moment difficile.
- La protection intervient seulement sur la traversée du réseau public, il n'y a pas de protection de bout en bout des communications.

Exemple 2 : extranet

Dans l'exemple précédent, on désirait permettre des communications sûres entre différents sites fixes. Un autre cas est celui où les communications à sécuriser ne sont pas fixes mais au contraire intermittentes et d'origines variables. C'est le cas, par exemple, lorsqu'on désire **permettre à des employés ou à des partenaires situés à l'extérieur de l'entreprise d'accéder au réseau interne sans diminuer le niveau de sécurité** (donc en mettant en œuvre une confidentialité et un contrôle d'accès forts). Les matériels impliqués sont les portes d'entrées du réseau (serveur d'accès distants, liaison Internet...) et les machines utilisées par les employés (ordinateur portable, ordinateur personnel au domicile...).

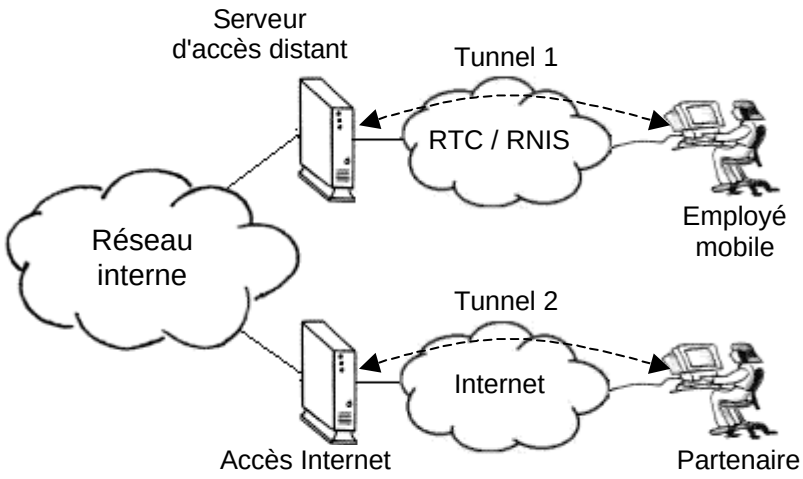

Figure 3. Extranet

Cette configuration nécessite l'installation d'IPsec sur les postes de tous les utilisateurs concernés et la gestion d'une éventuelle base de données adaptée pour stocker les profils individuels. En contrepartie, elle représente un gros apport pratique pour les employés qui se déplacent beaucoup, sans diminution de la sécurité du réseau.

Exemple 3 : protection d'un serveur sensible

Dans les deux exemples précédents, l'approche choisie était orientée vers la protection du réseau de l'entreprise dans son ensemble. On peut également vouloir utiliser IPsec pour protéger l'accès à une machine donnée. Par exemple, si un serveur contient des **données sensibles que seul un nombre réduit de personnes (internes ou externes à l'entreprise) doit pouvoir consulter**, IPsec permet de mettre en œuvre un **contrôle d'accès** fort et un **chiffrement des données** pendant leur transfert sur le réseau. Les matériels impliqués dans ce type de configuration sont le serveur sensible et les machines de toutes les personnes devant accéder aux données.

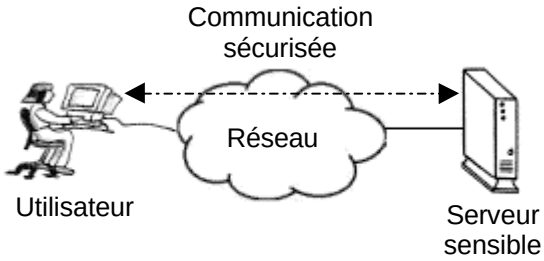

Figure 4. Serveur sensible

IPsec rend la sécurisation possible quelles que soient les applications utilisées pour accéder au serveur.

Conclusion

IPsec est un système très complet qui peut répondre à beaucoup de besoins en matière de sécurité et s'adapter à de nombreuses situations. Sa conception en fait un système très sûr et sa nature de norme garantit l'interopérabilité entre les équipements de différents fournisseurs. Ces avantages, couplés à la prédominance grandissante du protocole IP, vont certainement faire d'IPsec un acteur important de la sécurité des réseaux informatiques. Il lui manque encore, pour être utilisé à grande échelle, un peu de maturité et surtout un système de gestion centralisée et dynamique des politiques de sécurité. Les avancées actuelles dans ce domaine laissent à penser qu'il ne s'agit que d'une question de temps avant qu'un tel système ne voie le jour. L'apparition d'infrastructures à clefs publiques fonctionnelles et reconnues est également indispensable pour une utilisation pratique et répandue d'IPsec.