Haute école d'ingénierie et d'architecture Fribourg
Hochschule für Technik und Architektur Freiburg

Réseaux IP

742. Virtual Private Networks (VPN)

Hes·so FRIBOURG FREIBURG
Haute Ecole Spécialisée de Suisse occidentale
Fachhochschule Westschweiz
University of Applied Sciences and Arts Western Switzerland

Réseaux IP

742. *Virtual Private Networks - VPNs*

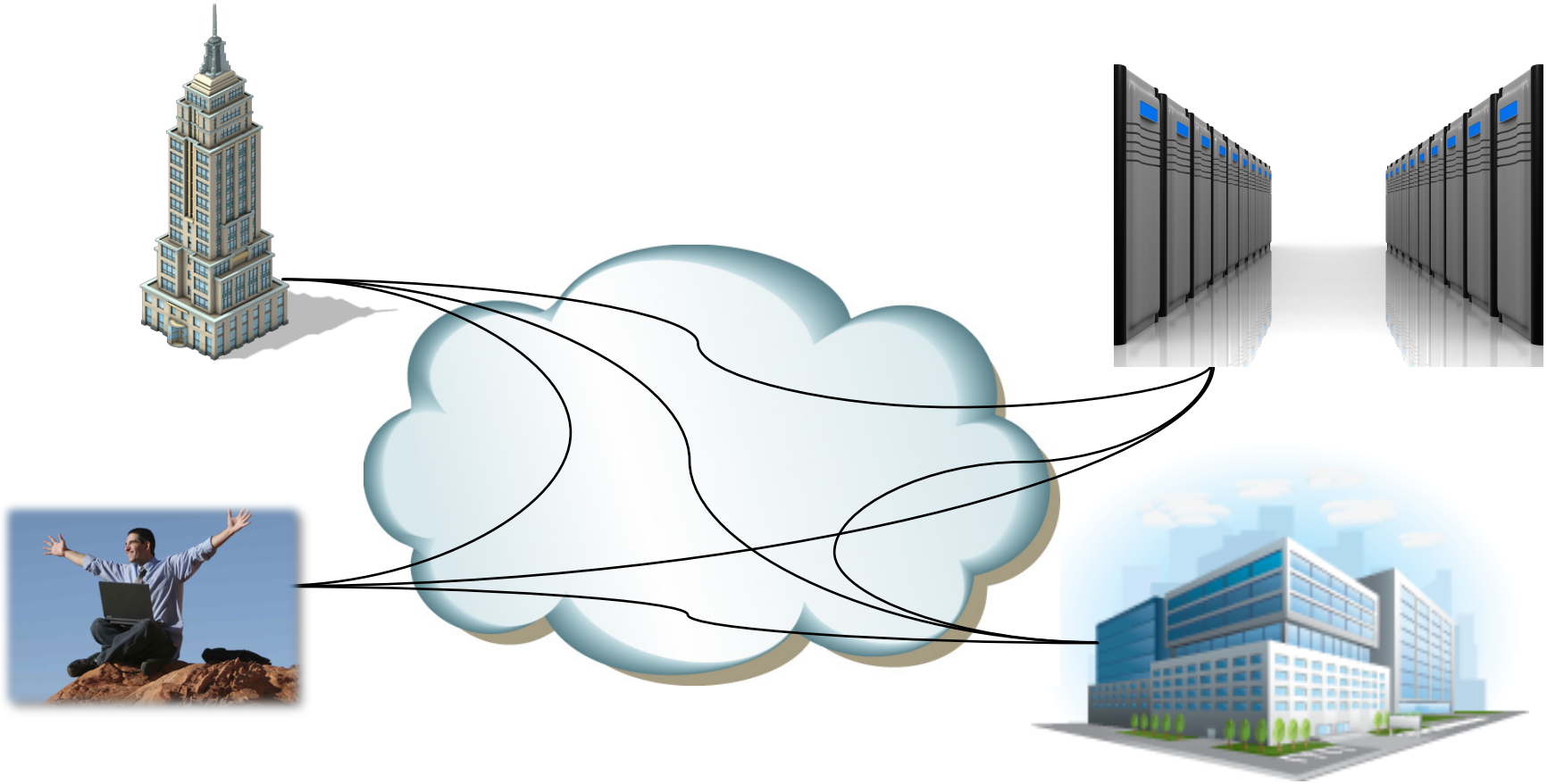
Introduction, Motivations, Technologies et protocoles, Evolution, GRE, L2TP, PPTP, IPSec

