Université Abderrahmane MIRA-Bejaïa

Faculté des Sciences Exactes

Département Informatique

Mémoire

En vue de l'obtention du diplôme de Master

En Informatique

Option : Administration et Sécurité des Réseaux Informatique

Thème

Mise en œuvre des VPNs: LAN-to-LAN et END-to-LAN en IPSec et IPSec/L2TP

Cas d'étude: Groupe INERGA

Présenté par :

Alaedine BOUHAFS

Layachi FENOUCHE

Sous la direction de :

M^me^ ZIDANI.F

Co-encadreur :

MEDDAH Lounes

Soutenus devant les membres de jury :

Président de jury : Dr SIDER Abderrahmane.

Examinateur : M^r^ AISSANI Sofiane.

2011/2012

Dédicaces

A mon très cher grand père

A mes très chers parents

A ma très chère fiancée

A mon frère

A toute la famille

A tous mes amis

Alaedine

A mes très chers parents,

A mes frères

A mes sœurs et belles sœurs

A ma princesse Damia et sa mère Alia

A la fiancée de mon ami

A tous mes amis

Layachi

Remerciements

Au terme de ce modeste travail, nous remercions DIEU tous puissant qui nous a procuré : courage, volonté et patience pour mener à bien ce travail.

Ainsi, nous remercions vivement notre promotrice M^{me} Zidani de nous avoir encadré, soutenu, conseillé et dirigé, tout au long de cette aventure, nous tenons à lui témoigner notre profonde gratitude et notre reconnaissance pour son aide précieuse et ses encouragements.

Nos remerciements s'adressent aux membres de jury, d'avoir accepté de lire et d'évaluer ce travail.

Nos remerciements vont également aux personnels de l'entreprise INERGA.

Enfin, nous remercions tous ceux qui nous ont aidés de prés ou de loin pour la réalisation de ce travail.

Table des matières

Liste des abréviations

3DES: Triple DES
ACL: Access Control List
AES: Advanced Encryption Standard
AH: Authentication Header
AKD: Area Key Distributors
CA: Certification Authority
DEP: Dual Encryption Protocol
DES: Data Encryption Standard
DKD: Domain Key Distributor
ESP: Encapsulating Security Payload
FAI : Fournisseurs d'Accès à l'Internet
FCS: Frame Check Sequence
GDH: Group Diffie-Hellman
GRE: Generic Routing Encapsulation
GPOM: Group Policy Object Management
HDLC: Hight Data Level Control
HMAC: Hashed Message Authentication Code
IGKMP: Intra-domain Group Key Management Protocol
IKE: Internet Key Exchange
ISAKMP: Internet Security Association and Key Management Protocol
IPSec: IP security
KEK: Key Encryption Keys
LAC: L2TP Access Concentrator
LAN: Local Area Network
LCP: Link Control Protocol
LNS: L2TP Network Server
L2F: Layer Two Forwarding
L2TP: Layer Two Tunneling Protocol
MAN: Metropolitan Area Network
MD5: Message Digest
MMC: Microsoft Management Consol
MPLS: Multiprotocol Label Switching

MPPC: Microsoft Point to Point Compression

MPPE Microsoft Point to Point Encryption

NAS: Network Access Server

NCP: Network Control Protocol

OSI: Open System Interconnection

PAP: Password Authentification Protocol

PFS: Perfect Forward Secrecy

PKI: Public key Infrastructure

POP: point Of Presence

PPP: Point to Point Protocol

PPTP: Point to Point Tunneling Protocol

PVC: Private Virtual Circuit

RRSA: Routing and Remote Access Service (Microsoft)

RSA: Rivest-Shamir-Adelman

SA: Security Association

SAD: Security Association Database

SHA-1 Secure Hash Algorithm

SMQ : Système de Management de la Qualité

SMKD: Scalable Multicast Key Distribution

SPD: Security Policy Database

SSL: Secure Socker Layer

STS: Station To Station

SSH: Secure Shell

SVC: Switched Virtual Circuit

TCP/IP: Transmission Control Protocol/Internet Protocol

TEK: Trafic Encription Key

TLS: Transport Layer Security

TRP: Two Round Protocol

VPN: Virtual Private Network

WAN: Wide Area Network

WS2003: Windows Server 2003

Liste des figures

Liste des tableaux

Introduction générale

Indéniablement, Internet est entré dans nos meurs. A travers, ce réseau informatique, tout un monde parallèle s'est développé : des sites marchands ont fleuris, les services pour les particuliers sont apparus. En outre, nous arrivons à échanger des données à travers des programmes d'échange de fichiers. Nous retiendrons de tout ce la qu'Internet est un véritable outil de communication. Internet n'a pas su évoluer dans l'utilisation de ses protocoles, la plupart des protocoles utilisés ont plusieurs années d'existence et certains n'ont pas été crée dans une optique où le réseau prendrait une telle envergure. Les mots de passe traversent ainsi les réseaux en clair, et là où transitent des applications de plus en plus critiques sur le réseau, la sécurité a peu évolué.

Quand nous parlons de sécurité, c'est en faisant référence aux pirates, virus, vers, cheval de Troie, etc. Ils profitent des failles des protocoles, du système, mais surtout du faite que le réseau n'était pas développé dans une optique de « sécurité ».

Internet dans ce contexte, n'a pas la vocation d'être une zone sécurisée. La plupart des données y circulent sans sécurité. Les entreprises alors font recours à des algorithmes de cryptage, pour garder leurs données, utilisées couramment, confidentielles.

Virtual Private Network (VPN) ou Réseau Privé Virtuel (RPV) en français est une technique permettant à un ou plusieurs postes distants de communiquer de manière sûre, tout en empruntant les infrastructures publiques.

Ce type de liaison est apparu suite à un besoin croissant des entreprises de relier ses différents sites, et ce de façon simple et économique. L'avènement des VPN ont permis de démocratiser ce type de liaisons.

Dés lors, l'objet de notre travail, est de mettre en œuvre une solution VPN avec IPSec, qui permet une communication sécurisée dans des réseaux publics comme l'Internet.

Notre travail est structuré en quatre chapitres, dont le premier traite les concepts théoriques relatifs à l'architecture et la sécurité Internet, ainsi le deuxième chapitre est consacré à la présentation générale des réseaux Virtuels Privés(VPN), en abordant leur définition, leur fonctionnement et les protocoles les plus utilisés et en se basant sur le protocole IPSec, que nous avons utilisé dans notre cas pratique, quand au troisième chapitre, nous avons présenté

l'organisme d'accueil(INERGA), en outre, nous avons avancé notre problématique de travail et quelques conceptions concernant la mise en œuvre des VPN.

Finalement, le dernier chapitre est réservé au cas pratique, dont nous avons mis en place deux stratégies IPSec, à savoir : l'accès à distance en utilisant IPSec/L2TP qui permet à certains utilisateurs d'accéder à distance au sein de l'entreprise et l'implémentation d'une solution VPN site à site entre les différentes bases stratégiques du groupe INERGA.

Chapitre1:Architecture et Sécurité Internet

Introduction

Aujourd'hui, l'utilisation de la technologie pour développer et renforcer notre réseau humain arrive à un tournant. La généralisation de l'utilisation d'Internet à l'échelle mondiale s'est opérée plus vite que quiconque aurait pu l'imaginer. L'évolution rapide de ce réseau mondial induit un bouleversement des interactions sociales, commerciales, politiques et même personnelles. L'étape suivante de notre développement verra les novateurs se servir d'Internet comme d'un tremplin pour créer de nouveaux produits et services spécialement conçus pour exploiter les capacités des réseaux.

Ce chapitre va présenter l'architecture d'Internet en générale et donne quelques notions de base de la sécurité informatique.

I. Architecture Internet

I.1.Internet : Historique et Evolution

Dans les années 1950-60, les données sont gérées sur de grands systèmes ou ordinateurs centraux, accessibles à partir des postes déportés qui sont à l'origine des terminaux ; simple écrans et claviers, ils disposent de matériels de communication leur permettant d'échanger des caractères avec le système central. Le partage d'informations et les services sont à l'origine des réseaux que nous connaissons aujourd'hui.

A la fin des années 60, on a aboutit à la constatation que les ressources sont globalement mal utilisées. Officieusement un climat de guerre froide a conduit le département de la défense américaine au développement de protocoles et de matériels en vue de disposer d'un réseau à forte tolérance de pannes. C'est ainsi que le réseau ARPANET (Advanced Research Project Agency NETwort) voit le jour en 1970. Avec lui l'utilisation des lignes téléphoniques existantes constitue un premier point d'appui.

ARPANET subit une croissance très rapide. En 1972 on compte une quarantaine d'institutions reliées entre elles et disposant des services de courrier électronique et de connexion à distance.

Au milieu des années1970, ARPANET adopte un nouveau mode de communication le TCP/IP (Transport Control Protocol /Internet Protocol), ce modèle ne décrit pas les protocoles des couches basses, les organisations peuvent développer leurs réseaux physiques en interne

selon leurs besoins et leurs contraintes, elles disposent d'une passerelle qui se charge du transfert des paquets vers Internet.

Le succès d'Internet se confirme dans les années 1980. De nombreuses organisations publiques et privées, d'abord américaines puis de toutes origines, s'y sont raccordées , des applications désormais indispensables à la vie quotidienne sont développées, comme la messagerie électronique en 1972, ou le World Wide Web en 1989, le réseau initialement réservé aux données informatiques , se révèle en 90 concurrent du réseau téléphonique , grâce à des protocoles permettant de transporter des échantillons de voix dans les paquets IP et sert aujourd'hui de réseau de transport pour la télévision et la radio . (Quidelleur, 2010)

I.2. Point sur Le model TCP/IP

Dans les années 1970, le département de la Défense américain, ou DOD (Department Of Defense), décide, devant le foisonnement de machines utilisant des protocoles de communication différents et incompatibles, de définir sa propre architecture. Cette architecture, dite TCP/IP, est à la source du réseau Internet. Elle est aussi adoptée par de nombreux réseaux privés, appelés intranet.

Les deux principaux protocoles définis dans cette architecture sont les suivants :

• IP (Internet Protocol), de niveau réseau, qui assure un service sans connexion.

• TCP (Transmission Control Protocol), de niveau transport, qui fournit un service fiable avec connexion. (Pujolle, 2008)

TCP/IP définit une architecture en couches, chaque couche destinée à accomplir des fonctionnalités. En effet, de nombreux sous-réseaux distincts peuvent être pris en compte dans l'architecture TCP/IP, de type aussi bien local qu'étendu. Cette architecture et les différentes fonctionnalités de chaque couche sont illustrées à la figure ci-dessous.

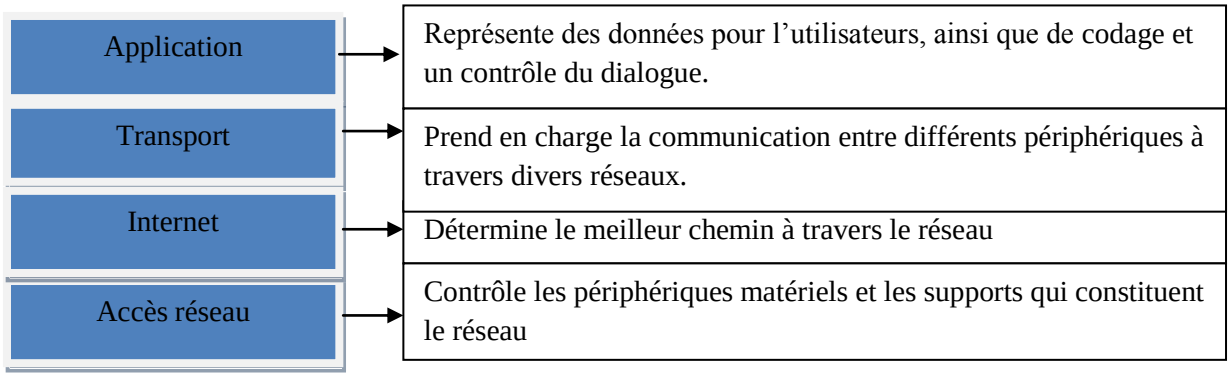


Figure 1 model TCP/IP

I.3. Structure Internet

Internet : est un ensemble de réseaux privés et publics interconnectés disposant d'une structure en couches hiérarchisées pour les services d'adressage, de désignation et de connectivité. À chaque niveau, ou couche, de la hiérarchie, des opérateurs réseau individuels maintiennent les relations d'homologues entre opérateurs du même niveau. En Conséquence, le trafic réseau destiné à des services locaux ou régionaux n'a pas besoin de transiter par un point central pour être distribué. Les services communs peuvent être dupliqués dans différentes régions, ce qui écarte le trafic des réseaux fédérateurs de niveau supérieur.

Bien qu'Internet ne soit pas régulé par une organisation unique, les opérateurs des nombreux réseaux individuels qui assurent la connectivité d'Internet collaborent et respectent des normes et protocoles établis. (Quidelleur, 2010)

Comme le montre la figure ci-dessous le réseau Internet est formé de plusieurs fournisseurs d'accès de différents niveaux :

- **FAI (Fournisseur d'Accès à Internet) niveau 1** : Au cœur de d'Internet, les FAI de niveau 1 assurent les connexions nationales et internationales. Ils sont constitués de liaisons terrestres, sous-marines, satellitaires. Les backbones des FAI sont reliés entre eux par des NAP (Network Access Point) eux même interconnectés par des liaisons dont le débit atteint 40 Gbits/s. Ces différents FAI se traitent d'égale à égale.
- **FAI niveau 2 :** Les FAI de niveau 2 sont moins importants et fournissent souvent des services régionaux. Les FAI de niveau 2 rémunnèrent généralement les FAI de niveau 1 pour être connectés au reste d'internet.
- **FAI niveau 3(local) :** Les FAI de niveau 3 sont les fournisseur de services locaux en contact direct avec les utilisateurs finaux. Les FAI de niveau 3 sont généralement connectés à des FAI de niveau 2 qu'ils rémunèrent pour avoir accés à Internet.

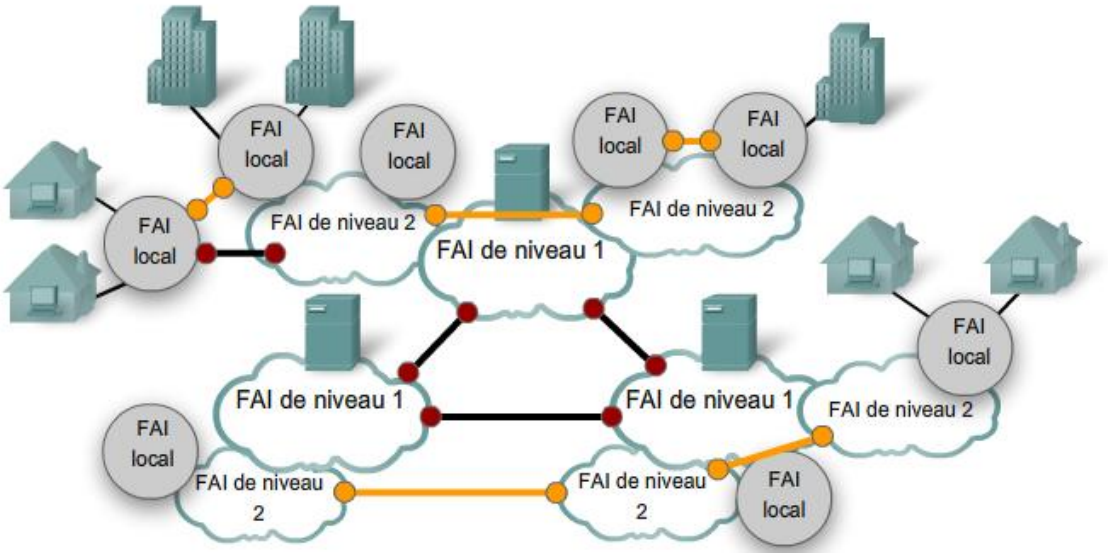


Figure 2 Architecture Internet

Les connexions peer-to-peer dites d'homologues entre réseaux de même niveau fournissent des connexions directes qui évitent les routes les plus longues et permettent de ne pas congestionner le réseau fédérateur. (CCNA, 2007-2008)

I.4. Exemple d'architecture d'un FAI Niveau 2

Télécom Algérie est notre fournisseur d'accès à Internet son réseau multiservice repose sur un Backbone IP/MPLS complètement maillé, déployé dans les quatre (04) grandes villes (Alger, Oran, Constantine, Ouargla) du pays et couvre tout le territoire national.

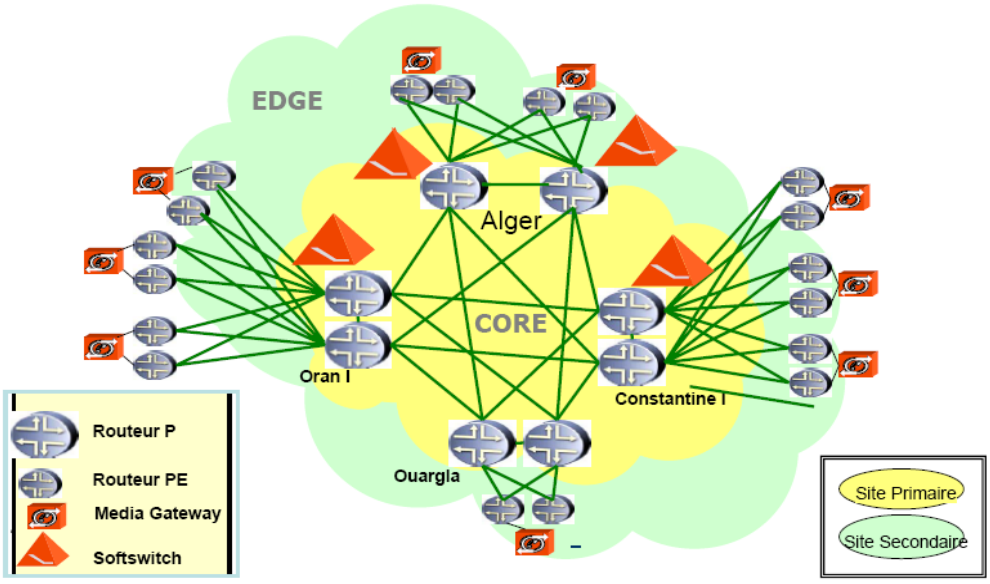


Figure 3 Architecteur du Backbone IP/MPLS de Télécom Algérie

Comme le montre cette figure le réseau de Télécom Algérie est constitué de :

- **Router P** (routeur core) : d'une puissance de commutation de 320Gp/s optimisée pour les services basés sur MPLS et prêt à supporter les interfaces de 10Gbps.
- **Router PE** (Provider Edge): Possède une très large gamme d'interface qu'il supporte allant des interfaces sériels de 64kbps jusqu'au niveau SDH de STM-16.
- **Media Gataway** : Fonctionne principalement comme médiateur entre les réseaux traditionnels TDM et les nouveaux réseaux multiservices basés sur IP.
- **Softswitch** : est un Media Gateway Controller de nouvelle génération. (LOUNIS, 2006)

I.5. Quelques services offerts par Internet

Les ressources disponibles sur Internet peuvent nous aider à :

- Déterminer le trajet le moins embouteillé en visualisant les vidéos du trafic routier et des conditions météo transmises par les webcams ;
- Consulter notre compte bancaire et payer nos factures en ligne; (commerce électronique)
- Recevoir et envoyer des courriels ou passer un appel téléphonique via Internet depuis un cybercafé lors de notre pause déjeuner ;
- Rechercher des informations médicales et obtenir des conseils nutritionnels d'experts du monde entier, puis publier un message sur un forum pour partager des renseignements sur une maladie ou un traitement ;
- Publier nos photographies, vidéos personnelles et expériences et les partager avec nos amis ou avec le monde entier.

I.6. Gouvernance d'Internet

Bien qu'Internet ne soit pas régulé par une organisation unique plusieurs organismes au niveau international coopèrent entre eux pour le développement de l'Internet est on peut citer : (Quidelleur, 2010).

- **ISOC (Internet SOCiety)** : créée en 1992 est un organisme international à but non lucratif qui supervise le développement de l'Internet en veillant à ce qu'il reste un modèle ouvert. Elle exerce autorité morale et technique sur les autres organisations gérant Internet comme ICANN.

❖ **ICANN (Internet Corporation for Assigned Names and Numbres)** : créée en 1998 est une association à but non lucratif de droits californien qui gère la distribution des adresses IP, des noms de domaines de haut niveau (.com , .org , .fr,…) ,des numéros identifiants les protocoles de l'Internet .

❖ **IAB (Internet Architecture Board):** est un comité chargé du suivi de l'évolution des protocoles du modèle TCP/IP. Il supervise IRTF et IETF .Parmi ces membres CISCO, Microsoft,… .

❖ **IRSG (Internet Research Steenig Group) :** supervise la création et l'orientation des groupes de travaux.

❖ **IRTF (Internet Research Task Force):** comité technique qui prévoit l'évolution des protocoles, des architectures et des technologies d'Internet sur long terme, et prépare les future travaux, l'IETF il est placé sous la direction IRSG.

❖ **IRSG (Internet Research Steering group) :** est le comité de validation technique de l'IRTF.

❖ **IETF (Internet Enginerring Task Force) :** comité technique supervisé par IFSG qui établit les spécifications et réalise la première implantation des nouveaux protocoles du modèle TCP/IP .Il produit les normes de l'Internet appelées RFC (Request For Comments) .

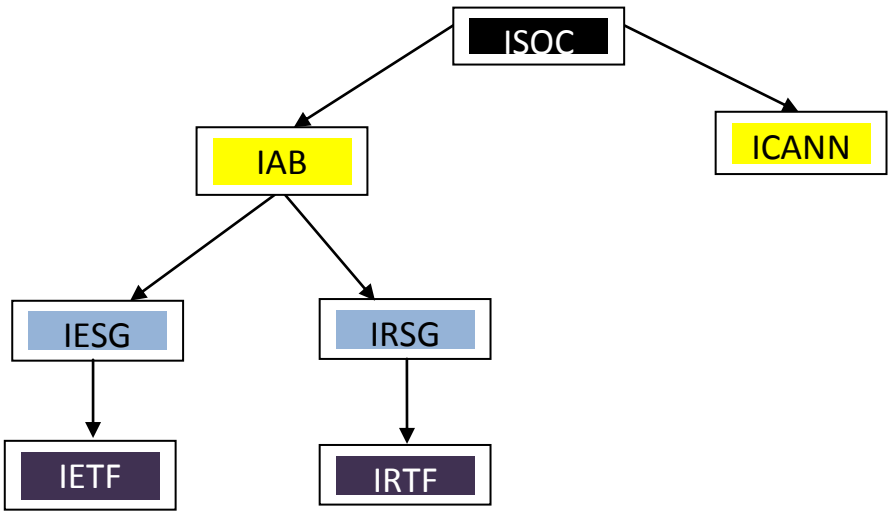


Figure 4 Les gouvernances de l'Internet.

I.7. Options connexion à Internet

Les utilisateurs nécessitent une connexion à un fournisseur de services Internet pour accéder à Internet. Ces fournisseurs proposent plusieurs options de connexion. Les particuliers et les petites entreprises ont principalement recours aux choix suivants :

- **Accès par ligne téléphonique** : Option peu onéreuse nécessitant une ligne de téléphone et un modem. Pour se connecter au FAI, un utilisateur appelle son numéro de téléphone d'accès. Cette connexion est la plus lente. Elle est généralement utilisée par les travailleurs mobiles dans des zones géographiques où une connexion à plus grande vitesse n'existe pas.
- **DSL (Digital Subscriber line)** : est une technologie de connexion permanente qui utilise les lignes téléphoniques à paires torsadées existantes pour transporter des données à haut débit et fournir des services IP aux abonnés. Un modem DSL convertit un signal Ethernet provenant d'un périphérique d'utilisateur en signal DSL, qui est transmis au central téléphonique.
- **Sans fil à large bande**

La technologie sans fil utilise le spectre des radiofréquences pour envoyer et recevoir des données. Le spectre est accessible à toutes les personnes disposant d'un routeur sans fil et d'un appareil équipé de la technologie sans fil. (WiFi municipal,WiMax, Internet par satellite)

- **Modem câble**

Option offerte par les fournisseurs de services de télévision câblée. Le signal Internet se situe sur le même câble coaxial qui fournit la télévision câblée. Un modem câble spécial distingue le signal Internet des autres signaux se situant sur le câble et fournit une connexion Ethernet à un ordinateur hôte ou à un réseau local.

La figure ci-dessous montre ces différentes options de connexions au fournisseur d'accès à Internet

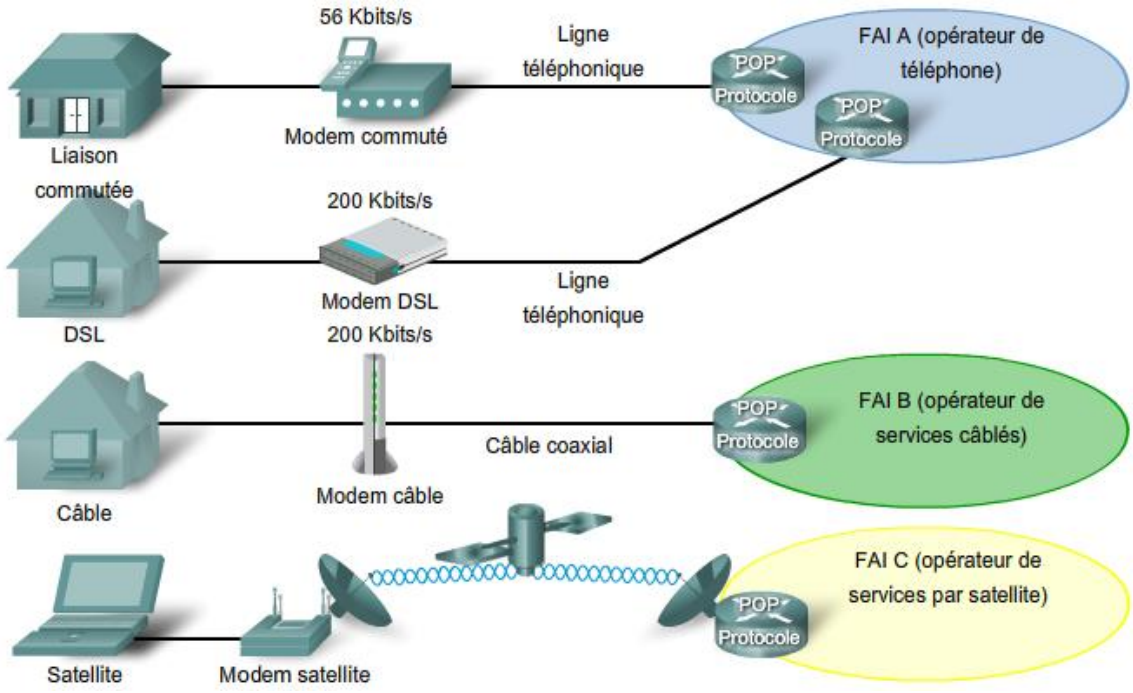


Figure 5 types de connexions (CCNA, 2007-2008)

I.8. Réseau étendu d'entreprise

I.8.1. Définition et caractéristiques

Un réseau étendu est un réseau de communication de données qui fonctionne au-delà de la portée géographique d'un réseau local.

Les principales caractéristiques des réseaux étendus sont les suivantes :

- ❖ Ils connectent généralement des périphériques séparés par une zone géographique plus étendue que ne peut couvrir un réseau local ;
- ❖ Ils utilisent les services d'opérateurs, tels que des compagnies de téléphone ou de câble, des systèmes satellite et des fournisseurs de réseau ;
- ❖ Ils utilisent divers types de connexions série pour permettre l'accès à la bande passante sur de vastes zones géographiques.

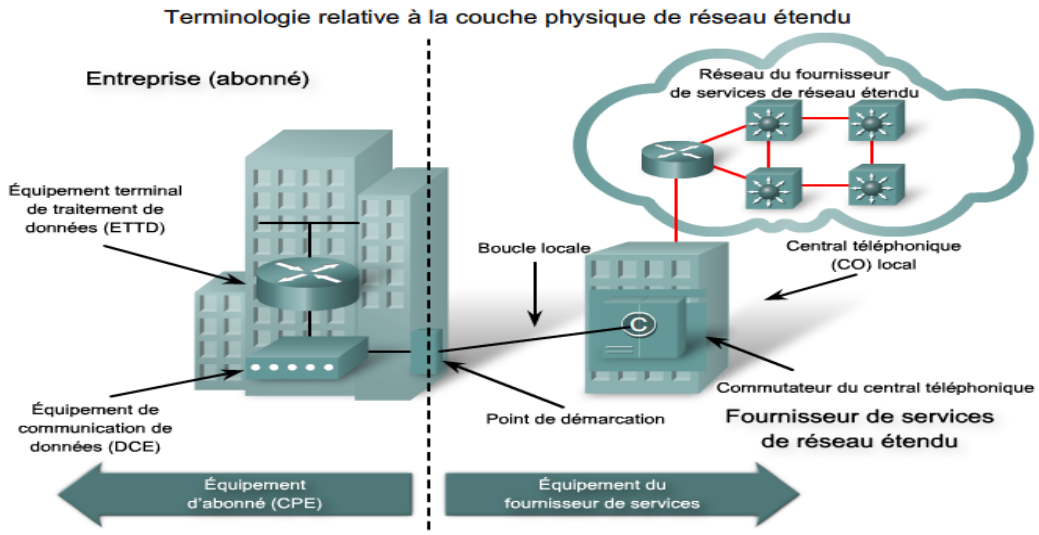


Figure 6 Terminologie de réseau étendu. (CCNA, 2007-2008)

Les réseaux étendus requièrent des protocoles de couche liaison de données pour établir la liaison sur la ligne de communication entre le périphérique d'envoi et de réception.ces protocoles(Les protocoles de la couche liaison de données) définissent la manière dont les données sont encapsulées en vue d'être transmises vers des sites distants, ainsi que les mécanismes de transfert des trames obtenues. Différentes technologies sont utilisées, notamment RNIS, le relais de trames, ou le mode de transfert asynchrone ATM.

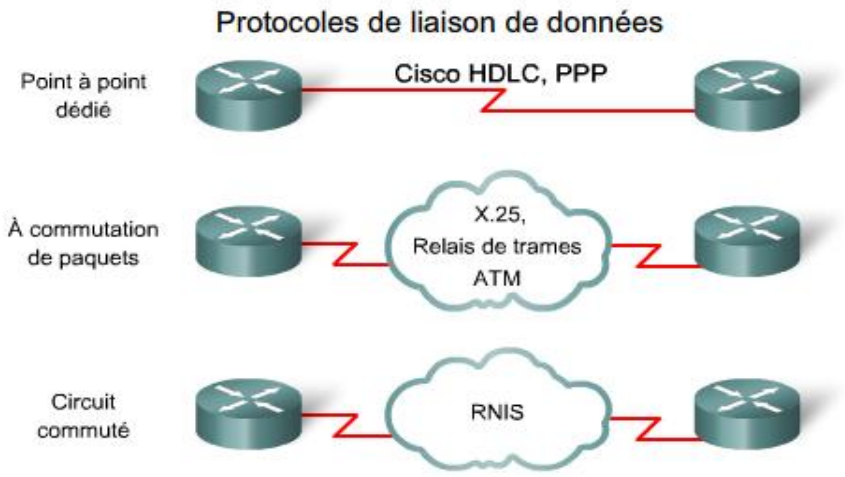


Figure 7 Protocole de liaison de données. (CCNA, 2007-2008)

I.8.2. Option de connexion de réseau étendu

De nombreuses options d'implémentation de solutions de réseau étendu sont actuellement disponibles. Elles diffèrent au niveau de la technologie, de la vitesse et du coût nous avons :

- **Lignes louées**

Lorsque des connexions dédiées permanentes sont requises, une liaison point à point est utilisée pour fournir un chemin de communication de réseau étendu préétabli entre les locaux du client et une destination distante par l'intermédiaire du réseau du fournisseur d'accès. Les lignes point à point sont généralement louées à un opérateur et prennent le nom de lignes louées.

- **Liaisons de communication à commutation de circuits**

La commutation de circuits établit de façon dynamique une connexion virtuelle dédiée pour la voix ou les données entre un expéditeur et un récepteur. Avant que la communication ne soit établie, il est nécessaire d'établir la connexion via le réseau du fournisseur de services. Les connexions commutées analogiques (RTPC) et les lignes RNIS sont des exemples de liaisons de communication à commutation de circuits.

- **Liaison de communication à commutation de paquets**

De nombreux utilisateurs de réseau étendu n'utilisent pas de façon optimale la bande passante fixe à leur disposition avec des circuits dédiés, commutés ou permanents, car le flux de données fluctue. Les fournisseurs d'accès disposent de réseaux de données permettant de desservir ces utilisateurs de façon plus appropriée. Dans ces réseaux à commutation de paquets, les données sont transmises dans des trames, des cellules ou des paquets libellés. Le relais de trames, ATM, X.25 et Metro Ethernet sont des exemples de liaisons de communication à commutation de paquets.

II. SECURITE

II.1. Présentation de la sécurité du réseau

La sécurité se place actuellement au premier plan de la mise en œuvre et de l'administration réseau. La difficulté que représente la sécurité dans son ensemble est de trouver un compromis entre deux besoins essentiels : le besoin d'ouvrir des réseaux pour profiter des nouvelles opportunités commerciales et le besoin de protéger des informations privées ou publiques et des informations commerciales stratégiques.

L'application d'une stratégie de sécurité efficace est l'étape la plus importante qu'une entreprise doit franchir pour protéger son réseau. Cette stratégie définit les directives concernant les activités et les ressources nécessaires à la sécurisation d'un réseau d'entreprise.

II.2. Pourquoi la sécurité des réseaux

Les réseaux informatiques ont grandi en taille et en importance en très peu de temps. Lorsque la sécurité d'un réseau est compromise, de très graves conséquences peuvent en résulter, comme l'atteinte à la vie privée, le vol d'informations et même l'engagement de la responsabilité civile. Pour rendre cette situation encore plus difficile, les types de menaces potentielles sont en évolution constante.

Comme les applications Internet et le commerce électronique suivent la même croissance, la recherche de l'équilibre entre un réseau ouvert et un réseau fermé est une tâche cruciale.

De plus, la montée du commerce mobile et des réseaux sans fil demande des solutions de sécurité intégrées plus transparentes et plus flexibles.

II.3. Objectif de sécurité

La sécurité informatique en général vise à atteindre les objectifs suivants :

- **Confidentialité des données** :

Ensemble des mécanismes permettant qu'une communication de données reste privée entre un émetteur et un destinataire. le chiffrement des données est une solution fiable pour assurer la confidentialité des données.

Quelques algorithmes de chiffrement : la famille asymétrique : RSA, ELGmail, Deffie-Hellman, … etc. la famille symétrique : DES, 3DES, AES,…etc.

- **Intégrité des données** :

Les destinataires n'ont aucun contrôle sur le parcours emprunté par les données. C'est pourquoi ils ne savent pas si elles ont été consultées ou manipulées lors de leur passage sur Internet. L'éventuelle modification des données ne peut pas être exclue. L'intégrité des données garantit qu'aucune altération ou modification n'a été apportée aux données lors de leur parcours entre la source et la destination. En règle générale, on utilise les fonctions de hachage comme SHA-1(Secure Hash Algorithme), MD5 (Message Digest) pour garantir l'intégrité des données. Un hachage ressemble à une somme de contrôle ou à un sceau garantissant que personne n'a lu le contenu, tout en étant plus robuste.

- **Authentification** :

L'authentification garantit qu'un message provient d'une source authentique et accède à une destination authentique. Une identification assure à l'utilisateur que la personne avec qui il établit une communication est effectivement le destinataire escompté. on utilise des mots de passe, des certificats numériques, Signature numérique (RSA+SHA1, RSA+MD5,.. .), des cartes à puce et la biométrique pour vérifier l'identité des parties à l'autre extrémité du réseau.

- **Non-répudiation :**

Mécanisme permettant de garantir qu'un message a bien été envoyé par un émetteur et reçu par un destinataire.

Assuré par la signature numérique(RSA+SHA1, RSA+MD5,…) et les certificats.

- **Disponibilité.**

Ensemble des mécanismes garantissant que les ressources de l'entreprise sont accessibles, que ces dernières concernent l'architecture réseau, la bande passante, le plan de sauvegarde, etc.

- **Traçabilité.**

Ensemble des mécanismes permettant de retrouver les opérations réalisées sur les ressources de 'entreprise. Cela suppose que tout événement applicatif soit archivé pour investigation ultérieure. (C é d r i c L l o r e n s, 2006)

II.4. Menaces de sécurité courantes

- **Menace**

Les menaces viennent d'individus compétents intéressés par l'exploitation des faiblesses de sécurité. Il est prévisible que de tels individus continueront à rechercher de nouvelles faiblesses et de nouveaux exploits. Ces menaces sont mises en œuvre à l'aide d'une variété

d'outils, de scripts et de programmes permettant de lancer des attaques contre des réseaux et leurs périphériques.

