heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

Chapitre III

La sécurité sur Internet

Cours chap. 3
Tutorial IBM ch. 22.3
Chapitre 6 Chapman&Zwicky
Eléments de cryptographie, S. Robert

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

Les entreprises et l'Internet

- Internet est devenu un élément critique de la stratégie de communication des entreprises
- Utilisé dans deux buts
  1. Communication avec les partenaires externes et les clients
     - Ouverture du réseau d'entreprise vers l'extérieur
  2. Communication entre sites distants de la même entreprise
     - Précédemment réalisée avec des lignes louées → réseau privé
     - Aujourd'hui transmission des données sur une infrastructure publique

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Sécurité du réseau

- Qu'est-ce qu'il faut protéger
  - Les données – les ressources – la réputation

Aspects de la sécurité

L'intégrité des données
- Empêcher une modification non-autorisée

La confidentialité des données
- Protection des informations d'une divulgation non-autorisée

L'authentification de l'origine des données
- Permet d'être sûr qu'une de l'identité de la source originale d'un ensemble de données

La disponibilité des données
- Faire en sorte qu'on ne puisse pas empêcher l'accès légitime aux données

La disponibilité des ressources
- Protéger vos ordinateurs et votre réseau contre une utilisation illégitime qui pourrait empêcher l'accès légitime

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Menaces classiques sur IP

- **Malwares** (viruses, vers, cheveaux de Troie): programmes crapuleux.
- **Denial of Service** (DoS): Privation de l'accès à un service en bombardant les serveurs avec des paquets malveillants.
- **Détournement de trafic**: On prend possession de la connexion.
- **Man-in-the middle**: L'attaquant s'insère entre les interlocuteurs.

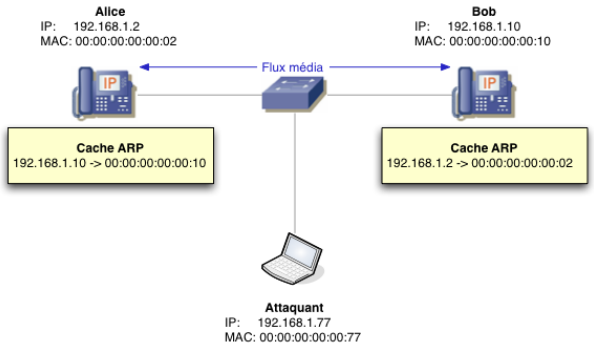
heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Menaces classiques sur IP (2)

- **Paquet sniffing**: obtenition d'informations après avoir détourné le trafic (outil: Wireshark)
- **Craquage de mots de passe** pour obtenir certains privilèges.
- **Exploitation de vulnérabilités** pour casser la sécurité d'un système (ex. buffer overflow).

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

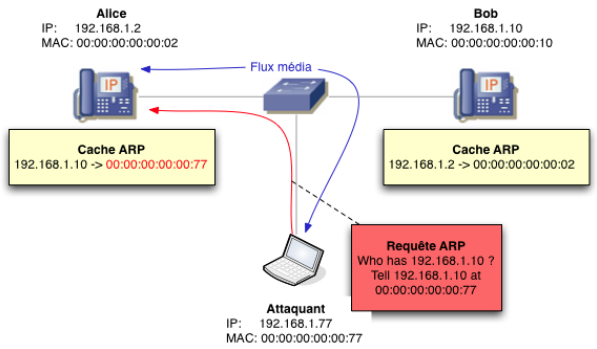
ARP Spoofing (avant l'attaque)



heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

Attaque ARP Spoofing

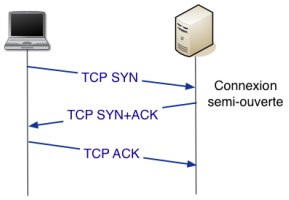


heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Inondation avec TCP SYN

- Le nombre de connexions semi-ouvertes est limité
- Fausse adresse source

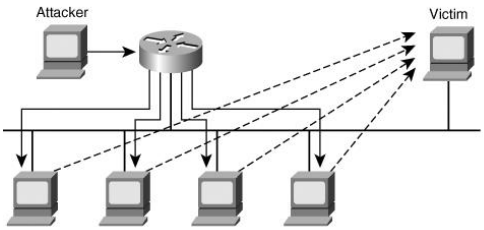
- Ejecter les SYN de la file



heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Smurf

- Ping en diffusion sur un LAN (40/seconde sur 200 machines)

