CHAPITRE 5 : Protocoles sécurisés

La plupart des protocoles de la pile TCP/IP ne sont pas sécurisés : c'est-à-dire que les données transitent en clair sur le réseau. Ainsi, des protocoles de plus haut niveau, dits ‘protocoles sécurisés’ ont été mis au point afin d’encapsuler les messages dans les paquets de données chiffrées.

5.1 Protocole SSL (Secure Socket Layer):
C’est un protocole destine à assurer la sécurisation des échanges de données sur Internet. Il est indépendant du protocole de niveau applicatif. Ce qui signifie qu’il permet de chiffrer et d’authentifier différents types de protocoles. Le plus connu d’entre eux est évidemment http qui devient HTTPS une fois sécurisé par SSL.

5.1.2 Les fonctions de SSL :
- La confidentialité des données échangées en chiffrant la communication.
- L’authentification du serveur avec la présentation de son certificat signé par une autorité de certification.
- L’intégrité des données.
- Optionnellement, l’authentification du client par certificat.

5.1.3 Fonctionnement de SSL :
SSL repose sur une infrastructure à clé publique et se base sur la gestion de certificats et la reconnaissance d’autorité de certification.
La mise en œuvre du protocole SSL débute par une phase de négociation pendant laquelle les parties se présentent (présentent leur certificat respectif ou au moins le certificat du serveur et éventuellement celui du client également). Puis intervient la négociation des protocoles de chiffrement et d’authentification à mettre en place. Enfin, la génération des clés de sessions est assurée de manière à chiffrer les échanges à venir.
Une URL correspondant à un site sécurisé par SSL se préfixe avec https://... Cette session sécurisée se reconnait dans la majorité des navigateurs à la présence d’un petit cadenas.

5.1.4 Surveillez les alertes SSL :
Un serveur HTTPS correctement configuré et disposant d’un certificat valide ne devrait pas normalement pas présenter d’avertissement SSL. S’il le fait c’est sans doute qu’il y a un problème quelconque.
Il existe en fait trois raisons différentes possibles à l’émission d’une alerte SLL :
- L’autorité de certification qui a signé le certificat n’est pas reconnue par le client comme étant une autorité de certification valide.
- On ne se situe pas dans la période de validité du certificat présenté.
- Le nom auquel a été attribué le certificat ne correspond pas au nom que nous avons écrit dans l’URL du serveur.

Éviter ces pièges courants : en procédant à la sécurisation de votre site à l'aide du protocole TLS, évitez les erreurs suivantes :

Problème	Action
Certificats expirés	Assurez-vous que votre certificat est toujours à jour.
Certificat enregistré pour un nom de site incorrect	Vérifiez que vous avez obtenu un certificat pour tous les noms d'hôte utilisés par votre site. Par exemple, si votre certificat ne couvre que www.example.com, un visiteur qui accède à votre site en utilisant seulement example.com (sans le préfixe "www.") sera bloqué par une erreur de correspondance de nom de certificat.
Non-compatibilité avec l'Indication du nom du serveur (Server name indication, SNI)	Assurez-vous que votre serveur Web accepte la SNI et que votre audience utilise des navigateurs compatibles de manière générale. SNI est supportée par tous les navigateurs modernes. Cependant, vous aurez besoin d'une adresse IP dédiée si vous devez accepter des navigateurs plus anciens.
Problèmes d'indexation	Autorisez autant que possible l'indexation de vos pages par les moteurs de recherche.
Anciennes versions du protocole	Les anciennes versions du protocole sont vulnérables. Assurez-vous que vous utilisez les versions les plus récentes des bibliothèques TLS, et mettez en œuvre les dernières versions du protocole.
Éléments de sécurité mélangés	Intégrez uniquement du contenu HTTPS sur les pages HTTPS.
Contenu différent sur le HTTP et le HTTPS	Assurez-vous que le contenu de vos sites HTTP et HTTPS est le même.
Erreurs de code d'état HTTP sur le HTTPS	Vérifiez que votre site renvoie le bon code d'état HTTP. Par exemple, 200 (OK) pour les pages accessibles, ou 404 ou 410 pour les pages qui n'existent pas.

5.1.5 configurer un Service HTTPS dans IIS :

5.1.5.1 Configuration de votre serveur Web pour SSL :

Pour activer SSL dans IIS, il faut d'abord obtenir un certificat qui est utilisé pour chiffrer et déchiffrer les informations qui sont transférées sur le réseau. IIS inclut son propre outil de demande de certificat que vous pouvez utiliser pour envoyer une demande de certificat à une autorité de certification. Si vous utilisez Apache, vous devez obtenir le certificat manuellement. Dans les services IIS et Apache, vous recevez un fichier de certificat de l'autorité de certification, vous devez configurer sur l'ordinateur. Apache lit le certificat à partir de son fichier source à l'aide de la directive SSLCACertificateFile. Toutefois, dans IIS, vous pouvez configurer et gérer des certificats à l'aide de l'onglet Sécurité du répertoire du site Web ou des propriétés de dossier.

