

Réseau

Par LAMANT Anthony

Pour informations :

Ce cours est basé sur les diapositifs mis à disposition par Madame Buseyne. Je me suis dit que c'était quand même plus facile à étudier sur des feuilles que sur des diapos. Si des choses venaient à manquer ou s'il y a des erreurs, merci de bien vouloir me prévenir. Bon courage à tous !

Adressage IP v4 :

Structure des adresses IP :

Une adresse IP est codée sur 32bits. Elle permet d'identifier chaque hôte et le réseau auquel il appartient. Elle est écrite soit en format décimal : w.x.y.z où w, x, y et z sont 4 champs de 8bits séparés par des points (Exemple : 192.168.13.5), soit au format binaire (Exemple : 10000011.01101011.00000011.00011000).

Classe d'adresses :

Les systèmes appartenant au même réseau ont une partie d'adresse commune : la partie d'adresse du réseau :

Classe A	0	Numéro du réseau (7 bits)	Numéro de l'hôte (24 bits)
----------	---	---------------------------	----------------------------

Classe B	10	Numéro du réseau (14 bits)	Numéro de l'hôte (16 bits)
----------	----	----------------------------	----------------------------

Classe C	110	Numéro du réseau (21 bits)	Numéro de l'hôte (8 bits)
----------	-----	----------------------------	---------------------------

Adresses multidestinatoires (routeurs, multicast, ...) :

Classe D	1110	Numéro de groupe (28 bits)
----------	------	----------------------------

Adresses expérimentales :

Classe E	1111	Usage Futur (27 bits)
----------	------	-----------------------

Adresses particulières et réservées :

0.0.0.0 : Adresse d'acheminement par défaut (hôte inconnu sur ce réseau)

127.x.x.x : Adresse de bouclage (127.0.0.1)

Adresse de réseau : Tous les bits de la partie hôte sont à 0.

Adresse de diffusion : Tous les bits de la partie hôte sont à 1.

Adresses privées : Classe A : 10.0.0.0

Classe B : 172.16.0.0 à 172.31.255.255

Classe C : 192.168.0.0 à 192.168.255.255

Les sous-réseaux:

Pourquoi des sous-réseaux ? :

Ils permettent :

- L'utilisation de plusieurs média
- Une réduction de l'encombrement
- Une économie de temps de calcul
- Une isolation d'un réseau
- Un renforcement de la sécurité
- Une optimisation de l'espace réservé à une adresse IP

Masque de sous-réseau :

Il permet de :

- Faire la séparation entre la partie réseau (bits à 1) et la partie hôte de la machine (bits à 0)
Exemple : IP 193.191.131.33 MSR 255.255.255.0 ou 193.191.131.33/24
Adresse réseau : 193.191.131.0 Adresse machine : 33
- Déterminer le nombre de machines d'un réseau
Exemple : Nombre de bits partie hôte: 8 => $2^8 - 2 = 256 - 2 = 254$ machines.
- Segmenter un réseau en plusieurs sous-réseaux. Il utilise les bits de poids fort de la partie hôte de l'adresse IP pour désigner un réseau (divisé en différents sous-réseaux).

Création de sous-réseaux :

Nombre de sous-réseaux :

Le nombre de sous-réseaux est égal à 2^n , n étant le nombre de bits empruntés (à 1) à la partie hôte pour coder les sous-réseaux.

Exemple :

- 1 → 2^1 (2 sous-réseaux)
- 2 → 2^2 (4 sous-réseaux)
- 3 → 2^3 (8 sous-réseaux)
- 4 → 2^4 (16 sous-réseaux)
- 5 → 2^5 (32 sous-réseaux)
- 6 → 2^6 (64 sous-réseaux)
- 7 → 2^7 (128 sous-réseaux)
- 8 → 2^8 (256 sous-réseaux) → Pas possible en Classe C.

Adresse des sous-réseaux :

Permet de trouver les adresses des sous-réseaux valides en utilisant les bits à 1 du masque de sous-réseau. Exemple : 193.104.1.145/255.255.255.0 par défaut, on emprunte 2 bits à la partie hôte

→ Nouveau Masque : 255.255.255.192

→ $2^2 = 4$ sous-réseaux avec comme adresse : 193.104.1.00000000 → 193.104.1.0

193.104.1.01000000 → 193.104.1.64

193.104.1.10000000 → 193.104.1.128

193.104.1.11000000 → 193.104.1.192

Adresse de diffusion d'un sous réseau :

Il faut mettre tous les bits de la partie hôte à 1.

Exemple précédent : 193.104.1.145/27 ou 193.104.1.145/255.255.255.192

SR 193.104.1.0 → AD 193.104.1.00111111 → 193.104.1.63
SR 193.104.1.64 → AD 193.104.1.01111111 → 193.104.1.127
SR 193.104.1.0 → AD 193.104.1.10111111 → 193.104.1.191
SR 193.104.1.0 → AD 193.104.1.11111111 → 193.104.1.255

Nombre de postes d'un sous réseau :

Le nombre de postes est égal à 2^n , n étant le nombre de bits à 0 du masque de sous-réseaux permettant de coder l'hôte.

A ce chiffre il faut enlever les 2 adresses réservées : - Tous les bits à 0 (le sous-réseau lui-même)
- Tous les bits à 1 (Adresse de diffusion pour le sous-réseau)

Exemple précédent : 193.104.1.145/27 ou 193.104.1.145/255.255.255.192

2 bits pour le sous-réseau et 6 bits pour l'hôte
→ Le nombre de postes est $2^6 - 2 = 64 - 2 = 62$ postes.

Adresse de postes sur sous réseau :

L'adresse de poste sur un sous-réseau est comprise dans la fourchette [adresse de sous-réseau +1, adresse de diffusion -1]

Exemple précédent : 193.104.1.145/27 ou 193.104.1.145/255.255.255.192

SR 193.104.1.0 → [193.104.1.1 à 193.104.1.62]
SR 193.104.1.64 → [193.104.1.65 à 193.104.1.126]
SR 193.104.1.128 → [193.104.1.129 à 193.104.1.190]
SR 193.104.1.190 → [193.104.1.193 à 193.104.1.254]

C.I.D.R. (Classless Inter Domain Routing) :

C'est un nouveau modèle qui simplifie le routage et permet un adressage plus fin.

Il permet l'allocation des réseaux sans classe, d'agréger les tables de routage, de découper les réseaux de classe A.

Exemple : Agrégation de réseaux 193.127.32.0 et 193.127.33.0 agrégés en 193.127.320/23

Il définit une convention d'écriture qui spécifie le nombre de bits utilisés pour identifier la partie réseau (les bits à 1 du masque de sous-réseau).

Exemple : 142.12.42.145/24 ↔ 142.12.42.145 255.255.255.0

10.0.0.0/255.0.0.0 ↔ 10.0.0.0/8

192.168.25.32/255.255.255.248 ↔ 192.168.25.32/29

Comment bien choisir son masque :

- En partant du masque existant.
- En fonction du nombre de machines.
- En découpant la plage d'adresses en plusieurs sous-réseaux.