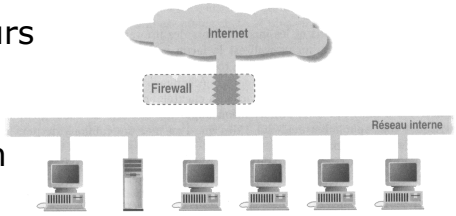


heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Les firewalls

Un firewall empêche les dangers provenant de l'Internet de se répandre à l'intérieur de votre réseau

- Il restreint l'accès à un point précis
- Il empêche les agresseurs de s'approcher de vos autres défenses
- Il restreint la sortie à un point précis



Source: Chapman/Zwicky

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Fonctions d'un firewall

Centre des décisions de sécurité

- Goulet d'étranglement par ou passe tout le trafic entre le réseau interne et l'Internet

Renforce le règlement de sécurité

- Sert à implémenter la politique de sécurité concernant p.ex. l'utilisation de services dangereux à travers Internet (i.e. serveur interne)

Monitoring du trafic depuis et vers l'Internet

- Permet de collecter de l'information sur l'utilisation d'Internet

Limite l'exposition du réseau

- Les firewalls internes peuvent isoler un problème de sécurité dans une des parties du réseau

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Que ne peut pas faire un firewall ?

Ne permet pas de protection contre des utilisateurs internes malveillants

- Si l'attaquant se trouve déjà à l'intérieur du réseau, un firewall n'offre pas de protection

Ne permet pas de protection contre des connexions qui ne passent pas par lui

- Un point d'accès WLAN mal sécurisé, installé sans autorisation, peut réduire à néant tous les efforts pour de sécuriser le réseau

Ne protège pas contre les virus

- Un firewall ne peut pas facilement examiner les données au niveau application

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Stratégies de sécurité

Refus par défaut

« Ce qui n'est pas expressément autorisé est interdit »

- Choix évident du point de vue de l'administrateur
- Difficile à défendre envers les utilisateurs

Permission par défaut

« Ce qui n'est pas expressément interdit est autorisé

- Suppose qu'on connaisse les dangers

➢ Vouée à l'échec

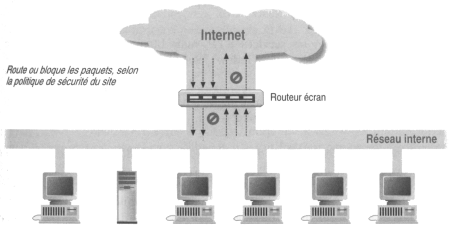
- Nouveaux services
- Nouveaux trous de sécurité
- Nouvelles manières d'exploiter les failles
- Nouvelles idées des utilisateurs

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Types de firewalls

Firewall du niveau réseau

- « *Routeur écran* »
- Route de manière sélective les paquets entre l'Internet et le réseau interne
- Filtre les paquets entrants et sortants selon
  - Les informations contenues dans les en-têtes (adresse source et destination, ports source et destination, protocole, …)
  - Les informations de routage (interface d'entrée, interface de sortie)



Source: Chapman/Zwicky

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Exemple de la configuration du filtrage

- Linux, Kernel 2.4 (+2.6)
  - Couche firewall 'NetFilter'
  - Configuration via la commande iptables
- Exemple
  - Refus par défaut

```
> iptables -F
> iptables -P INPUT DROP
> iptables -P OUTPUT DROP
> iptables -P FORWARD DROP
```

