République Algérienne Démocratique Et Populaire
Ministere De L'enseignement Supérieur Et De La Recherche Scientifique

Université SAAD DAHLEB de Blida
Département d'informatique
Année universitaire 2002/2003

Projet de fin d'étude pour l'obtention d'un diplôme d'ingénieur d'état en informatique

Intitulé du sujet :

Conception et mise en place d'une solution de sécurité pour le réseau bancaire de la Banque Extérieure d'Algérie

Projet Réalisé par : Mlle MAOUDJ Nabila.

Projet Encadré par : Mr TALEB Said.

Membres de la commission de suivit : Mr BALA.
Mr Hadj Yahia.

Président du jury : Mr BENNOUAR
Membres du jury : Mr HADJ YAHIA
Mlle BOUSTIA

Promotion 2003

REMERCIEMENTS

Ce projet a été réalisé grâce à la formation dont j'ai bénéficié et à toutes les personnes qui m'ont aidé à assimiler mon projet et de confectionner ce document

Mes remerciements iront tous naturellement à ma famille qui m'a soutenu durant toute la période de ma scolarité et de mon stage .

Je remercie mon promoteur Monsieur TALEB Said directeur de la cellule monétique de m'avoir encadré durant mon stage au sein de la BEA sans oublier tous les membres de son personnel.

Je remercie les membres de la commission de suivi, qui ont suivit le déroulement de ce projet et m'ont dirigé à bien le mener

J'adresse également mes vifs remerciements à Monsieur Bruno ADAMOLLE et tout le personnel d'AACom-Algerie et AACom-France, qui m'ont offert toute l'assistance et le matériel nécessaire pour mener à bien ce projet.

Sans oublier les personnes qui n'ont hésité à m'apporter leur aide et je cite; Monsieur AKROUR Djeloul, Monsieur CHAALAL Bilel, Monsieur FERRAG Djamel.

DEDICACES

Je dédie ce mémoire à mes parents et à mes frères et sœurs qui m'ont permis de mener à bien mes études et surtout de m'avoir soutenu au cours de mon projet.

Je dédie ce mémoire à tous mes amis ,mes collègues et à toutes les personnes qui m'ont soutenu.

Résumé

Les réseaux longues distances sont le symbole du millénaire, ils inquiètent et fascinent à la fois, ils concentrent les espoirs de modernité et les peurs d'un avenir encore incertain. Ils représentent la victoire informatique sur les distances et un défi contre le temps.

Etant donnés la croissance des systèmes informatiques, le nombre de plus en plus grand des réseaux interconnectés grâce au protocoles TCP\IP, le caractère de plus en plus sensible et confidentiel des données, le problème de la sécurité des données est aujourd'hui incontournable.

Pour dés réseaux longues distances, tels les réseaux bancaires, il est impératif de protéger le réseau local. Or ce n'est guère suffisant, surtout quand les données doivent être transférées, d'un réseau à un autre.

L'utilisation d'une solution permettant le transfert d'information d'un réseau local, vers un autre réseau local distant dans la plus grande confidentialité et intégrité devient une nécessité absolue.

IPSec est constitué par plusieurs protocoles. Ces protocole offrent une forte authentification de l'extrémités communicante et des données transmis , ainsi qu'il permet une confidentialité grâce au méthodes de cryptographie.

Le protocole IPSec est implementable sur des PIX selon une politique de sécurité adapté au besoin du réseau à sécurisé.

Le protocole IPSec peut aussi avoir une implémentation logicielle. FreeWan est un logiciel permettant l'implémentation IPSec, cet implementation se fait par manipulation des fichiers de configuration et un ensemble de commandes.

Une interface graphique pour un logiciel de sécurité peut être d'un très grand bénéfice tel que, la facilité à manipulé des concept nouveaux et difficiles à assimiler qui concerne la configuration d'IPSec, ainsi elle conduit l'utilisateur à commettre moins d'erreurs

Mots clefs: IPSec, PIX, TCO/IP ,Cryptographie, échange de clef, FreesWan, IKE.

Summary

The public wide area networks are symbols of progress of this millennium . They worry and fascinate at the same time. They focus on the hope of advance and the fear of an unsettled future. They represent the computer science's victory over long distances and a challenge against time.

Taking in consideration the development of the informatics systems, the great number of the interconnected networks -thanks to the protocols TCP\IP-, the character more and more sensitive and confidential of data; the problem of data's security is today unavoidable.

For the long distance network, such as banks networks, it is necessary to protect the local one. Otherwise it is hardly sufficient, especially when the data must be sent from a network to another.

The use of a solution which allow the sent of an information from a local network, toward another far network in the most high confidentiality and integrity becomes an absolute necessity.

IPSec is set up by many protocols. This protocols give a great authentication of peer communicants and of the transmitted data, thus they allow the confidentiality thanks to cryptography methods.

The IPSec protocol is implementable_on PIX according to a policy security which fits the need of the secured network.

The IPSec protocol may be also implementable on a software FreeWan, this implantation is made by the manipulation of configuration files and a set of commands.

A graphic interface for security software may be for a great advantage, such as the easiness to handle a new and difficult concept to assimilate which concerns the IPSec configuration; thus it can produce an advantage of a less configuration's mistakes.

Key words : IPSec, PIX, TCP/IP ,Cryptographie, échange de clef, FreesWan, IKE.

SOMMAIRE

CHAPITRE I

INTRODUCTION AUX RESEAUX INFORMATIQUES

I - RAPPEL SUR LE MODELE DE REFERENCE OSI.....3
I - 1- SERVICES ET PROTOCOLES.....4
I-1-1-Le service (N) SDU (Service Data Unit) :.....4
I-1-2-Le protocole (N) PDU (Protocol Data Unit) :.....4
I-1-3- Les points d'accès aux services (N) ou ((N) –Service Access Point) :.....4
I-2-LES SEPT COUCHES OSI.....4
I-2-1- LA COUCHE PHYSIQUE.....4
I-2-2- LA COUCHE LIAISON DE DONNÉES.....5
I-2-2- a) La couche MAC (Medium Access Control).....5
I-2-2- b) La couche LLC (Logical Link Control).....5
I-2-3 -LA COUCHE RÉSEAU.....5
I-2-3-a) Le contrôle de flux :.....6
I-2-3-b) L'adressage :.....6
I-2-3-c) Le routage :.....6
I-2-4- LA COUCHE TRANSPORT.....6
I-2-5- LA COUCHE SESSION.....8
I-2-6- LA COUCHE PRESENTATION.....9
I-2-7-LA COUCHE APPLICATION.....9

II - RAPPEL SUR LE PROTOCOLE TCP/IP.....9
II-1-LES PRINCIPAUX PROTOCOLES.....10
II-1-1- LE PROTOCOLE ARP.....10
II-1-2- LE PROTOCOLE IP.....10
II-1-2-a) Adressage IP.....11
II-1-2-b) Masque de sous réseau.....11
II-1-2-c) Fragmentation des datagrammes IP.....12
II-1-3-Le protocole ICMP.....12
II-1-4-Le protocole UDP.....12
II-1-5-Le protocole TCP.....13
II-1-6-Le protocole FTP (File Transfer Protocol).....13
II-1-7-Le Protocole DNS (Domaine Name Service).....13

CONCLUSION.....14

CHAPITRE II

SECURITE INFORMATIQUE

II-1 - OBJECTIFS DE LA SECURITE INFORMATIQUE.....16

II-2-LES VULNERABILITES DES SYSTEMES INFORMATIQUES.....17
II-2-1- Detournement de classe d'adresses internet.....17
II-2-2- Ecoute passive : 18
II-2-3- Le "sniffing" des paquets, ou interception des donnees.....18
II-2-4- IP spoofing :.....19
II-2-5-Falsification des adresses mac / arp spoofing.....19
II-2-6-Attaque par saturation de la bande passante des liaisons internet.....22
II-2-7-Attaque par overflow de service TCP.....22
II-2-8-Les dénis de services réseaux.....23

II-3- ETABLISSEMENT D'UNE POLITIQUE DE SECURITE :.....27

II-3-1- Politique de sécurité de site.....27
II-3-2- L'approche de la politique de sécurité.....28
II-3-3- Mise en place des responsabilités.....28

I-4-TECHNIQUES DE SECURITE.....28
II-4-1-La cryptographie.....28
II-4-1-1- Terminologie de la cryptographie 29
II-4-1-2-La cryptographie symétrique.....29
II-4-1-3- La cryptographie asymétrique.....30
. II-4-2-Les algorithmes de cryptage.....30
II-4-2-1- Systèmes à clef secrète.....31
II-4-2-2- Systèmes à clef publique 31
a) *Cryptage de Rivest-Shamir-Adelman RSA*.....32
II-4-3 - Distribution de clefs.....32
a)Echange de clefs symétrique:.....32
b) Echange de clefs symétrique avec serveur:.....33
c) Echange de clefs asymétrique:.....33
d)Echange de clef sasymétrique avec serveur:.....33
II-4-4 - Notion de certificat.....34
II-4-5- La signature numérique.....34
II-4-6- Authentification :.....35
II-4-6-1- Authentification de message 35
a)Cryptage de message: 35
b) "Checksum" cryptographique:.....37
c) Fonction de hachage: 37
II-4-6-2- Authentification des utilisateurs :.....38
a) Sécurisation d'architectures clients-serveurs 38
b) Protocoles d'authentification : 39
II-4-7 - L es protocoles d'authentifications mutuelles avec échange de clefs développés pour IP.....39
II-4- 7 - 1- Diffie-Hellman.....39
II-4- 7- 2- Les différents protocoles :.....40
a) SKIP.....40
b) Photuris.....41
c) SKEME.....42
d) Oakley.....44
e) La gestion des clefs pour IPsec : ISAKMP et IKE.....44
II-4-8- Mécanisme à jeton synchronise (securid).....45
II-4-8-1- Architecture matérielle de SecurID :.....45
II-4-9- Sécurisation des machines individuelles 46
II-4-10 - Firewalls :.....46
II-4-11- Détection d'intrusion 47
a- IDS à Bibliothèques de signatures.....47
b- IDS à Modèles comportementaux.....47
II-4-12- Translation d'adresse 48
a-Adressage.....48
b-Network Address Traduction (NAT).....48
c- Single User Account (SUA) :.....49

***CONCLUSION*.....50**

CHAPITRE III
Présentation du réseau bancaire de la Banque Exterieure d'Algerie

III-1-NECESSITE DU RESEAU.....52
III-2-LES ELEMENTS DU RESEAU.....52
III-2-1-Réseau local Ethernet.....52
III-2-2-La stratégie du réseau BEA.....53

a) Une agence.....53
b) La gestion des opérations de produit bancaire Dinars et devises.....53
c) Le site centrale.....53
d) La structure fonctionnelle de consolidation.....53

III-3-SCHEMAS DU RESEAUX.....54
Conclusion.....56

CHAPITRE IV
Solution de sécurité

VI-I-
PROBLEMATIQUE.....58

IV-2-LA TUNNELISATION (TUNNLING).....58
IV-2-1-Tunnels – Rôle-.....59
IV-2-2-Tunnels - Principe de fonctionnement.....59

IV-3-QU'EST-CE QU'UN VPN ?.....59
IV-3-1-Les avantages des VPN.....60

IV-4-ARCHITECTURE DES VPN.....60
IV-4-1-Types de VPN.....60
a) VPN à Accès Distant.....60
b) VPN Intranet.....61
c)VPN Extranet.....61

IV-5-COMPOSANTES NECESSAIRES AUX VPN.....61

IV-6-PROTOCOLES UTILISE DANS LE CADRE DES VPN.....62
IV-6-1-Point to Point Tunneling Protocol (PPTP).....63
IV-6-2-Layer 2 Forwarding (L2F).....64
IV-6-3-Layer 2 Tunneling Protocol (L2TP).....64
IV-6-4-IPSec.....65
a) Introduction sur Ipsec.....65
b) Architecture d'Ipsec.....66

IV-7-COMPARAISON DES PROTOCOLES DE TUNNELING.....68

IV-8-PRESENTATION APPROFONDIE D'IPSEC.....68
IV-8-1-Authentication Header (AH).....68
IV-8-2-Encapsulating Security Payload (ESP).....70
IV-8-3-Fonctionnement d'IPSec.....72
IV-8-4- Les différents modes.....74
a) Main mode - mode principal.....74
b) Agressive mode - mode agressif.....74

IV-9-LE CHOIX DE LA
SOLUTION.....75
IV-9-1-Type de solutions disponibles pour l'implémentation des VPN:.....75
a) Les systèmes matériels.....75
b) Solutions logicielles.....75

CONCLUSION.....76

CHAPITRE V
Conception de la solution de sécurité

V-1- ARCHITECTURE DE LA SOLUTION....78

V-2- DEFINITION DE LA POLITIQUE DE SECURITE....79
V-2-1-Planification de la sécurité du réseau....79

V-3-POLITIQUE DE SECURITE IPSEC....80
V-3-1- Echange de clefs et authentification....81
V-3-2-Le mode choisi....82
V-3-3- Déroulement du mode principal....83
V-3-4-Déroulement du mode rapide....88
V-3-5-La base de données de politique de sécurité (SPD)....90
V-3-6- La base de données des associations de sécurité (SAD)....90

V-4-DEROULEMENT DU MECANISME GLOBAL....90
V-4-1-Trafic sortant....91
V-4-2-Trafic entrant....92

CONCLUSION....93

CHAPITRE VI
Mise en place des VPN

VI-1-LE CHOIX DE L'IMPLEMENTATION....95

VI-2-LES CARACTERISTIQUES DU MATERIEL....95

VI-3-DESCRIPTION DE L'ENVIRONNEMENT....95

VI-4-INTEGRATION DU PIX DANS L'ENVIRONNEMENT....95

VI-5-LA CONFIGURATION D'IPSEC....96
VI-5-1-Création de la SAD....96
VI-5-3-Création de la crypto map....97

CONCLUSION....98

CHAPITRE VII
Conception d'une interface pour FreesWan

VII-1-PRESENTATION DE FREESWAN....100

VII-2-CONCEPTION DE L'INTERFACE....101
VII-2-1-Differentes manières d'organiser l'information....102
a) Modèle linéaire....102
b) Modèle arborescent....102
c) Modèle libre....102
d) Modèle complexe....103

VII-3-UNE APPROCHE A LA CONCEPTION....103
VII-3-1-analyse des requis (tâches)....103

VII-3-2- Evaluation de l'analyse.....103
VII-3-3-conception du modèle fonctionnel.....104
VII-3-4-Conception de la présentation.....104
VII-3-5-Conception des actions.....105

VII-4-ERGONOMIE DE L'INTERFACE.....105

VII-5-REALISATION DE L'INTERFACE.....106
VII-5-1-FICHIER ipsec.sercets.....106
VII-5-2-FICHIER ipsec.conf.....110

CONCLUSION.....121

CONCLUSION GENERALE

ANNEXE

GLOSSAIRE

BIBILIOGRAPHIE

Sommaire des figures

Figure I -1-Model en couche OSI 5
Figure I -2: Le model TCP/IP 10
Figure II-1:Action entrainé par une double propagation BGP effectué par un réseau pirate 18
Figure II-2 :Spoofing IP 19
Figure II-3 :Spoofing ARP 20
Figure II-4-Cryptage de message 9
Figure II.5 : *Algorithmes symétriques* *30*
Figure II-6- Cryptographie à clef publique 30
Figure II.6 : *Système à clef publique* *31*
Figure III.5 :*Authentification dans les Systèmes à publique* *34*
Figure II.6 : *Authentification et Confidentialité* *34*
Figure III-1-Architecture du réseau bancaire 55
Figure IV-1 Différents types de tunnels 59
Figure IV-2: Encapsulation d'un paquet dans un datagramme IP 62
Figure IV-3:Protocole PPP- 62
Figure IV-4:Protocole PPTP 63
Figure IV-5: Format du paquet L2TP 65
Figure IV-6: Format AH 69
Figure IV-7:Application de AH en mode transport et tunnel 71
Figure IV-8:Format de ESP 71
Figure IV- 9:Application du mode transport et tunnel avec ESP 72
Figure V-10:Architecture de la solution de sécurité 78
Figure V-11- Schémas fonctionnel du mode principal 86
Figure V-12 :1er échange du mode principal 87
Figure 13 : 2eme échange du mode principale 87
Figure V-14: 3eme échange du mode principal 88
Figure V- 15: Schéma fonctionnel du déroulement du mode rapide 88
Figure V-16:Les échanges du mode rapide 89
Figure V 17:Organigramme de l'évolution d'un paquet sortant 91
Figure V-18 :Organigramme de l'évolution d'un paquet entrant 92
Figure VII-19: Inter activité Homme-Machine 101
Figure VII-20:Fenêtre IPSec.secrets 107
Figure VII-21:Activation de l'icône du choix des clefs 108
Figure VII-22 : Choix d'utiliser l'ancienne clef PSK 109
Figure VII-23:Choix d'utiliser une nouvelle clef RSA 110
Figure VII-24:Fenêtre IPSec.conf 111
Figure VII- 25 :Icône config setup 112
Figure VII-26: Icône connexion (paramètres de négociation) 113
Figure VII-27: Icône connexion (adressage) 114
Figure VII-28: Fenêtre de commande 115
Figure VII-29: Lancement d'IPSec 116
Figure VII- 30: Echec de lancement d'IPSec 117
Figure VII-31: Consultation des erreurs de lancement 118
Figure VII-32: Etablissement réussit d'un vpn 119
Figure VII-33: Echec lors d'établissement d'un VPN 120
Figure VII-34: Consultation d'erreur pour l'échec de l'établissement d'un VPN 121

Sommaire des tables

Tableau II-1-Objectif de la securité informatique 16
Tableau IV-1-Comparatif VPN/Liaison loués 60
Tableau IV-2-Comparatif des protocoles des de tunneling 68
Tableau V-1-Représentation d'une politique de sécurité 80

INTRODUCTION

Les réseaux informatiques permettaient à l'origine de relier des terminaux passifs, à des ordinateurs centraux.

A l'heure actuelle, ils autorisent l'interconnexion de tous types d'ordinateurs : de grands serveurs, des stations de travail, des ordinateurs personnels, et tous sorte de ressources matériels.

De nos jours, il n'est plus à démontrer que les possibilités de violation de la sécurité des systèmes interconnectés, se sont multipliées par rapport aux systèmes classiques.

Un organisme comme la Banque Extérieure d'Algérie (BEA) ,doit gérer un nombre important de composants informatiques , distribués sur l'ensemble des agences et de directions , et qui sont reliées entres elles ,par l'intermédiaire du réseaux ***Intranet/Extranet*** *, via le protocole TCP/IP en utilisant les lignes X25 (pour les longues distances) .*

L'objectifs de ce projet est de mettre en place un système de sécurité, capable de protéger le réseau BEA des intrusions, et d'assurer la confidentialité des transmissions .

Mais avant d'aborder le thème de la sécurité, il faut tous d'abord étudier l'objet à sécurisé est qui n'est autre que le réseau.

C'est pour cela que ce projet commence d'abord, par une familiarisation avec ***le model de référence OSI*** *et* ***le protocole TCP/IP.*** *Ce qui permettra d'identifier les vulnérabilités des réseaux qui utilisent les protocoles cités ci-dessus*

Après avoir passé en revue ces différents systèmes et applications ainsi que la sécurité qu'ils proposent, on présentera les failles et les solutions apportées contre les malveillances.

Et finalement ce projet s'achèvera avec le choix de la meilleur solution pour sécuriser notre réseau.

En plus ce sujet a été enrichi, par l'ajout d'une partie qui consiste en la conception d'une interface graphique, pour la configuration IPSec sous Linux.

Ce mémoire s'achève par un glossaire des mot clé et une bibliographie-Webographie. .

CHAPITRE I

INTRODUCTION AUX RESEAUX INFORMATIQUES

Les réseaux informatiques sont nés du besoin de faire communiquer des terminaux distants avec un système central, des ordinateurs entre eux et enfin de connecter des machines terminales telles que des stations de travail avec leurs serveurs .
Dans un premier temps ,ces communications étaient destinées au transport de données informatiques . Aujourd'hui ,on se dirige vers des réseaux qui intègrent en plus des données, la parole et la vidéo.(multimédia)

Les réseaux informatiques ont vu le jour ; en réponse du besoin d'échange d'informations de manière simple et rapide entre les machines, lorsqu'on travaillait sur une même machine toutes les informations nécessaires au travail étaient centralisées sur cette machine et tous les utilisateurs et programmes avaient accès à ces informations .

Pour des raisons de performances, on est venu à multiplier le nombre de machines d'où la nécessité des entreprises et des établissements à décentraliser le traitement , et d'accéder à l'information de façon rapide.

I -1- RAPPEL SUR LE MODELE DE REFERENCE OSI

En 1977 l'Organisation Internationale de Normalisation (ISO) a créé pour des besoins de compatibilités entres les différentes machines, tout un ensemble de lois de compatibilité en différentes couches baptisées **modèle OSI** (Open System Interconnection model).

Chaque couche a un rôle bien particulier, et communique sur requête (sur demande) de la couche supérieure en utilisant des services de la couche inférieure (sauf pour la couche physique 1).

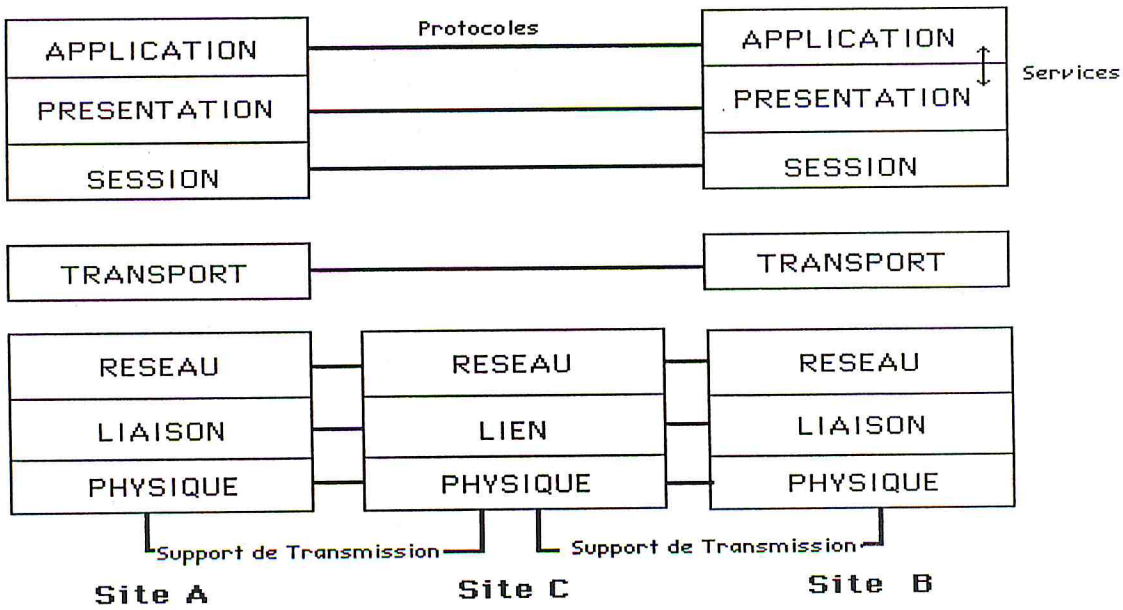


Figure - I . 1: Modèle en couche OSI [ISO03]

I -1- 1- SERVICES ET PROTOCOLES

Pour faire parvenir un message d'un émetteur A, vers le destinataire B ; le message doit passer par les couches de la station émettrice du plus haut niveau au plus bas (couche physique) . Puis le message va transiter par les connexions réseau (nœud,...), jusqu'à son arrivée sur la plus basse couche de la station B ,ainsi il va remonter les différentes couches jusqu'à son arrivée sur la plus haute couche .

Chaque couche a un niveau N . Le concept d'architecture en couche demande la définition de trois objets de niveau (N) :

I-1-1-1-Le service (N) SDU *(Service Data Unit)* :

Un service est un ensemble de primitives (opérations) qu'une couche fournit à la couche immédiatement supérieure à elle.

I-1-1-2-Le protocole (N) PDU (*Protocol Data Unit*) :

Le protocole de niveau (N) définit un ensemble de règles nécessaires pour que le service de niveau (N) soit réalisé,

I-1-1-3- Les points d'accès aux service (N) ou (*(N) –Service Access Point*) :

Le (N)-SAP constitue l'interface qui permet l'accès d'une couche supérieure vers une couche inférieure.

Chaque couche du modèle OSI est constituée d'éléments matériels et logiciels pour pouvoir offrir des service à la couche supérieure.

I-1-2-LES SEPT COUCHES OSI [BER99][MAN02][PUJ02]

I-1-2-1- LA COUCHE PHYSIQUE

La couche Physique définit les spécifications électriques, mécaniques, de procédures et fonctionnelles pour établir, maintenir et désactiver la liaison physique entre les systèmes d'extrémité. Les caractéristiques comme les niveaux de tension, la synchronisation des changements de tension, les débits physiques, les distances maximales de transmission, les connecteurs physiques et autres aspects de bas niveau sont définis par la couche physique.

Pour mener à bien sont rôle , on trouve dans cette couche le matériel et logiciel suivant :

- ***les interfaces de connexion des équipement informatique*** ou jonctions
- ***les modems*** qui transforment les signaux binaires provenant des composantes informatiques (ordinateurs, équipement terminaux ....) ,en des signaux binaires aussi mais sous forme sinusoïdale.

- ***Les multiplexeurs*** qui permettent de recevoir plusieurs émissions de machines différentes sur plusieurs lignes, et les concentrer sur une seule ligne de sortie.
- ***Les nœuds de commutation*** sont des intermédiaires entre l'émetteur et le récepteur, ils prennent en charge les données et les envoie dans la bonne direction .
- ***Divers équipements*** qui dépendent du réseau ,exemple :un satellite.

I-1-2-2- LA COUCHE LIAISON DE DONNÉES

Cette couche est chargée d'assurer les moyens fonctionnels et procéduraux nécessaires à l'établissement ,au maintien et à la libération des connexions ; comme elle s'occupe aussi du transfert des unités de données de service liaison. Cette couche est chargée du bon acheminement des données.

La couche liaison de données doit appliquer un ensemble de règles garantissant la transmission correcte de données :

- L'acquittement des trames
- Le contrôle de flux
- Le contrôle d'erreur

La couche liaison de données est divisée en deux sous-couches:

I-1-2-2- a) La couche MAC (*Medium Access Control*)

Elle a pour rôle de gérer l'adressage physique des cartes réseau, comme elle s'occupe aussi de gérer les problèmes d'accès au support physique,

I-1-2-2- b) La couche LLC (*Logical Link Control*)

Elle s'occupe du transfert des trames entre les stations du réseau en utilisant des protocoles comme : HDLC ou BSC.

Cette sous couche s'occupe aussi de corriger éventuellement les erreurs détectées par la sous-couche MAC, en se basant sur certains codes comme code **Hamming .**

I-1-2-3 -LA COUCHE RÉSEAU

La couche réseau assure toutes les fonctionnalités de relais et d'amélioration de services entre entité de réseau, à savoir : l'adressage, le routage, le contrôle de flux et la détection et la correction d'erreurs non réglées par la couche 2.

L'unité d'information est le ***paquet***. C'est à ce niveau qu'est définie la notion d'adresse réseau.

Ici interviennent les protocoles, IPX (voir annexe), **IP**,(dans TCP/IP) . A ce niveau interviennent aussi les protocoles de routage tels Routing Information Protocol (RIP)(voir annexe).

Les principales fonctionnalités de cette couche sont :

I-1-2-3-a) Le contrôle de flux :

Il faut contrôler le flux dans une liaison, de sorte que les tampons puissent traiter les données en entier. Pour cela des méthodes comme le mécanisme de fenêtrage ou la méthode du X-off / X-on peuvent être utilisées.

I-1-2-3-b) L'adressage :

Pour accéder à une ressource d'un réseau, il faut utiliser son adresse unique.

- l'adressage physique:
  A une adresse unique correspond un emplacement physique.
  Le parfait exemple est le Réseau Téléphonique Commuté (RTC): à un numéro de téléphone, un combiné téléphonique.

- l'adresse logique
  A une adresse unique correspond un équipement particulier, quelque soit son emplacement géographique ;par exemple un réseau local .

I-1-2-3-c) Le routage :

c'est la détermination du chemin emprunté dans un réseau par une communication ou un paquet de données . Un nœud devrait connaître l'état de tous les nœuds avant de décider ,vers lequel envoyer un paquet .

Pour mettre en place et développer les fonctionnalité réseau, deux grandes philosophies se présentent :

- **Le mode connecté**, où l'émetteur et le récepteur se mettent d'accord sur un comportement commun..
- **Le mode non connecté,** où aucune contrainte n'est imposée .

I-1-2-4- LA COUCHE TRANSPORT

Cette couche assure un contrôle de bout en bout ,en permettant à deux machines d'ouvrir une connexion pour communiquer .elle fournit le transfert de données entre les entités de session .

L'unité d'information est le **message** .Cette couche s'occupe aussi du découpage ou de la reconstitution des messages .

La couche transport doit assurer en mode connecté ou non connecté ,un transfert transparent de données entre les utilisateurs de service réseau ,en leur rendant invisible la manière dont les ressources de communication sont mises en œuvre.

Les différents paramètres de la qualité de service sont :

- le *temps d'établissement de la connexion transport*: c'est la durée qui s'écoule entre le moment où une demande de connexion est émise et le moment où la confirmation de cet établissement est reçu et plus ce délai est court meilleure est la qualité de service.
- la *probabilité d'échec d'établissement* mesure la chance (ou plutôt malchance) qu'une connexion ne puisse s'établir dans un délai maximum défini. On ne tient pas compte ici du refus de l'entité distante d'établir cette connexion, mais on considère plutôt les problèmes d'engorgement de réseau.
- le *débit de la liaison* mesure le nombre d'octets utiles qui peuvent être transférés en une seconde, ce débit est évalué séparément dans les deux sens.
- le *temps de transit* mesure le temps écoulé entre le moment où l'utilisateur du service de transport envoie un message et celui où l'entité de transport réceptrice le reçoit, ce temps est évalué séparément dans les deux sens.
- le *taux d'erreur résiduel* est le rapport entre le nombre de messages perdus ou mal transmis et le nombre total de messages émis au cours d'une période considérée. Ce nombre, en théorie nul, a une valeur faible en pratique.
- la *probabilité d'incident de transfert* mesure le bon fonctionnement du service transport. Lorsqu'une connexion est établie, un débit, un temps de transit, un taux résiduel d'erreurs sont négociés. La probabilité d'incident mesure la fraction de temps durant laquelle les valeurs fixées précédemment n'ont pas été respectées.
- le *temps de déconnexion* mesure la durée s'écoulant entre une demande de déconnexion émise et la déconnexion effective du système distant.
- la *probabilité d'erreur de déconnexion* est le taux de demandes de déconnexion non exécutées pendant le temps maximum défini.
- la *protection* est définie comme la possibilité de se prémunir contre les intrusions passives (interférences sur une même ligne) et actives (écoute et modification des données transmises).
- La *priorité* permet à l'utilisateur de privilégier certaines transmissions par rapport à d'autres.
- La *résiliation* est la liberté laissée à la couche transport de décider elle-même de la déconnexion suite à un problème.

En mode non connecté, ces paramètres indiquent uniquement les souhaits de l'utilisateur en ce qui concerne le débit, le délai de transit, le taux d'erreur résiduel et la priorité d'une transmission. Ces paramètres sont utilisés par la couche transport pour fixer des options de protocoles avant d'être soumis à la couche réseau.

Lorsqu'une connexion est demandée, tous ces paramètres sont transmis par l'utilisateur à la couche transport, les valeurs désirées et minimales sont spécifiées. Les différents cas de figure et étapes peuvent alors se présenter.

- Si la demande semble irréaliste pour certains paramètres alors la demande de connexion n'est même pas exécutée et un message d'erreur est renvoyé pour expliquer le problème.
- Si la demande ne peut pas être satisfaite complètement mais partiellement (par exemple avec un débit moindre mais acceptable), alors c'est cette demande avec des objectifs moindres qui est soumise.
- Si l'ordinateur distant ne peut satisfaire complètement la demande, mais reste au-dessus du minimum requis, alors il modifie aussi le paramètre.
- S'il ne peut pas rester au-dessus de ce minimum, il rejette la demande de connexion.
- Enfin, la couche transport avertit son utilisateur de la bonne fin (ou non) de la procédure de connexion et lui transmet les paramètres acceptés.

Cette procédure s'appelle la *négociation des options* lesquelles une fois fixées, restent inchangées pendant toute la connexion. Pour que tous les utilisateurs ne demandent pas une qualité de service optimale, les prix pratiqués par les fournisseurs de réseaux croissent avec cette qualité de service.

Les services qu'offrent la couche transport en mode connecté sont rendues par les primitives . (voir annexe).

I-1-2-5- LA COUCHE SESSION

Cette couche est responsable de l'organisation et de la synchronisation des échanges entre utilisateurs.

Elle concerne le dialogue entre les nœuds, quand un émetteur et un récepteur commencent à dialoguer, ils établissent une session. Ils dialoguent pour établir les règles de communications, *choisir les protocoles qu'ils vont utiliser.*

Le fonctionnement se fait en trois temps, établissement de la connexion, transfert, libération de la connexion.

La couche session peut être confondue avec la connexion transport , mais les deux couches ne sont pas identiques car :

- Il y a une correspondance entre une session et une connexion transport,
- On peut ouvrir et fermer plusieurs sessions sur une seule et même connexion de transport.
- En cas de panne de la connexion de transport ,le couche session établit une nouvelle connexion transport afin de poursuivre la connexion commencée .

I-1-2-6- LA COUCHE PRESENTATION

La couche présentation s'occupe de la syntaxe et de la sémantique des informations transportées en se chargeant notamment de la représentation des données.

La couche présentation permet à l'information envoyée par la couche application d'un système d'être lisible par la couche application d'un autre système. Si besoin est, la couche présentation traduit les différents formats de représentation des données en un format commun.

I-1-2-7-LA COUCHE APPLICATION

Cette couche a pour objectif de fournir des services aux utilisateurs d'un réseau. C'est elle qui contient l'application informatique (le programme) qui désire communiquer avec un ordinateur distant. C'est à ce niveau qu'on rencontrera des programmes transfert de fichiers, d'émulation de terminal, de soumission de travaux à distances, d'échange de courrier électronique, etc..

I-2 - RAPPEL SUR LE PROTOCOLE TCP/IP [MAN00]

Contrairement au modèle OSI, le modèle TCP/IP est né d'une implémentation ; la normalisation est venue ensuite. Cet historique fait toute la particularité de ce modèle, ses avantages et ses inconvénients.

TCP/IP est un protocole qui assure l'interconnexion et la communication entre des réseaux d'architecture différentes

Les rôles des différentes couches sont les suivants:

- **Couche accès réseau**: spécifie la forme sous laquelle les données doivent être acheminées quelque soit le type de réseau utilisé.
- **Couche Internet**: est chargée de fournir le paquet de données (datagramme).
- **Couche Transport**: assure l'acheminement des données, ainsi que les mécanismes permettant de connaître l'état actuel de la transmission.
- **Couche Application**: elle englobe les applications standard du réseau (Telnet, SMTP, FTP, ...).

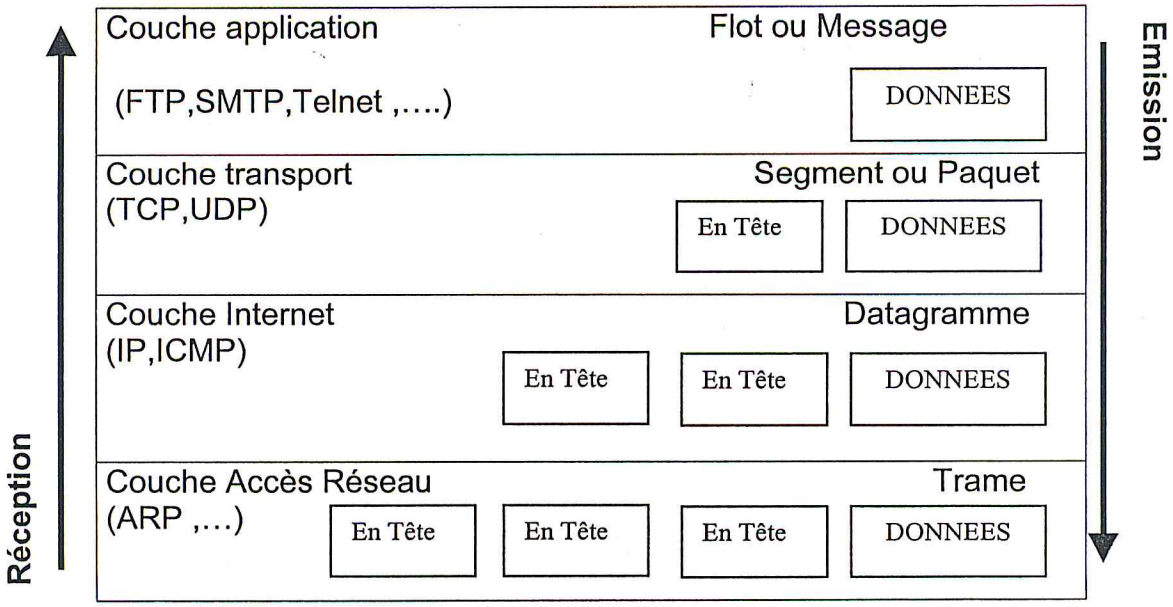


Figure I- 2 : Le modèle TCP/IP

Les principaux protocoles sont:

I-2-1- LE PROTOCOLE ARP [PIL02]

Le protocole ARP a un rôle phare parmi les protocoles de la couche Internet de la suite TCP/IP, car il permet de connaître l'adresse physique d'une carte réseau correspondant à une adresse IP, c'est pour cela qu'il s'appelle *Protocole de résolution d'adresse* (en anglais ARP signifie *Address Resolution Protocol*).

Ce problème est plus connu sous le nom de **problème de résolution d'adresse.**

Ainsi, pour faire correspondre les adresses physiques aux adresses logiques, le protocole ARP interroge les machines du réseau pour connaître leur adresse physique, puis crée une table de correspondance entre les adresses logiques et les adresses physiques dans une mémoire cache.

I-2-2- LE PROTOCOLE IP [PAS99][COM92]

Le protocole IP fait partie de la couche internet de la suite de protocoles TCP/IP. C'est un des protocoles les plus importants d'Internet car il permet l'élaboration et le transport des datagrammes IP (les paquets de données), sans toutefois en assurer la "livraison". En réalité le protocole IP traite les datagrammes IP indépendamment les uns des autres en définissant leur représentation, leur routage et leur expédition.

I-2-2-a) Adressage IP [PIL02]

Chaque machine du réseau Internet possède une adresse IP ,cette adresse a une longueur de 32 bits ,elle est divisée en deux parties

- Une partie réservée à l'identification du réseau.(netID)
- Une partie réservé à l'identification de la machine sur ce réseau.(host-ID)

Les adresses IP sont réparties en classes, c'est-à-dire selon le nombre d'octets qui représentent le réseau.

➢ ***Classe A***

les réseaux disponibles en classe A, sont les réseaux allant de **1.0.0.0** à **128.0.0.0**

➢ ***Classe B***

Les réseaux disponibles en classe B sont les réseaux allant de **128.0.0.0** à **191.255.0.0** .

➢ ***Classe C***

Les réseaux disponibles en classe C sont les réseaux allant de **192.0.0.0** à **223.255.255.0**

➢ ***Classe D***

Adresse de groupe (28 bits pour les hôtes appartenant au même groupe)

I-2-2-b) Masque de sous réseau [PUJ00]

On fabrique un masque contenant des "1" aux emplacements des bits que l'on désire conserver, et des "'0" pour ceux que l'on veut rendre égaux à zéro. Une fois ce masque créé, il suffit de faire un ET entre la valeur que l'on désire masquer et le masque afin de garder intacte la partie que l'on désire et annuler le reste.

Ainsi, un masque réseau se présente sous la forme de 4 octets séparés par des points (comme une adresse IP), il comprend (dans sa notation binaire) des zéros au niveau des bits de l'adresse IP que l'on veut annuler (et des 1 au niveau de ceux que l'on désire conserver).

L'intérêt d'un tel masque est de pouvoir connaître le réseau associé à une adresse IP . Le réseau est déterminé par un certain nombre d'octets de l'adresse IP (1 octet pour les adresses de classe A, 2 octets pour les adresses de classe B, et 3 octets pour les adresses de la classe C)

En généralisant, on obtient les masques suivants pour chaque classe:

- Pour une adresse de **Classe A** seul le premier octet nous intéresse, **255.0.0.0**

- Pour une adresse de **Classe B**, les deux premiers octets nous intéresse, **255.255.0.0**
- Pour une adresse de **Classe C** on s'intéresse aux trois premiers octets, **255.255.255.0**

I-2-2-c) Fragmentation des datagrammes IP [PUJ00]

La taille maximale d'une trame est appelée *MTU* (Maximum Transfer Unit), elle entraînera la fragmentation du datagramme si celui-ci a une taille plus importante que le MTU du réseau.

La fragmentation d'un datagramme se fait au niveau des routeurs, c'est-à-dire lors de la transition d'un réseau dont le MTU est important à un réseau dont le MTU est plus faible. Si le datagramme est trop grand pour passer sur le réseau, le routeur va le fragmenter, c'est-à-dire le découper en fragments de tailles inférieures au MTU du réseau et de telle façon que la taille du fragment soit un multiple de 8 octets.

Le routeur va ensuite envoyer ces fragments de manière indépendante et réencapsulée (il ajoute un en-tête à chaque fragment) de telle façon à tenir compte de la nouvelle taille du fragment, et en ajoutant des informations afin que la machine de destination puisse réassembler les fragments dans le bon ordre (rien ne dit que les fragments vont arriver dans le bon ordre étant donné qu'ils sont acheminés indépendamment les uns des autres...).