- **Vulnérabilités**

La vulnérabilité est une faiblesse la plus cachée touchant une infrastructure informatique (erreur de configuration d'un équipement réseau, mot de passe vide,.. .) (Tableau n°1). On parle aussi de faille de sécurité.

Les technologies informatiques et de réseau ont des faiblesses de sécurité intrinsèques. Celles-ci comprennent les faiblesses du protocole TCP/IP, du système d'exploitation et de l'équipement réseau. Il existe des risques de sécurité pour le réseau si les utilisateurs ne respectent pas la stratégie de sécurité.

Faiblesse
Equipment réseau mal configuré
Comptes utilisateurs non sécurisés
Paramètres par défaut non sécurisée dans les Produits logiciels
Vulnérabilité de protocole TCP/IP
Vulnérabilité des systèmes d'exploitation
Vulnérabilité des équipements réseau

Tableau 1 Quelques vulnérabilités (CCNA, 2007-2008)

II.5. Types d'attaques

- **Reconnaissances**

La reconnaissance est la découverte non autorisée des systèmes, de leurs adresses et de leurs services, ou encore la découverte de leurs vulnérabilités. Il s'agit d'une collecte d'informations qui, dans la plupart des cas, précède un autre type d'attaque. La reconnaissance est similaire au repérage effectué par un cambrioleur à la recherche d'habitations vulnérables, comme des maisons inoccupées, des portes faciles à ouvrir ou des fenêtres ouvertes.

➢ **Accès non autorisé**

L'accès au système est la possibilité pour un intrus d'accéder à un périphérique pour lequel il ne dispose pas d'un compte ou d'un mot de passe. La pénétration dans un système implique généralement l'utilisation d'un moyen de piratage, d'un script ou d'un outil exploitant une vulnérabilité connue de ce système ou de l'application attaquée.

➢ **Déni de services**

Le déni de service (DoS Denial of Service, en anglais) apparaît lorsqu'un pirate désactive ou altère un réseau, des systèmes ou des services dans le but de refuser le service prévu aux utilisateurs normaux. Les attaques par déni de service mettent le système en panne ou le ralentissent au point de le rendre inutilisable. Le déni de service peut consister simplement à supprimer ou altérer des informations. Dans la plupart des cas, l'attaque se résume à exécuter un programme pirate ou un script. C'est pour cette raison que les attaques par déni de service sont les plus redoutées.

➢ **Malwares**

On appelle malware un programme ou une partie de programme destiné à perturber, altérer ou détruire tout ou partie des éléments logiciels indispensables au bon fonctionnement d'un système informatique. (Jean-Philippe, 2009)

On peut citer quelque type de Malwares :

- **Virus**

Est un petit programme informatique situé dans le corps d'un autre, qui, lorsqu'on le lance, se charge en mémoire et exécute les instructions que son auteur a programmées.

Le champ d'application des virus va de la simple balle de ping-pong qui traverse l'écran au virus destructeur de données, ce dernier étant la forme de virus la plus dangereuse.

- **Vers réseau**

Un ver est un programme informatique qui peut se produire et se déplacer à travers un réseau en utilisant ses mécanismes, sans avoir réellement besoin d'un support physique ou logique (disque dur, fichier,…) pour se propager ; un ver est virus réseau. La plus célèbre anecdote à propos des vers date de 1988. Un étudiant Robert T. MORRIS de Cornell Université avait fabriqué un programme capable de se propager sur un réseau.

- **Chevaux de Troie**

On appelle cheval de Troie (trojan horse) un programme informatique ouvrant une porte dérobé (backdoor) dans un système pour y faire entrer le hacker ou d'autre programmes indésirables.

Un cheval de Troie peut par exemple voler des mots de passes, copier des données sensibles, exécuter toute autre action nuisible. Une infection par un cheval de Troie fait généralement suite à l'ouverture d'un fichier contaminé contenant le cheval de Troie. Il y a quelques indications de présence de cheval de Troie comme réaction curieuse de la souris, activité anormale du modem ou de la carte réseau (données sont échangées en absence d'activité de l'utilisateur …

- **Bombes logiques**

Une bombe logique est un programme dont le déclenchement s'effectue à un moment déterminé en exploitant la date de système, le lancement d'une commande, ou n'importe quel appel au système, Ainsi ce type de virus est capable de s'activer à un moment précis sur un grand nombre de machine, par exemple le jour de saint valentin …

- **Un spyware** (espiogiciel)

Est un programme chargé de recueillir des informations sur l'utilisateur de l'ordinateur dans lequel est installé (comme les adresses web URL , mots-clés saisis dans les moteurs de recherche , …) afin de les envoyer à la société qui le diffuse pour lui permettre de dresser le profil des internautes. Les spywares s'installent généralement en même temps que d'autre logiciel.

II.6. Techniques générales d'atténuation des risques

Logiciel antivirus

Installation d'un logiciel antivirus sur les hôtes pour les protéger contre les virus connus. Les logiciels antivirus peuvent détecter la plupart des virus et des chevaux de Troie et les empêcher de se propager dans le réseau.

Le logiciel antivirus peut procéder de deux manières différentes :

- Il analyse les codes de source des fichiers, en cherchant les signatures des virus connus. Les virus détectés sont signalés selon la méthode définie par l'utilisateur.
- Il surveille les processus suspects sur un hôte susceptible d'être infecté. Cette surveillance comprend la saisie de données, la surveillance des ports et d'autres méthodes.

Pare-feu personnel

Les ordinateurs personnels connectés au réseau Internet par une ligne téléphonique, un câble DSL ou un modem câble sont aussi vulnérables que les ordinateurs d'entreprise. Le pare-feu personnel réside sur l'ordinateur de l'utilisateur et tente d'empêcher les attaques. Les pare-feu personnels ne sont pas conçus pour une mise en œuvre dans un réseau local, comme les pare-feu hébergés par un périphérique ou un serveur. De plus, ils peuvent empêcher l'accès au réseau s'ils sont installés en même temps que d'autres clients, services, protocoles ou adaptateurs réseau.

Correctifs du système d'exploitation

La meilleure façon de limiter les risques liés aux vers et à leurs variantes consiste à télécharger les mises à jour de sécurité du fournisseur du système d'exploitation et d'appliquer les correctifs aux systèmes vulnérables.

Détection des intrusions et méthodes de prévention

Les systèmes de détection des intrusions (IDS) détectent les attaques contre un réseau et envoient des données de journalisation à une console de gestion. Les systèmes de protection contre les intrusions (IPS) empêchent les attaques contre le réseau et doivent être dotés des mécanismes de défense suivants en plus de la détection :

- Un mécanisme de prévention pour empêcher l'exécution de l'attaque détectée.
- Un mécanisme de réaction pour immuniser le système contre les attaques ultérieures provenant d'une source malveillante.

Les VPN (Virtual Private Network):

La technologie des réseaux privés virtuels permet aux entreprises de créer des réseaux privés sur l'infrastructure publique d'Internet on utilisant des liaisons logiques tout en garantissant la confidentialité et la sécurité.

Grâce aux réseaux privés virtuels, les entreprises bénéficient d'une meilleure souplesse et d'une productivité accrue. Les sites distants et les télétravailleurs peuvent se connecter de manière sécurisée au réseau d'entreprise, quel que soit leur emplacement. Les données circulant sur un réseau privé virtuel sont chiffrées, elles ne sont déchiffrables que par les personnes y étant habilitées. Les réseaux privés virtuels englobent les hôtes distants dans le pare-feu, leur donnant des niveaux d'accès aux périphériques réseau quasiment identiques, comme s'ils se trouvaient à la direction générale de l'entreprise.

Les VLAN (Virtual Local Area Network):

Un VLAN permet à un administrateur réseau de créer des groupes de périphériques en réseau logique qui se comportent comme s'ils se trouvaient sur un réseau indépendant, même s'ils partagent une infrastructure commune avec d'autres réseaux locaux virtuels.

La technologie VLAN offre de nombreux avantages aux administrateurs réseau. Les VLAN permettent notamment de contrôler les multicast de couche 3 ; ils améliorent la sécurité du réseau et facilitent le regroupement logique des utilisateurs du réseau.

II.7. Stratégie de sécurité de l'entreprise

II.7.1. Politique de sécurité

Compte tenu de la nouvelle importance accordée à la sécurité et à la manière stratégique et globale de l'appréhender, une politique de sécurité devient l'expression de la stratégie sécuritaire des organisations, elle constitue un outil indispensable non seulement à la gouvernance de la sécurité mais aussi à la réalisation du plan stratégique de sécurité.

Une politique de sécurité exprime la volonté managériale de protéger les valeurs informationnelles et les ressources technologiques de l'organisation. Elle spécifie les moyens (ressources, procédures, outils,…) qui répondent de façon complète et cohérente aux objectifs stratégiques de sécurité.

II.7.2. Norme de sécurité

La norme ISO 17799 : basée sur la norme BS 7799 élaborée par l'association de normalisation Britannique 1995.

Basées sur la gestion de risque, la norme propose un code de pratique pour la gestion de la sécurité identifie des exigences de sécurité sans toute fois spécifier la manière de les réaliser. Son intérêt réside dans le fait que la norme abord des aspects organisationnels, humains, juridiques et technologiques de la sécurité en rapport aux différentes étapes de conception, mise en œuvre et maintien de la sécurité. Elle traite dix domaines de sécurité (Tableau n°2), de 36 objectifs, 127 points de contrôle, une nouvelle version cette norme (ISO/IEC) 17799 a été éditée. (Ghernaouti-Hélie, 2003)

1. Politique de sécurité	6. Exploitation et gestion de système et de réseaux
2. Organisation de la sécurité	7. Contrôle d'accès
3. Classification et contrôle des actifs	8. Développement et maintenance des systèmes
4. Sécurité et gestion des ressources humaines	9. Continuité de service
5. Sécurité physique et environnementale	10. Conformité

Tableau 2 : Dix domaines sécurité

Conclusion

Les réseaux de données prennent en charge la façon dont nous vivons, apprenons, travaillons et nous divertissons. Ils constituent la plateforme des services qui nous permettent de nous connecter, à l'échelon local aussi bien que mondial, à nos familles, nos amis, notre travail et nos centres d'intérêt. Cette plateforme qui véhicule tous les types de communications (données, audio et vidéo) sur une même infrastructure, permettent de réduire les coûts et offrent aux utilisateurs des services et contenus aux nombreuses fonctionnalités. Cependant, la conception et la gestion des réseaux convergents ce qui nécessite de solides connaissances et compétences en matière de réseaux pour que tous les services puissent être fournis aux utilisateurs voulus. Et il est indispensable d'intégrer les mesures de sécurité aux réseaux de données afin d'empêcher que nos communications privées, personnelles et professionnelles ne soient interceptées, volées ou endommagées.

Dans les prochains chapitres, nous allons utiliser cette plate-forme pour un but professionnel, économique au profit d'une entreprise publique (INERGA), tout en garantissant la sécurité des échanges de données en utilisant un moyen très répondu actuellement qui sont les VPNs.

Chapitre2 : Définition, concept et Fonctionnement des VPN

Introduction

Les données transmises sur Internet sont beaucoup plus vulnérables que lorsqu'elles circulent sur un réseau interne à une organisation, car le chemin emprunté n'est pas défini à l'avance, car les données empruntent une infrastructure réseau publique appartenant à différents opérateurs. Ainsi il n'est pas impossible que sur le chemin parcouru, le réseau soit écouté par un utilisateur indiscret ou même détourné. Il n'est donc pas concevable de transmettre dans de telles conditions des informations sensibles pour l'organisation ou l'entreprise.

Dans ces conditions, l'internet fournit des solutions d'interconnections avec une disponibilité de couverture mondiale, la solution VPN est idéale pour pouvoir exploiter au mieux les capacités de ce réseau, et de relier des sites distants à l'échelle de la planète.

Ce chapitre présente la notion de VPN, les différentes typologies utilisables (site à site, poste à site, poste à poste) avec leurs buts et leurs avantages, ainsi qu'un bref panorama des protocoles VPN les plus usités.

1. Définition

Avant de définir la technologie de VPN il faut comprendre certains concepts :

1.1 Un réseau

Il s'agit donc d'un support pour des échanges électronique de données

1.2 Réseau privé

Un réseau privé est un réseau qui utilise les plages d'adressage IP définies par la RFC 1918 « *Address Allocation for Private Internets* ». Ces adresses ne sont pas routées sur Internet. Un réseau privé peut être numéroté librement avec les plages d'adresses privées prévues à cet effet. Par opposition aux adresses publiques d'Internet, ces adresses ne sont pas uniques, plusieurs réseaux pouvant utiliser les mêmes adresses. (Rafael CORVALAN, 2003)

1.3 Réseau privé virtuel (VPN)

n VPN est un tunnel sécurisé permettant la communication entre deux entités y compris au travers de réseaux peu sûrs comme peut l'être le réseau Internet.

Les VPN ont pour objectif de contribuer à la sécurisation des échanges de données privées, sensible, sur les réseaux publics. (ARCHIER, 2010)

La figure suivante représente l'architecture générale d'un VPN

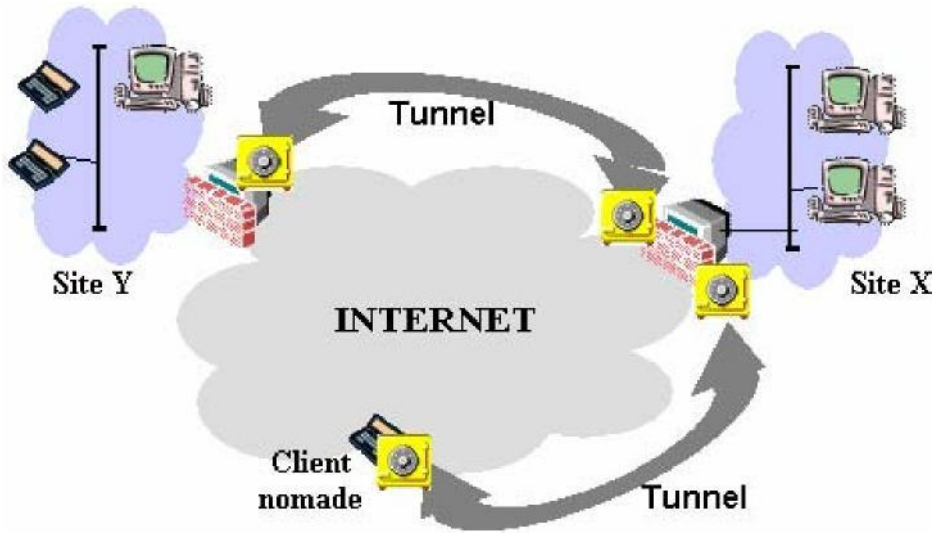


Figure 8 Architecture VPN

2. Principe de fonctionnement

La technologie des VPN repose sur la possibilité d'émettre de données privées sur un réseau public, et de les acheminer jusqu'au destinataire en assurant leur sécurité. À l'origine, Internet n'est pas prévu pour ce genre d'utilisation et des mécanismes supplémentaires doivent être mis en œuvre pour permettre le déploiement de cette technologie. (Rafael CORVALAN, 2003)
Parmi les fonctionnalités principales de VPN, nous trouvons :

2.1 Tunnelage

Les informations échangées entre deux entités internes sont rarement routables sur internet, soit parce que les entreprises utilisent un protocole autre qu'IP (IPX, Apple Talk…), soit parce qu'elles utilisent des adresses IP valides seulement en environnement interne (Ce sont les plages d'adresse IP RFC 1918 créées pour prévenir la pénurie d'adresse IP sur Internet). Les réseaux privés virtuels utilisent le tonnelage pour encapsuler un paquet non routable dans un paquet routable pour l'acheminer vers sa destination, en le protégeant grâce aux mécanismes de chiffrement et de signature.

2.2 Authentification

Des millions de serveurs et autres ordinateurs sont connectés en permanence à Internet et peuvent potentiellement se connecter à nos ressources. Il est donc indispensable, lors de l'implémentation d'un VPN, d'assurer de l'identité du ou des sites se connectant à des ressources via un réseau privé virtuel.

2.3 Contrôle d'accès

Tous les membres d'un VPN n'ont pas nécessairement les mêmes besoins en termes d'accès aux ressources du système d'information. Des mécanismes de contrôle d'accès devront être mis en place pour gérer ces différences.

2.4 Chiffrement et Signature

Le principal atout des VPN réside dans l'utilisation d'une infrastructure publique. La confidentialité et l'intégrité des données ne sont pas assurées par une telle infrastructure car elle est mutualisée.
Les VPN utilisent des mécanismes de chiffrement et de signature électronique pour assurer que seul le destinataire puisse utiliser les données échangées (confidentialité) et que ces données ne puissent être modifiées en transite (intégrité).

3. Typologie des VPN

Selon l'entité disposant de la maîtrise du ou des VPN, nous pouvons distinguer deux grandes catégories de VPN : le VPN d'entreprise et le VPN d'opérateur. Chacune d'entre elles présente ses avantages et inconvénients et elles ne sont pas exclusives l'une de l'autre puisqu'il n'est pas rare de trouver les deux présentes simultanément au sein d'une même entreprise. (ARCHIER, 2010)

3.1 VPN d'entreprise

Dans ce cas l'entreprise garde le contrôle de l'établissement des VPN entre ses différents points de présence ainsi qu'entre ses postes situés à l'extérieur de l'entreprise et les sites principaux.

a. VPN Site à site

But

C'est un des cas les plus fréquents. Il s'agit de relier deux sites d'une même entreprise ou bien le site d'une entreprise et celui d'un fournisseur, d'un prestataire ou d'un client. Mais il faut également que tout ou partie des machines des deux réseaux puissent communiquer avec celles du réseau distant en utilisant les adresses privées de chaque réseau.

Matériels mis en œuvre

Généralement ce type de VPN est mis en place par l'interconnexion de deux éléments matériels (routeurs ou pare-feu) situés à la frontière entre le réseau interne et le réseau public de chaque site. Ce sont ces matériels qui prennent en charge le cryptage, l'authentification et
le routage des paquets. Lorsque ce sont des matériels spécifiques, et non pas seulement des firewalls logiciels implantés sur un PC banal, des processeurs spécialisés peuvent prendre en charge la partie cryptographique la plus consommatrice de ressources CPU.

b. VPN poste à site

But

C'est également une utilisation très fréquente des VPN qui permet à des utilisateurs distants (nomades, travailleurs à domicile, commerciaux...) d'accéder aux ressources de l'entreprise via un VPN.

Outils mis en œuvre

Pour construire cette solution, il nous faut sur le site central un matériel (firewall, routeur, concentrateur SSL) constituant le point de terminaison de tous les VPN côté central. Du côté des postes de travail distants, il faut un logiciel gérant le type de protocole choisi et compatible avec le matériel du site central. Dans certains cas ce logiciel est déjà présent dans le système d'exploitation de ces postes. Dans d'autres cas il est nécessaire d'installer ce composant logiciel.

c. VPN poste à poste

But

Dans ce dernier cas, l'objectif est d'établir un canal sécurisé de bout en bout entre deux postes ou, plus couramment, entre un poste et un serveur. Le poste et le serveur peuvent être situés sur le même réseau ou sur deux réseaux distants reliés eux-mêmes par un VPN site à site.

Outils mis en œuvre

Ici nous ne faisons intervenir que des composants logiciels : un logiciel client sur le poste "demandeur" et un logiciel utilisé en serveur sur le poste "destinataire".

3.2 VPN Opérateur

Lorsqu'il s'agit d'interconnecter plusieurs sites d'une même entreprise avec des engagements de performances et de disponibilité il est plus judicieux, mais évidemment plus coûteux, de faire appel à un opérateur qui va donc mettre en place un réseau privatif entre tous les sites.

a. Caractéristiques du VPN opérateur site à site

Chaque site est relié au POP (Point Of Presence) le plus proche avec le médium souhaité (ADSL, SDSL, Fibre Optique...) et un routeur complètement contrôlé par l'opérateur. Ensuite l'opérateur établit des tunnels ou des circuits privatifs entre les différents sites au moyen des différents liens interconnectant ses POP. La technologie pour ce faire varie en fonction des avancées technologiques et c'est ainsi que nous sommes passés des réseaux en Frame-Relay aux réseaux MPLS qui sont maintenant les plus courants dans ce cadre là.

Selon le désir du client et les possibilités techniques ou budgétaires, ce réseau privatif peut être bâti avec différentes topologies :

- Tous les sites secondaires convergent vers le site central et c'est celui-ci qui fait le relais : technologie en hub (ou en étoile).
- Tous les sites peuvent communiquer directement entre eux : full mesh ou maillage complet.
- Les sites les plus importants peuvent communiquer entre eux et les secondaires passent obligatoirement par un des sites principaux.

L'opérateur supervise la totalité du réseau et peut affecter des classes de service selon le type de trafic, ce qui permet de rendre prioritaires certains flux.

b. En option : VPN Nomade à réseau

En complément des VPN site à site mis en place par son opérateur, l'entreprise souhaite souvent permettre à ses collaborateurs de se connecter au réseau interne depuis l'extérieur. Dans ce cas le nomade utilise une connexion banalisée généralement en ADSL ou 3G pour appeler une passerelle de l'opérateur. Ensuite, après une authentification plus ou moins forte, il se voit doté d'une adresse IP interne et autorisé à se connecter aux réseaux de l'entreprise.

4. Avantages des VPN

Les réseaux privés virtuels procurent les avantages ci-dessous :

- ❖ Le coût des VPN est plus faible.
- ❖ Le temps de mise en œuvre des VPN est plus rapide.
- ❖ La disponibilité des connexions (la configuration de réseau est entièrement maillée).
- ❖ Plus flexible en cas d'évolution et de nouvelles implantations.
- ❖ La sécurité est assurée par des technologies de chiffrement très solides, et pas de dépendance à la sécurité du FAI.
- ❖ Rapidité des accès nomades grâce à l'utilisation des technologies émergentes telles que l'ADSL. (Rafael CORVALAN, 2003)

5. Protocoles utilisés dans les VPN

Les VPN s'appuient, comme la plupart des technologies réseaux, sur des protocoles. Plusieurs protocoles sont utilisés dans les technologies de VPN. Certains d'entre eux visent uniquement à établir un tunnel, d'autres y ajoutent la composante sécurité.

Les différents protocoles utilisés sont :

5.1 Protocoles de niveau 2

5.1.1. GRE (Generic Routing Encapsulation)

GRE est un protocole générique d'encapsulation de paquet défini originellement en 1994 par la RFC 1701, puis mis à jour en 2000 par la RFC 2784. GRE est un protocole développé par Cisco. Le protocole intègre la notion d'encapsulation de protocole. Il permet ainsi de supporter plusieurs types de protocoles pour les transporter sur de l'IP.

GRE à l'avantage de pouvoir interconnecter des réseaux IP ou non à travers un réseau IP comme internet,

La figure suivante illustre comment effectuer l'encapsulation par GRE

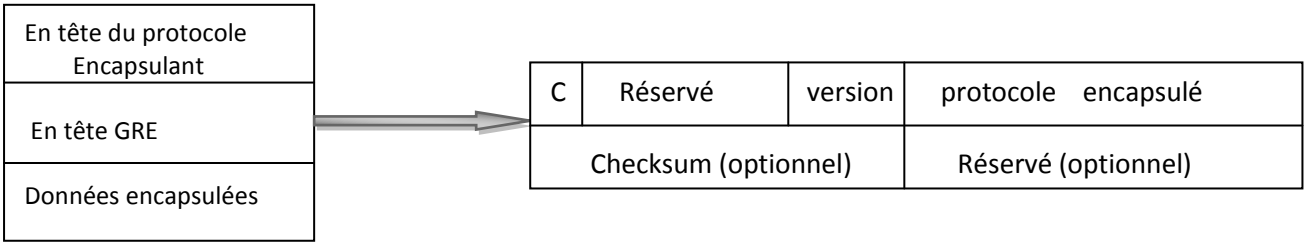


Figure 9 GRE pour encapsuler des données

Comme on peut le constater, GRE n'est rien d'autre qu'une colle entre un protocole encapsulant et un protocole encapsulé. (Rafael CORVALAN, 2003)

5.1.2. PPP (Point to Point Protocol)

PPP est un protocole de liaison (couche 2 du modèle OSI) standard, définit par la RFC 1661. Il permet l'échange de paquet entre deux acteurs et il est souvent utilisé pour échanger des données entre deux ordinateurs reliés par une ligne sérielle ou téléphonique.

Une connexion PPP est composée principalement de trois parties :

- Une méthode pour encapsuler les datagrammes sur la liaison série. PPP utilise le format de trame HDLC (Hight Data Level Control) de l'ISO (International Standardisation Organisation).
- Un protocole de contrôle de liaison (LCP - Link Control Protocol) pour établir, configurer et tester la connexion de liaison de données.
- Plusieurs protocoles de contrôle de réseaux (NCP - Network Control Protocol) pour établir et configurer les différents protocoles de couche réseau. Certains des protocoles NCP les plus courants sont : TCP/IP (Transmission Control Protocol/Internet Protocol), le protocole de contrôle Appletalk (Appletalk Control Protocol), le protocole de contrôle Novell IPx (Novell IPx Control Protocol), le protocole de contrôle Cisco Systems (Cisco Systems Control Protocol), le protocole de contrôle SNA (SNA Control Protocol) et le protocole de contrôle de compression (Compression Control Protocol). (GUERMAH, 2010)

Le format de la trame PPP est :

Fanion 01111110	Adresse 11111111	Contrôle 00000011	Protocole 16 bits	Données	FCS 16 bits	Fanion 01111110

Figure 10 La trame de PPP

5.1.3. PPTP (Point to Point Tunneling Protocol)

L'idée originelle du protocole est de permettre l'encapsulation de datagrammes non TCP/IP, comme Apple Talk et IPX pour être téléportés à travers un réseau IP. Ce protocole est présent dans beaucoup de matériels et de systèmes d'exploitation. Même s'il tombe maintenant en déshérence, concurrencé par le succès d'IPSec et du SSL, il est quand même intéressant de l'aborder car il est encore présent dans beaucoup de cas et il est parfois la base de certains autres protocoles de tunnel, dont notamment L2TP et, dans une moindre mesure, d'IPSec.

Ce protocole était normalement destiné à permettre la connexion d'utilisateurs distants au site central d'une entreprise. Son usage s'est élargi à la connexion Site à Site car nous le trouvons

également dans beaucoup de routeurs ou de pare-feu. Il a été créé à l'origine par Microsoft, Ascend et 3Com. Il n'a jamais été un standard reconnu par l'IETF mais son atout majeur a été sa présence sur tous les postes Windows depuis sa naissance. Il est néanmoins décrit depuis 1999 dans la RFC2637 mais il s'est enrichi depuis de nombreuses options, notamment en termes d'authentification. La figure suivante montre comment établir une connexion avec le protocole PPTP. (Rafael CORVALAN, 2003)

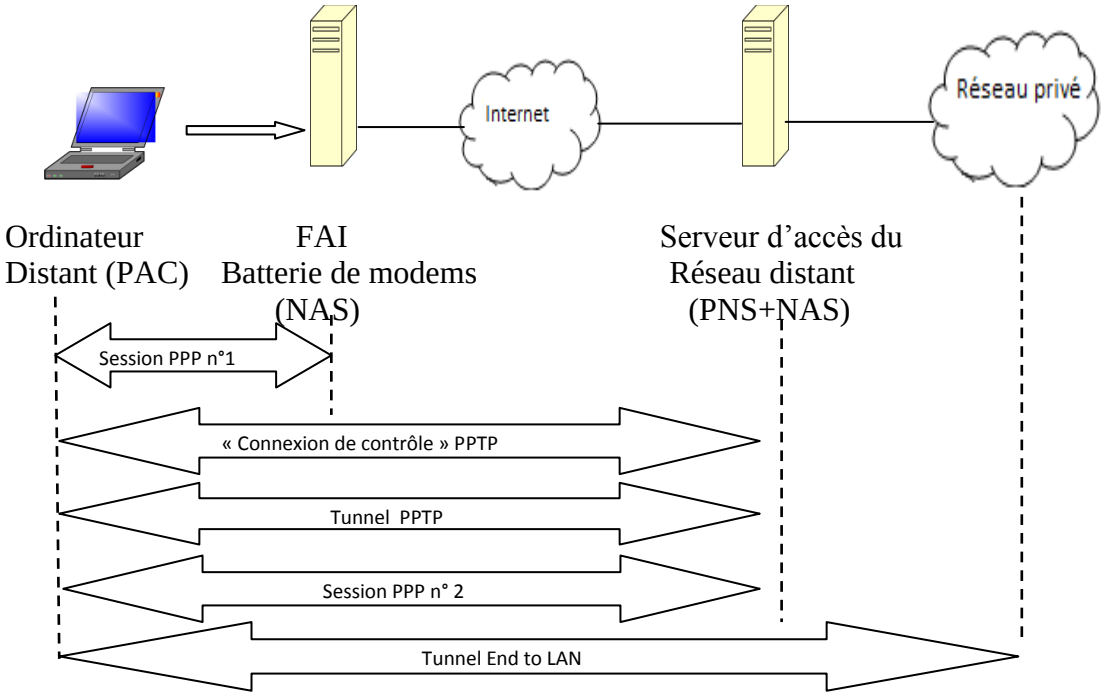


Figure 11 Déroulement d'une session avec PPTP

5.1.4. L2F (Layer Two Forwarding)

Alors que PPTP a été publié par l'IETF en juillet 1999, Cisco avait déjà annoncé L2F depuis 3ans, L2F est un protocole de tunnelage assez similaire sur le principe à PPTP en ce sens qu'il démarre par l'ouverture d'une connexion PPP du client vers un fournisseur d'accès Internet. La spécification de L2F a été publiée par l'IETF en mai 1998 dans la RFC 2341 (Cisco layer Two Forwarding (Protoco) « L2F»). La figure ci-dessous montre le principe de L2F.

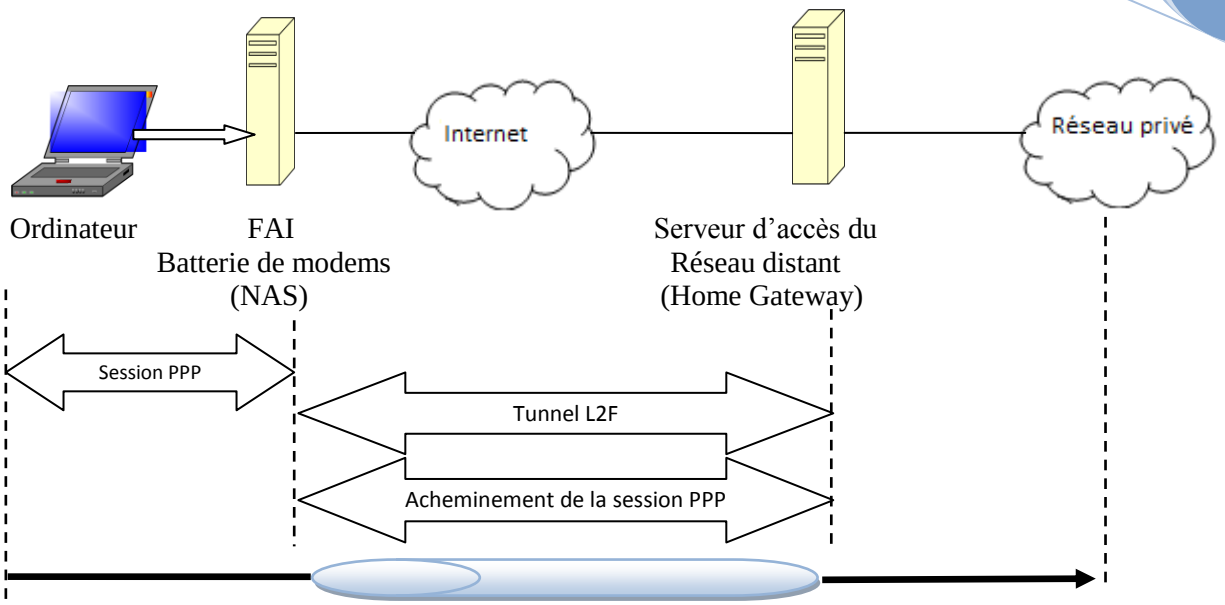


Figure 12 le principe de protocole L2F

L2F étant de nos jours largement remplacé par L2TP, on se contente de souligner les deux principales différences entre PPTP et L2F :

- Dans L2F, le tunnel est complètement transparent pour l'ordinateur distant. C'est le NAS (Network Access Server) du fournisseur d'accès Internet qui se charge de mettre en place le tunnel entre lui et le réseau de l'entreprise.
- Le tunnel ne commence donc qu'à partir du FAI et non de l'ordinateur distant. Comme dans tous les cas d'externalisation (outsourcing), la délégation a son prix, à savoir la perte de la maîtrise de la sécurité, puisqu'avec L2F, le FAI a une visibilité accrue sur les données qui circulent entre l'ordinateur distant et le réseau de l'entreprise.

5.1.5 L2TP

Principe générale

Microsoft et Cisco, reconnaissant les mérites des deux protocoles L2F et PPTP, se sont associés pour créer le protocole L2TP. Ce protocole réunit les avantages de PPTP et L2F. L2TP est un protocole réseau qui encapsule des trames PPP pour les envoyer sur des réseaux IP. Lorsqu'il est configuré pour transporter les données sur IP, L2TP peut être utilisé pour faire du tunneling sur Internet. Mais L2TP peut aussi être directement mis en œuvre sur des supports WAN (relais de trames) sans utiliser la couche de transport IP.

On utilise souvent ce protocole pour créer des VPN sur Internet. Dans ce cas, L2TP transporte des trames PPP dans des paquets IP. Il sert d'une série de messages L2TP pour assurer la maintenance du tunnel et d'UDP pour envoyer les trames PPP dans du L2TP.
La figure suivante illustre le principe de protocole L2TP :

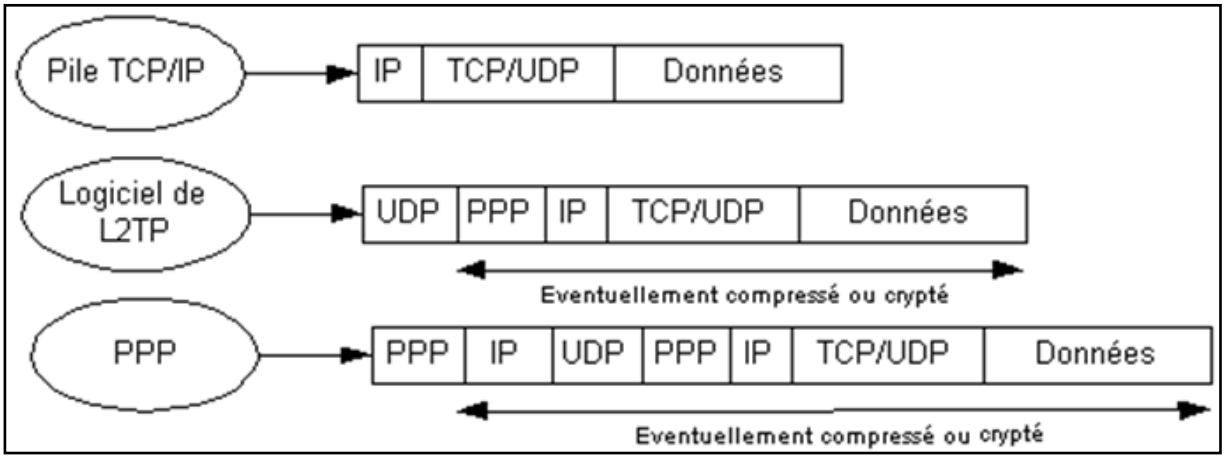


Figure 13 Principe de fonctionnement du protocole L2TP.

L2TP repose sur deux concepts :

1. Concentrateurs d'accès L2TP (LAC : L2TP Access Concentrator)

Les périphériques LAC fournissent un support physique aux connexions L2TP. Le trafic étant alors transféré sur les serveurs réseau L2TP. Ces serveurs peuvent s'intégrer à la structure d'un réseau commuté RTC ou alors à un système d'extrémité PPP prenant en charge le protocole L2TP. Ils assurent le fractionnement en canaux de tous les protocoles basés sur PPP. Le LAC est l'émetteur des appels entrants et le destinataire des appels sortants.

