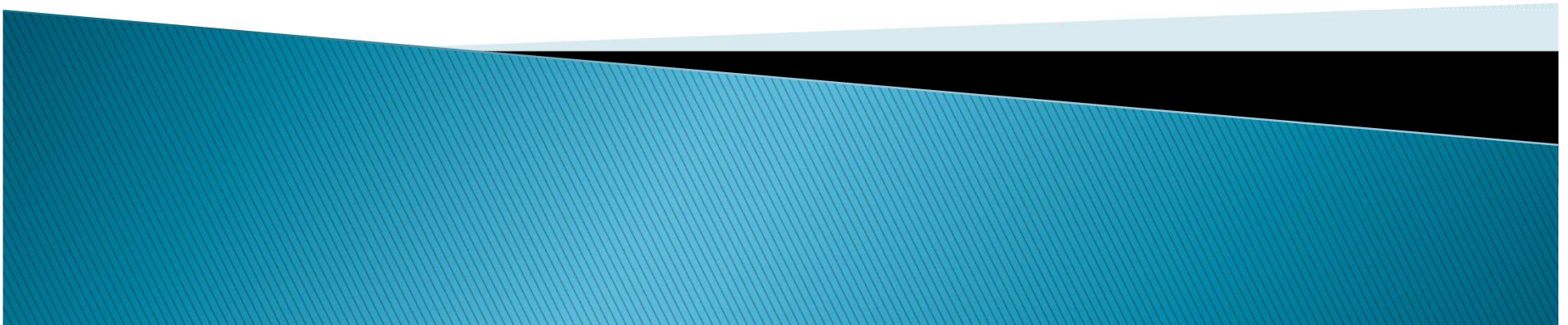


VPN–Virtual Private Network

Protocoles et services



▶ Introduction

- Présentation
- Principaux protocoles
 - PPTP
 - GRE
 - L2TP
 - IPSec
 - MPLS
 - SSL
 - Comparatif
- Démonstration



▶ Conclusion

Présentation



Utilisation d'un VPN

- ▶ Besoins d'une entreprise
 - Avoir accès a un réseau local de n'importe où
 - Relier deux réseaux (ex: Supinfo Paris à Supinfo Lille).
- ▶ Alternative aux lignes spécialisées
 - Coût beaucoup moins important



Tunneling

- ▶ Le tunneling est le fait de créer un « tunnel » entre deux points.



Principaux protocoles

PPTP

GRE

L2TP

IPSec

MPLS

SSL



PPTP

(Point-to-point tunneling protocol)

- ▶ Protocole permettant l'encryptage et la compression des données défini dans la Rfc 2637.
- ▶ Il ouvre deux canaux:
 - un canal de contrôle connexion TCP sur le port 1723 du serveur.
 - un canal de données transportant le trafic du réseau privé et utilisant l'IP protocole 47, le protocole Generic Routing Encapsulation (GRE).
- ▶ Implémenté par Microsoft et intégré à Windows depuis Windows 95.



PPTP principe

- ▶ Établissement d'une connexion PPTP :
 - une initialisation du client
 - une connexion de contrôle entre le client et le serveur
 - clôture du tunnel par le serveur
- ▶ Création des paquets sous le protocole Ppp(RFC 1661) et encapsulation dans des datagrammes IP.



PPTP : sécurité

- ▶ Authentification grâce au Ms-Chap ou Pap.
Ms-Chapv1 non fiable corrigé Ms-Chapv2
- ▶ Chiffrage des données avec le protocole Mppe (Microsoft Point-to-Point Encryption)
- ▶ Compression des données avec le protocole Mppc (Microsoft Point-to-Point Compression)



GRE

(Generic Routing Encapsulation)

- ▶ Le GRE est souvent utilisé avec le pptp dans un VPN.
- ▶ Ce Protocole à pour rôle d'encapsuler n'importe quel paquet de la couche réseau (couche 3) définit dans la RFC1701.
- ▶ Pas de maintien d'état => pas d'informations d'état ou de disponibilité de la terminaison distante.