Le Routage :

Définition du routage :

Le routage est une technique basée sur les adresses de niveau réseau (3) permettant d'aiguiller une trame quelconque émise par un nœud d'un sous-réseau vers un nœud de destination pouvant être situé sur un autre sous-réseau.

Un routeur (ou passerelle) est un équipement qui fait le lien entre différents réseaux ou sous-réseaux.

Principe du routage :

Il comprend 2 étapes : La détermination du chemin et la commutation.

Quelques règles :

- Aucune machine ni aucun routeur ne connaît le chemin complet du réseau.
- Chaque machine et chaque routeur stocke les informations de routage dans une table de routage.
- Chaque routeur ne connaît que le routeur suivant.

Acheminement des paquets TCP/IP :

Etapes de transmission d'un paquet d'un émetteur A à un destinataire B :

1. Extraire l'adresse IP réseau de B et adresse IP réseau de A et voir s'ils sont dans le même réseau. S'ils le sont, le paquet est transmis directement grâce à l'ARP.
2. S'ils ne sont pas du même réseau, A cherche dans la table de routage une correspondance B/Destinataire intermédiaire (routeur, passerelle).
3. A recherche d'abord l'adresse complète de B dans sa table de routage.
4. S'il ne trouve pas, il cherche l'adresse du sous-réseau du destinataire.
5. S'il ne trouve pas, il cherche l'adresse du réseau.
6. S'il ne trouve aucune correspondance, A cherche dans sa table de routage l'adresse de la passerelle à utiliser par défaut (0.0.0.0).
7. S'il échoue encore le paquet est supprimé.
8. Si l'une des recherches aboutit, A construit le paquet avec l'adresse IP de B, Il l'encapsule dans une trame ayant comme adresse MAC de destination, l'adresse MAC du routeur. La couche 2 du routeur lit la trame et la transmet (ARP) à la couche 3. Celle-ci remarque qu'elle ne lui est pas adressée, elle regarde sa table de routage et décide vers quel routeur la transmettre et encapsule le paquet dans une nouvelle trame et ainsi de suite de routeur en routeur jusqu'à destination.

Table de routage :

Elle est un regroupement d'informations permettant de déterminer le prochain routeur à utiliser pour accéder au réseau sur lequel se trouve la machine de destination.

Son rôle est de déterminer le chemin le plus court pour acheminer les paquets de la source à la destination.

Elle comprend 5 colonnes :

- Réseau de destination
- Masque de sous-réseau
- Adresse de la passerelle (routeur)
- Interface de sortie
- Métrique

La commande ROUTE :

Elle permet de configurer manuellement la table de routage.

- Pour afficher ma table de routage, il faut utiliser la commande : ROUTE PRINT.
- Pour ajouter une route dans la table de routage : ROUTE ADD -p [réseau destination] MASK [masque destination] [passerelle] METRIC [métrique] IF [interface utilisée].
- Pour modifier une route existante : ROUTE CHANGE -p [réseau destination] MASK [masque destination] [passerelle] METRIC [métrique] IF [interface utilisée].
- Supprimer une route existante : ROUTE DELETE [réseau destination].

L'utilitaire TRACERT :

Il vérifie le trajet suivi par un paquet pour atteindre sa destination.

Il est utile pour savoir si un routeur est en panne ou s'il est lent.

Routage statique et dynamique :

Le routage statique est configuré manuellement. Il permet d'ajouter manuellement une route dans la table de routage. Il est adapté aux petits réseaux.

Le routage dynamique permet d'attribuer la meilleure route en se basant sur un algorithme. Cette route est modifiable de manière dynamique par le routeur en vue d'atteindre la destination.

Il existe 2 types de protocole de routage :

- Interne (RIP) ou externe (EGP)
- A vecteur de distance (RIP) ou à état de lien (OSPF)

Protocole de routage RIP (Routing Information Protocol (RFC 1058)):

Généralités :

Extension de RIP : RIP2 en 1994 (RFC 2453).

Il est basé sur l'algorithme du vecteur distance.

Il transmet les couples adresse/distance (= vecteurs de distance)

Il utilise les métriques pour calculer la distance qui sépare 2 nœuds d'un réseau.

Le nombre de sauts maximal autorisé est de 15 (16 est l'infini).

Il envoie ses paquets par UDP sur le port 520.

Format des paquets :

➤ Format du paquet RIP v1 :

Command (1)	Version (1)	Zéros (2)	AFI (2)	Zéros (2)	IP Adresse (4)	Zéros (4)	Zéros (4)	Métrique (4)
----------------	----------------	--------------	------------	--------------	----------------------	--------------	--------------	-----------------

➤ Format du paquet RIP v2 :

Command (1)	Version (1)	Zéros (2)	AFI (2)	Route Tag (2)	IP Adresse (4)	Masque SR (4)	Saut suivant (4)	Métrique (4)
----------------	----------------	--------------	------------	---------------------	----------------------	---------------------	------------------------	-----------------

Fonctionnement :

Lors de l'initialisation, il détermine l'adresse réseau de ses interfaces puis envoie sur chacune une demande d'informations (table RIP) aux routeurs voisins.

Lors de la réception d'une réponse, il met à jour sa table si nécessaire :

- Pour une nouvelle route : incrémente sa distance (<15) et diffuse le vecteur distance correspondant.
- Pour une route existante mais avec une distance plus faible, la table est mise à jour.

Les routes doivent être retirées de la table RIP si un réseau devient inaccessible, si un routeur est en panne.

Boucle de routage :

Une boucle de routage se produit quand 2 routeurs ou plus possèdent des informations de routage incorrectes indiquant l'existence d'une route valide pour une destination non accessible.

Techniques pour lutter contre les boucles de routage :

- Split Horizon
- Route Poisoning
- Poison Reverse
- Holdown Timers
- Triggered Updates

Installation du protocole de routage dynamique RIP :

Démonstration installation sous Windows Server 2003.

Protocole de routage OSPF (Open Shortest Path First (RFC 1583)) :

Généralités :

C'est un protocole de routage d'état de lien.

Il est ouvert (Open) et est basé sur l'algorithme SPF (Le chemin le plus court d'abord) de Dijkstra.

Il utilise la notion de coût pour privilégier l'élection de certaines routes (plus le coût est faible, plus le lien est intéressant).

Le routage est hiérarchisé pour simplifier le calcul des coûts (découpage en zone).

Zone (Area) : Ensemble de réseaux contigus. Chaque zone se comporte comme un réseau indépendant et ne connaît que l'état des liaisons internes.

Fonctionnement :

L'OSPF attribue un coût à chaque liaison afin de privilégier l'élection de certaines routes. Plus le coût est faible, plus le lien est intéressant.

Tous les routeurs d'un même réseau (zone) travaillent sur une base de données de topologie identique qui décrit le réseau.