I-2-3-Protocole ICMP [RFC792]

Le protocole ICMP (Internet control and error message protocol) permet de gérer les informations relatives aux erreurs des machines connectées.

Étant donné le peu de contrôles que le protocole IP réalise ,il permet non pas de corriger ces erreurs mais de faire part de ces erreurs aux protocoles des couches voisines ; aussi ce protocole n'envoie pas d'accusé de réception

I-2-4-Le protocole UDP [PUJ00][TAN98]

Le protocole UDP (*User Datagram Protocol*) est un protocole non fiable et sans connexion. Son utilisation présuppose que l'on n'a pas besoin ni du contrôle de flux, ni de la conservation de l'ordre de remise des paquets.
Les messages UDP peuvent être perdus ,dupliqués ,remis hors séquence ou arrivés trop tôt pour être traités lors de leur réception.

UDP intervient lorsque le temps de remise des paquets est prédominant. Son principal avantage est l'exécution en un temps très court , qui permet de tenir compte des contraintes temps réel .
Les applications qui demandent ce protocole sont celles qui ne demandent pas un niveau de sécurité élevé ,ainsi que les logiciels qui demandent une interrogation rapide des ressources.

I-2-5-Le protocole TCP [PUJ00][TAN98]

Contrairement au protocole UDP ,TCP est dédié au transfert de gros volumes de données avec une remise fiable ,sans duplication et perte de paquets

Son rôle est de fragmenter le message à transmettre de manière à pouvoir le faire passer sur la couche internet.

A l'inverse, sur la machine destination, TCP replace dans l'ordre les fragments transmis sur la couche internet pour reconstruire le message initial

Lors d'une communication à travers le protocole TCP, les deux machines doivent établir une connexion. La machine émettrice (celle qui demande la connexion) est appelée **client** , tandis que la machine réceptrice est appelée **serveur** .

On dit qu'on est alors dans un environnement **client/ serveur** .

I-2-6-FTP (File Transfer Protocol)

Le protocole FTP a pour objectifs de :

- permettre un partage de fichiers entre machines distantes
- permettre une indépendance aux systèmes de fichiers des machines clientes et serveurs
- permettre de transférer des données de manière efficace.

Le protocole FTP s'inscrit dans un modèle client-serveur, c'est-à-dire qu'une machine envoie des ordres (le client) et que l'autre attend des requêtes pour effectuer des actions (le serveur)..

I-2-7- Le DNS (Domaine Name Service)

Comme vu précédemment ,les structures d'adresses sont complexes à manipuler , de par leur présentation en groupes de chiffres décimaux sous la forme abc.def.efg.hij avec une valeur maximum de 255 pour chacun des quatre groupes.

C'est la raison pour laquelle l'adressage utilise une structure hiérarchique , complètement différente ,beaucoup plus simple à manipuler et à mémoriser.

Le DNS est un modèle qui permet d'affecter des noms symboliques significatifs à de grands ensembles de machines. Le nom de domaine est composé de suite de composants significatifs (com,gov,..)séparés par un délimiteur :le point .

Pour la traduction d'un nom de domaine en adresse IP ,un client doit contacter un serveur de nom .

I-2-7-TELNET

Le protocole Telnet est un protocole standard d'Internet permettant l'interfaçage de terminaux et d'applications à travers Internet. Ce protocole fournit les règles de base pour permettre de relier un client (système composé d'un affichage et d'un clavier) à un interpréteur de commande (côté serveur).

Un programme client telenet permet de désigner une machine distante soit par son nom ou par son adresse IP . Le protocole Telnet repose sur trois services fondamentaux :

- Un terminal réseau virtuel (NVT),qui offre une interface normalisée aux systèmes distants ;
- Le principe d'options négociées entre le client et le serveur ;
- Les règles de négociation

Le reste des protocoles est abordé en annexe ainsi que le déroulement d'une connexion TCP.

Conclusion

Afin d'organiser les échanges au sein d'un réseau et permettre une compréhension commune , le modèle OSI qui forme la base de la communication inter machine, a été défini sous ses sept couches conceptuelles. De même, ce modèle a été le départ à l'apparition du protocole de communication TCP/IP , ce protocole a été défini dans son implémentation hiérarchique (couche par couche).

C'est sur cette base de protocoles que des réseaux de longue distance ont vu le jour, comme **"internet" .** Dans ces débuts ce type de réseau ne présentait pas de problème . puisqu'il était limité à un nombre restreint d'utilisateurs.

Dans le chapitre suivant, intitulé sécurité informatique et qui se devise en deux parties (risques , mécanismes), plusieurs menaces et attaques sont définies; ainsi que les techniques de sécurités adéquates.

CHAPITRE II

Sécurité Informatique

Le réseau d'entreprise est le centre nerveux de tout système d'information. Il s'articule autour de technologies TCP/IP, standard de fait adopté par tous. Les principes mêmes de TCP/IP sont basés sur des notions d'ouverture et de partage.

C'est d'ailleurs là un des points qui ont poussé à l'émergence de ces technologies. A l'instar d'autres technologies comme ATM, SNA, X25 qui supportent des outils permettant, à bas niveau, de filtrer les accès.

De fait, ces technologies demandent une attention toute particulière à l'aspect "sécurité" d'un réseau d'entreprise. Le partage de données sensibles, l'accès à des services internes, la diffusion de données parfois vitales pour l'entreprise, doivent être contrôlés et gérés avec des outils adéquats, par des hommes sensibilisés et compétents.

Par ailleurs, l'évolution progressive de l'informatique centralisée vers l'informatique distribuée; pose de nouveaux termes du problème de la sécurité.

II-1 - OBJECTIFS DE LA SECURITE INFORMATIQUE

Pour atteindre le niveau de sûreté requis, la sécurité informatique se fixe l'objectif suivant:

" Protéger les actifs informatiques de l'entreprise contre les risques et ça, d'une manière qui est adaptée à l'entreprise, à son environnement et à l'état de son outil informatique "[FLO96] FLORIN (~~the~~ tech de cyber)

Chaque aspect de cet objectif est couvert par une activité spécifique

Objectif:	**Ce qui implique :**
Protéger...	Conception, mise en œuvre, et maintenance des contre-mesures de sécurité
...les actifs informatiques de l'entreprise...	Identification des actifs informatiques (information, applications, systèmes, ressources humaines). Détermination de la valeur des actifs: • pour l'entreprise, et • pour les intrus potentiels
...contre les risques...	Identification des risques, ce qui implique l'identification des actifs vulnérables sur lesquels pèsent des menaces significatives
...et ça, d'une manière qui est adaptée à l'entreprise,...	Détermination du niveau de criticité des différents actifs informatiques. Détermination du meilleur équilibre entre risques et coût de protection
...à son environnement...	Identification des menaces: • internes et externes, • d'origine accidentelle ou intentionnelle
...et à l'état de son outil informatique.	Identification des vulnérabilités des actifs informatiques

Tableau II-1: Objectifs de la sécurité

les trois points clés de la sécurité informatique sont :

- ***Confidentialité*** *:* les données ne doivent pas être visibles aux personnes non autorisées.
- ***Intégrité*** : les données ne doivent pas subir de modification pendant leur transmission.
- ***Disponibilité*** : les données doivent être accessibles aux utilisateurs légitimes.

Avant la mise en place de tout système de sécurité, on doit d'abord identifier les menaces, et les types d'attaques qui pèsent sur le système informatique.

Les statistiques montrent que 60 % des incidents d'attaques et d'intrusions viennent de l'intérieur du réseau (dont 20 % non volontaires et 40 % volontaires) et 40 % de l'extérieur. Cela dit, la protection contre les attaques informatiques doit englober la totalité du réseau.

II-2-LES VULNERABILITES DES SYSTEMES INFORMATIQUES

II-2-1-DETOURNEMENT DE CLASSE D'ADRESSES INTERNET.

Voici, une attaque globale sur Internet qui permet de détourner toutes les connexions Internet d'une entreprise vers un réseau précis, celle-ci a déjà été mise en œuvre.

Le détournement de classe IP permet par exemple de "***re-router***" l'ensemble des paquets IP à destination d'une entreprise vers un réseau dit pirate.

Ce détournement permet des attaques de n'importe où dans le monde.
Sur Internet, chaque propriétaire des classes IP annonce aux réseaux où il est connecté qu'il est propriétaire et ensuite ces réseaux répercutent cette information en indiquant que pour aller vers ce réseau, les paquets peuvent utiliser ce réseau.

Ceci définit une route qui n'est ni plus ni moins que nos chemins définis par nos cartes routières.
Si des pirates décident de capturer l'ensemble des flux des emails et web d'une société, ceux-ci peuvent annoncer à partir de leur réseau la classe IP de leur victime. Lors de cette double propagation BGP (Border Gateway Protocol), le fait d'avoir une classe IP annoncée par deux réseaux. [BGP 02] [PUJ 00] ,distincts, sera assimilé à un réseau connecté à Internet par deux providers, considéré comme un AS (Autonomous System), les routeurs envoient les paquets vers le réseau qui est le plus proche.

Donc, pour une partie du monde, l'ensemble des communications sera redirigé vers le réseau pirate, puis, dans l'autre partie du monde, les communications iront vers le réseau « officiel ».

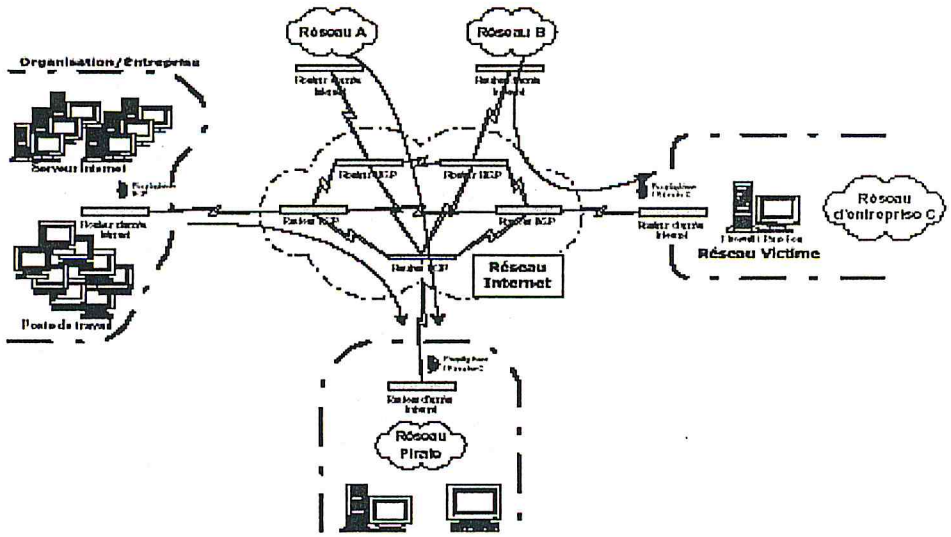


Figure II-1: Action entraînées par une double propagation BGP effectuée par un réseau pirate [BGP02]

II-2-2- ECOUTE PASSIVE :

L'écoute passive est un type d'attaque contre la confidentialité, qui consiste à accéder sans modification aux informations qui sont générées, transmises, stockées ou affichées dans des composants vulnérables du SI (voies de communication, périphériques tels que les écrans de terminaux, les claviers ou les imprimantes, les mémoires et les disques).

La méthode de prélèvement varie suivant le type du réseau (branchement sur une ligne de transmission, capture des signaux hertziens, analyse de rayonnement ...), l'information n'est pas altérée par celui qui en prélève une copie. Ces attaques sont donc indétectables par le système.

II-2-3- LE "SNIFFING" DES PAQUETS, OU INTERCEPTION DES DONNEES

La plupart des réseaux locaux utilise la technologie du "*broadcasting*". Chaque message (ou "paquet" contenant les adresses de l'expéditeur et du destinataire), qu'un ordinateur transmet sur le réseau, peut être lu par n'importe lequel d'entre eux. Ceux à qui le message n'est pas destiné l'ignoreront. Certains ordinateurs sont programmés pour contrôler chacun des messages qui transite.

Sur le réseau étendu , un paquet IP, ou datagramme, transite d'un site à l'autre jusqu'à ce que sa destination finale soit atteinte. Le fait qu'un paquet

soit adressé à un autre site, ou nœud de réseau, n'empêche pas que son contenu ne soit examiné en route. On n'a même aucun moyen d'être sûr que le paquet envoyé a bien été reçu par son destinataire, ni que le paquet reçu soit le même que celui qui a été envoyé.

D'ailleurs, Il existe des outils logiciels qui surveillent et identifient le trafic de paquets ; afin de capturer des *logins* et des *mots de passe* pour être utilisés ultérieurement.

De même, cet outil peut aussi être utilisé légalement par le personnel d'opération et de maintenance du réseau pour résoudre les problèmes liées à ce dernier.

II-2-4-IP SPOOFING : [ETH02]

La mascarade d'adresse *IP* ou *spoofing* permet à une machine du réseau extérieur de se faire passer pour une machine du réseau intérieur et ainsi de profiter de tous ses droits. Pour atteindre ce but, l'attaquant donne à son ordinateur l'adresse *IP* d'une machine appartenant au réseau interne.

Remarque : Le site interne peut aussi donner des droits à un site externe dit *"ami"*. L'attaquant pourra alors se faire passer pour l'une des machines externes du site ami.

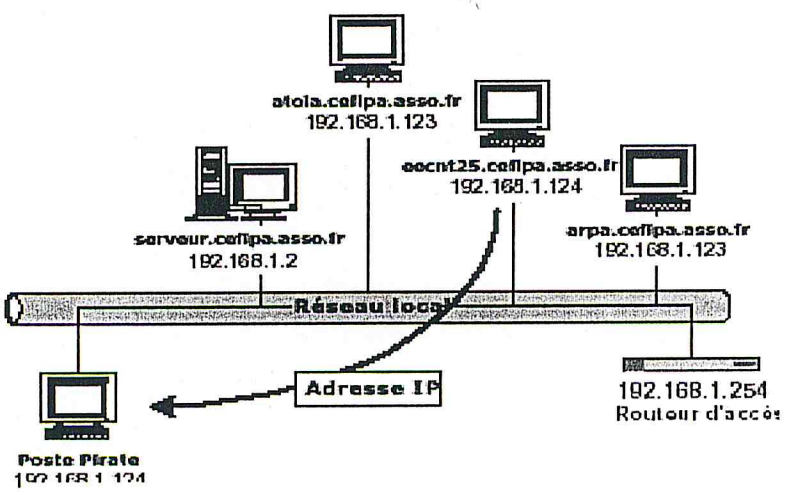


Figure II-2: Spoofing IP [YAY02]

II-2-5-FALSIFICATION DES ADRESSES MAC / ARP SPOOFING

Dans l'attaque précédente, on a vu une parade par duplication d'adresse IP. Pour ceci, il suffisait de créer une liste de références entre les adresses MAC des cartes réseaux et les adresses IP.

Les adresses MAC sont uniques et inscrites dans la carte réseau par le constructeur.

Normalement, il est impossible de changer cette adresse qui est envoyée dans chaque trame réseau. Mais on peut observer que dans la plupart des algorithmes des systèmes d'exploitation d'envoi de trames réseaux, le système d'exploitation fait une requête à la carte réseau, puis place l'adresse MAC en mémoire, et ensuite constitue les trames réseaux en fonction de cette adresse en mémoire et des données à envoyer.

A partir du moment où cette adresse est stockée en mémoire, il est simple dans le cas d'un système d'exploitation dont on a les sources, de modifier celles-ci afin de déclarer l'adresse MAC que l'on souhaite en dur dans le système. Dans ce cas, le système demande l'adresse MAC, mais celle-ci n'est pas modifiée en mémoire car elle est définie comme une déclaration système.

Donc, à partir de ce moment, il n'y a plus aucun moyen de différencier, au niveau du réseau local, la station pirate de la station victime.
Ce genre de manipulation est rendu réalisable uniquement sur les systèmes d'exploitation libres tels que FreeBSD, OpenBSD, ou Linux, car ces systèmes d'exploitation fournissent leurs sources…

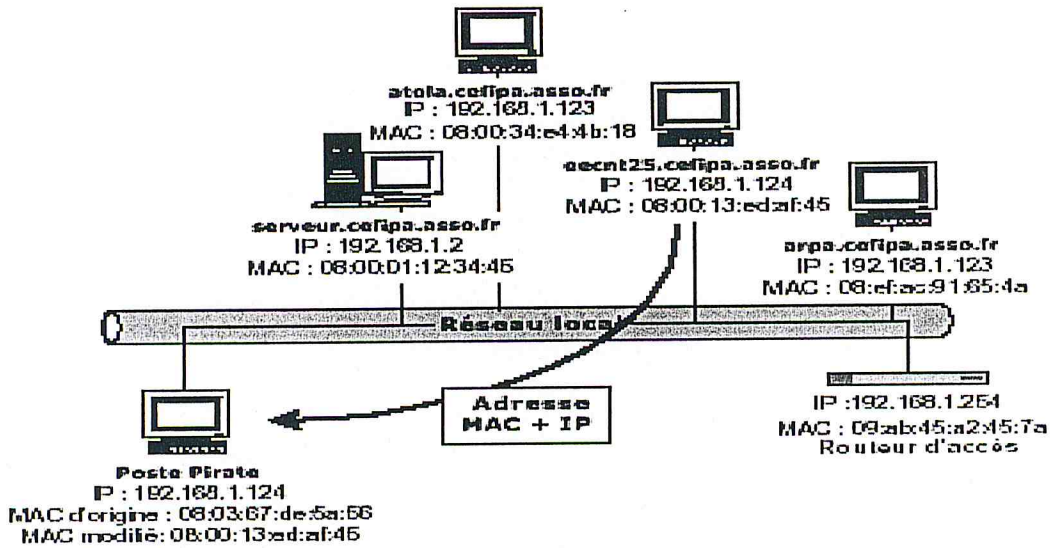


Figure II - 3: Spoofing ARP [YAY02]

Lorsque le poste falsifie son adresse MAC, celui-ci ne peut émettre et récupérer des trames sans avoir aucune possibilité de contrôle sur l'auteur exact des trames.

Afin de contrer ces attaques, une solution est possible sur les architectures des réseaux évoluées.
On ajoute à la liste IP-MAC, le lieu de connexion de la machine, c'est-à-dire le port de connexion sur l'équipement réseau.
On suppose que cette attaque est distante, donc celle-ci ne pourra que ce faire en utilisant un autre port de l'équipement réseau interconnectant les stations.

Donc on utilisera une base de données de contrôle au niveau du commutateur contenant IP, MAC, port de connexion.

Pour mettre en œuvre une attaque ARP Spoofing, on peut utiliser un générateur de paquet ARP comme arpspoof [APF 02].

Exemple: Soit la machine victime 10.0.0.171, sa passerelle par défaut 10.0.0.1 et la machine du pirate 10.0.0.227.

Avant l'attaque un traceroute donne comme résultat :

```
[root@cible -> ~]$ traceroute 10.0.0.1
traceroute to 10.0.0.1 (10.0.0.1), 30 hops max, 40 byte packets
 1  10.0.0.1  (10.0.0.1)  1.218 ms  1.061 ms  0.849 ms
```

Et le cache ARP de la machine cible est :

```
[root@cible -> ~]$ arp
Address      HWtype     HWAddress          Flags Mask  Iface
10.0.0.1     ether      00:b0:c2:88:de:65  C           eth0
10.0.0.227   ether      00:00:86:35:c9:3f  C           eth0
```

Le pirate lance alors arpspoof :

```
[root@pirate -> ~]$ arpspoof -t 10.0.0.171 10.0.0.1
0:0:86:35:c9:3f 0:60:8:de:64:f0 0806 42: arp reply 10.0.0.1 is-at 0:0:86:35:c9:3f
0:0:86:35:c9:3f 0:60:8:de:64:f0 0806 42: arp reply 10.0.0.1 is-at 0:0:86:35:c9:3f
0:0:86:35:c9:3f 0:60:8:de:64:f0 0806 42: arp reply 10.0.0.1 is-at 0:0:86:35:c9:3f
0:0:86:35:c9:3f 0:60:8:de:64:f0 0806 42: arp reply 10.0.0.1 is-at 0:0:86:35:c9:3f
0:0:86:35:c9:3f 0:60:8:de:64:f0 0806 42: arp reply 10.0.0.1 is-at 0:0:86:35:c9:3f
0:0:86:35:c9:3f 0:60:8:de:64:f0 0806 42: arp reply 10.0.0.1 is-at 0:0:86:35:c9:3f
0:0:86:35:c9:3f 0:60:8:de:64:f0 0806 42: arp reply 10.0.0.1 is-at 0:0:86:35:c9:3f
```

Les paquets envoyés sont des paquets ARP empoisonnant le cache ARP de la machine 10.0.0.171 avec des ARP Reply indiquant que l'adresse MAC associée à 10.0.0.1 est maintenant 00:00:86:35:c9:3f.

Désormais, le cache ARP de la machine 10.0.0.171 est :

```
[root@cible -> ~]$ arp
Address          HWtype     HWAddress          Flags Mask  Iface
10.0.0.1         ether      00:00:86:35:c9:3f  C           eth0
10.0.0.227       ether      00:00:86:35:c9:3f  C           eth0
```

Pour vérifier que le trafic passe maintenant par la machine 10.0.0.227 il suffit de faire un nouveau traceroute vers la passerelle 10.0.0.1 :

```
[root@cible -> ~]$ traceroute 10.0.0.1
traceroute to 10.0.0.1 (10.0.0.1), 30 hops max, 40 byte packets
 1  10.0.0.227  (10.0.0.227)  1.712 ms  1.465 ms  1.501 ms
 2  10.0.0.1  (10.0.0.1)  2.238 ms  2.121 ms  2.169 ms
```

L'agresseur est désormais capable de sniffer le trafic de la machine 10.0.0.171 vers 10.0.0.1. Il ne faut pas qu'il oublie d'activer le routage IP sur sa machine 10.0.0.227 (avec l'IP Forwarding - activer la clé > net.ipv4.ip_forward dans /etc/sysctl.conf).

II-2-6-ATTAQUE PAR SATURATION DE LA BANDE PASSANTE DES LIAISONS INTERNET

Voici une attaque très connue sur Internet. Elle est très simple. Les tuyaux de connexion à Internet ont une certaine dimension, donc une capacité.

Afin de mettre hors service un accès à une entreprise, il suffit de prendre plusieurs machines sur Internet avec un accès à très haut débit. Il suffit de lancer un programme en boucle qui effectue de nombreuses requêtes sur n serveurs de l'entreprise cible. Au bout de quelques secondes, ces requêtes saturent la liaison Internet de l'entreprise cible, ce qui met hors-service l'ensemble de ses connexions Internet.

Il existe peu de moyen pour filtrer ce type d'attaque. S'il s'agit de requêtes formelles sur des serveurs, on peut utiliser des systèmes de gestion de bande passante, mais s'il s'agit d'overflow par demande de connexion, la ligne spécialisée vers Internet ainsi que les routeurs d'accès ne peuvent pas contenir et répondre aux multiples demandes de connexions.

II-2-7-ATTAQUE PAR OVERFLOW DE SERVICE TCP

Cette attaque est similaire à la précédente, sauf qu'elle joue simplement sur la capacité d'un serveur à fournir des connexions de type TCP. Normalement un serveur non modifié est capable de fournir 65535 connexions TCP. Donc en utilisant

quelques machines sur Internet, on fait établir le nombre maximal de connexions aux serveurs cibles, ce qui ne laisse plus de place pour les requêtes dites standard.

Il y a eu des attaques sur de nombreux sites de recherche (Yahoo), la technique était similaire à celle exposée, sauf que pour ces sites, les serveurs web ferment très rapidement les connexions TCP.

Afin de faire tenir plus longuement les connexions en erreur ou de saturer les serveurs, les agresseurs utilisent des requêtes formées d'adresses Internet non-utilisées, donc sans réponse. Lors de la requête, la connexion s'établie, le serveur cible génère une trame pour le contrôle de connexion.
Celle-ci ne parvient jamais à son destinataire car il n'existe pas, donc pour que la connexion du serveur se ferme, il faudra qu'il attende les "time out" (temps avant fermeture de la connexion).

Il suffisait donc de générer n fois le nombre de serveurs, n*65535 requêtes toutes les 120 secondes (timeout) au minimum.

II-2-8-Les dénis de services réseaux

Il existe différents types de dénis de services utilisant les spécificités des protocoles de la pile TCP/IP.

- ***SYN Flooding***

Nous avons vu qu'une connexion TCP s'établie en trois phases. Le SYN Flooding exploite ce mécanisme, les trois étapes sont l'envoi d'un SYN, la réception d'un SYN-ACK et l'envoi d'un ACK.

Le principe est de laisser sur la machine cible un nombre important de connexions TCP en attentes. Pour cela, le pirate envoie un très grand nombre de demandes de connexions (flag SYN = 1), la machine cible renvoie les SYN-ACK en réponse au SYN reçus. Le pirate ne répondra jamais avec un ACK, et donc pour chaque SYN reçu la cible aura une connexion TCP en attente. Etant donné que ces connexions semi-ouvertes consomment des ressources mémoires au bout d'un certain temps la machine est saturée et ne peut plus accepter de connexion.

Ce type de déni de service n'affecte que la machine cible.
Le pirate utilise un SYN Flooder comme synk4 [SNK 02], en indiquant le port TCP cible et l'utilisation d'adresses IP source aléatoire pour éviter toute identification de la machine du pirate.

- ***UDP Flooding***

Ce déni de service exploite le mode non connecté du protocole UDP. Il crée un «UDP Packet Storm »
(génération d'une grande quantité de paquets UDP), soit à destination d'une machine, soit entre deux machines.

Une telle attaque entraîne une congestion du réseau ainsi qu'une saturation des ressources des hôtes victimes. La congestion est plus importante du fait que le trafic UDP est prioritaire sur le trafic TCP.

En effet, le protocole TCP possède un mécanisme de contrôle de congestion, dans le cas où l'acquittement d'un paquet arrive après un long délai, ce mécanisme adapte la fréquence d'émission des paquets TCP, le débit diminue.

Le protocole UDP ne possède pas ce mécanisme. Au bout d'un certain temps le trafic UDP occupe donc toute la bande passante n'en laissant qu'une infime partie au trafic TCP.

L'exemple le plus connu d'UDP Flooding est le « Chargen Denial of Service Attack ».
La mise en pratique de cette attaque est simple, il suffit de faire communiquer le service chargen d'une machine avec le service echo d'une autre. Le service chargen génère des caractères tandis que echo se contente de réémettre les données qu'il reçoit. Il suffit alors au pirate d'envoyer des paquets UDP sur le port 19 (chargen) à une des victimes en spoofant l'adresse IP et le port source de l'autre (dans ce cas le port source est le port UDP 7 pour echo).

L'UDP Flooding entraîne une saturation de la bande passante entres les deux machines. Un réseau complet peut donc être victime d'un UDP Flooding.

- ***Smurfing***

Cette attaque utilise le protocole ICMP. Quand un ping (message ICMP ECHO) est envoyé à une adresse de broadcast (par exemple 10.255.255.255), celui-ci est démultiplié et envoyé à chacune des machines du réseau.

Le principe de l'attaque est de spoofer les paquets « ICMP ECHO REQUEST» envoyés en mettant comme adresse IP source, celle de la cible. Le pirate envoie un flux continu de ping vers l'adresse de broadcast d'un réseau et toutes les machines répondent alors par un message « ICMP ECHO REPLY » en direction de la cible.
Le flux est alors multiplié par le nombre d'hôte composant le réseau. Dans ce cas, tout le réseau cible subira le déni de service, puisque l'énorme quantité de trafic généré par cette attaque entraîne une congestion du réseau.

Faire la sécurité d'un réseau consiste à : s'assurer que celui qui consulte ou modifie des données du système, en a l'autorisation et qu'il peut le faire correctement car le service est disponible.

Les entreprises possèdent des informations sensibles et des secrets industriels. La circulation de ce type de données sur les réseaux doit être protégé exactement comme des actifs de valeurs. [KAR 96]

La première étape de conception d'un système de sécurité est bien la définition d'une politique de sécurité, viendra ensuite le choix des techniques appropriées.

II-3- ETABLISSEMENT D'UNE POLITIQUE DE SECURITE :

Définition :

Les politiques de sécurité sont des règles électroniques programmées et stockées dans un dispositif de sécurité destinées à contrôler des aspects comme les droits d'accès.

Ces politiques de sécurité sont, également des règlements écrits ou oraux régissant le fonctionnement d'une société. De plus, les sociétés doivent désigner le responsable de l'application et de la gestion de ces politiques et déterminer le mode d'information des employés à propos des règles et des protections.[CIS 03]

Avant toute mise en œuvre d'une politique de sécurité de réseau, il faudra étudier et répondre à un ensemble de questions tel que :

1. quelles ressources faut il protéger ?
2. contre qui faut il se protéger ?
3. qu'elle est l'importance d'une ressource ?
4. qu'elle sont les mesures qui vont être prises pour protéger les actifs de manière rentable et dans des délais corrects ?
5. comment faire une « révision » périodique de la politique ,pour détecter l'évolution de la situation par rapport aux objectifs. [TAR 96]

la politique de sécurité se compose d'éléments, qu'utilisateurs et administrateurs vont trouver acceptables et désireux d'appliquer.

II-3-1- Politique de sécurité de site

Un site est définie comme une partie quelconque d 'une entreprise possédant des ordinateurs et des ressources reliées entre elles par un réseau.

Par ressources on entend entre autres :

- Station de travail
- Ordinateur hôte et des serveurs
- Dispositif d'interconnexion :Routeurs, pont ,..etc
- Serveur de terminaux
- Logiciels de réseaux et applicatifs
- Câble de réseaux
- Fichiers et base de données

C'est la protection de l'ensemble des ces ressources, que la politique de sécurité doit prendre en compte.

Si le site est connecté à d'autres réseaux, la politique de sécurité du site doit prendre en compte, des besoins en matière de sécurité et des exigences de tous les réseaux connectés entre eux.

II-3-2- L'approche de la politique sécurité

Le choix d'une approche de sécurité, détermine si la sécurité du réseau nécessite de : *ne rien autoriser, n'autoriser que, autoriser tout sauf, ou tout autoriser.*

II-3-3- Mise en place des responsabilités

Pour que la politique de sécurité de réseau fonctionne, il faut que chaque utilisateur connaisse sa responsabilité par rapport à cette politique.

Par exemple :
Chaque utilisateurs du réseau doit être responsable de son mot de passe
Les administrateurs de réseaux et les responsables systèmes sont responsables de la maintenance de la sécurité du réseau.

II-4-TECHNIQUES DE SECURITE

II-4-1-La cryptographie

Depuis Jules César, qui a été sans doute le premier a l'avoir utilisé pour communiquer avec ses troupes, jusqu'à l'armée allemande qui s'est servie de machines électromécaniques lors de la deuxième guerre mondiale, la cryptographie a fait d'énormes progrès avec l'arrivée de l'informatique.

Car la cryptographie se sert de la puissance des ordinateurs et des progrès mathématiques pour rendre tout message incompréhensible par un tiers.

Définition *: La cryptographie*

Le *cryptage* se définit comme le processus permettant de coder un message afin de le rendre sans signification, et de rendre l'information brouillée. Le décryptage est le processus inverse.

Les termes *codage*, *chiffrement* et *cryptage* sont régulièrement substitués les uns aux autres.

La cryptographie répond à différents besoins **:** [VIV 97].

- **La confidentialité** : qui consiste à rendre l'information inintelligible à tous ceux qui pourraient intercepter le message.

- **Le contrôle d'accès** : qui permet de limiter l'accès aux données, serveurs aux personnes autorisées (mot de passe Unix, par exemple).
- **L'intégrité des données** : qui consiste à vérifier que cette donnée n'a pas été altérée frauduleusement.
- **L'identification** : qui permet d'assurer de l'authentification des partenaires et de l'origine des messages.
- **La non répudiation** : pour que les partenaires ne puissent nier le contenu des informations.

II-4-1-1- *Terminologie de la cryptographie* [SCH97]

Un message est appelé ***texte en claire***. le processus de transformation d'un message de telle manière à le rendre incompréhensible est appelé ***chiffrement*** (ou ***encryption***).

Le résultat de ce processus de chiffrement est appelé ***texte chiffré***(ou ***cryptogramme***).Le processus de reconstitution du texte en clair a partir du texte chiffré est appelé ***déchiffrement (décryptage).***

Le *message clair* est noté « **M** » et le *message chiffré* est noté **"C"**. l'algorithme de codage ou de cryptage est noté « **E** », et pour la fonction inverse (le déchiffrement) cette dernière est notée **"D"** .

C = E(P) et P = D(C), soit P = D(E(P)).

Figure II-4-Cryptage de message

Pour une vraie sécurité , tous les algorithmes modernes de chiffrement utilisent une **clef,** notée **K,** on obtient C = E(K,M) .

Il y a deux principaux algorithmes à base de clefs :à ***clef secrète*** ou à ***clef publique***

II-4-1-2-*La cryptographie symétrique*

ou a *clef secrète* : la même clef (le code secret) est utilisée pour décrypter l'information. Le problème de cette méthode est qu'il faut trouver le moyen de transmettre de manière sécurisée la clef à son correspondant.

Figure II.5 : *Algorithmes symétriques*

II-4-1-3- *La cryptographie asymétrique*

ou a *clef publique* : ce n'est pas la même clef qui crypte et qui décrypte les messages. L'utilisateur possède une clef privée et une clef publique. Il distribue sa clef publique et garde secrète sa clef privée. Dans ce type d'application, tout le monde peut lui écrire en utilisant la clef publique, mais seul l'utilisateur destinataire pourra décrypter et donc lire le message avec sa clef privée. [VIV 97]

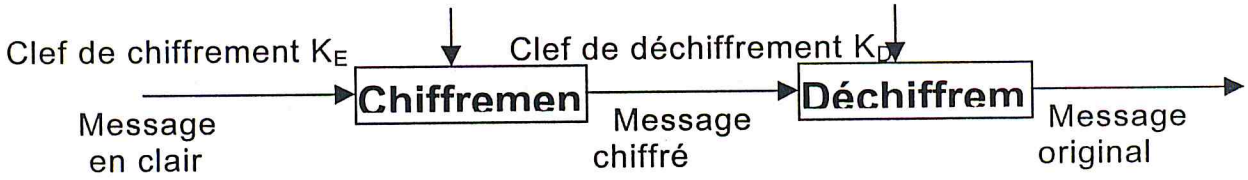


Figure II-6- Cryptographie à clef publique

II-4-2-LES ALGORITHMES DE CRYPTAGE

II-4-2-1- Systèmes à clef secrète

Parmi les algorithmes les plus connus et utilisés et qui se basent sur ce système à clef secrète : l'algorithme *DES (Data Encryption Standard).*

DES (Data Encryption Standard).[BAY02] [SCH97]

Jusque dans les années 1970, seuls les militaires possédaient des algorithmes à clef secrète fiables. Devant l'émergence de besoins civils, le NBS (*National Bureau of Standards*) lança le 15 mai 1973 un appel d'offres dans le Federal Register (l'équivalent du Journal Officiel américain) pour la création d'un système cryptographique.

Les efforts conjoints d'IBM, qui propose Lucifer fin 1974, et de la NSA (*National Security Agency*) conduisent à l'élaboration du DES (*Data Encryption Standard*), l'algorithme de chiffrement le plus utilisé au monde durant le dernier quart du XXiè siecle.

Le chiffrement DES a un niveau de sûreté uniquement lié à la clef, et non à la confidentialité de l'algorithme.

Le DES est un système de chiffrement par bloc ; il chiffre les données par bloc de 64 bits.

La clef du DES est une chaîne de 64 bits (succession de 0 et de 1), mais en fait seuls 56 bits servent réellement à définir la clef. Les bits 8,16,24,32,40,48,56,64 sont des bits de parité

Un bloc de 64 bits du texte clair entre par l'algorithme et un bloc de 64 bits de texte chiffré en sort. L'algorithme est relativement simple puisqu'il combine des permutations et des substitutions. On parle en cryptologie de techniques de confusion et de diffusion.

- *La diffusion*: l'information contenue dans le texte clair doit être répartie dans l'ensemble du texte codé. De ce fait, un changement dans le texte clair affecte de nombreuses parties du texte crypté.

- *La confusion*: cette notion recouvre le fait qu'un intercepteur ne doit pas être capable de prédire ce qu'un changement de symbole dans le texte clair affectera dans le texte codé. La relation entre le message crypté et la paire clef / message clair doit être complexe.

II-4-2-2- Systèmes à clef publique [FLO96]

Contrairement au système à clef secrète où une seule clef est utilisée pour le cryptage et le décryptage, les systèmes à clef publique font appel à deux clefs. Les deux clefs sont différentes mais liées par des propriétés et il est nécessaire que la clef de décryptage ne puisse pas être déterminée à partir de l'algorithme de codage et de la clef de cryptage.

Les deux termes *clef publique / clef privée* caractérisent ce système ; la clef publique est associée à la clef qui sera utilisée pour le cryptage, et est distribuée ou mise à disposition de l'ensemble des utilisateurs. L'autre clef (*clef privée*), est gardée secrète par un des utilisateurs pour décrypter les messages cryptés reçus.

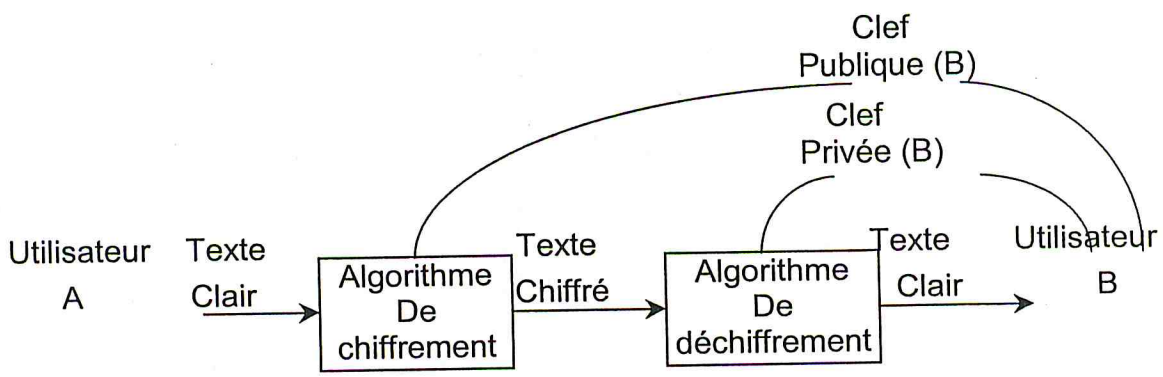


Figure II.6 : *Système à clef publique*

Le plus célèbre des algorithmes de cryptage à clef publique est bien le cryptage RSA

II-4-2-2- a) Cryptage de Rivest-Shamir-Adelman RSA [RSA02]

RSA est le plus célèbre et le plus répandu des algorithmes asymétriques. Il a été inventé en 1977 par Ron Rivest, Adi Shamir et Leonard Adleman.

Le cryptage *RSA* est un algorithme à clef publique qui a la propriété que n'importe laquelle des deux clefs de la paire peut être utilisée pour coder le message, tant qu'on utilise l'autre clef pour le décoder et cela sans rendre les deux clefs publiques.

Caractéristiques :

- Le *RSA* est un cryptage par bloc dans lequel les messages (blocs) sont des entiers compris entre *0* et *n-1* pour un certain *n*.
- Deux clefs *e* et *d* (utilisées respectivement pour le cryptage et le décryptage). Le texte clair *P* sera codé de la manière suivante: $P^e \bmod n$.
- Afin de pouvoir déchiffrer le message, on choisit *d* de telle manière que: $(P^e)^d \bmod n = P$.
- Le cryptage et le décryptage sont mutuellement commutatifs, soit: $P = (P^e)^d \bmod n = (P^d)^e \bmod n$.

II-4-3 DISTRIBUTION DE CLEFS [VAN97]

De nombreux protocoles ont été développés pour la distribution de clefs. Ils dépendent du type de clef, ainsi que de la quantité d'information déjà détenue par l'émetteur et le récepteur.

a) Echange de clef symétrique:

La communication entre deux utilisateurs est possible dés qu'ils auront une copie de la clef symétrique *K*.

Par souci de sécurité, les utilisateurs peuvent changer de clef tous les X temps ; Pour cela, une des deux entités va générer une clef K_{NEW} qu'elle va envoyer cryptée par la clef de base à l'autre utilisateur : $E(K_{NEW}, K)$.

Des termes génériques ont été inventés pour décrire de tels systèmes. La clef *K* est appelée *clef maîtresse*, alors que K_{NEW} est appelée *clef de trafic* ou *clef de session*.

Ce système nécessite $n(n+1)/2$ clefs pour un ensemble de *n* utilisateurs.

b- Echanges de clefs symétriques avec serveur:

Les deux utilisateurs peuvent faire appel à un service central de distribution de clefs.

Au départ, le nombre de clefs est réduit (une par utilisateur, pour communiquer avec le serveur). En Supposant que les deux utilisateurs (A et B) veulent communiquer, mais qu'ils ne possèdent pas de clef commune. Cependant, ils partagent chacun une clef avec le serveur soit K_A et K_B. On aura alors le scénario suivant :

A envoie un message au serveur contenant son identificateur, l'identificateur de B et un identificateur de son message soit *(idA, idB,* I_A *)*.

Ce message n'a pas besoin d'être crypté car qu'importe l'essai d'intrusion, il pourra être détecté par la suite.

Le centre de distribution va générer une nouvelle *clef de session* (K_{AB}) et envoyer à A le message crypté (avec la clef K_A) suivant:

$E((I_A, idB, K_{AB}, E((K_{AB}, idA), K_B)), K_A)$.

En décryptant ce message au moyen de K_A , A obtient l'identificateur de message et le destinataire, qui lui permettent de faire certains types de vérifications. Il obtient également la *nouvelle clef de session* ainsi qu'une chaîne qu'il ne sait décoder, mais qu'il va envoyer à B.

