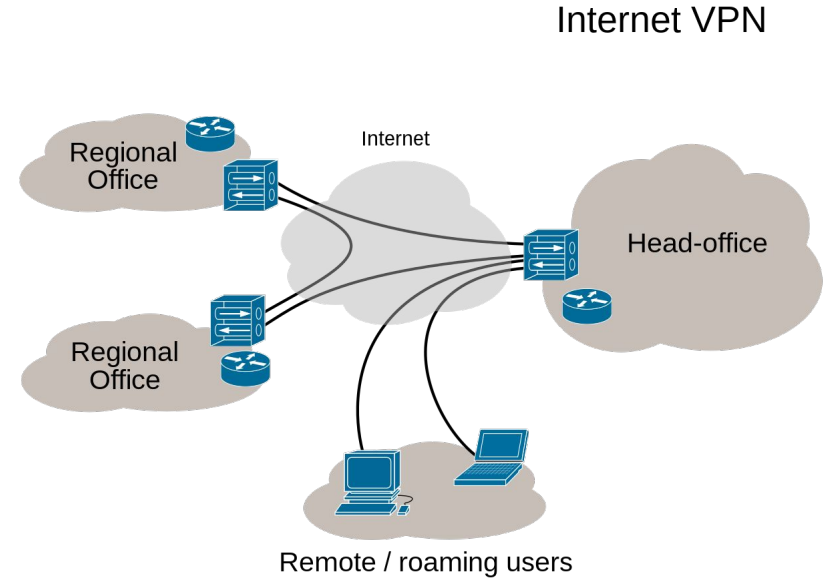




Virtual Private Networks

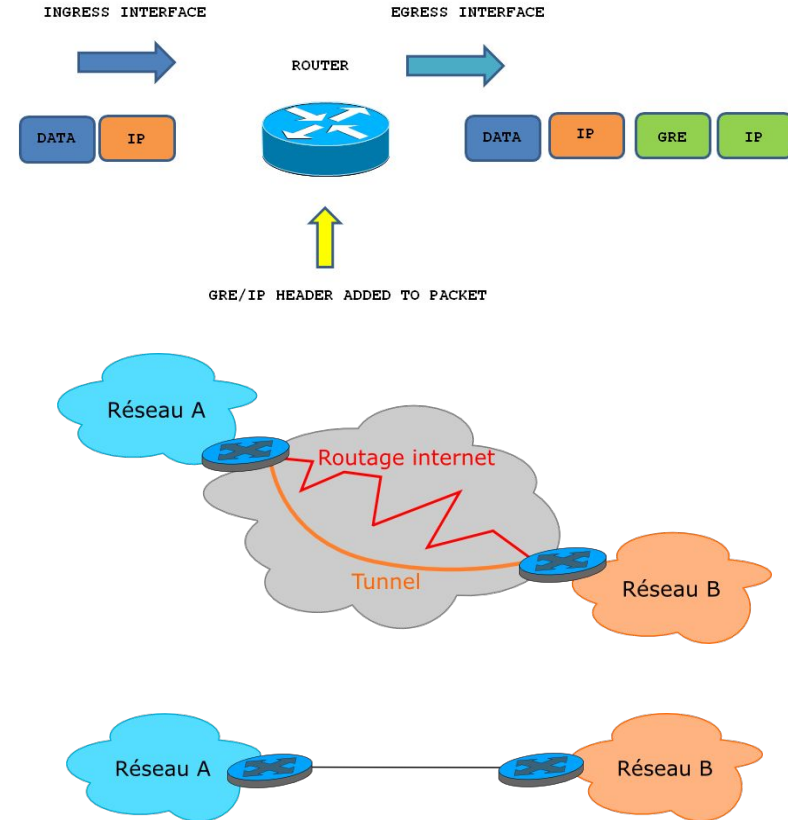
# Principe du VPN

- Réseau privé virtuel (VPN) permet de
  - Simuler un réseau privé sur une infrastructure à accès partagé (Internet)
  - Interconnecter de réseaux répartis sur de grandes distances géographiques
  - Fournir un accès sécurisé au réseau de l'entreprise
- Repose sur un protocole appelé « **protocole de tunneling** »
  - Consiste à construire un chemin virtuel entre l'émetteur et le destinataire
  - Permet de faire circuler les informations de façon sécurisée d'un bout à l'autre du tunnel



# Exemple d'un tunnel

- Encapsulation d'un protocole dans un autre protocole de même niveau (IP dans IP)
- Première couche IP circule normalement sur l'internet et transporte une seconde couche IP
- Sur la première couche tout va se passer comme si les deux routeurs communiquent directement
- Grâce à ce tunnel, tout nœud du réseau A pourra communiquer avec tout nœud du réseau B, les deux réseaux étant construits avec des adresses IP **privées**



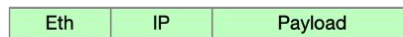
# Pourquoi faire du VPN?