Références:

- Cours IntSec1 (Hochschule für Technik, Rapperswyl, Dr Andreas Steffen)
- Cisco Networking Academy (http://www.cisco-academy.ch)
- Les Réseaux, Edition 2011 (Ed. Eyrolles, Pujolle)

VPN (Virtual Private Network)

Définition: Un VPN est un réseau informatique **privé** construit sur une infrastructure partagée de couche 2 ou 3 (Dial-up, WAN, Internet ou *backbone* IP)



Fonctionnement des VPNs

Un VPN fonctionne à la couche IP au moyen de tunnels encryptés ou non, qui "émulent" des circuits

Avantages:

- ↗ Important potentiel d'économies par rapport à un réseau WAN traditionnel – moins de connexions, moins de protocoles différents
- ↗ Grande souplesse d'accès – facile d'ajouter des connexions
- ↗ Pas de limitations du nombre de sites grâce à la disponibilité d'Internet et la nature en maillage complet d'IP
- ↗ Sécurité notablement améliorée par rapport à un accès « *dial-in* » non-sécurisé

Risques:

- ? Fiabilité parfois difficile à quantifier
- ? Sécurité doit être garantie au moyen d'un chiffrage approprié
- ? La qualité de service et les performances sont parfois difficiles à garantir

Motivations des VPNs

- Un éclatement et une internationalisation toujours plus grand des entreprises (*intranet*)
- La mobilité des employés et le travail à la maison/sur la route (*remote access*)
- La dynamique des alliances et des partenariats (*extranet*)
- La perspective d'économies substantielles comparé à une solution WAN traditionnelle
- La perspective d'augmenter la quantité et la qualité des échanges d'information au sein d'une entreprise et avec les partenaires (fournisseurs, clients, partenaires, consortiums)
- Les perspectives du commerce électronique (en particulier pour les aspects de sécurité)
- L'expansion rapide des applications basées sur IP

Réalisation d'un VPN

On distingue actuellement :

- Les solutions VPN proposées par un **opérateur** ou ISP (*Internet Service provider*) utilisent des protocoles comme MPLS (*Multi Protocol Label Switching*) pour isoler et sécuriser les connexions appartenant à un même VPN.