Par contre B est capable de décoder cette chaîne car elle est crypté avec la clef privée qu'il partage avec le serveur soit K_B . En décodant le message reçu, il découvre l'identité de l'émetteur ID_A ainsi que la *clef de session*: K_{AB} .

c) Echanges de clefs asymétriques:

Utiliser des techniques symétriques permet de réduire le nombre de clefs mais également augmente la vulnérabilité. Si la clef est connue, le système de transmission est évident.

Dans le systèmes à clefs asymétriques, la connaissance de la clef privée est strictement réservée aux utilisateurs.

Dans de nombreux cas, les algorithmes asymétriques sont considérés comme trop lents. D'où, la préférence d'utiliser les techniques asymétriques uniquement pour protéger l'échange d'une clef symétrique, qu'un des deux utilisateurs aurait générée et qu'ils utiliseront pour le restant de la communication.

d- Echanges de clefs asymétriques avec serveur:

Soient deux utilisateurs n'ayant aucune connaissance commune, possédant une *clef privée* (D_A et D_B) chacun, et voulant communiquer entre eux via un serveur possédant lui aussi une *clef privée* (D_S) et qui a diffusé sa *clef publique* (E_S).

L'utilisateur voulant initier la communication va envoyer une demande au serveur en spécifiant le doublet émetteur-récepteur: *(A,B)* ; Le serveur lui renvoie $D_S(E_B, B)$.

L'utilisateur A possède maintenant la *clef publique* associée à la *clef privée* de B. Il va pouvoir communiquer avec lui. Si l'utilisateur B veut lui répondre, il devra demander la *clef publique* associée à la *clef privée* de A au serveur de la même manière.

II-4-3 - Notion de certificat [VAN97]:

L'utilisation d'un serveur pour chaque transfert de message le rend encombré. C'est pourquoi *Kohnfelder* a développé la notion de certificat. Ces certificats permettent à des entités d'échanger des clefs sans devoir passer par un tiers et d'une manière aussi sûre.

Chaque certificat contient une *clef publique* ainsi qu'un *identificateur* de personne lié à la *clef publique*. Pour lancer le système, chaque utilisateur fait appel au tiers, en demandant qu'il lui crée un certificat. Le tiers va générer un certificat pour chaque utilisateur et le lui renvoyer, crypté au moyen de la *clef privée* du tiers. Soit, avec *l'identificateur* de l'utilisateur, E_X sa *clef publique* et D_S la *clef privée* du serveur. Chaque utilisateur reçoit: $D_S(E_X, ID_X)$

Qu'il peut décrypter, car la clef publique du serveur E_S est connue de tous.

Pour communiquer avec un autre utilisateur on doit avoir son certificat. Si cette personne nous envoie son certificat, on peut vérifier qu'il provient bien du tiers qui fournit les certificats en le décodant au moyen de la *clef publique* E_S. Ensuite, à l'intérieur du certificat, on découvre la *clef publique* du correspondant ainsi que son *identificateur.*

II.4.4 La signature numérique [SCH97, FLO96]

La cryptographie asymétrique permet de signer numériquement des messages. Une *Signature numérique* s'obtient par l'inversion de la technique de cryptographie asymétrique à clef publique. Elle permet de garantir l'intégrité et l'origine d'un message, ce qui fait de cette technique une méthode efficace contre la *non répudiation.*

Exemple : *Signature numérique*

Soit un utilisateur A qui va chiffrer son message avec sa clef privée et l'envoie à B.

B reçoit le message de A et le déchiffre avec la clef publique de A.
Il est à noter que n'importe qui peut lire des messages de A s'il détient sa clef publique. Par contre, seul A peut avoir écrit ce message car lui seul possède la clef privée (théoriquement). La *Signature numérique* s'attache surtout à garantir l'origine du message et non sa confidentialité.

III- 4- 5 - Authentification :

L'authentification fournit l'assurance que l'entité (utilisateurs, machine, ...) demandant un accès est bien l'entité qu'elle prétend être. [CAT96]

Car, la sécurité doit être également basée sur une authentification certaine de l'utilisateur et non en faisant confiance aux adresses IP tel qu'on procède dans les systèmes par filtrage de paquets. Les utilisateurs extérieurs doivent posséder "quelque chose" (Jeton de sécurité ou carte intelligente (smart card)) et connaître "quelque chose" (Numéro personnel d'identification) unique à chaque individu.

Car faire confiance aux adresses IP de machines sur un réseau externe est extrêmement dangereux, puisque, ces machines connues peuvent subir une intrusion.

On peut distinguer deux classes d'authentification :

- Authentification de message.
- Authentification des utilisateurs.

III-4-5-1- Authentification de message *:* [VAN97]

L'authentification des messages est une procédure qui permet de vérifier qu'un message n'a pas été transformé au cours de son transfert, et permet même d'assurer sa confidentialité et la non répudiation.

Dans cette classe on trouve :

a. Cryptage de message:

Le cryptage de message peut être vu comme une mesure d'authentification. On distingue deux cas en cryptage de message :

- *Système à clef secrète :* sans connaître la *clef secrète,* le message ne subit pas de changement ; d'où l'authentification sera assurée ; si ce n'est pas le cas et que n'importe quelle séquence peut survenir, alors, l'authentification n'est pas assurée.

- *Système à clef publique :* L'utilisation directe de ce système ne fournit pas d'authentification directe. Puisque n'importe qui peut utiliser la *clef publique* de l'un des deux utilisateurs pour coder un message destiné à l'autre, il n'y aura pas d'authentification possible.

Par contre, si l'un des utilisateurs (A) crypte son message au moyen de sa *clef privée* D_A. Le deuxième (B) utilisera la clef publique correspondante soit E_A pour décoder le message qui ne pourra provenir que de A vu qu'il est le seul à pouvoir crypter le message. Ceci est résumé de la manière suivante :

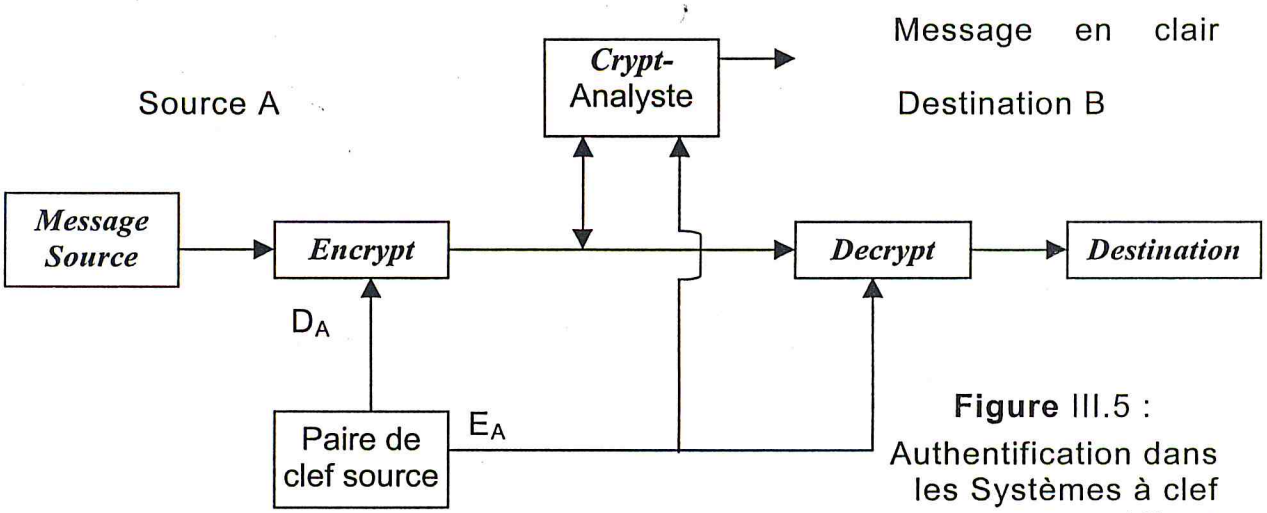


Figure III.5 : Authentification dans les Systèmes à clef publique

Par contre, en présence de la cryptanalyse , et à partir du texte chiffré (crypté) et de la clef publique de la source, le chiffrement peut être cassé, et le texte original peut être reconstitué. L'authentification dans ce cas est assurée, mais la confidentialité ne l'est pas ; Puisque une tierce partie peut exister.[TER96]

Si on veut obtenir la confidentialité ainsi que l'authentification, il faudra passer par deux boucles de cryptage. En cryptant le message en premier avec la *clef privée* de la source et le résultat avec la *clef publique* du destinataire,

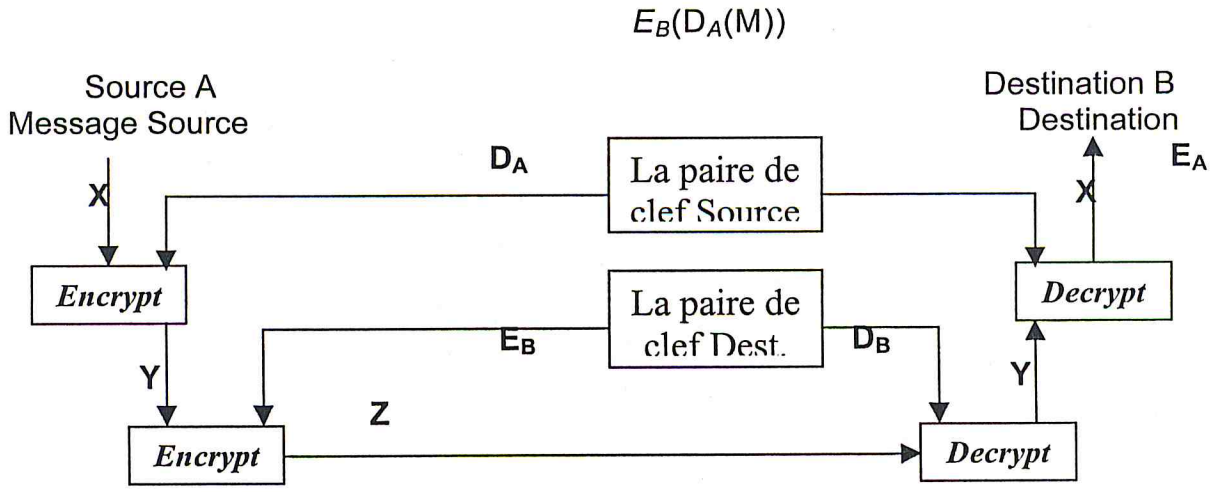


Figure II.6 : *Authentification et Confidentialité*

Avec : En émission $Y=D_A(X)$; $Z=E_B(Y) = E_B(D_A(X))$;

En réception $Y= D_B(Z)$; $X= E_A(Y)= E_A(D_B(Z))$;

b. "Checksum" cryptographique:

Le "checksum" cryptographique (*Code d'Authentification de Message*) est un petit bloc de données de taille fixe qui est ajouté à la fin du message.

En général, il est calculé comme une fonction du message original et d'une clef secrète partagée entre les deux parties communicantes. Lors de la réception, on applique la même fonction sur le message et on vérifie que le résultat est bien le même que le checksum envoyé.

Le message ne peut être transformé car le checksum ne correspondrait plus (le checksum lui-même ne peut être changé sans connaître la clef secrète). De même, le récepteur est certain que le message provient du bon émetteur.

Cette technique se rapproche de l'authentification par cryptage . Il est cependant important de noter que, la fonction utilisée est appliquée les deux fois dans le même sens, et qu'elle ne doit donc pas être réversible.

c. *Fonction de hachage:* [SCH97]

Une des variations du *Code d'Authentification de Message* est l'utilisation de la *fonction de hachage unidirectionnelle* ou *à sens unique*. Elle permet de générer à partir du message, un code de taille fixe appelé *code de hachage*. Une variation d'un seul des bits du message donnera un *code de hachage* différent.

Du côté du récepteur, la même fonction de hachage sera appliquée au message et le résultat sera comparé au *code de hachage* transmis avec le message.

Le fait que la *fonction de hachage* ne dépend pas dans sa définition d'une quelconque clef permet de l'utiliser dans un tas de situations diverses.

Définition :

Fonction de *hachage à sens unique :* Une fonction H est dite fonction de Hachage à sens unique si :

- Pour chaque message, il existe un algorithme polynomial :
  H/ h= H(message).

- Avec h seulement, il impossible de trouver un message tel que H (message)=h.

- H opère sur un message de longueur arbitraire. Elle fournit une valeur de Hachage (code de hachage) de longueur fixe h (souvent de taille inférieure).

- Pour tout message M, il est impossible (à l'échelle humaine) de trouver un message M' tel que : H (M) = H (M') .

II-4-5-2- Authentification des utilisateurs :

L'authentification des utilisateurs est la manière d'associer l'identité à son utilisateur, et le but est de prouver à un correspondant distant que l'identité de son interlocuteur est correcte. [CAT96]

II-4-5-2-a) Sécurisation d'architectures clients-serveurs : [REF01]

La diversité des équipements interconnectés amène les utilisateurs et les administrateurs à demander une unification d'utilisation des ressources, indépendante de l'environnement auquel ils accèdent ou qu'ils administrent.

L'*utilisateur* souhaite accéder de manière homogène aux applications ou aux services auxquels il a droit, en s'identifiant et en s'authentifiant une seule fois, sans se soucier de la plate-forme sur laquelle ces applications ou services se trouvent.

L'*administrateur* veut pouvoir administrer dans une base centrale, de manière homogène, et sur l'ensemble du système d'information, les utilisateurs et leurs privilèges. Le besoin d'outils globaux pour administrer les systèmes et les réseaux des architectures informatiques distribuées et hétérogènes, est une donnée fonctionnelle.

Dans la plupart des systèmes traditionnels , la protection des ressources est principalement mise en œuvre grâce à un mot de passe (password) saisi à l'ouverture de la connexion, et transmis en clair et sans protection sur le réseau. Le système authentifie l'usager, et suivant son identité, détermine son champ d'application. Ce processus d'authentification possède un certain nombre d'inconvénients :

- Ce procédé est *peu sécurisé*, puisque le risque d'écoute du réseau et d'interception du mot de passe est éminent.

- Il est *peu confortable* pour un utilisateur d'avoir à mémoriser et à taper autant de mots de passe que de serveurs auxquels il veut accéder.

- L'utilisateur *n'est pas reconnu par le système de façon unique*, et par conséquent, il n'y a pas de coordination entre les différents serveurs du système distribué. Seul le couple application-serveur est unique.

De plus, une méthode d'authentification unique, même lorsqu'elle pallie à l'ensemble des problèmes énumérés ci-dessus, peut s'avérer ne pas répondre à telle ou telle politique de sécurisation.

Dans certains cas, on veut s'assurer de la confidentialité et/ou de l'intégrité des données transmises sur le réseau. Dans d'autres, on veut aussi pouvoir contrôler les privilèges de chaque utilisateur, en l'autorisant à accéder seulement aux applications ou aux données qui lui sont nécessaires.

Dans le paragraphe suivant, on va essayer de définir un ensemble de protocoles d'authentification les plus représentatifs en matière de sécurisation client/serveur.

II-4-5-2-b) Protocoles d'authentification :

L'utilisation d'un protocole donné est fait suivant la politique suivie car chaque protocole a ses points forts en chaque matières de sécurité. Par exemple, on trouve ceux qui sont fiables, pour l'authentification mais posent des problèmes pour l'intégrité et la confidentialité des données. L'utilisation de ce genre de protocole peut se faire si l'administrateur cherche seulement à authentifier l'utilisateur. Chaque politique a donc son propre protocole d'authentification.

Parmi ces protocoles on trouve :

- *OTP (One Time Password).*
- *SSL (Secure Socket Layer).*

II-4-6 - Les protocoles d'authentification mutuelle avec échanges de clefs développés pour IP [CTF 02][HSC03]

Il existe de nombreux protocoles d'authentification mutuelle avec échange de clef, qui se différencient suivant les prérequis qu'ils imposent (secret partagé préalable, infrastructure à clef publique...) et les propriétés qu'ils vérifient (*direct authentication*, *perfect forward secrecy*...).

D'autre part, Diffie-Hellman est très utilisé dans tous les protocoles présentés ici, les différences venant de la durée de vie des valeurs publiques utilisées et de la façon dont elles sont authentifiées et échangées.

II-4- 6 - 1- Diffie-Hellman [SCH97]

Inventé en 1976 par Diffie et Hellman, ce protocole permet à deux tiers de **générer un secret partagé sans avoir aucune information préalable l'un sur l'autre**. Il est basé sur la cryptologie à clef publique (dont il est d'ailleurs à l'origine), car il fait intervenir des valeurs publiques et des valeurs privées. Sa sécurité dépend de la difficulté de calculer des logarithmes discrets sur un corps fini.
Le secret généré à l'aide de ce protocole peut ensuite être utilisé pour dériver une ou plusieurs clefs (clef secrète, clef de chiffrement de clefs...).
Voici le déroulement du protocole :

1. **Ap** et **Bp** se mettent d'accord sur un grand entier n tel que $(n-1)/2$ soit premier et sur un entier g primitif par rapport à n. Ces deux entiers sont publics.
2. **Ap** choisit de manière aléatoire un grand nombre entier a, qu'il garde secret, et calcule sa valeur publique, $A = g^a \bmod n$. **B** fait de même et génère b et $B = g^b \bmod n$.
3. **Ap** envoie A à **Bp** ; **Bp** envoie B à **Ap**
4. **Ap** calcule $K_{AB} = B^a \bmod n$; **Bp** calcule $K_{BA} = A^b \bmod n$. $K_{AB} = K_{BA} = g^{ab} \bmod n$ est le secret partagé par **Ap** et **Bp.**

Une personne qui écoute la communication connaît g, n, $A=g^a \bmod n$ et $B=g^b \bmod n$, ce qui ne lui permet pas de calculer $g^{ab} \bmod n$: il lui faudrait pour cela calculer le logarithme de A ou B pour retrouver a ou b.

II-4- 6 - 2- Les différents protocoles :[HSC03]

a. *SKIP*

SKIP (*Simple Key management for Internet Protocols*) est un exemple de **protocole qui ne se base pas sur l'établissement d'une "connexion".** En effet, aucun échange préalable de messages n'est nécessaire avant de pouvoir envoyer un paquet chiffré et **chaque paquet transporte l'information qui permettra de le déchiffrer.**
Au niveau des couches réseau, cela se traduit par le fait que SKIP se situe au niveau IP, et non au-dessus de TCP ou UDP comme la plupart des protocoles de gestion de clefs.

D'autre part, SKIP se base sur une génération de secret partagé Diffie-Hellman avec valeurs publiques authentifiées, donc le seul prérequis est que chaque participant doit être en possession d'une valeur publique Diffie-Hellman authentifiée.

- ***Principe***

SKIP est basé sur le principe de génération de secret partagé Diffie-Hellman, avec authentification pour éviter une possible attaque de l'intercepteur.
Les deux tiers possédant chacun une valeur publique Diffie-Hellman authentifiée, ils peuvent, à partir de la connaissance de la valeur publique de l'interlocuteur et de leur propre valeur privée, générer un secret partagé.

Pour implémenter SKIP, chaque tiers doit donc posséder une valeur publique Diffie-Hellman authentifiée. Cette authentification peut être obtenue de différentes façons : certificat X.509, DNS sécurisé, clef PGP signée...

D'autre part, pour communiquer avec un interlocuteur choisi, un tiers doit obtenir sa valeur publique. Une façon de réaliser cela est de distribuer les valeurs publiques à l'aide d'un "service d'annuaire" (*directory service*) ou à l'aide du "protocole de découverte de certificats" (*Certificate Discovery Protocol, CDP*).

Soient I et J les deux tiers. Les valeurs privées sont respectivement i et j et les valeurs publiques $g^i \bmod p$ et $g^j \bmod p$. Chaque tiers obtient le secret partagé en élevant la valeur publique de son interlocuteur à la puissance sa valeur privée :

$(g^j \bmod p)^i = (g^j \bmod p)^j$.

$g^{ij} \bmod p$ est appelé secret partagé à long terme et sert à dériver une clef secrète K_{ij}.

En effet, $g^{ij} \bmod p$ sera typiquement de longueur 1024 bits ou plus, alors que K_{ij} est une clef secrète de longueur 40 à 256 bits typiquement. Dans SKIP, K_{ij} est constituée des bits de poids faible de g^{ij} mod p.

Voilà pour la partie échange de clef proprement dite. SKIP va plus loin en précisant comment cette clef est ensuite utilisée pour protéger les échanges entre I et J. K_{ij} est en fait une clef de chiffrement de clef, c'est-à-dire qu'elle est utilisée exclusivement pour chiffrer des clefs de durée de vie beaucoup plus faible.

En effet, K_{ij} est utilisée pour chiffrer une clef K_p, appelée clef de paquet, qui est elle-même utilisée pour générer deux clefs, servant respectivement au chiffrement et à l'authentification d'un paquet IP ou d'un ensemble réduit de paquets.

Le mode de fonctionnement de SKIP, s'il ne requiert pas d'échange préalable à l'envoi de paquet chiffré, implique en revanche une augmentation de la taille de chaque paquet. En effet, un en-tête supplémentaire, dit en-tête SKIP, est adjoint au datagramme IP ; il sert notamment à transmettre la clef K_p (chiffrée avec K_{ij}) et à indiquer les algorithmes utilisés.

SKIP fut proposé comme protocole de gestion des clefs standard pour IPsec, et un certain nombre *d'Internet conscription* furent publiés dans ce sens jusqu'en août 1996.

À cette époque, les deux standards possibles pour la gestion des clefs avec IPsec étaient SKIP et ISAKMP/Oakley. Un choix s'imposait, et la question fut tranchée en faveur de ISAKMP/Oakley en septembre 1996.

Si ISAKMP/Oakley a été choisi pour être le protocole imposé dans toute implémentation, l'utilisation de SKIP n'est pas exclue.

Cependant, la publication d'*Internet drafts* à son sujet a cessé depuis cette date. Sun Microsystems continue à développer ce protocole et à l'intégrer dans un certain nombre de produits, notamment *SunScreen SKIP*. SKIP est également utilisable pour la gestion des clefs IPsec dans le produit *Firewall-1* de Check Point.

b. Photuris

Développé depuis 1995 par Phil Karn de chez Qualcomm et William Simpson de chez DayDreamer, *Photuris* utilise le même principe que le protocole STS (*Station-To-Station*) créé par Diffie, Van Oorschot et Wiener

Il a fait l'objet d'*Internet drafts* et de RFC indépendants de tout groupe de travail, et est utilisable avec IPsec. Quelques implémentations l'utilisent d'ailleurs actuellement, même si IKE est bien plus répandu.

Contrairement à SKIP, **Photuris est un protocole "orienté connexion"** au sens où il comporte un certain nombre d'échanges (pour la négociation d'options et la génération de clef) préalable à tout échange de messages chiffré. Photuris s'est vu attribué le port UDP 468.

- ***Principe***

Photuris est basé sur la génération d'un secret partagé selon le principe de Diffie-Hellman. **Ce secret partagé a une durée de vie faible : il sert à générer les clefs de session nécessaires pour protéger la suite des échanges.** Afin de contrer l'attaque de l'intercepteur à laquelle est vulnérable Diffie-Hellman, l'échange des valeurs servant à générer le secret partagé est suivi d'une authentification de ces valeurs à l'aide des secrets à long terme. Ces secrets servant uniquement à l'authentification, Photuris fournit la propriété de *perfect forward secrecy*.

Un problème de Diffie-Hellman est que ce protocole requiert des opérations coûteuses en ressources système, ce qui le rend vulnérable à des attaques en **déni de service** appelées "attaques par inondation" (*flooding attacks*). **Afin de rendre de telles attaques plus difficiles, Photuris a recours à un échange de *cookies*** avant de procéder à l'échange de valeurs Diffie-Hellman.

La valeur du *cookie* dépend des tiers en présence, en particulier par l'intermédiaire de l'adresse IP et du port UDP, ceci afin d'empêcher un attaquant d'obtenir un *cookie* valable puis de l'utiliser pour inonder la victime de requêtes provenant d'adresses IP et/ou de ports arbitraires.

D'autre part, il ne doit pas être possible, pour un attaquant, de générer des *cookies* qui seront acceptés par une entité comme générés par elle-même. Ceci implique que l'entité émettrice utilise une information locale secrète dans la génération de ses *cookies* et dans leur vérification ultérieure.

Le protocole Photuris est composé des trois étapes suivantes :

1. Un **échange de *cookies*** permet de contrer certaines attaques simples en déni de service. Chaque tiers en présence génère un *cookie*, et les *cookies* sont répétés dans chaque message transmis.
2. Un **échange de valeurs publiques** pour la génération d'un secret partagé.
3. Un **échange d'identités** afin que les tiers s'identifient l'un l'autre et vérifient l'authenticité des valeurs échangées durant la phase précédente. Cet échange est protégé en confidentialité grâce à des clefs privées dérivées du secret partagé et des *cookies* entre autres.

c-SKEME

Développé spécifiquement pour IPsec, SKEME est une extension de Photuris proposée en 1996 par Hugo Krawczyk de l'IBM T. J. Watson Research Center. Contrairement à Photuris, qui impose un déroulement précis du protocole, SKEME fournit **divers modes d'échange de clef possibles**.

Principe

De la même façon que les protocoles STS et Photuris, le mode de base de SKEME repose sur l'utilisation de **clefs publiques** et sur une génération de secret partagé **Diffie-Hellman**. SKEME n'est cependant pas restreint à l'utilisation de clefs publiques, mais **permet également l'utilisation d'une clef précédemment partagée.**

Cette clef peut avoir été obtenue par distribution manuelle ou par l'intermédiaire d'un centre de distribution de clef (*Key Distribution Center*, KDC), comme pour Kerberos.

Le KDC permet aux entités communicantes de partager un secret par l'intermédiaire d'un tiers de confiance. L'utilisation de ce secret pour l'authentification du secret Diffie-Hellman et non directement en tant que clef de session diminue la confiance requise en le KDC.

Enfin, SKEME permet également d'effectuer des échanges plus rapides en omettant d'utiliser Diffie-Hellman lorsque la propriété de *perfect forward secrecy* n'est pas requise.

En résumé, SKEME comporte quatre modes distincts :

- Le mode de base, qui fournit un échange de clef basé sur des clefs publiques et présentant la propriété de PFS grâce à Diffie-Hellman.
- Un échange de clef basé sur l'utilisation de clefs publiques, mais sans Diffie-Hellman.
- Un échange de clef basé sur l'utilisation d'une clef partagée précédemment et sur Diffie-Hellman.
- Un mécanisme de changement de clef rapide basé uniquement sur des algorithmes symétriques.
-

D'autre part, SKEME se décompose en trois phases : SHARE, EXCH et AUTH.

- Durant la **phase de partage (SHARE)**, les tiers échangent des demi-clefs, chiffrées avec la clef publique l'un de l'autre. Ces deux demi-clefs permettent de générer une clef secrète K. Si l'on désire protéger l'anonymat des tiers en présence, leur identité est également chiffrée. Dans le cas où l'on possède déjà un secret partagé, cette phase est sautée.
- La **phase d'échange (EXCH)** est utilisée, suivant le mode choisi, pour échanger des valeurs publiques Diffie-Hellman ou des nombres aléatoires. Le secret partagé Diffie-Hellman ne sera calculé qu'après la fin des échanges.
- Les valeurs publiques ou nombres aléatoires précédents sont authentifiées pendant la **phase d'authentification (AUTH)**, à l'aide de la clef secrète établie durant la phase SHARE.

Il va de soi que les messages correspondant à ces trois phases ne se suivent pas nécessairement de la façon décrite ci-dessus, mais sont en pratique combinés pour minimiser le nombre de messages à échanger.

d-Oakley

Oakley est un protocole d'échange de clef qui ressemble beaucoup à SKEME, en ce sens qu'il possède également plusieurs modes. Il a recours aux *cookies* et ne nécessite pas le calcul du secret partagé Diffie-Hellman avant la fin du protocole. Il se distingue des protocoles présentés jusqu'à présent par le fait qu'il **permet explicitement aux tiers en présence de se mettre d'accord sur les mécanismes d'échange de clef, de chiffrement et d'authentification utilisés.**

De fait, le but d'Oakley est de permettre le partage, de façon sûre entre les tiers, d'un ensemble d'informations relatives au chiffrement : nom de la clef, clef secrète, identités des tiers, algorithmes de chiffrement, d'authentification et fonction de hachage.

Plusieurs options sont disponibles dans Oakley. En plus du classique Diffie-Hellman, Oakley peut être utilisé pour dériver une nouvelle clef d'une clef ancienne ou pour distribuer une clef en la chiffrant. Ces options se traduisent par l'existence de plusieurs modes.

Le principe général d'Oakley est que l'initiateur de l'échange commence par spécifier autant d'information qu'il le désire dans un premier message. Son interlocuteur lui répond en fournissant également autant d'information qu'il le désire. La conversation se poursuit jusqu'à ce que l'état recherché soit atteint.

e) La gestion des clefs pour IPsec : ISAKMP et IKE [SHC02][JOS03]

IKE (*Internet Key Exchange*) est un système développé spécifiquement pour IPsec qui vise à fournir des mécanismes d'authentification et d'échange de clef adaptés à l'ensemble des situations qui peuvent se présenter sur l'Internet. Il est composé de plusieurs éléments : le cadre générique ISAKMP et une partie des protocoles Oakley et SKEME

ISAKMP est a priori utilisable pour négocier, sous forme d'associations de sécurité, les paramètres relatifs à n'importe quels mécanismes de sécurité : IPsec, TLS... Il est en effet prévu pour supporter la négociation de SA pour n'importe quel protocole de niveau supérieur ou égal à IP.

ISAKMP comporte deux phases, qui permettent une séparation nette de la négociation des SA pour un protocole donné et de la protection du trafic propre à ISAKMP :

- Durant la **première phase**, un ensemble d'attributs relatifs à la sécurité est négocié, les identités des tiers sont authentifiées et des clefs sont générées. Ces éléments constituent une première "association de sécurité", dite **SA ISAKMP**. Contrairement aux SA IPsec, la SA ISAKMP est bidirectionnelle. Elle servira à sécuriser l'ensemble des échanges ISAKMP futurs.

- La **seconde phase** permet de négocier les paramètres de sécurité relatifs à une **SA à établir pour le compte d'un mécanisme de sécurité donné** (par exemple AH ou ESP). Les échanges de cette phase sont sécurisés (confidentialité, authenticité...) grâce à la SA ISAKMP. Celle-ci peut bien sûr être utilisée pour négocier plusieurs SA destinées à d'autres mécanismes de sécurité.

II-4-7- MECANISME A JETON SYNCHRONISE (SecurID)

Security Dynamics est la seule société à pouvoir proposer le mécanisme à jeton synchronisé, solution brevetée sous le nom de *SecurID*.

SecurID est une technique qui permet aux utilisateurs authentifiés d'accéder à des ressources système ou réseau. Ces utilisateurs peuvent se trouver sur le réseau interne ou à l'extérieur.

II-4-7-1- Architecture matérielle de SecurID :

L'authentification par jetons de Security Dynamics nécessite une architecture matérielle particulière :

- Une carte securID possédée par l'utilisateur.
- Un moteur d'authentification ; Ce moteur peut être physique (*ACM*) ou logique (*ACE/Server de Security Dynamics*). Seul *ACE/Server* permet à des utilisateurs Internet d'être authentifiés.
- un ensemble de règles installées sur un serveur d'accès distant.

II- 4- 7- 2- L'authentification :

Pour s'assurer de façon fiable de l'identité d'un utilisateur, on dispose de deux informations : un code secret connu de l'utilisateur et un élément physique, une carte que l'utilisateur possède. L'utilisateur sera autorisé par un moteur d'authentification présent sur le réseau.

II- 4- 7- 3 - Fonctionnement :

Pour accéder à une ressource protégée du réseau , un utilisateur sur un réseau externe (Internet) utilise sa carte *SecurID*. La carte *securID* possède un microprocesseur qui affiche un code unique pour le possesseur de la carte toutes les 30 ou 60 secondes. Ce dernier code est uniquement valable pour un utilisateur et à un instant donné.

L'utilisateur initie d'abord une connexion vers le réseau . La connexion est interceptée par le serveur contrôleur du réseau cible sur lequel se trouvent les règles de contrôle de SecurID. Le serveur contrôleur demande alors à l'utilisateur de s'identifier.

L'utilisateur entre son login et fournit un mot de passe particulier constitué par la concaténation de son code secret et du code affiché sur la carte *securID*. Ces informations passent au moteur de contrôle d'accès contenant une base de données d'authentification. Si l'utilisateur est validé, la

connexion est autorisée et le code délivré par la carte *SecurID* rendu inutilisable.

L'association de ces deux codes permet au moteur d'authentification, ACE/Server, d'identifier l'utilisateur.

II- 4- 7- 4- Configuration pour l'Internet

SecurID est un mécanisme d'authentification. Il n'assure ni l'intégrité ni la confidentialité des informations qui transitent sur l'Internet. Le code d'authentification est unique mais non chiffré avec la carte *securID*. Pour un niveau de sécurité supérieur, *Security Dynamics* propose la carte *securID PINPAD* qui dispose d'un clavier où l'utilisateur entre son code secret.

Le code généré automatiquement par la carte toutes les 30 ou 60 secondes est chiffré avec le code secret de l'utilisateur pour former le mot de passe unique utilisé pour la connexion.

II-4-8- Sécurisation des machines individuelles [TER96] :

Comme son nom l'indique, elle consiste à configurer chaque station de travail sur le réseau pour résister à une intrusion en utilisant :

- Une identification de chaque entité sur le réseau.
- Des contrôleurs d'intégrité comme les anti virus.
- Des mécanismes d'*audit* et de *journalisation* qui sont respectivement des procédés qui permettent d'observer le comportement du réseau, tout en permettant la surveillance et la maintenance des systèmes.
- Des *mises à jours (patchs)* des logiciels, afin de supprimer les bogues et d'éventuelles failles ou trous.

II-4-9- Firewalls :

Une autre technique de sécurité Internet est l'utilisation d'un dispositif matériel ou logiciel isolé pour contrôler le trafic entrant ou/et sortant du réseau interne : le *Firewall.*

Le *Firewall* permet de protéger un réseau d'un autre. En principe, on protège le réseau local d'entreprise contre un réseau qui est externe, en qui on ne peut avoir confiance et à partir duquel des attaques peuvent survenir.

La protection du réseau consiste à empêcher l'accès aux utilisateurs non autorisés à des informations sensibles, tout en permettant aux utilisateurs légitimes le libre accès aux ressources du réseau.

Le *Firewall* se compose d'un ou plusieurs éléments bien spécifiques (routeurs filtrants, machines bastions avec service mandataire (proxy) et authentification d'utilisateurs, ...), créant ainsi une interface entre deux réseaux. un réseau protégé et un réseau externe (en général Internet).

Notre mémoire s'intéresse en particulier à cette technique de sécurité. Ce concept sera développé en détail dans le chapitre suivant.

. II-4-10- Détection d'intrusion: [GUI01]

La détection d'intrusion est définie comme "la capacité à identifier les individus utilisant un système informatique sans autorisation, et identifier ceux qui ont un accès légitime au système mais qui abusent de leur privilèges". On ajoute à cette définition l'identification des *tentatives* d'utilisation d'un système informatique sans autorisation et des abus de privilèges. Ainsi, l'intrusion est définie comme "toute tentative visant à compromettre l'intégrité, la confidentialité ou la disponibilité d'une ressource". [JAI 98]

On parle souvent d'IDS (Intrusion Detection System) pour désigner l'ensemble des outils de détection d 'intrusion.

Les outils de détection d'intrusion peuvent être classés selon deux modes de fonctionnement : soit sur des signatures d'attaques, ou bien sur des modèles comportementaux.

a- IDS à Bibliothèques de signatures

Cette approche consiste à rechercher dans l'activité de l'élément surveillé les empreintes (ou signatures) d'attaques connues. Ce concept est très similaire à celui des outils *anti-virus* et présente les même inconvénients que celui-ci.

En effet, ce type d'*IDS* est purement réactif ; il ne peut détecter que les attaques dont il possède la signature. De ce fait, il nécessite des mises à jour très fréquentes. De plus, si les signatures sont erronées ou incorrectement conçues alors c'est l'ensemble du système qui est inefficace. C'est pourquoi ces systèmes sont souvent contournés par des techniques dites " d'évasion " qui consistent à faire varier les signatures des attaques, qui, ainsi, ne sont plus reconnues par l'*IDS*.

Ce modèle est par contre très aisé à implémenter et à optimiser. Il permet également une classification relativement facile de la criticité des attaques signalées.

b- IDS à Modèles comportementaux

Ils ont pour principe la détection d'anomalies. La mise en œuvre de ce principe comprend une phase d'apprentissage, au cours de laquelle, les *IDS* vont " découvrir " le fonctionnement " normal " des éléments surveillés. Une fois cet apprentissage effectué, ces *IDS* signaleront les divergences par rapport au fonctionnement de référence.

Les modèles comportementaux peuvent être élaborés à partir d'analyses statistiques ou de techniques proches de l'intelligence artificielle. La principale promesse des *IDS* comportementaux est la détection des nouveaux types d'attaque.

En effet, ces *IDS* ne sont pas programmés pour reconnaître des attaques spécifiques mais signalent toute activité " anormale ". De ce fait, une attaque ne doit pas nécessairement être connue d'avance ; dès lors qu'elle représente une activité anormale elle peut être détectée par l'*IDS* comportemental. Du fait même de leur conception ces *IDS* sont incapables de qualifier la criticité des attaques.

De plus, ces *IDS* signaleront par exemple tout changement dans le comportement d'un utilisateur qu'il soit hostile ou non. De fréquents ajustements sont nécessaires afin de faire évoluer le modèle de référence de sorte qu'il reflète l'activité normale des utilisateurs et réduire le nombre de fausses alertes générées.

. II-4-11- Translation d'adresse :[PAS99]

Pour une meilleure sécurité d'un réseau local donné, il est plus intéressant de masquer l'identité (adresses) réelle des machines locales, afin d'éviter leurs localisation et une éventuelle attaque ou exploitation non autorisé.

Ainsi, il est plus intéressant d'attribuer un mécanisme de translation d'adresse afin de protéger le réseau d'une agression ultérieure.

a- Adressage

Un réseau privé peut posséder des adresses réservées, également dite privées, non routable sur le réseau internet.

La RFC 1918 impose l'utilisation de certaines catégories d'adresses pour chacune des classes:

- Classe A : 10.0.0.0 avec un masque de sous réseau : 255.0.0.0.
- Classe B : 172.16.0.0 - 172.31.0.0, soit 16 classes B.
- Classe C : 192.168.0.0 soit 254 réseaux de classe C (de 192.168.1.0 à 192.168.254.0)

b- Network Address Traduction (NAT)

Comme les adresses d'un réseau privé ne sont pas valides sur le réseau Internet (adresses non routable), le concept de translation d'adresses *NAT* (*Network Address Traduction)* permet l'accès au réseau Internet aux utilisateurs internes du réseau.

En effet, il possède une réserve d'adresses valides qui permettront à tout utilisateur du réseau interne de communiquer à l'extérieur du réseau.

Lorsqu'un utilisateur envoie un message avec une adresse interne, cette dernière sera transformée en adresse valide et le mécanisme *NAT* fait la correspondance entre les deux adresses grâce à une table. Lorsque le destinataire envoie une réponse, de nouveau l'adresse se transforme dans l'autre sens afin de restituer le message au bon utilisateur.

En réalité, il existe un nombre limité d'adresses valides à attribuer, et la récupération se fait grâce à un mécanisme de "time-out", lorsqu'elles ne sont plus utilisées pendant un certain temps.

Ce système *NAT* permet une légère sécurité : Le seul moyen de rentrer sur le réseau interne est d'utiliser une adresse valide parmi celles disponibles.

Ainsi, pour une machine qui n'accède jamais à Internet, jamais son adresse interne ne figurera sur la table de routage du routeur. Il sera ainsi impossible de contacter directement cet ordinateur depuis l'extérieur.

c. Single User Account (SUA) :

Dans cette technique, une seule adresse *IP*, celle de l'interface externe du routeur, est utilisée. Cependant, pour différencier entre les utilisateurs, le routeur attribue à chacun d'entre eux un numéro de port (>1024), qui lui permettra ainsi de faire suivre les réponses en fonction des ports sur lesquels elles arrivent.

Avec cette méthode, il n'y a plus de limitation du nombre d'utilisateurs autorisés à communiquer à l'extérieur. En effet, il y a plus de 64000 ports disponibles.

Le système *SUA* garantit une sécurité un peu supérieure au simple *NAT*, puisque l'attaquant doit alors deviner le numéro de port associé a chaque utilisateur, et qu'il n'a aucun moyen de contrôler l'assignation de ces ports. Quand bien même l'attaquant trouverait un port, il ne peut pas savoir quel service est utilisé derrière, car les ports sont alloués "aléatoirement", en fonction des services demandés.

Cependant, un problème se pose lorsque le réseau interne comporte des applications fonctionnant en mode serveur et non plus en mode client. Tant que le serveur est utilisé en interne, il n'y a aucun problème : le *SUA* ne pose pas de problème.

Lorsque le client se trouve à l'extérieur (sur Internet) et en voulant accéder au service *Telnet* par exemple sur un serveur du réseau interne, un problème surgira : en effet, il essayera d'atteindre la machine sur le port 23 (celui du *Telnet*).

Malheureusement, aucune correspondance n'existe pour le port 23. Ce port n'a jamais été utilisé "en sortie", et donc le routeur ne peut faire aucune correspondance.

Pour résoudre ce problème, on convertit tous les paquets "sans correspondance" vers une adresse *IP* par défaut sans changer quoi que ce soit sur le numéro de port.

Cette solution permet de résoudre le problème, mais un seul serveur pourra être atteint de cette manière. Ceci permet par exemple de faire fonctionner un et un seul serveur Web.