- Interconnection des réseaux distants
- Connection sécurisé au réseau de l'entreprise
- Communications sécurisés
- Faire du L2 au dessus de L3
- Changer d'ip pour être identifié dans un autre pays
- Forcer le passage dans un équipement de sécurité
- ...

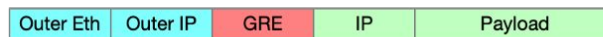
# GRE (Generic Routing Encapsulation)

- Protocole générique de tunneling
- Développé par Cisco
- Conçu pour encapsuler
  - IP (*gretun*)
  - Ethernet (*gretap*)
- N'implémente pas de chiffrement ou d'authentification
  - doit être utilisé avec IPsec
- Est sans état

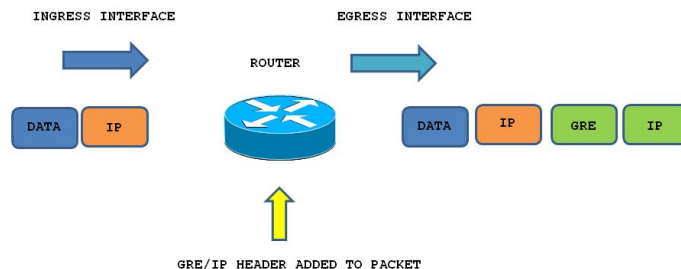
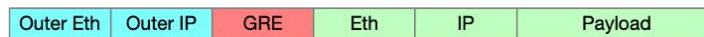
original packet



gretun

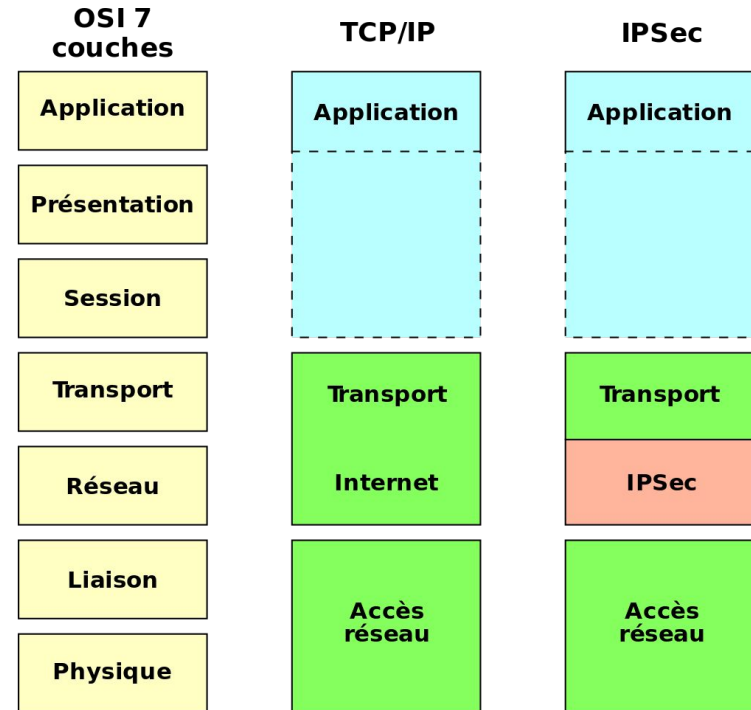


gretap



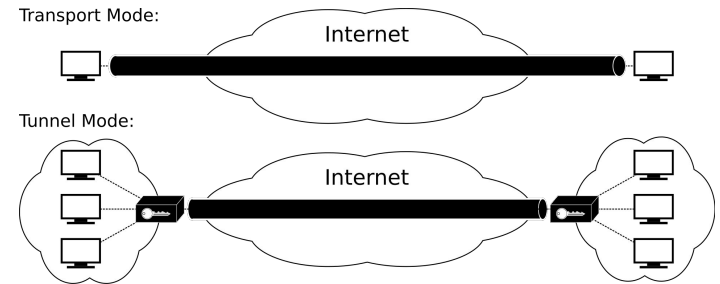
# IPsec

- Un framework ouvert pour assurer des communications privées sécurisées
- Assure la confidentialité, l'intégrité et l'authenticité des communications de données sur un réseau public
- Norme prévue pour IPv6 mais adaptée pour IPv4
- Vise à sécuriser l'échange de données au niveau de la couche **Réseau**
- Permet de créer des VPN sécurisés et sécuriser les accès distants
- Généralement implémenté dans le noyau