2. Serveurs réseau L2TP (LNS : L2TP Network Server)

Les serveurs réseau L2TP ou LNS peuvent fonctionner sur toute plate-forme prenant en charge la terminaison PPP. Le LNS gère le protocole L2TP côté serveur. Le protocole L2TP n'utilise qu'un seul support, sur lequel arrivent les canaux L2TP. C'est pourquoi, les serveurs réseau LNS, ne peuvent avoir qu'une seule interface de réseau local (LAN) ou étendu (WAN). Ils sont cependant capables de terminer les appels en provenance de n'importe quelle interface PPP du concentrateur d'accès LAC. Le LNS est l'émetteur des appels sortants et le destinataire des appels entrants. C'est le LNS qui sera responsable de l'authentification du tunnel. (MOGHRANI, 2011)

Le schéma de la figure 14 ci-dessus représente l'architecture générale de L2TP

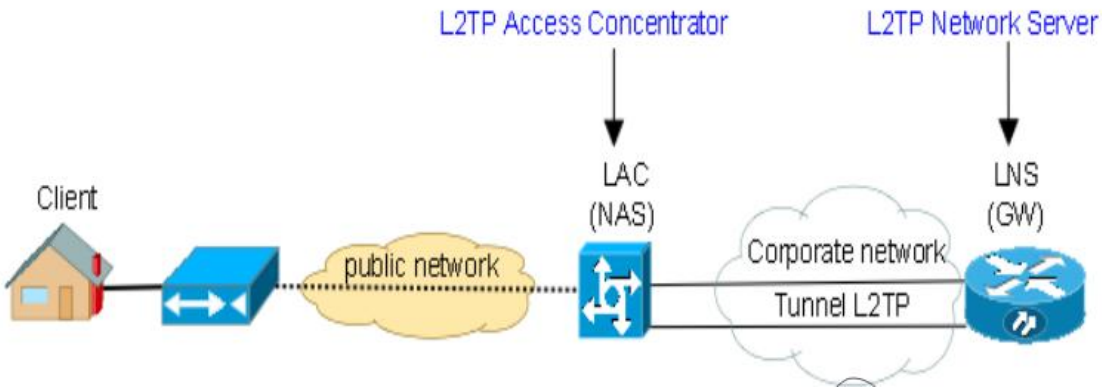


Figure 14 l'architecture L2TP

5.2 Protocoles de niveau supérieur

5.2.1 IPSEC

IPSec (Internet Protocol Security) a été conçu pour sécuriser les communications réseau à partir de la couche 3 du modèle OSI. Il a été conçu de manière à être supporté par Ipv4 et a été intégré dans le protocole Ipv6.

Il décrit des protocoles permettant de mettre en œuvre des tunnels sécurisés, au niveau 3 (IP).ces tunnels sont utilisés pour la sécurisation des protocoles des couches supérieures tels que TCP, UDP…

IPSec fournit les services de sécurité suivant :

- Confidentialité,
- Authentification mutuelle,
- Contrôle d'accès,
- Anti-rejeu (consiste à s'assurer qu'un message licite ne peut pas être réémis par une personne malveillante).

IPSec est basé sur deux mécanismes différents assurant les rôles de sécurisation des données: AH (Authentification header) et ESP (Encapsuling Security Payload). (Denis de REYNAL, 2004)

5.2.1.1 Détails du protocole

Le mécanisme interne d'IPSec est complexe. Le fait que ce protocole soit hautement configurable introduit des notions de gestion et de configuration inconnues du monde IP.

1. Gestion des flux IPSec

Les flux IPSec sont gérés unidirectionnellement. Ainsi, une communication bidirectionnelle entre deux machines utilisant IPSec sera définie par divers processus pour chacun des sens de communication. Les procédés détaillés ci-dessous respectent tout deux cette lois.

a. Security Policy (SP)

Une SP défini ce qui doit être traité sur un flux. Comment nous voulons transformer un paquet ?
Il y sera indiqué pour un flux donné :

- Les adresses IP de l'émetteur et du récepteur (unicast, mulitcast ou broadcast);
- Par quel protocole il devra être traité (AH ou ESP) ;
- Le mode IPSec à utiliser (tunnel ou transport) ;
- Le sens de la liaison (entrante ou sortante) ;

Notons qu'une SP ne défini qu'un protocole de traitement à la fois. Pour utiliser AH et ESP sur une communication, deux SP devront être créée.

b. Security Association (SA)

Une SA défini comment sera traité le paquet en fonction de sa SP associée. Elles ne sont que la "réalisation" des SP. Elle possède l'ensemble des propriétés de la liaison. Ainsi, elle sera représentée par une structure de donnée contenant les informations suivantes :

- Un compteur permettant de générer les numéros de séquence des entêtes AH et ESP ;
- Un flag (drapeau) permettant d'avertir qu'en cas de dépassement du compteur précédemment décrit, on doit interrompre la communication ;
- Une fenêtre d'anti répétition dans laquelle doit tomber le prochain numéro de séquence ;
- Information sur l'AH : algorithme d'authentification, clefs, durée de vie, etc ;
- Information sur l'ESP : algorithme d'authentification et de chiffrement, clefs, etc ;
- Mode IPSec : tunnel ou transport ;
- Durée de vie de la SA.

Une SA est identifiée à un seul et unique flux unidirectionnel grâce à trois champs :

- L'adresse IP de destination (unicast, multicast ou broadcast);
- Le protocole utilisé, AH ou ESP ;
- Le SPI (Security Parameter Index).

Une SA ne sera associée qu'a un seul des protocoles AH ou ESP. si nous voulons protéger un flux avec ces deux protocoles, deux SA devront être créé.

LE SPI est un indice (ou ID) sur 32 bits attribué au SA lors de sa création. Nous verrons plus loin que sa génération dépendra du mode de gestion des clés de sessions. Il sert à distinguer les différentes SA qui aboutissent à une même destination et utilisant le même protocole.

c. Bases de données SPD et SAD

Tout système implémentant IPSec possède donc 2 bases de donnée distinctes dans laquelle ils stockent leurs SP (ici, SPDatabase) et leurs SA (ici, SADatabase).

La SPD défini donc le traitement de chaque type de trafic entrant ou sortant, en fonction des émetteurs / récepteurs, selon trois type :

- DISCARD, dans ce cas celui-ci sera tout simplement jeté. Il n'est pas autorisé à sortir de la passerelle ni à la traverser ni à être délivré à une quelconque application.
- BYPASS IPSEC laisse passer le trafic sans traitement IPSec.
- APPLY IPSEC signifie que des services IPSec sont à appliquer à ce trafic.

Pour chaque trafic soumis à des services IPSec, la base SPD possède une référence vers la SA correspondante dans la base SAD. Si cette entrés n'est pas définie, dans le cas d'une gestion dynamique des clés, celle-ci sera alors créée en accord avec la configuration définie par l'administrateur. (Denis de REYNAL, 2004)

2. Modes d'IPSec

Il existe deux modes d'utilisation d'IPSec : le mode transport et le mode tunnel. La génération des datagrammes sera différente selon le mode utilisé.

a. Mode Transport

Ce mode est utilisé pour créer une communication entre deux hôtes qui supportent IPSec. Une SA est établie entre les deux hôtes. Les entêtes IP ne sont pas modifiées et les protocoles AH et ESP sont intégrés entre cette entête et l'entête du protocole transporté.

Ce mode est souvent utilisé pour sécuriser une connexion Point-To-Point.

b. Mode Tunnel

Ce mode est utilisé pour encapsuler les datagrammes IP dans IPSec. La SA est appliquée sur un tunnel IP. Ainsi, les entêtes IP originales ne sont pas modifiés et un entête propre à IPSec est créé. Ce mode est souvent utilisé pour créer des tunnels entre réseaux LAN distant. Effectivement, il permet de relier deux passerelles étant capable d'utiliser IPSec sans perturber le trafic IP des machines du réseau qui ne sont donc pas forcément prête à utiliser le protocole IPSec.

3. Détails des protocoles ajoutés

Nous verrons que certains champs sont présent dans les deux protocoles AH et ESP. En cas d'utilisation des deux protocoles pour un même flux de donnée, il n'y aura cependant pas redondance d'information.

Effectivement, il faut garder à l'esprit que AH et ESP seront géré séparément par des SA différents.

AH et ESP sont deux protocoles utilisant des clés des sessions utiles à leurs traitement sur le datagramme IP.

a. AH

AH ne crypte pas les données de paquet IP, mais il offre les services d'authentification et l'intégrité. AH n'empêche pas les utilisateurs non autorisés de lire le contenu des paquets capturés, mais il garantit que les paquet n'ont pas été modifiés en route et qu'ils proviennent bien des systèmes identifié par l'adresse IP source contenu dans le paquet. (Rafael CORVALAN, 2003)

Les deux figures ci-après illustrent la trame AH en mode transport et mode tunnel :

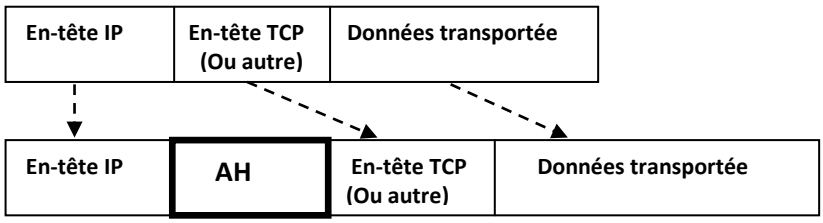


Figure 15 Trame AH en mode Transport

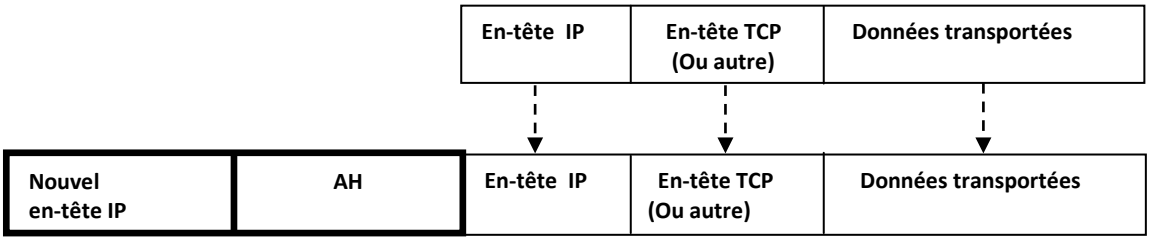


Figure 16 Trame AH en mode tunnel

Détails des champs de l'en-tête AH :

Le champ de l'en-tête AH est défini comme suit :

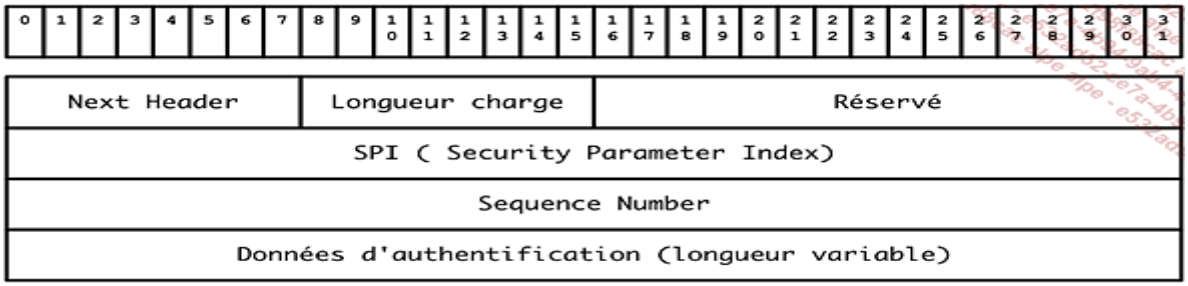


Figure 17 Structure de l'en-tête AH

- Entête suivante : ce champs permet de spécifier le type du protocole transporté ;
- Longueur des données : longueur de l'entête AH par facteur de 32-bit, le minimum étant 2;
- SPI : index unique définissant la SA pour ce paquet ;
- Numéros de séquence: compteur utile au mécanisme d'anti-répétition ;
- Données Authentification (variable) : champs contenant les signatures de hachages permettant d'authentifier l'émetteur et l'authenticité des données. la taille de ce champ dépend des protocoles de hachage utilisés. (Denis de REYNAL, 2004)

b. ESP

ESP permet la sécurisation des données du datagramme IP par le chiffrement (confidentialité), l'intégrité et l'authentification des données. En mode transport, seules les données transportées par le datagramme seront protégée, en mode tunnels, ce sera l'intégralité du datagramme qui sera protégé. Les formats de champ ESP en deux modes d'IPSec sont :

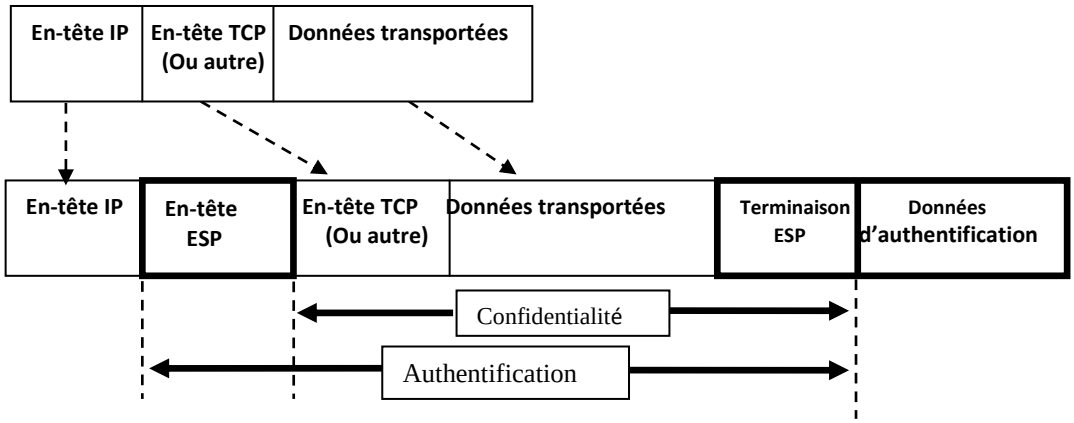


Figure 18 Trame ESP en mode Transport

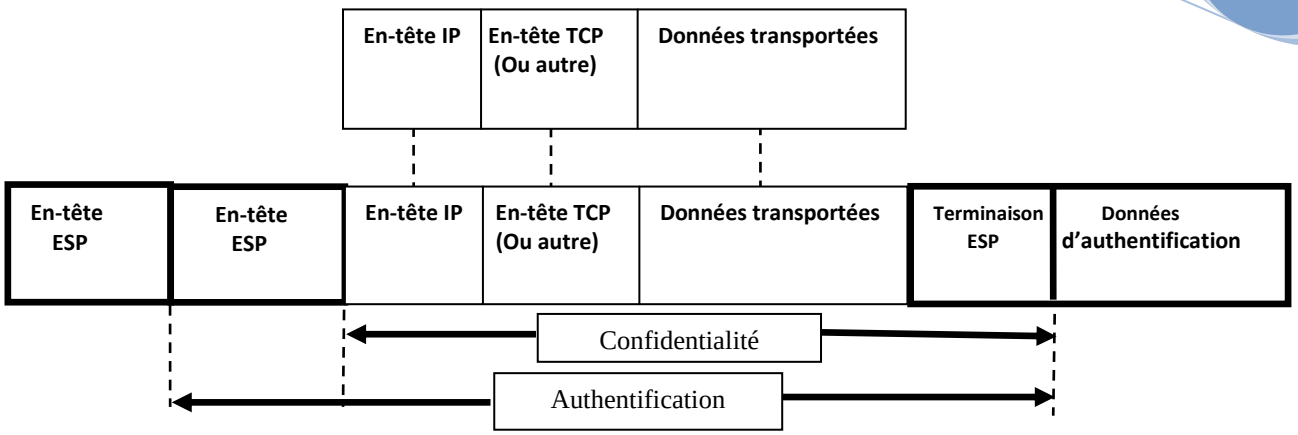


Figure 19 Trame ESP en mode Tunnel

Détails des champs du protocole ESP :

Le champ de protocole ESP est défini comme suit :

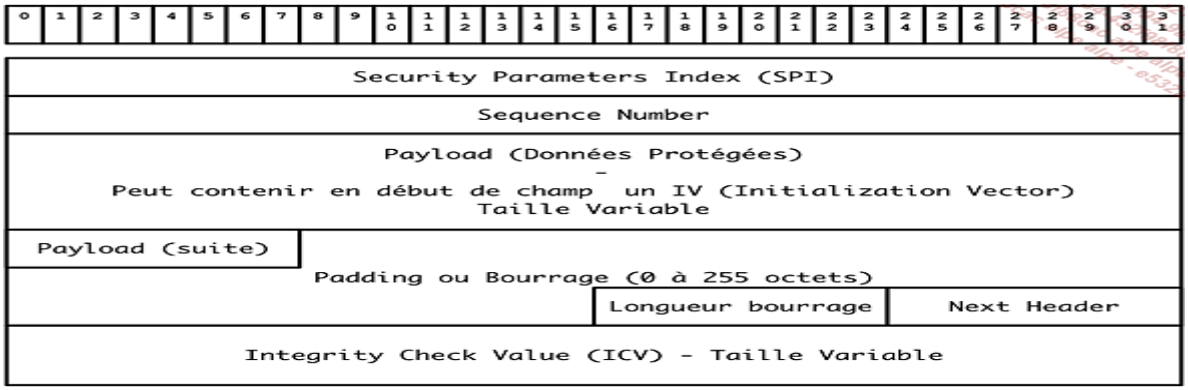


Figure 20 Structure de l'en-tête ESP

- SPI : index unique définissant la SA pour ce paquet ;
- Numéros de séquence: compteur utile au mécanisme d'anti-répétition ;
- Données : donnée du protocole de couche supérieure ;
- Bourrage : sert à l'encryption des données. Certains protocoles nécessitent une certaine taille afin d'être plus efficace et/ou applicable ;
- Taille du bourrage : indique la taille du bourrage ;
- Entête suivante : ce champs permet de spécifier le type du protocole transporté ;
- Données Authentification (variable) : champs contenant les signatures de hachages permettant d'authentifier l'émetteur et l'authenticité des données. La taille de ce champ dépend des protocoles de hachage et d'encryption utilisés.

Tous les processus que nous venons de découvrir son donc basé sur des mécanisme de cryptage et de hachage qui utilisent des clés de longueurs variable. Avant d'utiliser un VPN, il faut donc s'intéresser à la gestion de ses clés. (Denis de REYNAL, 2004)

4. Gestion des clefs IPSec

a. Les différents types de clefs

● Clefs de chiffrement de clefs

Ces clefs sont utilisées afin de chiffrer d'autres clefs et ont généralement une durée de vie longue. Les clefs étant des valeurs aléatoires, l'utilisation d'autres clefs pour les chiffrer rend les attaques par cryptanalyse (tentatives de déchiffrement du message) plus difficiles à leur niveau. La cryptographie à clef publique est souvent utilisée pour le transport de clefs, en chiffrant la clef à transporter à l'aide d'une clef publique.

● Clefs maîtresses

Les clefs maîtresses sont des clefs qui ne servent pas à chiffrer mais uniquement à générer d'autres clefs par dérivation. Une clef maîtresse peut ainsi être utilisée, par exemple, pour générer deux clefs : une pour le chiffrement et une pour la signature.

● Clefs de session ou de chiffrement de données

Ces clefs, contrairement aux précédentes, servent à chiffrer des données.

b. PKI - Public Key Infrastructure

De nombreuses applications et protocoles utilisent le cryptage à clef publiques sur d'importants réseaux. Il est nécessaire de pouvoir gérer dans ce cas un nombre important de clefs publiques. Pour cela, on a recours à des Infrastructures à Clefs Publiques, ou PKI (Public Key Infrastructure). Ces infrastructures se basent généralement sur des autorités de certification (CA : Certificate Authorities), qui garantissent l'authenticité des clefs publiques et permettent une gestion hiérarchisée de celles-ci.

c. Echange de clefs et authentification

La première étape lors de l'établissement d'une communication sécurisée, est l'authentification des interlocuteurs. Ensuite, 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 (L'échange de clef devant bien sur être authentifié).

Les types d'échange de clef sont:

1. Les mécanismes de sécurisation des échanges

Le « Perfect Forward Secrecy » (PFS) est assurée par une renégociation régulière des clefs. Dans le cas ou un attaquant intercepterait et déchiffrerait une clef de session, celle ci serait probablement déjà « périmée » avant qu'il puisse l'utiliser.

L'Identity Protection, ou protection de l'identité, est respectée si un message intercepté ne permet pas de déterminer l'identité des tiers communiquant.

Le Back Traffic Protection consiste en une génération de nouvelles clefs de sessions sans utilisation de clefs maîtresses. Les nouvelles clefs étant indépendantes des clefs précédentes, 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.

2. Algorithme de Diffie-Hellman

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 un mécanisme de cryptage à clef publique, et fait donc intervenir les valeurs publiques et privées des tiers. 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...).

Cet algorithme est très simple pour l'échange des clefs :

Soient 2 personnes A et B désirant communiquer sans utiliser une clef secrète. Pour cela ils se mettent d'accord sur 2 nombres g et n tels que n soit supérieur à g et g supérieur à 1, et cela sur un canal non sécurisé (il faut que n soit grand: de l'ordre de 512 ou 1024 bits pour que l'échange des clefs soit sécurisé). Ils prennent chacun chez eux un nombre aléatoire :

- A choisit x, calcul $X=g^x \bmod n$ et l'envoie à B ;
- B choisit y, calcul $Y=g^y \bmod n$ et l'envoie à A.

Ainsi le pirate peut intercepter X, et Y mais il lui est très très difficile d'en déduire x et y (c'est sur ce principe que repose la sécurité de l'algorithme). Une fois dans son coin, A calcule $k=Y^x \bmod n$ et B calcule $k'=X^y \bmod n$. En regardant de plus près, on constate que : $k=k'=g^{xy} \bmod n$. Ainsi, A et B ont réussi à créer un clef privée dont ils sont les seuls détenteurs. (Denis de REYNAL, 2004)

5.2.1.2 Le protocole IKE (Internet Key Exchange)

Ce protocole sert donc à assurer la gestion des clés entre les deux extrémités d'un tunnel. Il existe maintenant en deux versions : IKEv1 (décrit dans le RFC 2409 de novembre 1998) et

IKEv2 (décrit dans le RFC 4306 de décembre 2005). Il faut savoir que les deux versions ne sont pas interopérables, (les deux extrémités du tunnel doivent utiliser la même version). Par contre un même équipement peut parfaitement gérer certains tunnels dans la version 1 et d'autres dans la version 2.

Ce protocole emprunte des éléments à trois protocoles :

Le premier est *ISAKMP* (Internet security Association and Key Management Prtocol) qui permet la négociation, l'établissement, et la suppression d'associations de sécurité (SA), permettant ainsi la sécurisation de paquets devant être acheminés.

Il présente un mécanisme d'authentification et d'échange de clés et des algorithmes de chiffrement.

ISAKMP décrit actuellement cinq types d'échanges offrant des mécanismes de sécurité différents :

- Base Exchange,
- Identity Protection Exchange,
- Authentication Only Exchange,
- Aggressive Exchange,
- Informational Exchange;

Oakley a été développé par ORMAN HILARIE de l'université d'Arizona et a été formalisé dans la RFC 2412 en Novembre 1998. Il s'appuie fortement sur les mécanismes de Diffie-Hellman et STS (Station To Station). Il utilise également la protection contre le déni de service. Il permet aux deux entités de communication de se mettre d'accord sur les mécanismes d'échange de clés, de chiffrement et d'authentification qui seront utilisés pour sécuriser les échanges. Ceci se concrétise par la mise en place de différents modes d'échanges :

- Main Mode,
- Aggressive Mode,
- Quick Mode,
- Group Mode.

SKEME (Secure Key Exchange Mechanism) décrit une technique d'échange de clés permettant un renouvellement rapide des clés, développé spécifiquement pour IPSec. Il propose plusieurs modes d'échange de clés :

- Echange de clés utilisant le chiffrement asymétrique et l'algorithme diffie-Hellman.
- Echange de clés utilisant le chiffrement asymétrique seulement.
- Echange de clés utilisant une clé partagée au préalable.
- Echange rapide de clés utilisant des mécanismes de hachage.

IKE utilise ISAKMP, pour construire un protocole pratique. Le protocole de gestion des clefs associé à ISAKMP dans ce but est inspiré à la fois d'Oakley et de SKEME. Plus exactement, IKE utilise certains des modes définis par Oakley et emprunte à SKEME son utilisation du chiffrement à clef publique pour l'authentification et sa méthode de changement de clef.

Le protocole IKE définit quatre modes :

- Le mode principal (Main Mode) : est une instance de l'échange ISAKMP Identity Protection Exchange.
- Le mode agressif (Aggressive Mode) : est une instance de l'échange ISAKMP Aggressive Exchange.
- Le mode rapide (Quick Mode): permit la négociation rapide de clés de chiffrement quand une SA est déjà créée.
- Le mode nouveau groupe (New Group Mode) : permit la négociation de groupe à utiliser pour les échanges Diffie-Hellman.

Main Mode et Aggressive Mode sont utilisés durant la phase 1.

Quick Mode est un échange de phase 2.

a) Phase 1

Les attributs suivants sont utilisés par IKE et négociés durant la phase 1 : un algorithme de chiffrement, une fonction de hachage, une méthode d'authentification et un groupe pour Diffie-Hellman.

Trois clefs sont générées à l'issue de la phase 1 : une pour le chiffrement, une pour l'authentification et une pour la dérivation d'autres clefs. Ces clefs dépendent des cookies, des aléas échangés et des valeurs publiques Diffie-Hellman ou du secret partagé préalable.

Leur calcul fait intervenir la fonction de hachage choisie pour la SA ISAKMP et dépend du mode d'authentification choisi.

b) Phase 2 : Quick Mode

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.

Quick Mode est utilisé pour la négociation de SA pour des protocoles de sécurité donnés comme IPsec.

Chaque négociation aboutit en fait à deux SA, une dans chaque sens de la communication.

Durant cette phase, il s'agit de :

- Négocier les paramètres IPSec ;
- Générer une nouvelle clef dérivée de celle négociée en phase 1 grâce au protocole Diffie-Hellman. (si on prend on compte les mécanismes de sécurisation des échanges tels que PFS Perfect Forward Secrecy, ou le Back trafic Protection cus plus hauts, il peut y avoir d'autres échanges tels qu'une nouvelle négociation Diffie-Hellman..) ;
- Identifier le trafic que les SA négociées protégeront. (ARCHIER, 2010).

5.2.2 Tunnel sur la couche transport

Parmi les protocoles de tunnelage qui existe dans la couche de transport nous trouverons :

5.2.2.1. SSL/TLS

Apres avoir expliqué l'un des plus importants protocoles qui est IPESC. Nous allons maintenant passer à une autre grande famille de protocoles de tunnels en abordant SSL (Secure Sockets Layer) et TLS (Transport Layer Security). C'est une famille qui prend de plus en plus de place dans les implémentations de tunnels et nombreux sont maintenant les pare-feu proposant des tunnels SSL.

L'origine de ces protocoles remonte à un des navigateurs historiques : Netscape. Les équipes de développement de ce produit ont cherché dès 1994 à mettre en place un canal sécurisé afin de permettre l'échange de données confidentielles (authentification, carte bancaire...) entre le navigateur et le serveur. C'est ainsi qu'ont été successivement développées la version SSLv1 peu diffusée, puis la version SSL v2. Mais cette version souffrant d'un certain nombre de défauts importants en matière de sécurité a été remplacée fin 1995 par la v3.

En 1996 l'IETF (Internet Engineering Task Force) souhaita normaliser un protocole de type SSL. C'est ainsi que fut mis en place un groupe de travail TLS (Transport Layer Security).

Après diverses péripéties le groupe décida de publier le résultat de ses travaux sous le nom TLS v1.0 dans le RFC 2246 (janvier 1999). En avril 2006 la version TLS v1.1 a été publiée dans la RFC 4346, puis en août 2008 la v1.2 dans la RFC 5246. Il est à noter que, même si les différences entre les deux familles de protocoles ne sont pas majeures, elles sont suffisantes pour que TLS et SSL ne soient pas directement interopérables. Il faut donc que les deux extrémités d'un même tunnel utilisent le même protocole pour que cela puisse fonctionner. Mais la plupart des implémentations TLS savent revenir en SSLv3 quand cela est nécessaire.

De même, beaucoup de navigateurs savent utiliser les deux protocoles, même si certains ne prennent pas en charge les versions les plus récentes de TLS.(OPPLIGER, 2008)

Les mécanismes fournis par ces protocoles sont :

❖ Echange sécurité de clés de chiffrement ;

- Authentification du serveur ;
- Authentification du client.

La figure ci-dessous présente le mécanisme d'établissement d'un tunnel SSL entre un client et un serveur. (openssl)

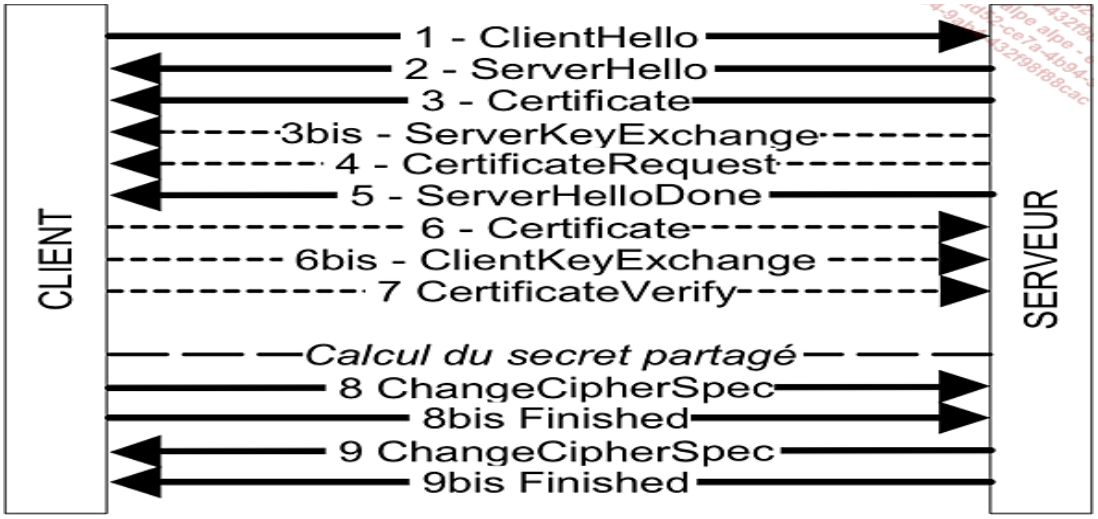


Figure 21 Le mécanisme d'établissement d'un tunnel SSL entre un client et un serveur

5.2.2.2. Secure Shell (SSH)

Est un protocole qui a été développé par Tatu Ylonen, qui deviendra par la suite fondateur de SSH communication. La première version de ce protocole (Version 1.5) fut publiée en novembre 1995. Il fut conçu pour remplacer les r-commandes (rlogin, rsh, rcp) et Telnet, offrant un niveau de sécurité insuffisant, surtout dans des cas d'utilisation sur un réseau public : pas d'authentification serveur, mots de passe transitant en clair …

Aujourd'hui la version 2 de SSH est soumise à l'IETF comme standard. Outre le remplacement des r-commandes et de Telnet, SSH permet de tunneliser des protocoles de niveau 4 par redirection des ports TCP. L'IANA a affecté le port 22 à SSH.

Le protocole SSH s'appuie sur des techniques de chiffrement symétrique et asymétrique, l'algorithme d'échange de clé Déffie-Hellman, et des algorithmes de hachage pour fournir les services de sécurité suivants :

- Authentification du serveur ;
- Authentification du client ;
- Protection en confidentialité des flux ;
- Protection en intégrité des flux.

SSH V1 et 2 permettent de tunneliser des flux TCP dans un tunnel SSH par la mise en œuvre d'une redirection de port. Le principe est globalement identique à celui utilisé par le tunnel SSL. Reprenons le cas de mise en œuvre pour la protection d'un serveur POP3 :

- ❖ Le démon SSH est lancé sur une passerelle SSH ;
- ❖ Le client se connecte sur le port SSH (TCP/22) ;
- ❖ Un port local est ouvert (POP3 TCP/110), et la redirection vers le serveur POP originel est paramétrée ;
- ❖ Le client pointe son client POP3 pour accéder au serveur localhost sur le port 110. (ARCHIER, 2010)

Comme l'illustre la figure suivante :

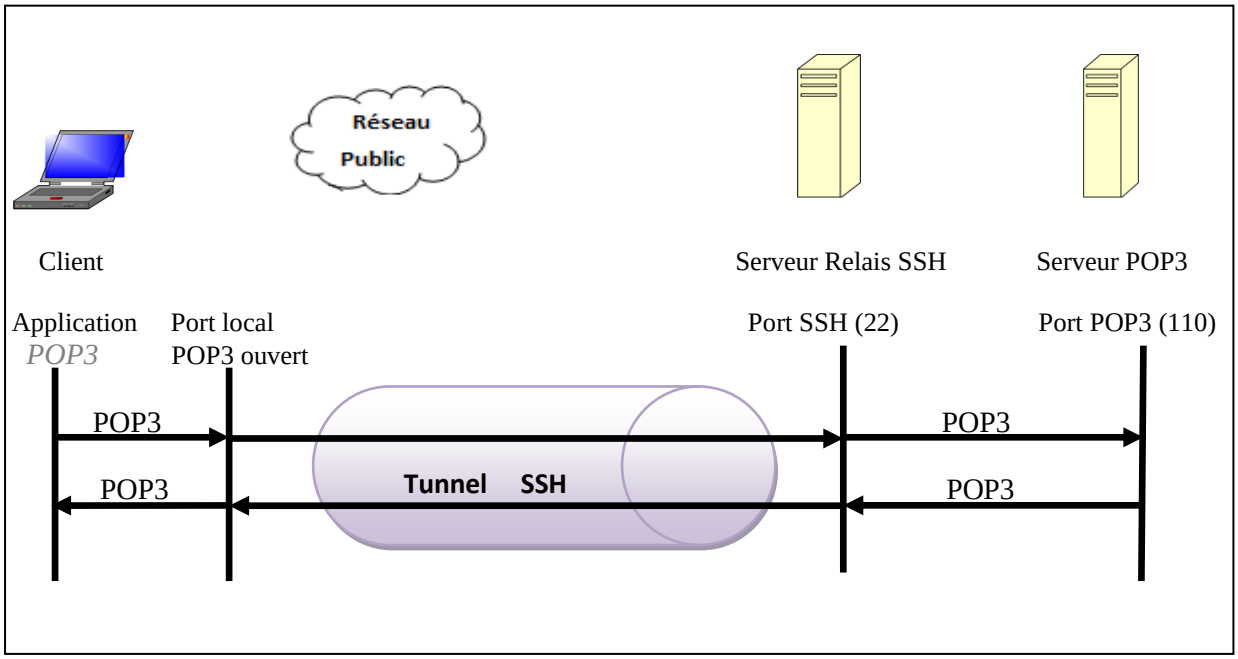


Figure 22 Mise en œuvre d'un tunnel SSH

5.3 MPLS/VPN

MPLS est une technique de pointe qui permet d'assurer une transmission des paquets très performante. Cette nouvelle technologie a de nombreuses utilisations, que se soit dans un environnement de fournisseur de services ou dans un réseau d'entreprise. De nos jours, MPLS est surtout déployé pour la mise en place de réseaux privés virtuels (MPLS/VPN).

MPLS décrit les mécanismes qui permettent de réaliser la commutation de labels, laquelle associe les avantages de la transmission de paquets fondée sur la commutation de couche 2 avec ceux de routage de couche 3. (GUICHARD, 2005)

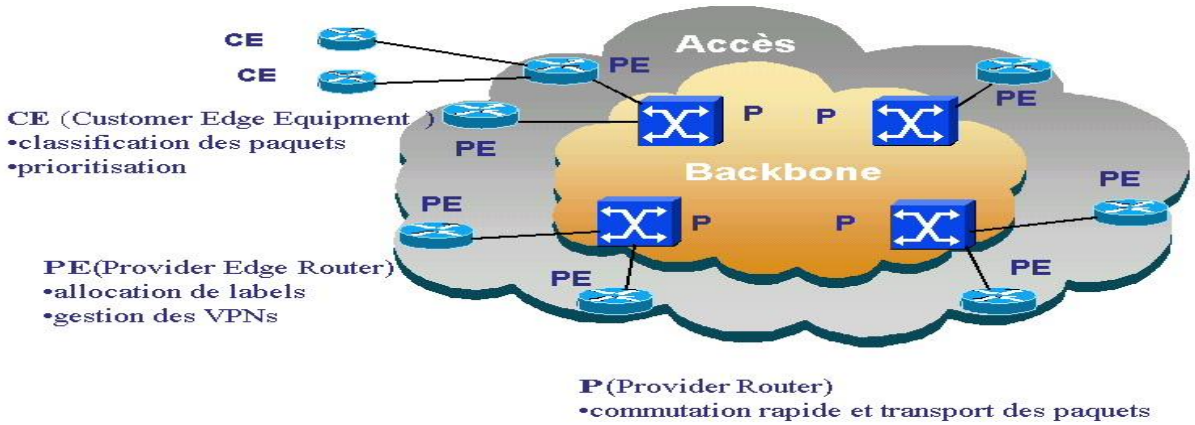


Figure 23 Le protocole MPLS

Conclusion

A travers ce chapitre, nous avons vu un aperçu des différentes possibilités afin de déployer un VPN, et particulièrement la solution que représente IPSec. Nous avions en effet pour objectif de vous donner les concepts qui tournent autour de cette solution. Mais également que le terme de VPN ne se référençait pas qu'a la solution IPSec. Certes cette solution est la plus utilisée et elle est une référence mais le VPN est avant tout un concept et ne précise rien concernant ses moyens.