CONCLUSION :

Dans ce chapitre, différentes menaces, risques et techniques d'exploitations non autorisées, qui pèsent sur le système informatique, ont été présentés. Ces différents risques et menaces peuvent aller de la simple écoute et prélèvement de données, jusqu'à la paralysie totale du réseau privé.

Ceci nécessite la présence et la mise en œuvre d'un mécanisme de sécurité, pour préserver le système informatique (réseau local privé), de toute violation de son périmètre, et veiller à faire communiquer de l'information en toute intégrité et confidentialité ces solutions.

Parmi ces solutions et qui est considérée comme étant la base de la sécurité informatique, la solution cryptographique et l'authentification des différentes entités constituant le système informatique.

CHAPITRE III

Présentation du réseau bancaire de la Banque Exterieure d'Algerie

Le système d'information de la BEA (Banque Extérieure d'Algérie) est vaste et complexe . Sa construction matérielle a nécessité un certain laps de temps assez important .
La construction de ce système d'information nécessite l'implémentation d'un réseau national qui sera son support technique et matériel et permettra l'acheminement de l'information dans tous les sens.

Lors de la mise en place du support physique du réseau Le choix des équipements informatiques a pris en charge les critères suivants:

- Performances
- Évolutivité
- Puissance actuelle
- Durée de vie
- Leur intégration (compatibilité) avec les autres équipements existant ou à acquérir

III-1-NECESSITE DU RESEAU

La BEA réalise des opérations bancaires en agences . cela se traduit par une gestion directe de la clientèle étalée dans l'espace et dans le temps .

La BEA dispose aujourd'hui d'un nombre important de réseaux locaux géographiquement éloignés les uns des autres qui sont sur des sites d'AGENCE et de structures centrales dans toutes les WILAYA du pays

Aussi à tous moment chaque structure peut avoir besoin d'informations détenues par l'autre pour conditionner et coordonner les actions .
Fonctionnellement ,il devient impératif alors à tout décideur de pouvoir naviguer sur les sites disposant d'informations nécessaires à toute prise de décision .

L'architecture de ce système doit assurer :

- La centralisation de l'information qui permette une analyse et une aide à la prise de décision
- Une décentralisation pour la collecte de données par les opérateur concernés
- Des traitements locaux et à distance aux niveaux de toutes les structures
- Des percées en matière d'intégration de logiciels de modélisation et de calcul complexe

La solution adoptée par la BEA a été une solution Client /Serveur en réseau local et réseau distant .

III-2-LES ELEMENTS DU RESEAU

III-2-1-Réseau local Ethernet

Le réseau local de la BEA fonctionne suivant la méthode CSMA/CD :Norme 802.3.

En 100 base T ; les stations sont raccordées à un concentrateur (HUB ,SWITCH) .La longueur maximale d'un segment entre un concentrateur et une station est de 100 m.

Lorsque deux concentrateurs sont cascadés entre eux pour former un concentrateur composite et pour permettre la liaison entre plusieurs centaines de poste .
. la longueur entre ces deux éléments ne dépasse pas 10metre

La topologie du réseau local 100Base T est celle d'une étoiles en cascade d'étoiles reliées entre elles .

III-2-2-La stratégie du réseau BEA

a) Une agence

A la BEA ,la cellule de base qui génère l'information est une entité organique et géographique dénommée AGENCE ,qui utilise un ou plusieurs modules d'un système d'information dénommé DELTA .

Au niveau des agences l'information produite et traitée concerne essentiellement :

b) La gestion des opérations de produit bancaire Dinars et devises

- La gestion du porte feuille
- La gestion des comptes client Dinars et Devise
- La gestion du change
- La comptabilisation de la journée

Aussi, chaque jour les agences transmettent quotidiennement 3 fichiers au site central :

1. Fichier comptes
2. fichier mouvements
3. fichier client

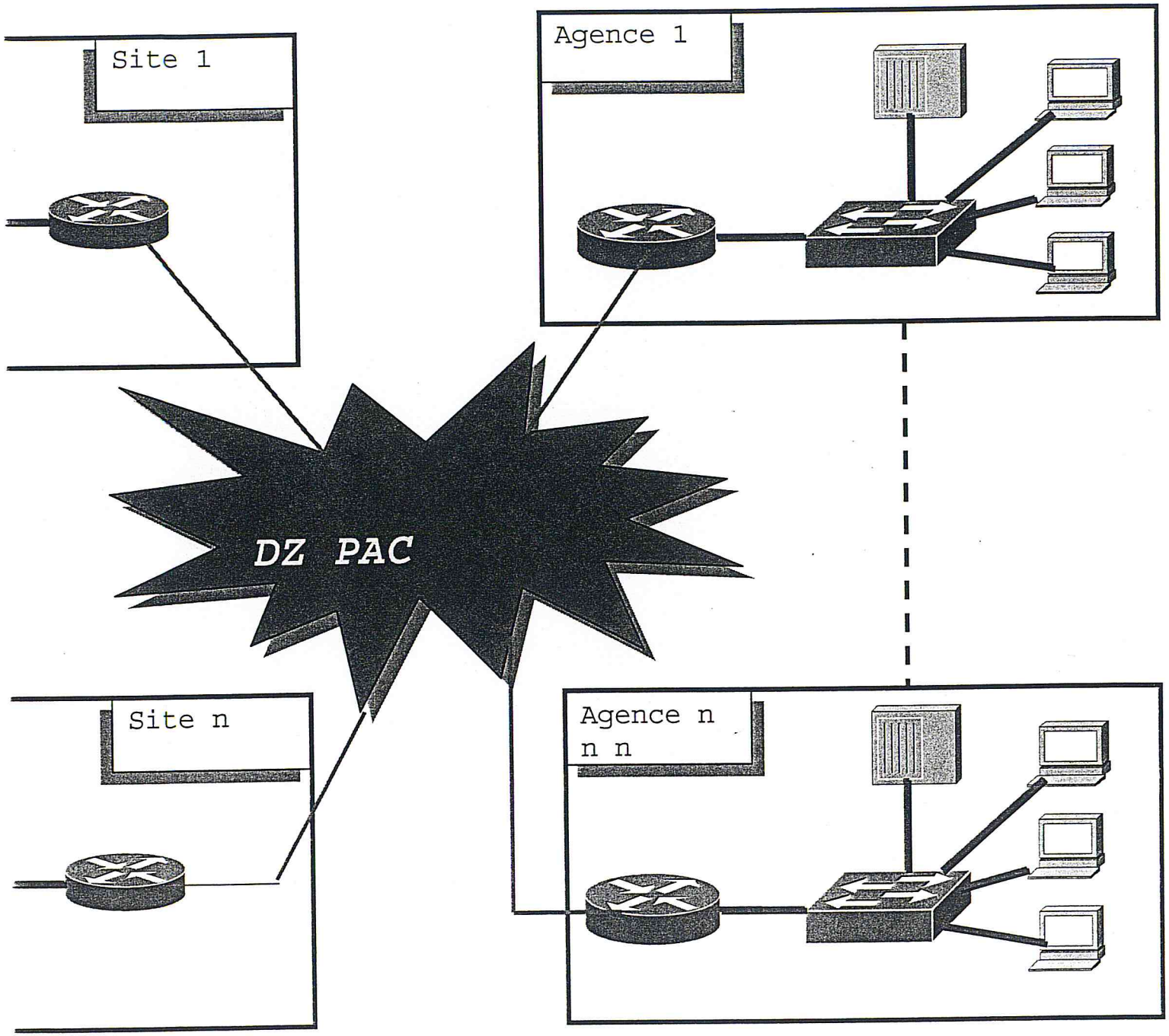
c) Le site centrale

le site central , au vu des informations générées par les agences assure la fonction de consolidation, de maintenance de fichiers des clients, de la comptabilité et du suivi des mouvements inter agence et des données statiques

d) La structure fonctionnelle de consolidation

le système d'information de la banque repose globalement sur 6 sites fonctionnels de consolidation :

1. site de développement
2. site logistique
3. site de messagerie
4. site décisionnel


Site 1
Agence 1
DZ PAC
Site n
Agence n
n n

Conclusion

Dans ce chapitre a été présenté l'architecture du réseau informatique de la banque extérieure d'Algérie (BEA) , avec ces composants et ces caractéristiques.

Bien sur ce réseau n'échappe pas aux risques informatiques cités auparavant. Le chapitre suivant exprime clairement la problématique de la sécurité au sein du réseau informatique BEA

CHAPITRE IV

Solution de sécurité

IV-I- PROBLEMATIQUE

Comme c'est déjà décrit, le réseau bancaire a besoin d'un réseau longue distance, pour transmettre les fichiers nécessaires, entre les différentes agences ; et cela dans la plus grande confidentialité et intégrité .

Les données qui doivent transiter d'un site (agence, direction, ...) à un autre passent par le routeur de chaque site. Ici seul le contrôle d'accès est réalisé grâce au *access-list* et une légère authentification par les adresses IP .

Le contrôle d'accès à lui seul ne suffit pas pour protéger les informations sensibles contre le vandalisme et le piratage . (démontré précédemment)

Les données circulent en clair sur le réseau public DZ PAC, il serait facile pour n'importe quel *hacker,* ayant accès à ce réseau d'utiliser l'une des méthodes présenté auparavant pour connaître le contenu du flux de données bancaires .

Les deux besoins qui se posent actuellement sont :

- Il faudrait tout d'abord, que chaque extrémité soit sûre, qu'elle communique avec l'extrémité voulue, et non avec une imposture .
- Il faudrait s'assurer que personne n'espionne le trafic sur le réseau , ou du moins, ne puisse le déchiffrer.

Pour cela ; la mise en place d'un ***tunnel*** sécurisé entre deux extrémités d'une liaison est indispensable.
Avec un certain niveau d'authentification des extrémités .

Les structures de la BEA concernées de la mise en point du canal sont les agences car elles effectuent le transfert des fichier de comptabilité .

IV-2-LA TUNNELISATION (TUNNLING)

- La plupart des VPN reposent sur l'utilisation de tunnels.
- Le but de la tunnelisation (tunneling) est en quelque sorte d'étendre le réseau interne : l'utilisateur doit pouvoir utiliser les services du réseau interne comme s'il s'y trouvait, sans modification des applications.
- La tunnelisation reposant souvent sur l'utilisation d'un réseau public, elle est généralement associée à une sécurisation des échanges (authentification, chiffrement).

IV-2-1-Tunnels – Rôle-

- Un tunnel sert à transporter des données d'un point A à un point B, au sens où les données qui "entrent" dans le tunnel en A "ressortent" nécessairement en B.

- Représentation :

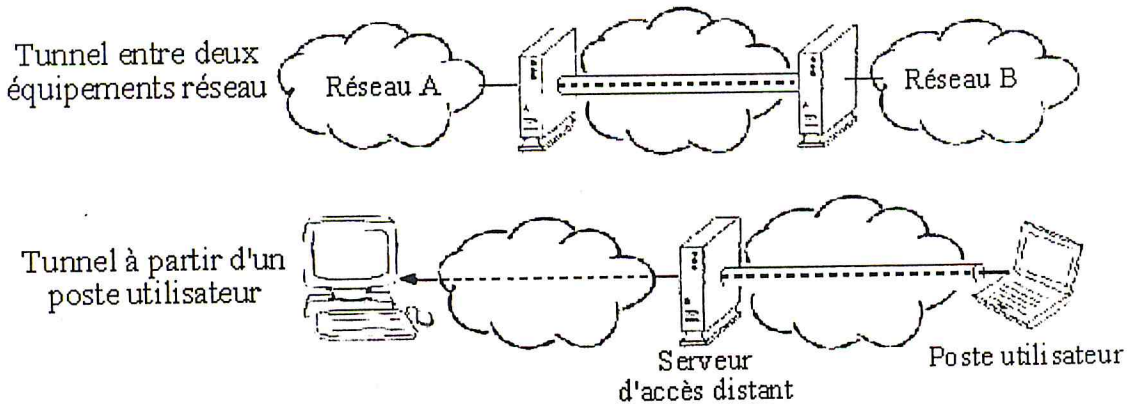


Figure IV-1 Différents types de tunnels [JOS03]

IV-2-2-Tunnels - Principe de fonctionnement

- Le transport des données se fait par "encapsulation" :
  - A l'extrémité du tunnel, les données à transporter sont insérées dans un paquet du protocole de tunnelisation, puis dans un paquet du protocole utilisé pour le transport de données entre les deux extrémités du tunnel
  - A l'autre extrémité, les données sont extraites du protocole de tunnelisation et poursuivent leur chemin sous leur forme initiale

- *Un exemple de méthode d'encapsulation : GRE* (Generic Routing Encapsulation)
  - L'encapsulation GRE consiste en l'ajout d'un en-tête qui contient les informations relatives au tunnel

IV-3-Qu'est-ce qu'un VPN ?

Un VPN (Virtual Private Network), Réseau Prive Virtuel en français (RPV) désigne de façon générale un réseau d'entreprise supporté par un réseau public (par exemple Internet).
Les principales alternatives au VPN sont les liaisons louées ou encore Numeris.

Les connexions économiques et sécurisées VPN passent par un réseau public partagé (Internet). Elles exploitent des technologies de tunnelisation et de

sécurisation standard pour offrir à l'utilisateur une connexion allant de la station de bureau à la périphérie du réseau, prenant l'apparence d'une liaison dédiée identique à celle d'une ligne louée.

L'administration du VPN peut relever de la responsabilité exclusive de l'entreprise ou être partagée avec l'opérateur par le biais de services contractuels.

IV-3-1-Les avantages des VPN

Les avantages des VPN contrebalancent largement les craintes de nombreuses sociétés lorsqu'il s'agit de la sous-traitance de domaines d'activités vitaux.

Le coût des appels peut être réduit par l'utilisation de numéros d'accès locaux.
Au lieu d'un investissement de départ conséquent, l'accès distant par VPN représente une charge mensuelle prévisible en fonction du nombre d'utilisateurs
De plus des économies substantielles peuvent être réalisées sur les équipements et les lignes, l'administration des utilisateurs distants, la maintenance et le support.

Points Positifs	Points négatifs
Liaisons louées	
Sécurité basique	Coût d'exploitations
Fiabilité	Rigidité
VPN	
Evolution facile	Coût d'investissement
Coût (Economie en utilisant Internet)	Complexité de mise en œuvre et d'exploitation
Sécurisation évoluée	

Comparatif VPN / liaisons louées

Tableau IV-1:comparatifVPN/Liaison louées [YAY02]

IV-4-ARCHITECTURE DES VPN

IV-4-1-Types de VPN

On distingue généralement 3 types de VPN : les VPN à accès distant, les VPN Intranet et les VPN Extranet. A chacun de ces types de VPN correspondent des problèmes de sécurité et de qualité de service spécifiques.

a) VPN à Accès Distant

Les VPN à accès distant (Remote Access VPN) permettent de connecter les

télétravailleurs, les utilisateurs mobiles ou même parfois des bureaux distants de très petite taille ou ayant un trafic faible, vers le WAN de l'entreprise afin de permettre l'accès aux ressources informatiques de l'entreprise.

La mise en place de VPN à accès distant se fait traditionnellement par l'intermédiaire du réseau téléphonique commuté analogique (RTC) ou numérique (RNIS).
Les VPN permettent de fournir à un utilisateur distant, à un réseau distant, un accès que l'on peut qualifier de privé vers, par exemple un Intranet, tout en utilisant une infrastructure de réseau publique ou partagée.

b) VPN Intranet

Un Intranet est un réseau d'entreprise interne à une société. Il met en relation les sites et/ou les utilisateurs habilités, à l'intérieur d'une même organisation.
L'un des enjeux majeurs des VPN Intranet est d'offrir une qualité comparable à un réseau d'entreprise composé de liaisons louées classiques.

d)VPN Extranet

L'Extranet correspond à une ouverture d'une partie de l'Intranet à des partenaires commerciaux, des clients ou des fournisseurs par exemple.
Les règles de sécurité d'un Extranet sont beaucoup plus strictes et plus complexes que pour un intranet, puisqu'il faut gérer l'accès aux membres de la société mais également l'accès à des personnes extérieures.

IV-5-1-COMPOSANTES NECESSAIRES AUX VPN

Il y a 2 éléments primordiaux pour le bon fonctionnement des VPN : la sécurité et la performance du réseau.
La sécurisation des échanges est l'un des points clef des VPN. Compte tenu des techniques mises en œuvre, les liens VPN sont devenus presque plus sécurisés que les liens loués.

Il existe plusieurs techniques de sécurisation des échanges : tunneling, authentification et cryptage. Pour assurer un bon niveau de sécurité, il est recommandé de mettre ces techniques en œuvre simultanément lors de la mise en place de VPN.

Le tunneling permet de privatiser les échanges. C'est en fait une connexion privée point à point établie entre les deux extrémités d'une communication. Le tunneling repose essentiellement sur l'encapsulation des datagrammes IP.

La technique de tunneling permet de transmettre des paquets de données

dans un réseau public par l'intermédiaire d'un tunnel privé, qui simule une connexion point à point. Cette technique va permettre de faire transiter des paquets provenant de sources différentes via des tunnels séparés sur la même infrastructure.
Cette technique permet d'isoler le trafic de l'entreprise du reste du trafic.

L'encapsulation permet également de faire passer sur le réseau IP des paquets provenant d'autres protocoles (IPX, Appletalk, ...). Cela représente un intérêt non négligeable dans la mesure où tous les réseaux locaux n'utilisent pas nécessairement TCP/IP.

L'encapsulation du paquet à l'intérieur d'un datagramme IP consiste à créer un paquet IP ayant pour corps le paquet d'origine, pour adresse source l'adresse du point d'entrée dans le tunnel et pour adresse destination l'adresse de terminaison du tunnel.

Adresse du point d'accès au tunnel	Adresse de la terminaison du tunnel	Paquet initial

Figure IV-2: Encapsulation d'un paquet dans un datagramme IP [JOS03]

Plusieurs protocoles de tunneling sont utilisés pour la mise en place de VPN :
- les protocoles de tunneling de niveau 2 (L2F, L2TP et PPTP)
- les protocoles de tunneling de niveau 3 (IPsec).

IV-6-PROTOCOLES UTILISES DANS LE CADRE DES VPN

IV-6-1-Les protocoles de tunneling de niveau 2

Rappel sur PPP

PPP est un protocole full duplex assurant l'échange de données point à point .
Il permet le transport de données en provenance de plusieurs protocoles (IP, IPX...)

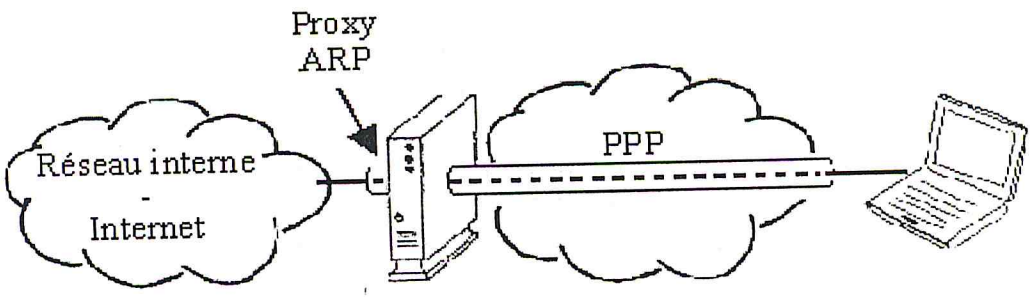


Figure IV-3: Protocole PPP

IV-6-1-Point to Point Tunneling Protocol (PPTP)

L'attribution de l'adresse IP se fait de façon dynamique.
PPTP a été développé par Microsoft, en collaboration avec Ascend et 3Com. Il s'inspire du protocole PPP (Point to Point Protocol) et permet d'établir des connexions PPP au travers de réseaux IP comme l'Internet. PPTP est un protocole natif dans Windows95 et Windows NT.

Le tunnel consiste en une encapsulation de niveau 3 définie par le protocole GRE (Generic Routing Encapsulation).

Le tunnel PPTP se caractérise par les points suivants :

- le tunnel est initié par le client ;
- Le serveur d'accès laisse passer les connexions PPTP ;
- Le tunnel est terminé par un serveur;
- Une connexion de contrôle entre client et serveur ;
- Les paquets PPP sont encapsulés dans IP.

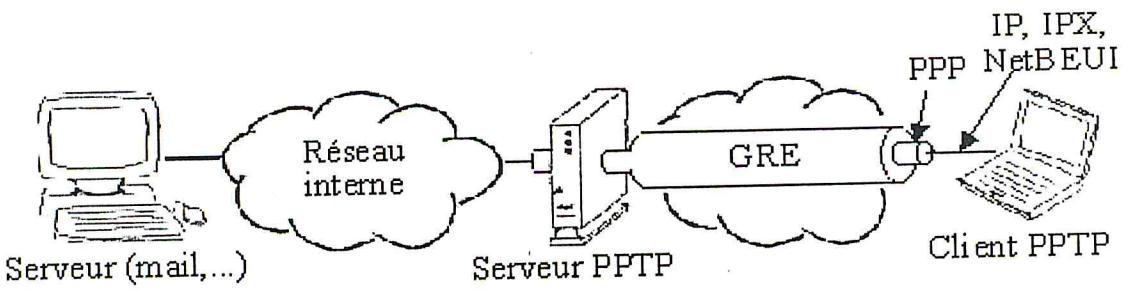


Figure IV-4: Protocole PPTP [SCH03]

Ce protocole utilise comme processus d'authentification les protocoles PAP (Password Authentification Protocol) ou CHAP (Challenge Handshake Authentification Protocol).

Il peut aussi utiliser aussi les fonctions MPPE (Microsoft Point to Poin Encryption) et MPPC (Microsoft Point to Point Compression) pour respectivement le cryptage et la compression de bout en bout

Toutefois, ce protocole s'avère limité assez rapidement : lorsqu'on ajoute PPTP à un système NT déjà très sollicité, on aboutit assez rapidement à des problèmes de surcharge.

IV-6-2-Layer 2 Forwarding (L2F)

L2F (Layer 2 Forwarding) est un protocole similaire à PPTP développé par CISCO, Northern Telecom et Shiva, permettant d'encapsuler PPP dans IP afin de créer des réseaux privés virtuels

L2F fournit des mécanismes permettant de créer des tunnels pour transporter des trames de niveau 2 ou provenant de protocoles de niveaux supérieurs.

Le tunnel L2F se caractérise par les points suivants :

- Les clients se connectent en PPP;
- Les tunnels sont démarrés par les NAS des ISP ou des opérateurs;
- Les tunnels sont terminés par un routeur positionné chez le client;
- Les tunnels L2F ne sont pas cryptés;
- Deux niveaux d'authentification de l'utilisateur(ISP & passerelle de l'entreprise).

Comme le protocole précédent, il permet de faire du chiffrement MPPE, et de la compression MPPC de bout en bout.
Une différence majeur par rapport à PPTP est que le tunneling de L2F n'est pas dépendant de IP et peut donc très bien fonctionner avec du Frame Relay ou de l'ATM .

IV-6-3-Layer 2 Tunneling Protocol (L2TP)

L2TP est issu de la convergence des protocoles PPTP et L2F . L2TP permet l'encapsulation des paquets de données au niveau des couches 2 (Frame Relay et ATM) et 3 (IP) pour créer un tunnel de communication entre deux utilisateurs.
L2TP, comme PPTP sont utilisés pour transférer des datagrammes de type PPP via un tunnel supporté par IP.

Fonctionnement

L2TP isole le trafic de l'entreprise, assure la protection des données et utilise l'infrastructure d'Internet pour créer des liens privés (tunneling) entre deux utilisateurs. Il encapsule les données en paquets IP afin de les faire transiter sur l'Internet, et ce quel que soit le protocole utilisé dans l'entreprise (IP, IPX, AppleTalk ou NetBEUI). Toutefois, L2TP n'inclut pas directement le chiffrement des données.

- ***Paquet L2TP***

On distingue 2 composantes principales dans L2TP:
- Les paquets d'information, utilisés pour le transport de L2TP encapsulés dans des paquets PPP pour les sessions utilisateurs.
- Le protocole de signalisation qui utilise le contrôle de l'information L2TP encapsulé dans des paquets UDP/IP (on fait du L2TP/UDP/IP/PPP).

L'établissement d'un tunnel L2TP permet d'encapsuler différents protocoles dans des paquets IP, mais cela permet également d'assurer l'intégrité du réseau de l'entreprise. Les routeurs sont en effet capables de différencier le trafic VPN du simple trafic Internet grâce à l'encapsulation.

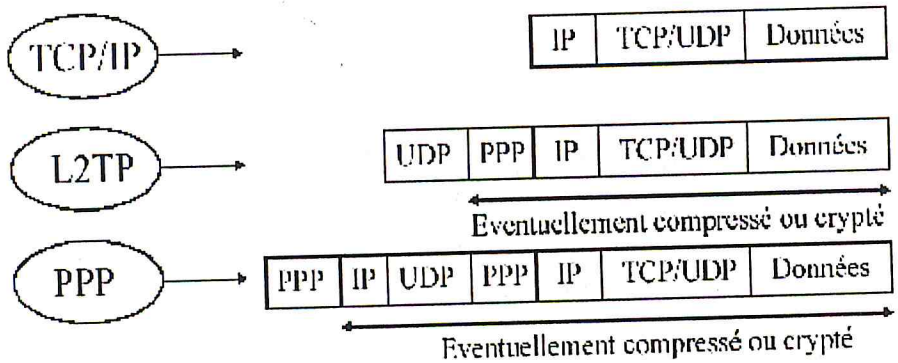


Figure IV-5: Format du paquet L2TP [SCH03]

IV-6-4-IPSEC (IP security)

- ***Rappels de cryptographie***

Le cryptage joue un rôle essentiel dans les VPN IP puisqu'il permet d'assurer la confidentialité des informations transmises sur le réseau.
On distingue deux types d'algorithmes de chiffrement : les algorithmes symétriques (ou à clef privée) et les algorithmes asymétriques (ou à clef publique

a) Introduction sur IPsec

Le terme IPsec (IP Security Protocol) définit un ensemble de protocoles et de formats permettant d'améliorer la sécurité des transmissions dans un réseau privé virtuel IP.

Le développement d'IPsec découle directement des travaux sur IPv6 dont il est un sous-ensemble (fonctionnement avec IPv4 actuellement utilisé sur Internet).

IPsec peut être implémenté au niveau d'un client ou d'une passerelle de sécurité (firewall ou routeur implémentant IPsec).

IPsec apporte un deuxième niveau d'encapsulation par rapport à L2TP, et intègre le chiffrement des données (algorithmes de chiffrements libres…).

b) Architecture d'IPsec

- **Les mécanismes AH et ESP**

IPsec fait appel à deux mécanismes de sécurité pour le trafic IP, les « protocoles » AH et ESP, qui viennent s'ajouter au traitement IP classique :

- ***Authentication Header (AH)*** est conçu pour assurer l'intégrité et l'authentification des datagrammes IP sans chiffrement des données (i.e. sans confidentialité).

- ***Encapsulating Security Payload (ESP)*** a pour rôle premier d'assurer la confidentialité, mais peut aussi assurer l'authenticité des données.
Ces mécanismes peuvent être utilisés seuls ou combinés pour obtenir les fonctions de sécurité désirées.

- **La gestion des clefs et des associations de sécurité**

Les SA (Security Association) contiennent tous les paramètres nécessaires à IPsec, notamment les clefs utilisées.

Le protocole de négociation des SA développé pour IPsec s'appelle « protocole de gestion des clefs et des associations de sécurité pour Internet » (Internet Security Association and Key Management Protocol, **ISAKMP)**.

ISAKMP est en fait, inutilisable seul : c'est un cadre générique qui permet l'utilisation de plusieurs protocoles d'échange de clefs et qui peut être utilisé pour d'autres mécanismes de sécurité que ceux d'IPsec. Dans le cadre de la standardisation d'IPsec, ISAKMP est associé à une partie des protocoles SKEME et Oakley pour donner un protocole final du nom d'IKE (Internet Key Exchange).

- **Équipement fournissant Ipsec**

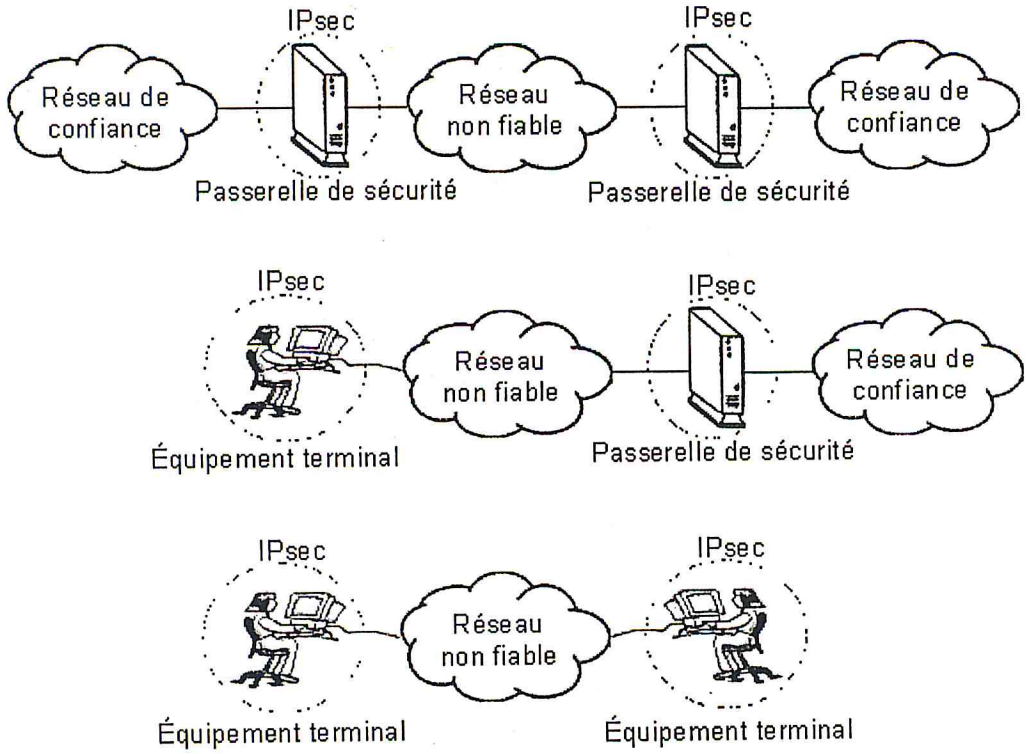


Figure IV-6: Equipements fournissants IPSec [YAY02]

IPsec peut être utilisé au niveau d'**équipements terminaux** ou au niveau de **passerelles de sécurité** (*security gateway*), permettant ainsi des approches de sécurisation lien par lien comme de bout en bout. Trois configurations de base sont possibles :

La première situation est celle où l'on désire relier des réseaux privés distants par l'intermédiaire d'un réseau non fiable, typiquement Internet.
Les deux passerelles de sécurité permettent ici d'établir un **réseau privé virtuel** (en anglais *Virtual Private Network, VPN*).

La deuxième situation correspond au cas où l'on **désire fournir un accès sécurisé au réseau interne pour des postes nomades**. Le réseau non fiable peut être Internet, le réseau téléphonique...

Enfin, dans ***la troisième situation***, deux tiers désirent communiquer de façon sécurisée mais n'ont aucune confiance dans le réseau qui les sépare.

- **Modes de fonctionnement**

Pour chacun des mécanismes de sécurité d'IPsec, il existe deux modes : le mode transport et le mode tunnel.

En mode transport, seules les données en provenance du protocole de niveau supérieur et transportées par le datagramme IP sont **protégées**. Ce mode n'est utilisable que sur des équipements terminaux ; en effet, en cas d'utilisation sur des équipements intermédiaires, on courrait le risque, suivant les aléas du routage, que le paquet atteigne sa destination finale sans avoir traversé la passerelle sensée le déchiffrer.

En mode tunnel, l'en-tête IP est également protégé (authentification, intégrité et/ou confidentialité) et remplacé par un nouvel en-tête. Ce nouvel en-tête sert à transporter le paquet jusqu'à la fin du tunnel, où l'en-tête original est rétabli. Le mode tunnel est donc utilisable à la fois sur des équipements terminaux et sur des passerelles de sécurité. Ce mode permet d'assurer une **protection plus importante contre l'analyse du trafic**, car il masque les adresses de l'expéditeur et du destinataire final.

Comparaison des protocoles de tunneling

	PPTP	L2PT	IPSec
Mode	Client-Serveur	Client-Serveur	Client à Client
Utilisation	Accès distant via du tunneling	Accès distant via du tunneling	Intranet , Extranet , accés distant via tunneling
Couche OSI	Couche 2	Couche 2	Couche 3
Protocole encapsulés	IP ,IPX, Appeltalk	IP ,IPX ,Appletalk	IP
Securité authentification de l'utilisation	Non (utilisation PAP, CHAP ,Kerbros,Token)	Non (utilisation PAP, CHAP ,Kerbros,Token)	Non (utilisation PAP, CHAP ,Kerbros,Token)
Authentification de paquet	Non	Non	Oui : En-tête **AH**
Cryptage du paquet	Non	Non	Oui :En – tête **ESP**
Serveur de tunneling	Tunnel simple point a point ;pas d'accès simultané	Tunnel simple point à point , pas d'accès simultané	Tunnel multipoint ; accès VPN et Public simultané.
Gestion des clefs	Non	Non	IKE, SKIP

Tableau IV-2: comparaison entre différents protocoles de tunneling

Après avoir examiné les différents protocoles, et leur propriétés , il en ressort, que le protocole IPSec offre de meilleurs avantages en matière de sécurité.

IV-7-PRESENTATION APPROFONDIE D'IPSEC

IV-7-1-Authentication Header (AH)

AH assure l'intégrité des données en mode non connecté, l'authentification de l'origine des données et, de façon optionnelle, la protection contre le rejeu.

L'absence de confidentialité dans AH permet de s'assurer que ce standard pourra être largement répandu sur l'Internet, y compris dans les endroits où l'exportation, l'importation ou l'utilisation du chiffrement dans des buts de confidentialité est restreint par la loi.

Cela constitue l'une des raisons de l'utilisation de deux mécanismes distincts. Dans AH, intégrité et authentification sont fournies ensembles, à l'aide d'un bloc de données supplémentaire adjoint au message à protéger.

Ce bloc de données est appelé "valeur de vérification d'intégrité" (*Integrity Check Value, ICV),*terme générique pour désigner soit un code d'authentification de message (*Message Authentication Code, MAC*), soit une signature numérique. Pour des raisons de performances, les algorithmes proposés actuellement sont tous des algorithmes de scellement (code d'authentification de message et non signature).

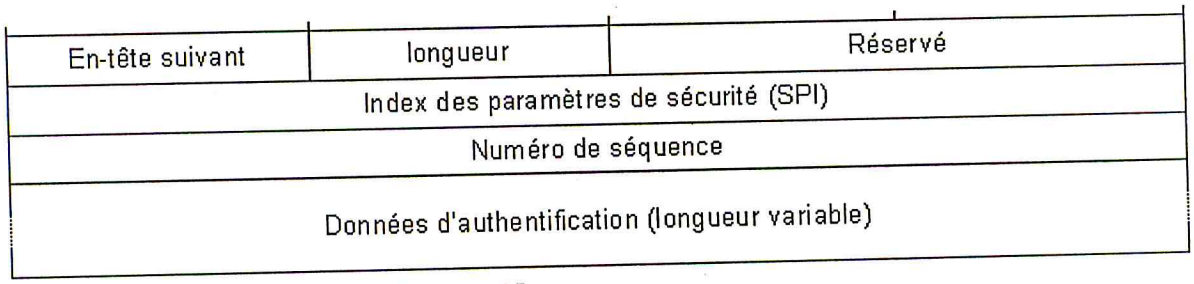


Figure IV-6: Format AH [SCH03]

L'expéditeur calcule les données d'authentification à partir de l'ensemble des champs invariants du datagramme IP final, AH compris, ce qui permet d'étendre l'authentification au SPI et au numéro de séquence notamment.

Les champs variables (TTL, routage...) et le champ destiné à recevoir les données d'authentification sont considérés comme égaux à zéro pour le calcul.

Les données d'authentification sont alors adjointes au paquet IP par le biais de l'en-tête d'authentification (AH).

Le récepteur vérifie l'exactitude de ces données à la réception.
Les figures suivantes indiquent la position de AH et le service apporté en fonction du mode choisi (transport ou tunnel).

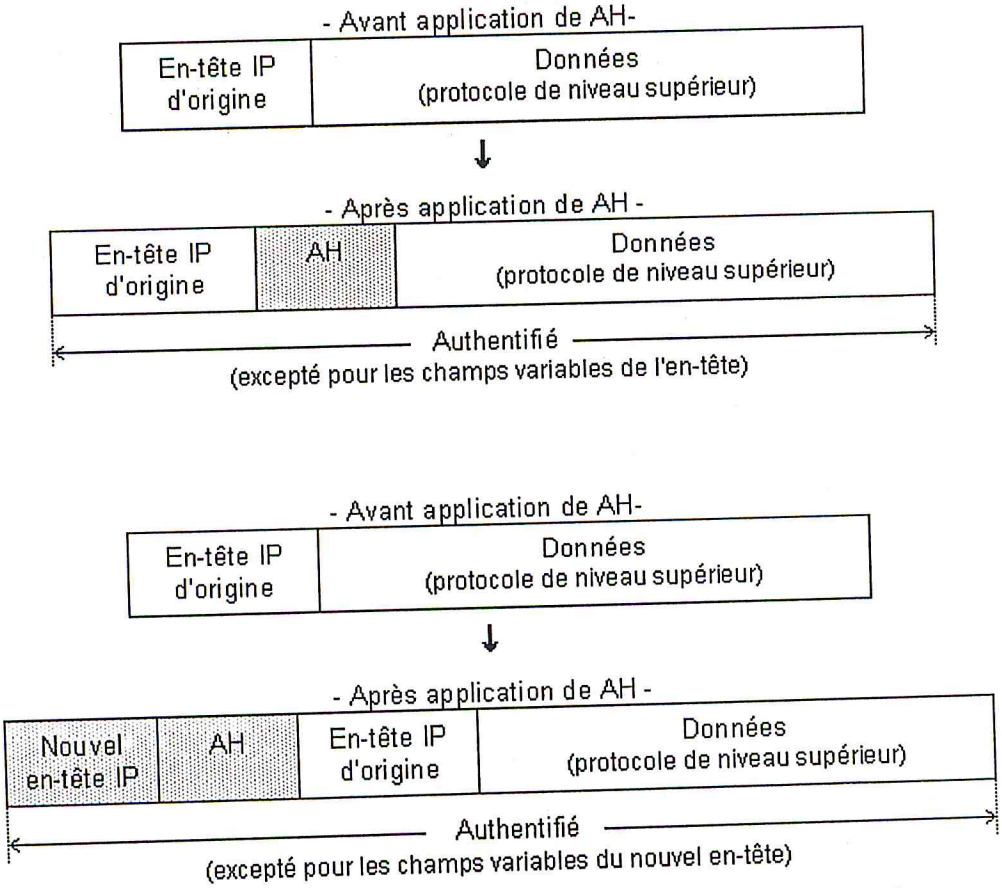


Figure IV-7: Application de AH en mode transport et tunnel [SCH03]

Les algorithmes par défaut que doit fournir toute réalisation de IPsec pour AH sont, au moment où ce document est rédigé, **HMAC-MD5** et **HMAC-SHA-1.** Les autres algorithmes prévus sont **KPDK-MD5, DES-MAC** et **HMAC-RIPE-MD.**

IV-7-2-Encapsulating Security Payload (ESP)

ESP peut assurer, au choix, un ou plusieurs des services suivants :

- **confidentialité** (confidentialité des données et protection partielle contre l'analyse du trafic si l'on utilise le mode tunnel),
- **intégrité** des données en mode non connecté et **authentification de l'origine** des données, protection contre le **rejeu.**

Contrairement à AH, où l'on se contentait d'ajouter un en-tête supplémentaire au paquet IP, ESP fonctionne suivant le principe de l'encapsulation : **les données originales sont chiffrées puis encapsulées** entre un en-tête et un *trailer.* Voici l'organisation de ESP :

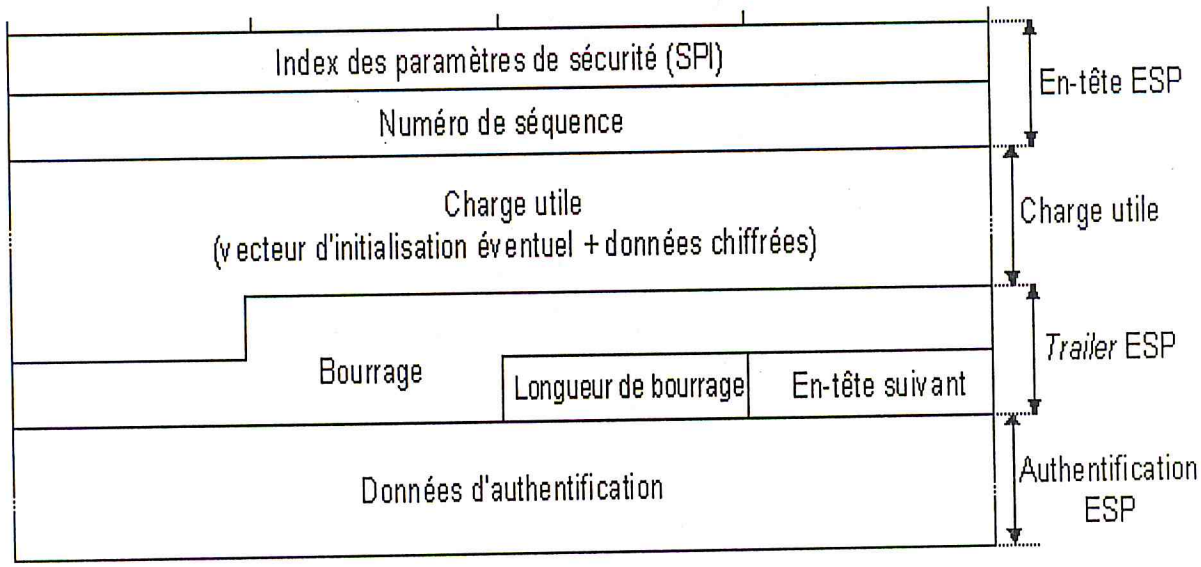


Figure IV-8: Format de ESP [SCH03]

Le champ bourrage peut être nécessaire pour les algorithmes de chiffrement par blocs ou pour aligner le texte chiffré sur une limite de 4 octets.