# IPsec - Modes de fonctionnement

- **Mode transport**
  - Connexion hôte à hôte
- **Mode tunnel**
  - Tunnel réseau
  - Utilisé pour
    - Communication de réseau à réseau (création des VPNs)
    - Communication d'hôte à réseau (accès à distance d'un utilisateur)
    - Communication hôte à hôte (messagerie privée)



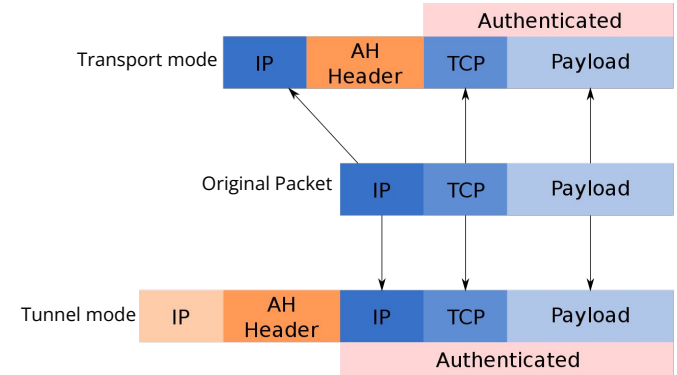
# IPsec - Modes de fonctionnement

- **Mode transport**

- Uniquement les données transférées sont chiffrées et/ou authentifiées (la partie *payload* du paquet IP)

- **Mode tunnel**

- La totalité du paquet IP qui est chiffré et/ou authentifié
- Paquet est encapsulé dans un nouveau paquet IP avec un nouvel en-tête IP





# IPsec - Composants

- **Mécanismes de sécurité**
  - Authentication Header (AH)
  - Encapsulation Security Payload (ESP)
- **Bases de données internes**
  - Security Association Database (SAD)
  - Security Policy Database (SPD)
- **Protocole d'échange de clés**
  - Internet Key Exchange (IKE)

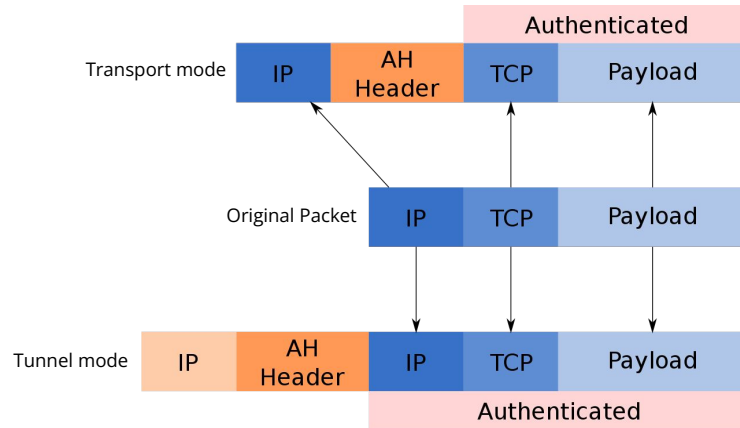
# IPsec - Mécanismes de sécurité

- **AH (Authentication Header)**
  - Intégrité, unicité et authenticité des données
  - Pas de confidentialité!
- **ESP (Encapsulating Security Payload)**
  - Confidentialité (Chiffrement des données)
  - Intégrité, unicité et authenticité des données

