# Sécurité des Réseaux

## Chapitre 5:
## Virtual Private Networks (VPNs)

Souheil Ben Ayed

Ecole Nationale d'Ingénieurs de Sousse (ENISo)
Université de Sousse

Département Informatique Industrielle
2ème année Génie Télécoms Embarquée

2020 - 2021



## Introduction

- Le réseau IP (Internet) n'est pas sécurisé:
  - Attaques DoDs, eavesdropping, capture des paquets, usurpation d'identité, ...
- Il faut prendre des précautions lorsque l'on souhaite naviguer en toute confidentialité.
- Chaque fois que des données personnelles sont collectées elles doivent être protégées.
  - Payement en ligne, postuler à un emploi ou demander un prêt bancaire.



## Introduction

- Un réseau public non sécurisé ne doit jamais être utilisé pour la transmission des données sensibles
- Solutions:
  - Le cryptage des données avant transmission.
  - L'utilisation d'une ligne spécialisée pour la liaison inter sites.
  - VPN: Virtual Private Network



## Pourquoi utiliser un VPN?

- Echanger des données confidentiels de façon sécurisé entre deux réseaux ou deux machines distantes.
- Naviguer en tout anonymat sur Internet
  - En accédant à un serveur distinct pour l'utilisation d'Internet, les VPN rendent beaucoup plus difficile le suivi des activités en ligne par les pirates et / ou une tiers partie.
- Les VPN réduisent les coûts d'accès à distance en utilisant les ressources du réseau public.
  - Par rapport à d'autres solutions, y compris les réseaux privés, un VPN est peu coûteux.

## Qu'est ce qu'un VPN.

- Un réseau privé virtuel (VPN) crée un tunnel de communication sécurisé privé entre deux entités sur un réseau intermédiaire.
- Dans la plupart des cas, le réseau intermédiaire est un réseau non sécurisé ou publique, tel qu'Internet
- Généralement, le tunnel de communication est crypté se qui permet de créer un tunnel sécurisé.

## Virtual Private Networks (VPNs)

- Une fois qu'un lien VPN est établi entre deux entités, la connectivité réseau du client VPN est identique à celle d'un réseau local connecté par une connexion par câble.
- La seule différence entre une connexion directe par câble LAN et une liaison VPN est la vitesse de transmission.

## Virtual Private Networks (VPNs)

- Il s'agit de créer un tunnel (liaison virtuelle) de communication qui assure la transmission point à point de l'authentification et du trafic de données sur un réseau intermédiaire non sécurisé tel que Internet.
- La plupart des VPN utilisent le cryptage pour protéger le trafic encapsulé, mais le cryptage n'est pas nécessaire pour que la connexion soit considérée comme un VPN.

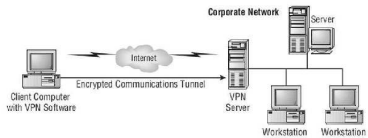
## Virtual Private Networks (VPNs)

- Les VPN peuvent exister au sein des réseaux privés ou entre des terminaux d'utilisateurs finaux connectés à un fournisseur de services Internet.
- Le VPN peut relier deux réseaux ou deux systèmes individuels.
- Ils peuvent relier des clients, des serveurs, des routeurs, des pare-feu et des commutateurs.

## Virtual Private Networks (VPNs)




## Virtual Private Networks (VPNs)






## Virtual Private Networks (VPNs)

- Le VPN utilise le cryptage des données et d'autres mécanismes de sécurité pour empêcher les utilisateurs non autorisés d'accéder aux données et pour garantir que les données ne peuvent pas être modifiées sans être détectées au fur et à mesure qu'elles circulent sur Internet.



## Virtual Private Networks (VPNs)

- Les VPN fournissent les fonctions suivantes:
  - **L'authentification**: prouve l'identité des partenaires de communication.
  - **Le contrôle d'accès**: empêche les utilisateurs d'accéder aux ressources d'un réseau.
  - **La confidentialité**: empêche la divulgation non autorisée de données sécurisées.
  - **L'intégrité des données**: empêche les modifications non désirées des données pendant le transit.

## Tunneling

- Le VPN est basé sur la technique du tunneling pour transporter les données cryptées sur Internet
- Tunneling est un mécanisme d'encapsulation d'un protocole dans un autre protocole.