Si elle a été sélectionnée, **l'authentification est toujours appliquée après que les données ne soient chiffrées**. Cela **permet, à la réception, de vérifier la validité du datagramme avant de se lancer dans la coûteuse tâche de déchiffrement**. Contrairement à AH, l'authentification dans ESP est appliquée uniquement sur le "paquet" (en-tête + charge utile + *trailer*) ESP et n'inclut ni l'en-tête IP ni le champ d'authentification.

Les figures suivantes indiquent la position de ESP et les services apportés en fonction du mode choisi (transport ou tunnel).

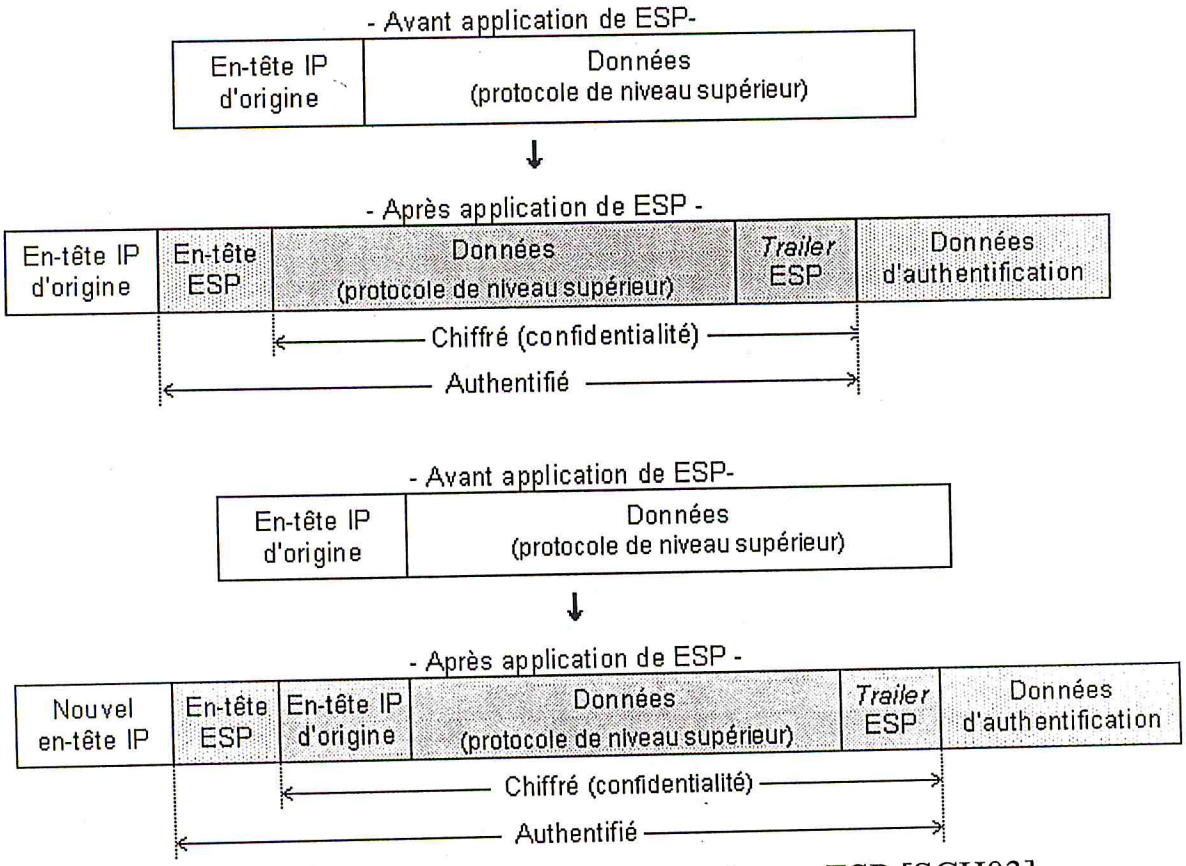


Figure 9: Application du mode transport et tunnel avec ESP [SCH03]

Les algorithmes prévus pour être utilisés avec ESP sont

- Confidentialité : **DES triple , DES, RC5, CAST, IDEA, IDEA triple, Blowfish, RC4 et NULL** pour le cas ou le chiffrement n'est pas souhaité.
- Authentification : HMAC-MD5 , HMAC-SHA-1 , DES-MAC, HMAC-RIPE-MD, KPDK-MD5 et NULL pour le cas où l'authenticité n'est pas sélectionnée.

IV-7-3-Fonctionnement d'IPSec

Une communication IPSec peut se découper en 3 étapes et 2 tunnels.

- ***Etape 1 = Tunnel 1 = Tunnel IKE :***

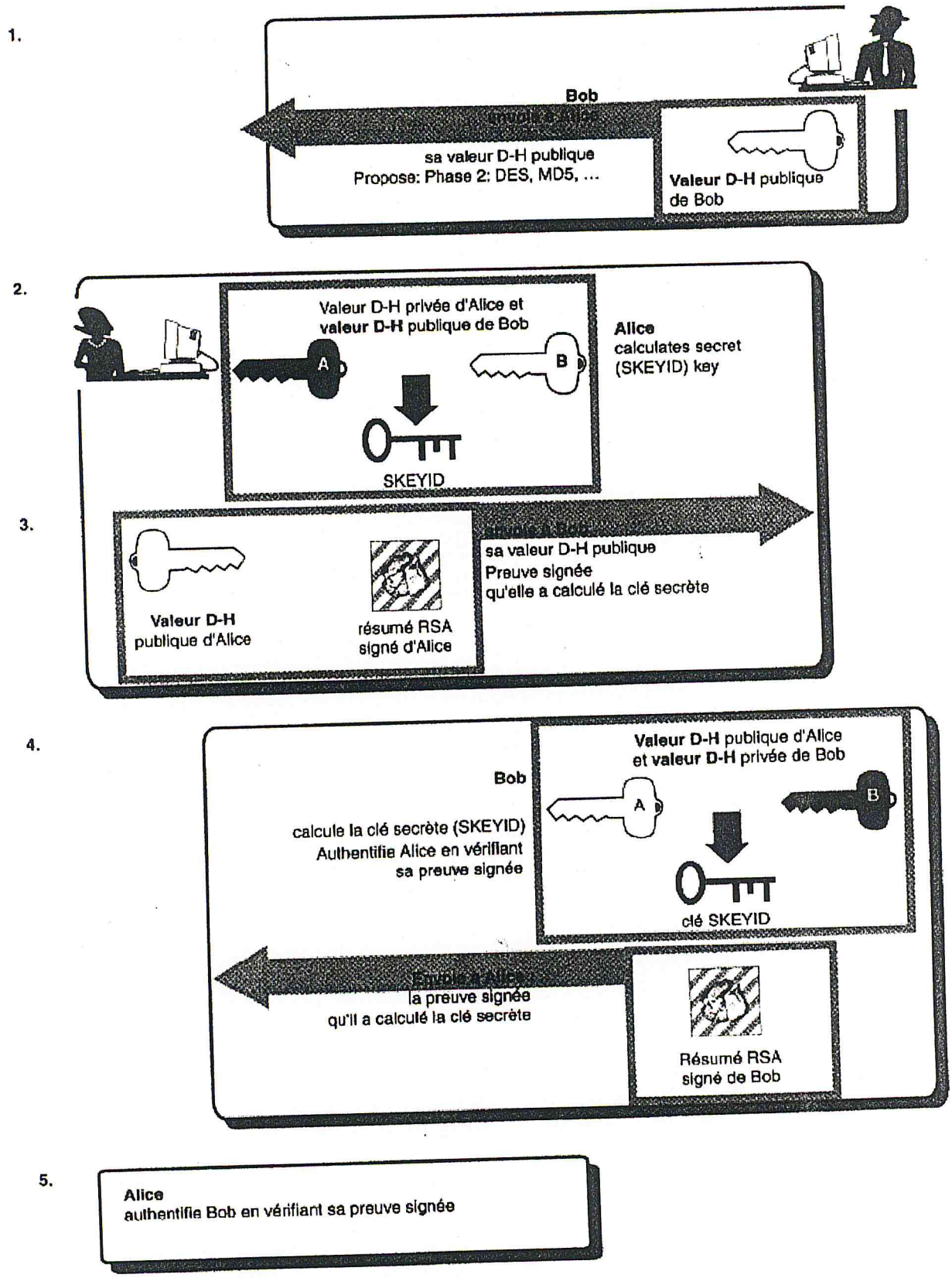
IKE Phase 1 : Authentification des entités, plus négociation des SA IKE, plus montage du tunnel crypté pour la négociation des SA IPSec en phase 2.

IKE négocie les SA (Security Associations) pour IPSec.

IKE négocie les IPSec security associations (SAs). Ce processus nécessite que les systèmes IPSec s'authentifient entre eux et établissent les clefs IKE (= ISAKMP) partagées.

La phase 1 a pour but de paramétrer un canal d'authentification sécurisé entre les deux parties. Les premiers messages sont en clair. Ils servent à déterminer les paramètres qui sécuriseront les échanges futurs. IKE emploie l'algorithme d'échange de clef Diffie-Hellman pour générer les clefs secrètes partagées.

Les clefs servent à chiffrer et à authentifier les échanges de la phase 2.



Etape 2 = Tunnel 2 = Tunnel IPSec :

IKE Phase 2 : négociation des paramètres des SA IPSec + mise en place de ces SA sur chaque entité.

Tous les messages de la phase 2 sont chiffrés et authentifiés par la SA IKE et les clefs secrètes partagées. La phase 2 comporte toujours trois phases. Étant donné qu'aucune opération de cette phase ne prend du temps, on lui a donné le nom de "Quick mode" (mode rapide). Durant cette phase, les deux parties négocient les paramètres des SAs IPsec et calculent leur second jeu de clefs secrètes partagées. le second jeu de clef est calculé à partir de l'autre valeur secrète générée lors de la phase 1 et de nouveaux nombres aléatoires.

La raison de la rapidité de la phase 2 est qu'elle utilise la cryptographie à clefs secrètes et non celle à clefs publiques qui est beaucoup plus lente et coûteuse.

- ***Etape 3 :***

Transfert des données.

Les données sont transférées entre les entités IPSec en utilisant les paramètres IPSec + les clefs enregistrées au niveau des SA.

IV-7-4- Les différents modes

Les modes sont des façons de réaliser une phase. Les deux premiers que nous traiterons ici sont relatifs à la phase 1. Il s'agit du mode principal et du mode agressif. Le mode rapide (Quick mode) est en fait la phase 2

Voyons le mécanisme de chacun des modes.

a) *Main mode - mode principal*

Le mode principal est le mode "prudent" de la phase 1. Il requiert six messages et offre des protections supplémentaires. Les données échangées entre les deux parties sont identiques en mode normal et agressif. Simplement, cette information est répartie sur plus de messages pour le mode principal.
Les deux premiers messages négocient la politique de sécurité (c'est-à-dire les paramètres cryptographiques) pour le reste de l'échange. Les deux messages suivants sont utilisés pour l'échange Diffie-Hellman. Et enfin, les deux derniers messages servent à l'authentification (par certificat, signatures, etc...). Ces deux messages sont chiffrés par les clefs déduites précédemment, ainsi l'identité des parties ne peut pas être connue d'un tiers.

b) *Agressive mode - mode agressif*

Le mode agressif est le mode hâtif de la phase 1. Il ne comprend que trois messages. Puisque la quantité d'information est la même que dans le mode principal, chacun des messages doit comporter plus d'informations. De plus, le répondeur doit effectuer des calculs de clefs publiques coûteux avant de pouvoir envoyer son premier message. Cette particularité est bien entendu sujette à attaque.

CHAPITRE V

Conception de la solution de sécurité

Dans ce chapitre ,nous allons concevoir une solution, pour isoler le réseau local des agences, de la Banque Extérieur d'Algerie BEA, et le transfert des fichiers sur les lignes publique du réseau X25.

La solution proposée sera dotée de trois niveaux de sécurité essentiels qui sont:

- Un contrôle d'accès au réseau
- Un mécanisme d'authentification
- Une confidentialité des données

V-1- ARCHITECTURE DE LA SOLUTION

Il existe plusieurs méthodes de structuration du réseau, pour protéger l'ensemble du réseau des *hacker*s.

L'architecture adoptée est la suivante:

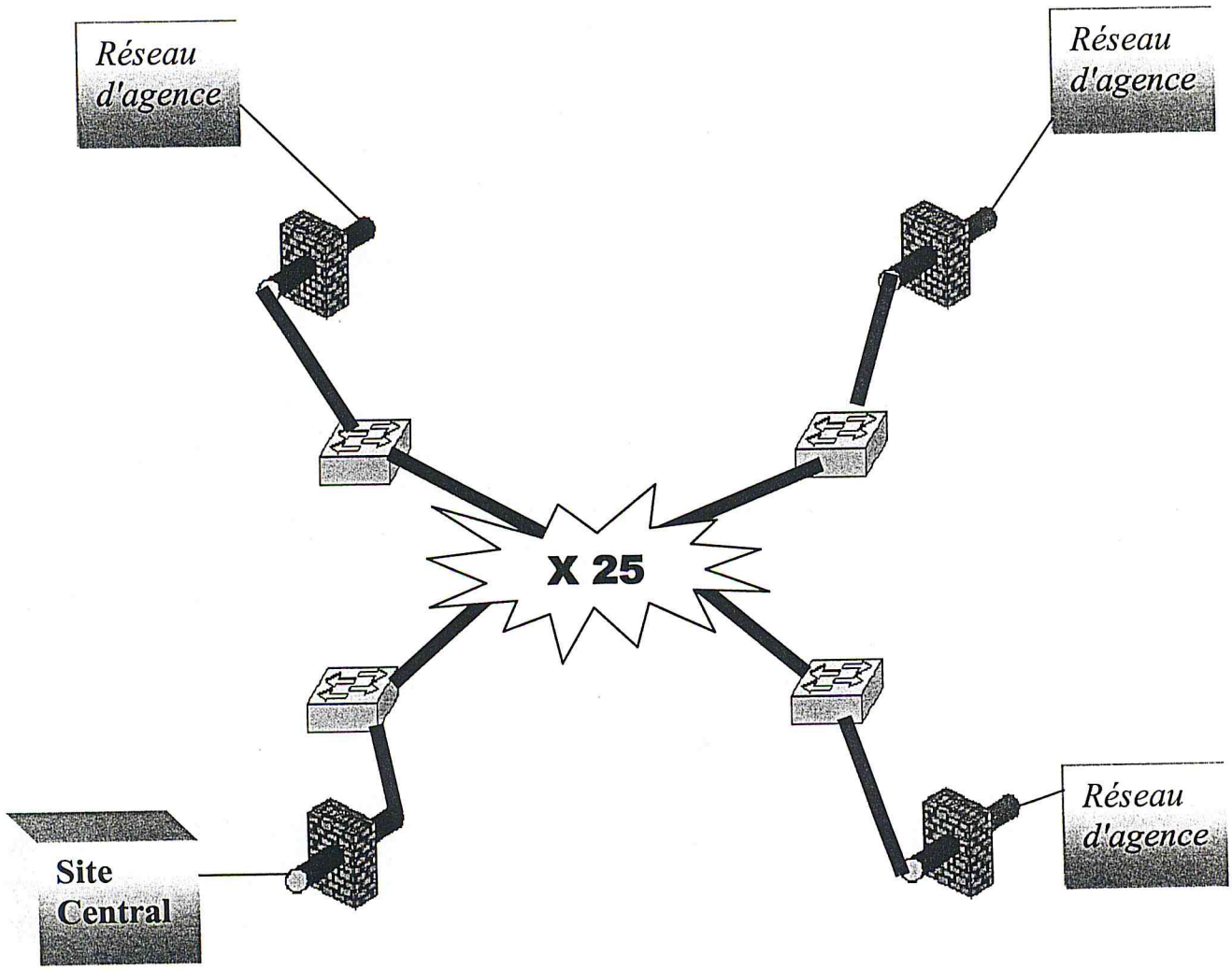
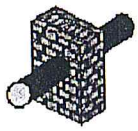
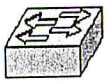


Figure V-1: Architecture de la solution de sécurité

Légendes :



: PIX.



: Routeur

: liaison sécurisé

:liaison non sécurisé .

Le PIX aurait bien pu jouer le rôle de routage, mais étant donné que le réseau bancaire dispose déjà de routeurs , alors on a préféré diminuer les tâches du PIX en lui confiant que la tâche de sécurité.

Le choix de l'architecture de sécurité étant défini, il y a lieu d'établir une politique de sécurité du réseau .

V-2- DEFINITION DE LA POLITIQUE DE SECURITE

Le réseau d'agence de la BEA, étant connecté au réseau public X25 , il est impératif de connaître exactement quelles ressources, et services il faut protéger.

V-2-1-Planification de la sécurité du réseau

La Banque Extérieur d'Algérie, où se déroule ce projet , possède des informations d'une **extrême sensibilité** et des secrets client et personnel. La circulation de ce genre de données sur les réseaux doit être protégée contre le vandalisme et le piratage. Il faut donc protéger les liaisons qui transportent ce type de données .

Avant toute mise en place d'une politique de sécurité du réseau, il faudrait étudier et répondre à un ensemble de questions telle que:

Question 1: Quelles sont les ressources à protéger ?

Réponse : Dans ce cas, c'est les fichiers comptables, et les serveurs d'agences , ainsi que les serveurs du site central.

Question 2: Quelle est l'ordre d'importance des ressources à protéger ?

Réponse : Etablir une échelle d'évaluation de la ressource : moyenne, faible ,importante , sensible ,etc..

Question 3: Quelles mesures peuvent être mises en œuvre pour protéger les actifs de manière rentable ?

Réponse : pour les ressources ***"exposées"*** comme les fichiers comptables lors de leurs transferts, une cryptographie sera mise en œuvre pour la confidentialité .

Question 4: Contre qui les ressources doivent elles être protégées ?

Réponse : Toute personne mal intentionné essayant de récupérer les donnés sensibles.

			Utilisateurs douteux	Menaces	Type de menaces	Mesures
N°	Nom	Importance				
1	Fichiers comptables	Sensible	Externe	Importante	Atteinte à la confidentialité et l'intégrité	Cryptographie + authentification
2	Serveur agence	Sensible	Externe et interne	importante	Accès non autorisé	Contrôle d'accès
3	Serveur Site central	Sensible	Externe et interne	Importante	Accès non autorisé	Contrôle d'accès

Tableau V-1: Représentation d'une politique de sécurité

V-3-POLITIQUES DE SECURITE IPSec

Les protections offertes par IPSec sont basées sur des choix définis dans une "base de données de politique de sécurité" (*Security Policy Database, SPD*). Cette base de données est établie et maintenue par un utilisateur, un administrateur système ou une application mise en place par ceux-ci. Elle permet de décider, pour chaque paquet, s'il se verra apporter des services de sécurité, sera autorisé à passer outre ou sera rejeté.

La SPD contient une liste ordonnée de règles, comportant chacune un certain nombre de critères qui permettent de déterminer quelle partie du trafic est concernée.

Les critères utilisables sont l'ensemble des informations disponibles par le biais des en-têtes des couches IP et transport. Ils permettent de définir la granularité selon laquelle les services de sécurité sont applicables et influencent directement le nombre de SA correspondante . Dans le cas où le trafic correspondant à une règle, il doit se voir attribuer des services de sécurité, la règle indique les caractéristiques de la SA (ou paquet de SA) correspondante : protocole(s), modes, algorithmes requis...

V-3-1- Echange de clefs et authentification

Pour établir une communication sécurisée, on procède ,en premier lieu, à une authentification à des fins de contrôle d'accès. Puis, un échange de clef permet l'utilisation d'un mécanisme de sécurisation des échanges : l'authentification est ainsi étendue à la suite de la communication.
Il va de soi que l'échange de clef doit nécessairement être authentifié. La combinaison de l'authentification et de l'échange de clef prend la forme d'un échange de messages appelé ***protocole d'authentification mutuelle avec échange de clef.***

V-3-1-a) Propriétés des protocoles d'échange de clef

Un protocole est dit sûr; si les deux conditions citées ci-après sont valables dans chaque instance du protocole où l'un des deux tiers, exécute le protocole honnêtement et accepte l'identité de l'autre tiers :

- Au moment où **A** accepte l'identité de **B**, les enregistrements des messages échangés par les deux tiers se correspondent (i.e. les messages n'ont pas été altérés en route).
- Il est matériellement impossible pour toute personne autre que les tiers en présence de retrouver la clef échangée.

Cependant, d'autres propriétés des protocoles d'échange de clefs peuvent être mises en œuvres :

- La propriété dite de ***Perfect Forward Secrecy*** *(PFS)* est garantie si ***la découverte par un adversaire du ou des secrets à long terme ne compromet pas les clefs de session générées précédemment*** : les clefs de session passées ne pourront pas être retrouvées à partir des secrets à long terme. On considère généralement que cette propriété assure également que ***la découverte d'une clef de session ne compromet ni les secrets à long terme ni les autres clefs de session***

- La propriété dite de ***Back Traffic Protection*** est fournie si la génération de chaque clef de session se fait de manière indépendante : les nouvelles clefs ne dépendent pas des clefs précédentes et **la découverte d'une clef de session ne permet ni de retrouver les clefs de session passées ni d'en déduire les clefs à venir.**

Le protocole utilisé pour effectuer l'opération d'échange de clefs , est le protocole IKE , le choix de ce protocole a été imposé ,en rapport à une question de standardisation d'IPSec , car il y a aussi un protocole développé pour IPSec qui a été abordé au cours de ce document , qui est SKIP.

Néanmoins, le protocole IKE présente beaucoup d'avantages, et sa force réside, en sa faculté de permettre à deux tiers, de **générer un secret partagé sans avoir aucune information préalable l'un sur l'autre.**

V-3-2-LE MODE CHOISI

Trois modes ont été abordés précédemment, deux d'entre eux concernaient la première phase du protocole IKE , ***mode agressif*** (agressive mod) et le ***mode principal*** (main mod) , et le troisième mode concernait le phase deux d'IKE, et c'est le ***mode rapide*** (Quiq mod),

Pour la conception de la solution de sécurité , le choix s'est porté sur le mode principal pour les raisons décrites ci-après .

V- 3- 2- a) Critères de choix

- ***Le mode agressif*** est le mode *hâtif* de la phase 1, il ne comprend que trois messages. Puisque la quantité d'information est la même que dans le mode principal, chacun des messages doit comporter plus d'informations.

  De plus, le répondeur doit effectuer des calculs de clefs publiques coûteux avant de pouvoir envoyer son premier message. Cette particularité est bien entendu sujette à attaque

  Le premier message sert à négocier les paramètres et les valeurs DH de l'initiateur.

  Le second message vient du répondeur. Ce message authentifie le répondeur, termine le choix des paramètres cryptographiques et l'échange DH. A ce stade toute l'information pour le chiffrement est connue. Le dernier message pourrait être chiffré mais n'a pas besoin de l'être. En effet, il sert juste à authentifier l'initiateur et assure la non-répudiation.

  Le mode agressif fournit une rapide authentification et un échange de clefs ,sans protection de l'identité.

- **Le mode principal** est le mode "prudent" de la phase 1. Il requiert six messages et offre des protections supplémentaires. Les données échangées entre les deux parties sont identiques en mode normal et agressif. Simplement, cette information est répartie sur plus de messages pour le mode principal.

  Les deux premiers messages négocient la politique de sécurité (c'est-à-dire les paramètres cryptographiques) pour le reste de l'échange.

  Les deux messages suivants sont utilisés pour l'échange Diffie-Hellman. Et enfin, les deux derniers messages servent à l'authentification (par certificat, signatures, etc...).

Ces deux messages sont chiffrés par les clefs déduites précédemment, ainsi l'identité des parties ne peut pas être connue d'un tiers.

Le mode principal offre; une authentification , un échange de clef , et une identité préservée .

V-3-3- DEROULEMENT DU MODE PRINCIPAL

La construction des messages ISAKMP repose sur le **chaînage de blocs.** ISAKMP définit 13 types de blocs différents :

Nom	**Sigle**
Security Association	SA
Proposal	P
Transform	T
Key Exchange	KE
Identification	ID
Certificate	CERT
Certificate Request	CR
Hash	HASH
Signature	SIG
Nonce	NONCE
Notification	N
Delete	D
Vendor ID	VID

Tableau V-2: Tableau des identifiants de bloc ISAKMP [JOS03]

- **Le bloc *Security Association (SA)* est utilisé pour négocier les attributs de sécurité.**
  En lui-même, il contient des champs qui indiquent le contexte de la négociation (DOI et situation). La **situation** est un paramètre qui dépend du DOI et qui permet d'indiquer quel type de politique de sécurité on désire utiliser. Une valeur de 0 pour le **DOI** pendant la phase 1 indique que l'on négocie une SA ISAKMP générique. Une valeur de 1 indique le DOI IPSec.
  Un bloc SA est toujours suivi d'un ou plusieurs blocs *Proposal*, qui permettent de faire des propositions (présentées par ordre de préférence) à l'interlocuteur.
- **Chaque bloc *Proposal* constitue une proposition d'un ensemble d'attributs relatifs à une association de sécurité.**
  En lui-même, le bloc *Proposal* indique le **mécanisme de sécurité** que l'on désire utiliser (AH, ESP...) ainsi que le **SPI** à associer à la SA si cette proposition est retenue. Comme il est possible de laisser le choix à l'interlocuteur en lui faisant plusieurs propositions, chaque bloc *Proposal* est

numéroté. Lorsque plusieurs propositions constituent un tout (par exemple si l'on veut négocier une protection par AH + ESP), elles portent le même numéro et résulteront en la création d'un paquet de SA.
Un bloc P est toujours suivi d'un ou plusieurs blocs *Transform*, qui permettent de préciser les attributs choisis pour la SA en question.

- **Chaque bloc *Transform* indique une transformation (algorithme de chiffrement, fonction de hachage...) et ses attributs.** Ces éléments dépendent bien sûr du DOI et du mécanisme de sécurité sélectionné dans les blocs précédents.
  Comme pour les blocs *Proposal*, les blocs *Transform* sont numérotés : si deux blocs portent le même numéro, ils forment un tout et doivent être sélectionnés ensemble ; des blocs de numéros différents indiquent une possibilité de choix.

Ces trois premiers types de blocs ne sont pas indépendants et on peut considérer qu'ils sont emboîtés. On désigne donc souvent par le bloc SA seul l'ensemble des blocs SA, P et T.

SA	P1	T1.1	T1.2	T1.3	P2	T2.1	T2.2
→DOI →Situation	→ Mécanisme → SPI	→ Transfo. → Attributs	→ Transfo. → Attributs	→ Transfo. → Attributs	→ Mécanisme → SPI	→ Transfo. → Attributs	→ Transfo. → Attributs

Figure V-2 Format de l'entête ISAKMP [JOS03]

L'ensemble représenté dans le schéma ci-dessus pourrait être un ensemble de propositions envoyé par un tiers à un autre. Le destinataire de ce message doit répondre par une suite identique dans laquelle il ne conserve que la proposition (ou le groupe de propositions) retenue. L'association de sécurité (ou le paquet d'associations de sécurité) résultant de cette négociation se verra attribué le SPI de la proposition retenue.

- **Le bloc *Key Exchange* sert à transporter les données nécessaires à la génération de la clef de session.** Son interprétation dépend du DOI et du protocole d'échange de clefs choisi.
- **Le bloc *Identification* sert à transporter les données nécessaires à l'identification des tiers.** Son interprétation dépend du DOI.
  Un champ intitulé *ID Type* indique le type de donnée d'identification contenu dans le bloc. Pour ISAKMP ce sont une adresse IP (IPv4 ou IPv6) ou une plage d'adresses IP (adresse / masque de sous-réseau). Chaque DOI peut définir différents types d'identification.
- **Le bloc *Certificate* fournit un moyen de transporter des certificats ou toute autre information en relation avec les certificats.**
  Un champ intitulé *Certificate Encoding* indique le type de certificat ou de donnée relative aux certificats contenue dans le champ *Certificate Data*. Les types définis actuellement sont :
  - *PKCS #7 wrapped X.509 certificate*
  - *PGP certificate*
  - *DNS signed key*
  - *X.509 certificate - signature*
  - *X.509 certificate - key exchange*
  - *Kerberos tokens*

- *Certificate revocation list (CRL)*
- *Authority revocation list (ARL)*
- *SPKI certificate*
- *X.509 certificate - attribute*

- **Le bloc *Certificate Request* permet à un tiers de réclamer un certificat à son interlocuteur.**
  Comme dans le bloc précédent, un champ indique le type de certificat requis. Un second champ, intitulé *Certificate Authority*, contient les références d'une autorité de certification acceptable par le demandeur. Ce champ est facultatif.
- **Le bloc *Hash* contient le résultat de l'application d'une fonction de hachage sélectionnée au préalable à tout ou partie du message ou à une variable d'état donnée.**
  Ce bloc peut être utilisé à des fins de vérification de l'authenticité d'un message ISAKMP.
- De même, **le bloc *Signature* contient le résultat de l'application d'une fonction de signature numérique sélectionnée au préalable à tout ou partie du message ou à une variable d'état donnée.**
  L'utilisation est la même que pour le bloc *Hash*.
- **Le bloc *Nonce* sert à transporter des aléas.**
- **Le bloc *Notification* sert à véhiculer des messages d'erreur ou d'information sur l'état actuel des négociations.** Son interprétation dépendant du DOI, celui-ci est indiqué au début du bloc.
  Le début du bloc contient également les références de l'association de sécurité concernée (mécanisme et SPI). Le message est représenté par deux champs : *Notify Message Type* et *Notification Data* (facultatif).
- **Le bloc *Delete* permet à l'émetteur de signaler à son interlocuteur qu'il vient de supprimer une association de sécurité et que celle-ci n'est donc plus valable.**
  Un seul bloc permet éventuellement d'indiquer plusieurs SA, à condition qu'elles soient toutes relatives au même mécanisme.
  Dans ISAKMP, la modification des SA se fait en créant une nouvelle SA puis en supprimant l'ancienne.
- **Le bloc *Vendor ID* peut être utilisé par un programmeur pour permettre à deux instances de son implémentation de se reconnaître** et de pouvoir ensuite utiliser des éléments propres à cette implémentation.

Dans notre cas l'échange se déroule de la manière suivante :

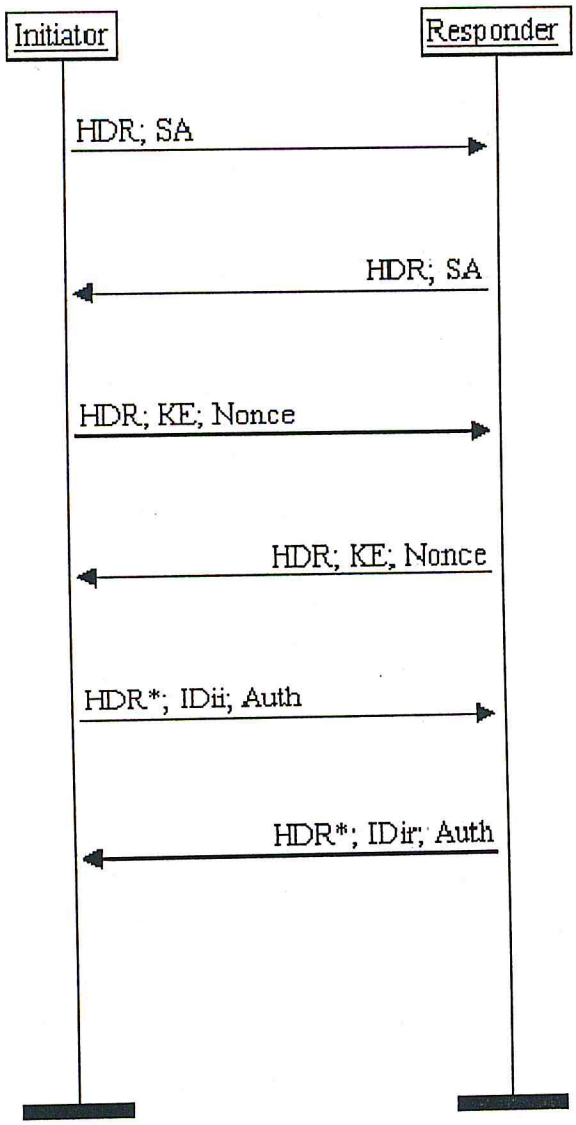


Figure V-3- Schémas fonctionnel du mode principal

- Les deux premiers messages servent à **négocier les paramètres IKE** : algorithme de chiffrement, fonction de hachage, méthode d'authentification des tiers et groupe pour Diffie-Hellman.

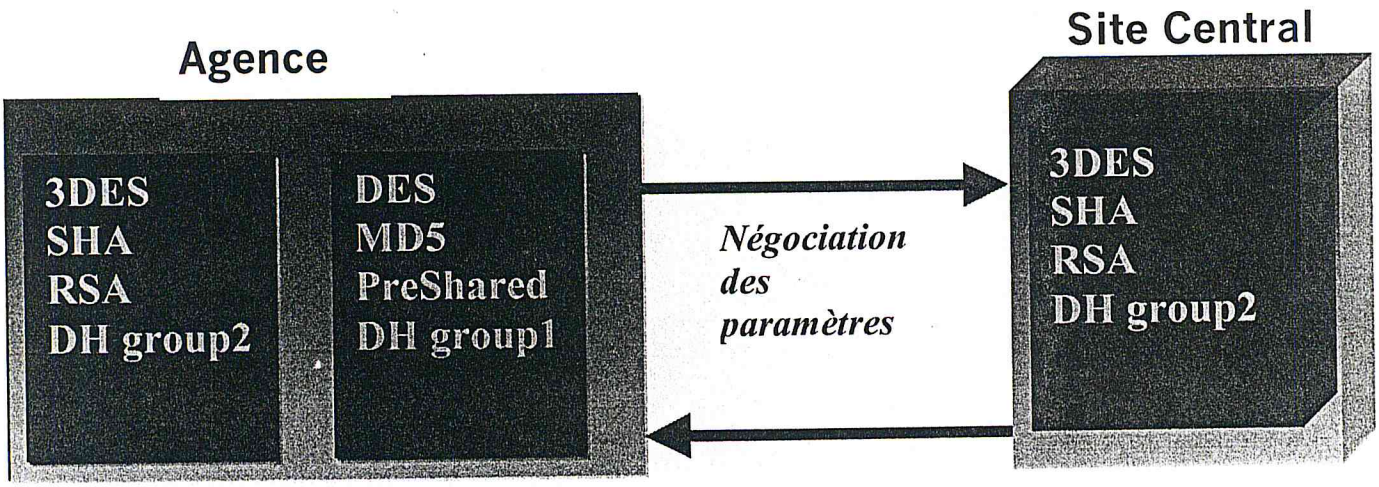


Figure V-4 :1er échange du mode principal

- Les deux seconds messages permettent l'**établissement d'un secret partagé** *via* l'utilisation du protocole Diffie-Hellman.

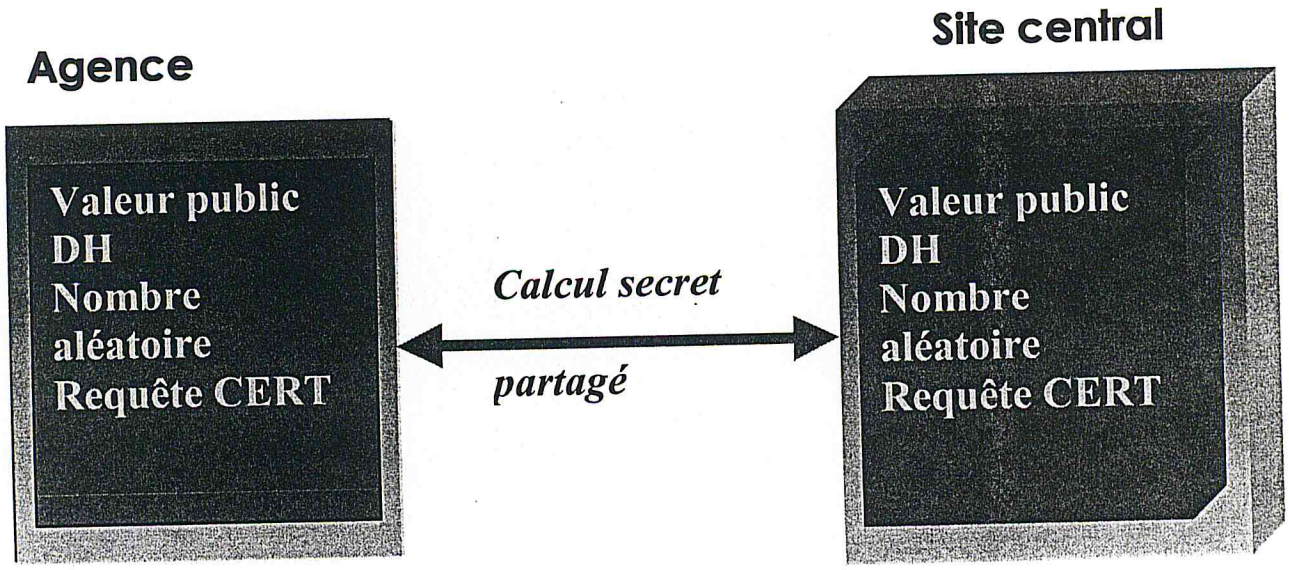


Figure 5 : 2eme échange du mode principale

- Les deux derniers messages servent à l'authentification des échanges et notamment des valeurs publiques.

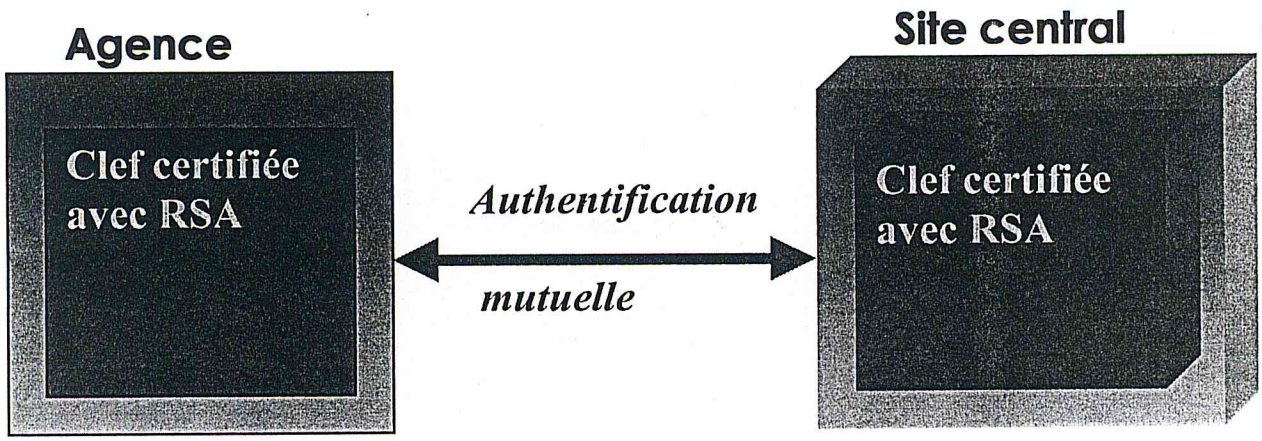


Figure V-6: 3eme échange du mode principal

V-3-4-DEROULEMENT DU MODE RAPIDE

Les messages échangés durant la phase 2 sont protégés en authenticité et en confidentialité grâce aux éléments négociés durant la phase 1. L'authenticité des messages est assurée par l'ajout d'un bloc HASH après l'en-tête ISAKMP, et la confidentialité est assurée par le chiffrement de l'ensemble des blocs du message

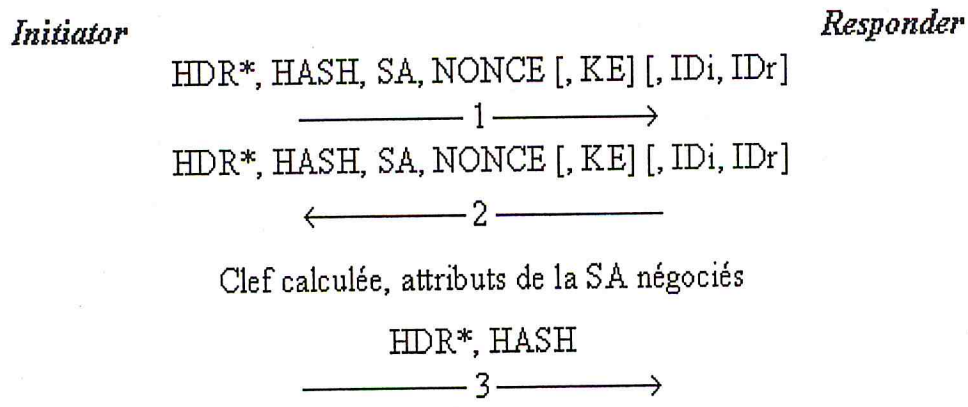


Figure V- 7: Schéma fonctionnel du déroulement du mode rapide

Dans notre cas voilà comment se déroule l'échange:

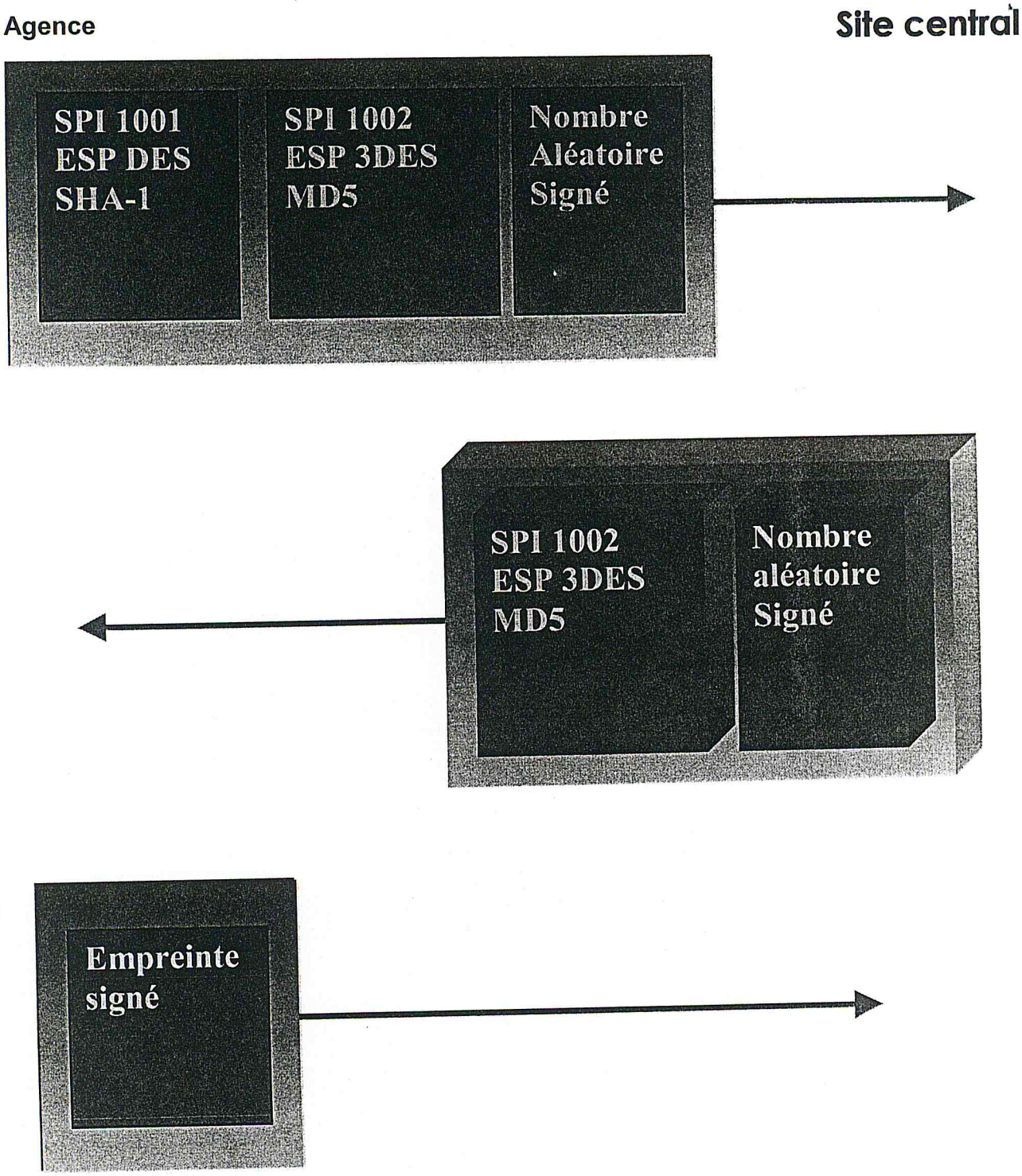


Figure V-8: Les échanges du mode rapide

V-3-5-La base de données de politique de sécurité (SPD)

Bien sûr; tous les transferts de l'agence, vers le site central, ne sont pas sujet au mécanisme de sécurité; seul le transfert de fichiers comptables, doit obligatoirement subir les mécanisme décrit ci-dessus.