Ainsi s'achève notre étude sur les VPNs. nous nous rendons compte que derrière ce concept, une multitude de protocoles, techniques et architectures existent pour leur déploiement.

Chapitre 3 : Présentation de l’organisme d’accueil et Conception

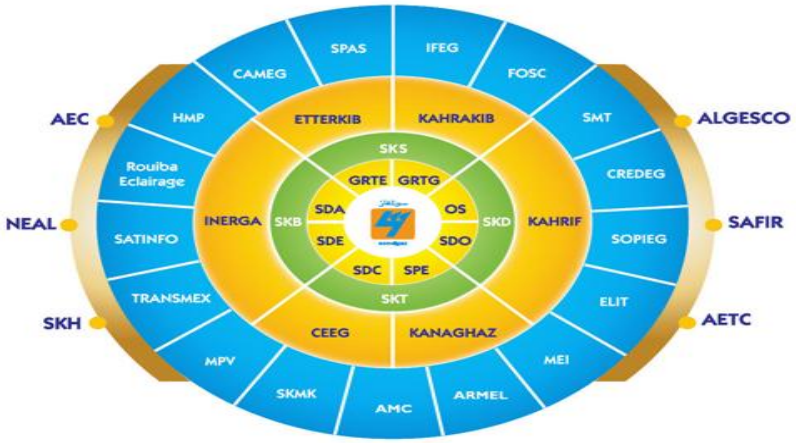
I. Présentation de l'organisme d'accueil

1. Historique d'INERGA

Crée par SONELGAZ (Société Nationale d'Electricité et du Gaz) en 1979 en tant qu'unité de génie civil "KC", elle avait pour mission de contribuer à réaliser les infrastructures électriques et immobilières inscrites dans son propre programme d'investissement. A la faveur des réformes économiques mises en œuvre en Algérie à compter de 1982 :

- L'unité KC est érigée en Entreprise de Réalisation d'Infrastructures Energétiques (dénommée en abrégé INERGA), le 1er Janvier 1984 (cf. décret N° 83- 681 du 29 octobre 1983), dépendant du Ministère de l'Energie et des Mines.
- INERGA obtient son autonomie, à compter du 03 mars 1990, en devenant Entreprise publique Economique, Société par Actions (EPE/spa). A ce titre, elle est régie par le code du commerce et dotée d'organes de délibération (Assemblée Générale) et d'administration (Conseil d'Administration). Son capital est détenu entièrement par l'Etat.
- En janvier 2006, INERGA réintègre Sonelgaz et devient filiale.

Relativement jeune, INERGA a réussi, en une courte période de temps (une vingtaine d'années d'âge), à compter parmi les plus importantes entreprises Algériennes dans son domaine. (INERGA, 2007)



Filiales métiers de base

Filiales production en partenariat

Filiales travaux

Filiales métiers périphériques

Sociétés en participation

Figure 24 l'architecture générale de sonelgaz

2. Présentation d'INERGA

INERGA est une société par action filiale de Sonelgaz qui a pour finalité la réalisation d'infrastructures. Elle détient un capital social de 350 000 000 DA. INERGA est l'une des plus grandes entreprises nationales de construction spécialisée dans le domaine des réalisations d'infrastructures à caractère énergétique, industriel et immobilier. INERGA est chargée de :

- Etudier et réaliser les infrastructures d'ouvrages énergétiques et leurs annexes, à savoir, les travaux de :
  - Génie civil industriel, notamment à caractère énergétique.
  - Réseaux divers.
  - Eventuellement, tous corps d'état secondaires.
- Mener, d'une manière générale, toutes les opérations commerciales, industrielles, mobilières, immobilières et financières inhérentes à ses activités et de nature à favoriser son développement.

3. Les valeurs d'INERGA

La réussite d'INERGA repose sur la capacité de ses équipes à relever les plus grands défis, tout en respectant les exigences de résultat qu'elle s'impose. Cette culture trouve ses fondements dans les valeurs suivantes :

- **La confiance et l'honnêteté :**

INERGA n'accepte ni dérive, ni négligence quand il s'agit de respect des exigences explicites ou implicites. De plus, avec ses Clients, INERGA cherche à dépasser les relations économiques Client -Fournisseur, en vue de privilégier la dimension noble qu'est l'honnêteté.

- **Le sérieux, la discipline, le respect et la considération de l'autre :**

Que cela soit en interne ou en externe, chaque partenaire est traité avec égard dans un esprit imprégné de discipline et de respect de l'organisation et de ses règlements.

Se considérant, par ailleurs, comme une entreprise sérieuse, INERGA cultive cette valeur à tous les niveaux. Ses Clients peuvent compter sur elle pour réaliser leurs projets.

- **Le respect des engagements :**

Quelles que soient les conditions, les engagements d'INERGA sont tenus. Dés lors que le Client confie à INERGA un projet à réaliser, et que les règles sont bien définies au préalable, celui-ci a l'assurance que ses exigences sont satisfaites.

- **La reconnaissance des efforts et la fierté d'appartenir à INERGA :**

Considérer les hommes et les femmes d'INERGA dans toutes leurs dimensions : professionnelle, affective et sociale. Se distinguer par des efforts exceptionnels ne doit passer sans une

reconnaissance formelle qui fait connaître l'auteur et lui témoigner reconnaissance. Avoir le souci de développer de ses capacités et le motiver sont des motifs de fierté et développement de la solidarité.

4. Qualité d'INERGA

La satisfaction du Client et la qualité de ses prestations sont au centre de toutes les préoccupations d'INERGA. Cela est d'autant plus évident et important qu'elle a réuni, en plus, toutes les conditions pour que son système qualité soit reconnu capable de répondre aux exigences de la norme ISO 9002/1994, par AFAQ Ascert International depuis le 15 Décembre 1999.

A vrai dire, la diversification de ses Clients, nationaux et étrangers, tous de renom et aussi exigeants les uns que les autres, est à l'origine de la volonté de l'Entreprise d'effectuer ce saut qualitatif, en optant, en 1998, pour une démarche qualité qui a débouché sur la certification de son système assurance qualité. Ainsi, INERGA est la seconde Entreprise algérienne et la première dans son secteur à obtenir le certificat ISO 9002/1994. Emboîtant le pas à la norme dans sa version 2000, INERGA a fait évoluer son Système d'Assurance de la Qualité (SAQ) à un Système de Management de la Qualité (SMQ). INERGA a obtenu la certification de son système Management Qualité selon le référentiel ISO9001 version 2000 depuis le 15 septembre 2003.

Le pilotage de son SMQ est fondé sur une démarche basée, d'une part, sur un pragmatisme forgé par l'expérience et le souci d'efficacité des processus, et, d'autre part, par une vision et des orientations claires et simples de la Direction Générale, comme énoncé dans la déclaration (Politique Qualité) du Président Directeur Général. Cette dernière est axée sur :

- La satisfaction du client.
- La valorisation de l'homme au travail.
- La garantie de la maîtrise des processus et de leur amélioration.
- L'esprit de partenariat entre l'Entreprise, le Personnel, ses Clients et ses Fournisseurs.

Sur le même sillage, une démarche HSE est en cours ayant pour objectif d'ancrer davantage chez le Personnel, déjà bien imprégné par cet esprit, les réflexes liés à la santé et sécurité au travail. Les résultats enregistrés dans ce domaine sont très encourageants et ont valu à **INERGA** de nombreuses distinctions par ses Client.

5. L'organigramme de la division d'accueil (INERGA):

La figure suivante montre l'organigramme de la division d'accueil d'INERGA :

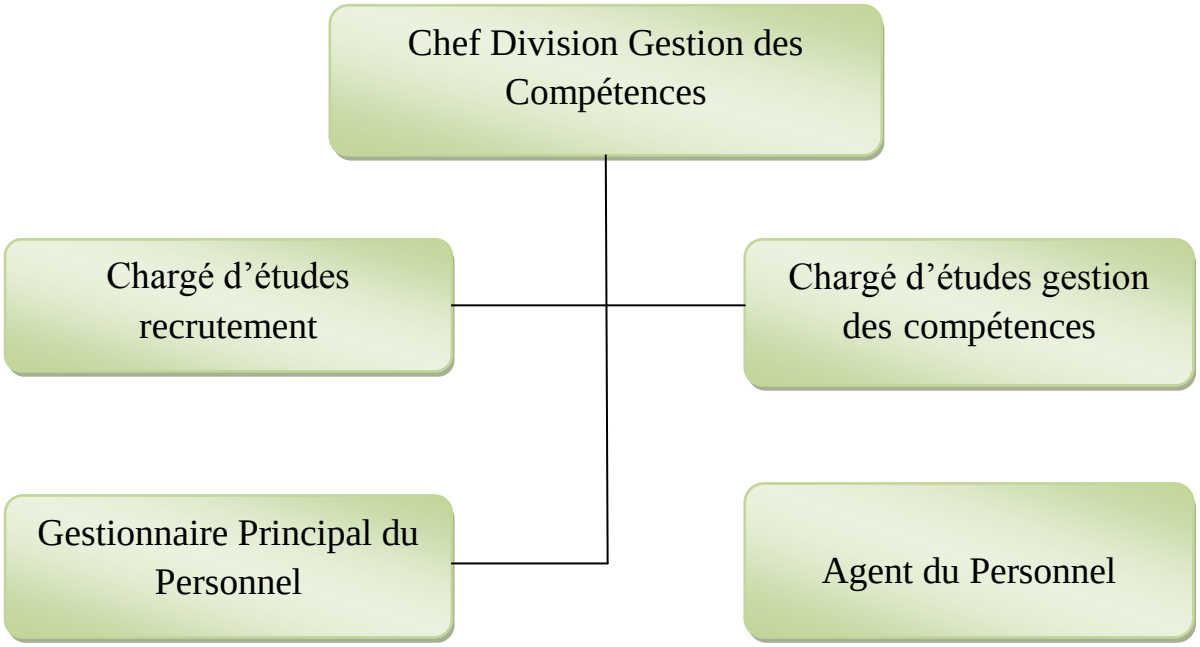


Figure 25 Organigramme d'INERGA

6. Ressources humaines

C'est, sans doute, la ressource la plus précieuse dont dispose INERGA. Douée d'une adaptabilité remarquable et possédant un savoir-faire qui lui permet de valoriser toutes les autres ressources. Elle est composée d'un noyau dur capable d'encadrer toutes les catégories de Personnel, dans toutes les spécialités techniques et de management.

En moyenne, l'Entreprise emploie 2300 Agents dont 75 % ont des relations de travail à durée déterminée (CDD).

Pour être en mesure d'épouser le plan de charge, sans cesse évolutif et diversifié, INERGA s'est organisée de façon à rendre ses structures et ses équipes flexibles et adaptables.

Elle a mis en place un système de recrutement rigoureux qui s'appuie sur une sélection basée sur des exigences claires, et favorise l'émergence de compétences grâce à des évaluations régulières et une formation permanente touchant toutes les catégories.

Enfin, INERGA dispose d'un fichier de compétences mobilisables en fonction des besoins exprimés par les différentes activités.

Particulièrement, pour son encadrement, l'Entreprise organise annuellement une "Conférence des Cadres" qui constitue un espace d'échange, d'information, de réflexion, de propositions, de connaissance mutuelle des membres de cette catégorie qui se regroupent dans une structure hôtelière où l'ambiance amicale et de travail se côtoient.

S'agissant des activités socioculturelles, INERGA dispose d'un Service, fonctionnant grâce à un budget spécial, chargé d'organiser des vacances pour l'ensemble des Travailleurs et leurs enfants,

des activités sportives et de détente, des actions d'aide à certaines familles en difficultés, des prêts sociaux, etc.

La structure globale de la Ressource Humaine présente ainsi :

- ✓ Ingénieurs et Cadres : 7%
- ✓ Techniciens et Agents de Maîtrise : 13%
- ✓ Personnel opérationnel : 80%

7. Les clients d'INERGA

Nombreux sont les Clients d'INERGA, en raison des divers projets réalisés dans différentes régions, avec, toutefois, une concentration de plus en plus forte de ceux qui activent dans le secteur de l'énergie. Ils sont soit des donneurs d'ordre nationaux soit leurs partenaires multinationaux.

Evoquer les Clients, c'est rappeler l'incontestable enrichissement dont a bénéficié INERGA grâce à leurs exigences et leur professionnalisme qui sont la source indéniable de son développement et de son évolution, et qui font d'elle un partenaire incontournable aujourd'hui dans son marché. La reconnaissance du sérieux et du professionnalisme d'INERGA, par ses clients, est manifestée à différentes étapes des réalisations, et témoigne du souci d'INERGA à assurer une écoute permanente qui à l'origine de sa réactivité, singulièrement appréciée par tous ses Partenaires.

8. Réseau étendu d'INERGA

Une interconnexion par réseau informatique a été établit entre le siège social et la Direction Matériel (Blida) et les bases logistiques de Hassi Massoud et Oran, ce qui, facilitera, désormais, les échanges électroniques des différentes données professionnelles et l'utilisation du système

d'information.

Cette réalisation s'inscrit dans le cadre du projet *« réseau étendu Intranet/VPN sécurisé »* pour l'interconnexion des trois sites d'INERGA (les trois bases Logistiques).

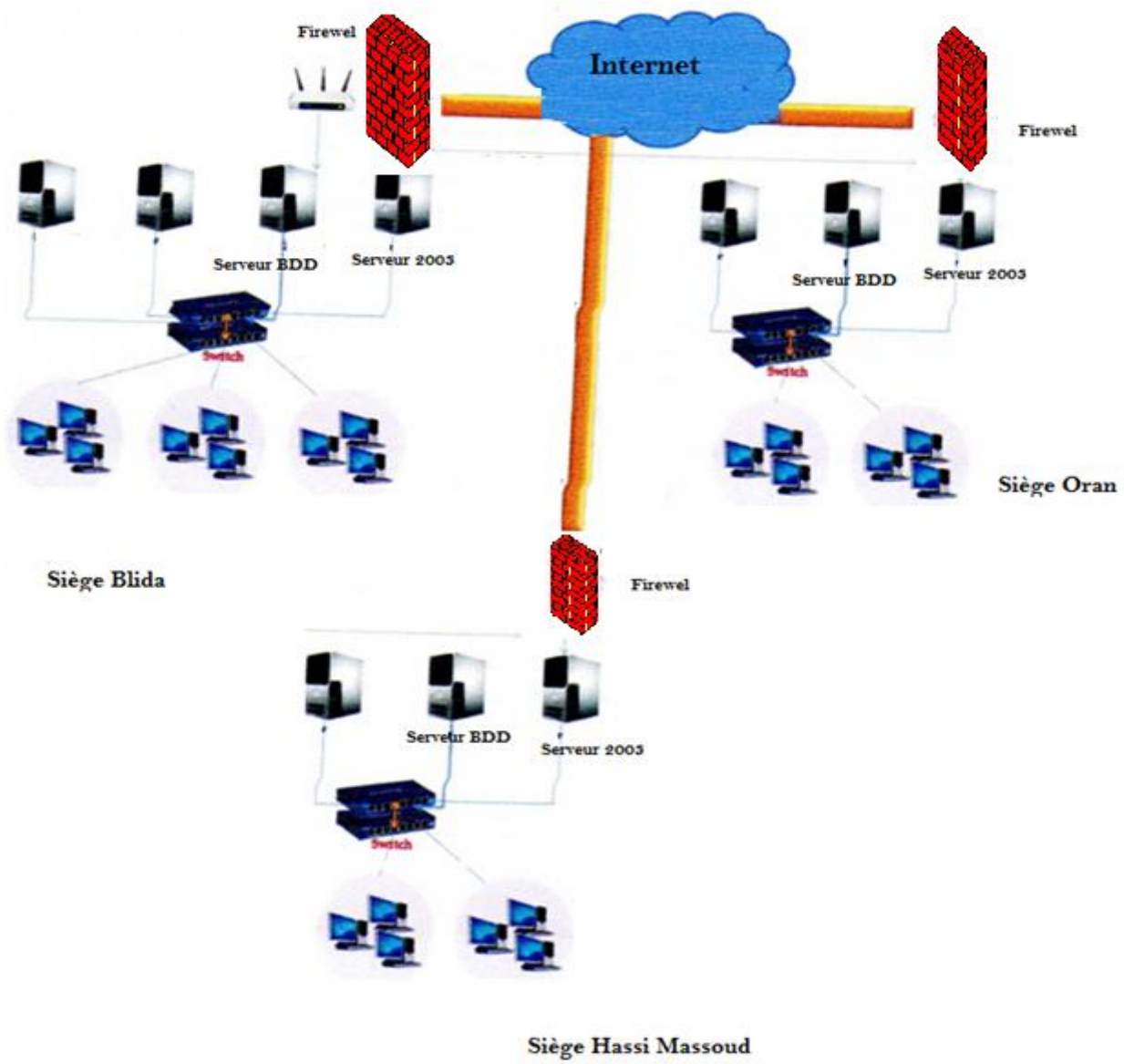


Figure 26 L'architecture réseau des trois sièges d'INERGA

La figure ci-dessus montre l'interconnexion des réseaux de trois sièges de groupe INERGA, avec une connexion internet.

Problématique

INERGA est une entreprise composée de trois sites distants qui souhaite en tirer les avantages d'une liaison Internet entre ses sites en intégrant une connexion site à site pour d'éventuelles tâches d'administration à distance. Mais comment assurer la sécurité des échanges de données entre les trois sites ?et comment assurer un accès à distance sécurisé de chaque site pour ses utilisateurs nomades ?

II. Conception

1. La solution proposée

Pour sécuriser les communications entre les trois sièges de groupe INERGA, en prenant en compte tout les types de trafics réseau, nous utilisons d'une part, des VPN (site à site) de niveau 3, en se basant sur le protocole IPSec, pour les raisons suivantes :

- Les trois directions disposent des adresses publiques ce qui convient efficacement au mode tunneling d'IPSec, qui assure la sécurité maximale (traitement total des paquets par IPSec) des trafics réseau inter direction.

- Les systèmes de communications n'implémentent pas les protocoles IPSec (les utilisateurs internes de réseau), ce sont les passerelles situées aux bouts de la connexion WAN qui le font (ce qui diminue le trafic IPSec).

Et d'autre part, nous allons utiliser les protocoles L2TP/IPSec pour garantir l'accès sécurisé à distance des utilisateurs pour chaque site, sachant que L2TP assure l'établissement des tunnels sécurisés et IPSec en mode transport, assure l'authentification et la confidentialité des données.

En effet, nous allons présenter l'architecteur et la typologie choisie, pour l'interconnexion (site à site) des trois sièges d'INERGA (Blida, Oran et Hassi Massoud), ainsi que celle d'accès à distance (poste à site). La solution proposée est présentées dans les deux figures ci-dessous :

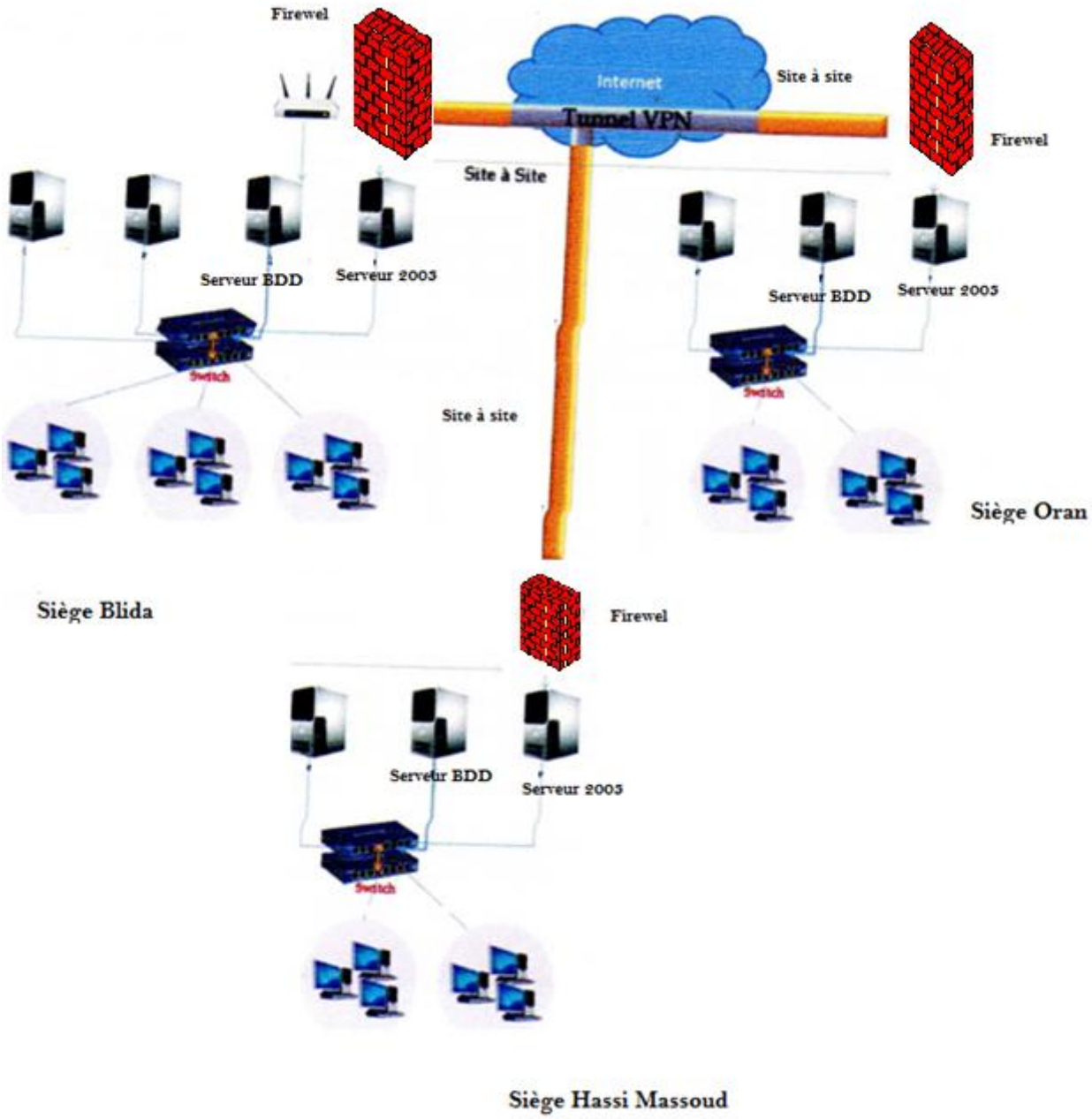


Figure 27 La Solution site à site

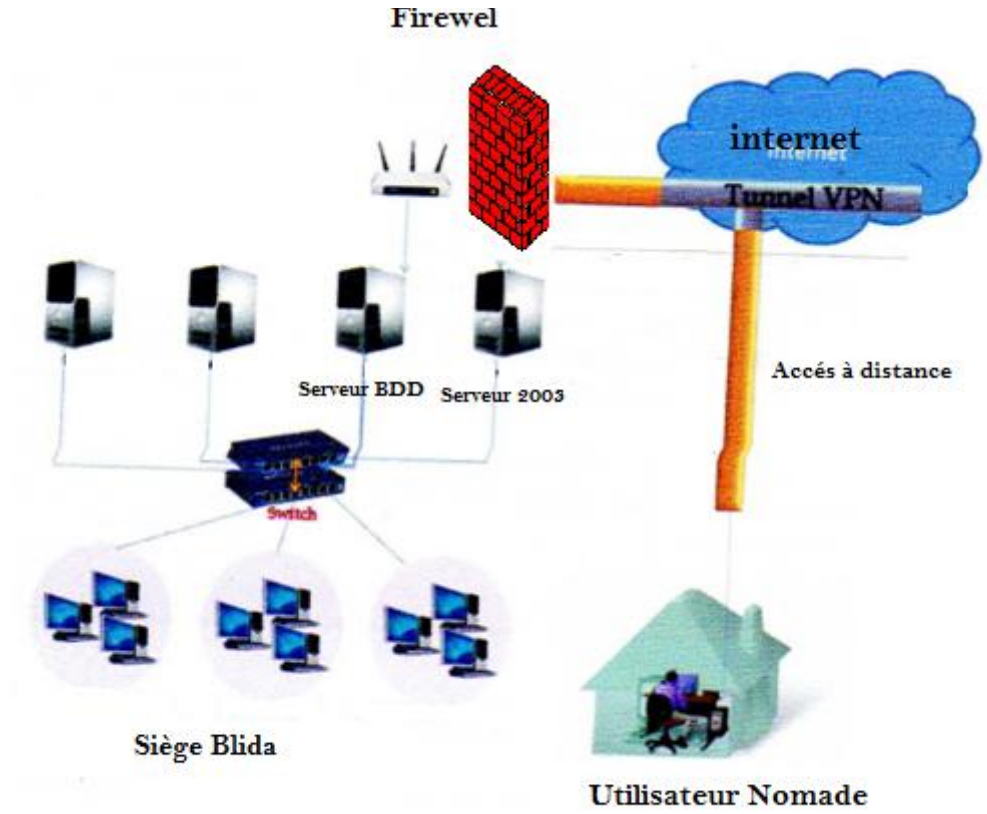


Figure 28 La solution d'accès à distance

2.1. Description de la solution

Pour mettre en place la solution, nous allons utiliser la notion « politique de sécurité IP » qui contrôle et sécurise tout le trafic réseau inter-direction, et qui sera définit sur les passerelles d'extrémité des trois sites (site à site), ainsi que une autre politique qui sera partagée entre les passerelles et les utilisateurs nomades pour l'architecture poste à site.
Pour cela nous allons recourir aux concepts d'IPSec pour définir notre politique de sécurité sous forme de stratégies.

2.2. La stratégie IPSec

Une stratégie IPSec est une collection de filtres de paquets imposant la stratégie de sécurité au trafic IP. Chaque filtre décrit une certaine action de protocole réseau. Si le trafic arrivant ou quittant le périphérique réseau sur lequel la stratégie est activée correspond à un de ces filtres, ce trafic est

bloqué, autorisé ou, avant qu'il ne puisse continuer, une connexion IPSec est négociée entre les périphériques expéditeurs et récepteurs.

Un filtre peut être la réception ou l'initialisation d'un protocole spécifique, d'une requête de connexion depuis ou vers un périphérique particulier ou toute autre action pouvant être déterminée d'après le protocole, le port, l'adresse IP ou la plage IP. Ces filtres sont définis comme règles dans une stratégie IPSec.

Les filtres sont rassemblés en listes de filtres, appartenant elles-mêmes à des règles. Chaque règle définit également une action de filtre ainsi que des informations potentiellement imposantes définissant les caractéristiques spécifiques à employer lors de négociation de connexion IPSec. Les actions de filtre sont : refuser, autoriser ou négocier la sécurité. Toute règle ne peut posséder qu'une action de filtre, mais une stratégie comporte nombreuses règles.

La figure suivante illustre la stratégie IPSec :

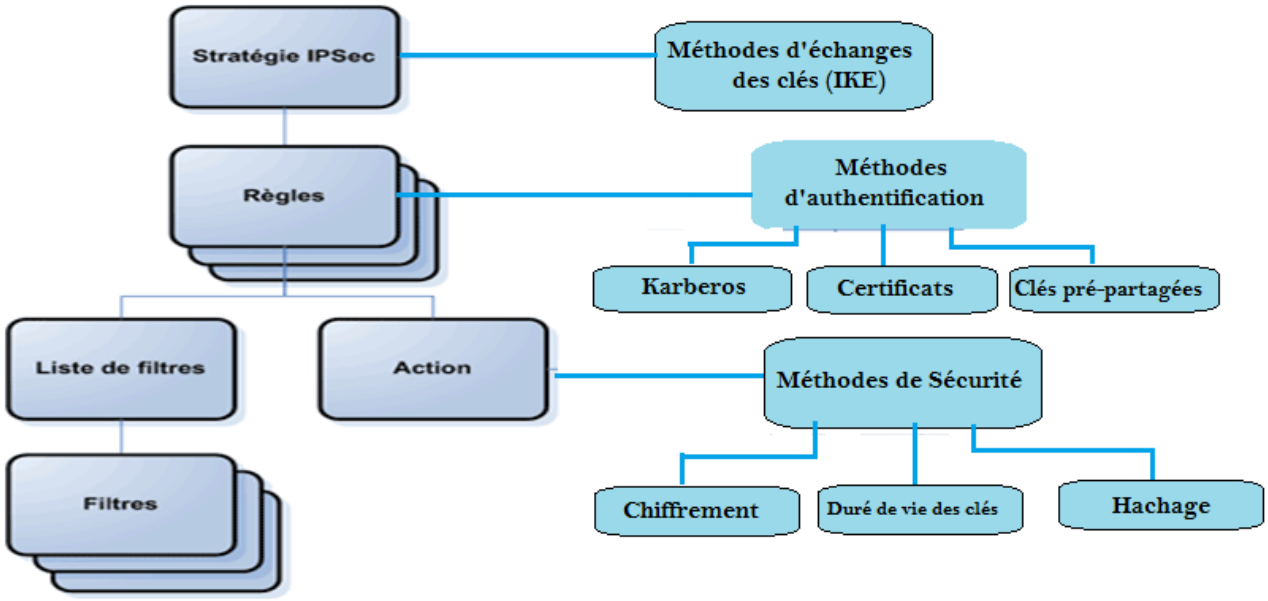


Figure 29 La stratégie IPSec

Diagramme de contrôle des connexions site à site :

Tout le trafic réseau est contrôlé par la stratégie IPSec, si un trafic repend aux conditions d'un filtre IP de la liste des filtres, ce dernier déclenche l'action correspondante pour établir un chemin sécurisé vers la destination identifiée par l'adresse IP.

Le diagramme suivant illustre comment avoir une connexion site à site sécurisée :

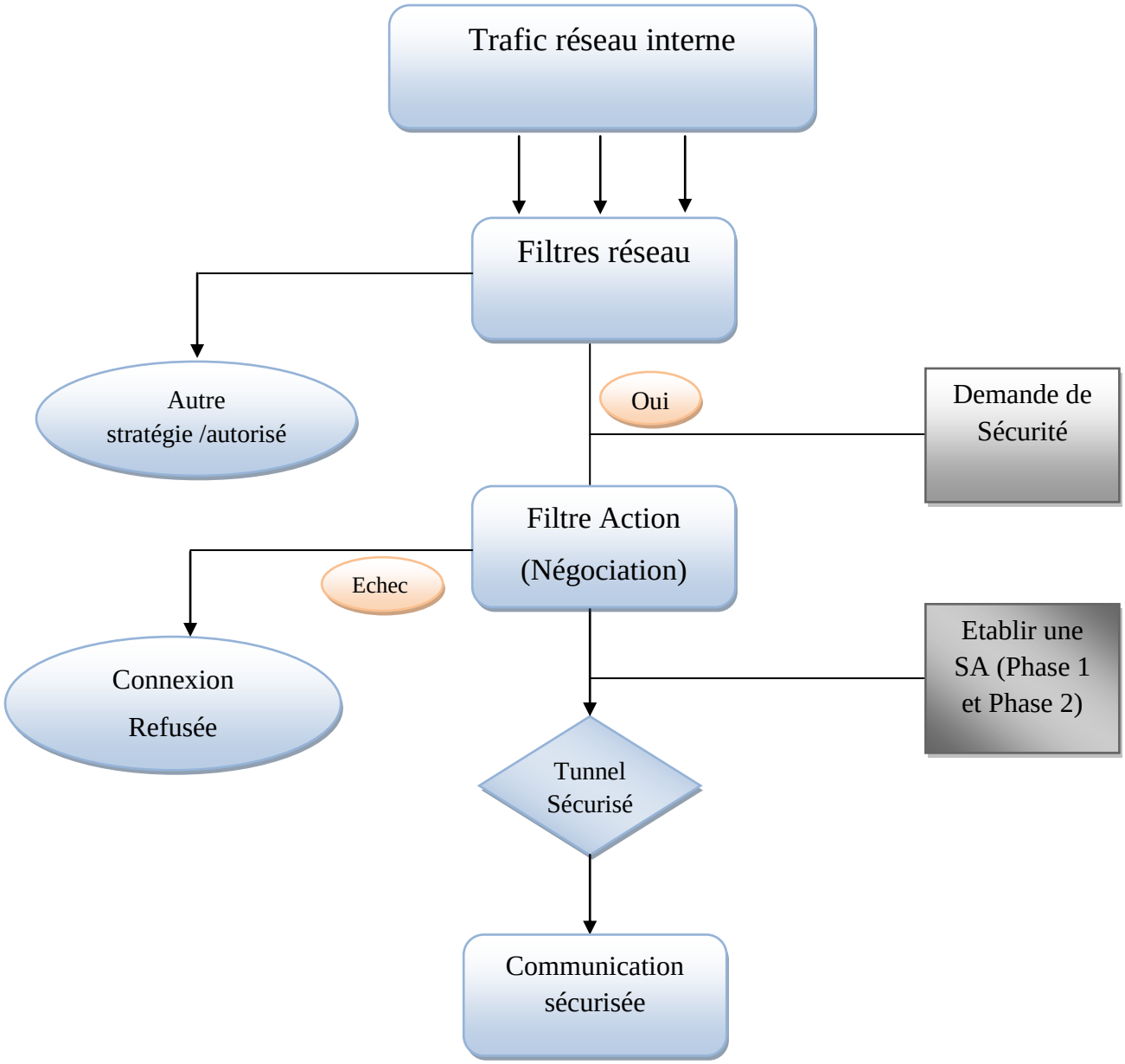


Figure 30 Diagramme d'accès site à site

Diagramme de contrôle poste à site :

A la demande de client d'une connexion sécurisé, des négociations IPSec sont déclenchées pour établir des associations de sécurité de mode rapide et de mode principal d'IPSec, puis L2TP négocie le tunnel, et notamment ses options de compression et d'authentification.