L'algorithme traite cette base de données pour déterminer les routes les moins coûteuses.

Il annonce les informations de topologie par des données structurées appelées LSA (Link State Advertissement).

Les routeurs doivent préalablement remplir les tâches suivantes avant de pouvoir effectuer le travail de routage :

1. Établir la liste des routeurs voisins.
2. Elire le routeur désigné et celui de secours.
3. Découvrir les routes.
4. Elire les routes à utiliser.
5. Maintenir la base de données topologique.

Installation du protocole de routage OSPF :

Démonstration installation sous Windows Server 2003.

La commutation LAN :

Les réseaux Ethernet :

Présentation :

Il a été conçu à Hawaï dans les années 70.

Au cours des années 80, mise en place de la norme 802.3 par l'IEEE à partir d'Ethernet.

Ethernet repose sur les principes suivants :

- Accès au média non déterministe.
- Remise de type broadcast des trames de données Ethernet/IEEE802.3.
- Utilisation de CSMA/CD.
- Sensibilité aux problèmes de congestion et de latence.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) :

Carrier Sense : détection de la porteuse.

Multiple Access : accès multiple.

Collision Detection : détection des collisions.

Différents types d'Ethernet :

Ethernet Half Duplex :

- Transmission (Tx) et réception (Rx) alternée.
- Utilisation de 50 à 60% de la bande passante en raison des collisions et de la latence.
- Détection des collisions.

Ethernet Full Duplex :

- Permet l'émission et la réception simultanée.
- Nécessite l'utilisation d'un câble contenant 2 paires de fils et d'une connexion commutée entre les 2.
- Lors d'une communication, une communication point à point sans collision est créée.
- Utilisation de 100% de la bande passante.

La commutation LAN :

Problèmes des réseaux Ethernet :

- Les collisions.
- La latence des équipements réseaux.
- La remise de données de type broadcast.
- Afin d'optimiser les performances du réseau, la segmentation est nécessaire.

La segmentation LAN :

Le but est d'obtenir une réduction de la taille des domaines de collision afin d'économiser la bande passante disponible.

Elle permet un meilleur accès au média :

- Bande passante dédiée.
- Moins de conflits d'accès.
- Collisions réduites.

Le trafic est dirigé vers la station spécifié.

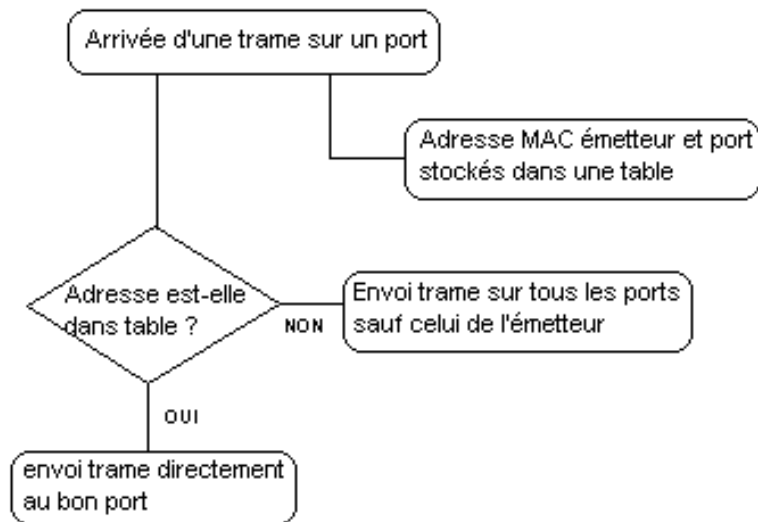
Les "broadcast" sont diffusé plus vite.

L'évolutivité reste un problème.

Définition de commutateur :

Le commutateur ou switch est un équipement qui connecte plusieurs segments dans un réseau informatique. Il permet de connecter plusieurs segments et de maintenir les connexions aussi longtemps que des données sont envoyées.

Fonctionnement :



Les différents types de commutation :

Commutation caractérisée par la façon de transmettre les paquets :

- Store and forward : Commutation où le commutateur attend d'avoir reçu toute la trame avant de la commuter.
- Cut Through : Dès que l'adresse de destination est connue, la trame commence à être commutée.
- Fragment Free : Les paquets sont passés à un débit fixé.
- Adaptive switching : mode automatique.

Commutation caractérisée en fonction de la bande passante attribuée à chaque port :

- Commutation symétrique : Les connexions commutées offrent la même bande passante à chaque port.
- Commutation asymétrique : Les connexions commutées offrent des bandes passantes différentes.

Le protocole Spanning Tree :

Son but est de calculer une topologie stable.

BPDU: Bridge Protocol Data Unit

BRIDGE TYPES:

- Root Bridge
- Designated Bridge

PORT TYPES:

- Root Port
- Designated Ports

PORT STATES:

- Blocking
- Listening
- Learning
- Forwarding
- Desactivating

Le protocole Spanning Tree, Paramètres de configurations :

Paramètres réseau:

- Hello interval
- Forward delay
- Max age
- Bridge priority (per bridge)

Paramètres liés au port:

- Port cost
- Port priority

Les LAN virtuels (VLAN) :

Définitions :

VLAN → Virtual Local Area Network, réseau local virtuel utilisant la technologie Ethernet pour regrouper les éléments du réseau sans se heurter à des contraintes physiques.

Il permet de constituer autant de réseaux logiques sur une seule infrastructure physique.

Avantages des VLAN :

Limiter les domaines de broadcast.

Garantir la sécurité.

Permettre la mobilité des utilisateurs.

Permet la gestion dynamique de la mobilité.

Permet a des utilisateurs géographiquement dispersés de partager des données.

Maintient la sécurité.

Conserve les domaines de broacast traditionnels des LANs.

Requiert une couche 3 pour la communication entre VLANs.

Différents types de VLAN :

VLAN de niveau 1 :

Appartenance par port:

- Association port-utilisateur, association port-segment.
- Aucun paquet ne quitte son domaine.
- Sécurité maximale entre VLANs .
- Facilement contrôlable dans le réseau.

Plusieurs VLAN par port ?

- Quand plusieurs clients sont derrière le même port.
- Nécessitent de rechercher les adresses.
- Pas de filtrage des broadcasts sur les segments partagés.
- Beaucoup d'administration.

VLAN de niveau 2 :

Appartenance par MAC:

- Filtrage requis.
– impact sur les performances.
- Echange des tables d'adresses des VLANs entre les commutateurs.
– overhead dû à l'administration.
- Indépendant de la localisation de la station.