Ceci étant abordé dans la politique de sécurité précédemment .
Les paquets concernés par le mécanisme de sécurité sont placés dans la SPD.

Cette base est consultée à chaque demande d'une connexion IPSec.

Dans la cas de l'envoi des paquets par une agence; cette base est consultée, pour voir si ce paquet se verra attribué certains mécanismes de sécurité.

Ainsi que lors de la réception, de paquets cette base est consultée, pour savoir si ce paquet a le droit de passer.

V-3-6- La base de données des associations de sécurité (SAD)

Des associations de sécurité ont été abordées, celles-ci sont stockées dans la base de données SAD .

Cette base est consultée, après avoir déterminé, la politique de sécurité a appliquer sur un paquet sortant de l'agence; pour savoir si SA existe déjà , ou une nouvelle SA sera établie pour ce paquet.

Cette base est aussi sujet à la consultation, lors de la réception d'un paquet IPSec, pour connaître les référence de la SA appliquée à ce paquet .

V-4-DEROULEMENT DU MECANISME GLOBAL

V-4-1-Trafic sortant

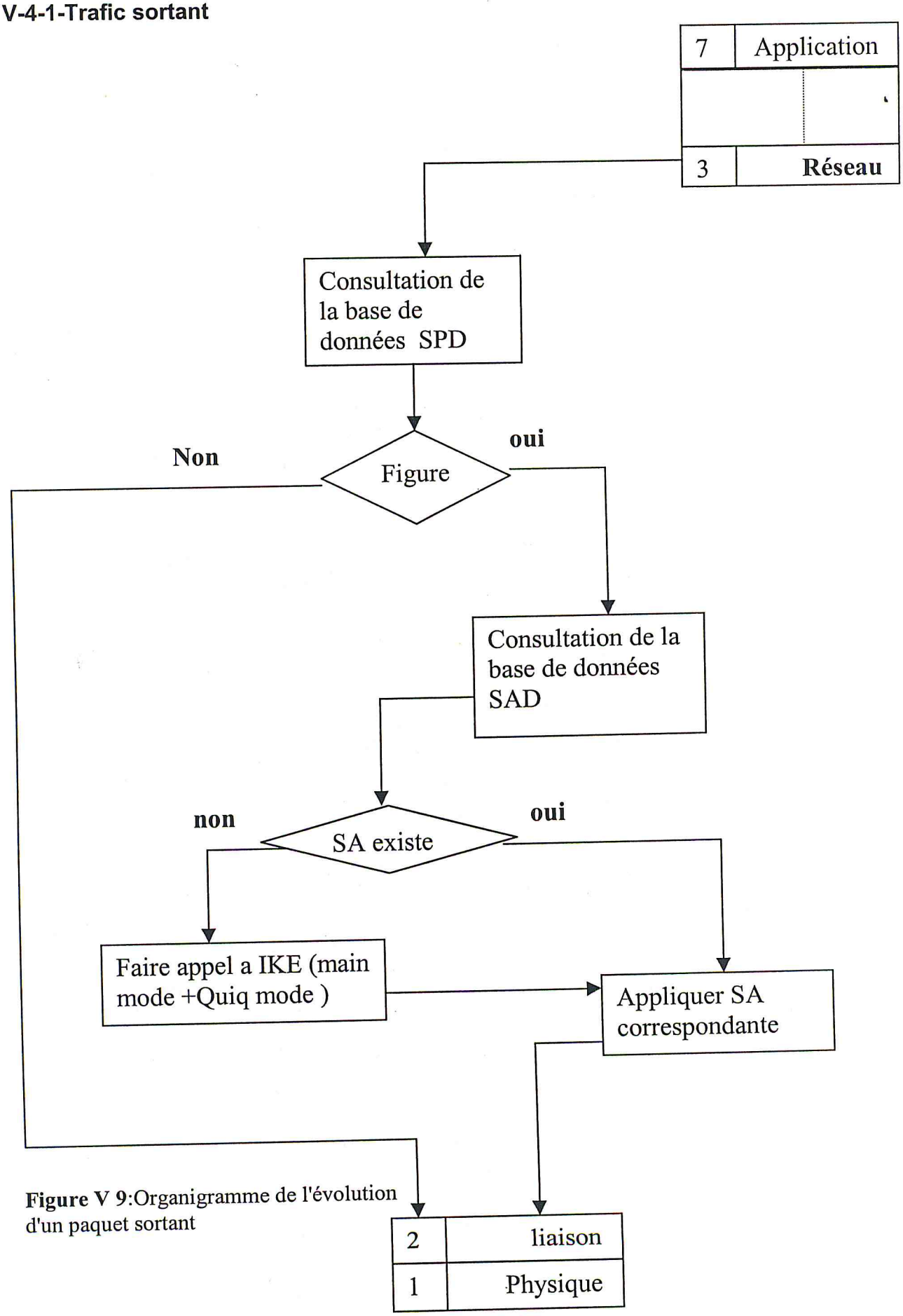


Figure V 9:Organigramme de l'évolution d'un paquet sortant

V-3-5-La base de données de politique de sécurité (SPD)

Bien sûr; tous les transferts de l'agence, vers le site central, ne sont pas sujet au mécanisme de sécurité; seul le transfert de fichiers comptables, doit obligatoirement subir les mécanisme décrit ci-dessus.

Ceci étant abordé dans la politique de sécurité précédemment .
Les paquets concernés par le mécanisme de sécurité sont placés dans la SPD.

Cette base est consultée à chaque demande d'une connexion IPSec.

Dans la cas de l'envoi des paquets par une agence; cette base est consultée, pour voir si ce paquet se verra attribué certains mécanismes de sécurité.

Ainsi que lors de la réception, de paquets cette base est consultée, pour savoir si ce paquet a le droit de passer.

V-3-6- La base de données des associations de sécurité (SAD)

Des associations de sécurité ont été abordées, celles-ci sont stockées dans la base de données SAD .

Cette base est consultée, après avoir déterminé, la politique de sécurité a appliquer sur un paquet sortant de l'agence; pour savoir si SA existe déjà , ou une nouvelle SA sera établie pour ce paquet.

Cette base est aussi sujet à la consultation, lors de la réception d'un paquet IPSec, pour connaître les référence de la SA appliquée à ce paquet .

V-4-DEROULEMENT DU MECANISME GLOBAL

V-4-1-Trafic sortant

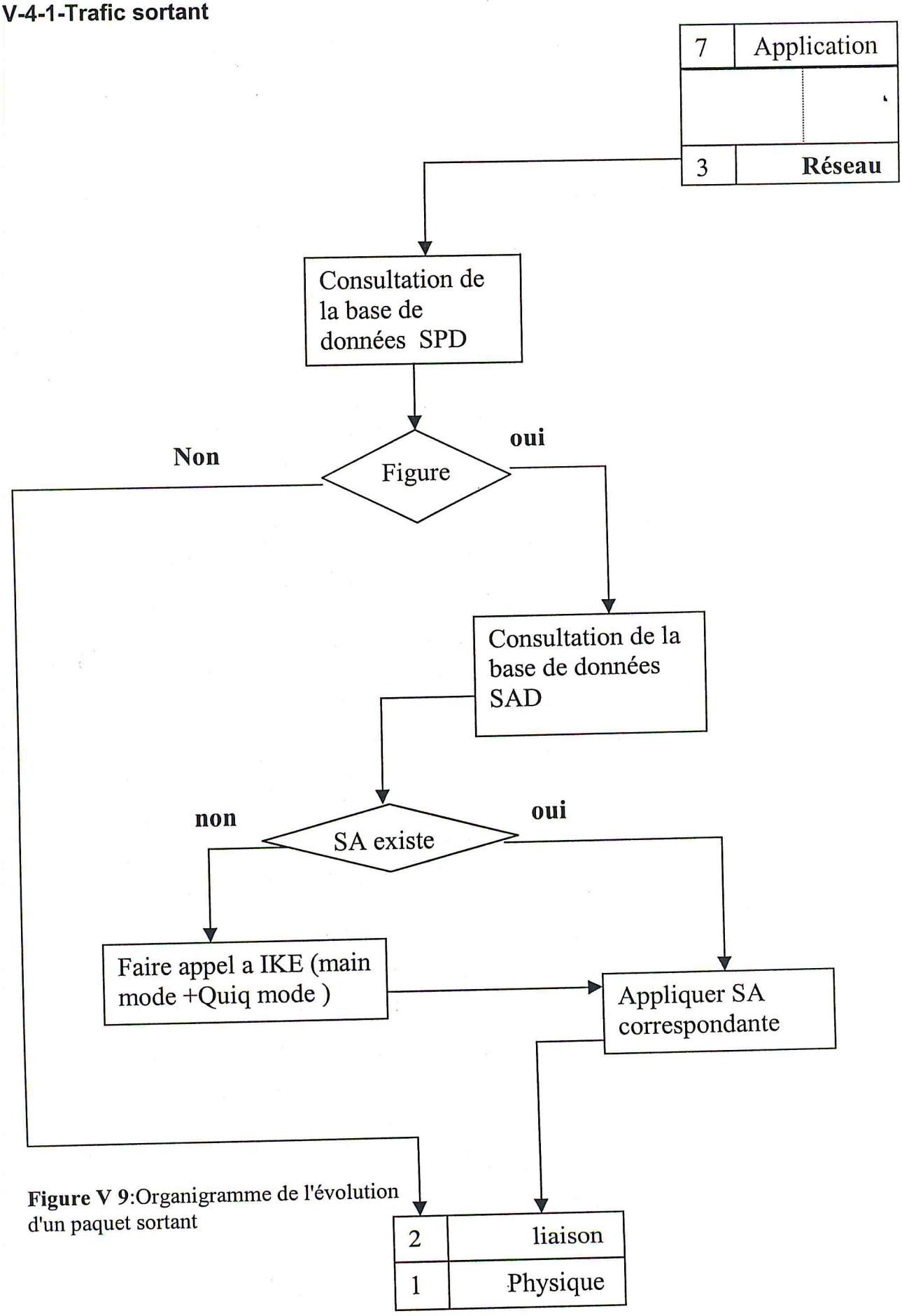


Figure V 9:Organigramme de l'évolution d'un paquet sortant

V-4-2-Trafic entrant :

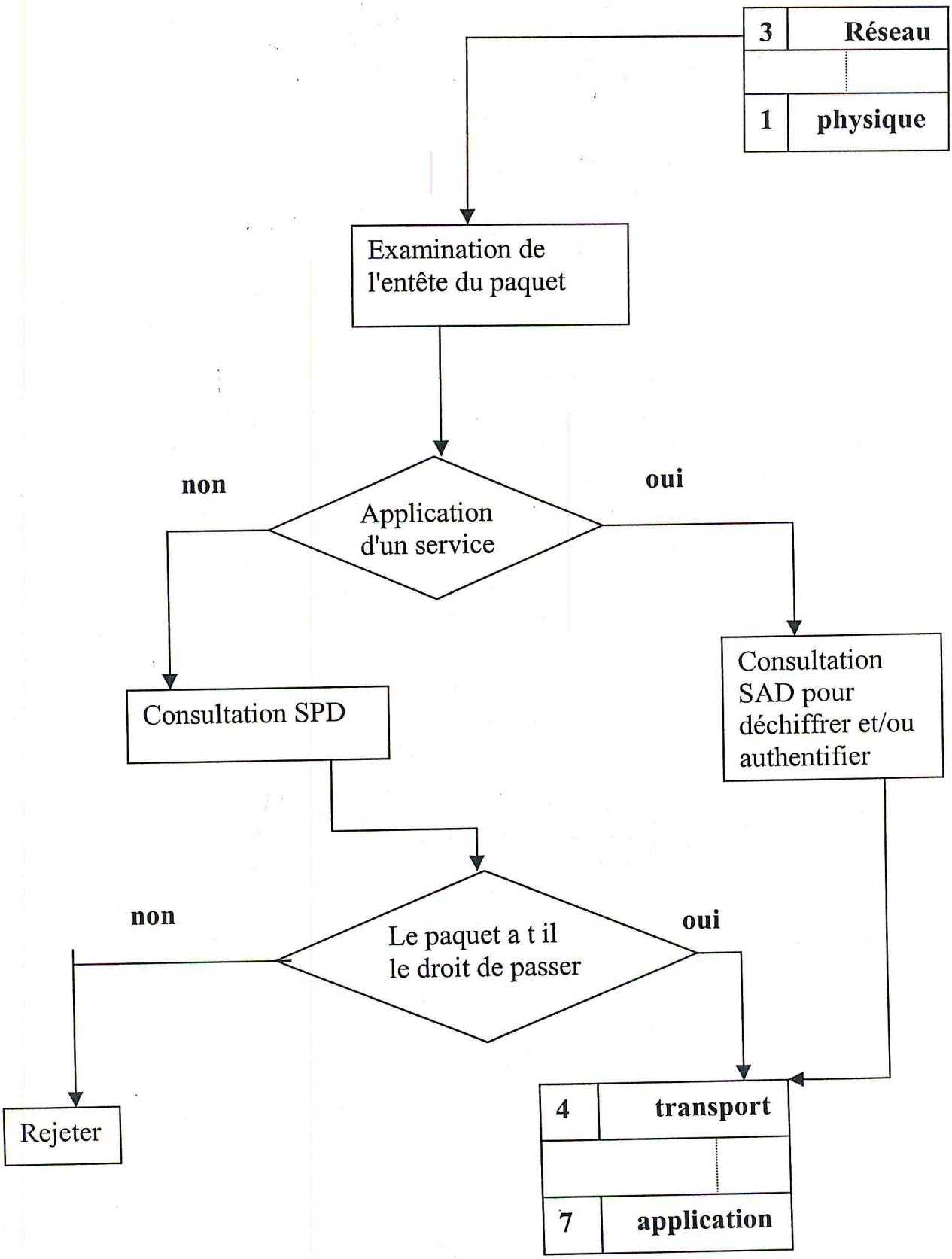


Figure V-10 : Organigramme de l'évolution d'un paquet entrant

CONCLUSION

Il y a plusieurs sortes d'implémentations de VPN . Il existe des implementations logicielles, comme materielles ,et chacune d'elle a ces aventages comme ces inconvenients , le choix de l'implementation dépendra du besoin de sécurité .

CHAPITRE VI

Mise en place des VPN

Et toutes les machines du réseau concerné par les mécanismes de sécurité auront la même adresse réseau que le PIX .

```
ip address ethernet1 @privé 255.255.255.0
```

L'autre interface sera reliée au routeur (étant donnée que les routeurs présent seront gardés, pour dégager les PIX de la tâche de routage).

Cette interface aura une adresse qui sera de même type que celle attribuée au routeur

```
ip address ethernet0 @public 255.255.255.248
```

Il faut aussi implémenter la politique de sécurité global adoptée pour le réseau. (par exemple interdire les ping)

```
access-list gl deny any any source-quench
access-list gl deny any any parameter-problem
access-list gl any any unreachable
access-list gl any any time-exceeded
access-group gl in interface ethernet0
access-group gl in interface ethernet1
```

Les règles définies ci dessus sont appliquées sur l'interface ethernet0 , et ethernet1.

Le reste de la configuration , en ce qui concerne le NAT , PAT , et les protocoles implémentés sera présentée en annexe .

VI-5-LA CONFIGURATION D'IPSEC

VI-5-1-Création de la SAD

a) SA ISAKMP

Définition des priorités des politiques de sécurité de la SAD; chaque politique étant identifiée par sa priorité .

```
isakmp policy 10
isakmp policy 20
```

Pour chaque politique il faut décrire un algorithme de cryptage :

VII-2-1-Differentes manières d'organiser l'information

L'information peut être organisée sous différentes formes allant du simple diaporama linéaire à une mise en scène complexe comme dans certains jeux.

a) Modèle linéaire

C'est la solution la plus simple à mettre en place. Le produit multimédia est vue comme un simple livre, dont on tourne les pages avec ci et là des possibilités de lancer une vidéo ou d'aller automatiquement à telle autre page qui ne soit pas la suivante ou la précédente.

b) Modèle arborescent

Evolution du linéaire, l'arborescence permet une première hiérarchisation des informations en les regroupant par thème. C'est une structure similaire à celle de l'organisation du disque dur de l'ordinateur, qui offre l'avantage d'une grande facilité de conception et d'implémentation

Quand une telle structure est choisie, certaines règles sont recommandées :

- La structure ne sera ni trop large, ni trop profonde : un maximum de 4 niveaux est conseillé.
- Pour chaque niveau, les informations sont regroupées en 5 à 7 blocs maximum car la mémoire à court terme de la majorité des individus ne peut retenir plus de données.
- Lorsque cela est possible et quand il y a beaucoup de données, un outil de recherche peut être intégré afin de faciliter l'accès à l'information : c'est le cas des sites Internet possédant un grand volume de pages-écrans.

c) Modèle libre

Dans ce cas, n'interviennent aucune (ou très peu de) linéarité ou ordre hiérarchique, chaque élément est indépendant des autres.

Quand ce modèle est adopté sur Internet avec les pages HTML, la structure peu donner un sentiment de labyrinthe, sentiment éprouvé par beaucoup d'internautes sur certains sites Web.

C'est la présence des hyperliens qui créent généralement cette impression de méandres au milieu desquels l'utilisateur peu averti risque de se perdre. En général, cette difficulté est solutionnée en introduisant un minimum de notion hiérarchique comme un retour au sommaire ou à la page précédente ou au niveau précédent.
Cette structure est la moins contraignante puisque totalement libre. La fluidité de circulation est maximum. Mais sa gestion est ardue car on a tôt fait de se perdre, aussi bien auteurs que lecteurs...

d) Modèle complexe

Ce modèle procède du graphe mathématique. Il permet d'indiquer très clairement les liens navigationnels entre les différents modules d'information. Cette représentation peut être utilisée dans le cas d'une structure présentant de nombreuses possibilités de chemins.

Par exemple, de l'unité B, on peut aller vers A C et D. Les liens peuvent être bidirectionnels : on peut aller de A vers D et de D vers A. Ils peuvent être aussi mono-directionnels : on peut aller de C vers D, mais pas de D vers C.

VII-3-UNE APPROCHE A LA CONCEPTION

VII-3-1-analyse des requis (tâches)

. qu'est-ce que l'usager veut accomplir et de quoi a-t-il besoin?

a) Scénarios d'utilisation

une suite de choix à faire et quelques informations à saisir, en fonction de la configuration adoptée.

b) Liste des informations nécessaires pour l'usager

Les informations de configuration nécessaire pour l'utilisateur lui sont fournit par l'interface, sauf les informations que l'usager lui même devra définir , celles ci sont indiquées mais pas fournies (les adresse IP par exemple).

c) Ensemble d'actions disponibles pour l'usager

l'ensemble des actions est :

- La confirmation d'ajout d'une connexion qui se traduit par la sauvegarde de la configuration;
- Faire des choix entre différentes options de configuration ;
- Génération de clefs RSA ;
- Démarrage et arrêt d'IPSec;
- Lancement et interruption des connexions VPN;

VII-3-2- Evaluation de l'analyse

. De quoi a l'air une session de travail typique?

a) fréquence des tâches

Ces tâches seront accomplies; à chaque ajout d'une nouvelle connexion, lors de la réinitialisation de la configuration , du démarrage ou l'arrêt d'IPSec, ainsi que le lancement ou l'interruption d'une connexion IPSec.

b) importance des tâches

Les tâches sont séquentielles; chacune dépend de la précédente .

VII-3-3-conception du modèle fonctionnel

. Quelle information va-t-on représenter dans l'application?

a) Informations représentées

L'information représentées; c'est des fichiers de configuration et des actions nécessaires à l'accomplissement et l'établissement d'un VPN

b) Déterminer quelles entités (objets) feront partie du modèle

Fenêtres, icônes, boutons et des check box .

c) déterminer les attributs et actions de chaque type d'entité

- ***Les boutons*** servent à valider la configuration, à visualiser les configurations ou les clefs existantes ,ils servent aussi au lancement, à l'arrêt, IPSec ,à l'établissement et l'interruption des connexions, ainsi qu'à la consultation d'erreurs.

- ***Les fenêtres*** : sont les " supports des fichiers" ,il y en à trois en tous; deux représentent les deux fichiers de configuration ; et la troisième, c'est la fenêtre de commande.

- ***Les icônes***: Elles servent à organiser les fenêtres; pour que l'utilisateur puisse se retrouver.

- ***Les check box*** : servent à faire des choix de configuration .

VII-3-4-Conception de la présentation

. Quelle sera la représentation visuelle du modèle à l'écran?

a) *disposition, hiérarchisation, standardisation*

Le model à adoptés suivant le rôle de l'interface est arborescent étant donné le séquencement des tâches ; néanmoins ,il peut arriver que l'utilisateur ai besoin de lancer une connexion déjà existante qui est désactivée , alors là, il n'aura pas besoin de passer par les étapes de configuration.

Pour cela le model choisi est un mixage entre le model hiérarchique et le model linéaire .

b) *Information immuable/modifiable*

Les informations sur l'interface ne sont pas modifiables .

c) *Choix des couleurs, tailles, icônes*

Les couleurs ont été choisit , en fonction du type d'utilisateur auquel est dédiée cette interface,: c'est une interface généralement à usage d'entreprise alors la configuration se fera par des usagers qui ont besoin de couleur apaisantes.

De nombreuse recherches et publications scientifiques, on certifié que la couleur qui apaise l'esprit humain est le ***vert.***

Aussi, la taille des polices est faite pour que l'utilisateur n'est aucun effort à faire pou lire les informations présentées.

VII-3-5-Conception des actions

. Comment manipulera-t-on les objets du modèle?

a) Choix du mode d'entrée:

- Clavier (pour saisir les informations que lui seul pourra générer) ,
- Souris (pour sélectionner les options et informations désirées).

VII-4-ERGONOMIE DE L'INTERFACE

L'ergonomie de l'interface dépend de nombreux facteurs :

- **Caractère esthétique**
- **Utilisation intuitive** : Cela signifie que, sans (ou presque sans) mode d'emploi l'utilisateur est capable de rentrer dans le produit sans trop de difficultés voire facilement (bien sur l'usager devra avoir un certain nombre de connaissance sur le produit, et qu'il sache ou il veut arriver) .
  Il y trouve les aides dont il a besoin pour continuer de manière autonome. Le caractère intuitif de l'interface repose surtout sur la manière dont la navigation a été mise en place (logique et symboles utilisés).
- **Adaptation** au niveau de l'utilisateur : Certains produits proposent d'emblée plusieurs niveaux. Indépendamment des niveaux, un produit peut être abordé de différentes manières : plusieurs entrées, choix des actions, choix des manipulations

- La **cohérence** tout au long du déroulement de l'action. L'utilisateur peut anticiper, découvrir une certaine logique qui lui permet d'avancer sans buter au moins dans le mode d'emploi du produit. L'harmonisation des écrans et la stabilité des symboles utilisés concourent à faciliter l'utilisation du produit.

- Le **contrôle** par l'utilisateur. L'impression qu'a l'utilisateur d'avoir un certain contrôle du produit est à prendre en considération. Cela peut se traduire par la possibilité d'annuler une action, de revenir en arrière, de pouvoir sortir du système, d'avoir un certain degré de liberté dans le choix du déroulement de l'action. Cependant cette notion est très variable d'un produit à un autre

- L'**interactivité** et le **feed-back**

VII-5-REALISATION DE L'INTERFACE

Le langage choisi pour la réalisation de cette interface, est le ***Kdevlop,*** et le **QTDesigner;** cette interface à été réalisée dans un environnement Linux avec une interface graphique KDE.

L'interface conçue est une interface presque intuitive; elle est conçu pour faciliter la configuration d'IPSec d'une manière conviviale et plus rapide, car l'utilisateur n'aura pas à saisir toute la syntaxe de la configuration, car il n'aura qu'à choisir entre les différentes options qui lui sont offertes par l'interface .

Aussi l'interface, suit un certain mode hiérarchique, et cela se perçoit dans l'ordre de positionnement des étapes de configuration.

VII-5-1-FICHIER *ipsec.sercets*

Dans cette interface, l'utilisateur aperçoit en premier lieu une fenêtre avec la plus part des icônes désactivées, sauf une, ce qui l'oblige à passer d'abord par elle.
Cette icône donne le choix entre l'ajout d'une nouvelle connexion ou l'effacement complet de l'ancienne configuration.

Afin de mieux diriger l'utilisateur pour connaître l'état de la configuration; il pourra se servir du bouton [**Afficher**] pour afficher la configuration existante.

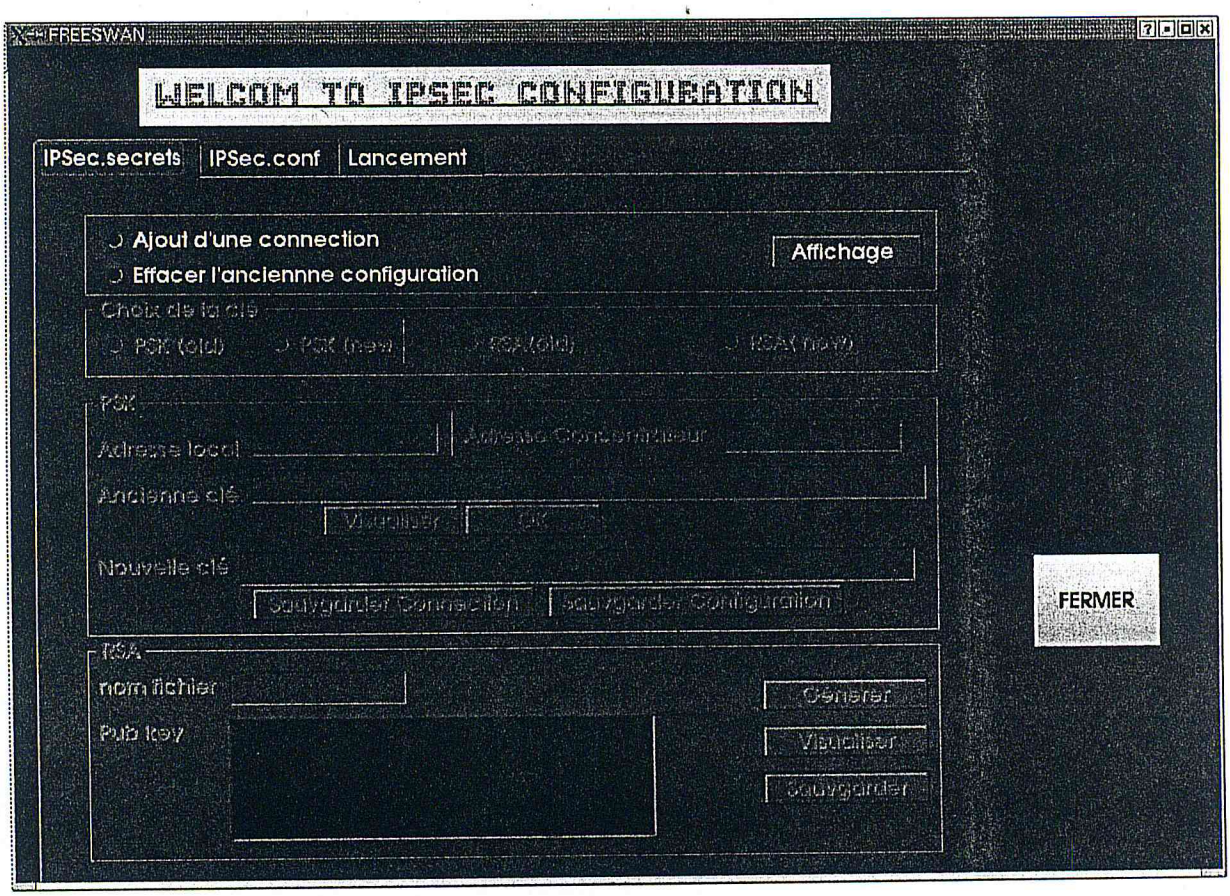


Figure VII-2: Fenêtre IPSec.secrets

Dès qu'une des deux options est cochée, les icônes concernées par la suite de la configuration s'activent

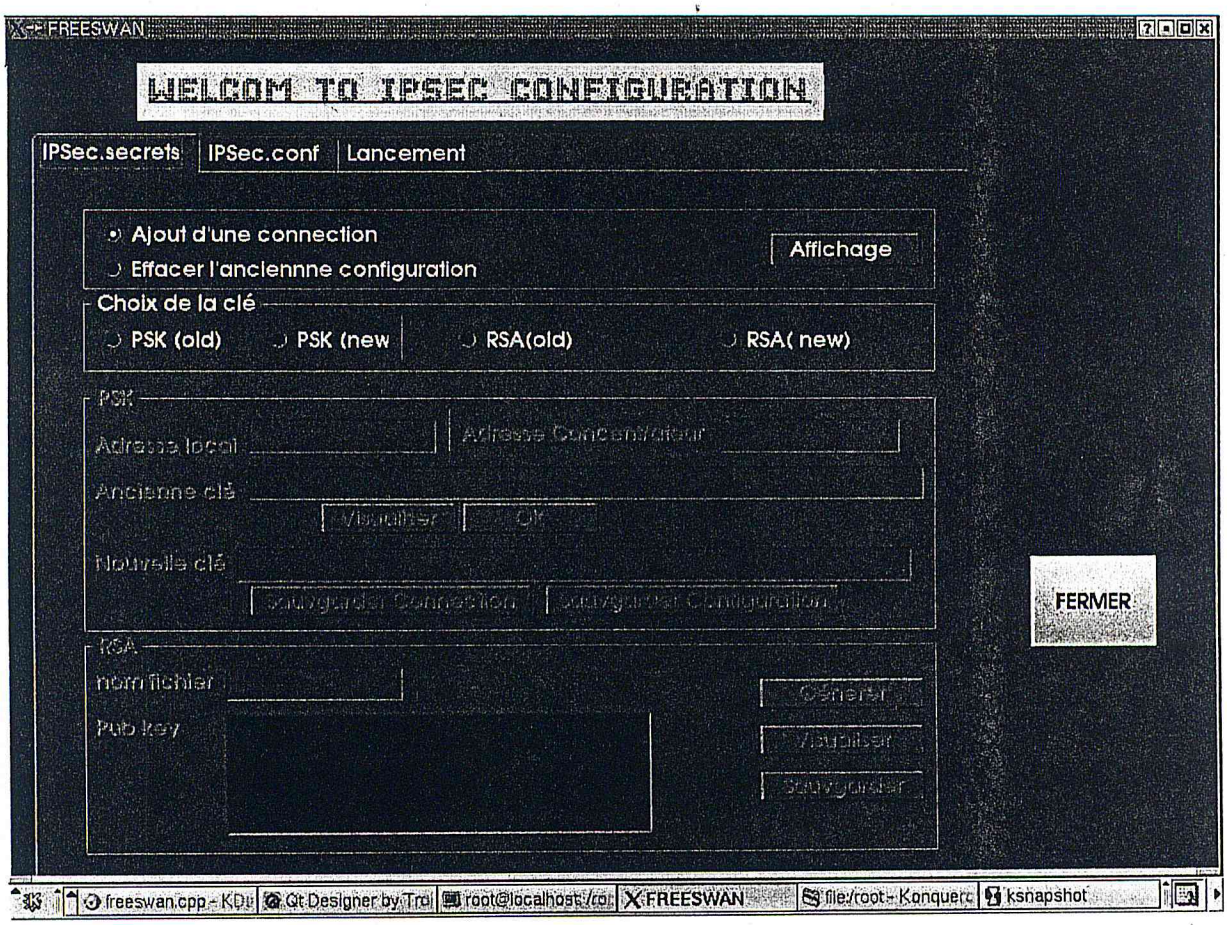


Figure VII-3 : Activation de l'icône du choix des clefs

La deuxième icône représente le choix de la clefs, sera t-elle de type RSA ou Pre Shared Key PSK?
Apres avoir choisi le type de clefs à utiliser, un autre choix s'impose pour l'utilisateur, celui d'utiliser les anciennes clefs ou de générer une nouvelle clef.

Si l'utilisateur choisit l'option [**PSK(old)**], il pourra visualiser cette clef en utilisant le bouton [**Visualiser**] . Il pourra ensuite et après avoir saisi l'adresse de l'extrémité avec laquelle il partagera sa clef secrète, il pourra la sauvegarder grâce au bouton [**OK**]

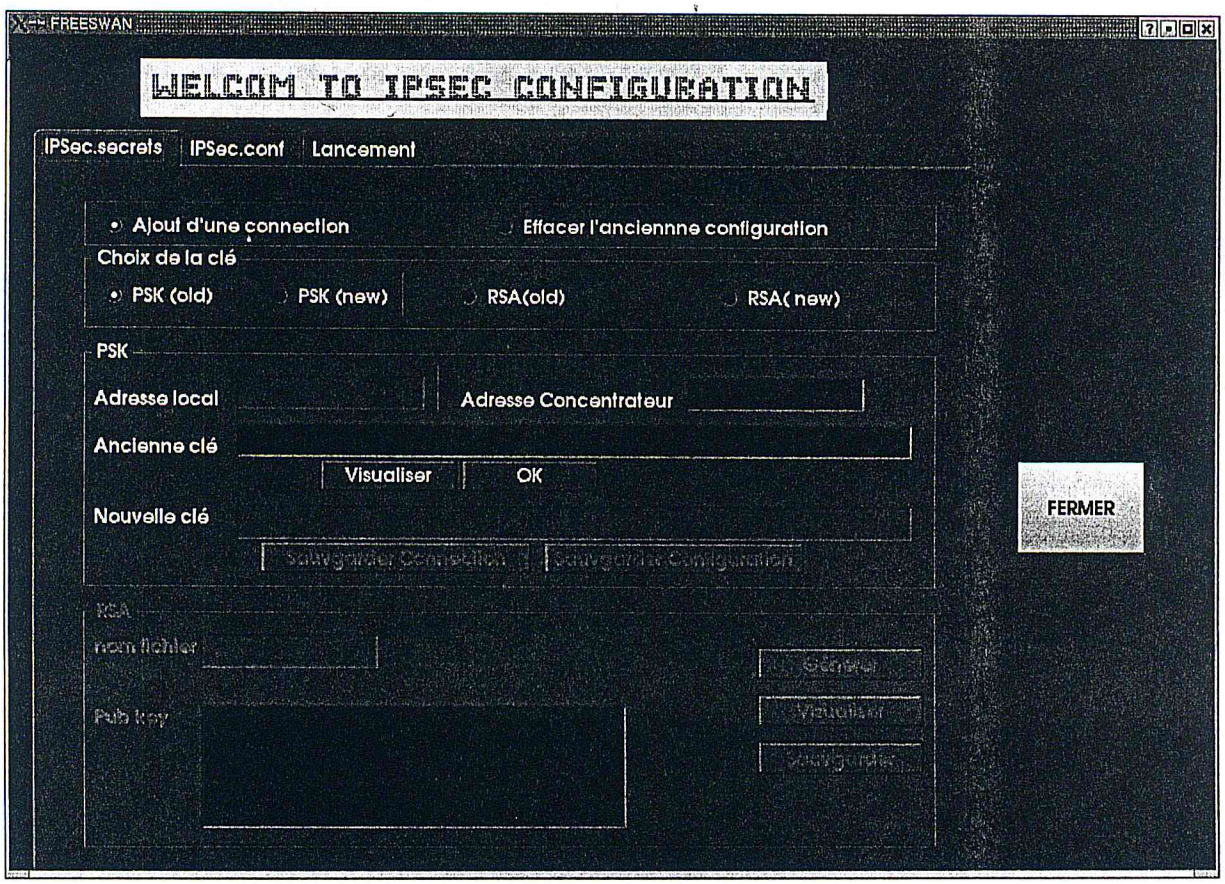


Figure VII-4 : Choix d'utiliser l'ancienne clef PSK

Dans le cas où l'utilisateur choisit l'option [**PSK(new)**], l'utilisateur n'aura qu'a saisir sa nouvelle clef PSK, et la sauvegarder.

Dans le cas où l'utilisateur choisit une configuration avec clef RSA, deux choix se présentent à lui comme dans le cas précèdent.

Seulement dans ce cas, la clef est générée et non saisie par l'utilisateur, et la partie publique (clef publique) est affichée à l'écran.

Et pour sauvegarder le tout, l'utilisateur n'aura qu'a appuyer sur le bouton [**Sauvegarder**]

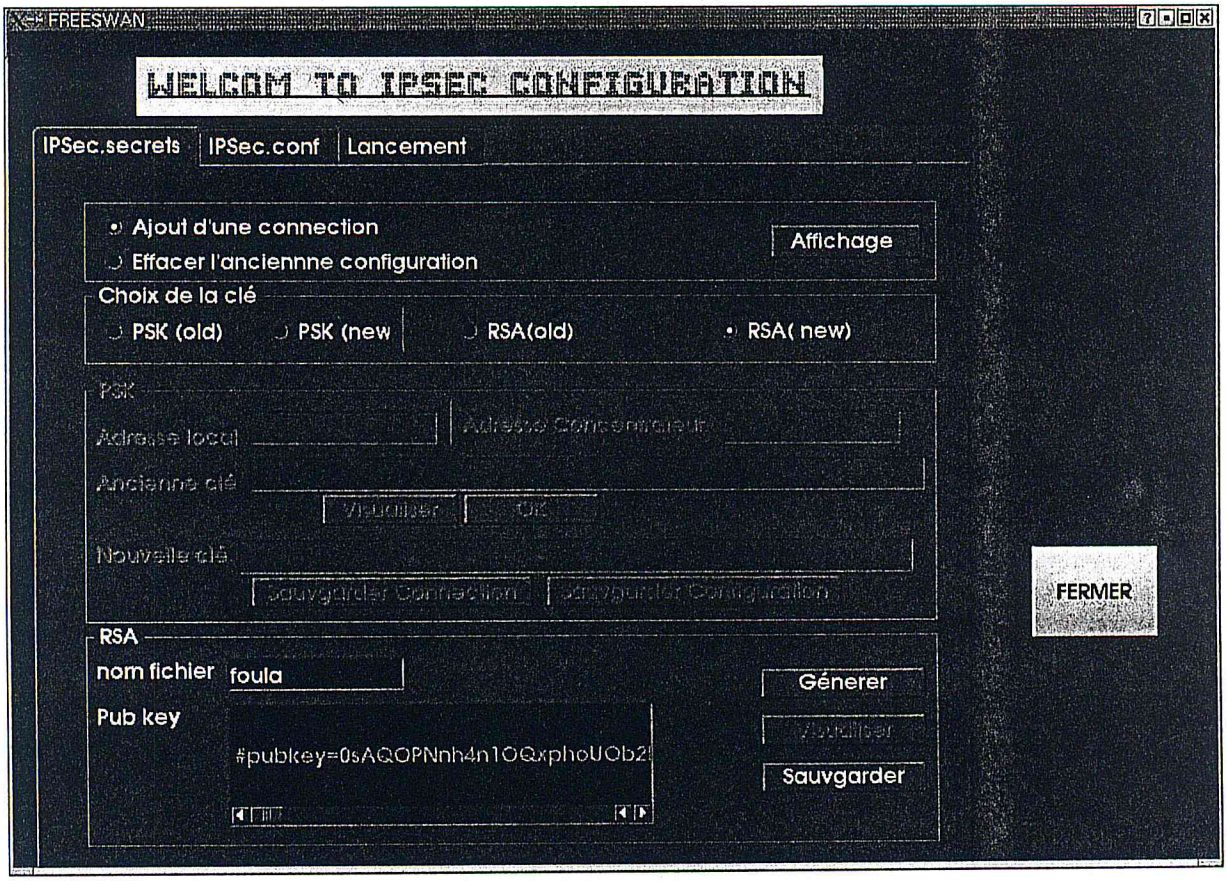


Figure VII-5: Choix d'utiliser une nouvelle clef RSA

VII-5-2-FICHIER ipsec.conf

Ce fichier nécessite deux types de configuration, l'une est faite lors d'une nouvelle configuration et l'autre à chaque nouveau besoin d'une connexion IPSec.