Le diagramme ci-après, montre les étapes principales pour établir une connexion à distance entre les utilisateurs nomades et leur propre entreprise :

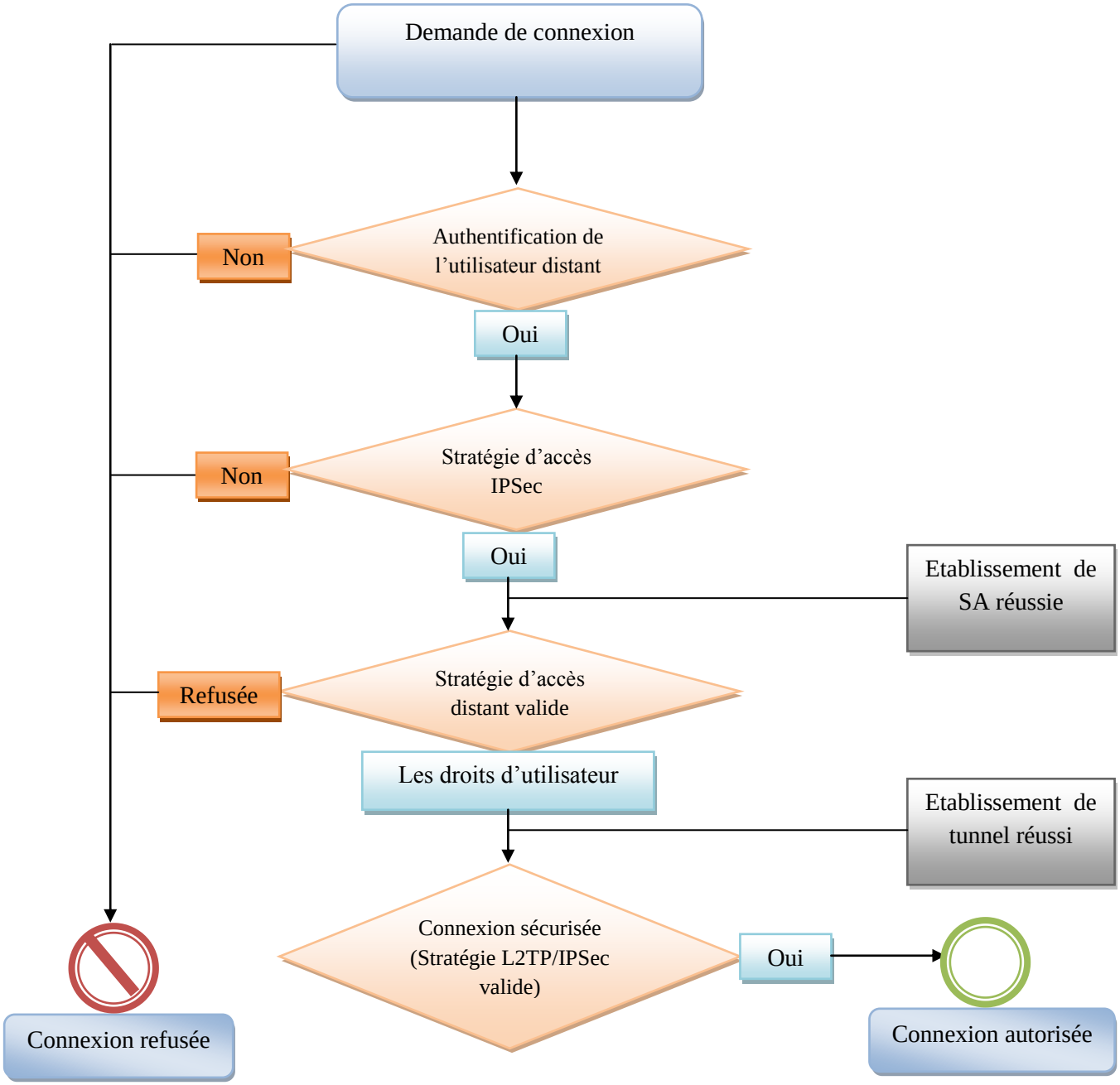


Figure 31 Diagramme d'accès distant (poste à site)

2.3. La stratégie d'authentification

Pour garantir une authentification mutuelle entre les utilisateurs et les passerelles ainsi que les passerelles entre elles nous allons utiliser des certificats électroniques, délivrés par autorité de certification (CA) racine (principale) de site central et deux autres CA subordonnées des autres sites.

Point sur le certificat : Un certificat électronique (aussi appelé certificat numérique ou certificat de clé publique) peut-être vu comme une carte d'identité numérique. Il est utilisé principalement pour identifier une entité physique ou morale, mais aussi pour chiffrer des échanges. Il est signé par un tiers de confiance qui atteste du lien entre l'identité physique et l'entité numérique (Virtuel). Le standard le plus utilisé pour la création des certificats numériques est le X.509.

L'utilisation de certificat garantie les différent objectifs de sécurité.

2.3.1. Autorité racine d'entreprise

Une autorité racine se situe tout en haut d'une chaîne de certificats. Une autorité racine d'entreprise sert d'autorité racine à toute l'entreprise : elle occupe la place la plus élevée dans la hiérarchie d'approbation des certificats émis par tous les composants de l'entreprise. L'autorité racine d'entreprise peut émettre des certificats pour des autorités subordonnées, pour des utilisateurs et pour les machines. Elle signe elle-même son propre certificat, garantissant ainsi que cette signature correspond à la racine ; cette auto-signature permettra ensuite, à la racine d'émettre des certificats pour les utilisateurs, les machines et les autorités subordonnées.

2.3.2. Autorité subordonnée d'entreprise

Exige un certificat émis par une autorité racine, de façon à former un maillon dans la hiérarchie des certificats. Comme fait office d'autorité de certification d'entreprise, elle peut émettre des certificats pour des autorités subordonnées ou, plus directement, pour des utilisateurs finals et des ordinateurs.

La figure ci-après illustre l'infrastructure des autorités de certification :

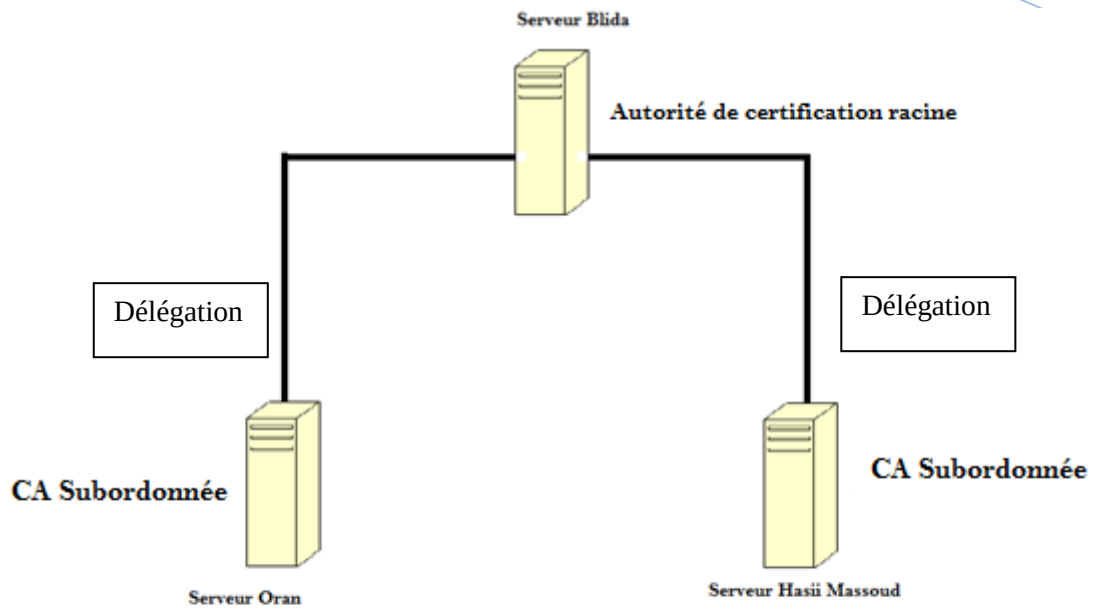


Figure 32 Infrastructure des autorités de certification

Conclusion

Dans ce chapitre, nous avons présenté l'organisme d'accueil qui est INERGA, et montré la vulnérabilité de l'interconnexion de trois sites de ce groupe, qui nous a guidé à poser une problématique dans ce sens, dés lors nous avons proposé une solution conceptuelle.

Dans le prochain chapitre nous allons suivre les démarches cités pour concrétiser les solutions proposées en tenant compte de matériels utilisés dans l'entreprise.

Chapitre 4 : Mise en œuvre

Introduction

Notre travail consiste à créer des chemins virtuels, et de relier un ou plusieurs sites distants entre eux à travers un réseau public en sécurisant les communications avec la solution VPN IPSec et VPN IPSec/L2TP sous Windows server 2003, ce dernier est pris comme un noyau réseau de chaque site de l'entreprise INERGA.

1. Présentation de l'environnement

Dans notre travail nous avons eu recours à Windows server 2003 comme un environnement de travail.

1.1. Windows server 2003

Windows Server 2003 est un système d'exploitation orienté serveur développé par Microsoft. Présenté le 24 avril 2003 comme le successeur de Windows Server 2000, il est considéré par Microsoft comme étant la pierre angulaire de la ligne de produits serveurs professionnels Windows Server System. Une version évoluée intitulée Windows Server 2003 R2 a été finalisée le 6 décembre 2005. Son successeur, Windows Server 2008 est sorti le 4 février 2008.

Parmi les produits de la famille Windows 2003, il existe quatre systèmes d'exploitation : Windows 2003 Web, Windows 2003 Standard, Windows 2003 Enterprise et Windows 2003 Datacenter.

Dans notre travail nous avons utilisé le Windows server 2003 Enterprise.

Les différents serveurs de Windows server 2003

La famille Windows Server 2003 fournit plusieurs rôles de serveur :

Serveur de fichiers, Serveurs d'impression, Serveurs d'applications, Serveurs de messagerie, Serveurs Terminal Server, Serveurs d'accès distant/VPN, Serveur DNS, Serveurs DHCP, Serveurs multimédia par flux et Serveur WINS.

Dans notre travail nous nous sommes basés sur les deux serveurs suivants :

Serveurs d'accès distant/VPN

Le service Routage et accès distant fournit un routeur logiciel complet ainsi qu'une connectivité d'accès à distance et VPN (Virtual Private Network) pour les ordinateurs distants. Il offre des services de routage aux environnements de réseau local (LAN, Local Area Network) et de réseau étendu (WAN, Wide Area Network). Il permet également aux utilisateurs distants ou mobiles d'accéder au réseau d'entreprise comme s'ils étaient directement connectés, par des services de connexion d'accès à distance ou par Internet en utilisant des connexions VPN. Si nous envisagions de connecter des utilisateurs distants à des réseaux d'entreprise, nous devons configurer ce serveur comme un serveur d'accès distant/VPN.

Les connexions d'accès distant activent tous les services habituellement à la disposition d'un utilisateur connecté au réseau local, y compris le partage des fichiers et des imprimantes, l'accès au serveur Web et la messagerie.

Après avoir configuré le rôle du serveur d'accès distant/VPN, nous pouvons exécuter les tâches suivantes :

- Contrôler comment et quand les utilisateurs distants accèdent à notre réseau.
- Fournir des services de traduction des adresses réseau aux ordinateurs de notre réseau.
- Créer des solutions réseau personnalisées à l'aide d'interfaces de programmation d'applications (API, Application Programming Interface).

Contrôleur de domaine (Active derectory):

Les contrôleurs de domaine stockent les données de l'annuaire et gèrent les communications entre les utilisateurs et les domaines, y compris les processus d'ouverture de session d'utilisateur, l'authentification et les recherches d'annuaire.

Active Directory est une base d'annuaire qui regroupe tous les objets réseaux permettant une administration simplifiée et une forte tolérance de panne.

Active Directory s'appuie sur un ensemble de protocoles standards qui rendent cette base d'annuaire un composant réseau sur lequel toutes les applications peuvent s'appuyer.

Remarques

- nous ne pouvons pas ajouter le rôle de contrôleur de domaine à une Autorité de certification (CA) si notre ordinateur dispose déjà d'une Autorité de certification,

Après avoir configuré le rôle du contrôleur de domaine, nous pouvons exécuter les tâches suivantes :

- Stocker les données d'annuaire et les mettre à la disposition des utilisateurs et des administrateurs du réseau. Active Directory stocke des informations sur les comptes d'utilisateurs (par exemple, les

noms, les mots de passe, les numéros de téléphone, etc.) et permet à d'autres utilisateurs autorisés du même réseau d'accéder à ces informations.

- Ajouter des contrôleurs de domaine supplémentaires à un domaine existant pour améliorer la disponibilité et la fiabilité des services réseau.
- Améliorer les performances du réseau entre les sites en plaçant un contrôleur de domaine dans chaque site. Avec un contrôleur de domaine dans chaque site, vous pouvez gérer les processus d'ouverture de session des clients dans le site sans utiliser la connexion réseau plus lente entre les sites.

1.2. Caractéristiques d'IPSec de Windows server 2003

- Un composant logiciel enfichable Moniteur de sécurité IP .
- Une clé principale de cryptage plus forte, Diffie-Hellman 2048 bits.
- L'outil de gestion de ligne de commande Netsh apporte la facilité d'utilisation.
- Seul le trafic IKE (Internet Key Exchange) échappe aux filtres de trafic. Cette restriction est indispensable pour autoriser l'établissement de communication sécurisées .
- Certaines restrictions déterminent quels ordinateurs sont autorisés à se connecter par domaine, par origine de certificats ou par groupe d'ordinateur.
- La fonctionnalité IPSec par-dessus NAT permet aux paquets ESP de passer par la traduction NAT autorisant le trafic IPSec.
- L'intégration avec l'équilibrage de charge réseau NLB est améliorée ce qui facilite l'équilibrage de charge pour des services VPN fondés sur IPSec.
- Le composant logiciel enfichable jeu de stratégie résultat est pris en charge pour les affectations de la stratégie IPSec existante.( )

2. Partie réalisation

Dans notre cas pratique nous avons pris le serveur de la direction centrale comme exemple d'application, nous avons suivi les étapes suivantes :

- Installation de serveur RRAS ;
- Installation de CA ;
- Création d'une stratégie IPSec/L2TP pour accès VPN distant ;
- Test et résultat ;
- Création d'une stratégie IPSec en mode tunnel ;
- Visualisation des résultats.

2.1. Installation de Serveur RRAS (Routing and Remote Acces Server)

Ce serveur gère le routage interne, vers le réseau Internet et les connexions à distances des utilisateurs :

1. A partir de la console « Manage your Server », nous sélectionnons RRAS puis Suivant, dans la page configuration, en choisissant Personnalisé puis Suivant. Ensuite nous Sélectionnons rôles routeur et VPN accès (comme le montre la figure ci-après), puis Terminer.

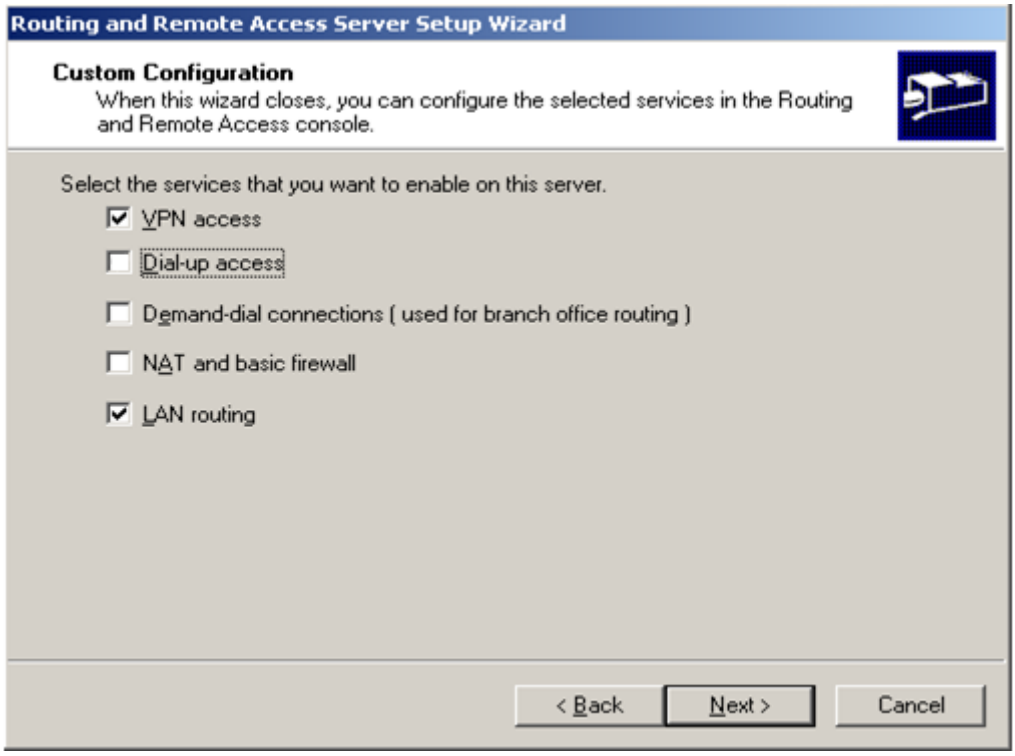


Figure 33 Rôles de RRAS

2. Windows 2003 permet d'accepter jusqu'à 1000 tunnels PPTP et 1000 tunnels L2TP simultanément, par défaut, 5 ports sont activés, et nous pouvons Augmenter ce nombre jusqu'à 100 (voir l'annexe).

2.2. Installation de la CA

Attribut des certificats aux utilisateurs pour l'authentification interne et à distant

1. A partir de panneau de configuration nous cliquons sur Ajout/Suppression de programmes, puis sur Ajout ou Supprimer des composants Windows. Ensuite, nous cliquons sur services de

certificats, puis sur Suivant. Rôle CA principale de l'entreprise. Nous introduisons les informations d'identité de CA (figure34) puis Terminer (voir l'annexe pour plus de détails).

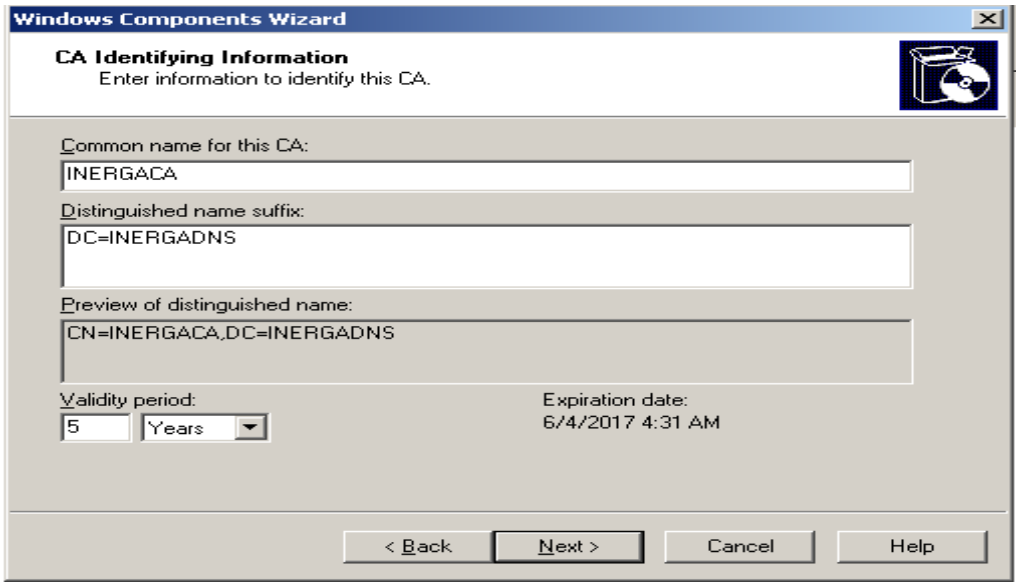


Figure 34 Informations d'identité de CA.

2.3. Création d'une stratégie IPSec/L2TP pour accès VPN distant

2.3.1. Créations de groupe d'accès

Pour regrouper les utilisateurs ayant le droit d'accès à distance, Windows 2003 définit une Organisation Unit (OU) qui repend aux besoins. Les utilisateurs sont ajoutés par l'administrateur.

Dans la console Active Directory, nous créons un groupe nommé « VPNACCESBlida ». Les membres obtiennent des certificats IPSec automatiquement comme l'illustre la figure ci-aprés :

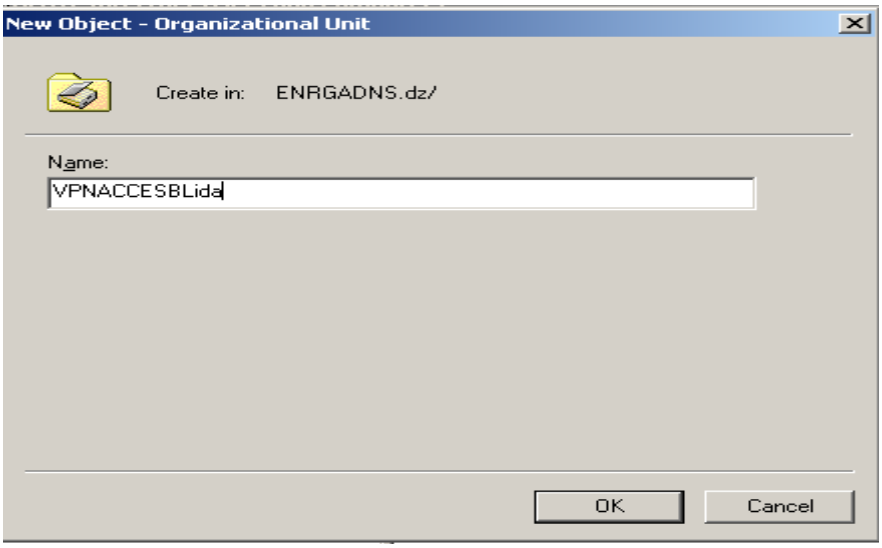


Figure 35 Ajout d'une Unité d'Organisation.

2.3.2. Création de stratégie IPSec en monde transport :

Cette stratégie a pour but d'assurer la confidentialité et l'intégrité des données pour l'accès VPN post à site.

1. Dans la console MMC (politique de sécurité de groupe), un clic droit sur « stratégie de sécurité IP », nous sélectionnons « créer une stratégie de sécurité IP ».
2. Comme méthode d'authentification, nous sélectionnons par certificat émis par CA principale d'entreprise (figure 36).

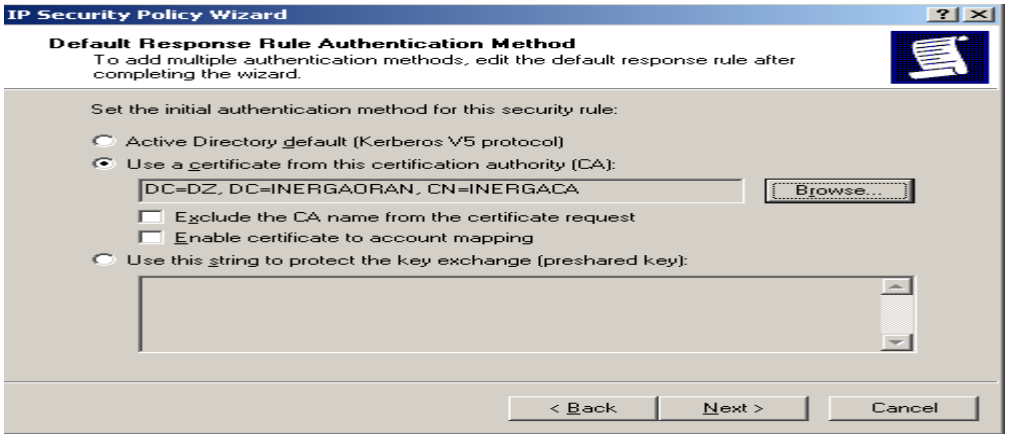


Figure 36 Méthode d'authentification

3. Dans la page liste des filtre IP, nous sélectionnons le filtre « All trafic IP », puis nous modifions les paramètres de filtre : l'adresse source (adresse de serveur), adresse destination (ALL), protocoles (Any). nous cochons sur « miroir. Faire coïncider les paquets possédant des adresses sources et de destination exactement opposées » pour éviter l'attaque déni de service.

4. Action de Filtre : nous sélectionnons l'option « Négocie la sécurité », pour la Sécurité de trafic IP, et l'option Personnalisé, en choisissant les Méthodes de sécurité (AH, ESP). nous cochons les cases « générer une nouvelle clé tous les 100000 Ko » et « générer une nouvelle clé toutes les 3600 sec (fréquence de changement de la clé de mode rapide)(figure 37).

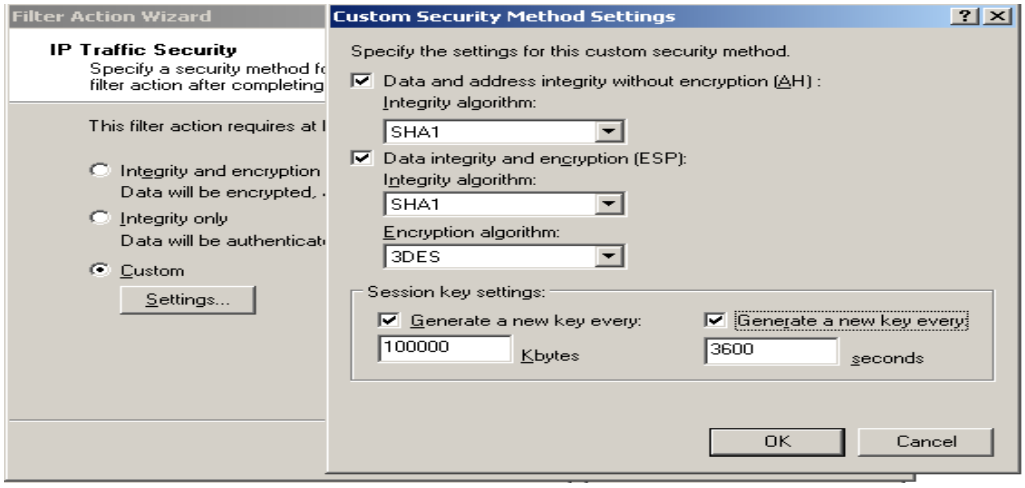


Figure 37 Méthode de sécurité de trafic IP.

5. Pour les méthodes de sécurité IKE, nous choisissons : SHA1 pour l'intégrité et 3DES pour le cryptage, un Groupe Diffie-Hellman pour la génération des clés (figure 38).

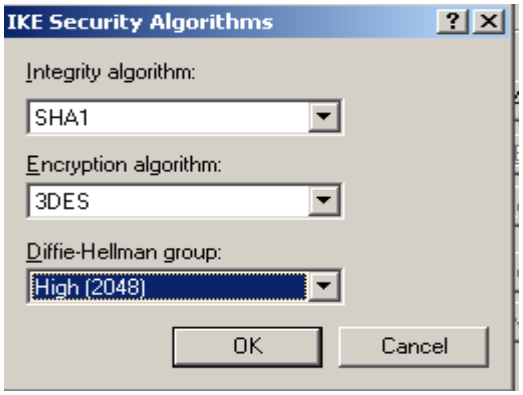


Figure 38 paramètres d'échange de clés

6. Attribution de cette stratégie, nous modifions la stratégie de groupe par défaut.

2.3.3. Création de stratégie d'accès distant :

Cette stratégie a pour but l'établissement des tunnels L2TP (niveau 2).

1. Dans la console RRAS clic droit sur « stratégie d'accès distant » puis nouvelle stratégie d'accès distant. Nous donnons le nom « VPN L2TP>IPSec » comme méthode d'accès « VPN », en autorisant l'accès pour le groupe créé précédemment (VPNACCESBlida), MS-

CHAPv2 comme protocole d'authentification et cryptage maximal (IPSec triple DES ou MPPE 128 bits).Enfin l'ajout un attribut « tunnel type » en choisissant « L2TP ». nous validons la configuration et l'attribution de la stratégie en changent son rang à 1.

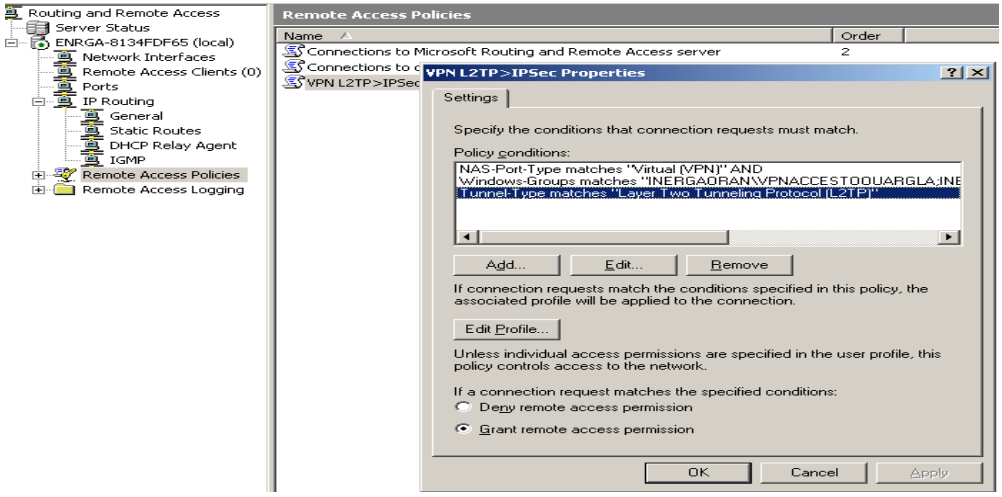


Figure 39 Propriétés de stratégie d'accès distant

2.3.4. Test et résultats

Sur la machine cliente distant après avoir importé la stratégie IPSec (auprès de serveur) et l'activé, nous créons une nouvelle connexion «connexion au réseau d'entreprise » : de type connexion réseau privé virtuel (VPN), Nommé (INERGABLIDA), puis nous introduisons l'adresse IP publique de serveur pour la demande de connexion distante. Dans l'anglet Propriétés de la connexion et dans l'onglet « gestion réseau », nous choisissons le type de réseau VPN soit : « VPN L2TP IPSec ». En saisissant le nom d'utilisateur et le mot de passe puis connecter.

La figure ci-après montre les résultats de la stratégie d'accès distant (activations de protocole tunneling L2TP et les protocoles IPSec) en niveau client :

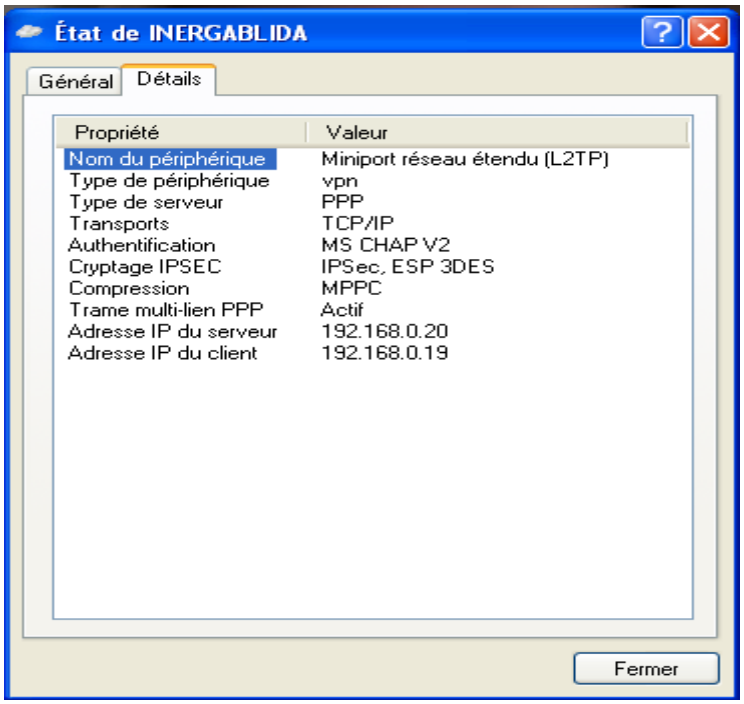


Figure 40 Etat de connexion

Nous testons la connexion (PING) après l'activation de la stratégie au niveau client, la figure ci-dessous montre le test de connexion vers le serveur : la connexion passe par la phase de négociation des paramètres de sécurité, une fois les paramètres sont acceptés mutuellement la connexion sera établie.

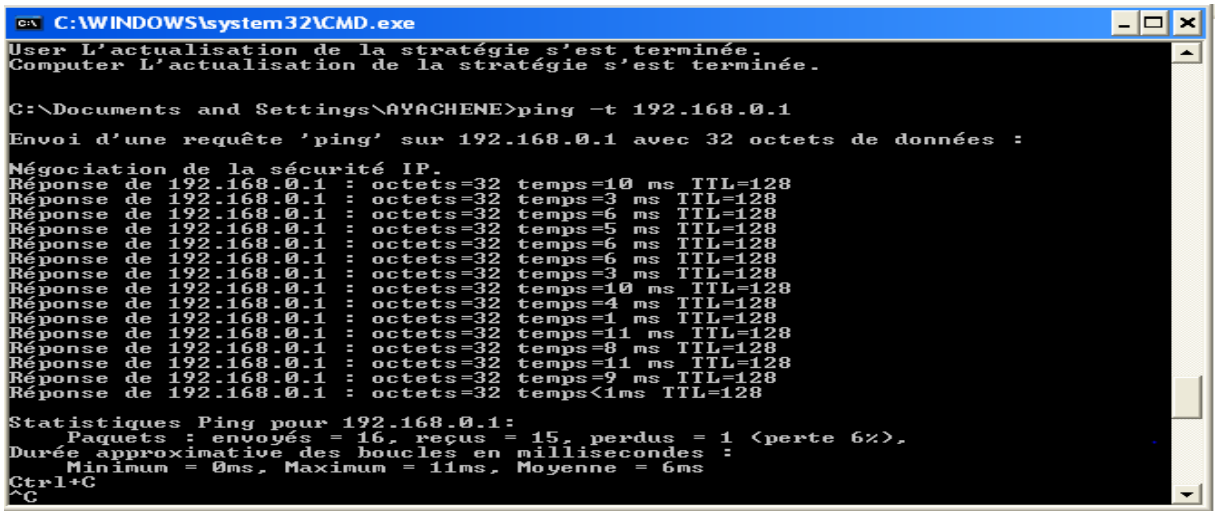


Figure 41 Test de connexion vers le serveur

L'analyse réseau au niveau serveur, comme la montre la figure ci-après, nous remarquons que le trafic IP est traité par la stratégie IPSec en appliquant les protocoles AH et ESP.

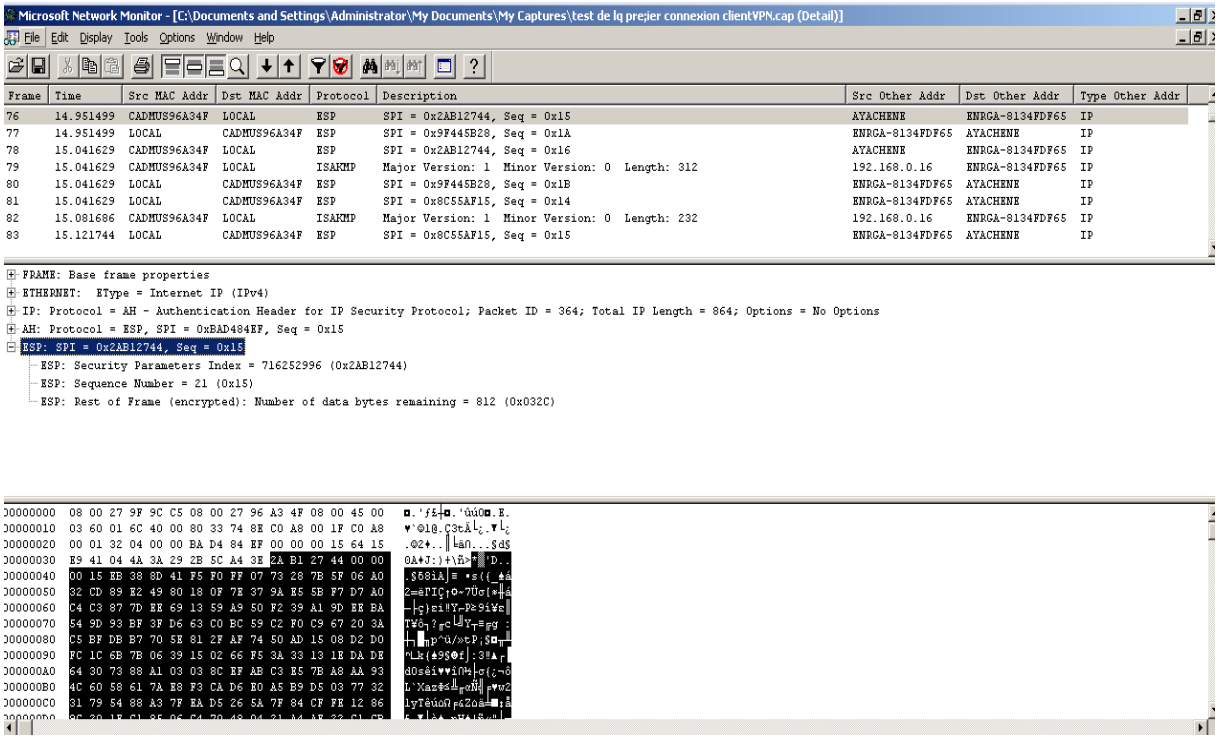


Figure 42 Capteur réseau de trafic IPSec.

3. Création d'une stratégie IPSec en mode tunnel

Cette stratégie a pour but de créer des connexions VPN site à site IPSec (de niveau 3)

1. Sur la console Gestion de la configuration de sécurité, clic droit sur Stratégie de sécurité IP sur Active Directory et Ordinateur local, nous sélectionnons Créer une stratégie de sécurité IP.
2. Méthodes de sécurité d'échanges de clés IKE : algorithme d'intégrité SHA1, et Algorithme de cryptage 3DES, puis Group Diffie-Helman Haute 2048.
3. Nous Définissons le point de sortie de tunnel : l'adresse IP de serveur destination (figure 43).