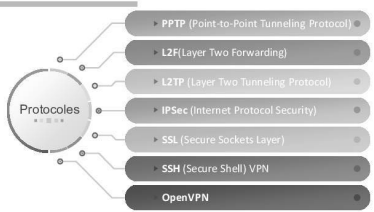


## Principaux avantages des VPN

- Les VPN sont peu coûteux
- Confidentialité
- Intégrité des données
- Authentification
- Protection contre le rejeu de paquets ( antireplay protection)



## Principaux protocoles de tunnelisation






## Principaux protocoles de tunnelisation

- **PPTP** (Point-to-Point Tunneling Protocol) un protocole de niveau 2 développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics. Il permettre le tunneling PPP (Point-to-Point Protocol) via un réseau public.
- **L2F**(Layer Two Forwarding) un protocole de niveau 2 développé par Cisco, Northern Telecom et Shiva .
- **L2TP** (Layer Two Tunneling Protocol) protocole de niveau 2. C'est un standard IETF qui combine les protocoles PPTP et L2F. Permet de créer des connexions VPN sécurisées pour des connexions client-serveur individuelles.

## Principaux protocoles de tunnelisation

- **IPSec** (Internet Protocol Security) est un standard ouvert IETF pour les VPN qui opère sur la couche réseau (couche 3) du modèle OSI. Il permet de transporter des données chiffrées pour les réseaux IP
- **SSL** (Secure Sockets Layer) offre une solution de tunneling. Il permet d'utiliser un navigateur Web comme client VPN.



## Principaux protocoles de tunnelisation

- **SSH** (Secure Shell) VPN - OpenSSH offre un tunneling VPN (distinct du transfert de port) pour sécuriser les connexions distantes à un réseau ou à des liaisons inter-réseaux. Le serveur OpenSSH fournit un nombre limité de tunnels concurrents.
- **OpenVPN** utilise un protocole de sécurité personnalisé qui utilise le protocole SSL / TLS pour l'échange de clés



## Types de VPN

- Il existe de nombreux chemins différents pour connecter un VPN:
  - VPN de site à site (Site-to-Site VPN)
    - Dans le VPN de site à site, le trafic est crypté entre les sites.
  - VPN hôte à site (Host to Site VPN)
    - C'est un type de VPN accessible à distance et nécessite un logiciel sur la machine de l'utilisateur.
  - VPN hôte à hôte (Host to Host VPN)
    - Dans l'hôte à l'hôte VPN, il existe un cryptage d'utilisateur à utilisateur. Il s'agit d'un logiciel et aucun matériel spécifique n'est requis.



## Les methods d'utilisation d'un VPN

- Les deux extrémités d'un VPN sont généralement implémentées en utilisant l'une des méthodes suivantes:
  - Client à Client
  - Client / VPN-Concentrateur (ou appareil)
  - Client à pare-feu
  - Pare-feu à pare-feu
  - Routeur à routeur

## *Internet Protocol Security (IPSec)*



## Internet Protocol Security (IPSec)

- Internet Protocol Security (IPSec) fournit une méthode de configuration d'un canal sécurisé pour l'échange de données protégé entre deux périphériques.
- IPSec est une norme largement acceptée pour la protection de la couche réseau.
- Il peut être plus flexible et moins coûteux que les méthodes de chiffrement de lien et de bout en bout.



## IPSec

- Les entités communiquant (les périphériques) qui partagent le canal sécurisé via IPsec peuvent être deux systèmes, deux routeurs, deux passerelles entre différents réseaux ou toute combinaison d'entités.
- IPSec est un protocole de la couche 3
  - IPv4: protocole optionnel.
  - IPv6: obligatoire (next header).



## IPSec

- Pour répondre aux besoin de sécurité, IPsec a été développé pour la dernière version du protocole Internet (IPv6).
- Le protocole IPv4 initiale a été développée avec peu de mesures de sécurité.
- Pour le protocole IPv4, IPSec est une amélioration du protocole qui offre un système de sécurité de la couche Internet.