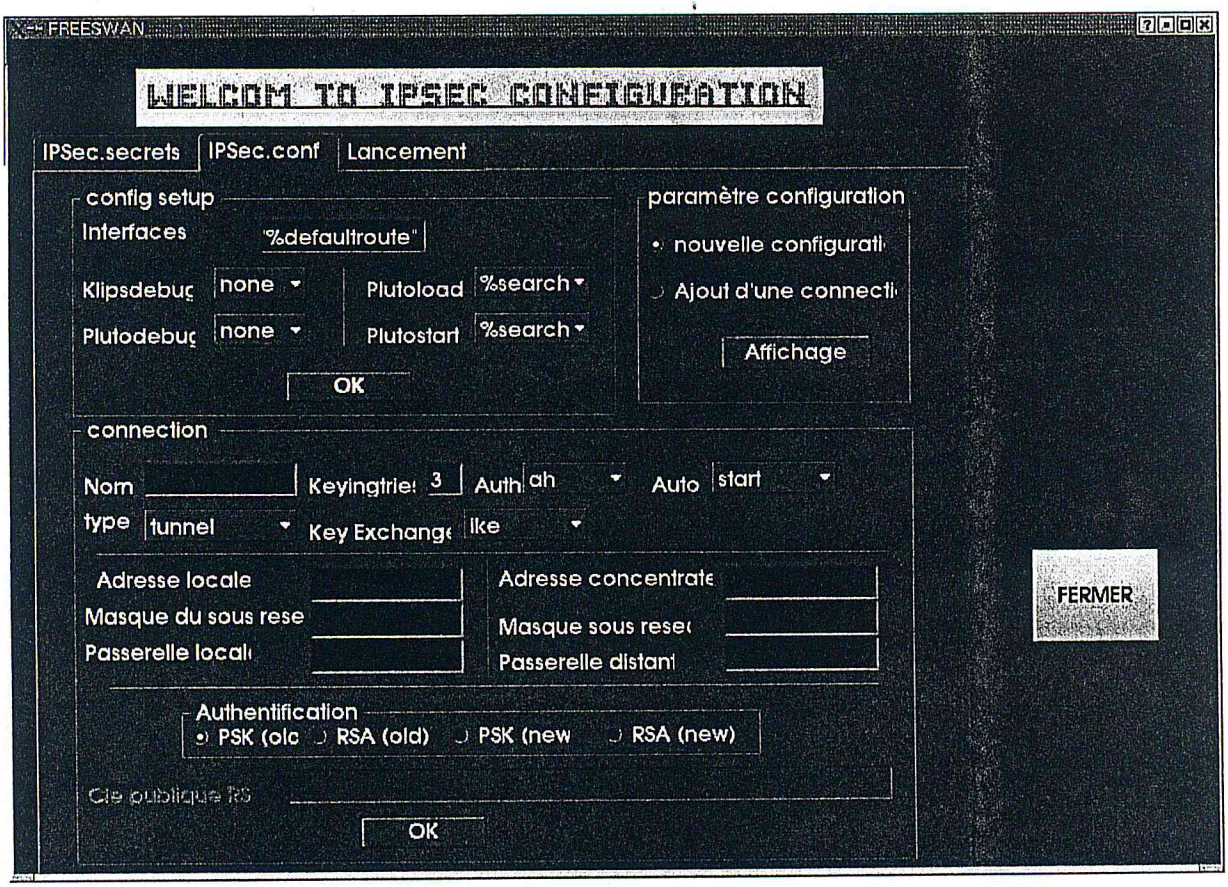


Figure VII-6: Fenêtre IPSec.conf

1- L'icône *config setup*

Cette icône contient les informations de démarrage d'IPSec :

➢ ***Interfaces :***

Exprime l'interface virtuelle et physique que IPSec utilise (l'interface sur laquelle le VPN est établi)

➢ ***Klipsdebug :***

Cette option donne le choix d'activer ou de désactiver la journalisation des logs de KLIPS et ceci par l'intermédiaire des deux options **all, none**

➢ **Plutodebug**

Cette option donne le choix d'activer ou de désactiver la journalisation des logs de PLUTO et ceci par l'intermédiaire des deux options **all, none**

➢ **Plutoload**

Définit quelle connexion doit être chargée dans la base de donnée de *pluto Pluto* au démarrage .

Si l'option **%search** est choisie alors toute les connexions, avec l'option **auto=add** ou **auto=start** seront chargées lors du lancement d'IPSec .

La valeur par défaut est **none .**

- **Plutostart**

Définit les connexions qui négocient lors du lancement d'IPSec .
La valeur **%search** définit que les connexions ayant l'option **auto =start** serons prises en charge au démarrage d'IPSec
La valeur par défaut est **none.**

Toutes les configurations précédentes sont faites qu'au début d'une configuration , lors de l'ajout d'une connexion, la configuration **SETUP CONF** n'est par touchée .

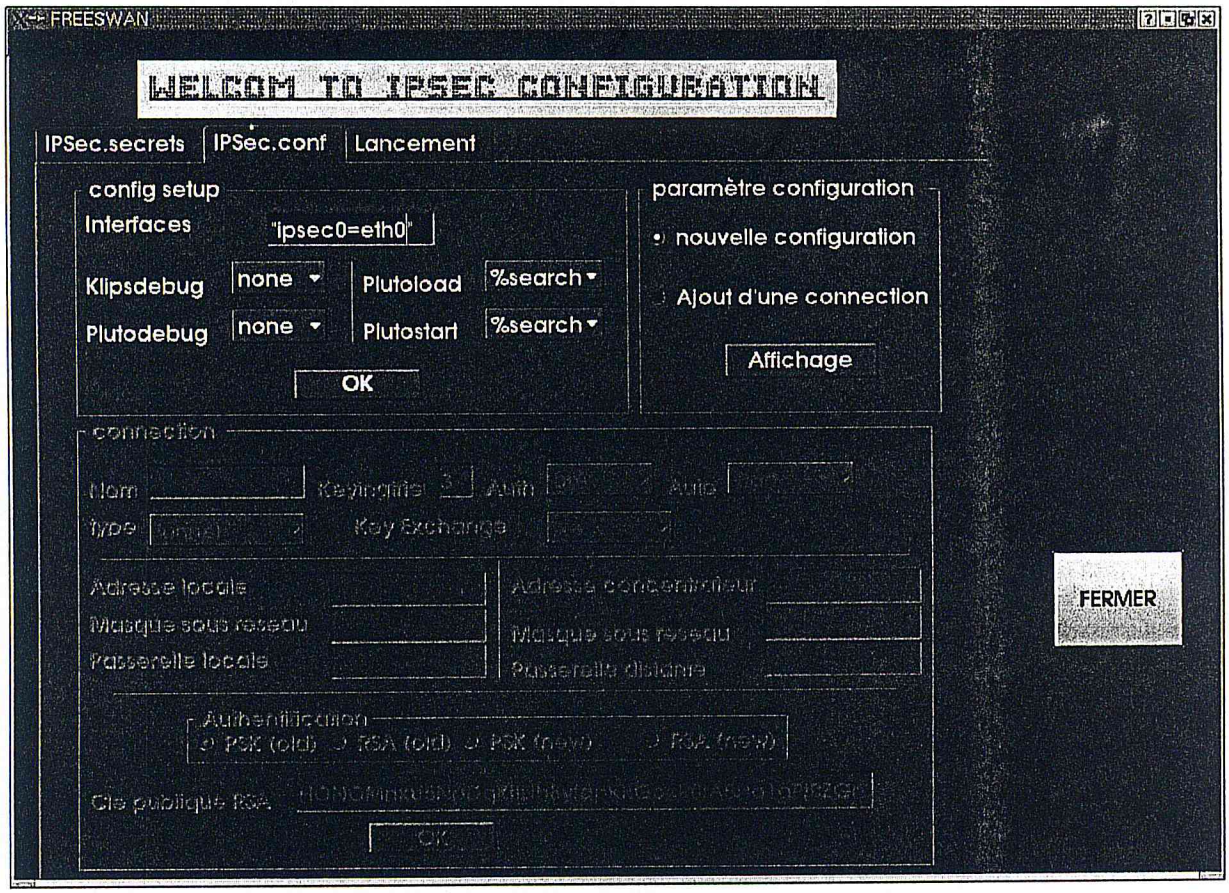


Figure VII- 7 : Icône config setup

Pour ajouter une nouvelle connexion, l'utilisateur devra cocher l'option d'ajout d'une connexion.

Comme aussi dans le fichier précédent, l'utilisateur pourra à n'importe qu'elle moment consulter la configuration existante en utilisant le bouton [**Afficher**] .

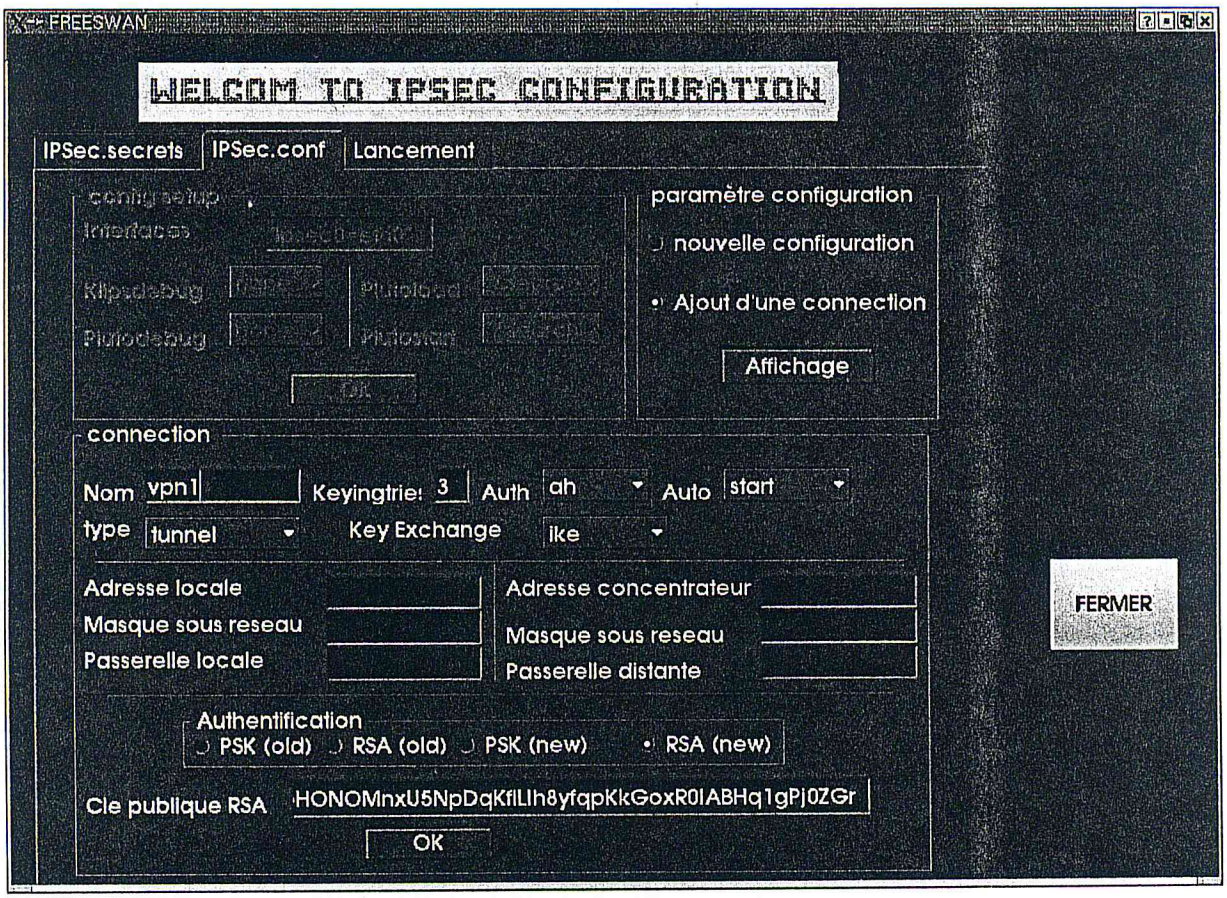


Figure VII-8: Icône connexion (paramètres de négociation)

2-L'icône connexion

Cette icône est divisée en trois parties :

La première partie définit les paramètres de négociation d'IPSec ;

- Nom : Sert à saisir le nom de la connexion, car chaque connexion est identifiée par son nom
- Type :Spécifie le type de connexion, et là deux choix se présentent; **transport** ou **tunnel .**
- Auto : Sert à spécifier si le connexion sera automatiquement charger lors du démarrage d'IPSec, et pour cela il faut choisir l'option **add;** ou bien la connexion sera lancée directement avec le lancement d'IPSec et cela en affectant l'option **start** à la variable auto
- Keyexchange : Définie la méthode d'échange de clefs
- Auth : Définie qu'elle type d'authentification (ESP avec confidentialité ou AH sans confidentialité))

- Keyingtries :combien de tentatives de négociation auront lieu; la valeur 0 définie une infinité de tentatives.

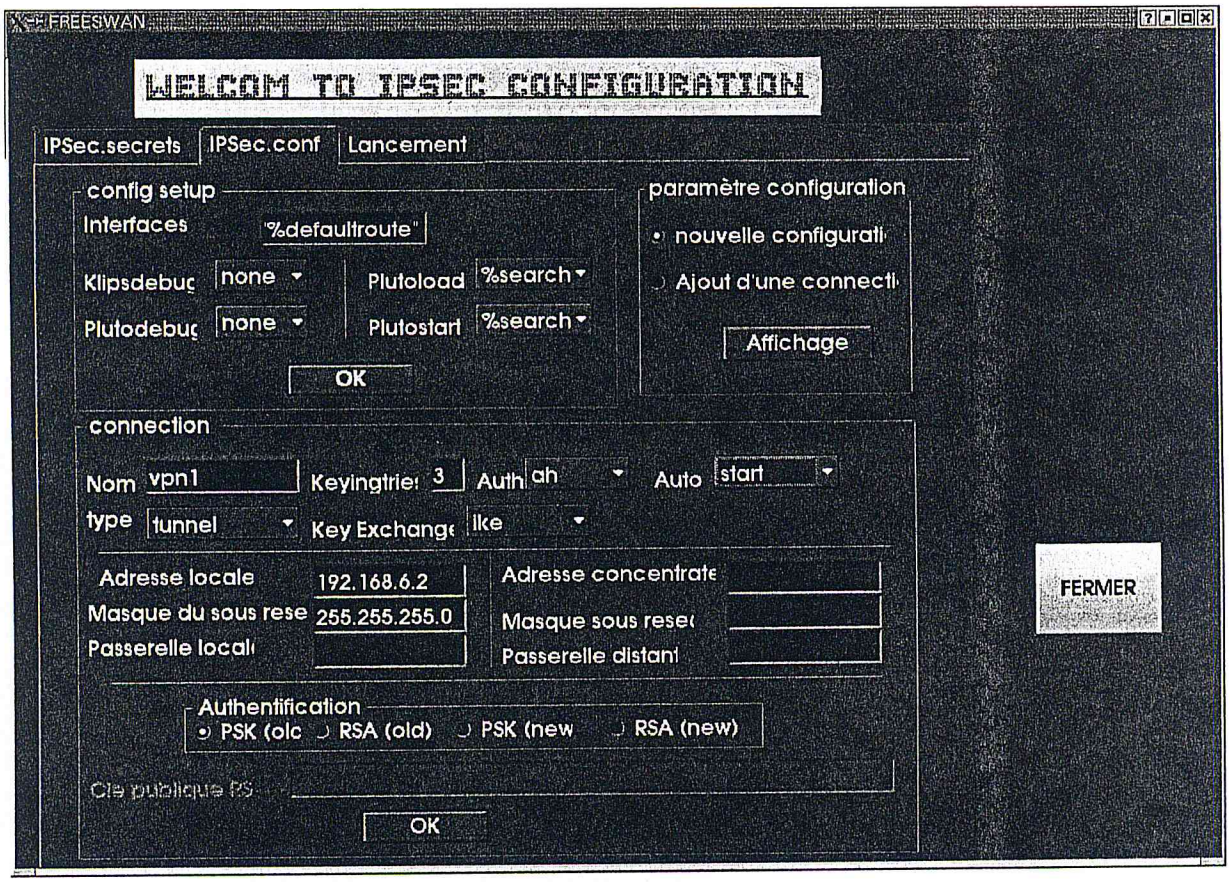


Figure VII-9: Icône connexion (adressage)

La deuxième partie est assez explicite, car elle ne consiste qu'à une simple indication du chemin.

La troisième partie consiste en le choix de la clef.

Si l'option de **PSK(old)** ou **PSK(new)** est retenue, ça veut dire que l'authentification se fera par clefs partagées .

Si l'option de **RSA(old)** ou **RSA(new)** est retenu, ca veut dire que l'authentification se fera par clef de RSA,

Et dans ce cas l'utilisateur devra reporter la clef publique de l'autre extrémité à l'endroit précisé dans l'écran .

LA FENETRE LANCEMENT

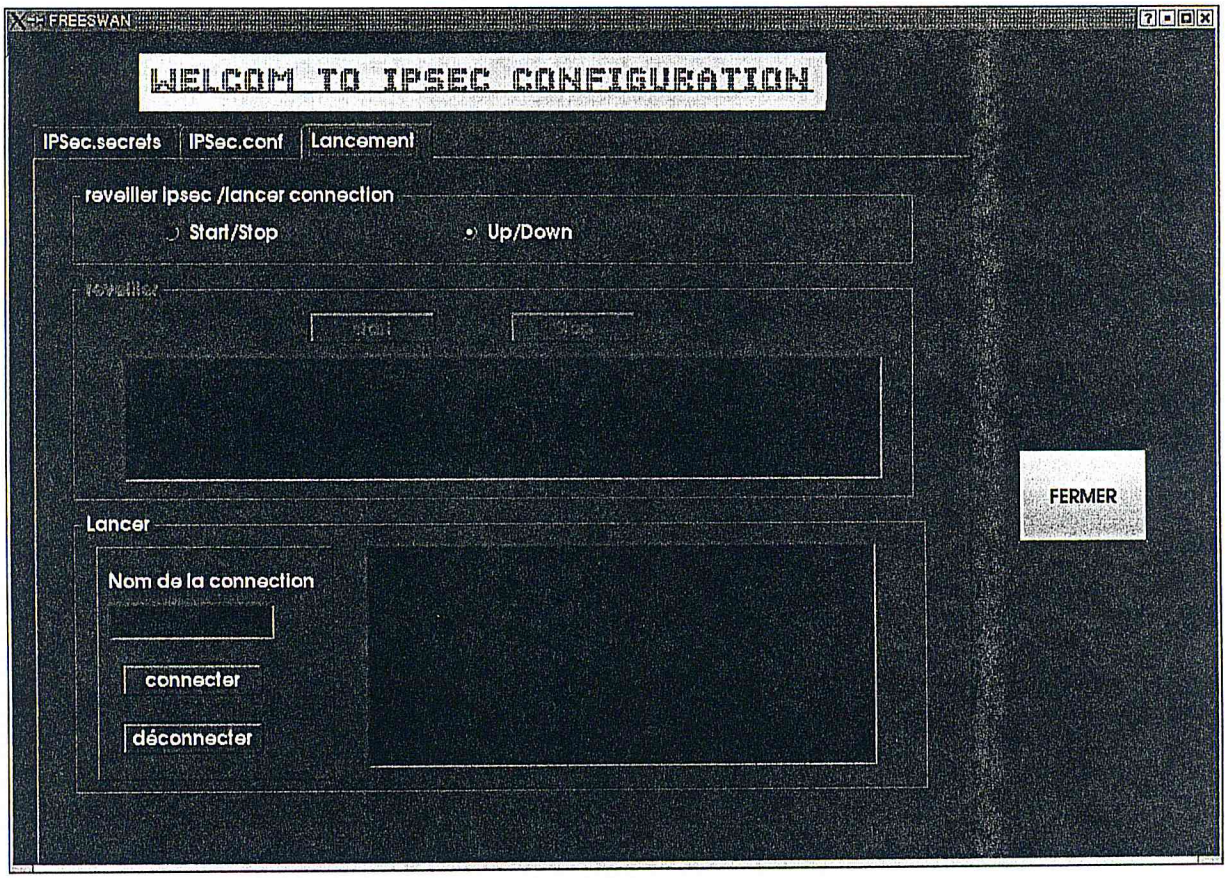


Figure VII-10: Fenêtre de commande

Cette fenêtre contient deux icônes principales:

L'icône **réveiller** :
Qui sert à démarrer le processus IPSec, grâce au bouton [**Démarrer**],
Et si tout ce passe bien le résultat se verra affiché sur l'écran de l'icône .

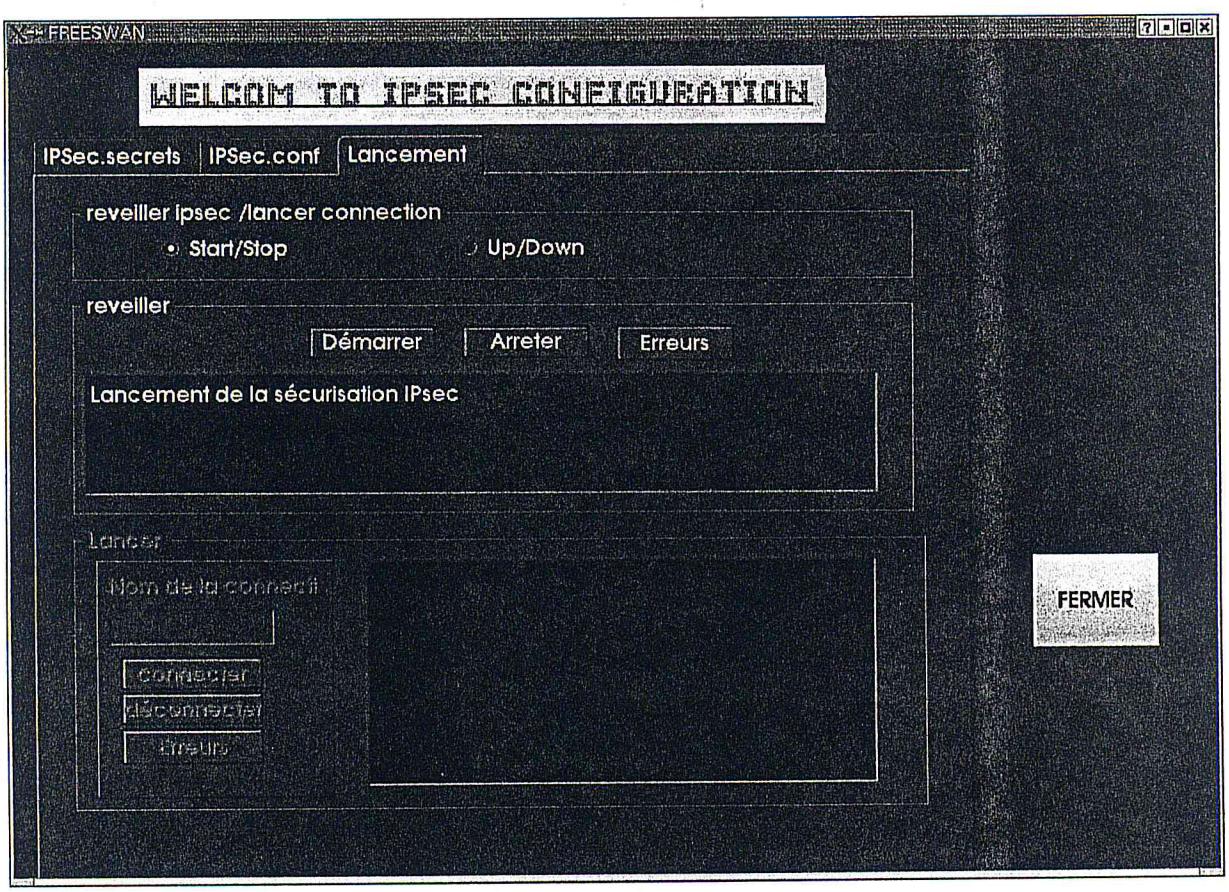


Figure VII-11: Lancement d'IPSec

Dans le cas d'un problème, un message d'échec est affiché:

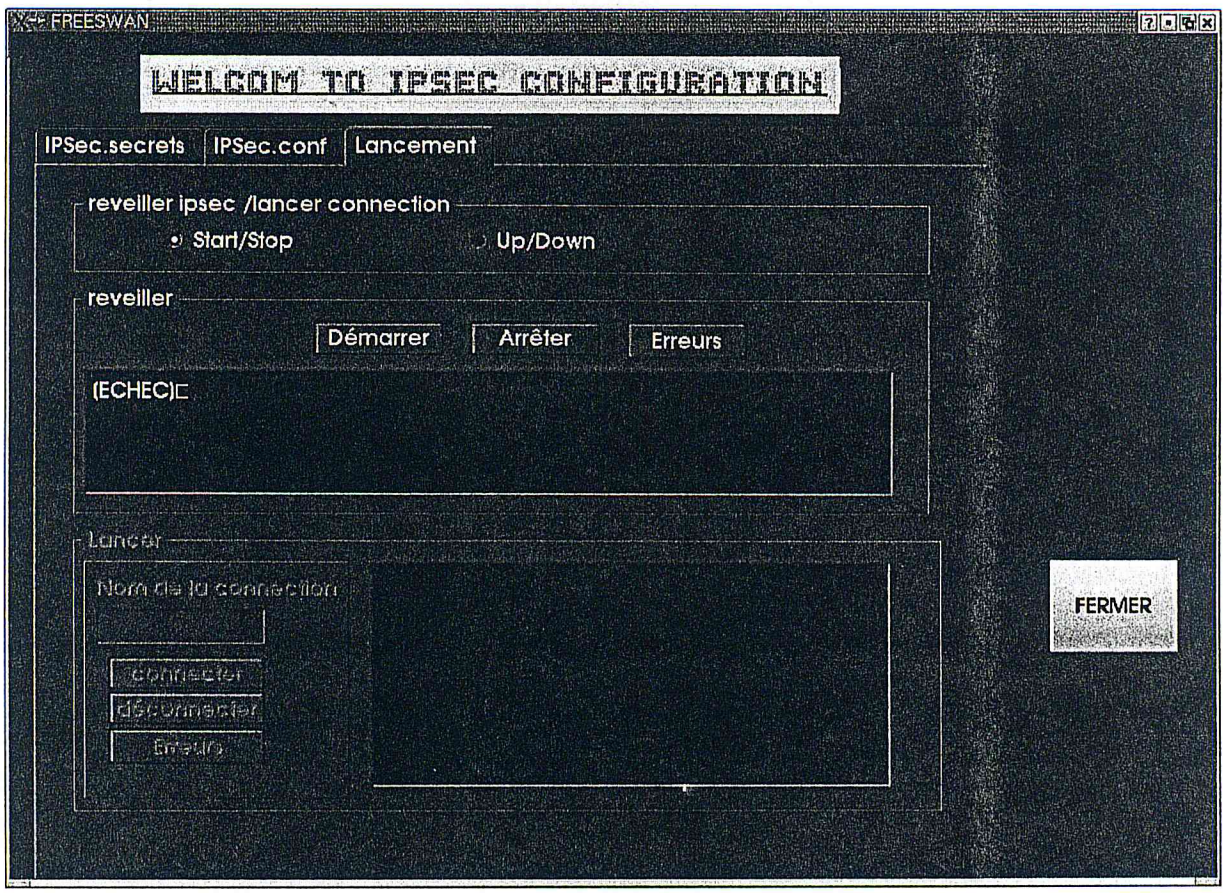


Figure VII- 12: Echec de lancement d'IPSec

Et pour l'arrêt du processus IPSec, la même procédure se répète seulement cette fois ci avec le bouton **[Arrêter]** .

Dans le cas ou l'utilisateur voudrait connaître plus de détails sur l'échec du lancement du processus, il n'a qu'a utiliser le bouton **[Erreurs]** pour afficher l'erreur qui s'est produite.

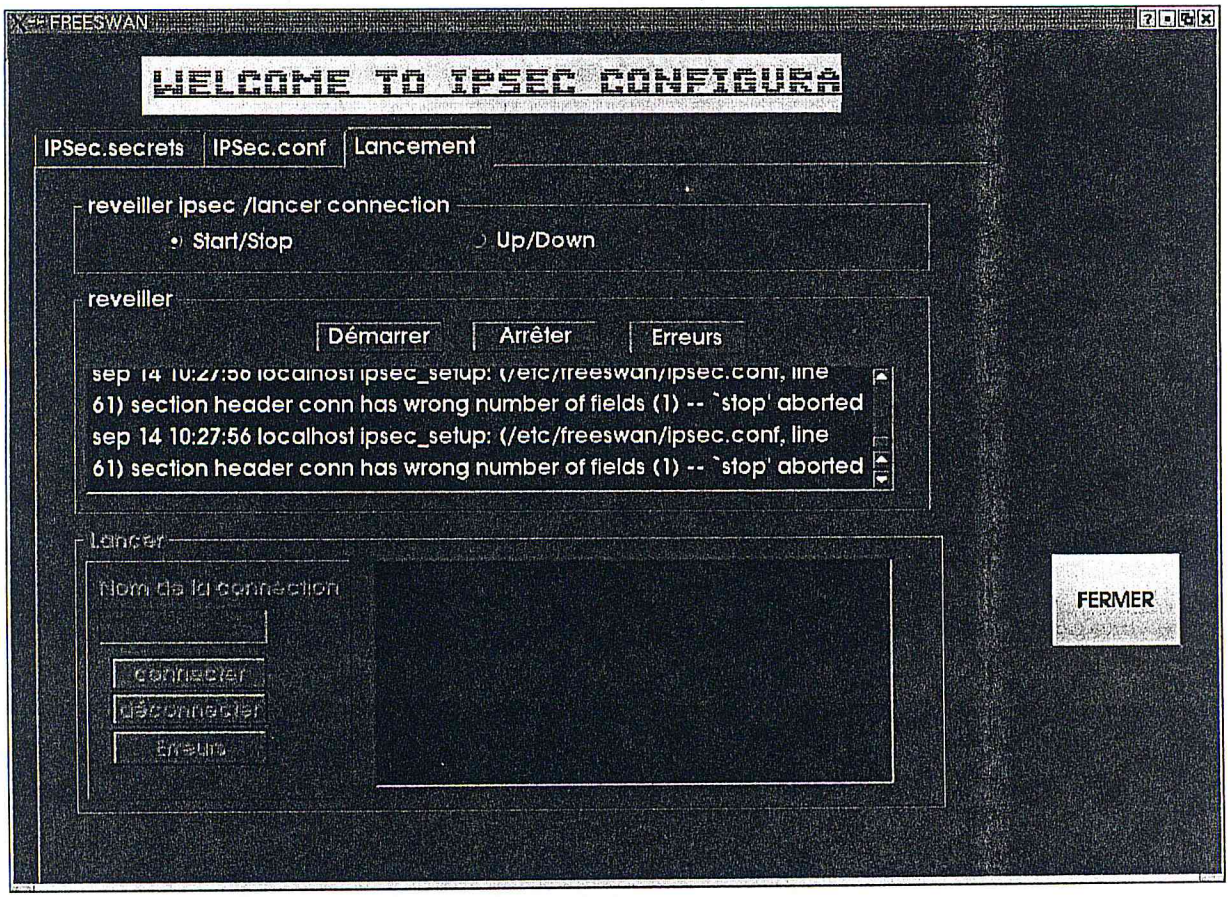


Figure VII-13: Consultation des erreurs de lancement

L'icône **lancer**

Cette icône permet le lancement et l'interruption d'une connexion VPN, en saisissant seulement le nom de la connexion et en choisissant le bouton souhaité.

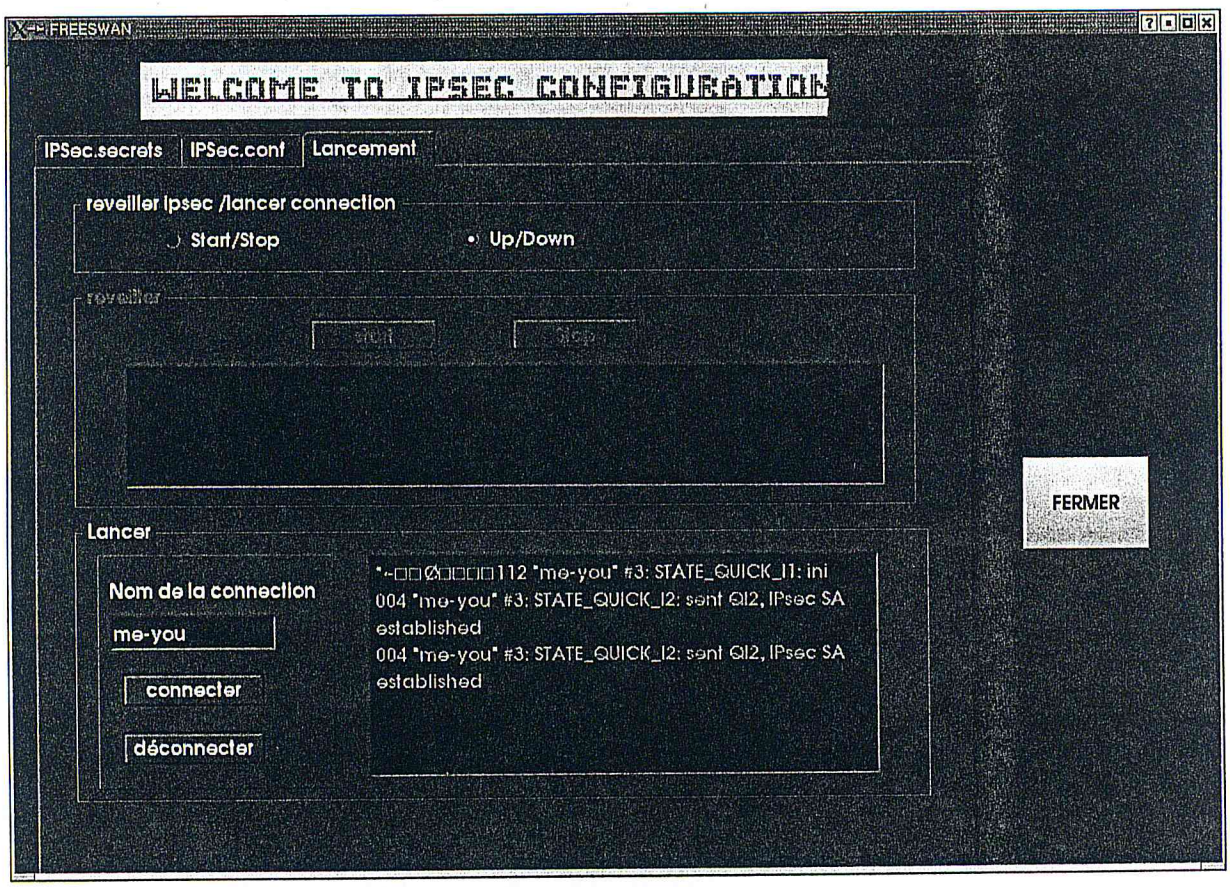


Figure VII-14: Etablissement réussit d'un VPN

L'utilisateur peut voir les phase de négociation sur l'écran de l'icône .

Aussi, il faut faire attention à bien saisir le nom de la connexion, sinon elle ne pourra jamais démarrer

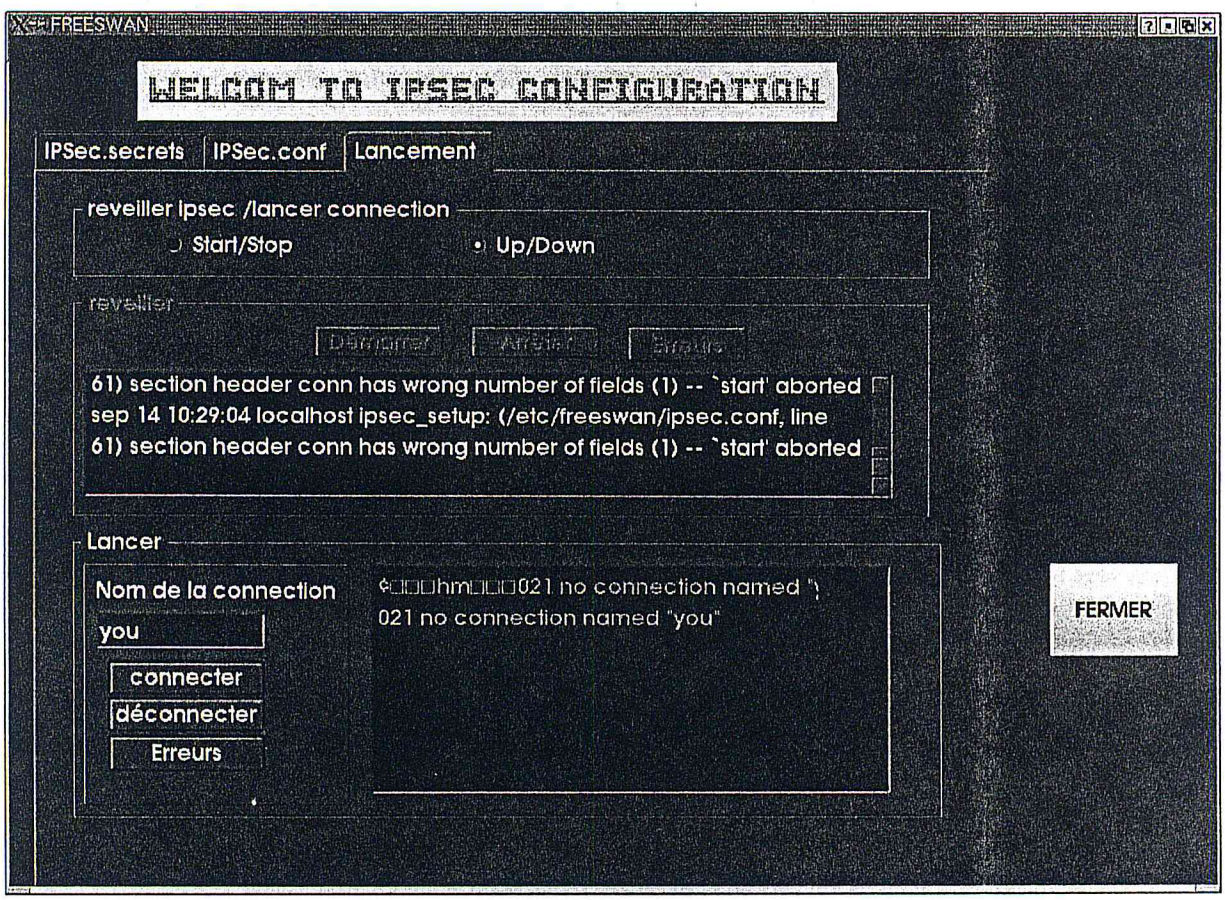


Figure VII-15: Echec lors d'établissement d'un VPN

Là aussi, si l'utilisateur veut consulter les erreurs, il n'a qu'a se servir du bouton **[Erreurs]** pour afficher les erreurs qui se sont produits.