L2TP

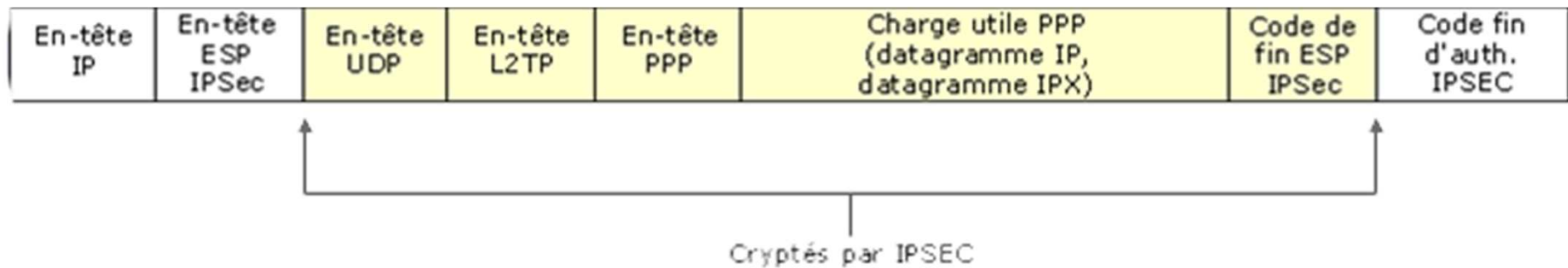
(Layer 2 Tunneling Protocol)

- ▶ Convergence des protocoles PPTP et L2F(RFC2341)
=> Rfc 2661.
- ▶ Développement collaboratif : Cisco, Microsoft, Ascend, 3Com,...
- ▶ Intégration de IPSec



L2TP

- ▶ Vue du paquet



IPSec

Définition :

développé pour:

- permettre de garantir l'authentification
- l'intégrité
- le contrôle d'accès et la confidentialité des données.

IPSec = formatage de trame permettant le chiffrement des données au niveau IP.



- Confidentialité des données
- Intégrité des données
- Authentification de l'origine des données
- Anti-rejeu



IPsec

- ▶ Compatible avec l'ipv6 et l'ipv4
- ▶ Pour sécurisé IPsec utilise deux protocoles
 - AH (Authentication Header)
 - ESP (Encapsuling Security Payload)



Le protocole AH

- ▶ Ajout d'une entête sur le paquet IP
- ▶ Utilise les algorithmes: SHA1 /256,MD5,AES-XCBC
- ▶ Assure :
 - L'authentification de l'émetteur
 - Anti-rejeu
 - L'intégrité des données