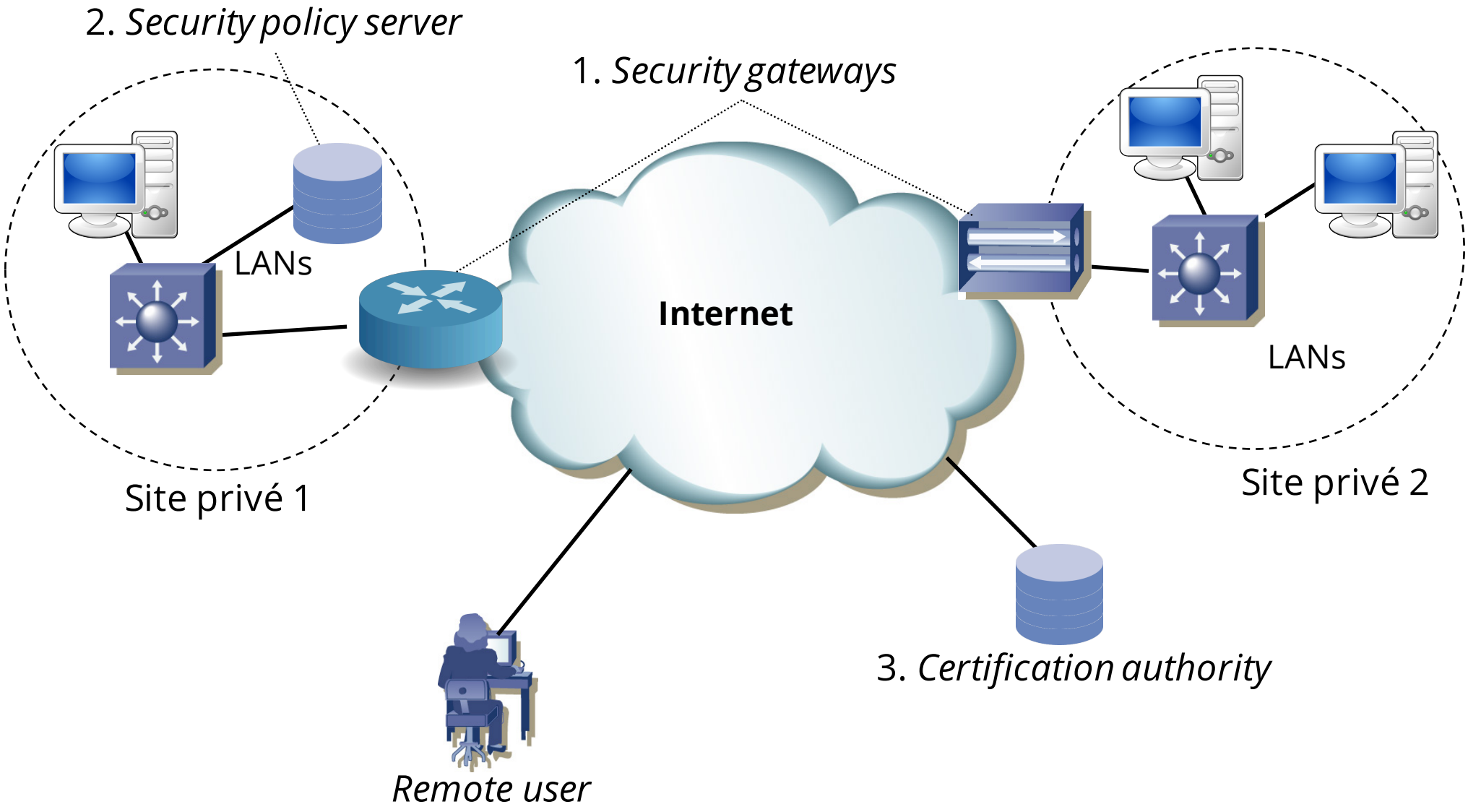
- Les solutions VPN appelées **implementations client** sont réalisées au moyen d'équipements chez les clients (*firewalls*, *routeurs*, PCs, ou serveurs). Ce VPN fonctionne alors sur un Internet transparent fourni par un opérateur ou ISP.

Solutions opérateur: Fiabilité, Performances, et Sécurité

Les performances d'un VPN sont réglées au-travers d'un SLA (*Service Level Agreement*) qui spécifie le service délivré par un ISP. Les critères généralement traités sont:

- **Fiabilité**: les ISPs investissent de très grands moyens de façon à garantir la disponibilité des connexions sur Internet
- **Qualité de service**: plusieurs initiatives sont en cours pour offrir sur Internet des qualités de service permettant le support de multi-services sur Internet et les réseaux IP. On citera en particulier l'initiative DiffServ (RFC 2474 et 2475) qui préconise l'emploi des champs de type de service dans les paquets IP et un modèle "*hop-by-hop*" et les technologies MPLS. De nombreuses inconnues quant au comportement à grande échelle de ces modèles subsistent néanmoins. L'aspect qualité de service concerne aussi bien la garantie des services sur le *backbone* que le partage de la capacité entre les utilisateurs d'un même VPN
- **Sécurité**: le domaine le plus développé avec en particulier le standard IETF IPSec (RFC 1825) qui définit des protocoles robustes d'établissement, d'authentification et de chiffrage pour des tunnels IP au-travers d'un réseau IP public (compatible avec les protocoles de tunnels de couche 2).

Composants d'un VPN



Composants d'un VPN

1. **Security gateway**. Equipement indépendant ou partie d'un autre équipement (routeur, *firewall*):
   - Empêche les accès non-autorisés dans le réseau privé
   - Etablit et libère les tunnels
   - S'occupe du chiffrage et déchiffrage

2. **Security policy server**. Identifie (*Authentification*) les utilisateurs et gère les listes d'accès.

3. **Certification authority**. Si la taille du VPN augmente et des partenaires extérieurs sont connectés, la gestion des clés de chiffrement devient une tâche considérable qui doit être gérée par une autorité extérieure.