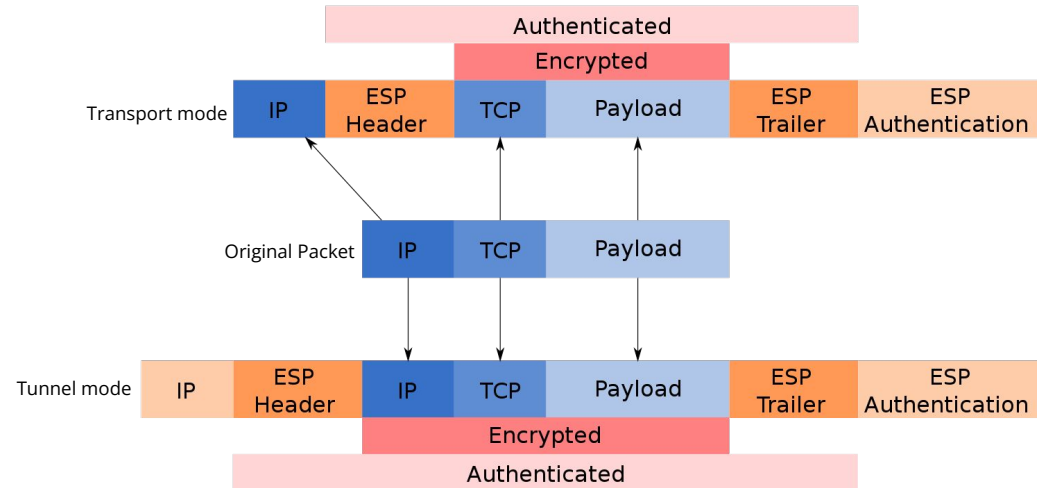
	AH	ESP (encryption only)	ESP (encryption plus authentication)
Access control	✓	✓	✓
Connectionless integrity	✓		✓
Data origin authentication	✓		✓
Rejection of replayed packets	✓	✓	✓
Confidentiality		✓	✓
Limited traffic flow confidentiality		✓	✓

# IPsec - Mécanismes de sécurité

## AH (Authentication Header)



## ESP (Encapsulating Security Payload)



# IPsec - Security Association (SA)

- IPsec utilise le concept de **Security Association (SA)** pour gérer les paramètres des mécanismes de sécurité
- **Association de sécurité (SA)**
  - Structure de données servant à stocker l'ensemble des paramètres associés à une communication donnée
  - Est unidirectionnelle (deux SA pour protéger deux sens de communications)
  - Une SA par protocole de sécurité (AH ou ESP)
  - Identifiée de manière unique à l'aide d'un triplet
    - Adresse de destination des paquets
    - Identifiant du protocole de sécurité utilisé (AH ou ESP)
    - Index des paramètres de sécurité (Security Parameter Index, SPI)
      - Un bloc de 32 bits inscrit en clair dans l'entête de chaque paquet échangé
      - Permet d'identifier quel SA utiliser pour une communication donnée
- SA actives sont stockés dans « base de données des associations de sécurité » (Security Association Database, SAD)
  - Consultée pour savoir comment traiter chaque paquet reçu ou à émettre

SA

Direction	Outbound	Inbound
SPI	1000	1001
Destination Address	POP Server B	Node A
IPsec Protocol	ESP	ESP
Algorithm	3DES-CBC	3DES-CBC
Key	The secret key from A to B	The secret key from B to A
Mode	Transport	Transport

# IPsec - Security Policy Database (SPD)

- Contient un ensemble de règles qui détermine si un paquet est soumis au traitement IPsec et gère les détails du traitement
  - Si le trafic doit être protégé par IPsec, il détermine également quelle SA spécifique le trafic doit utiliser
- Est établie et maintenue par un utilisateur, un administrateur système ou une application

**Règle SPD**

Direction	Outbound	Inbound
Source Address	Node A	POP Server B
Destination Address	POP server B	Node A
Upper Layer Protocol	TCP	TCP
Upper Layer Source Port	Any	POP3
Upper Layer Destination Port	POP3	Any
IPsec Protocol	ESP	ESP
Mode	Transport	Transport

# IPsec - Gestion des clefs

- Les protocoles sécurisés ont recours à des algorithmes cryptographiques et ont donc besoin de clefs
- **Problématique:** se mettre d'accord sur les algorithmes, les paramètres et clés à utiliser
- Solutions
  - Gestion des paramètres et des clés manuelle
  - Gestion dynamique à l'aide d'un protocole sécurisé
- **IKE (Internet Key Exchange)**
  - o Un protocole permettant de négocier un accord sur les protocoles, les algorithmes et les clés à utiliser
  - o Gère et échange des clés en toute sécurité
  - o Permet un établissement de SA à travers un réseau non sécurisé
  - o Basé sur l'amélioration des protocoles ISAKMP/Oakley
  - o Permet d'échanger les clés via
    - Clés pré-partagées (PSK)
    - Certificats (X.509)