  - Ouvrir le service SSH sur le serveur 128.178.24.12

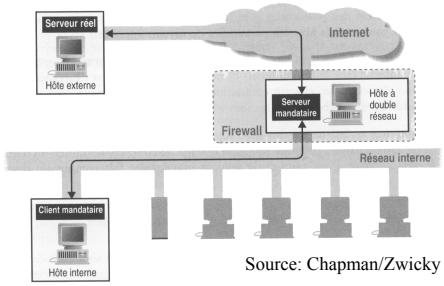
```
> iptables -t filter -A FORWARD -d 128.178.24.12
   -p tcp -dport 22 -j ACCEPT
> iptables -t filter -A FORWARD -s 128.178.24.12
   -p tcp -sport 22 -j ACCEPT
```

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Types de firewalls

Firewall du niveau application

- « *Serveur mandataire* » ou « *proxy* »
- Accepte les requêtes des client et les redirigent vers le vrai serveur
- Respectent la politique de sécurité de l'entreprise
- Transparent pour les utilisateurs
- Doit être complété par un mécanisme qui restreint les communications directes



Source: Chapman/Zwicky

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Architecture des firewalls

- Un firewall est généralement constitué de multiples parties
  - Un ou plusieurs routeurs écran
  - Un ou plusieurs serveurs mandataires
  - Réseaux intermédiaires

➢ La sécurité de dépend pas d'un seul élément

➢ Un agresseur doit franchir plusieurs barrières

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

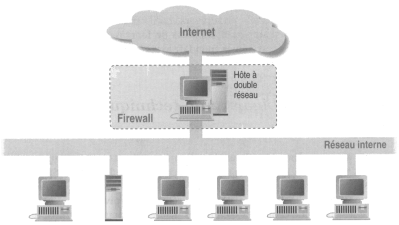
Architecture: Hôte à double réseau

- L'hôte à double réseau est connecté aux réseaux interne et externe
- Le routage est désactivé
- Connexions avec l'extérieur
  - Les utilisateur peuvent se loguer sur l'hôte et lancer le service souhaité

↑ Bon niveau de sécurité

↓ Solution peu commode pour les utilisateurs

↓ Gestion des comptes est vulnérable



Source: Chapman/Zwicky

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Architecture: Hôte à écran

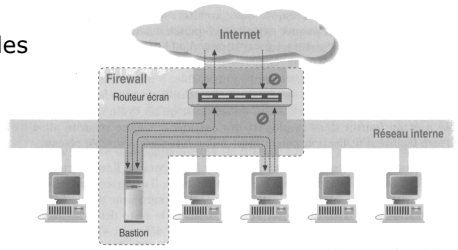
- Machine 'bastion' située sur le réseau interne
  - Travaille en proxy pour les connexions avec l'extérieur
  - Le routeur écran ne permet que les connexions depuis et vers le bastion

↑ Plus sécurisée que l'hôte à double réseau
  - Un routeur est plus facile à sécuriser qu'un hôte

↑ Plus commode pour les utilisateur
  - Possibilité d'autoriser quelques services directs, sans passer par le bastion

↓ Le bastion se trouve sur le réseau interne

↓ Le routeur écran est l'unique point de défense



Source: Chapman/Zwicky

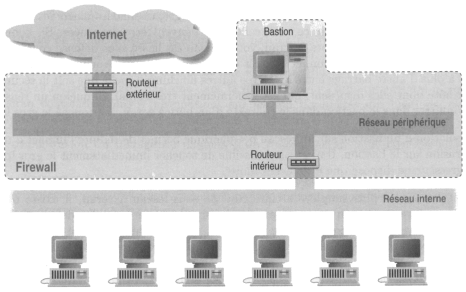
heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Architecture: Sous-réseau à écran

- Couche de sécurité supplémentaire: réseau périphérique ou DMZ (*demilitarized zone*)
  - Isole le bastion, qui est vulnérable aux attaques
  - Un intrus ayant réussi à s'infiltrer sur le bastion doit encore franchir le routeur écran intérieur
  - Le trafic LAN (p.ex. Ethernet partagé) ne peut pas être espionné depuis le bastion