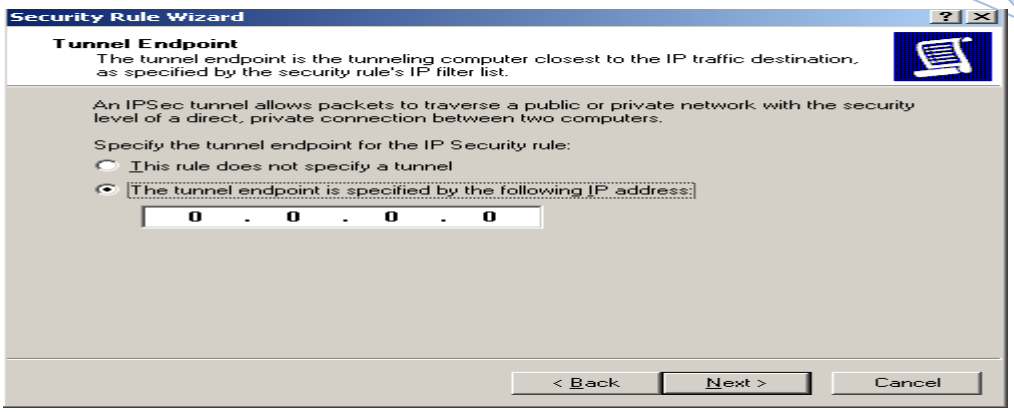


Figure 43 Spécification de tunnel.

4. Filtre IP : Comme source du trafic IP, nous spécifions la plage d'adresses de réseau local Dans la plage Destination du trafic IP adresses de réseau d'Oran et protocole IP, en sélectionnant Any.
5. Action de filtre IP : nous choisissons « Négocie la sécurité » , pour la Sécurité de trafic IP nous choisissons les algorithmes AH (SHA1) pour l'intégrité et ESP (SHA1 et 3DES) pour l'intégrité et le cryptage. Les paramètres de renouvellement des clés (chaque 1H ou 100000 KB).
6. Comme méthode d'authentification nous choisissons par certificat délivrées par la CA principale de l'entreprise. Terminer puis l'activation de la stratégie.

La figure suivante montre les propriétés de la stratégie IPSec :

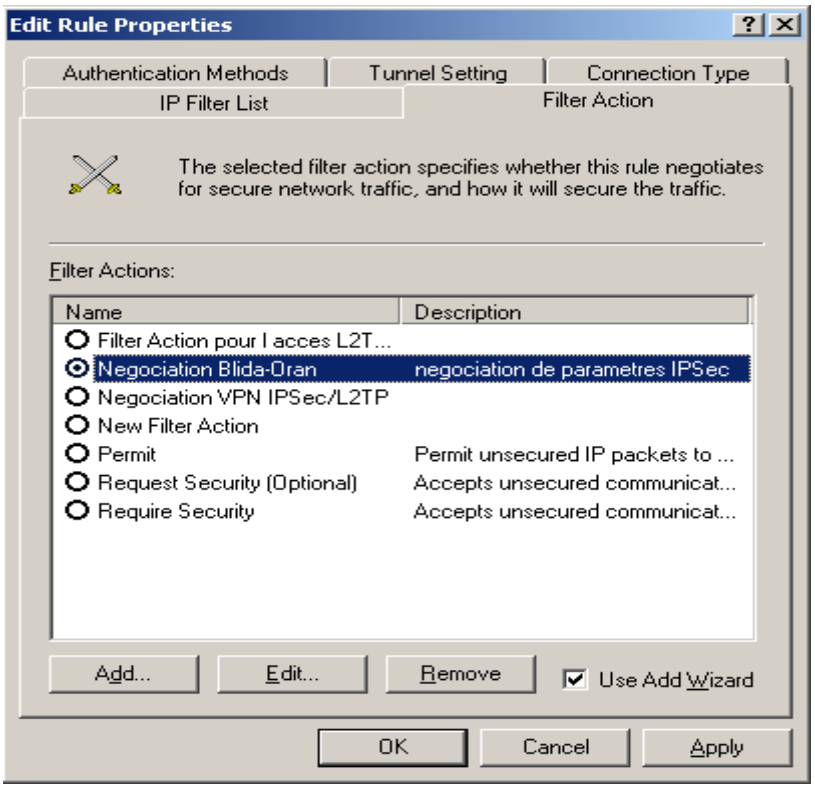


Figure 44 Propriétés de la Stratégie de sécurité IP.

3.1. Visualiser les résultats d'une stratégie

Prenant comme exemple le serveur de Blida vers le serveur d'Oran.

Nous pouvons visualiser les résultats de notre stratégie, en utilisant le composant logiciel enfichable Moniteur de sécurité IP. Nous développons le nœud du serveur, puis le nœud Mode rapide ou Mode principal, et nous sélectionnons le nœud Statistiques. Les deux tableaux dans l'annexe décrivent la signification des statistiques les plus courantes du mode principal et de mode rapide.

3.1.1. Résultats de test « Mode principale » sous Moniteur de sécurité IP

Les deux figures suivantes affichent les résultats de deux tests en mode principale sous moniteur IPSec et Netsh qui résultent les statistiques de mode principale (tableau n°1 de l'annexe).

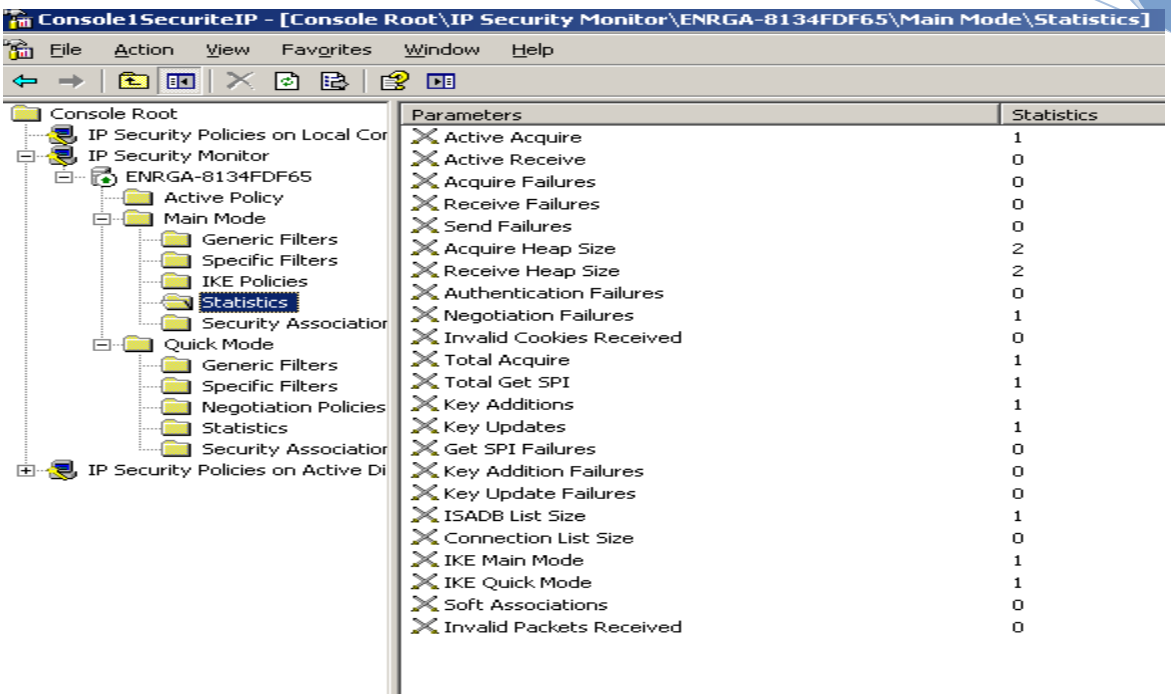


Figure 45 Statistiques de Mode principal.

Sous Netsh :

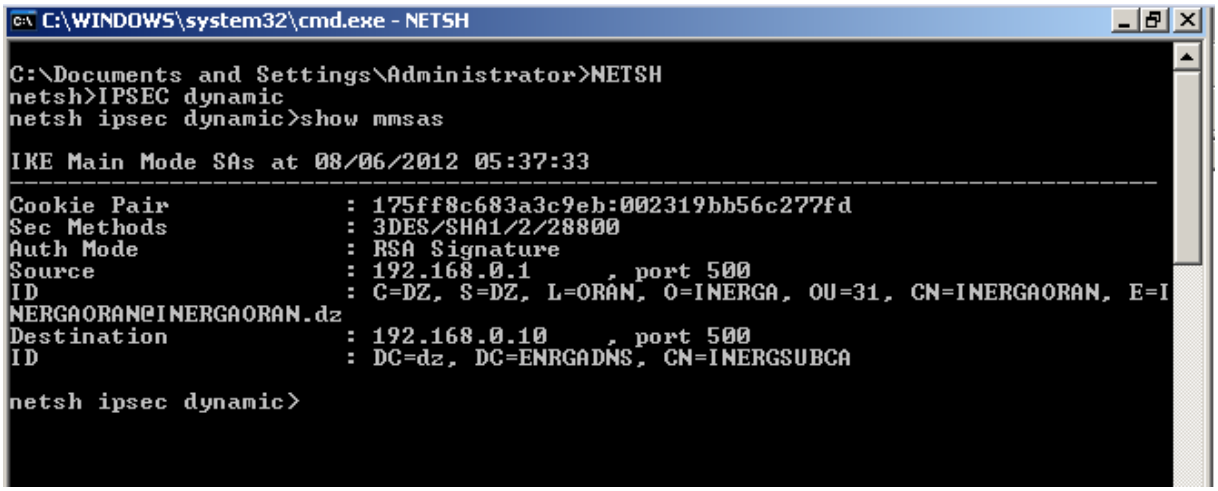


Figure 46 Résultats de mode principal sous Netsh.

3.1.2. Résultats de mode rapide

Les résultats de mode rapide sont affichés dans les figures ci-après :

La politique de sécurité est activée et les paramètres de SA est établie (figure 47).

Les statistiques de mode rapide (figure 48, tableau n°2 de l'annexe).

Sous Netsh :

```
Quick Mode SAs
--------------

Transport Filter

Policy Name             : Negociation Blida-Oran
Source Address          : 192.168.0.1
Destination Address     : 192.168.0.10
Protocol                : ANY
Source Port             : 0
Destination Port        : 0
Direction               : Outbound

Offer Used

  AH(b/r)   ESP Con(b/r) ESP Int  PFS DH Group
---------- ------------- -------  ------------
  None        3DES(24/0 )  SHA1     Medium (2)
SHA1(20/0 )   None         None     Medium (2)
netsh ipsec dynamic>_
```

Figure 47 Résultat Mode rapide sur Netsh.

Sous Moniteur de sécurité IP :

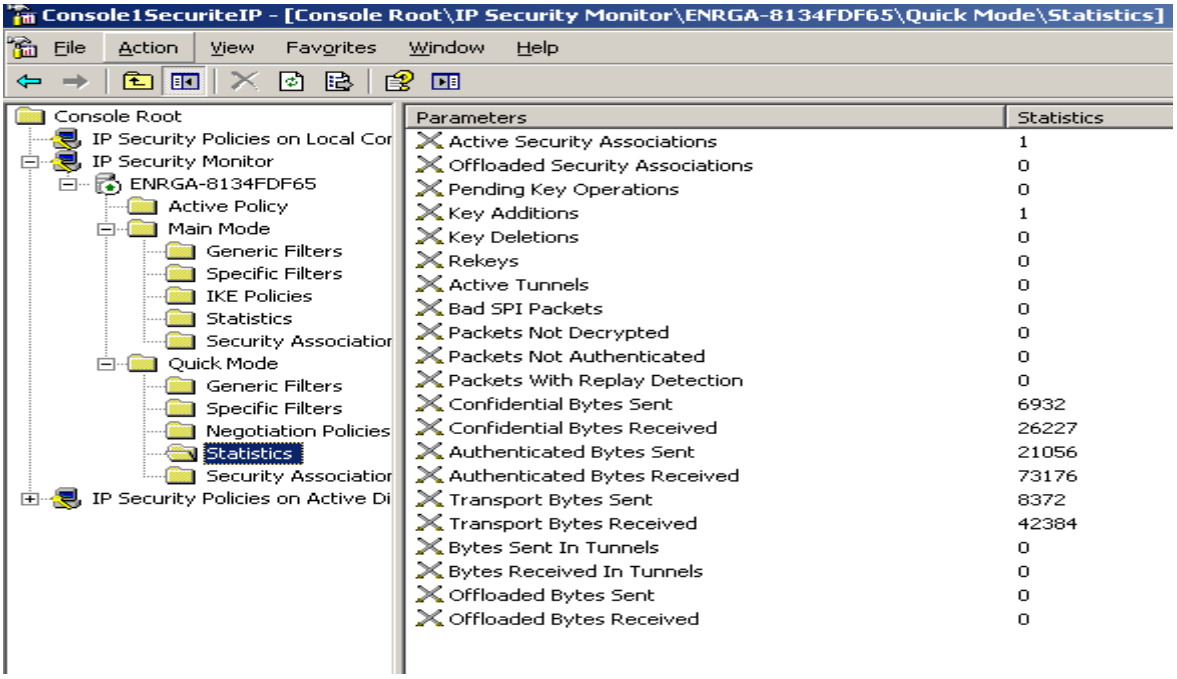


Figure 48 Résultats de mode rapide.

3.1.3. Résultats d'analyse de trafic IP

La figure suivante affiche les résultats d'application de protocole IPSec de trafic réseau sous moniteur réseau Windows :

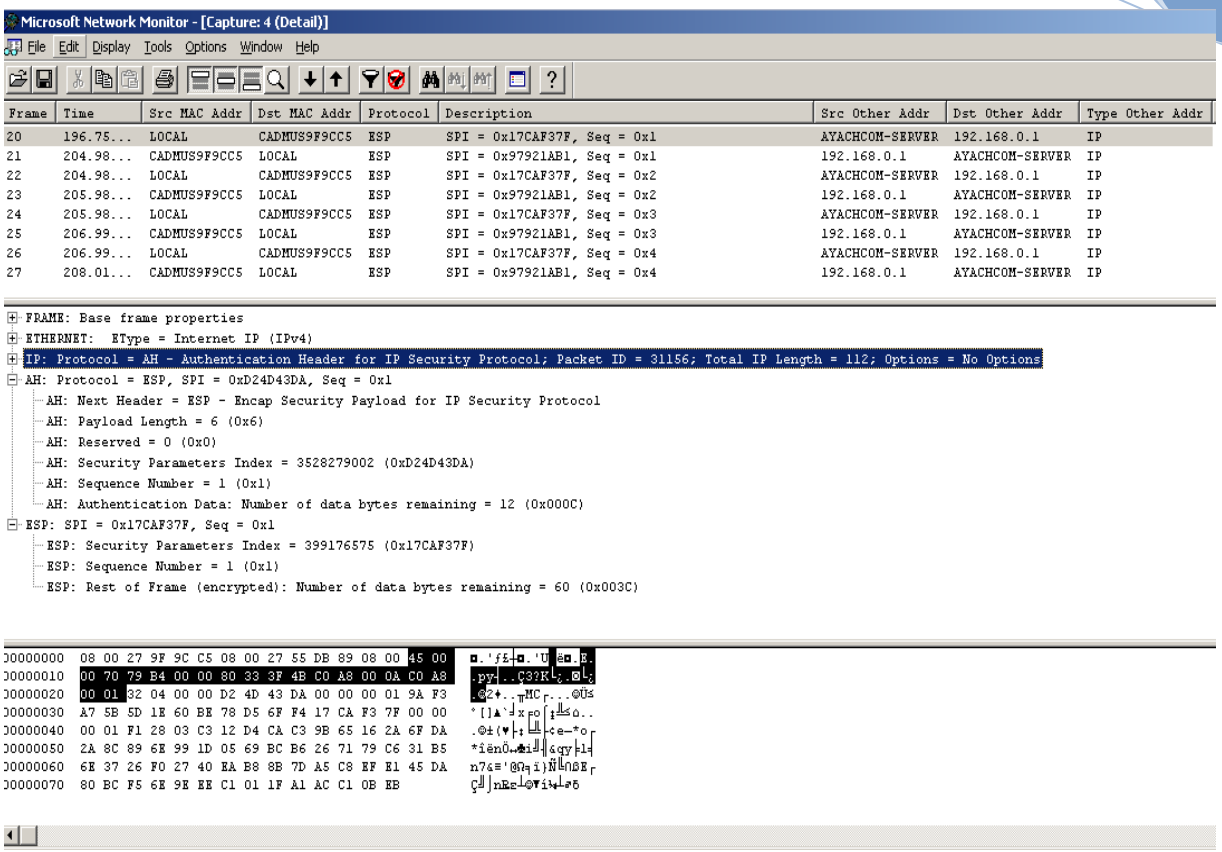


Figure 49 Capteur du trafic IP sous Moniteur réseau Windows.

Conclusion

A travers cette partie, nous avons montré les différentes étapes de mise en œuvre de deux solutions VPN: site à site et poste à site, en utilisant la stratégie IPSec en mode tunneling et IPSec en mode transport combiné avec L2TP respectivement, qui permettent d'une connexion sécurisée entre les différents sites d'INERGA, ainsi que l'accès à distance des utilisateurs nomades de ce groupe.

A l'aide de la gestion de la stratégie IP, le Moniteur d'IPSec et le Netch, nous ont permis de définir les stratégies IPSec et d'afficher les paramètres IPSec de mode principal (statique ou dynamique) et de mode rapide ainsi que les règles et les paramètres de configuration.

En outre, tous cela nous ont accordé la possibilité de découvrir une nouvelle technique dans le domaine de sécurité des réseaux.

Conclusion générale

Les VPN représentent une stratégie primordiale qui fournit l'un des mécanismes les plus utilisés dans le domaine de sécurité des réseaux, dont nous trouvons IPSec comme une solution la plus usée, qui permet de garantir les différents objectifs de sécurité, tel que l'authentification, la confidentialité et l'intégrité…etc.

En effet, nous avons tout au long de notre travail présenté, les différents concepts liés à la sécurité, ainsi que les protocoles les plus fréquents dans les VPN, dans le but de réaliser une solution VPN au sein d'une entreprise publique, après une large étude théorique concernant cette technologie ainsi que les protocoles les plus connus dans la littérature. Des lors, nous avons opté pour des protocoles prisent comme étant des modèles pour répondre à notre problématique qui consiste à montrer comment assurer la sécurité des échanges de données entre les trois sites et comment assurer un accès à distance sécurisé de chaque site pour ses utilisateurs nomades, qui sont :

- IPSec en mode tunnel qui garantie une interconnexion sécurisée entre les différents sites de l'entreprise.
- La combinaison de protocole IPSec en mode transport et le protocole de tunneling L2TP pour assurer des liaison sécurisées entre les utilisateurs nomades et leur entreprise.

Dans le but de réaliser notre projet, nous avons entamé par une étude théorique relative à l'architecture réseau de l'entreprise INERGA, en tenant en compte la proposition de leurs cadres dirigeants, qui est une phase très importante pour la réalisation de notre projet afin de structurer les étapes à suivre pour pouvoir implémenter la solution souhaitée.

Ce projet fait preuve d'une expérience professionnelle intéressante, qui nous a permis d'améliorer nos connaissances et nos compétences dans le domaine de la sécurité des réseaux.

Bibliographie

ARCHIER, J.-P. (2010). *« Les VPN : Fonctionnement, mise en œuvre et maintenance »* (éd. ENI). paris, 75, France: ENI.

C é d r i c L l o r e n s, L. a. (2006). *tableaux de bord de la sécurité réseau* (éd. 2édition). Paris, 75, France: eni.

CCNA, C. (2007-2008). CISCO Networking Academy. USA.

Denis de REYNAL, J.-G. d. (2004). *« Présentation sur les VPN »*. Paris: UFR Ingénieurs, France.

DOGDOIGNE, J. (Février 2011). *Réseaux informatiques Notions fondamentales* (éd. eni). Paris, 75, France: eni.

Ghernaouti-Hélie, S. (2003). *Sécurité informatique et réseaux.* Paris, 75, France: DUNDO.

GUERMAH, M. (2010). *« les réseaux privés virtuels : un accès sécurisé au réseau d'entreprise ».* BLIDA.: Société de SONALGAZ .

GUICHARD, I. P. (2005). *« Architecture MPLS/VPN »* (éd. Dunod, Vol. Volume 1). Paris, France: Dunod.

INERGA. (2007, Janvier). Consulté le Avril 2012, sur http://www.INERGA.com

Jean-Philippe, J.-F. P. (2009). *tout sur la sécurité informatique* (éd. DUNDO). Paris, 75, France: DUNDO.

LOUNIS, M. (2006, Juin). BACKBONE NATIONAL DE TRANSMISSION NUMERIQUE SUR CABLE FIBRE OPTIQUE ET FAISEAU HERTZIEN D 'ALGERIE TELECOM. *Algérie Telecom* , p. 23.

MOGHRANI, L. M. (2011). *implémentation d'un système de communication de groupe sécurisé sur un VPN*. Bejaia: Université de Bejaia.

MONTAGNIER, J.-L. (2006). *Réseau de l'entreprise par la pratique.* Paris, 75, France: EYROLLES.

MONTAGNIER, J.-L. (2007). *Réseaux d'entreprise par la pratique* (éd. EYROLLES). Paris, 75, France: EYROLLES.

OPPLIGER, R. (2008). *« SSL and TLS - Theory and Practice »*. Paris: Artech House.

Pujolle, G. (2008). *Les réseaux* (éd. EYROLLES). Paris, 75, France: EYROLLES.

Quidelleur, S. L. (2010). *Les Réseaux Internet Des Services aux infrastructure* (éd. DUNDO). Paris, 75, France: DUNDO.

Rafael CORVALAN, E. C. (2003). *« Les VPN : principes, conception et déploiement des RPV »* (éd. édition Dunod). Paris, 75, France: Dunod

Annexes

1. Dans la fenêtre Propriétés de ports, on sélectionne le port puis Configure, dans la boite de dialogue on augmente le nombre maximum de ports (max 1000).

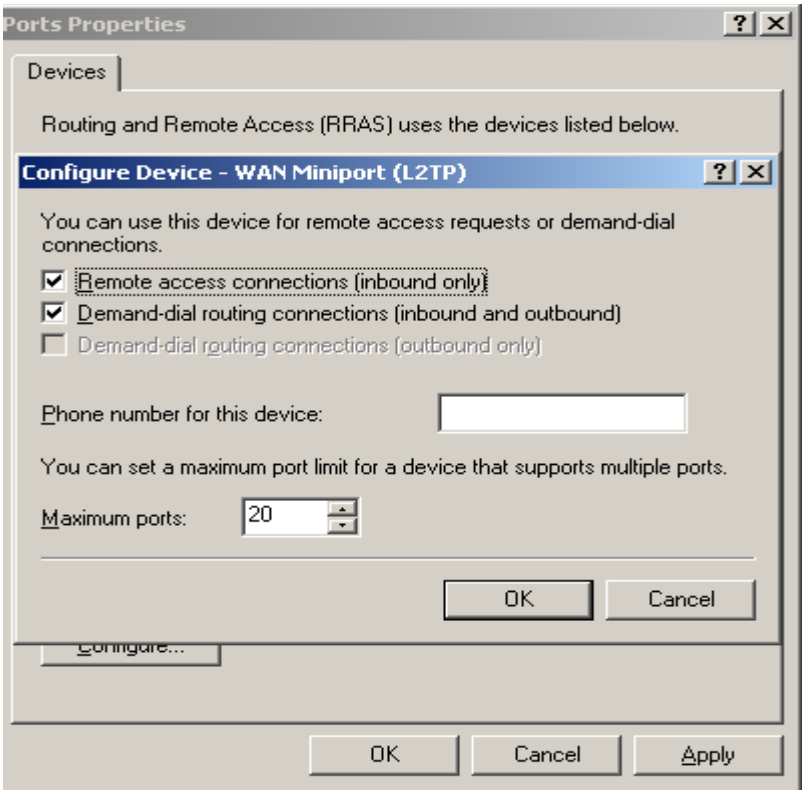


Figure1 gestion de port L2TP.

Installation de la CA.

Etapes d'installation d'une Autorité racine d'entreprise

1. A partir de panneau de configuration cliquer sur Ajout/Suppression de programmes, puis cliquer sur Ajout ou Supprimer des composants Windows.
1. Cliquer sur services de certificats, puis sur Détails. La boîte de dialogue Services de certificats apparaît.

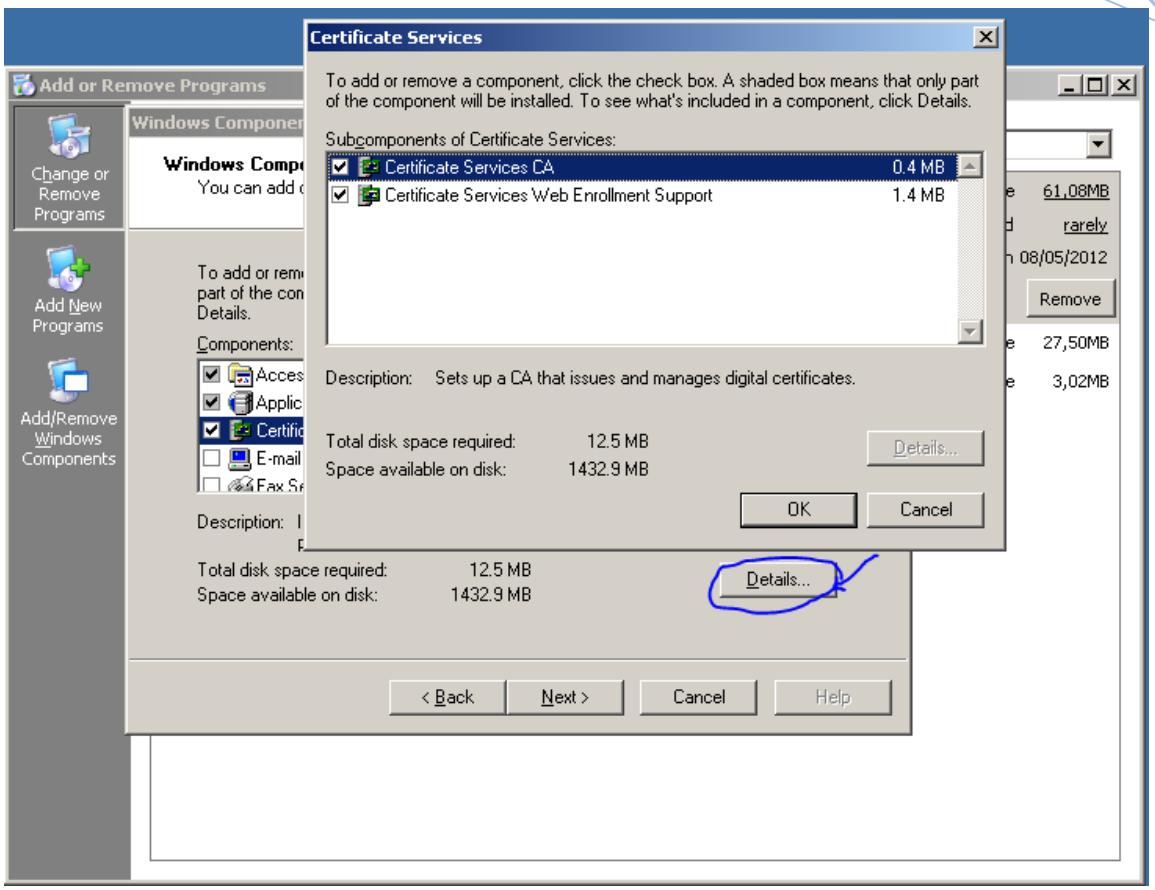


Figure2 Service de certification.

2. Cocher les deux cases proposées, puis cliquer sur OK. Apparaît une boîte de message Services de certificats Microsoft qui signale que, lorsque l'installation des services de certificats est faite, on ne peut plus modifier le nom de l'ordinateur, ni son appartenance de domaine, sans affecter les fonctionnalités de la CA. Puis cliquer sur Oui pour continuer.

3. Cliquer sur OK dans la boîte de dialogue Services de certificats.

4. Dans l'assistant Composants de Windows, cliquer sur Suivant. Apparaît la plage Type d'autorité de certification.

5. Cocher l'option Autorité racine d'entreprise et l'option utiliser les paramètres personnalisés pour générer la paire de clés et le certificat de l'autorité de certification, puis Suivant. Apparaît la plage d'information d'identification de l'autorité de certification.

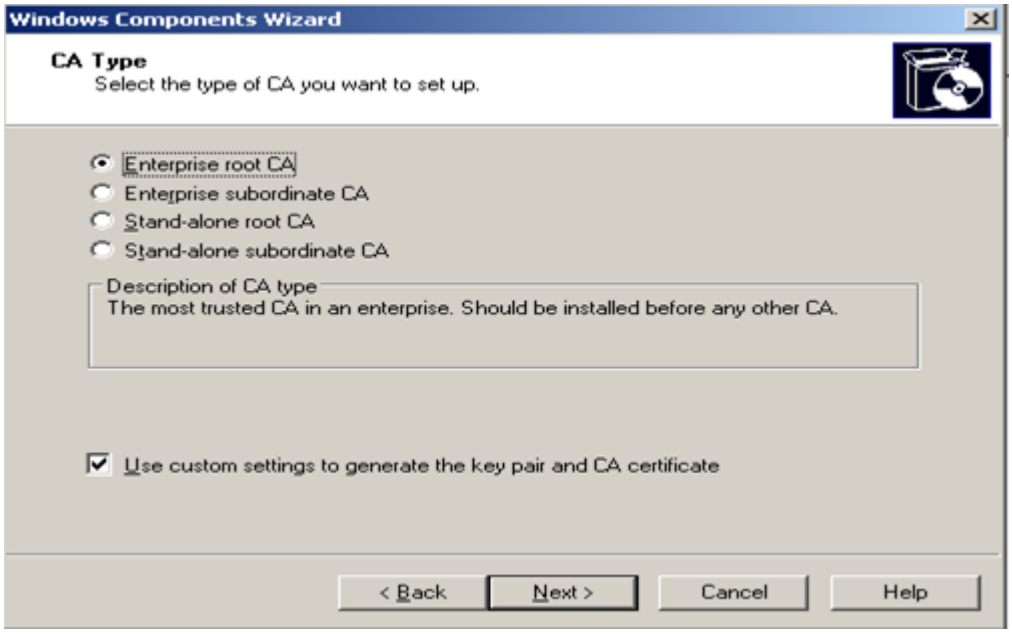


Figure 3 Type de CA.

6. Introduire ensuite les informations d'identification du CA : Le nom commun de cette autorité de certification Ex : « INERGACA » (c'est le nom d'hôte du contrôleur de domaine) et la durée de validité pour les certificats délivrés. Ex : 5 ans.

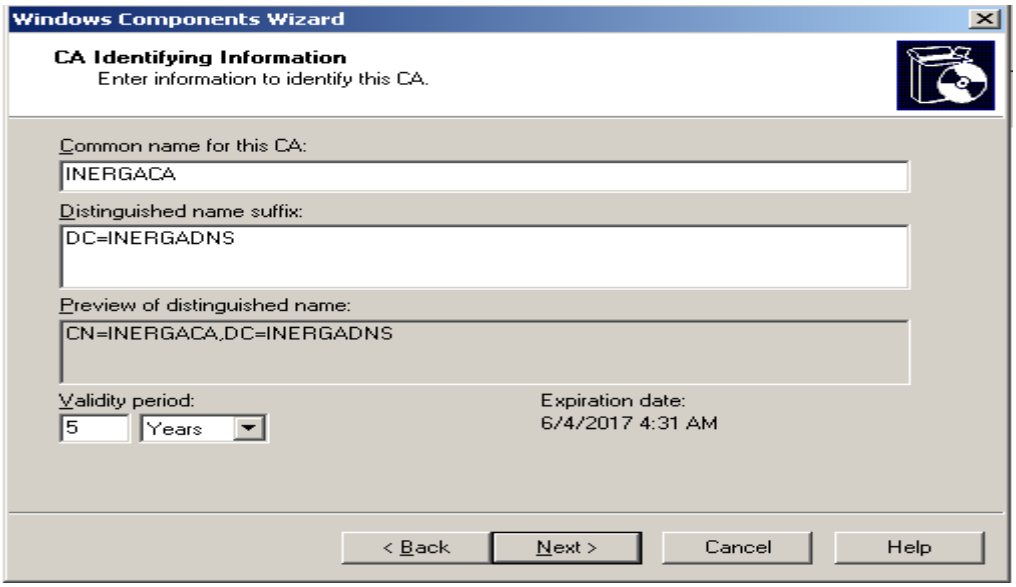


Figure 4 Informations d'identité de CA.

7. Indiquer l'emplacement du stockage de la base de données de certificats et du journal.

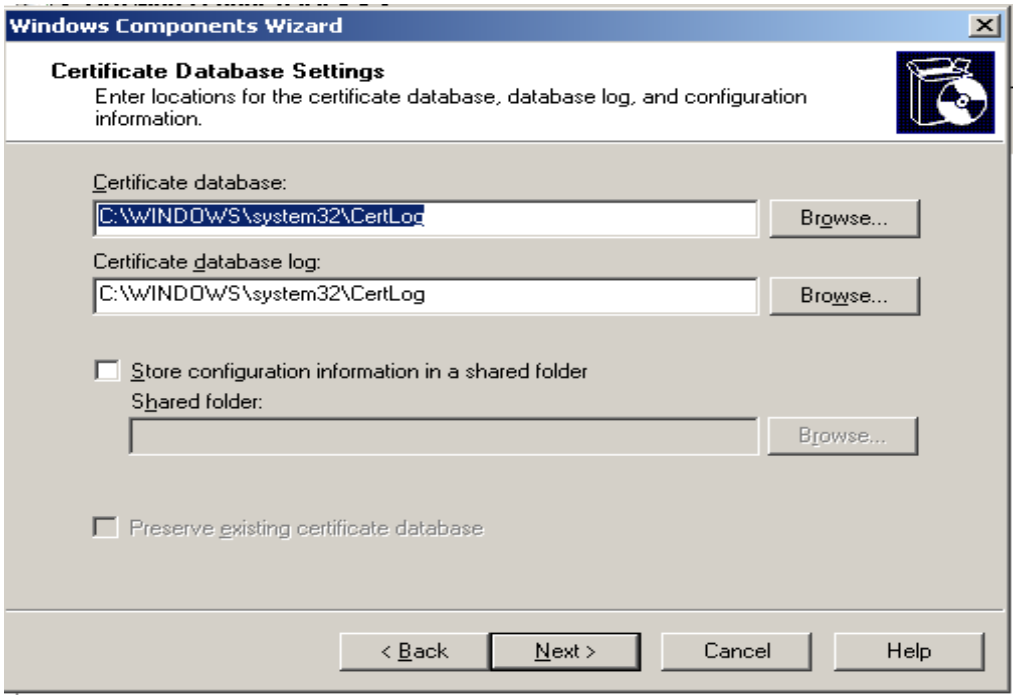


Figure 5 Stockage de base de données de CA.

8. Installation terminé.

NB : Dans le cas d'une CA subordonnée, on sélectionne dans l'étape 6 « CA subordonnée » puis on choisie demander un certificat de délégation auprès de CA racine de l'entreprise.

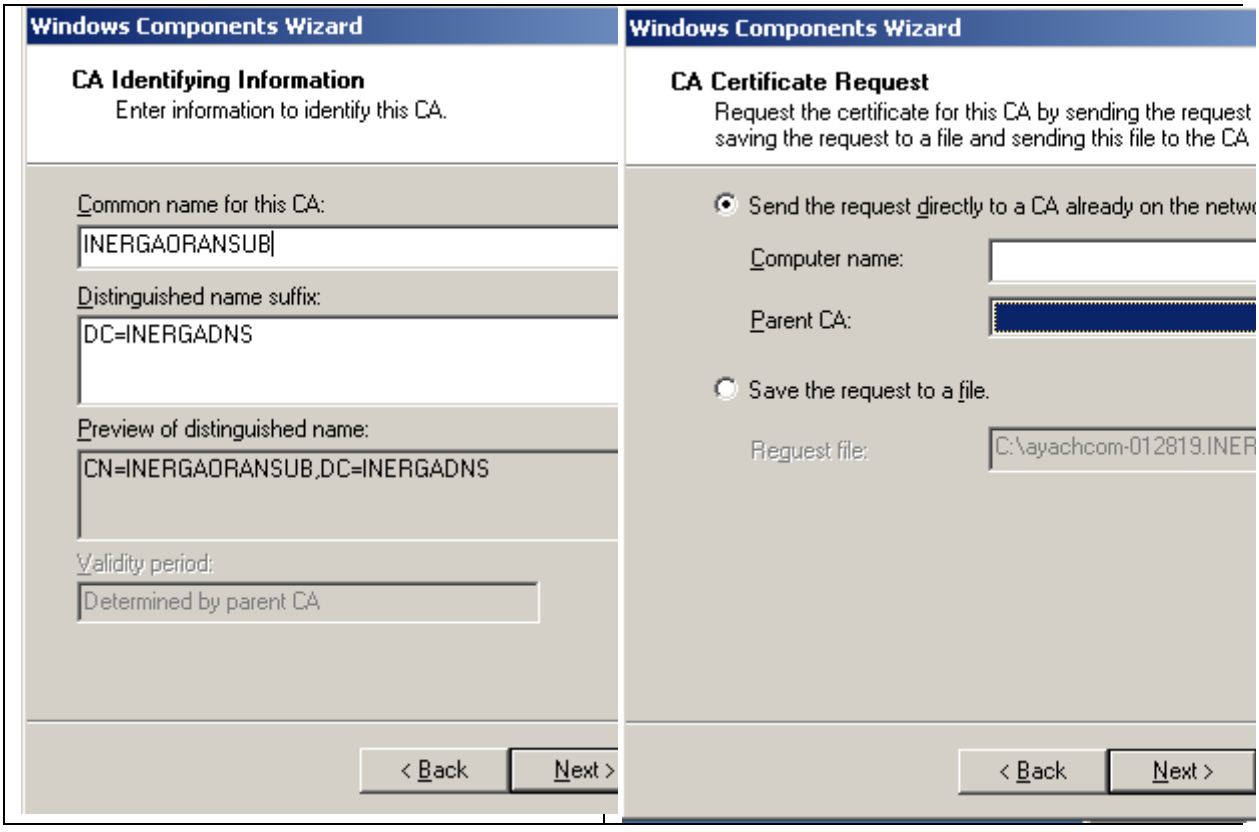


Figure 6 Identité de CA subordonnée et demande de son certificat de délégation.