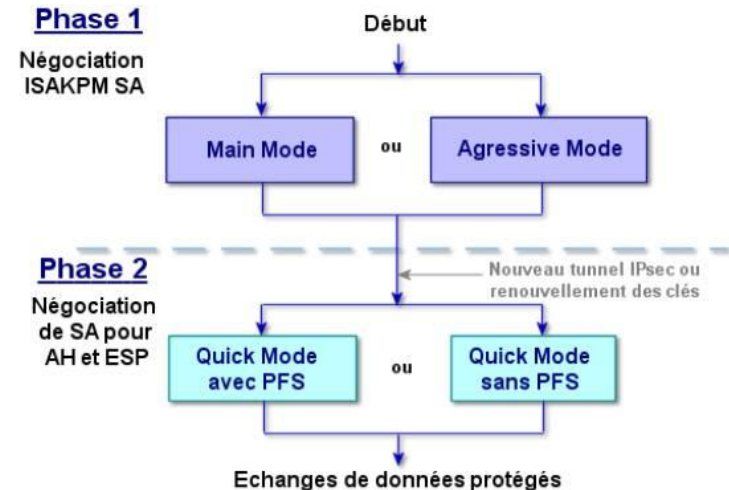
# IPsec - IKE (Internet Key Exchange)

## - Phase 1

- Les attributs suivants sont négociés
  - un algorithme de chiffrement, une fonction de hachage, une méthode d'authentification et un groupe pour Diffie-Hellman
- Trois clés sont générées
  - une pour le chiffrement, une pour l'authentification et une pour la dérivation d'autres clés

## - Phase 2

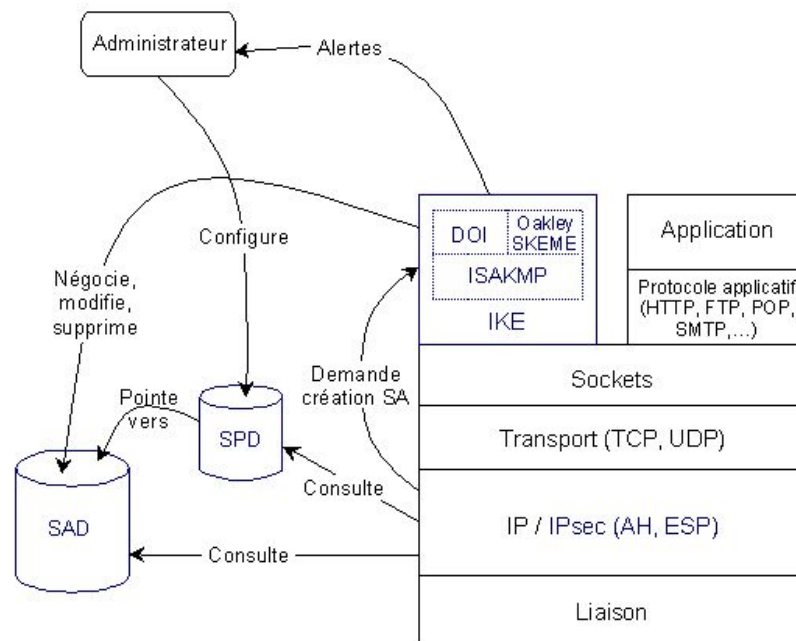
- La négociation de SA pour des protocoles de sécurité (AH et ESP)
  - Chaque négociation aboutit à deux SA, une dans chaque sens de la communication



# IPsec - Fonctionnement

## - Traffic sortant

- IPsec reçoit des données à envoyer
- Consulte la base de données des politiques de sécurité (SPD) pour savoir comment traiter ces données
- Si il faut appliquer des mécanismes de sécurité, récupère les caractéristiques requises pour la SA correspondante et va consulter la base des SA (SAD)
- La SA nécessaire existe déjà, elle est utilisée pour traiter le trafic en question
- Sinon, IPsec fait appel à IKE pour établir une nouvelle SA avec les caractéristiques requises