↑ Solution très sécurisée

↓ Solution coûteuse



Source: Chapman/Zwicky

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

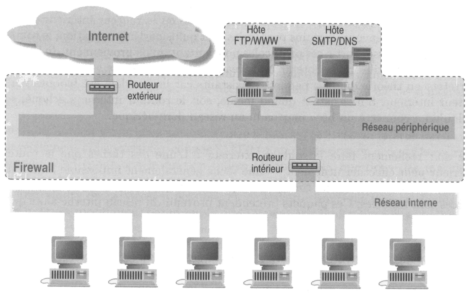
Variation: Plusieurs bastions

- Séparation des serveurs mandataires, par exemple
  - Bastions pour les services aux utilisateurs internes plus bastion pour les utilisateurs externes
  - Isolation des services vulnérables (FTP)

↑ Performances améliorées

↑ Différents niveaux de sécurité

↓ Coûts



Source: Chapman/Zwicky

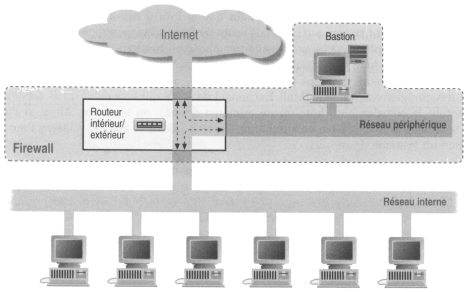
heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Variation: Fusion des routeurs externe et interne

- Le bastion reste isolé sur le réseau périphérique
  - Gère les services critiques
- Le routeur peut autoriser le passage directe de certains services

↑ N'augmente que peu la vulnérabilité

↓ Le routeur est le seul élément de défense



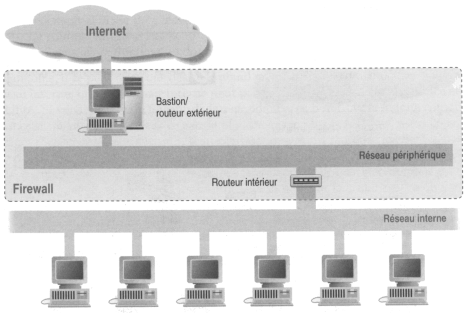
Source: Chapman/Zwicky

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Variation: Fusion du router externe et le bastion

- Architecture pratique pour les petits sites
  - Connexion modem ou ADSL
  - Machine à l'entrée fonctionne comme routeur et bastion

↑ N'augmente que peu la vulnérabilité

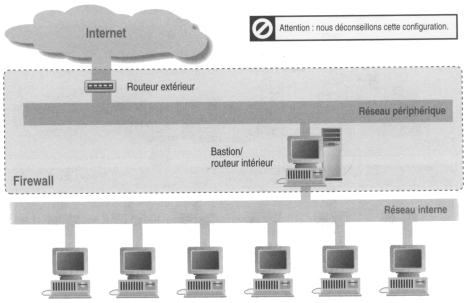


Source: Chapman/Zwicky

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Attention: Ne pas fusionner le bastion et le routeur interne

- Rend inutile le réseau périphérique
  - Si le bastion est infiltré, l'agresseur a accès au trafic LAN
  - Résulte en une architecture hôte à écran

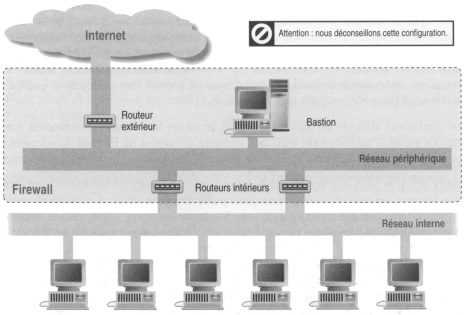


Source: Chapman/Zwicky

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Attention: Ne pas utiliser plusieurs routeurs internes pour *un* réseau interne

- Peut compromettre l'effet du réseau périphérique
  - Le routage peut décider de traverser le réseau périphérique pour le trafic LAN
  - Double l'effort de gestion