VLAN de niveau 3 :

Appartenance par protocole:

- Apprentissage de la configuration
- Moins performante car analyse des informations

Appartenance par sous-réseau :

- Utilise les adresses IP
- Filtrage requis
– impact sur les performances
- Apprentissage de la configuration

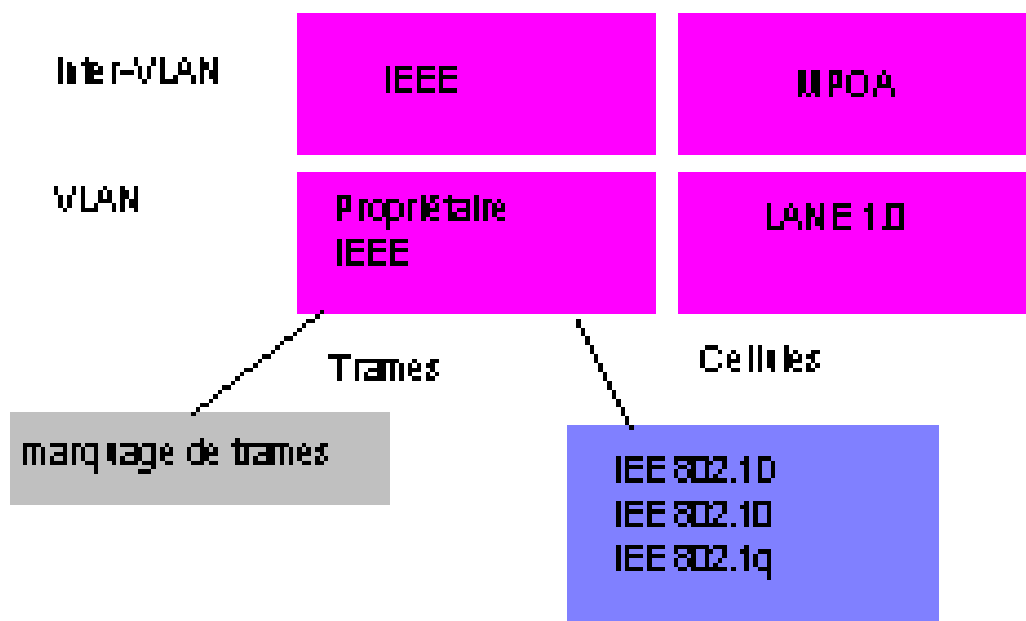
Les trunks :

Un trunk est une connexion physique unique sur laquelle on transmet le trafic de plusieurs réseaux virtuels.

Les trunks peuvent être utilisés :

- **entre deux commutateurs**
- **entre un commutateur et un hôte**
- **entre un commutateur et un routeur**

VLAN et standards :



VLAN et standards: IEEE 802.1D :

Présence de ponts transparents aux stations.

Toutes les décisions de routage, au niveau 2, sont exclusivement faites par les ponts.

Un pont maintient une base de données pour l'aiguillage des trames : « Forwarding Data Base(FDB) »

Auto apprentissage :

- à la mise en service : FDB vide.
 - réception d'une trame.
 - @ source et le port d'arrivée dans la FDB.
 - port de transmission inconnu : copie de la trame sur tous les autres ports.
 - tous les segments sont concernés.
- => convergence rapide du processus (spanning tree).

VLAN et standards: IEEE 802.10 :

IEEE 802.10 correspond aux besoins de segmentation du trafic et de sécurité dans les réseaux LAN/MAN.

– à la base, gestion des Groupes Fermés d'Abonnés.

Indépendance vis à vis des équipements intermédiaires.

Son utilisation semble être limitée à FDDI.

VLAN et standards: IEEE 802.1Q :

Standard VLAN pour des LAN commutés/bridgés.

Construit sur IEEE 802.1D et IEEE 802.1P.

Marquage des trames :

– Etiquette implicite

- Pas d'étiquette dans la trame.
- Appartenance d'une trame à un VLAN basée sur son contenu (@MAC,@IP) et le port.

– Etiquette explicite

- Etiquette dans la trame.

Supporte la priorisation.

Draft Standard P802.1Q/D11.

Méthodes de regroupement des utilisateurs en VLAN :

Le filtrage de trames : un examen de chaque trame permet d'élaborer pour chaque commutateur une table de filtrage afin de permettre de prendre les décisions appropriées.

L'étiquetage de trames : attribution d'un code d'identification VLAN unique à chaque trame (norme privilégiée par la norme IEEE802.1q).

Méthodes d'attribution des VLAN :

LAN virtuels statiques :

- Les ports du commutateur sont affectés à un LAN virtuel
 - Facilité d'administration.
 - Fonctionnent bien dans les réseaux où les déplacements sont contrôlés et gérés.
- LAN virtuels dynamiques :
 - Les ports des commutateurs peuvent automatiquement déterminer leur Vlan d'appartenance.
 - Filtrage basé sur les adresses MAC.

Les FIREWALL :

Définitions :

Un pare-feu (firewall en anglais), est un système physique ou logique servant de système de protection pour les ordinateurs.

Il comprend au minimum 2 interfaces:

- * une interface pour le réseau à protéger (réseau interne).
- * une interface pour le réseau externe.

Différents types de firewall :

- Firewall logiciel:
 - Installé directement sur l'ordinateur (firewall personnel).
 - Vérifie et indique sur quels ports les programmes accèdent à internet depuis votre pc.
 - Annonce les ports sur lesquels rentrent ou tentent de rentrer des applications sur votre pc.
- Firewall matériel:
 - Machine dédiée et intégrée (firewall d'entreprise).
 - Placé entre internet et le réseau.
 - Protège des différentes menaces internet.
 - Intègre les protections suivantes:
 - > Statefull packet inspection.
 - > Content filtering.

Fonctionnement :

Il contient un ensemble de règles prédéfinies permettant :

- Soit d'autoriser uniquement les communications ayant été explicitement autorisées:
Tout ce qui n'est pas explicitement autorisé est interdit.
- Soit d'empêcher les échanges qui ont été explicitement interdits.

Ses fonctions sont:

- Autoriser ou interdire l'ouverture d'un service.
- Utiliser un protocole.
- Autoriser ou bannir une adresse IP source/destination.
- Vérifier/inspecter la conformité du trafic.

Filtrage :

Filtrage des paquets :

Analyse des en-têtes des paquets échangés entre 2 machines en considérant les éléments suivants:

- Adresse IP de la machine émettrice.
- Adresse IP de la machine réceptrice.
- Type de paquet (TCP, UDP, IP, ICMP).
- Service ou port demandé.

Filtrage dynamique :

Basé sur l'inspection des couches 3 et 4 du modèle OSI.

Permet d'effectuer un suivi des transactions entre le client et le serveur.

Assure la bonne circulation des données de la session en cours.

Filtrage applicatif :

Filtre les communications application par application.

Vérifie le protocole applicatif utilisé, instructions, codification.

Se situe au niveau 7 du modèle OSI.

Firewall applicatif=passerelle applicative.