## IPSec

- IPSec n'est pas un protocole unique, mais plutôt un ensemble de protocoles.
- C'est une architecture standard définie par l'IETF (Internet Engineering Task Force) pour la mise en place d'un canal (Tunnel) sécurisé permettant l'échange d'informations entre deux entités.



## IPSec

- Documents références IETF:
  - RFC 4301: Security Architecture for the Internet Protocol
  - RFC 4302: IP Authentication Header
  - RFC 4303: IP Encapsulating Security Payload
  - RFC 4304: Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)
  - RFC 4307: Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
  - RFC 4308: Cryptographic Suites for Ipsec
  - ...



## IPSec

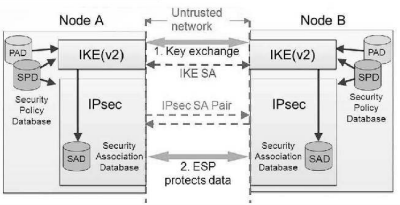
- IPsec utilise la cryptographie à clé publique pour assurer **le cryptage**, le **contrôle d'accès**, la **non répudiation** et l'**authentification de message**, le tout à l'aide du protocole IP.
- IPSec dispose de méthodes de cryptage et d'authentification solides et, bien qu'il puisse être utilisé pour permettre la communication en tunnel entre deux ordinateurs, il est généralement utilisé pour établir des réseaux privés virtuels (VPN) entre réseaux sur Internet.



## IPSec

- IPSec n'est pas un protocole strict qui dicte le type d'algorithme, les clés et la méthode d'authentification à utiliser.
- Il s'agit plutôt d'un cadre ouvert et modulaire offrant une grande flexibilité aux entreprises lorsqu'elles choisissent d'utiliser ce type de technologie.

## IPSec






## Composants d'IPSec

- Il peut être divisé en trois groupes de fonctions.
  - Protocoles de sécurité :
    - Les protocoles AH et ESP
  - Protocoles de d'échange et de gestion des clés
    - Les protocoles IKE et ISAKMP
  - Bases de données internes
    - Security Association Database (SAD)
    - Security Policy Database (SPD)



## Protocoles IPSec

- IPSec utilise deux protocoles de sécurité de base:
  - **Authentication Header (AH)**
    - Protocole d'authentification
  - **Encapsulating Security Payload (ESP)**.
    - Protocole d'authentification et de cryptage.
    - Authentification de la source, la confidentialité et l'intégrité des messages.



## Authentication Header (AH)

- L'en tête d'authentification( **Authentication Header (AH))** offre des services d'authentification et d'intégrité des paquets IP.
- AH fournit également une authentification et un contrôle d'accès et empêche les attaques par rejeu.
- Ce protocole de sécurité signe les paquets IP et garantit leur intégrité.
- Le contenu du datagramme n'est pas chiffré.
- Le destinataire est sûr que le contenu du paquet n'a subi aucune modification et que c'est l'expéditeur qui a envoyé les paquets.

## Authentication Header (AH)

- Format de l'en tête d'authentification (AH)




## Authentication Header (AH)

- Next Header (8 bit) specify the next header
- Payload Length (8 bit) length of AH in 32-bit word minus two
- Reserved (16 bit) future uses
- SPI (32 bit)
- Sequence number (32 bit)
- Authentication data: contains Integrity Check Value
- Variable length
  - multiple of 32 bits (default 96)
  - MAC or a truncated version (96 bit)



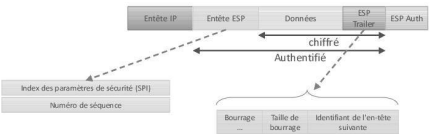
## Encapsulating Security Payload (ESP)

- L'en-tête de confidentialité-authentification (Encapsulating Security Payload (ESP)) assure la confidentialité et l'intégrité du contenu des paquets.
- ESP propose des services d'authentification similaire a ceux proposes par l'AH.
- Il permet d'empêcher les attaques par rejeu.
- Il fonctionne au niveau de la couche réseau (couche 3) et peut être utilisé en mode transport ou en mode tunnel.