Figure 6 console MMC de CA.

9. Accès au page web de CA.

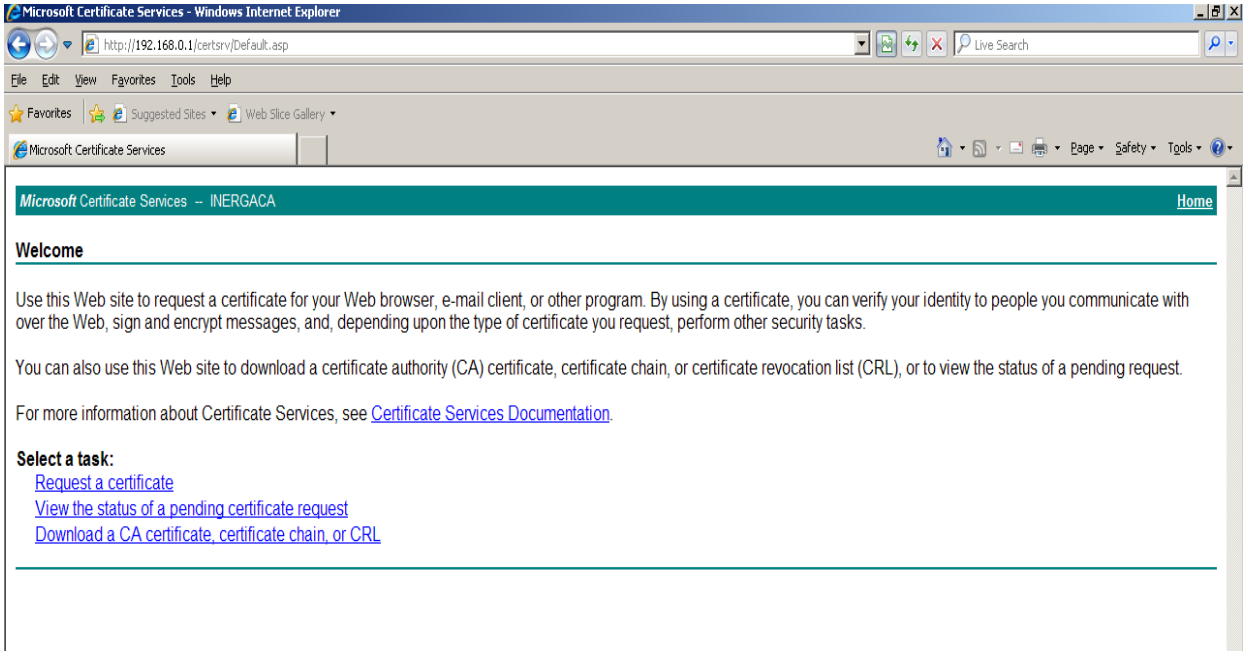


Figure 7 Page d'accueil de la CA principale.

10. certificat de la CA.

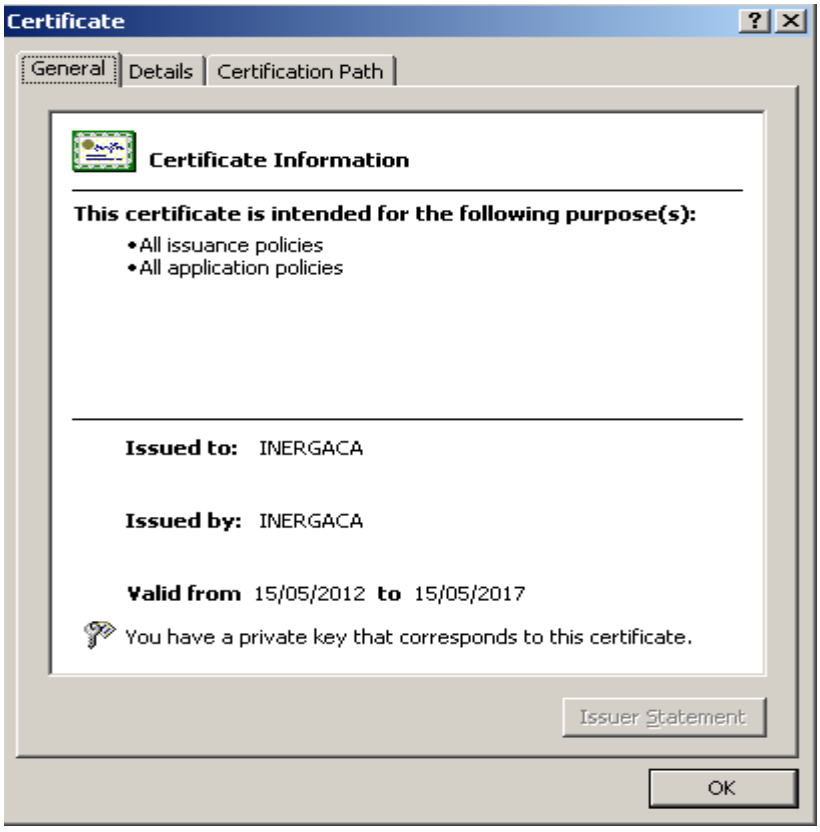


Figure 8 CA certificat.

11. Demande d'un certificat IPSec par web.

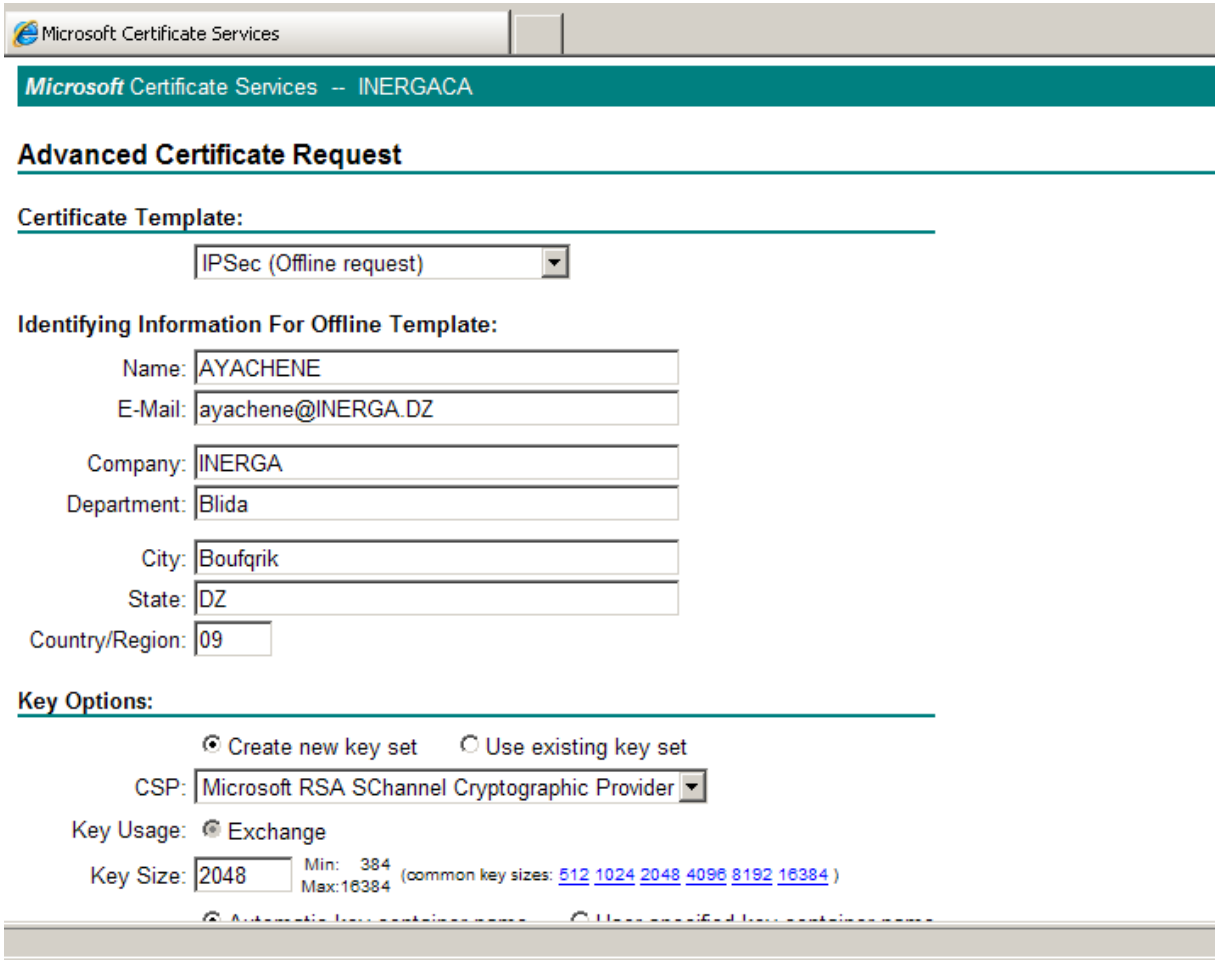


Figure 9 page web de CA pour la demande de certificat.

Création d'une stratégie IPSec/L2TP pour accès VPN distant

Demande automatique de certificat

1. Sous « configuration ordinateur/paramètres Windows/paramètres de sécurité/stratégie de clé publique/paramètres de demande automatique de certificat » Clic droit puis « nouveau » puis « demande automatique de certificat »

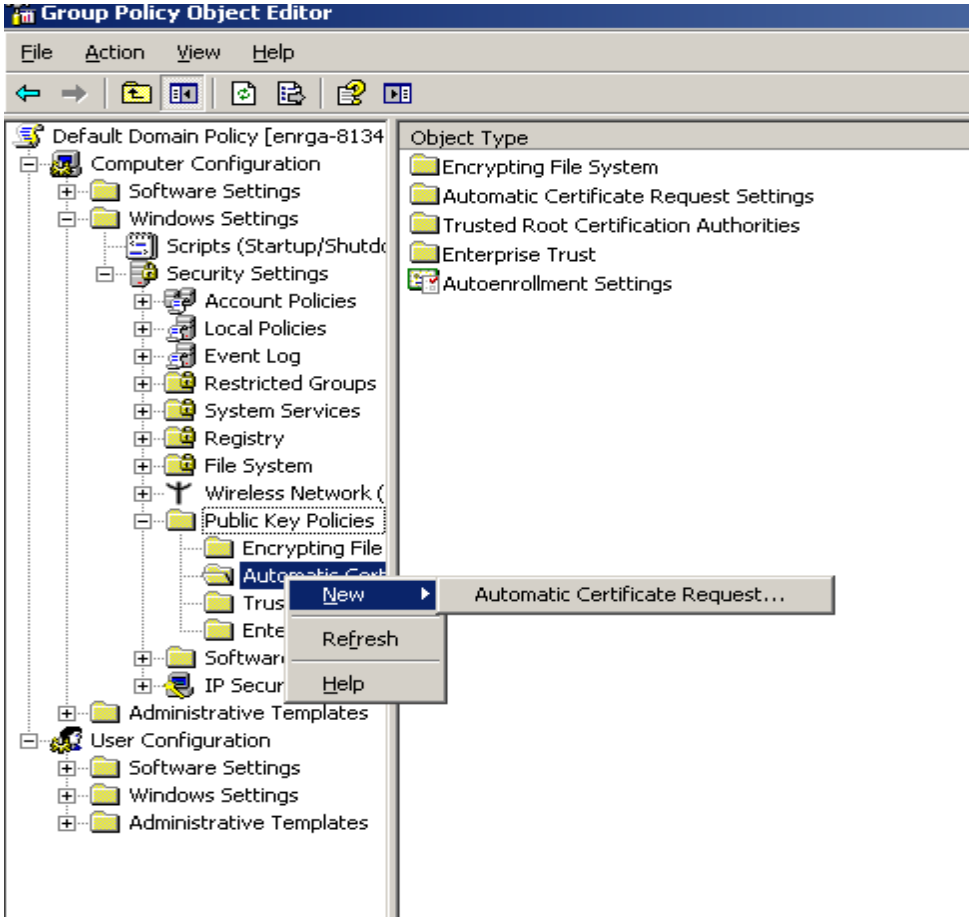


Figure 10 Configuration de demande automatique de certificat.

2. Choisissant le type « Ordinateur » puis Suivant et Terminer. Refaire la procédure pour le type « IPSec ».

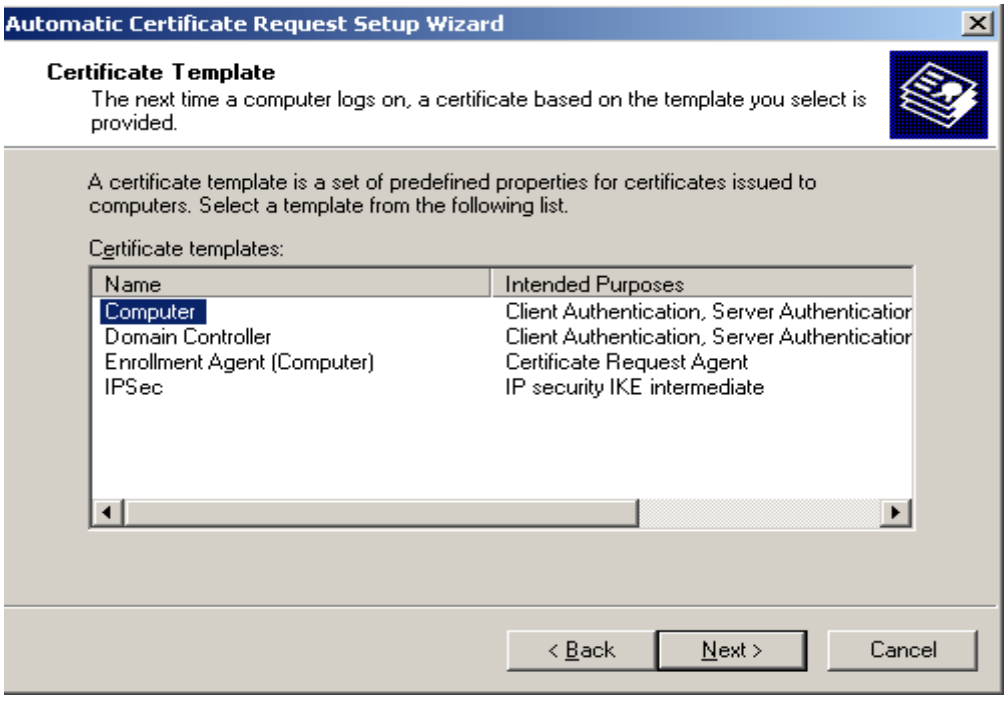


Figure 11 Types de certificats.

3. Sous « configuration ordinateur/paramètres Windows/paramètres de sécurité/stratégie de clé publique/paramètres d'inscription automatique »,clic droit sur « propriétés de demande automatique de certificat » puis propriétés. Cocher « inscrire les certificats automatiquement » et « renouveler les certificats expirés, mettre à jour les certificats en attente, et supprimer les certificats révoqués » puis « mettre à jour les certificats qui utilisent les modèles de certificats », Appliquer.

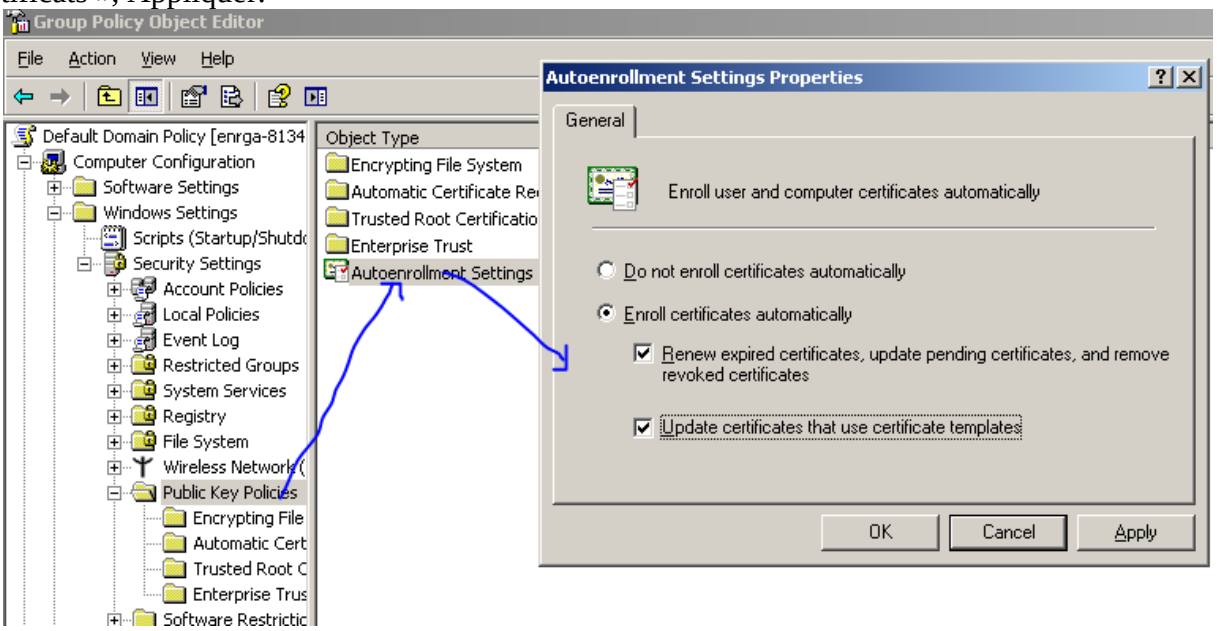


Figure 12 Propriétés de demande automatique de certificats.

4. Refaire l'étape 6 sous configuration utilisateur/paramètres Windows/paramètres de sécurité/stratégie de clé publique/paramètres d'inscription automatique ».
5. Mise à jour de configuration de groupe on tapant la commande « gpupdate/force »

Sous MCD.

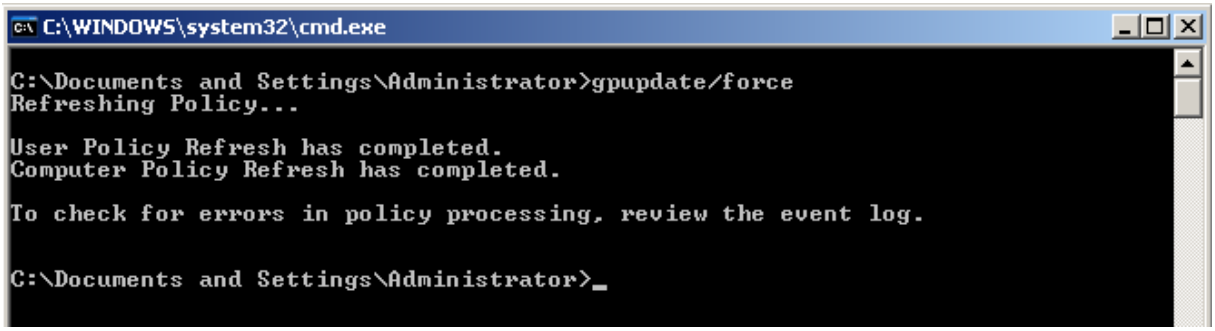


Figure 13 Mise à jour de configuration de groupe.

Stratégie d'IPSec/L2TP :

1. Clic droit sur l'OU puis propriétés, dans l'anglet Group Policy on sélectionne la stratégie par défaut ensuite on clic sur modifie

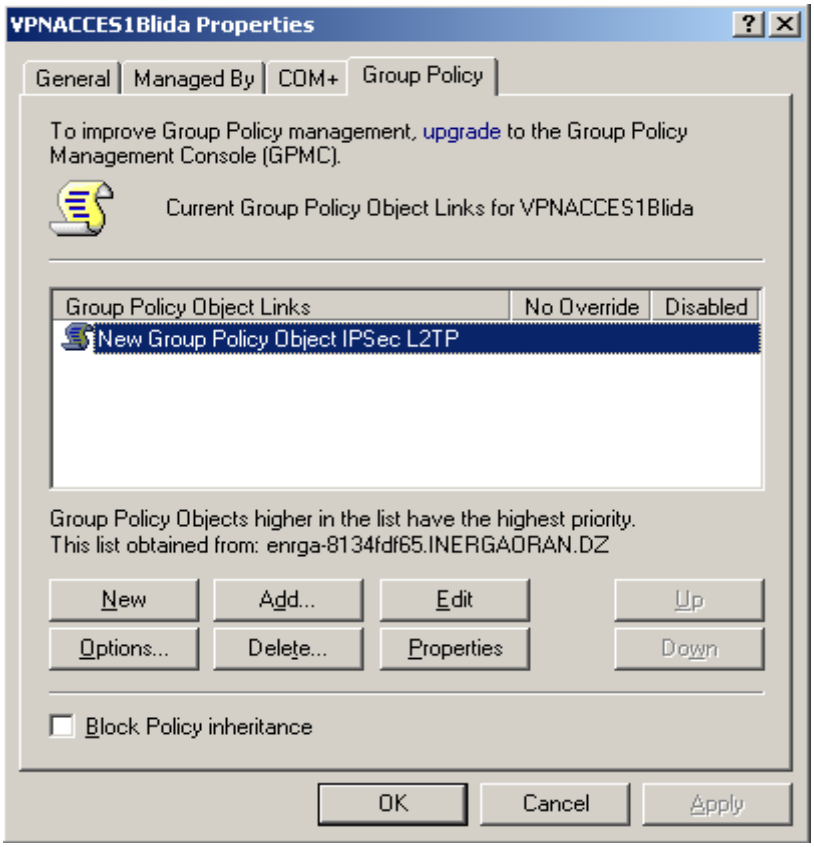


Figure 14 Propriétés de OU.

6. Dans la console MMC (politique de sécurité de groupe), un clic droit sur « stratégie de sécurité IP », Sélectionner « créer une stratégie de sécurité IP »

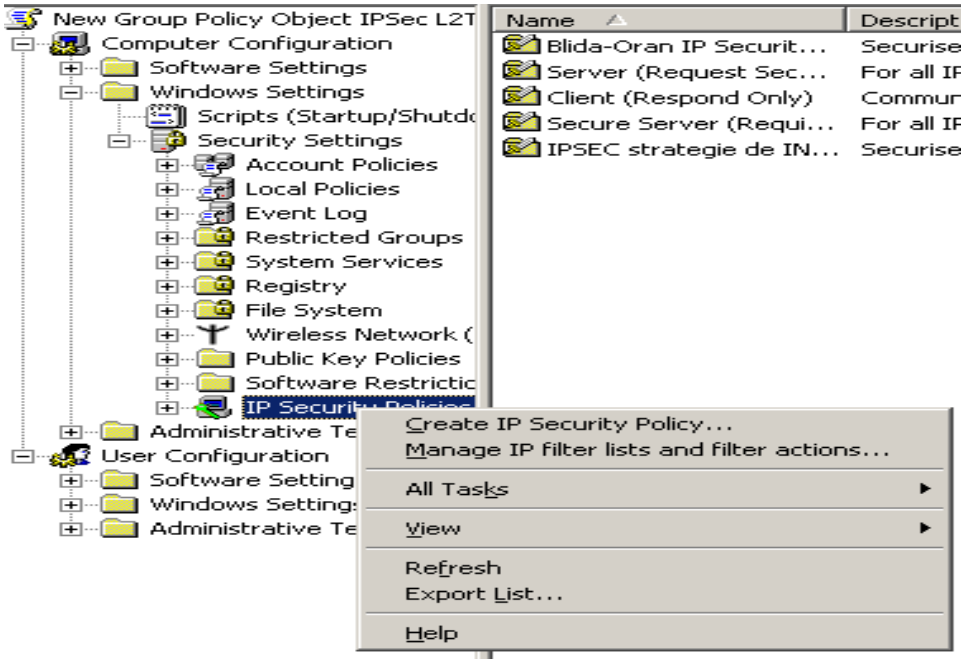


Figure 15 Console de GPOE.

7. Dans la page de bienvenue on clic sur suivant pour accéder à la page de nom de politique, par exemple« VPN ACCES WITH IP Security Policy », puis introduire une description, ensuite suivant.

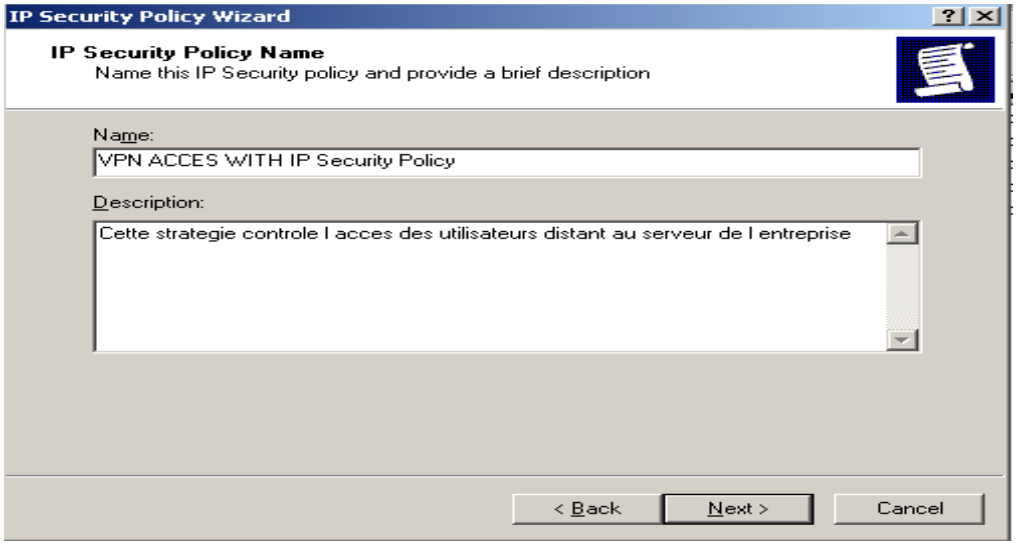


Figure 16 Nom et description de la stratégie

8. Cocher la case « activer la règle de réponse par défaut », puis suivant. Dans la Règles d'authentification on choisie la méthode par certificat émit par CA principale de l'entreprise. puis on clic sur suivant puis sur Terminer.

9. La règle est créée et la boite propriétés apparait.

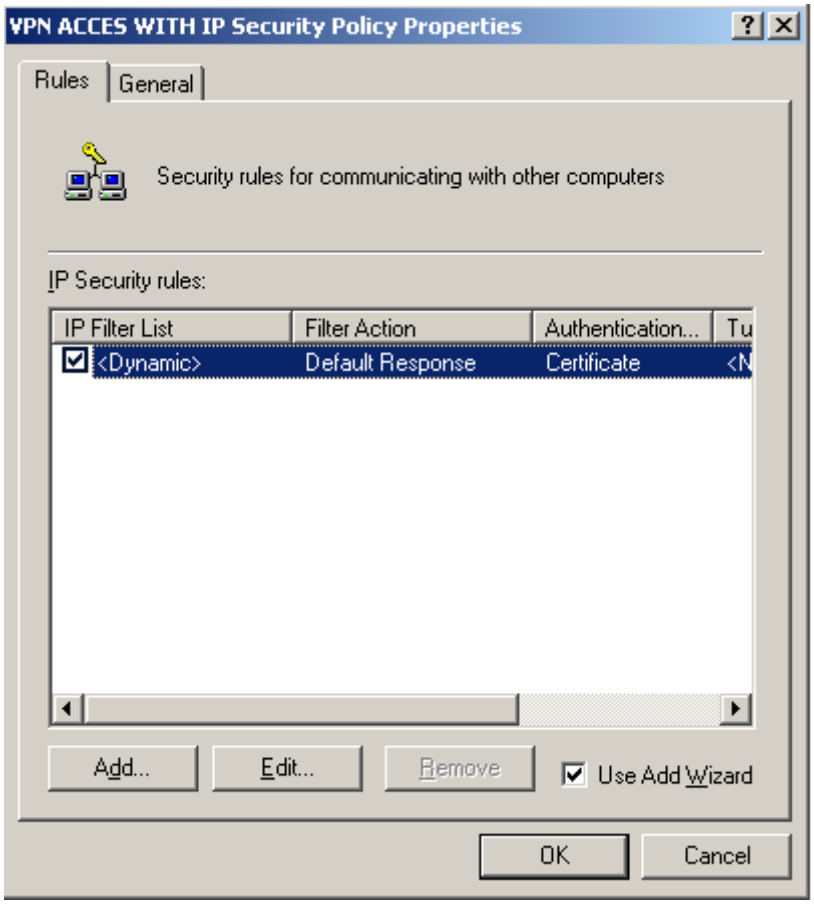


Figure 17 Boite propriétés de la politique de sécurité

10. décochez l'assistant d'ajout et cliquer sur le bouton ajouter, puis on sélectionne « ALL IP trafic IP » puis sur Modifier.

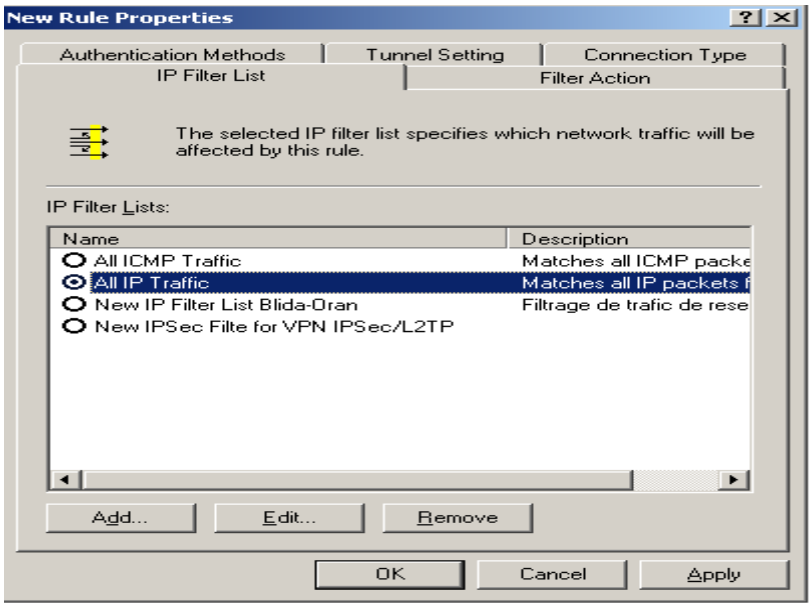


Figure 18 Propriétés de la règle

11. Dans la page liste des filtre IP on clic sur Ajouter pour ajouter un filre IP, la page paramètres de filtre apparait,

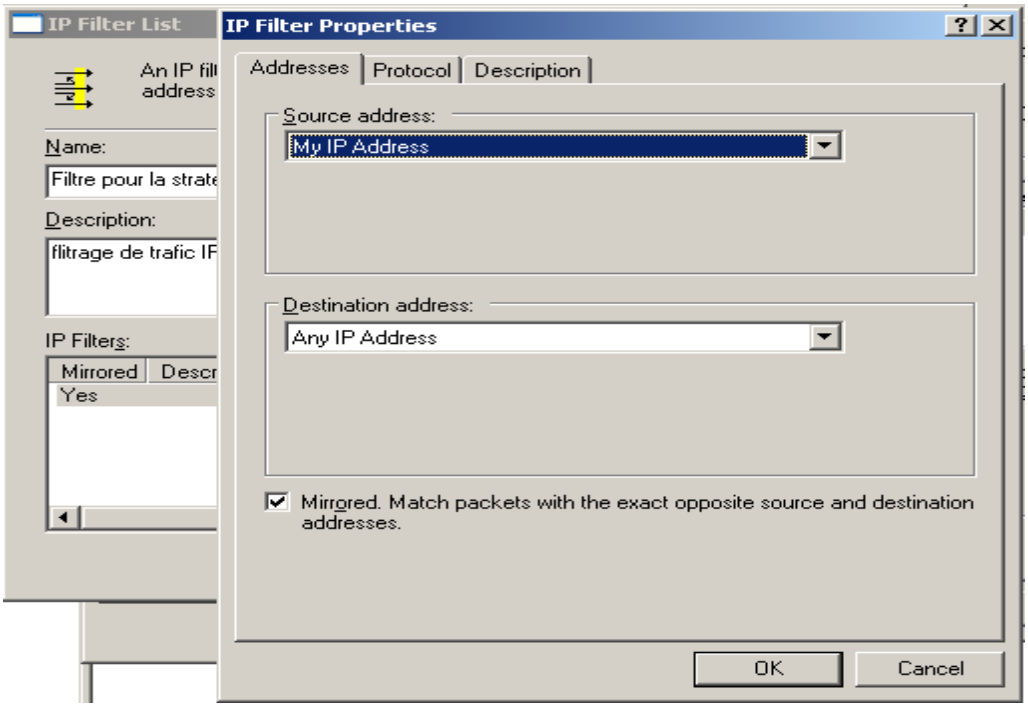


Figure 19 Paramètres de filtre.

12. Dans l'onglet méthodes d'authentification, cliquer sur « ajouter »,puis on sélectionne la méthode par certificat délivrée par la CA principale.

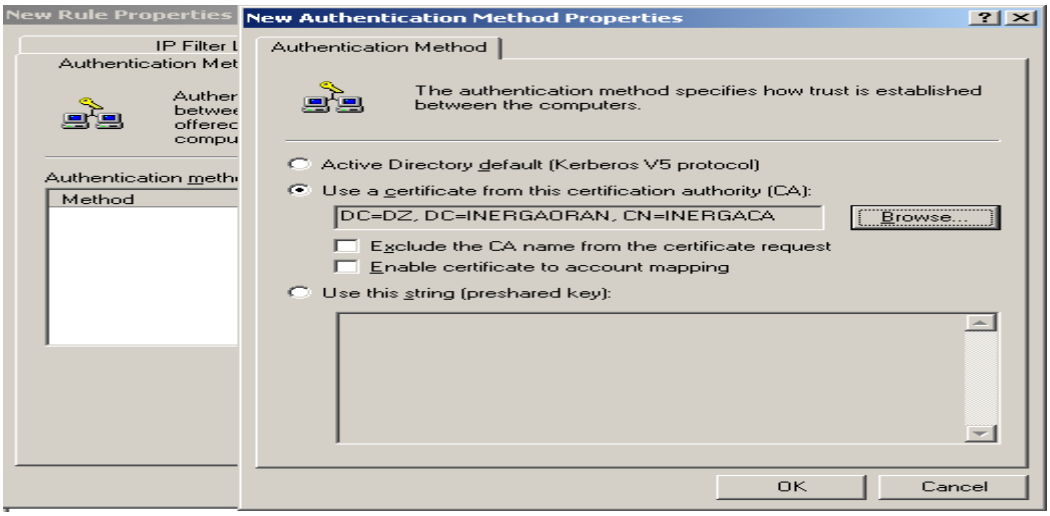


Figure 20 Méthode d'authentification.

13. Dans l'onglet « paramètres du tunnel », garder l'option « cette règle ne spécifie aucun tunnel IPSec », et dans l'onglet « type de connexion », garder aussi « toutes les connexion réseau »

14. Accès des utilisateurs : On stocke la stratégie localement (au niveau serveur) ou sur une disquette ou clé USB, par mail ou par FTP afin que l'utilisateur distant

puisse y accéder et l'importer., pour importer cette stratégie de sécurité IP, Sur le poste de l'utilisateur : Lance une console MMC , Ajouter le composant logiciel enfichable « gestion de la stratégie de sécurité IP » , clic droit sur « stratégies de sécurité IP », « toutes les tâches » puis « importer des stratégies » , localise la stratégie « Importer ». Clic droit sur la stratégie et attribuer cette stratégie.