NAT (Network Address Translation) :

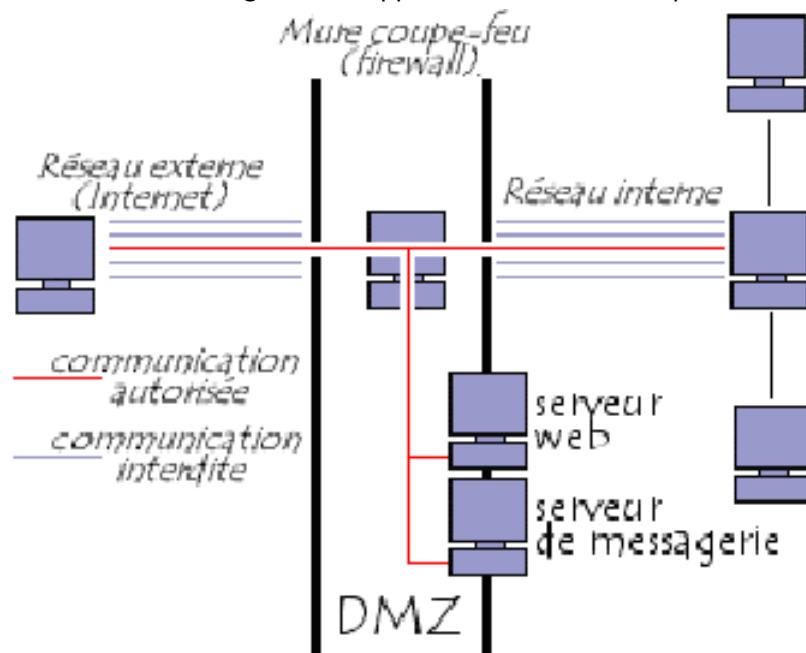
Permet de renuméroter les adresses source et destination.

Traduction dynamique ou statique des ports.

Table de correspondance adresse arrivée/adresse traduite.

DMZ (DeMilitarized Zone) :

Zone démilitarisée : zone isolée hébergeant des applications mises à la disposition du public.



Menaces contrées :

Attaques de type intrusion réseau.
Chevaux de Troie.
Vers.

Illustration sur firewall Netscreen :

Voir démonstration.

La cryptographie :

Définitions :

Processus de brouillage mathématique qui s'effectue par l'application de conventions secrètes (clés) et qui convertit une information intelligible en une information inintelligible. L'opération inverse ne peut être réalisée que par celui qui détient la clé.

Le fait de coder un message de façon à le rendre secret s'appelle *chiffrement*. La méthode inverse consistant à retrouver le message original, est appelée *déchiffrement*.

Confidentialité - Intégrité - Authentification :

Confidentialité:

Les informations doivent rester cachées aux personnes qui ne peuvent y accéder.

Intégrité:

Les données ne peuvent être modifiées.

Authentification:

Les informations reçues viennent bien de quelqu'un de qui on peut recevoir des informations.

Non répudiation:

Message reçu par destinataire alors que l'émetteur ne l'a pas envoyé.

Utilisation de cryptage par clé symétrique :

Définitions :

Les données sont cryptées sur l'ordinateur client et sur l'ordinateur serveur à l'aide de la même clé.

Il utilise la même clé pour crypter et décrypter les données.

Il est appelé également cryptage par clé secrète partagée.

Utilisé pour la confidentialité.

Fonctionnement :



Algorithmes utilisés :

- Le plus ancien: algorithme de César.
- DES (Data Encryption Standard).
- 3DES.
- AES (Advanced Encryption Standard).

Exemples d'utilisation :

Méthode très efficace pour crypter des gros volumes de données.

Il protège les données d'applications pour le système de fichiers cryptés (EFS, Encrypting File System).

Utilisé dans les clés de session pour les communications confidentielles.

IP Sec (Internet Protocol Security) et TLS (Transport Layer Security) utilisent des clés symétriques avec des algorithmes de cryptage standard pour crypter et décrypter des communications confidentielles entre un émetteur et un destinataire.

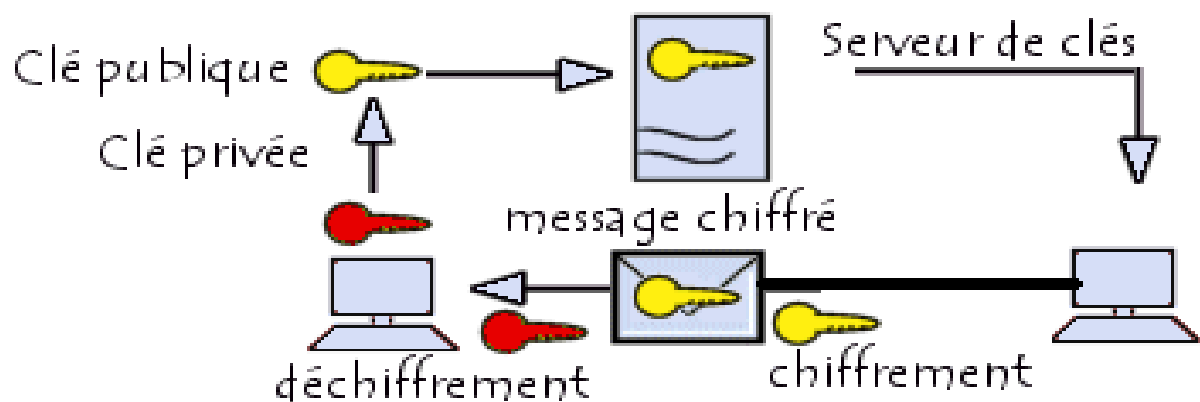
Utilisation de cryptage par clé publique :

Définitions :

Les données sont cryptées à l'aide d'une paire de clés. La première est utilisée pour le processus de cryptage et l'autre pour le processus de décryptage.

Il est appelé également cryptage par clé asymétrique.

Fonctionnement :



Caractéristiques :

Offre un meilleur niveau de sécurité que le cryptage par clé symétrique.

Utilisé pour la confidentialité.

Rien ne garantit que la clé est bien celle de l'utilisateur à qui elle est associée.

Utilisé pour:

- Cryptage des clés symétriques .
- Protection de clés symétriques stockées dans les documents protégés à l'aide du système EFS.
- S/MIME (Secure Multipurpose Internet Mail Extension).

Algorithmes utilisés :

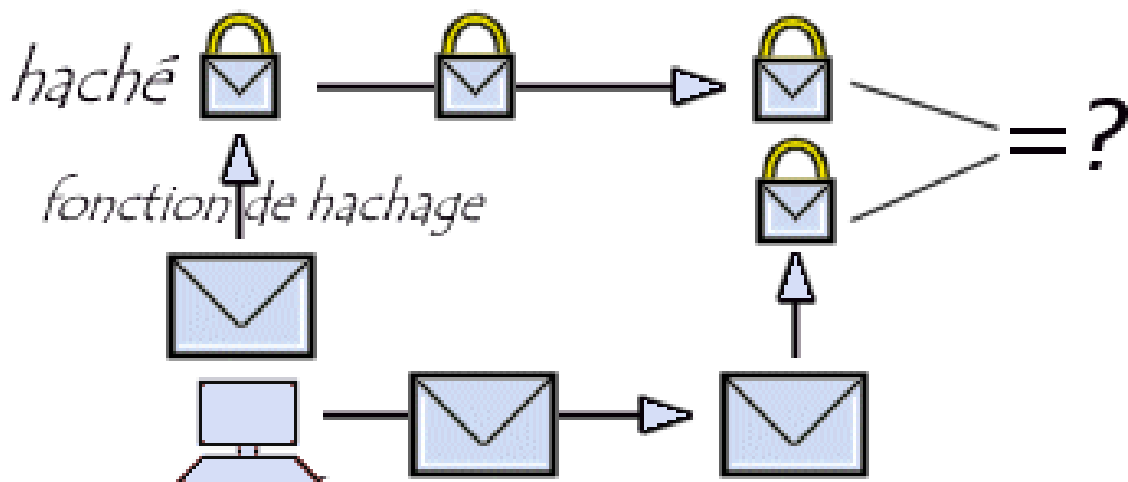
- RSA (Rivest Shamir et Adelman).
- DH (Diffie-Hellman).