5.1.5.2 Configurer le dossier ou le Site Web pour utiliser SSL/HTTPS

Cette procédure suppose que votre site dispose déjà d'un certificat qui lui est assigné.

1. Ouvrez une session sur l'ordinateur serveur Web en tant qu'administrateur.
2. Cliquez sur Démarrer, pointez sur Paramètres, puis cliquez sur Panneau de configuration.
3. Double-cliquez sur Outils d'administration, puis double-cliquez sur Gestionnaire des Services Internet.
4. Dans la liste des différents sites servis dans le volet gauche, sélectionnez le site Web.
5. Cliquez droit sur le site Web, le dossier ou le fichier pour lequel vous souhaitez configurer des communications SSL, puis cliquez sur Propriétés.
6. Cliquez sur l'onglet Sécurité de répertoire .

7. Cliquez sur Modifier.
8. Si vous souhaitez que le site Web, le dossier ou le fichier exige des communications SSL, cliquez sur exiger canal sécurisé (SSL) .
9. Cliquez sur cryptage requièrent de 128 bits pour configurer 128-bit (40 bits) prise en charge du cryptage.
10. Pour permettre aux utilisateurs de se connecter sans fournir leurs propres certificats, cliquez sur Ignorer les certificats clients. Vous pouvez également, pour permettre à un utilisateur de fournir son propre certificat, utiliser accepter les certificats clients.
11. Pour configurer le mappage client, cliquez sur Activer le mappage de certificat client, puis cliquez sur Modifier pour mapper des certificats clients à des utilisateurs. Si vous configurez cette fonctionnalité, vous pouvez mapper des certificats clients à des utilisateurs individuels dans Active Directory. Vous pouvez utiliser cette fonctionnalité pour identifier automatiquement un utilisateur en fonction du certificat qu'ils fournis lorsqu'ils accèdent au site Web. Vous pouvez mapper les utilisateurs aux certificats sur une base individuelle (un certificat qui identifie un utilisateur) ou vous pouvez mapper de nombreux certificats à un seul utilisateur (une liste de certificats est mis en correspondance avec un utilisateur spécifique en fonction de règles spécifiques. La première correspondance valide devient la mise en correspondance).
12. Cliquez sur OK.

Appliquer les connexions SSL

Maintenant que le certificat de serveur est installé, vous pouvez appliquer les communications par canal sécurisé SSL avec les clients du serveur web. Tout d'abord, vous devez activer le port 443 pour établir des communications sécurisées avec le site web. Pour cela, procédez comme suit :

1. Dans la console de gestion de l'ordinateur, cliquez avec le bouton droit sur le site web sur lequel vous souhaitez appliquer le protocole SSL, puis cliquez sur Propriétés.
2. Cliquez sur l'onglet Site web. Dans la section Identification du site Web, vérifiez que le champ Port SSL contient la valeur numérique 443.
3. Cliquez sur Options avancées. Vous devriez voir deux champs. L'adresse IP et le port du site Web doivent déjà figurer dans le champ Identités multiples pour ce site Web. Sous le champ Identités SSL multiples pour ce site Web, cliquez sur Ajouter si le port 443 n'est pas déjà répertorié. Sélectionnez l'adresse IP du serveur et tapez la valeur numérique 443 dans le champ Port SSL. Cliquez sur OK.

Maintenant que le port 443 est activé, vous pouvez appliquer les connexions SSL. Pour cela, procédez comme suit :

1. Cliquez sur l'onglet Sécurité de répertoire. Dans la section Communications sécurisées, notez que Modifier est maintenant disponible. Cliquez sur Modifier.
2. Sélectionnez Requérir un canal sécurisé (SSL).REMARQUE : Si vous spécifiez un cryptage 128 bits, les clients qui utilisent un navigateur avec une puissance de 40 ou

56 bits ne pourront pas communiquer avec votre site, à moins de mettre à niveau leur force de cryptage.

3. Ouvrez votre navigateur et essayez de vous connecter à votre serveur Web en utilisant le protocole http:// standard. Si SSL est en cours d'application, vous recevez le message d'erreur suivant :

   La page doit être affichée sur un canal sécurisé
   La page que vous essayez d'afficher nécessite l'utilisation de « https » dans l'adresse.

   Essayez de la manière suivante : Réessayez en tapant https:// au début de l'adresse que vous essayez d'atteindre. HTTP 403.4 - Interdit : SSL a requis Internet Information Services
   Informations techniques (pour le personnel technique) - Contexte : Cette erreur indique que la page à laquelle vous tentez d'accéder est sécurisée à l'aide du protocole SSL (Secure Sockets Layer).