Source: Chapman/Zwicky

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Exercices

Tutorial IBM ch. 22.4 + 22.10
Cours ch. 3
VPNs, O'Reilly, C. Scott, P. Wolfe, M. Erwin

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

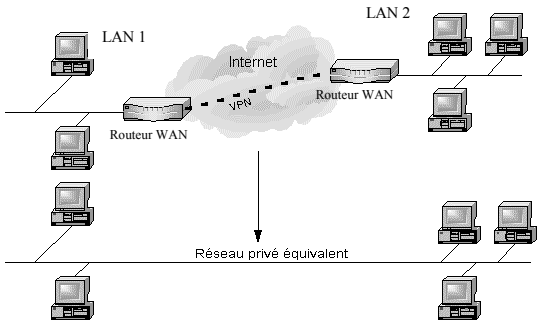
Réseaux virtuels privés VPN

- VPN (Virtual Private Network)
  - « *Technologie qui permet de transmettre des données sur une infrastructure partagée sans compromettre la sécurité des données* »
- Avant l'apparition des VPN
  - Interconnexion de sites distants à l'aide de lignes louées ou des circuits virtuels comme ATM
    - Configuration statique par l'opérateur
    - Impossible pour un intrus de modifier l'acheminement ou d'injecter des paquets dans un circuit virtuel

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Utilisation des VPN: LAN to LAN

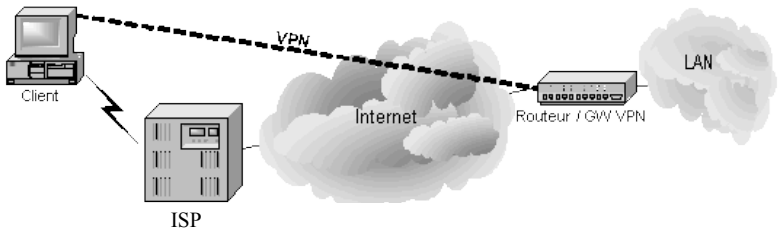
- Interconnexion transparente de LAN distants



heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Utilisation des VPN: Host to LAN

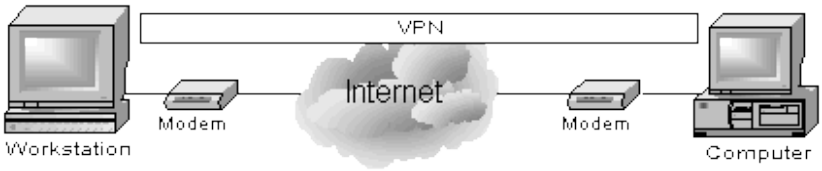
- Permet la connexion au réseau d'entreprise depuis un site distant
  - Connexion modem vers un ISP
  - Connexion 'logique' sécurisée au réseau d'entreprise
    - L'hôte fait logiquement partie du réseau d'entreprise



heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Utilisation des VPN: Host to Host

- Connexion sécurisée entre deux machines



heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Exigences de sécurité

Les VPN permettent de configurer plusieurs réseaux séparés et sécurisés sur la même infrastructure

Que signifie la 'sécurité des données' ?

- Séparation de l'adressage et du routage
  - Deux VPN doivent pouvoir utiliser le même adressage (p.ex. 10.x.x.x) sans conflits
  - Le routage doit garantir que les paquets restent à l'intérieur du VPN
- Résistance aux attaques
  - Déni de Service (DoS)
    - Le VPN doit restreindre l'accès depuis l'extérieur
  - Intrusion
    - Le VPN doit empêcher des attaques de 'IP spoofing'

Le protocole IPSec

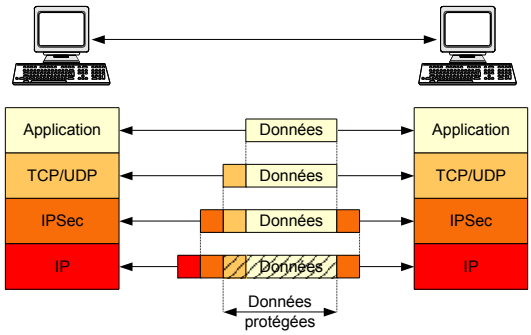
heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