Utilisation des fonctions de hachage :

Définition :

Une fonction de hachage permet d'obtenir un condensé d'un texte et doit être telle qu'elle associe un seul haché au texte en clair.

Fonctionnement :



Caractéristiques :

Utilisé pour vérifier l'intégrité des données.

Utilisé pour garantir, en plus, l'authentification du message => signature électronique.

Algorithmes utilisés :

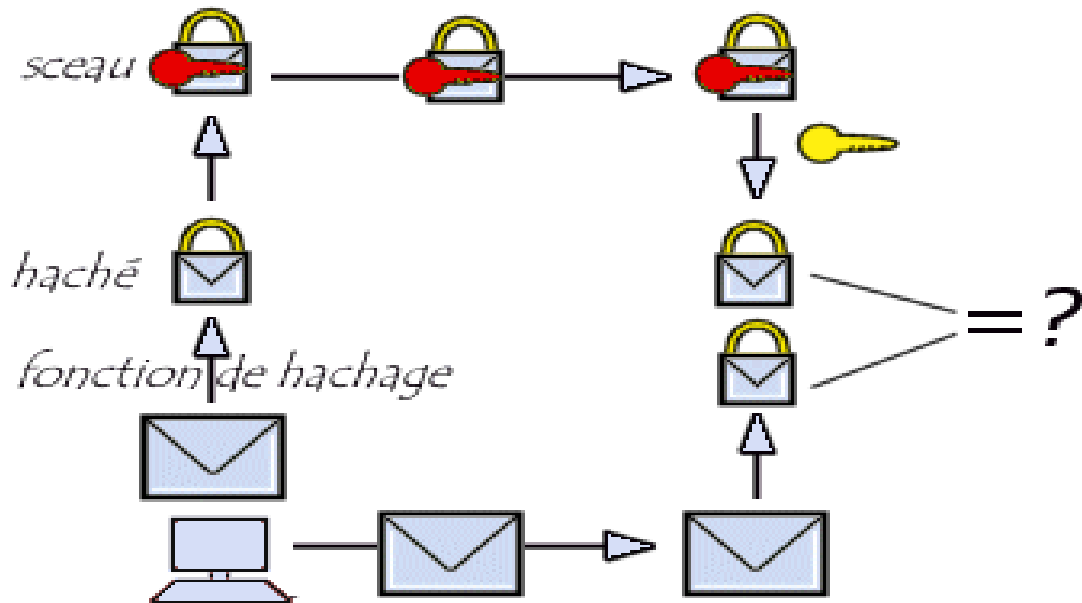
- MD5 (Message Digest 5) crée une empreinte digitale de 128 bits.
- SHA (Secure Hash Algorithm) crée une empreinte de 160 bits.

Utilisation des signatures numériques :

Définition :

Procédé permettant de garantir l'authenticité de l'expéditeur et de vérifier l'intégrité du message reçu.

Fonctionnement :



Caractéristiques :

Permet de garantir l'authentification et l'intégrité d'un message.

Utilise un cryptage à clé asymétrique et une fonction de hachage.

Exemple :

PGP (Pretty Good Privacy) : système de cryptographie hybride permettant de combiner les fonctionnalités de la cryptographie à clé publique et à clé secrète. En plus, les données sont hachées avant d'être transmises.

PKI: Public Key Infrastructure.

Utilisation des certificats :

Définition :

Un certificat permet d'associer une clé publique à une entité pour en assurer la validité.

Un certificat est une carte d'identité de la clé publique délivré par une autorité de certification (CA).

Caractéristiques :

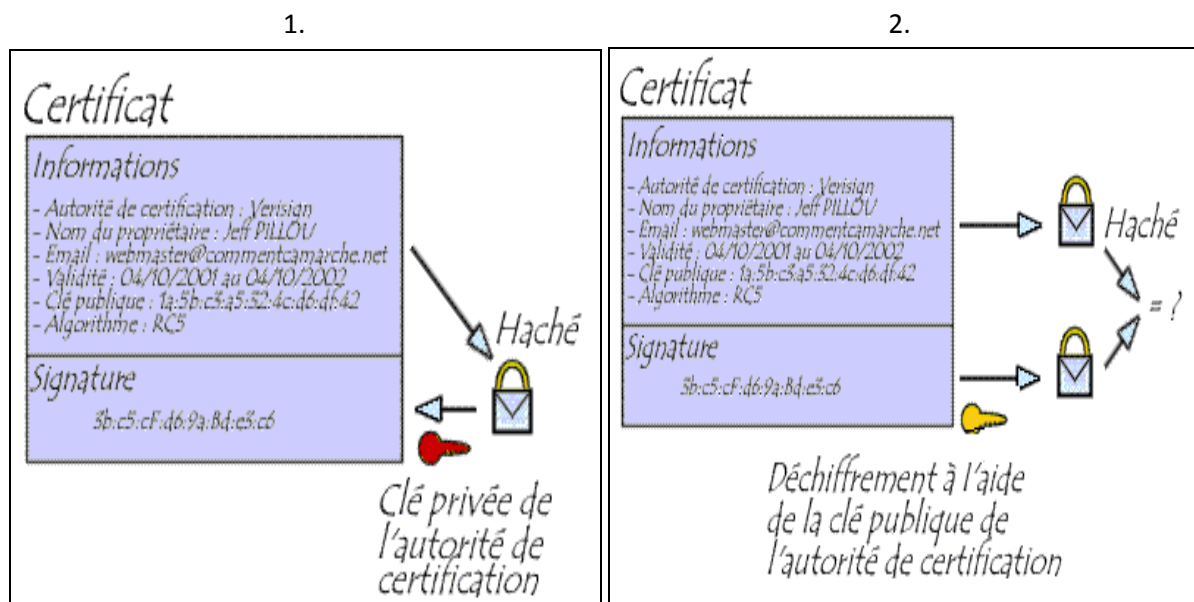
Les certificats sont des petits fichiers divisés en 2 parties:

- La partie contenant les informations
- La partie contenant la signature de l'autorité de certification

Leur structure (normalisée par le standard x.509) est la suivante:

- La version de X.509 à laquelle le certificat correspond ;
- Le numéro de série du certificat ;
- L'algorithme de chiffrement utilisé pour signer le certificat ;
- Le nom (DN, pour *Distinguished Name*) de l'autorité de certification émettrice ;
- La date de début de validité du certificat ;
- La date de fin de validité du certificat ;
- L'objet de l'utilisation de la clé publique ;
- La clé publique du propriétaire du certificat ;
- La signature de l'émetteur du certificat.