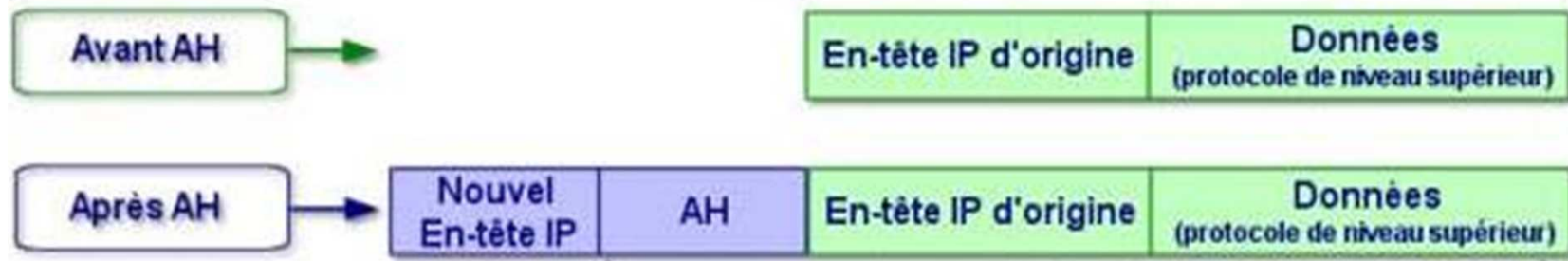


Les différents mode d'utilisation d'AH

Mode Transport



Mode Tunnel



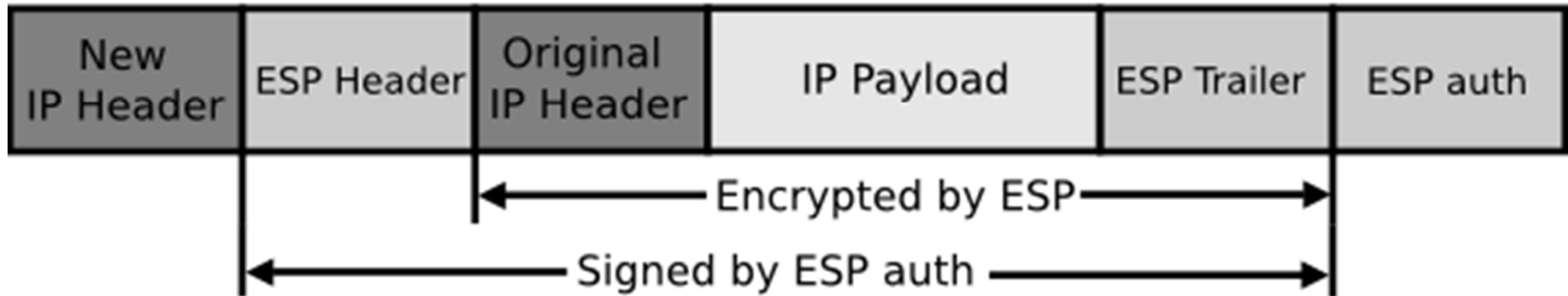
Le protocole ESP

- ▶ Il encapsule et crypte le paquet IP
- ▶ Algorithmes utilisés pour le cryptage: AES, 3DES, DES
- ▶ Il assure :
 - La confidentialité des paquets
 - L'authentification (optionnel)
 - L'anti-rejeu
 - L'Intégrité des données



Le protocole ESP

IPSec Tunnel mode (ESP)



MPLS

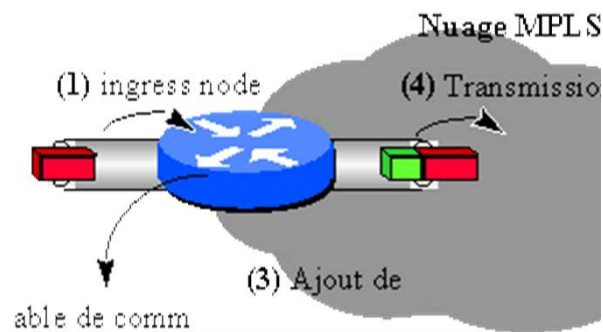
(MultiProtocol Label Switching)

- ▶ Le MPLS est un mécanisme de transport de donnée qui opère sur la couche données (2).
- ▶ Il permet de transporté n'importe quel protocole aussi bien en IPv4 et IPv6.
- ▶ Il utilise un principe de label
 - Exemple:
 - "Si je reçois un paquet avec tel label sur telle interface, je met tel label et je l'envoie sur telle interface"
- ▶ RFC3031.

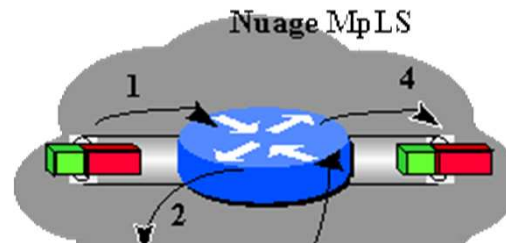


Exemple Label (étiquette)

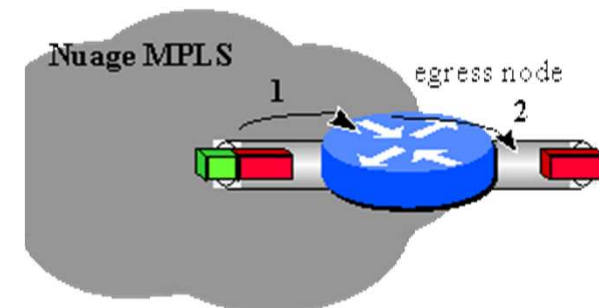
Routeur en entrée



Routeur
intermédiaire



Routeur de
sortie



SSL (Secure Socket Layer)

- ▶ C'est un protocole de sécurisation des échanges, développé par Netscape. Pris en charge par les navigateurs depuis 1994.

- ▶ Il permet :

- La confidentialité
- L'intégrité
- L'authentification



Comparatif

Protocole	Avantages	Inconvénients
PPTP	-Très répandu	-Peu fiable -Performance faible
L2TP	- Mobilité	- L'overHead (durée de traitement)
IPSec	-Confidentialité/Intégrité des données	-Pas d'authentification des utilisateurs -Pas de QoS -Lourdeur des opérations
MPLS	-Rapidité	-Manque d'homogénéité des équipements
SSL	- Déploiement	- Maîtrise client

Vue de principe de fonctionnement



Liens

- ▶ RFC protocoles => <http://tools.ietf.org/rfc/index>
- ▶ Wikipédia => <http://fr.wikipedia.org/wiki/Portail:Informatique>
- ▶ Commentcamarche => <http://www.commentcamarche.net/>
- ▶ Sécurité info => <http://www.securiteinfo.com/>
- ▶ Cisco => http://www.cisco.com/web/EA/cisco_library/cisco_library_online.html
- ▶ Frameip => <http://frameip.com/>