Création d'une stratégie d'accès distant

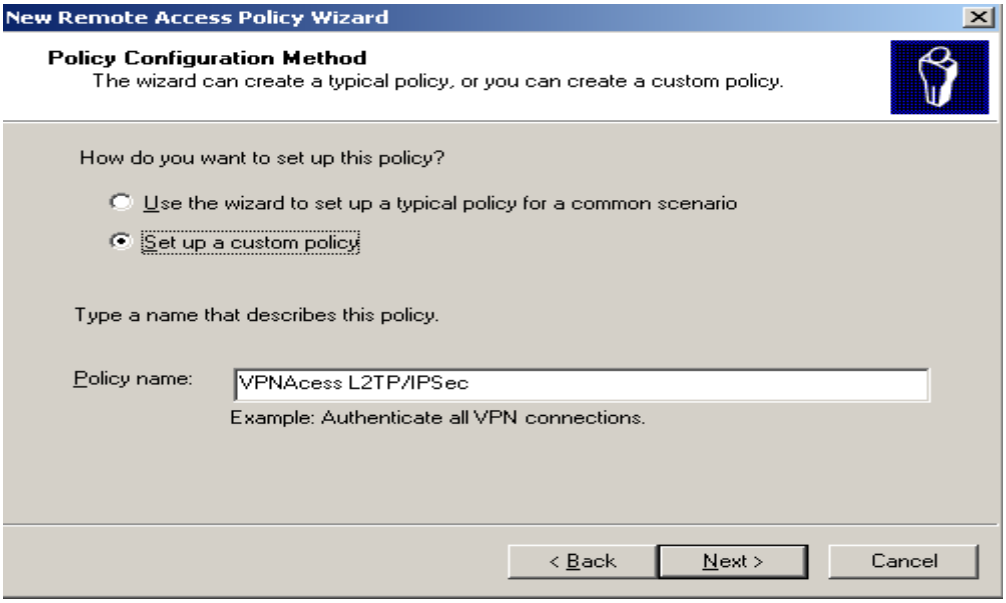


Figure 21 Nom de la stratégie.

15. Laisser la méthode d'accès « VPN ».

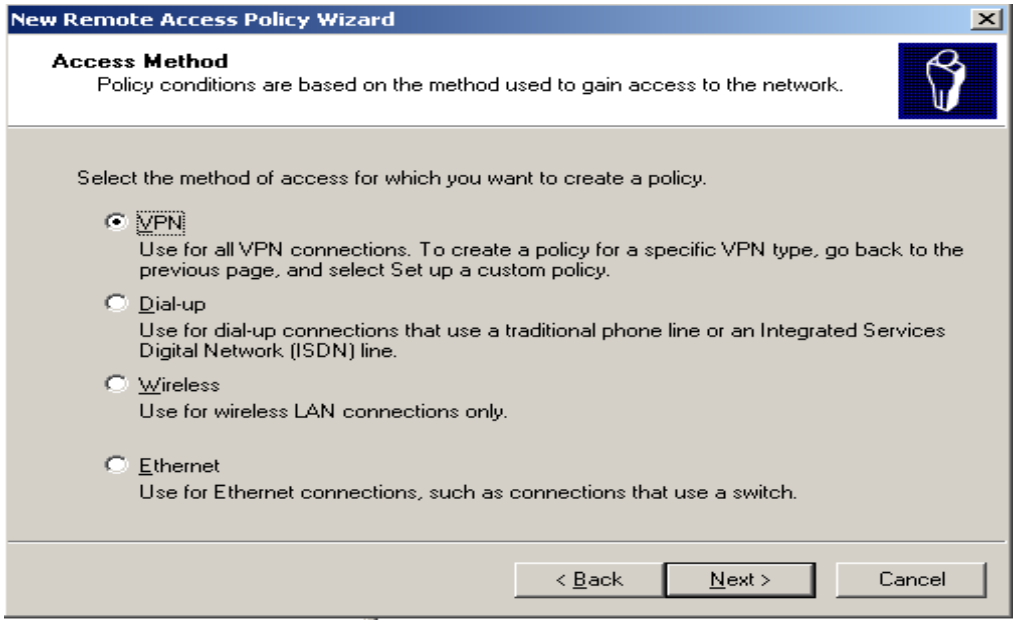


Figure 22 Méthode d'accès « VPN ».

16. en autorisant l'accès pour le groupe créé précédemment VPNACCESBlida ().pour cela cliquer sur Ajouter , puis chercher le croupe concerné.

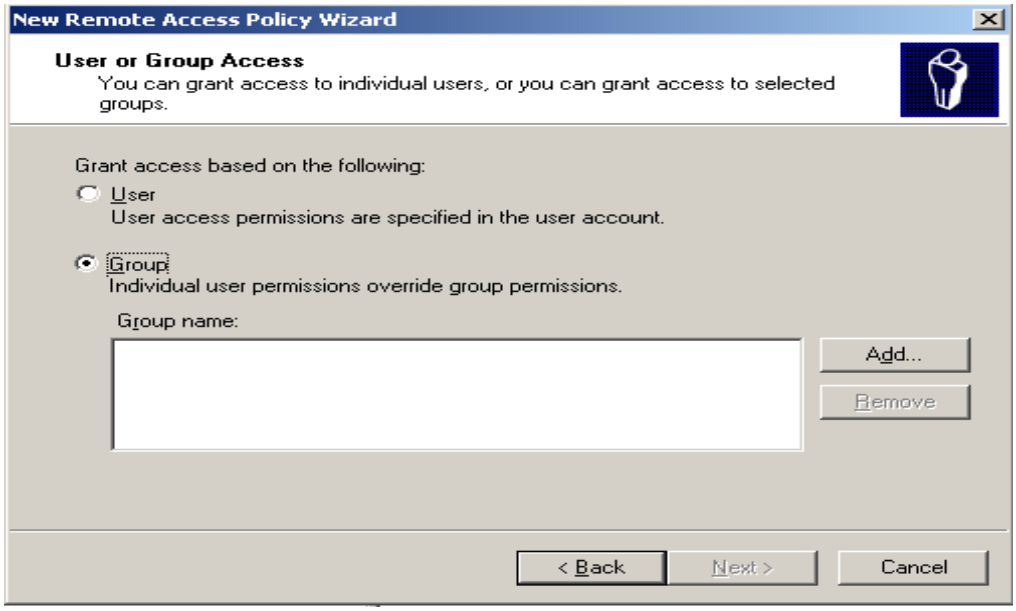


Figure 23 Ajout de croupe d'accès VPN.

17. On Laisse MS-CHAPv2 comme protocole d'authentification. Choisir le cryptage maximal (IPSec triple DES ou MPPE 128 bits).

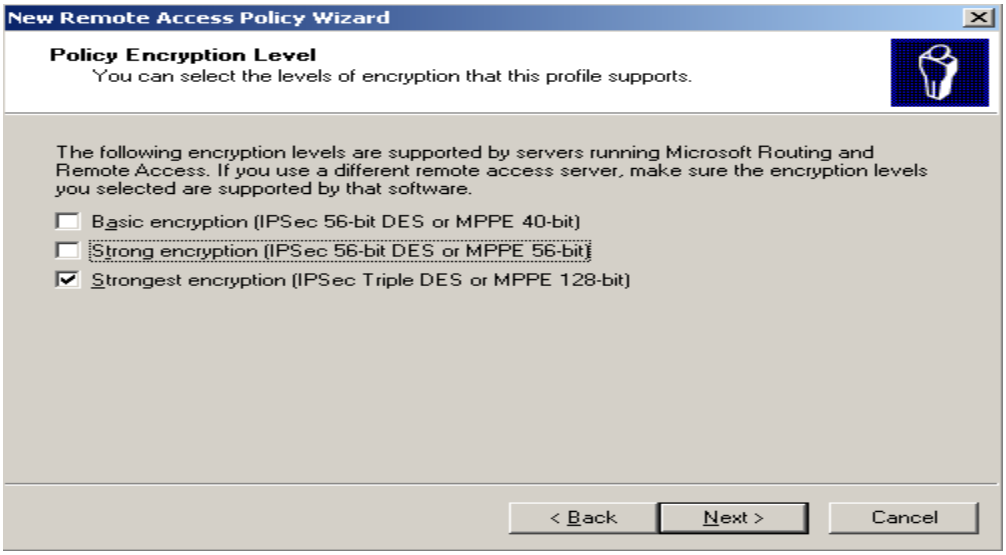


Figure 24 Méthode de cryptage.

18. Dans la boite propriétés de la stratégie, clic sur Ajouter puis ajouter un attribut « tunnel type » en choisissant « L2TP ». Valider la configuration.

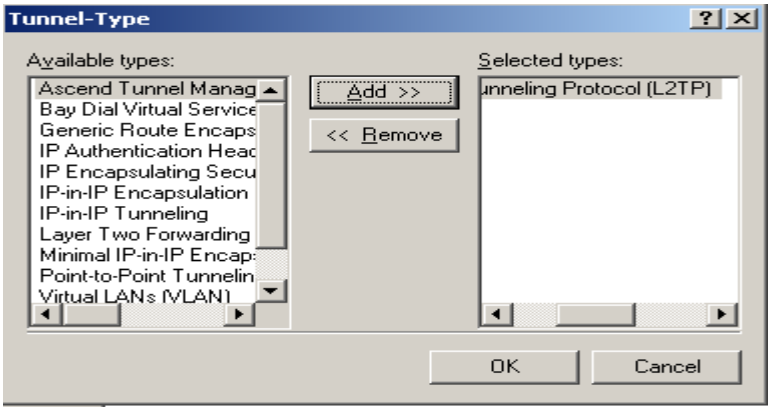


Figure 25 Ajout de tunnel L2TP.

19. changeant le rang de la stratégie à « 1 » clic doit sur la stratégie puis on cliquant à chaque fois sur « move-up ».

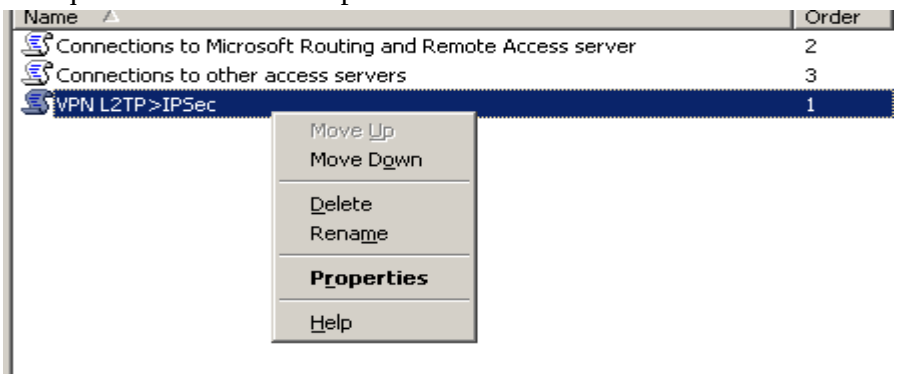


Figure 26 Ordre de la stratégie.

Création d'une stratégie IPSec en mode tunnel

Création d'une stratégie de négociation

1. ouvrir la console Gestion de la configuration de sécurité (pour cela ouvrir une console MMC dans l'angle ajouter cliquer sur ajouter un composant enfichable Windows puis sélectionner le, puis cliquer ajouter).

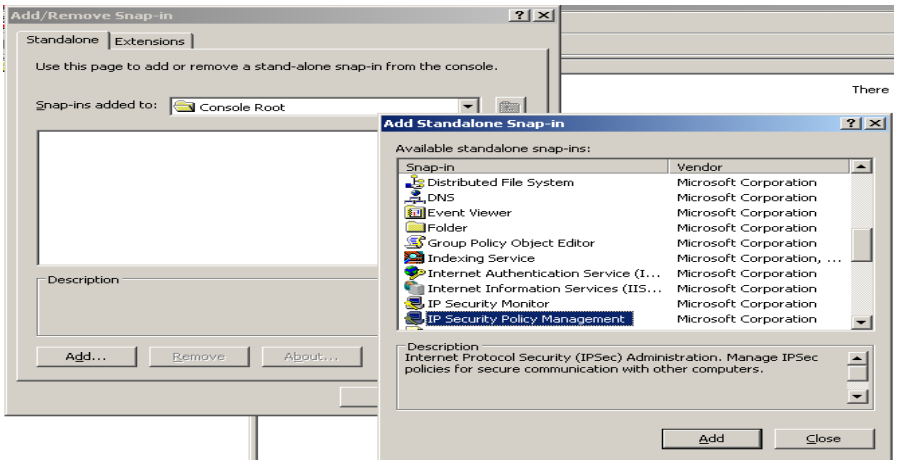


Figure 27 Ajout de MMC de sécurité IP.

2. effectuer un clic droit sur Stratégie de sécurité IP sur Active Directory et Ordinateur local et sélectionner Créer une stratégie de sécurité IP. L'assistant Stratégie de sécurité IP apparaît.

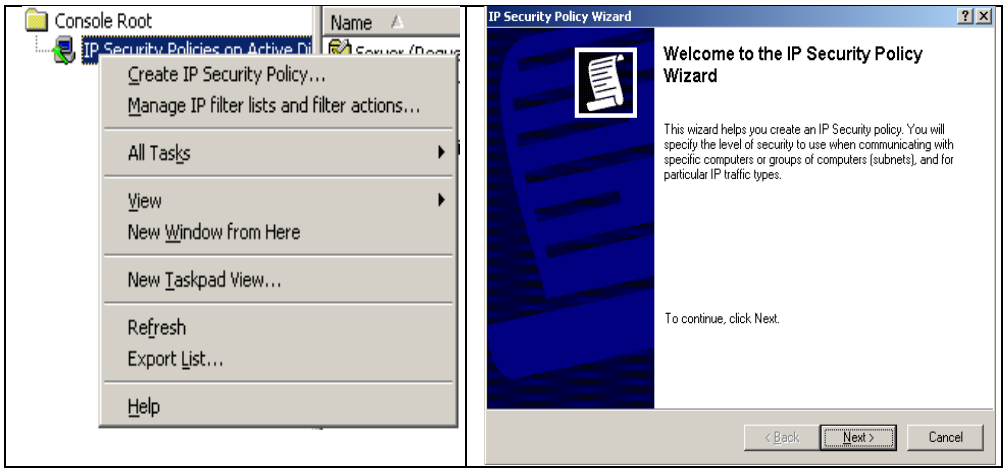


Figure 28 Démarrage de l'assistante de création de SIP .

3. Cliquer sur suivant dans la page d'accueil.

4. Dans la zone de texte Nom : taper « nom de la stratégie » exemple : Blida-Oran IP Security Policy, et taper une description, puis suivant.

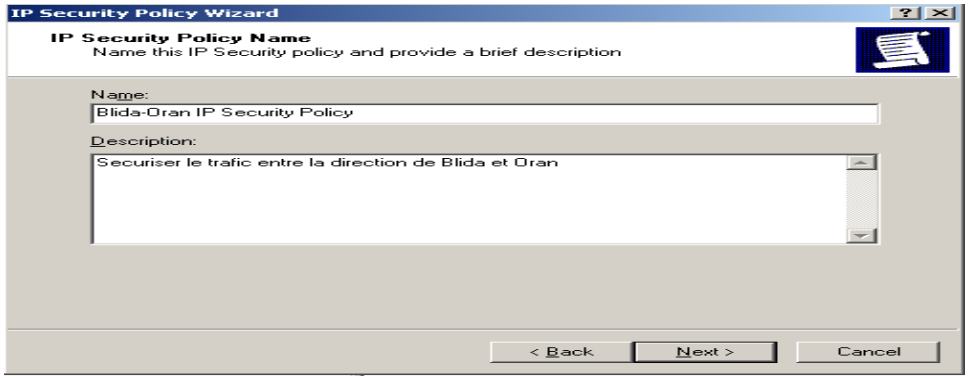


Figure 29 Nom et description de stratégie IP.

5. Désactiver l'option « activer la règle de réponse par défaut », cliquer sur suivant, puis cliquer sur terminer.

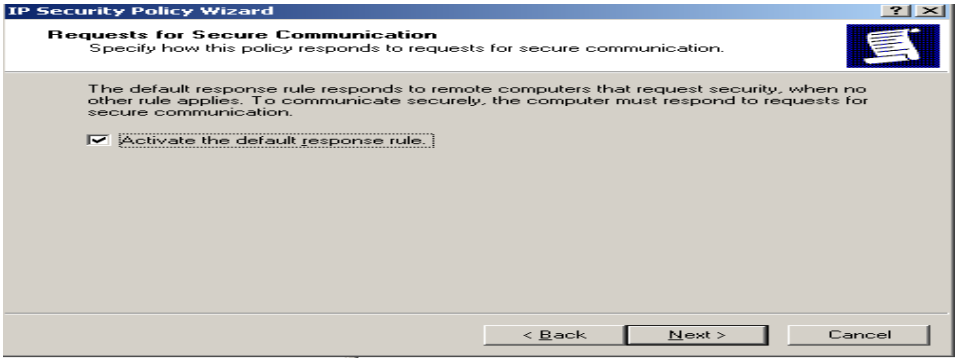


Figure 30 Activation ou désactivation de réponse par défaut.

6. Clic droit sur la stratégie, puis propriétés de la stratégie, en cliquant sur l'ongle général, puis sur paramètres pour atteindre et modifier les règles d'échanges de clés.

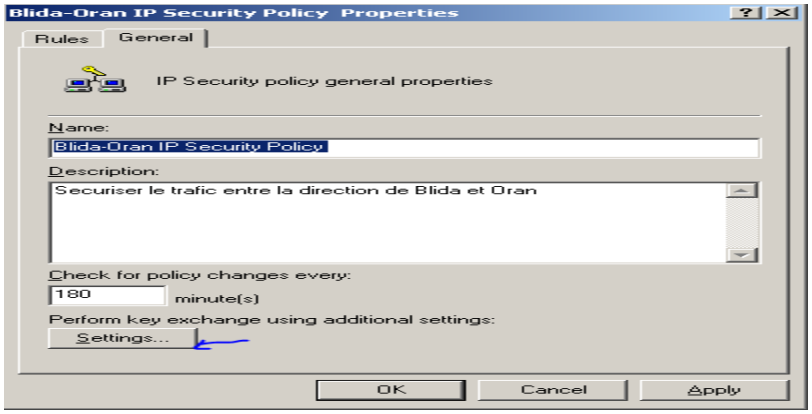


Figure 31 Accès aux paramètres d'échange de clés.

7. Dans la boite de dialogue « paramètres d'échange de clés », cliquer sur méthodes. C'est dans la boite de dialogue paramètres d'échange de clés qu'on peut modifier les caractéristiques de génération de clé principale.sur « Méthodes de sécurité d'échanges de clés», Ajouter ou Modifier des méthodes.

8. sous l'onglet Règles. Cocher Utiliser l'assistant ajout et cliquer sur Ajouter pour ajouter une règle. L'assistant Création d'une règle de sécurité IP se lance.Cliquer sur suivant sur la plage bienvenue. Définir le point de sortie de tunnel, puis cliquer sur suivant.

9. Sur la plage type de réseau, sélectionner Toutes les connexions réseau. Cette stratégie reste active quelle que soit la provenance de la connexion, puis cliquer sur suivant.

10. Sur la plage Listes de filtres IP, cliquer sur ajouter pour ajouter une liste de filtres.

11. Dans la zone texte Nom, taper « négocie ». dans la zone description, spécifier une description.

12. Sélectionner la case Utiliser l'assistant Ajout et cliquer sur Ajouter pour ajouter un filtre IP. L'assistant Filtre d'adresses IP se lance. Cliquer sur suivant.

13. Dans la zone de texte Description taper une description pour le filtre et cliquer sur suivant. Comme source du trafic IP, dans la zone de liste déroulante Adresse source, sélectionner la source d'adresses réseau local puis suivant. Dans la plage Destination du trafic IP, sélectionner l'adresse IP destination, puis cliquer sur

suivant. Sur la plage type de protocole IP, sélectionnez Any, puis cliquez sur suivant.Choisir le port destination, puis suivant, cliquer sur Terminer.

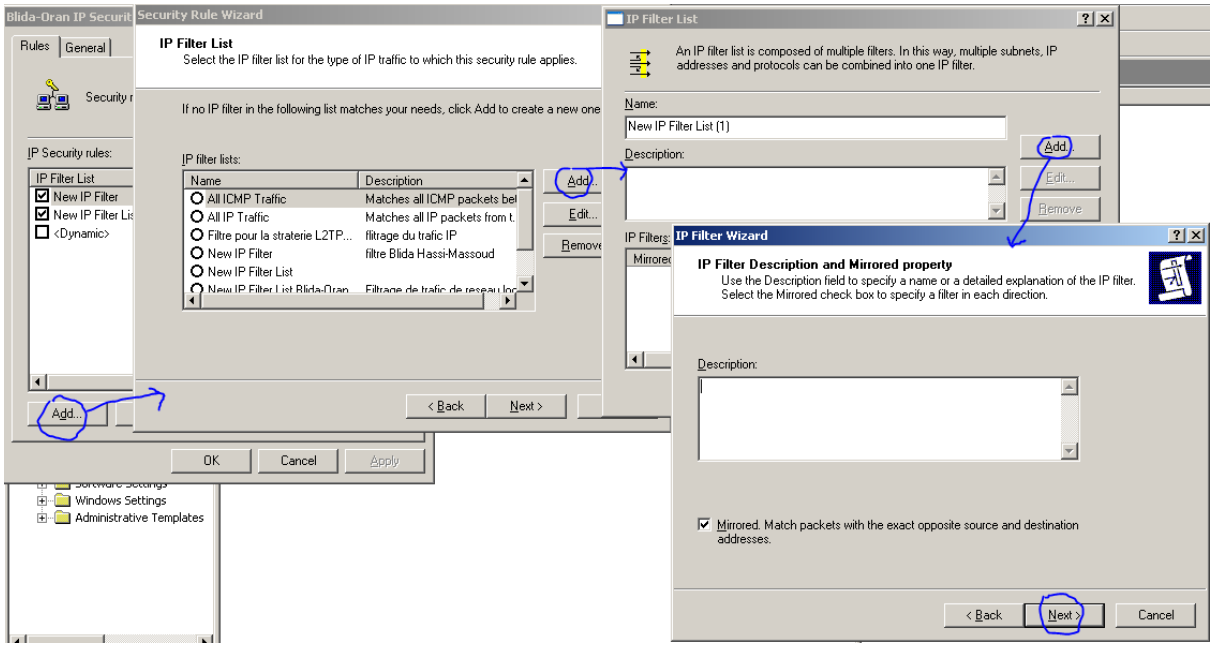


Figure 32 Création de filtre IP.

14. Cliquer OK pour revenir à la plage Liste de filtres IP de l'assistant règle de sécurité.

15. Sélectionner le filtre créé puis sur Suivant. Tout on gardant l'assistant d'ajout activé, puis on clic sur Ajouter. Dans la page Action de filtre IP on clic Suivant, on donne le nom et la description de filtre Action, puis Suivant. On choisie « Négocie la sécurité » comme Action de filtre, puis Suivant.

16. Sélectionner « Non pas communiques avec les ordinateurs son IPSec », puis Suivant.

17. Sur la page Sécurité de trafic IP, on choisie Personnalisé puis on clic sur Méthodes, dans la boite de dialogue on sélectionne AH(SHA1) pour l'intégrité et ESP (SHA1 et 3DES pour l'intégrité et le cryptage) et les paramètres de renouvellement des clés (chaque 1H ou 100000 KB). OK puis Terminer.

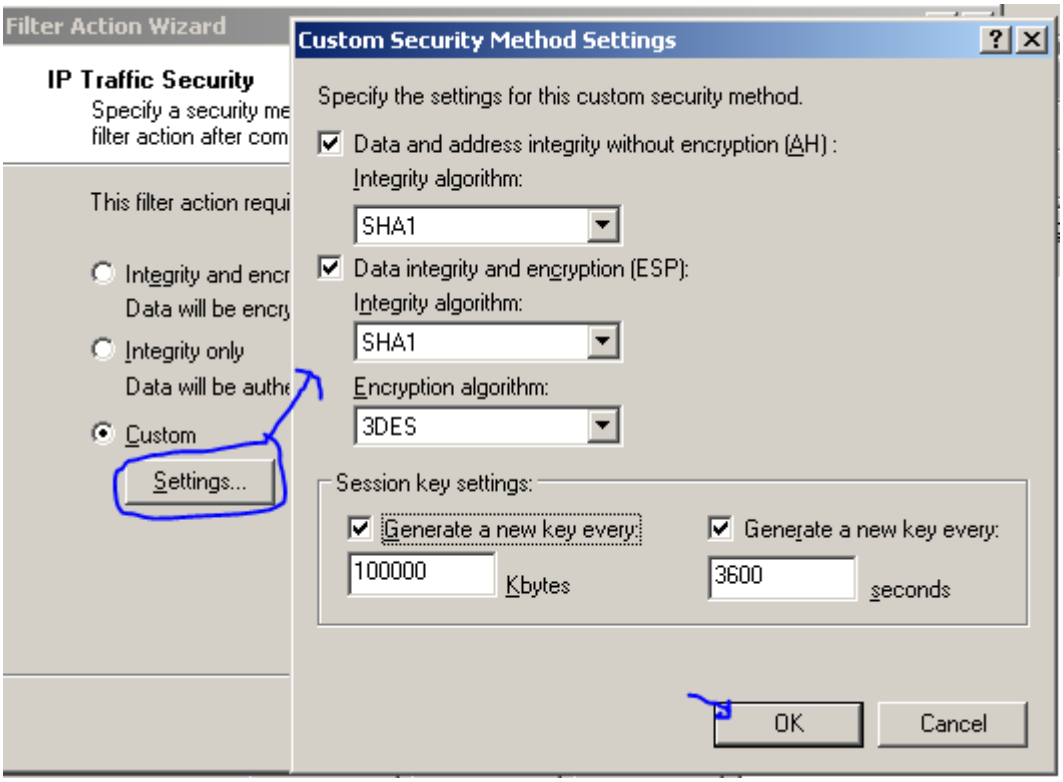


Figure 33 Méthodes de sécurité du trafic IP.

18. Sélectionner le filtre puis Suivant. Sélectionnez la méthode d'authentification par certificat délivrées par la CA principale de l'entreprise, puis Terminer.

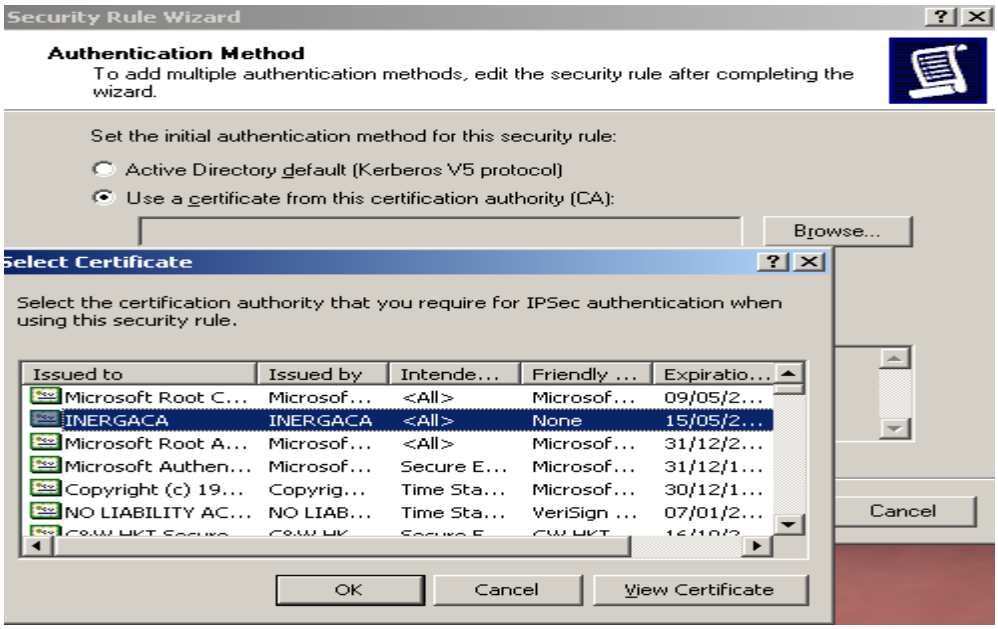


Figure 34 Méthode d'authentification par certificat.

19. Cliquez sur OK pour terminer la règle, puis cliquez à nouveau sur OK pour finir la procédure.

20. Clic droit sur la stratégie puis Appliquer. notre stratégie est bien active.

21. Pour la règle de sécurité IP en mode tunnel du destination de Hassi-Massoud : nous les paramètres suivants :

1. point de sortie de tunnel, adresse public de serveur de direction de Hassi-Massoud.
2. pour la plage IP de réseau destination.

22. Cette stratégie peut être exportée avec des moyens sécurisés (flash disque,…) vers le serveur d'Oran et celui de Hassi-Massoud et la modifier. Ou bien refaire toutes les étapes suivies dans le premier serveur(Blida).

Le tableau ci-après détaille tout les résultats affichés précédemment dans le mode rapide sous moniteur d'IPSec :

Acquisition active	Nombre de demandes en attente de négociation IKE pour établir une association de sécurité entre des homologues IPSec.
Réception active	Nombre de messages IKE reçus mis en file d'attente avant d'être traités.
Echecs d'acquisition	Nombre total de demandes d'acquisition sortantes ayant échoué depuis le dernier démarrage du service IPSec.
Echecs de réception	Nombre total d'erreurs ayant eu lieu au cours du processus de réception des messages IKE depuis le dernier démarrage du service IPSec.
Réception de la taille du segment	Nombre d'entrées des tampons de réception IKE. Les tampons de réception stockent les messages IKE entrants.
Echecs d'authentification	Nombre total d'authentification des identités (Kerberos, certificat et clé partagée)qui ont eu lieu durant la négociation de monde principal depuis le dernier démarrage du service IPSec.
Echecs de négociations	Nombre total d'échecs de négociation ayant eu lieu au cours de la négociation de mode principal.
Obtention totale de SPI	Nombre total de demandes soumises par IKE au pilote IPSec.

Ajout de clés	Nombre total d'association de sécurité de mode rapide entrantes.
Mise à jour de clés	Nombre total d'association de sécurité de mode rapide sortantes ayant été ajoutées par IKE au pilote IPSec.
Taille de la liste de connexion	Nombre de négociation de mode rapide en cours.
Mode principal IKE	Nombre total de réussites de création de SA au cours des négociations de mode principal.
Taille de la liste ISADB	Nombre d'entrées d'état de mode principal, dont les négociation de mode principal réussies, les négociations de mode principal en cours, ainsi que celles ayant échoué ou expiré et qui n'ont pas encore été supprimées
Mode rapide IKE	Nombre total de réussites de création de SA au cours des négociation de mode rapide depuis le dernier démarrage du service IPSec
Paquets non valides reçus	Nombre total de messages IKE non valides reçus depuis le dernier démarrage du service IPSec. Ce nombre inclut les messages IKE présentant des champs d'en-tête non valides, des longueurs de charge incorrectes et des valeurs incorrectes pour le cookie du répondeur. Les messages IKE non valides résultent souvent de la retransmission de messages IKE.

Tableau 1 : les Statistiques de mode rapide

Le tableau suivant détaille tout les résultats affichés précédemment dans le mode principal sous moniteur d'IPSec :

Associations de sécurité actives	Nombre d'associations de sécurité de mode rapide actives.
Opérations de clés en cours	Nombre d'opérations d'échange de clés

	IPSec en cours(non terminées).
Ajouts de clés	Nombre total de clés pour la négociation de SA de mode rapide ajoutées avec succès depuis le dernier démarrage de l'ordinateur
Suppression de clé	Nombre total de clés de SA de mode rapide supprimées avec succès depuis le dernier démarrage de l'ordinateur.
Nouvelles clés	Nombre total d'opération réussies de génération de nouvelles clés de mode rapide.
Tunnels actifs	Nombre de tunnels IPSec actifs.
Paquets SPI erronés	Nombre total de paquets pour lesquels l'index SPI était incorrect. Un index SPI incorrect peut signifier que la SA entrante a expiré et qu'un paquet utilisant l'ancien SPI vient d'arriver. Ce nombre est susceptible d'augmenter si les intervalles de changement de clé sont courts et que le nombre de SA est élevé. Peut indiquer une attaque d'usurpation de paquet.
Paquets non décryptés	Nombre total de paquets n'ayant pu être décryptés depuis le dernier démarrage de l'ordinateur. Le décryptage d'un paquet peut échouer en cas de d'échec d'une vérification de validation.
Paquets non authentifiés	Nombre total de paquets pour lesquels des données n'ont pas pu être vérifiées (pour lesquels la vérification de hachage d'intégrité a échoué) depuis le dernier démarrage de l' ordinateur. Les augmentations de ce chiffre peuvent indiquer une attaque d'usurpation ou modification de paquets par des périphériques réseau.
Octets confidentiels envoyés	Nombre total d'octets envoyés à l'aide du

	protocole ESP.
Octets confidentiels reçus	Nombre total d'octets reçus à l'aide du protocole ESP, à l'exception du protocole ESP non crypté, depuis le dernier démarrage de l'ordinateur.
Octets authentifiés envoyés	Nombre total Octets authentifiés envoyés à l'aide du protocole AH ou du protocole ESP , depuis le dernier démarrage de l'ordinateur.
Octets authentifiés reçus	Nombre total Octets authentifiés reçus à l'aide du protocole AH ou de protocole ESP depuis le dernier démarrage de l'ordinateur.
Octets envoyés dans les tunnels	Nombre total d'octets envoyés à l'aide du mode de tunnel IPSec.
Octets reçus dans les tunnels	Nombre total d'octets reçus à l'aide du mode de tunnel IPSec.

Tableau 2 Les statistiques de mode rapide

Dépannage de la stratégie IPSec

1. Redémarrer l'ordinateur pour que les modifications soient mises en application.
2. La stratégie est-elle appliquée ? utiliser le moniteur IPSec pour savoir quelle est la stratégie actuellement employée, ou la commande Netsh ipsec static show gpoassignedpolicy .
3. Les détails de la stratégie ? la commande Netsh ipsec static show all. Confirmer que la stratégie est attribuée et que les paramètres sont corrects.
4. Si la stratégie diffère de celle attendu ? la commande Netsh ipsec static show gpoassigned policy ou le composant logiciel gestion de la stratégie IP.
5. La négociation IKE réussit-elle ? vérification de journal des événement. La négociation IKE se sert de catégorie événement d'ouverture de session (Logon Event) pour signaler l'échec ou la réussite. Si la négociation IKE échoue, on vérification les réglages de IKE. L'authentification, le cryptage et les modifications de clé sont-ils identiques sur les deux ordinateurs.

Si IKE réussit, qu'en est-il de mode rapide ?vérification de journal des événement de sécurité. Si le mode rapide échoue, vérification des réglages du mode rapide (cryptage, intégrité, force de clé, modification de clé, etc.) sont identiques.

Résumé

Pour facilité les différentes tâches d'administration et le partage de données entre le personnel des trois directions de l'entreprise en toute sécurité et en minimisant les coûts .Nous nous sommes basés sur des solutions de sécurité standardisées.

En effet, nous avons opté d'une part, pour la solution VPN site à site qui permet l'interconnexion des trois sites, en se basant sur le protocole IPSec en mode tunneling, qui est le plus répondu, et devenu comme standard pour VPN, fournissant les services de sécurité comme la confidentialité, l'intégrité, l' authentification mutuelle, le contrôle d'accès. Les tunnels sont utilisés pour la sécurisation des protocoles de couches supérieures tel que : TCP, UDP,…etc.

Et d'autre part, la solution VPN poste à site pour la connexion des clients nomades de chaque site, en s'appuyant sur les avantages du protocole IPSec en mode transport et le protocole L2TP qui fournit les services d'authentification et la garantie de tunnels sûrs. La combinaison IPSec/L2TP est publiée par IETF en RFC(3193), est très utilisée dans ce type de connexion.

Mots clés :

Réseau, Sécurité, protocole, Site à site, Poste à site, VPN, IPSec, L2TP.

Summary

To ease the various administrative tasks and data sharing between staff of the three directions of the company safely and minimizing costs. We relied on standardized security solutions.

Indeed, we chose the one hand, to the site to site VPN solution that allows the interconnection of the three sites, based on IPSec tunneling mode, which is the answer, and become as standard for VPN providing security services such as confidentiality, integrity, mutual authentication, access control, the tunnels are used to secure higher layer protocols such as

TCP, UDP ...etc.

And secondly, the VPN peer-to site for connecting mobile clients in each site, based on the benefits of IPSec in transport mode and L2TP protocol that provides authentication services and guarantee secure tunnels. The combination IPSec/L2TP which is published by IETF RFC (3193), is widely used in this type of connection.

Keywords:

Network, security, protocol, site to site, post to site VPN, IPSec, L2TP.