Fonctionnement :



Exemple :

Certificats PGP.

Autorité de certification sous Windows Server 2003.

Le VPN :

Définition :

VPN → Virtual Private Network.

Un VPN est une connexion logique et non physique entre 2 points et permet à 2 ordinateurs de communiquer via Internet, comme s'il existait entre eux un réseau privé dédié et sécurisé.

Un VPN repose sur un protocole de tunneling qui fait circuler les informations de façon cryptée d'un bout à l'autre du tunnel.

Utilités :

Créer une connexion sécurisée entre 2 réseaux privés.

Assurer un accès sécurisé au sein de structures réparties sur des grandes distances géographiques.

Accéder au réseau local à distance et de façon sécurisée pour les travailleurs itinérants.

Mettre en place un réseau partagé avec des partenaires.

Objectifs :

L'objectif principal est d'établir une connexion sécurisée entre 2 sites.

Les objectifs à réaliser sont :

- Confidentialité.
- Intégrité.
- Authentification.
- Unicité du paquet.

Principe de fonctionnement :

Une session VPN se déroule de la façon suivante :

1. L'utilisateur distant demande une connexion VPN.
2. La machine destinataire reçoit la requête et établit un tunnel temporaire.
3. L'ordinateur et la machine destinataire partagent leurs clés (phase 1) et le réseau de destination définit comment le trafic va être encapsulé dans les enveloppes cryptées.
4. La machine destinataire envoie un test à l'utilisateur distant pour l'authentifier.
5. L'utilisateur distant utilise son ID utilisateur et son mot de passe et tout ce qui est requis pour authentifier le réseau de destination.
6. Le réseau de destination vérifie l'utilisateur distant et assigne une adresse IP temporaire à la machine distante.
7. Le canal de communication crypté est établi (Phase 2).

Protocoles utilisés pour réaliser une connexion VPN :

But des protocoles :

Construire un chemin virtuel après avoir identifié l'émetteur et le récepteur.

Chiffrer les données et les acheminer en utilisant le chemin virtuel.

Sécuriser les données lorsqu'elles traversent le réseau public.

Encapsuler les données à l'émission en ajoutant un entête, l'envoyer et décapsuler les données à la réception.

Protocole de niveau 2: PPTP (Point to Point Tunneling Protocol) :

Définit par la RFC 2637.

Utilise une connexion PPP à travers un réseau IP en créant un VPN.

Permet le cryptage des données, leur compression, l'authentification et le chiffrement avec des protocoles supplémentaires.

Crée des paquets sous le protocole PPP et les encapsule dans des datagrammes IP.

Est caractérisé par une initialisation du client, une connexion de contrôle entre le client et le serveur ainsi que par la clôture du tunnel par le serveur.

Protocole de niveau 2: L2TP (Layer Two Tunneling Protocol) :

Définit par la RFC 2661.

Evolution du protocole PPTP.

Permet l'encapsulation des paquets PPP au niveau des couches 2 et 3.

Contient des paquets d'informations encapsulés dans des paquets PPP pour les sessions utilisateurs servant pour le transport de L2TP.

Contient une signalisation qui contrôle l'information et qui est encapsulée dans des paquets UDP.

Permet l'authentification, la compression et est basé sur IP Sec pour le cryptage.

Protocole de niveau 3: IP Sec (IP Security Protocol) :

Description :

Définit par la RFC 2401.

Protocole qui vise à sécuriser l'échange des données au niveau de la couche réseau.

Permet de chiffrer puis d'encapsuler dans une entête IP des données pour les envoyer à travers un inter-réseau.

Il est basé sur 3 mécanismes:

- AH pour assurer intégrité, authenticité des datagrammes IP.
- ESP pour assurer le cryptage et l'authentification des données.

SA pour définir l'échange de clé et les paramètres de sécurité.

Différents modes de fonctionnement :

Mode transport: permet une protection aux protocoles de niveau supérieur (TCP, UDP) mais ne modifie pas la partie IP.

Mode tunnel: permet d'encapsuler la totalité des datagrammes IP dans d'autres datagrammes IP dont le contenu est protégé.

Protocole AH :

Authentication Header.

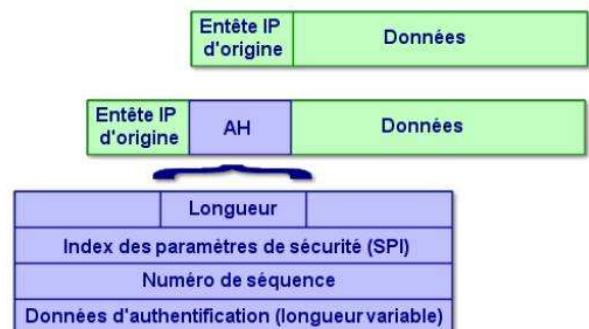
Définit par la RFC 2402.

Il garantit:

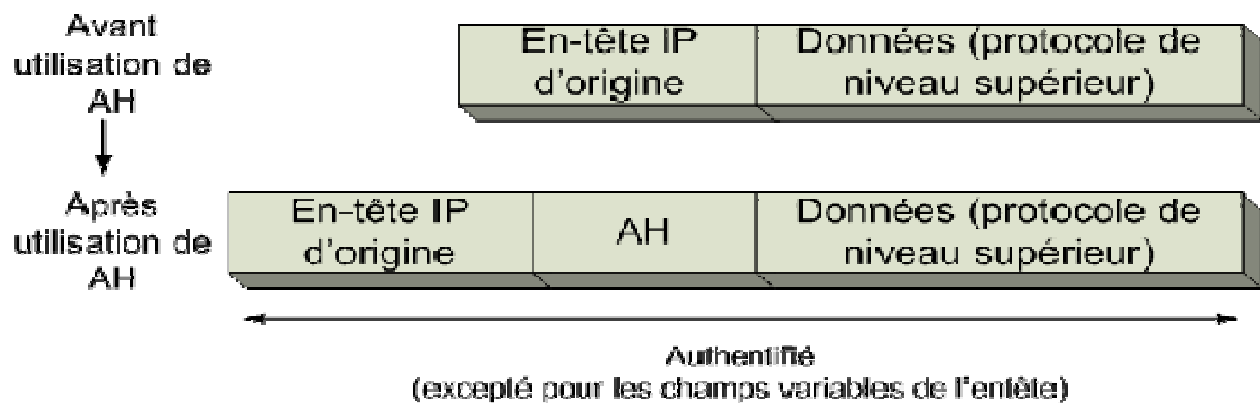
- l'authentification des paquets IP
- L'intégrité des champs IP non modifiés pendant le routage
- L'unicité

Il n'assure pas la confidentialité.