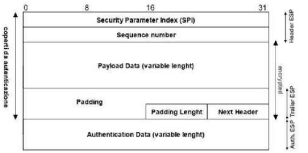


## Encapsulating Security Payload (ESP)

- Format de l'en tête d'authentification (AH)



## Encapsulating Security Payload (ESP)






## Encapsulating Security Payload (ESP)

- *Security Parameters Index* (SPI)
- *Sequence number* (32 bit): anti replay
- *Payload data* encrypted data
  - A possible initialization vector is placed at the beginning of the field
- *Padding* (0 – 255 byte)
- *Padding length*
- *Next Header* (8 bit): type of data in the payload
- *Authentication Data*: ICV



## Encapsulating Security Payload (ESP)

- *Header ESP* is composed of
  - SPI
  - Sequence Number
- *Trailer ESP* is composed of
  - Padding,
  - Padding Length
  - Next Header
- *Authentication* ESP contains Authentication Data



## AH & ESP

| | AH | ESP (chiff.) | ESP (chiff. & auth.) |
|---|---|---|---|
| Access control | ✓ | ✓ | ✓ |
| Datagram integrity | ✓ | | ✓ |
| Data origin authentication | ✓ | | ✓ |
| Anti-reply | ✓ | ✓ | ✓ |
| Confidentiality | | ✓ | ✓ |
| Partial confidentiality | | ✓ | ✓ |

# Modes de fonctionnement IPSec

- IPSec peut fonctionner dans l'un des deux modes suivants:
  - Mode de transport, dans lequel la charge utile du message est protégée
  - Mode tunnel, dans lequel la charge utile et les informations de routage et d'en-tête sont protégées.
  - En mode de transport, ESP crypte les informations du message afin qu'il ne puisse pas être détecté et découvert par une entité non autorisée. Le mode tunnel offre un niveau de protection plus élevé en protégeant également les en-têtes et les données de fin qu'un attaquant peut trouver utiles.



# Mode tunnel

- En mode tunnel, IPSec fournit une protection de chiffrement à la fois pour le payload et l'en-tête de message en encapsulant l'ensemble du paquet de protocole de réseau local d'origine et en ajoutant son propre en-tête IPSec temporaire.
- L'entête IP d'origine est encapsulée dans les données IPSec
- Une entête IP est ajouté pour le transport sur le réseau public
- Contrôle total sur l'entête IP et l'ensemble des communications via VPN peuvent être sécurisées.
- Nécessite des passerelles VPN . Latence lors des opérations de cryptographie.

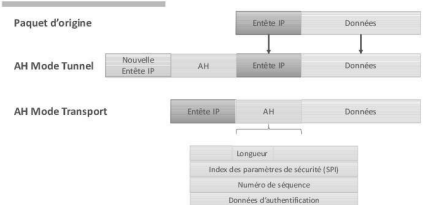



# Mode transport

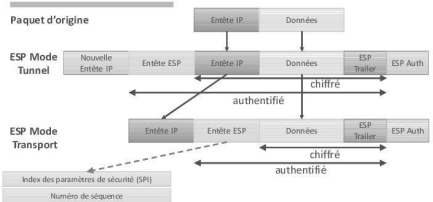
- En mode de transport, IPSec fournit une protection de chiffrement pour uniquement le Payload et laisse l'entête du message d'origine intact.
- Ne modifie pas l'en-tête initial. Il s'intercale entre le protocole réseau (IP) et le protocole de transport (TCP, UDP...)
- La session est sécurisée de bout en bout
- Nécessité d'une implémentation de IPSec sur tous les hosts; autant de sessions IPSec que de couples de hosts




# AH & mode de fonctionnement



# ESP & mode de fonctionnement






# ESP & AH

- Il est aussi possible d'utiliser les deux protocoles ESP et AH.

**ESP & AH mode tunnel**


**ESP & AH mode transport**




# SA (security association)

- Une association de sécurité (SA, Security Association) spécifie les propriétés de sécurité que reconnaissent les hôtes lors de la communication.
- Une seule SA protège les données dans une direction. Une association unidirectionnelle entre deux hôtes.
  - Pour une sécurité bidirectionnelle, il est nécessaire d'avoir deux associations.
- Identifiée par trois paramètres:
  - Index de Paramètre de Sécurité (SPI)
  - Adresse de destination IP
  - Identifiant du protocole de sécurité : AH ou ESP



# Paramètres d'une SA

- Sequence number counter (32 bit counter, obligatoire)
- Sequence counter overflow (flag, obligatoire)
- Anti-replay window
- AH information
- ESP information
- Lifetime
- IPSec protocol mode (tunnel, transport)
- Path MTU

## Security Association Database (SAD)

- Security Association Database (SAD) base de données des associations de sécurité):
  - Associe un protocole de sécurité à une adresse IP de destination et un numéro d'indexation.
  - Le numéro d'indexation est appelé index du paramètre de sécurité.
  - Les trois éléments (protocole de sécurité, adresse de destination et SPI) identifient un seul paquet IPSec.