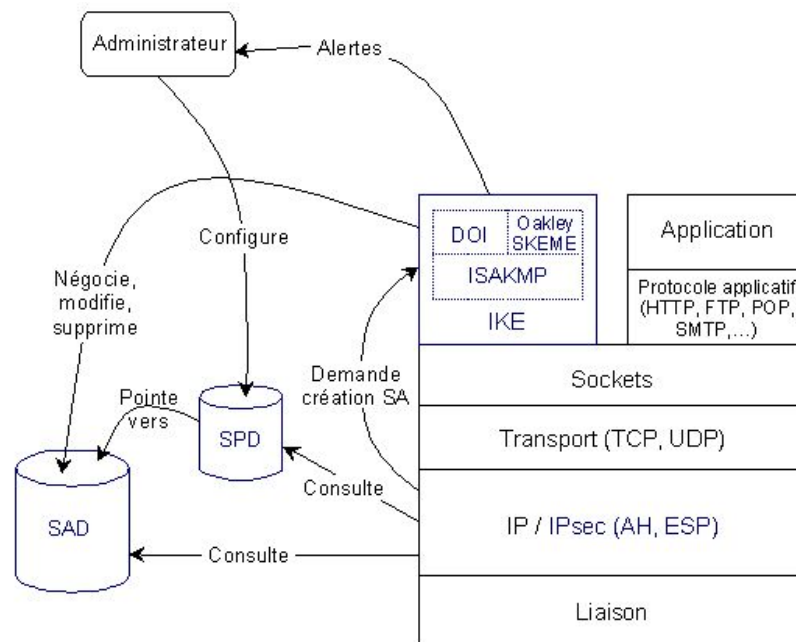




# IPsec - Fonctionnement

## - Traffic entrant

- IPsec reçoit un paquet en provenance du réseau
- Examine l'en tête pour savoir si ce paquet s'est vu appliquer un ou plusieurs services IPsec
- Si oui, quelles sont les références de la SA
- Consulte la SAD pour connaître les paramètres à utiliser pour la vérification et/ou le déchiffrement du paquet
- Une fois le paquet vérifié et/ou déchiffré, la SPD est consultée pour savoir si l'association de sécurité appliquée au paquet correspondait bien à celle requise par les politiques de sécurité



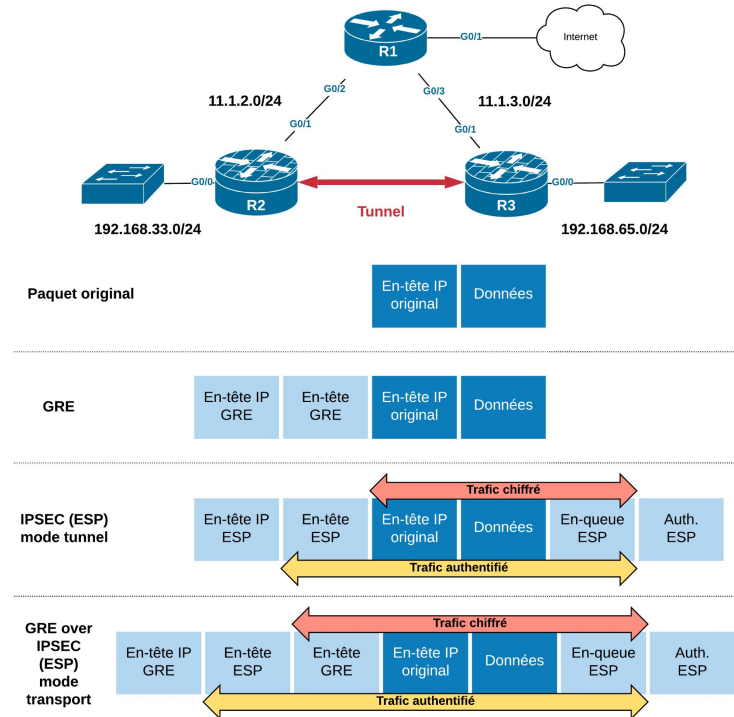
# GRE avec IPsec

## - GRE IPsec Tunnel Mode

- Ensemble du paquet GRE (qui comprend le paquet d'en-tête IP d'origine) est encapsulé, chiffré et protégé dans un paquet IPsec
- Surcharge importante ajoutée au paquet (76 octets)

## - GRE IPsec Transport Mode

- Paquet GRE est encapsulé et chiffré à l'intérieur du paquet IPsec, cependant, l'en-tête IP GRE est placé à l'avant
- Moins de surcharge, mais certaines restrictions lors de NAT ou PAT