Les protocoles “VPN” (1)

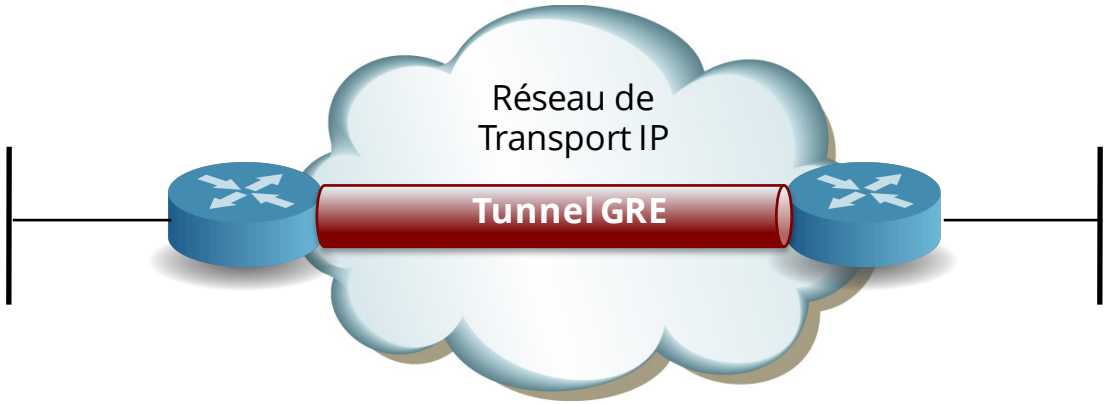
Plusieurs protocoles ont été développé pour créer des VPN, que l’on peut classer selon les couches du modèle OSI à laquelle ils opèrent:

- **Couche 2:**
  - **Microsoft Point-to-Point Encryption (MPPE):** Une manière de convertir des paquets PPP dans une forme encryptée. MPPE utilise l’algorithme RSA RC4 pour garantir la confidentialité des données
  - **Layer 2 Forwarding (L2F):** RFC 2341. Un protocole d’encapsulation (*tunneling*) développé par Cisco qui permit de créer un réseau privé d’accès vers une entreprise (*Virtual Private Dialup Network/VPDN*)
  - **Point-to-Point Protocol (PPTP):** Un protocole développé par Microsoft pour permettre le transfer sécurisé de donnée d’un client vers une entreprise
  - **Layer 2 Tunneling Protocol (L2TP):** Un protocole d’encapsulation développé par Cisco et Microsoft permettant la création d’un réseau privé d’accès (VPDN), L2TP est une extension du protocole PPP dans le cadre des VPN

Les protocoles “VPN” (2)

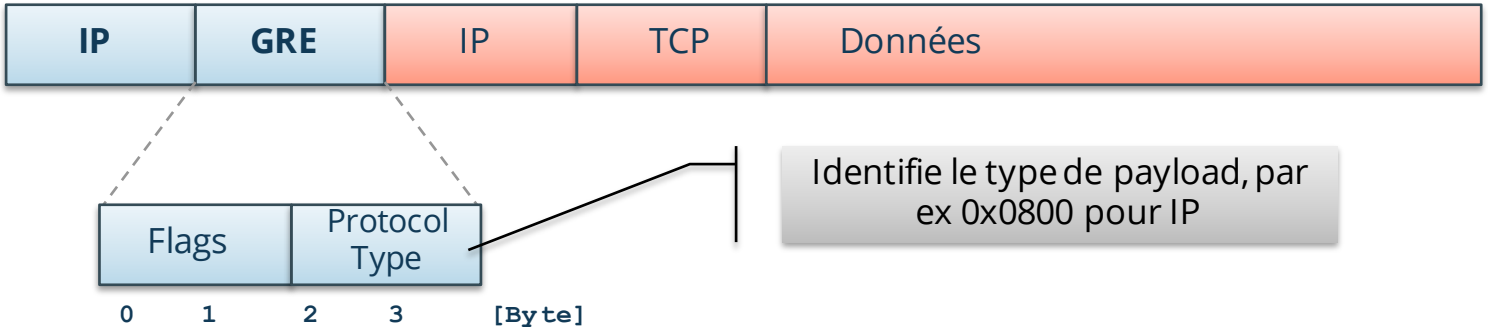
- **Couche 3:**
  - **IPSec**: IPSec suit les standard promulgué par l’Internet Engineering Task Force (IETF)
  - **Generic Routing Encapsulation (GRE):** Un protocole d’encapsulation (*tunneling*) développé par Cisco qui encapsule toute une variété de protocole dans des paquets IP (par exemple: IP dans IP, IPX dans IP, …)