- IPSec (RFC 2401) permet de sécuriser la couche réseau IP et donc toutes les applications qui travaillent en-dessus
- Services de sécurité d'IPSec
  - Authentification:
    S'assurer que la personne avec laquelle on communique est réellement cette personne et pas quelqu'un d'autre
  - Confidentialité
    S'assurer que des personnes non-autorisées ne peuvent pas écouter la communication
  - Intégrité
    S'assurer que les données reçues n'ont pas été modifiées

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Mode Transport d'IPSec

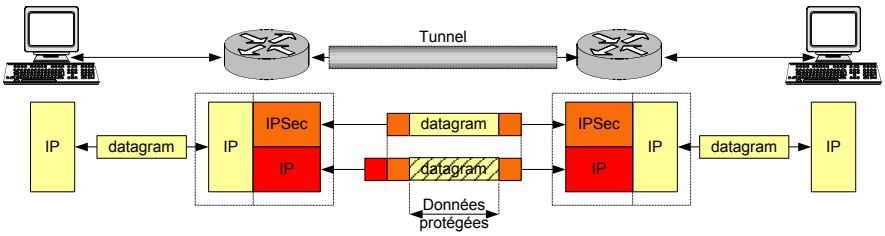
- Permet de sécuriser les données des couches supérieures (TCP + Application)
  - Souvent utilisé pour le 'Host to Host' ou 'Host to LAN'



heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Mode Tunnel d'IPSec

- Permet de sécuriser la couche IP et toutes les couches supérieures
  - Adresses IP source et destination sont aussi protégées
  - Souvent utilisé pour le 'LAN to LAN'
  - Des gateways IPSec créent un tunnel IPSec et encapsulent les datagrammes IP



heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Association de sécurité

- La protection des données utilise le chiffrement et des signatures numériques
  - L'algorithme, les clés, … doivent être négociés au début d'une transmission
  - Ces informations doivent être stockées sur les systèmes pairs afin de pouvoir traiter les paquets IPSec

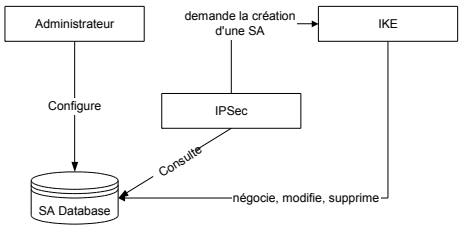
Association de Sécurité (SA)

  - Structure de données avec
    - Les paramètres d'authentification (algorithme et clés)
    - Les paramètres de cryptage (algorithme et clés)
    - Mode (tunnel ou transport)
    - …

Gestion des SA

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

- La source et le destinataire doivent utiliser la bonne SA afin de traite correctement les paquets
- Une SA est identifiée par
  - L'adresse IP du destinataire
  - Le protocole de sécurité (AH ou ESP)
  - Un Index des Paramètres de Sécurité (SPI)
- Les SA peuvent être créées
  - Dynamiquement à l'aide du protocole IKE (Internet Key Exchange)
  - Manuellement, par l'administrateur

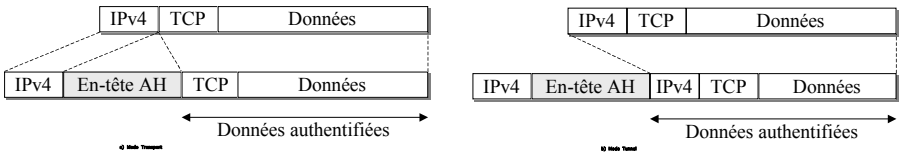


heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Service d'authentification d'IPSec

- Permet de s'assurer sur l'identité de la source des données et de leur intégrité
- Basé sur l'utilisation de signatures numériques
  - IPSec ne définit pas l'algorithme mais seulement la méthode (service générique)