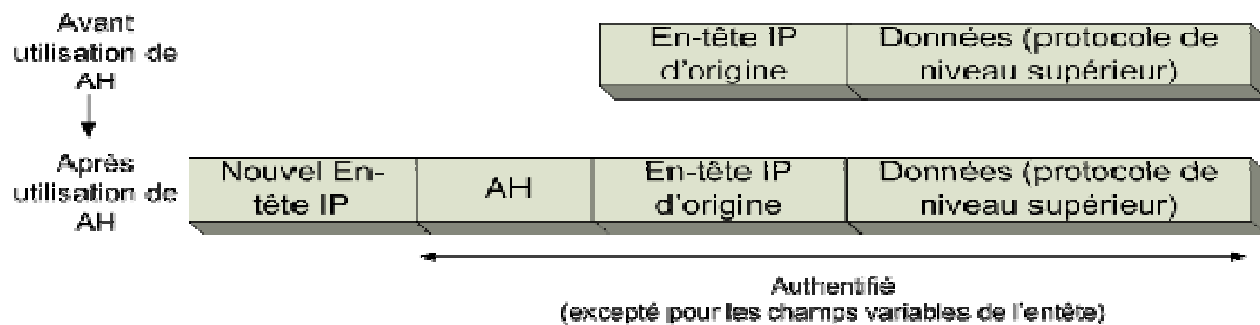
Il peut utiliser le mode transport et le mode tunnel.



Mode transport



Mode tunnel



Protocole ESP (Encapsulating Security Payload):

Défini par la RFC 2406.

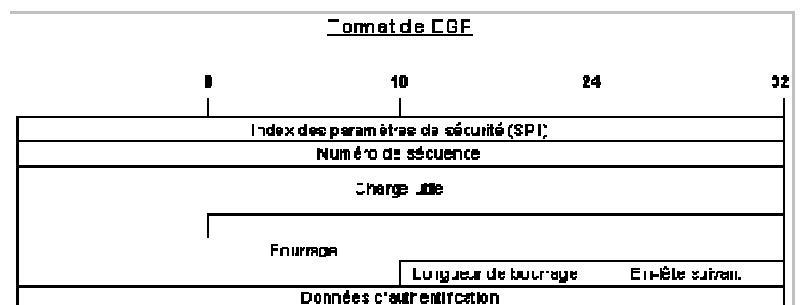
Il garantit:

- la confidentialité des données
- l'authenticité des datagrammes IP
- l'intégrité des données
- l'unicité

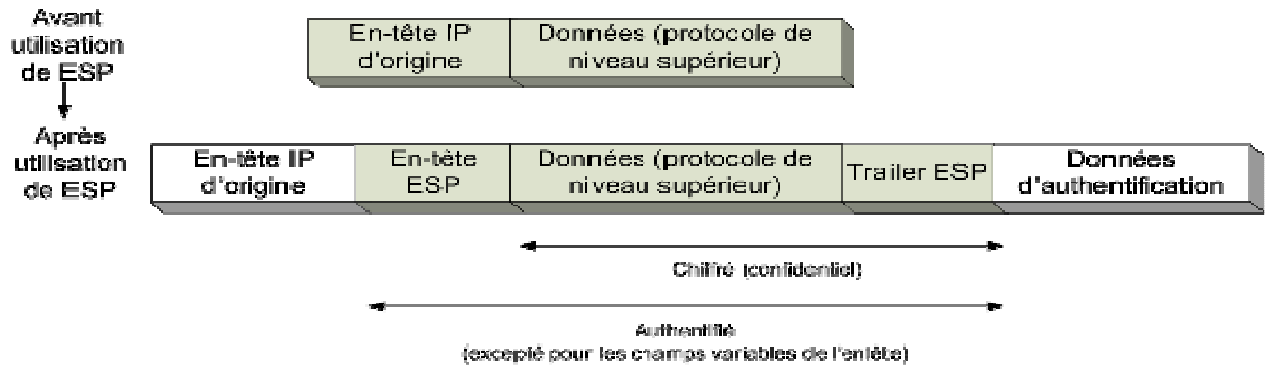
Il ne protège que les données des

datagrammes pas les entêtes.

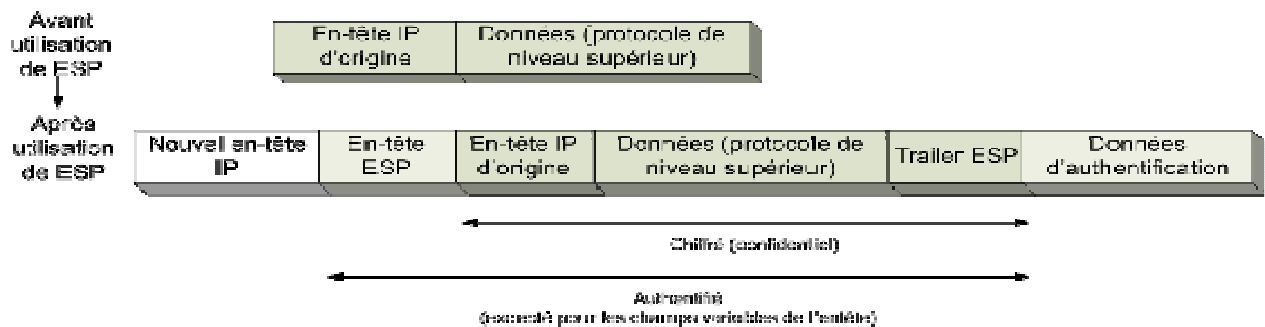
Il peut utiliser le mode transport et tunnel.



Mode transport



Mode tunnel



Protocole IKE (Internet Key Exchange):

Définit dans la RFC 2409.

Système développé pour IP Sec qui permet de fournir des mécanismes d'authentification et d'échange de clés.

Il permet une gestion dynamique des clés IP Sec (génération, distribution, stockage et suppression des clés).

Il a pour but dans sa première phase de construire un premier tunnel sécurisé entre les 2 hôtes (tunnel IKE). Ce tunnel est utilisé pour gérer les tunnels IP Sec (négociation des SA et leur mise à jour) constituant la deuxième phase du protocole IKE.

Etablissement d'un tunnel IP Sec :

Phase 1:

- Echange de clés
- Création d'une clé qui va permettre de générer 3 autres clés (authentification, chiffrement et pour phase 2) qui servent à la création du tunnel IKE sécurisé entre les hôtes.

Phase 2:

- Etablissement des associations de sécurité et des clés de session (générées à partir clé de phase 1), définition des modes de cryptage.

Quand phase 2 est réalisée avec succès, les données peuvent circuler via le tunnel IP Sec.

Implémentation :

Logicielle => Démonstration.

Matérielle : pare-feu, routeur crypté.