Generic Routing Encapsulation – GRE (1)



- GRE est un protocole d'encapsulation de couche 3 :
  - Encapsule une large variété de protocole dans un tunnel IP
  - Crée une liaison virtuelle point-à-point au dessus d'un réseau de transport IP
  - Utilise IP pour le transport
  - Utilise un entête additionnel pour supporter d'autres protocoles de couche 3 comme « passager », comme par exemple IP, IPv6, IPX, AppleTalk, etc.
  - Supporte le broadcast et le multicast

Entête GRE (1)



- GRE est un protocole sans état (pas de contrôle de flux).
- GRE n'offre aucune sécurité (pas de confidentialité, pas d'authenfication des données, pas de contrôle d'intégrité).
- GRE utilise un *overhead* de 24 octets par défaut (20 octets pour le nouvel entête IP et 4 octets pour l'entête GRE).

Entête GRE (2)

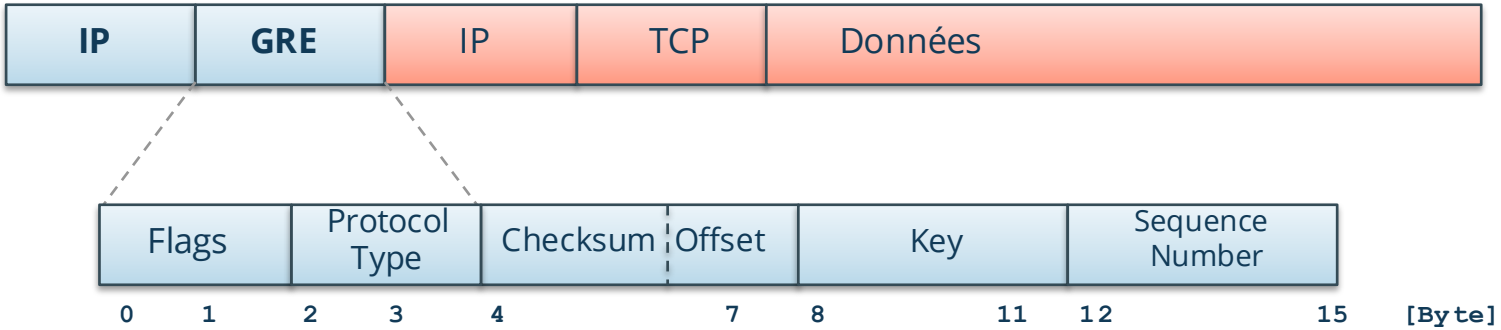
Les fanions (flags) sont encodés dans les deux premiers octets:

- **Checksum Present (bit 0):** Le champ optionnel *Checksum* est présent dans l'entête uniquement si ce bit a la valeur 1.
- **Key Present (bit 2):** Le champ optionnel *Key* est présent dans l'entête uniquement si ce bit a la valeur 1. Utilisé pour l'authentification des partenaires.
- **Sequence Number Present (bit 3):** Le champ optionnel *Sequence Number* est présent dans l'entête uniquement si ce bit a la valeur 1.
- **Version Number (bits 13–15):** Indique le numéro de version de l'implémentation GRE. Une valeur de 0 est typiquement utilisée pour une implémentation GRE de base. Point-to-Point Tunneling Protocol (PPTP) utilise la Version 1

Les deux octets suivants contiennent le type de protocole transporté:

- **Protocol Type:** Contient le type de protocole transporté dans le tunnel. En général, la valeur correspond au champ protocol de l'entête Ethernet. Par exemple 0x0800 opour IP.

Entête GRE (3)



- GRE contient de manière optionnelle les champs suivants:
  - Checksum: détection des paquets corrompus
  - Key: utilisé pour une authentification de base (en clair) ou pour identifier des tunnels utilisant les mêmes adresses de source et de destination (tunnels parallèles)
  - Sequence Number : Détection de l'ordre des paquets