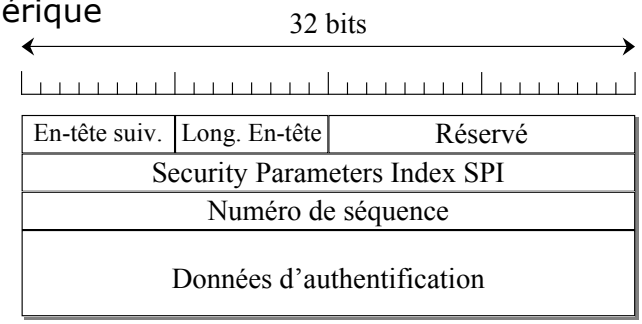
<u>En-tête d'authentification (AH)</u>



heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Format de l'en-tête AH

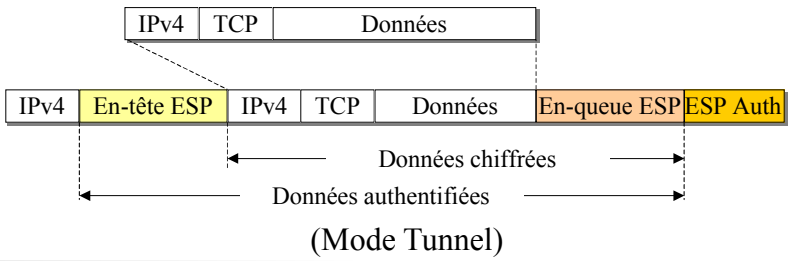
- SPI : identifie la SA utilisée
- Numéro de séquence: protection contre le rejeu de paquets
- Données d'authentification: p.ex. signature numérique



heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Service ESP

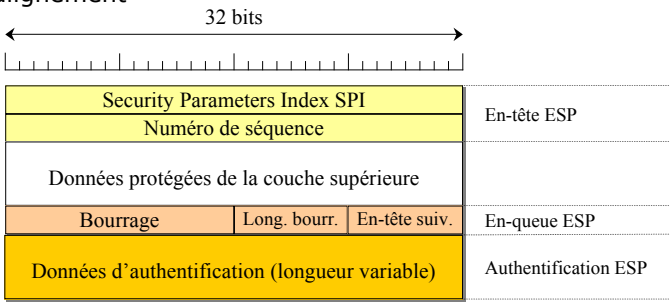
- ESP : Encapsulation Security Payload
  - Confidentialité des données
  - Authentification de l'origine des données
  - Protection d'anti-rejeu
  - Intégrité des données



heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Format des en-têtes et en-queues

- En-tête ESP:
  - Permet de retrouver la SA utilisée pour le paquet
- En-queue ESP:
  - Bourrage pour corriger l'alignement
- Authentification ESP:
  - Signature numérique, …
- Données
  - Chiffrées et authentifiées



Résumé

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

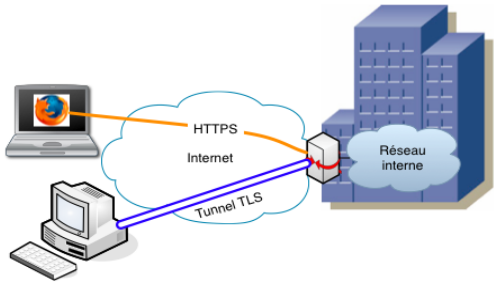
- *Les VPN permettent de créer des réseaux logiques et privés sur une infrastructure partagée par beaucoup d'utilisateurs*
- Méthode de réalisation : IPSec
  - Fournit une méthode générique pour créer des transmissions avec authentification, intégrité et confidentialité
  - Deux services
    - En-tête d'authentification → Authentification et intégrité
    - Encapsulation ESP → Authentification, intégrité et confidentialité
  - Deux modes
    - Mode Transport → Host to Host ou Host to LAN
    - Mode Tunnel → LAN to LAN à travers des passerelles