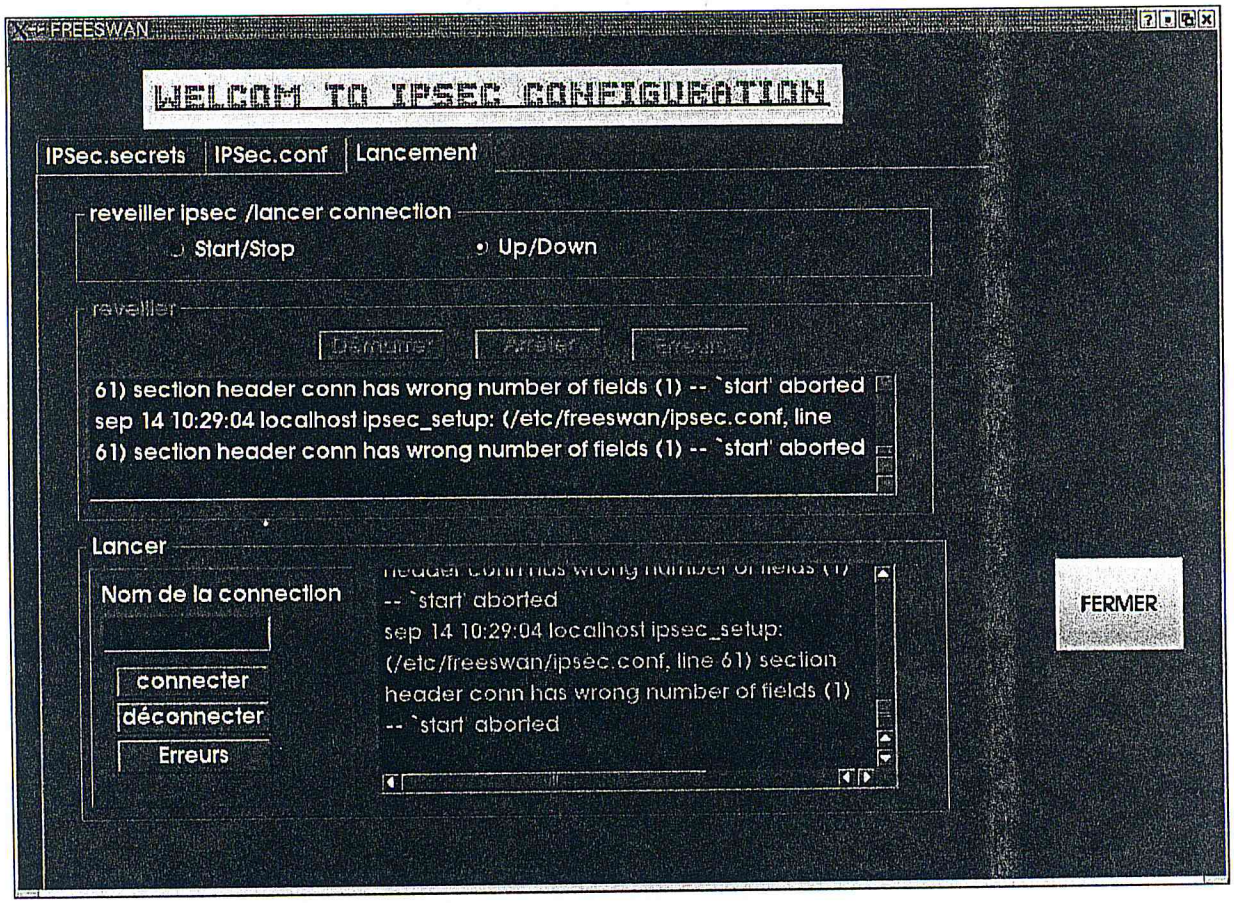


Figure VII-16: Consultation d'erreur pour l'échec de l'établissement d'un VPN

CONCLUSION

La configuration IPSec sous Linux à l'aide du logiciel FreesWan, peut être assez contraignante du fait de la manipulation de deux fichiers distincts, et du lancement des connexion par plusieurs commandes; ce qui peut induire l'utilisateur à commettre des erreurs sans qu'il se rende compte; aussi pour voir ces erreurs, il lui faut passer par plusieurs lignes de commandes.

Additionnant tous ces désagréments; et on se trouvera en face d'une perte de temps considérable .

Le but de cette application est non seulement d'offrir une interface conviviale pour l'utilisateur, mais aussi, de lui faire gagner un temps important lors de la configuration IPSec.

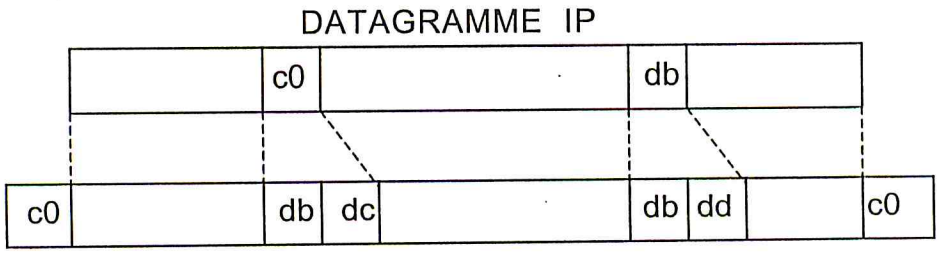
ANNEXES

ANNEXE A : SLIP/PPP

1. LE PROTOCOLE DE LIAISON SLIP:[PAS99, GIL97]

SLIP (*Serial Link Internet Protocol*, RFC 1055) est un protocole permettant d'envoyer des paquets *IP* entre deux ordinateurs reliés par une liaison série (par exemple, grâce à deux modems branchés sur les ports RS-232 et une ligne téléphonique).

Dans ce cas il n'y a pas besoin de prévoir un adressage de niveau 2, puisque la liaison est point à point (une seule machine à chaque extrémité du lien). Par contre, il s'agit de délimiter le début et la fin des paquets IP. L'encapsulation d'un paquet IP avant de l'envoyer sur la ligne consiste simplement à le faire terminer par le caractère spécial END (Oxc0) comme illustré dans la figure suivante :



Pour éviter des problèmes de bruit, certaines implantations de SLIP font également débuter l'envoi du paquet IP par un caractère END.

Pour qu'un caractère END faisant partie des données du paquet IP ne soit pas interprété comme la fin du paquet, l'émetteur le remplace par la séquence d'échappement SLIP_ESC ESC_END (0xdb 0xdc). Si le caractère SLIP_ESC fait partie des données à transmettre, alors la séquence SLIP_ESC ESC_ESC (0xdb 0xdd) est transmise à sa place.

Un des défauts de ce protocole est qu'il faut que les deux extrémités aient fixé préalablement leurs adresses IP, car la liaison SLIP ne leur permet pas de se les échanger. Si un site offre via un seul modem l'accès à Internet à plusieurs personnes, cela ne posera pas de problème.

En effet, chaque personne aura configuré son ordinateur avec le numéro IP fournit par l'administrateur du réseau et comme une seule connexion est possible à la fois la duplication du même numéro IP n'est pas gênante. Seulement, si le site offre un deuxième modem sur le même numéro téléphonique, les utilisateurs ignoreront à quel modem ils sont connectés.

À ce moment là, il faudra que le système indique à chaque utilisateur comment configurer son ordinateur en fonction de l'utilisation ou non de l'autre modem de telle manière que la même adresse IP ne soit pas donnée à deux personnes différentes simultanément.

Dans ce genre d'utilisation SLIP a le défaut de ne pas offrir d'accès contrôler par mot de passe. De plus, il n'y a pas de champ type donc la ligne ne peut pas être utilisée en même temps pour un autre protocole. Et enfin, il n'y a pas de contrôle de la transmission.

Si une trame subit des perturbations, c'est aux couches supérieures de le détecter. Malgré tout, SLIP est un protocole largement utilisé et existe aussi dans une version améliorée CSLIP (*Compressed SLIP*).

2. LE PROTOCOLE DE LIAISON PPP : [STAT98]

Le *"Point to Point Protocol"* a été conçu pour pallier les faiblesses du SLIP. Au niveau du Data Link Layer, il utilise une version modifiée du HDLC (High-level Data Link Control) et peut fonctionner au-dessus de connexions asynchrones ou synchrones. Sa seule limitation est qu'il nécessite une connexion full-duplex.

PPP recourt au LCP (Link Control Protocol) pour le contrôle de la ligne, l'établissement et la clôture de la connexion, l'échange de paramètres de configuration. Il supporte la configuration dynamique de l'adresse IP de l'appelant.

Au niveau de la couche Internet, PPP fait appel au NCP ou Network Control Protocol. En plus d'IP, PPP supporte DECNET, XNS (Xerox Network System), Appletalk, Novell IPX, NETBEUI et toute forme de LAN bridging.

PPP peut multiplexer des données en provenance de plusieurs sources ce qui rend son utilisation fort intéressante sur des lignes ISDN ou sur des connexions rapides entre bridges ou routeurs.

Lorsque la connexion d'une machine hôte vers un réseau distant s'opère via un réseau public, PPP est capable d'authentifier l'appelant via un des protocoles d'authentification associés au PPP : PAP (Password Authentication Protocol) ou CHAP (Challenge Handshake Authentication Protocol).

Format de la trame PPP

Fanion 01111110	Adresse 11111111	Contrôle 00000011	Protocole 16bits	Données	FCS 16bits	Fanion 01111110

Où :

Fanion : séparateur de trame. Un seul drapeau est nécessaire entre 2 trames.

Adresse : PPP ne permet pas un adressage individuel des stations donc ce champ doit être à 0xFF (toutes les stations), toute adresse non reconnue fera que la trame sera détruite.

Contrôle : Le champ contrôle doit être à 0x03, ce qui correspond à une trame HDLC non numérotée. Toute autre valeur fera que la trame sera détruite.

Protocole : La valeur contenue dans ce champ doit être impaire, l'octet de poids fort étant pair. Ce champ identifie le protocole encapsulé dans le champ informations de la trame.

ANNEXE A : SLIP/PPP

Informations : De longueur comprise entre 0 et 1500 octets, ce champ contient le datagramme du protocole supérieur indiqué dans le champ ''protocole''. Sa longueur est détectée par le drapeau de fin de trame, moins 2 octets de contrôle

FCS (Frappe Check Sequence) : Ce champ contient la valeur du checksum de la trame. PPP vérifie le contenu du FCS lorsqu'il reçoit un paquet. Le contrôle d'erreur appliqué par PPP est conforme à X25.

ANNEXE B : ARP

ARP : Address Resolution Protocol, ou Protocole de résolution d'adresse.

A l'allumage d'une machine, celle-ci ne connaît pas les adresses physiques (adresse MAC) de ces correspondants. Il est donc indispensable de mettre en oeuvre un mécanisme pour résoudre ce problème.

La machine commence par diffuser (broadcast) une requête ARP sur le réseau contenant l'adresse IP de la machine recherchée. Toutes les adresses MAC reçoivent la requête. Seule la machine qui reconnaît son adresse IP, répond en donnant sa adresse MAC. La machine émettrice inscrit dans un cache ARP, la correspondance entre adrese IP et adrese MAC.

Exemple de cache ARP :

IP Address	Hardware Address
193.194.3.2	0A:07:4B:12:82:36
193.194.3.3	0A:9C:28:71:32:8D
193.194.3.4	0A:11:C3:68:01:99
193.194.3.5	0A:74:59:32:CC:1F
193.194.3.6	0A:04:BC:00:03:28
193.194.3.7	0A:77:81:0E:52:FA

La structure d'une trame ARP est définie ci-dessous :

<table>
<tr><td colspan="2">Type Hardware</td><td>Type de protocole</td></tr>
<tr><td>Hlen</td><td>Plen</td><td>Opération</td></tr>
<tr><td colspan="3">Adresse hardware de l'expéditeur</td></tr>
<tr><td colspan="3">Adresse protocole de l'expéditeur</td></tr>
<tr><td colspan="3">Adresse hardware du destinataire</td></tr>
<tr><td colspan="3">Adresse protocole du destinataire</td></tr>
</table>

Où : Type Hardware : spécifie le type de l'interface hardware

Type de protocole : spécifie le type du protocole de haut niveau émis par l'expéditeur

Hlen : longueur de l'adresse hardware

Plen : longueur de l'adresse de haut niveau

Opération : type de l'opération effectuée.

ANNEXE B : ARP

Les différentes opérations qui peuvent être effectuées sont :

1 Requête ARP ; 2 Réponse ARP ;

3 Requête RARP ; 4 Réponse RARP ;

5 Requête RARP dynamique ; 6 Réponse RARP dynamique ;

7 Erreur RARP dynamique ; 8 Requête InARP ;

9 Réponse InARP.

Reverse ARP :

Le RARP est utilisé par des NetWork Computeurs (machines sans disque dur), qui ont une adresse MAC, mais ne connaissent pas leur propre adresse IP. Dans ce cas, ces machines interrogent un serveur spécialisé.

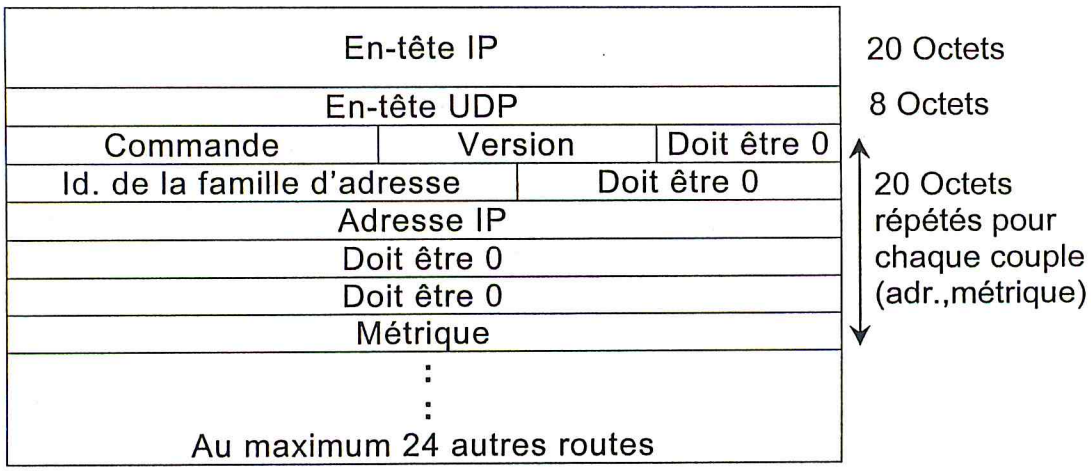
Les trames RARP ont le même format que les trames ARP. Dans une trame Ethernet, le protocole RARP est désigné par: 0835

ANNEXE C : RIP/OSPF

L'un des protocoles de routage les plus populaires est *RIP* (*Routing Information Protocol*) qui est un protocole de type *vecteur de distance*. C'est-à-dire que les messages échangés par des routeurs voisins contiennent un ensemble de distances entre routeur et destinations qui permet de réactualiser les tables de routage.

Ce protocole utilise une métrique simple : la distance entre une source et une destination est égale au nombre de sauts qui les séparent. Elle est comprise entre 1 et 15, la valeur 16 représentant l'*infini*. Ceci implique que RIP ne peut être utilisé qu'à l'intérieur de réseaux qui ne sont pas trop étendus.

Un message *RIP* est encapsulé dans un datagramme *UDP* de la manière décrite dans la figure suivante, *RIP* utilise *UDP* sur le port 520.



Le champ *commande* fixé à 1 indique une requête pour demander tout ou partie d'une table de routage et fixé à 2 pour transmettre une réponse (d'autres valeurs hors normes actuellement existent également).

Le champ *version* est positionné à 1 et à 2 dans la version de *RIP2*. Pour des adresses *IP*, le champ *identificateur de famille d'adresses* est toujours fixé à 2.

Quand un routeur *RIP* démarre, il interroge ses fichiers de configuration pour savoir à quels réseaux il est physiquement rattaché. Il envoie ensuite des paquets broadcast à ces réseaux pour annoncer ses services.

Le fonctionnement normal de *RIP* consiste à diffuser des réponses soit toutes les 30 secondes, soit pour une mise à jour déclenchée par la modification de la métrique d'une route.

Une réponse contient une adresse de destination, accompagnée de sa métrique, de l'adresse du prochain routeur, d'un indicateur de mise à jour récente et de temporisations.

ANNEXE C : RIP/OSPF

Le processus *RIP* met à jour sa table de routage locale en examinant les entrées retournées dont il vérifie d'abord la validité : adresse de classe A,B ou C, numéro de réseau différent de 127 et 0 (sauf pour l'adresse par défaut 0.0.0.0), numéro d'ordinateur différent de l'adresse de diffusion, métrique différente de l'*infini*. *RIP* effectue ensuite les mises à jour propres à l'algorithme *vecteur de distance* suivant :

- Si l'entrée n'existait pas dans la table et si la métrique reçue n'est pas infinie, alors on ajoute cette nouvelle entrée composée de la destination, de l'adresse du prochain routeur (c'est celui qui envoie la réponse), de la métrique reçue. On initialise la temporisation correspondante.

- Si l'entrée était présente avec une métrique supérieure à celle reçue, on met à jour la métrique et le prochain routeur et on réinitialise la temporisation.

- Si l'entrée était présente et que le routeur suivant correspond à l'émetteur de la réponse, on réinitialise la temporisation et on met à jour la métrique avec celle reçue si elles diffèrent.

- Dans les autres cas on ignore l'entrée.

Cette méthode correspond à l'algorithme de Bellman-Ford de recherche de plus courts chemins dans un graphe.

Un des défauts de *RIP* est de ne pas gérer les adresses de sous-réseaux. Mais de telles entrées peuvent être annoncées via une interface appartenant à ce sous-réseau pour pouvoir bénéficier du masque qui y est attaché et être correctement interprétées. Enfin, *RIP* met un temps assez long (quelques minutes) pour se stabiliser après la défaillance d'une liaison ou d'un routeur ce qui peut occasionner des boucles de routage.

RIP2 est un protocole qui étend *RIP* en utilisant les quatre champs laissés à 0 par *RIP* dans ses messages. Le premier sert à fixer un *domaine de routage* identifiant ainsi celui qui a émis le paquet et le quatrième *l'adresse IP d'un routeur de saut suivant*. Ces deux champs ont servi à lancer simultanément plusieurs initialisations de routage sur un même support, leur utilisation a été abandonnée.

Le deuxième champ est un *identificateur de route* pour supporter des protocoles de routes externes et le troisième sert à spécifier un *masque de sous-réseau* pour chaque entrée de la réponse.

OSPF (*Open Shortest Path First*) est un nouveau type de protocole de routage dynamique qui élimine les limitations de *RIP*. C'est un protocole *d'état de liens*, ici un routeur n'envoie pas des distances à ses voisins, mais il teste l'état de la connectivité qui le relie à chacun de ses voisins. Il envoie cette information à tous ses voisins, qui ensuite le propagent dans le réseau.

Ainsi, chaque routeur peut posséder une carte de la topologie du réseau qui se met à jour très rapidement lui permettant de calculer des routes aussi précises qu'avec un algorithme centralisé.

En fait, *RIP* et *OSPF*, sont des protocoles de type *IGP* (*Interior Gateway Protocol*) permettant d'établir les tables des routeurs internes des *systèmes autonomes*. Un système autonome peut être défini par un ensemble de routeurs et de réseaux sous une administration unique.

Cela peut donc aller d'un seul routeur connectant un réseau local à Internet, jusqu'à l'ensemble des réseaux locaux. La règle de base étant qu'un système autonome assure la connexité totale de tous les points qui le composent en utilisant notamment un protocole de routage unique.

À un niveau plus global, Internet apparaît donc comme une interconnexion de systèmes autonomes comme illustré dans la figure suivante :

Dans chaque système autonome les tables sont maintenus par un *IGP* et sont échangées uniquement entre routeurs du même sous-système. Pour obtenir des informations sur les réseaux externes, ceux de l'autre système autonome, ils doivent dialoguer avec les routeurs externes R1 et R2.

Ceux-ci sont des points d'entrée de chaque système et, via la liaison qui les relie, ils échangent des informations sur la connectivité grâce à *EGP* (*Exterior Gateway Protocol*) ou *BGP* (*Border Gateway Protocol*) qui remplace EGP actuellement.

ANNEXE D : Services de la couche transport

- **Les services de la couches transport du modèle OSI**

Les services qu'offrent la couche transport en mode connecté sont rendues par les primitives données ci-dessous. Celles-ci se décomposent comme dans tout dialogue entre couches en quatre catégories comme illustré dans la figure

- phase d'établissement de la connexion
  - T_CONNECT.request(adresse source, adresse distante, données_exprès, qos, données_utilisateur) pour demander une connexion
  - T_CONNECT.indication(adresse source, adresse distante, données_exprès, qos, données_utilisateur) pour indiquer une connexion de transport
  - T_CONNECT.response(adresse source, adresse distante, données_exprès, données_utilisateur) pour répondre à une demande de connexion de transport
  - T_CONNECT.confirm(adresse source, adresse distante, données_exprès, qos, données_utilisateur) pour confirmer l'établissement d'une connexion de transport
- phase de transfert de données
  - T_DATA.request(données_utilisateur) pour demander le transfert de données
  - T_DATA.indication(données_utilisateur) pour indiquer un transfert de données
  - T_EXPEDITED_DATA.request(données_utilisateur) pour demander le transfert de données exprès
  - T_EXPEDITED_DATA.indication(données_utilisateur) pour indiquer un transfert de données exprès
- phase de libération de la connexion
  - T_DISCONNECT.request(données utilisateur) pour demander une déconnexion de transport
  - T_DISCONNECT.indication(raison, données_utilisateur) pour indiquer une déconnexion de transport

'une machine réalisant le service de transport ne peut se trouver que dans l'un des quatre états représentés à savoir

- *veille* : aucune connexion n'est établie, une demande de connexion peut être émise ou reçue

ANNEXE D : Services de la couche transport

- *connexion sortante en attente* : la machine a demandé une connexion et la réponse de l'autre extrémité n'est pas encore arrivée
- *connexion entrante en attente* : la machine a reçu une demande de connexion qu'elle n'a pas encore acceptée ou rejetée.
- *transfert de données prêt* : une connexion a été établie, les transferts de données peuvent commencer

Pour ce qui est du mode non connecté seules les primitives suivantes sont disponibles.

- T_UNIDATA.request(appelé, appelant, qos, données utilisateur)
- T_UNIDATA.indication(appelé, appelant, qos, données utilisateur)

ANNEXE E:SMTP

- **Le protocoles SMTP (Simple Mail Transport Protocol):**

Ce protocole fournit un mécanisme de transport et d'échange de courrier électronique entre utilisateurs d'Internet.

SMTP utilise le port 25 et le protocole TCP pour établor une connexion fiable ; il se sert des adresses définies dans Internet de type ' ***nom@blida.dz*** 'où le deuxième partie représente le nom du domaine qui gère le serveur de messagerie.

Le système utilise le mécanisme de « **store and forward** »,c'està dire ,que les messages entrants et sortants sont tamponnés afin de permettre aux utilisateurs d'avoir d'autres activités pendant le transfert de leur messagerie.

La syntaxe utilisés dans la messagerie Internet est très simple .le message comprend un en-tête qui donne quelques éléments de base comme ;l'objet du message ,l'émetteur ,le récepteur et la date, et un corps qui contient le texte même du message .Le tout en ASCII.

Le fonctionnement du protocole SMTP :

1. Au départ ,le client établit une connexion vers le serveur et attend que le serveur lui envoie un message 220 (prêt pour l'échange de message ?)

2. Le client reçoit le message ;il répond par le commande **helo** .Le serveur répond en donnant son identité et le client envoi la commande **mail-from** pour s'identifier

3. Le serveur répond par un message 250(OK) .Le client envoie la commande **rept-to** en indiquant l'adresse DNS de la destination

4. Si l'adresse du récepteur n'existe pas au niveau du serveur ,il répond par un message 550 (utilisateur inconnu) sinon ,il répond par un message 250 (OK)

5. Le client envoie la commande **data** accompagnée du texte et attend l'acquittement positif du serveur .Enfin ,le client envoie la commande **quit** et attend le message 221 (terminer la session) du serveur .Les deux extrémités libèrent la connexion TCP.

Une des caractéristiques des SMTP est d'effectuer une remise différée du courrier ,c'est à dire que l'utilisateur recevra son courrier même si sa station de travail est en panne ou surchargée . Le secret de ce mécanisme est le suivant :

- Un courrier expédié par un utilisateur est d'abord copié dans une mémoire de **spool** avec le nom de l'expéditeur,et du récepteur de la machine destinataire et l'heure de dépôt .Puis le système active le processus de transfert qui devient client ;

- Le nom de la machine est associé à une adresse IP et établit une connexion TCP avec le serveur SMTP.Si l'étape de la connexion est réussie,le processus envoie une copie du message au récepteur qui le sauvegarde dans une mémoire de **spool** spécifique .

ANNEXE E:SMTP

- Lorsque le client et le serveur se sont confirmé l'envoi et la réception du message ,le client supprime la copie locale .

Dans le cas contraire ,si par exemple la connexion TCP est rompue, il enregistre l'heure de cette tentative et réactive le processus jusqu'à l'expiration d'un délai important où il recevra un message d'abandon .Ce mode de fonctionnement avec TCP assure le bon acheminement des messages.

CONFIGURATION PIX

```
/CONFIGURATION D'UN SITE CENTRAL
PIX Version 5.1(5)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security10
enable password <ProjetSecurité2003/SiteCentral> encrypted
passwd < ProjetSecurité2003/SiteCentral> encrypted
hostname SitCentral-PIX
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
names
access-list 101 permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255.0
pager lines 24
logging on
no logging timestamp
no logging standby
no logging console
no logging monitor
no logging buffered
no logging trap
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 192.168.1.52 255.255.255.0
ip address inside 10.1.1.1 255.255.255.0
no failover
arp timeout 14400
nat (inside) 0 access-list 101
route outside 0.0.0.0 0.0.0.0 192.168.1.1 1
timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00 udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
AAA-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset1  esp-des esp-sha-hmac
crypto ipsec transform-set  myset2  esp-3des esp-md5-hmac
crypto map map1 10 match address 101
crypto map map1 10  set peer 172.22.112.12
crypto map map1 10 set transform-set myset1 myset2
crypto map map1 interface outside

crypto map map2 20 match address 101
crypto map map2 20  set peer 172.22.112.12
crypto map map2 20 set transform-set myset1 myset2
```

```
isakmp enable outside
isakmp policy 10 authentication rsasig
crypto map map2 interface outside
ca generate rsa key 512
ca save all
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 1000
isakmp policy 20 authentication pre-share
isakmp key ********** address 172.22.112.12 netmask 255.255.255.255
isakmp policy 20 encryption des
isakmp policy 20 hash md5
isakmp policy 20 group 1
isakmp policy 20 lifetime 1000
telnet timeout 5
terminal width 80
Cryptochecksum:<ProjetSecurité2003/SiteCentral >
Write memory
: end
[OK]
```

```
/----CONFIGURATION D'UNE AGENCE----/
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password <ProjetSecurité2003/AGENCE>
passwd <ProjetSecurité2003> encrypted
hostname Agence1-PIX
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
names
access-list 101 permit ip 172.16.1.0 255.255.255.0 10.1.1.0 255.255.255.0
pager lines 24
logging on
no logging timestamp
no logging standby
no logging console
no logging monitor
no logging buffered
no logging trap
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
mtu outside 1500
mtu inside 1500
mtu intf2 1500
ip address outside 172.22.112.12 255.255.0.0
ip address inside 172.16.1.1 255.255.255.0
```

```
no failover
arp timeout 14400
nat (inside) 0 access-list 101
ip address inf2 127.0.0.1 255.255.255.255
route outside 0.0.0.0 0.0.0.0 172.22.112.1 1
timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00 udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat

crypto ipsec transform-set myset2Ag esp-3des esp-md5-hmac
crypto map map1Ag 10 match address 101
crypto map map1Ag 10  set peer 192.168.1.52
crypto map map1Ag 10 set transform-set myset2Ag
crypto map map1Ag interface outside

isakmp enable outside
isakmp policy 10 authentication rsasig
ca generate rsa key 512
ca save all
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 1000


telnet timeout 5
terminal width 80
Cryptochecksum:<ProjetSecurité2003/Agence>

: end
[OK]
```

GLOSSAIRE

GLOSSAIRE

AH :Authentification Header – entête d'authentification inclus dans IPsec

.

ARP : Address Resolution Protocol : Protocole permettant la résolution MAC.

Broadcast Un émetteur envoie un datagramme en diffusion générale

BSD : Berkeley Software Distribution : Licence pour le logiciel libre.

CA :Certificate Authority – Autorité de certification utilisée dans le cadre des certificats digitaux X.509

CBC : Cipher Block Chaining Mode: Mode de cryptage utilisé pour les fichiers.

CHAP : Challenge Handshake Protocol – Protocole d'authentification

CIFS : Common Internet File Sytem : Extension du protocole SMB

.

CIR Commited Information Rate -

CRL : Certificate Revocation List : Liste en ligne, à jour, de certificats qui ont été émis précédemment et ne sont plus valide.

DES : Data Encryption Standard – Algorithme de cryptage

D-H : Diffie-Hellman: Inventé en 1976 par Whitfield Diffie et Martin Hellman c'est le plus ancien crypto-sytème à clé publique.

DMZ : Demilitarized Zone – Zone spéciale d'un firewall réservée aux accès extérieurs vers une partie prédéfinie du réseau

DN : Domain Name : Nom de domaine déposé auprès d'un organisme (registrar).

DNS : Domain Name Service : Service internet faisant correspondre une adresse et un nom.

DSA : Digital Signature Algorithm: Algorithme de signature à clé publique.

ESP : Encapsulating Security Payload: Méthode d'encapsulation des packets pour le protocole IPsec.

FSF : Free Software Foundation: Association pour le logiciel libre présider par Richard Stallman.

FTP : File Transfer Protocol Protocole permettant la transmission de fichiers.

GID : Group Identifier: Numéro d'identification pour un groupe.

GNU : Gnu is Not Unix : Projet à l'origine des outils insérés dans Linux.

GPL : General Public Licence : License pour le logicie l libre.

HMAC : Hashed Message Authentification Code: Norme d'interconnexion

.

HTML :HyperText Markup Language Langage servant à générer des pages web.

HTTP :HyperText Transfer Protocol : protocole permettant la consultation de pages au format HTML.

IDEA : International Data Encryption Standard : Protocole de cryptage par blocs de 64bits et utilisant des clés de 128bits.

IETF : Internet Engineering Task Force – organisme de standardisation de l'Internet

IKE :Internet Key Exchange – méthode sécurisée d'échange de clés

IPsec ,IP secure: Protocole de sécurisation d'échange de données IP

IPv4: Internet Protocol version 4 – Protocole de niveau 3, version 4

IPv6 :Internet Protocol version 6 – Protocole de niveau 3, version 6 (dernière version)

ISAKMP : Internet Security Association & Key Management Protocol – Protocole d'échange de clé utilisé dans le cadre d'IKE

ISP: Internet Service Provider – Fournisseur d'accès à Internet

L2F: Layer 2 Forwarding – Protocole de tunneling de niveau 2 développé par CISCO

L2TP: Layer 2 Tunneling Protocol – Protocole de tunneling de niveau 2 en cours de standardisation à l'IETF

LAC L2TP : Access Concentrator – Concentrateur d'accès L2TP

LDAP : Lightweight Directory Access Protocol: Protocole de gestion d'annuaire.

LNS L2TP Network Server – Serveur réseau L2TP

MAC : Message Authentification Code: Norme d'interconnexion.

MD5 : Message Digest 5 : Fonction de hachage à sens unique de 128bits.

MPLS : Multi Protocol Label Switching – Protocole d 'optimisation des flux IP
Multicast Un émetteur envoie un datagramme à un groupe de destinataires prédéfini

NAT : Network Address Translation : Méthode de translation d'adresse IP.

NFS : Network FileSystem :Protocole de partage de fichiers pour les systèmes Unix.

NIS : Network Information Service: Permet le partage d'informations via des fichiers pour les systèmes Unix.

Oakeley : Fournit un échange de clé de session de Diffie Hellman hybride destiné à être utilisé dans un : cadre ISA/KMP.

OSI : Open Systems Interconnexion: Modèle réseau de réference en 7 couches.

PAM : Pluggable Authentication Modules: Modules d'authentification.

PAP :Password Authentification Protocol – Protocole d'authentification
Passante

PKI : Public Key Infrastructure: Organisme gérant les certificates.

PPP :Point to Point Protocol – Protocole de niveau 2 souvent utilisé sur les lignes

PPTP :Point to Point Tunneling Protocol – Protocole de tunneling

QoS :Quality of Service – Qualité de service

RADIUS :Remote Authentification Dial-In Service – Service d'authentification

RAS :Remote Access Server – Serveur d'accès distant

RFC : Request For Comment: Document officiel de description des normes.

RPC : Remote Procedure Call: Appel de procédure distante.

RPV: Réseau Privé Virtuel

RSA: Rivest Shamir Adleman : Algorithme de cryptage à clef publique .

RSVP :Resource Reservation Protocol – Protocole d'optimisation de la bande

SA : Security Association : Association de sécurité.

SAD : Security Association Database: Base de données gérant les associations de sécurité.

SHA : Secure Hash Algorithm : Algorithme de hachage.

SMTP : Simple Mail Transport Protocol: Protocole pour le transport des mails.

SPD : Security Policy Database: Base de données gérant les politiques de sécurité.

SPI : Security Parameter Index: Index pour les associations de sécurité (SA).

SSH : Secure Shell :Protocole perme ttant l'administration à distance des serveurs de manière sécurisée.

SSL : Secure Socket Layer : Méthode de sécurisation des communications.

TACACS: Terminal Access Controller Access Control – Protocole d'authentification

TCP : Transfert Control Protocol : Protocole de transport de la suite TCP/IP.

TLS : Transport Layer Security: Evolution de SSL.

UID : User Identifier: Numéro d'identification pour un utilisateur.

Unicast :Un émetteur envoie un datagramme à un destinataire unique

VPN :Virtual Private Network – voir RPV

BIBIOLGRAPHIE / WABOGRAPHIE

Bibliographie / Webographie

[KAR96] Karanjit Siyan &Chris Hare « Internet securité &firwalls « LE MACMILLAN 1996

[STU02] Stuart McClure & Joel Scambray & George Kurtz « Halte aux hackers » EOM 2002

[TAN98] Andrew Tanenbaum "Réseau 3éme edition"
DUNOD

[VIV97] THOMAS VIVET 1997 http://www.chez.com/vivett/public_html/crypto/"

[SCH97] :BRUCE SCHNEIER « Cryptographie appliquée « THOMSON PUBLISHING France, PARIS 1997

[BAY02] Frédéric Bayart 2002 http://www.bibmath.net/crypto/moderne/des.php3

[PUJ00] Gay Pujolle « les réseaux informatiques » EYROLLES 2000.

[ITL03] www.itel.ch/technologie/securité

[CTF 02] : http://www.tahi.org/report/USAGI/rh72-200203262000-cvs/ipsec4-udp– site contenant des informations sur les algorithmes Ipsec

[IPF 02] : http://coombs.anu.edu.au/ipfilter/ (visité au 20/05/2002) – site officiel d'IPFilter

[TDP 02] : http://www.tcpdump.org/ (visité au 20/03/2002) – site officiel de TCPdump

[WSN 01] : http://michel.arboi.free.fr/cryptFAQ/snakeoil.html (visité au 20/05/2002) – site de
cryptographie

[TLN 02] : http://www.faqs.org/rfcs/rfc854.html (visité au 4/05/2002) – site officiel de l'IETF, telnet

[RSA 02] : www.rsasecurity.com (visité au 05/01/2002) - site officiel de RSA

[CRY 02] : http://cryptosec.lautre.net/ (visité au 20/05/2002) – site sur la cryptographie et les
algorithmes associés

[HMC 02] : http://andrew2.andrew.cmu.edu/rfc/rfc2104.html (visité au 20/12/2001) - site contenant des
RFCs, HMAC

[PKI 02] : http://www.ietf.org/rfc/rfc2527.txt (visité au 20/05/2002) – site officiel de l'IETF, PKI

[BGP 02] : http://www.ietf.org/rfc/rfc1771.txt (visité au 10/05/2002) – site officiel de l'IETF, BGP

[MAT 99] : Neil Matthew, Richard Stones, « programmation Linux », Eyrolles 1999

[ETH 02] : http://www.uni-trier.de/infos/ether/descript-guide.html (visité au 10/02/2002) – site décrivant
Ethernet

[APF 02] : http://www.monkey.org/~dugsong/dsniff/ (visité au 20/05/2002) – site de Dsniff, arpsoof

[STE 00] : Stephen Northcutt, Judy Novak & Donald Mc Lachlan, « Détection des intrusions réseaux »,
CampusPress, Juin 2000

[SID01] "Authentification" :Philipe SIDLER – Ingénier ENSIMAG
http://psidler.multimania.com/authentification/

[CIS03] www.cisco.com /site officiel de cisco

[FLO96] G. FLORIN, "Les Technique de cryptographie", CNAM 96,
http://tulipe.cnam.fr.

[VAN97] www.tele.ucl.ac.be Alexandre Vanlangendonck -- Patrice Roulive 1997

[CAT96] "Sécurité Internet pour l'entreprise" ;
Par feu et au-delà Terry Berstein, Anish B.Bhimani, Eugene Shultz et Carole A. Seigel. Traduction de Catherine Reclus.

[GUI01] Guillaume Des George www.guill.net 2001.

[EST03] Armand PASSELAC-ESTRADA http://194.51.152.252/vpn/vpn.html

[GFD03] http://frlinux.net/section=réseau&article

[JOS03] http://benoit -joseph.mine.nu/tfe/node16.html

[SCH03] http://www. HCR.fr/resource/article/IPSec

[SCH03] http://www. HCR.fr/resource/article/crypto

[FRE03] http://www.decaseservices.com/docs/securite/vpn/freeswan.htm

[MUL03] http://linuxfocus.org/francais/may2003/article292.shtml

[AND03] www.kdevelop.org/doc/tutorial_setting/index_fr.html

[ANN02] http://users.skynet.be/dedjickerp/jonathan/informatique/linux.htm

[BER99] www.mines.u.nancy.fr/~tisseren/cours/réseaux/osi.html

[ISO00] www.iso.ch

[MAN02] www.themanualpage.org

[PIL02] www.comentcamarche.net Jean François PILLOU

[PAS99] www.info.univ.angers.fr/pub/pn
"coursde réseaux et TCP/IP "

[COM92] DouglasCOMER "TCP/IP architecture, protocoles et application" Interdiction 92

[RFC91] IP Protocoles "RFC791"

[SNK02] www.coolmacintosh.com

[YAY02] memoire de fin d'étude soutenu en mai 2002 en vu d'obtention le titre "d'ingénierie informatique et réseau " à l'Ecole Superieur de Génie Informatique
THEME " Le model open source et la sécurité des infrastructure UNIX"

Conclusion générale

Le travail réalisé dans ce mémoire a tenté une approche alternative aux méthodes classiques de sécurité informatiques; et en particulier des réseaux locaux connectés à des réseaux longues distances.

L'objet principal est de mettre en place une solution de sécurité, qui sécurisera les transferts transitant via un réseau public, le choix de la solution s'est porté sur le protocole IPSec .

Le travail réalisé dans ce projet m'a permis :

- *D'acquérir des connaissances dans le domaine des réseaux (OSI / TCP/IP) et de leur sécurité.*
- *De comprendre et de maîtriser l'implémentation du protocole IPSec.*
- *D'acquérir des connaissances dans le domaine de la conception et l'implémentation d'applications sous environnement Linux.*

Après un aperçu des problèmes de la sécurité informatique et des mécanismes qui les résolvent, les détails sur les techniques d'authentification avancée utilisées actuellement notamment ceux qui se basent sur l'échange de clefs et les techniques de cryptage de données.

Différentes sortes d'implémentations d'IPSec ont été exposées, qu'elles soient matérielles ou logicielles, elles offrent toutes des avantages comme des inconvénients.

L'option matérielle (PIX) a été adoptée pour une implémentation générale, mais dans le cas où une implémentation logicielle s'impose, une interface graphique pour la configuration d'IPSec a été développées.

Un environnement windows a suffit pour l'implémentation IPSec sous un PIX, pour l'interface de configuration, celle ci a été réalisée sous environnement Linux .

Résumé

Les réseaux longues distances sont le symbole du millénaire, ils inquiètent et fascinent à la fois, ils concentrent les espoirs de modernité et les peurs d'un avenir encore incertain. Ils représentent la victoire informatique sur les distances et un défi contre le temps.

Etant donnés la croissance des systèmes informatiques, le nombre de plus en plus grand des réseaux interconnectés grâce au protocoles TCP\IP, le caractère de plus en plus sensible et confidentiel des données, le problème de la sécurité des données est aujourd'hui incontournable.

Pour dés réseaux longues distances, tels les réseaux bancaires, il est impératif de protéger le réseau local. Or ce n'est guère suffisant, surtout quand les données doivent être transférées, d'un réseau à un autre.

L'utilisation d'une solution permettant le transfert d'information d'un réseau local, vers un autre réseau local distant dans la plus grande confidentialité et intégrité devient une nécessité absolue.

IPSec est constitué par plusieurs protocoles. Ces protocole offrent une forte authentification de l'extrémités communicante et des données transmis , ainsi qu'il permet une confidentialité grâce au méthodes de cryptographie.

Le protocole IPSec est implementable sur des PIX selon une politique de sécurité adapté au besoin du réseau à sécurisé.

Le protocole IPSec peut aussi avoir une implémentation logicielle. FreeWan est un logiciel permettant l'implémentation IPSec, cet implementation se fait par manipulation des fichiers de configuration et un ensemble de commandes.

Une interface graphique pour un logiciel de sécurité peut être d'un très grand bénéfice tel que, la facilité à manipulé des concept nouveaux et difficiles à assimiler qui concerne la configuration d'IPSec, ainsi elle conduit l'utilisateur à commettre moins d'erreurs

Mots clefs: IPSec, PIX, TCO/IP ,Cryptographie, échange de clef, FreesWan, IKE.

Summary

The public wide area networks are symbols of progress of this millennium . They worry and fascinate at the same time. They focus on the hope of advance and the fear of an unsettled future. They represent the computer science's victory over long distances and a challenge against time.

Taking in consideration the development of the informatics systems, the great number of the interconnected networks -thanks to the protocols TCP\IP-, the character more and more sensitive and confidential of data; the problem of data's security is today unavoidable.

For the long distance network, such as banks networks, it is necessary to protect the local one. Otherwise it is hardly sufficient, especially when the data must be sent from a network to another.

The use of a solution which allow the sent of an information from a local network, toward another far network in the most high confidentiality and integrity becomes an absolute necessity.

IPSec is set up by many protocols. This protocols give a great authentication of peer communicants and of the transmitted data, thus they allow the confidentiality thanks to cryptography methods.

The IPSec protocol is implementable_on PIX according to a policy security which fits the need of the secured network.

The IPSec protocol may be also implementable on a software FreeWan, this implantation is made by the manipulation of configuration files and a set of commands.

A graphic interface for security software may be for a great advantage, such as the easiness to handle a new and difficult concept to assimilate which concerns the IPSec configuration; thus it can produce an advantage of a less configuration's mistakes.

Key words : IPSec, PIX, TCO/IP ,Cryptographie, échange de clef, FreesWan, IKE.