   Vous ne pouvez désormais vous connecter à votre site Web qu'à l'aide du protocole https://.

5.2 SSH (Secure Shell) :

Il est apparu au début des années 90 pour pallier au manque de sécurité des protocoles Telnet et RSH (Remote Shell) ; ces protocoles ont pour but premier de fournir un shell sur une machine distante.
Le but de SSH est d'obtenir un environnement d'exécution sur une machine distante sans compromettre la sécurité de l'une ou l'autre des parties.
SSH assure une authentification réciproque des parties : le client authentifie d'abord le serveur et qu'il s'authentifie lui-même vis-à-vis de celui-ci.
L'authentification du serveur se fait au moyen de sa clé publique. Lors de l'établissement d'une session, le client se voit présenter la clé publique du serveur, il l'accepte ou la refuse.
L'authentification du client peut se passer de deux façons. La première, la plus simple et la moins sécurisée, est le couple : utilisateur/mot de passe. A l'établissement de la connexion, le serveur demande au client son nom puis le mot de passe associé.
La seconde option consiste à se baser sur une architecture clé publique/clé privée. Il faut avoir préalablement déposé sa clé publique dans un fichier prévu à cet effet sur la machine distante vers laquelle on souhaite établir une connexion (e serveur SSH).
Dans les deux cas, l'utilisation qui se présente est un utilisateur déclaré sur le serveur.
Pour la majorité des distributions Linux, le package OpenSSH est souvent installé, mais il n'est généralement pas démarré. Pour le démarrer, il est possible de lancer le binaire /usr/sbin/sshd après avoir pris soin de générer des clés.

5.3 IPSec (IP Secure) :

C'est un protocole de la couche réseau. Il est issu de la suite protocolaire IPv6. Il s'agit de l'une des nombreuses options possibles. IPSec va assurer à ses utilisateurs, tous à la fois : confidentialité, intégrité et authentification ainsi que la gestion des clés.
IPSec fournit 04 services de sécurité permettant l'authentification et/ou la confidentialité :

- Authentification des données : IPSec permet de s'assurer que chaque paquet échangé, il a bien été émis par la bonne machine et qu'il est bien à destination de la seconde machine.

- Confidentialité des données échangées : on peut décider de chiffrer le contenu des paquets IP pour empêcher qu'une personne extérieure ne le lise.
- Intégrité des données échangées : IPSec permet de s'assurer qu'aucun paquet n'a subit une quelconque modification durant son trajet.
- Protection contre l'analyse du trafic : IPSec permet de chiffrer les adresses réelles de l'expéditeur et du destinataire, ainsi que tout l'entête IP correspondant : c'est le principe du tunneling.

5.3.1 Architecture :

IPSec est constitué de deux protocoles. Le premier AH (Authentication Header) est responsable de l'authentification des parties ; mais ne garantit aucune confidentialité. Le second ESP 5Encapsulating Security Payload) est responsable du chiffrement des données. Il peut garantir l'authentification des parties, mais apporte une certaine redondance avec AH. Ces deux protocoles peuvent être alors utilisés séparément ou combinés.

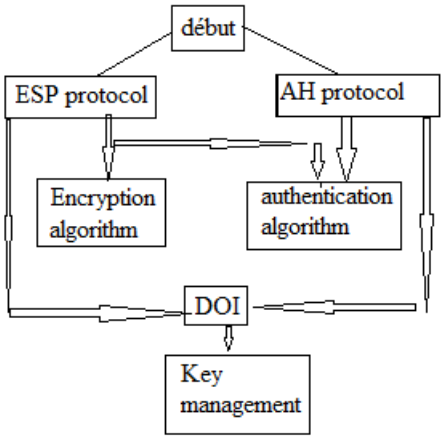

Figure 5.1Architecture IPSec

IPSec négocie les paramètres de sécurité entre les deux parties et notamment les algorithmes qui seront utilisés. IPSec propose également un cadre permettant de renégocier régulièrement les clés utilisées sur la base de leur temps de vie.

5.3.1.1 Phase de négociation:

IPSec repose sur deux phases distinctes :

- La première ISAKMP (Internet Security Association and Key Management Protocol) est responsable de la mise en place d'un premier tunnel qui authentifie les parties en œuvre. Elle va également permettre d'échanger une clé secrète qui chiffre les échanges de la seconde phase.
- La seconde phase, nommée IPSec, négocie les clés qui serviront à chiffrer les données échangées par la suite.