## Security Association Database (SAD)

- Security Association Database (SAD) base de données des associations de sécurité):
  - La base de données garantit que le paquet protégé est reconnu par le récepteur à son arrivée.
  - Elle permet également au récepteur de déchiffrer la communication, de vérifier que les paquets n'ont pas été altérés, de rassembler les paquets et de livrer les paquets à leur destination finale.



## Security Policy Database (SPD)

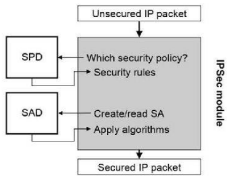
- Security Policy Database (SPD), base de données de stratégie de sécurité base de données:
  - Indiquant le niveau de protection à appliquer à un paquet.
  - La base de données SPD filtre le trafic IP et identifie le mode de traitement des paquets.
  - Un paquet peut être rejeté, passé au clair ou protégé à l'aide d'IPSec.



## Security Policy Database (SPD)

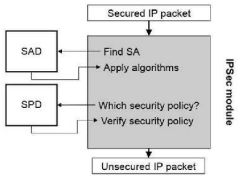
- Security Policy Database (SPD), base de données de stratégie de sécurité base de données:
  - En ce qui concerne les paquets sortants, les bases de données SPD et SAD déterminent le niveau de protection à appliquer.
  - Pour les paquets entrants, la base de données SPD permet de déterminer l'acceptabilité du niveau de protection. Si le paquet est protégé par IPsec, une consultation de la base de données SPD est effectuée après déchiffrement et vérification du paquet.

## Envoie de paquets






## Réception de paquets






## Gestion des clés de chiffrement

- La confidentialité est assurée par la réalisation d'algorithmes de chiffrement qui utilisent des clés qui sont à générer et à diffuser.
- Deux alternatives ont été identifiée:
  - Manuelle: effectue par l'administrateur système. Valable pour de petits environnements statiques.
  - Automatique: Invoque un protocole d'échange de clés. Adaptée aux grands environnements à configuration évolutive.



## Gestion des clés de chiffrement

- **Oakley** key Determination Protocol: basé sur l'algorithme d'échange de clés Diffie-Hellman.
- **ISAKMP** (Internet Security Association and Key Management Protocol): Procédures et formats des paquets pour établir, négocier, modifier, terminer et détruire une association de sécurité.
- **IKE** (Internet Key Exchange ): implémentation de ISAKMP. Permet de réaliser l'échange de clés (clés authentifiées) et de négocier les services de sécurité pour une association de sécurité.

## Internet Key Exchange (IKE)

- IKE implémente les fonctions suivantes
  - Négociation des paramètres de sécurité
  - Authentification
  - Établissement clé
  - Gestion des clés (après établissement)
  - Protocole UDP / 500



## Internet Key Exchange (IKE)

- un ensemble de protocoles et de mécanismes assurant une gestion sécurisée et dynamique des paramètres de sécurité utilisés dans IPSec
  - IKE = échange de clés d'authentification + gestion des SA
- Basé sur des amélioration des protocoles ISAKMP/Oakley
- Deux manières d'échanger des clefs :
  - clefs pré-partagées
  - certificats X.509



## IKE - ISAKMP

ISAKMP : Internet Security Association and Key Management Protocol

- associé à une partie des protocoles SKEME et Oakley
- négociation des paramètres (algorithmes de chiffrement…)
- mécanisme de négociation découpé en deux phases:
  - **Phase 1: définition des moyens pour protéger les échanges suivants.**
    **2 modes possibles :**
    - **normal (6 messages et protection d'identité)**
    - **agressif (3 messages)**
  - **Phase 2: négociation des paramètres des futures SA**