# OpenVPN

- Système VPN open source
  - Pour créer des connexions point-à-point ou site-à-site sécurisées
- Authentification et chiffrement avec OpenSSL SSL/TLS
  - Moins efficace que IPsec, mais plus facile à mettre en oeuvre
- Architecture client/serveur
- VPN en espace utilisateur
  - Crée une interface réseau virtuelle en espace utilisateur à chaque extrémité du réseau
- Supporte TCP et UDP pour transmettre les données
- **Méthodes d'authentification**
  - Clés secrètes pré-partagées (PSK)
  - Certificats (PKI)
  - Nom d'utilisateur/mot de passe (nécessite un module externe)



# OpenVPN: Modes

- **Mode TAP**
  - Traffic Ethernet
- **Mode TUN**
  - Traffic IP
  - Topologies réseau disponibles
    - **Net30 (obsolète)** - chaque client se voit attribuer un /30 virtuel, a été utilisé lorsqu'il était impossible de définir IP + netmask sur l'adaptateur tun
    - **P2p** - pas utilisable avec Windows, tous les nœuds sont configurés comme de vrais liens point à point, un /30 entre le client et le serveur
    - **Subnet** - topologie actuelle recommandée, comme dans un réseau classique, l'interface tun est configuré avec une adresse IP et un netmask, un réseau /24 dans lequel se trouvent les clients

# OpenVPN: Plusieurs LANS derrière le VPN

- **Comment un client peut annoncer un LAN derrière lui?**
  - Client doit avoir le routage IP activé
  - Configurer le serveur pour router le LAN du client sur le VPN
    - **route** et **push "route ..."** dans la configuration du serveur
  - Indiquer au serveur quel client est responsable du réseau avec **iroute**
- **iroute** est une route interne à OpenVPN qui indique au serveur quel client possède quel réseau
  - Ajoutée à une entrée **CCD** (Configuration du serveur pour un client spécifique)

# WireGuard

- Une solution VPN la plus sécurisée, la plus facile à utiliser et la plus simple de l'industrie
  - Plus performante que OpenVPN
  - Plus simple que IPsec
- Implémenté dans le noyau Linux
  - Intégré dans le noyau Linux officiel à partir de la version 5.6
- Encapsulé en toute sécurité les paquets IP via UDP (pas de TCP)
- Authentification avec une paire des clés privées/publiques (x25519)
  - Pas des mécanismes de distribution des clés ou de configuration
- Fonctionne en ajoutant une interface réseau virtuel (ou plusieurs), appelée **wgX**



# WireGuard - Cryptokey Routing

- Utilise le concept appelé **Cryptokey Routing** qui simplifie la gestion du réseau et le contrôle d'accès
  - Associe des clés publiques à une liste d'adresses IP de tunnel autorisées à l'intérieur du tunnel
  - Lors de l'envoi de paquets
    - La liste des IP autorisées se comporte comme une sorte de table de routage
  - Lors de la réception de paquets
    - La liste des IP autorisées se comporte comme une sorte de liste de contrôle

## Configuration Serveur

```
[Interface]
PrivateKey = yAnz5TF+IXXJte14tji3zIMNq+hd2rYUlgJBgB3fBmk=
ListenPort = 51820

[Peer]
PublicKey = TrMvSoP4jYQIY6RIzBgbssQqY3vxI2Pi+y71IOWWXX0=
AllowedIPs = 10.192.122.4/32, 192.168.0.0/16

[Peer]
PublicKey = gN65BkIKy1eCE9pP1wdc8ROUtkHLf2PfAqYdyYBz6EA=
AllowedIPs = 10.10.10.230/32
```

## Configuration Client

```
[Interface]
PrivateKey = gl6EdUSYvn8ugXOt8QQD6Yc+JyiZxIhp3GlnSWRfWGE=
ListenPort = 51820

[Peer]
PublicKey = HIgo9xNzJMWLKASShTqIybxZ0U3wGLiUeJ1PKf8ykw=
Endpoint = 192.95.5.69:51820
AllowedIPs = 0.0.0.0/0
```

Merci pour votre attention!



## Références

- <https://irp.nain-t.net/doku.php/280vpn:start>
- <https://www.frameip.com/vpn/>
- <https://www.frameip.com/ipsec/>
- <https://www.sans.org/white-papers/1459/>
- <https://community.openvpn.net/openvpn/wiki/GettingStartedwithOVPN>
- <https://www.wireguard.com/>