Chaque tunnel (phase1 ou phase2) est en fait constituée par une SA (Security Association) qui reprend l'ensemble des points négociés pendant son établissement.
Si les négociations n'aboutissent pas, dans l'une ou l'autre de ces phases, les SA ne sont pas crées.
IKE (Internet Key Exchange) est le protocole responsable de l'établissement des tunnels. Il s'appuie sur ISAKMP pour négocier l'association de sécurité (SA) de la première phase et sur le protocole de génération de clés OAKLEY pour négocier les SA de la seconde phase IPSec.

a. **SA : Security Association :**
   Une SA de ISAKMP (correspondant à la première phase) contient :

- L'identité de son vis-à-vis qui peut être son adresses IP ou son nom DNS.
- Le choix de l'algorithme de chiffrement (chiffrement symétrique). Il peut s'agir de DES, AES,…
- Le choix de l'algorithme d'authentification (fonction de hachage) qui peut être MD ou SHA.
- Le mécanisme d'authentification réciproque mis en place (secret partagé ou certificat)
- Durée de vie.

Une SA IPSec (seconde phase) contient :

- Un numéro unique d'index permettant d'y faire référence, le SPI (Security Policy Index).
- Choix de l'algorithme de chiffrement
- Choix de l'algorithme d'authentification
- Clés secrètes utilisées
- Durée de vie
- Domaine de chiffrement (DOI : Domain Of Interpretation) associé à cette SA.

b. **SPD : Security Policy Database:**

La SPD est une base de données présente sur chaque système capable d'utiliser IPSec. Elle permet de déterminer la politique de sécurité à appliquer à un certain trafic. Chaque entrée de cette base est identifiée grâce à plusieurs 'sélecteurs' tels que l'adrese IP source et destination, le numéro de port ou le protocole de transport. Ce sont ces sélecteurs qui permettent de retourner les SA associées à un type de trafic.
La SPD est consultée pendant tout transfert de données, entrant ou sortant,, IPSec ou non IPSec.
Trois choix sont possibles :

- Appliquer les paramètres IPSec
- Laisser passer le trafic
- Rejeter le trafic

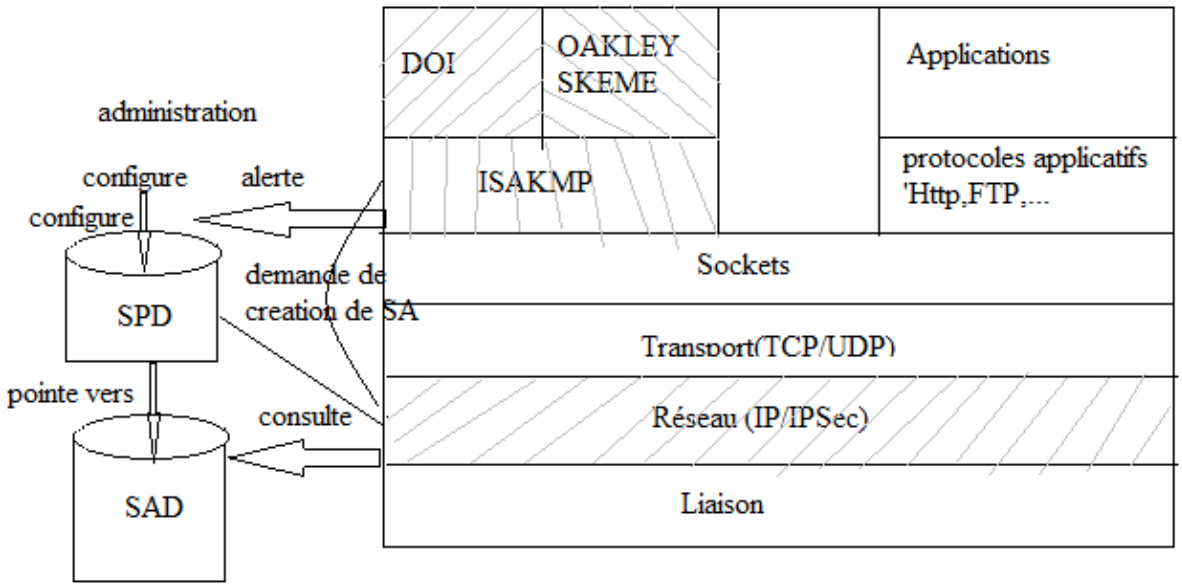

Figure 5.2 Environnement de fonctionnement d' IPSec

a. **Gestion des clés ;**

IPSec gère la génération et la destruction des clés. Dans le cadre, d'une gestion manuelle, l'administration système configure manuellement chaque système ; c'est une solution lourde.

Avec IPSec, la gestion des clés est automatisée (IKE). Un système automatisé est présent pour la création sur demande des clés pour la création des SA dans de grands systèmes. La partie responsable de la gestion des clés dans IPSSec repose sur les protocoles OAKLEY et ISAKMP.