Tutorial IBM ch. 22.7 + 22.8

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

VPNs avec SSL/TLS

- Développé originellement par Netscape et RSA
- TLS est le successeur de SSL (RFC 2246)
- Sécurisation de FTP (FTPS), HTTP (HTTPS),…
- Tous les navigateurs intègrent SSL/TLS
- Aucun client VPN nécessaire à travers le navigateur



heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

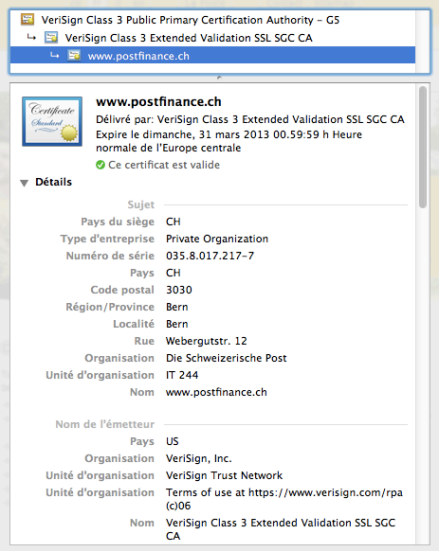
Protocoles SSL et TLS

- SSL Version 1: Version oroginale, plus utilisée
- Version 2: Négociation originale pas protégée, attaquable, déconseillée.
- Version 3: Corrige les défaults de la version 2

Protocoles SSL et TLS

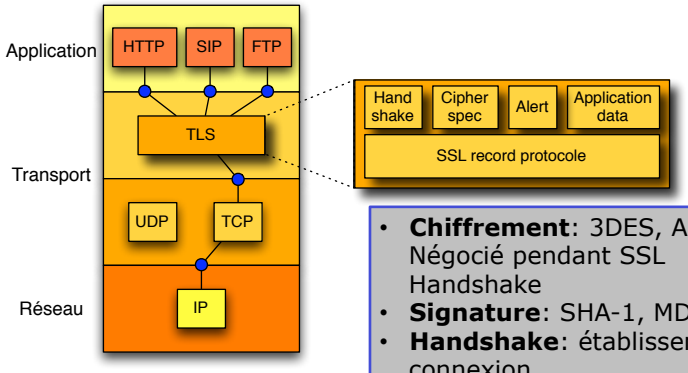
heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

Exemple avec Postfinance:



heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

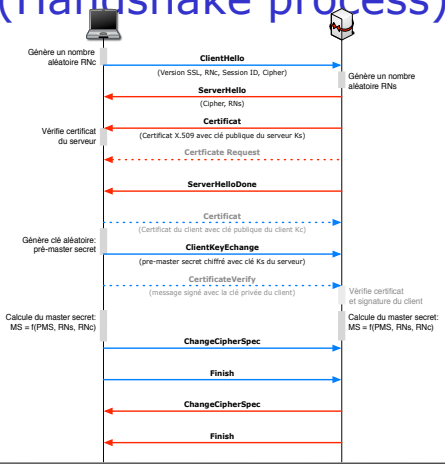
TLS dans le modèle TCP/IP



- **Chiffrement**: 3DES, AES… Négocié pendant SSL Handshake
- **Signature**: SHA-1, MD5
- **Handshake**: établissement connexion
- **Alert**: Signale erreurs lors établissment connexion

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

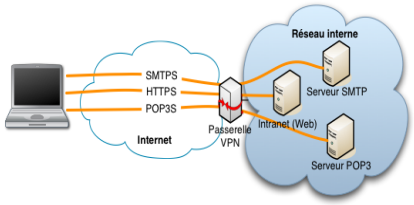
Etablissement d'une connexion TLS avec échange de clé RSA (Handshake process)



heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

VPN TLS sans client

Avantage: aucune installation
Utilisation: Internet cafés



VPN TLS avec client

- Service similaire à IPSec
- Host-to-LAN: interface virtuelle à laquelle une adresse du réseau est assignée. Tout le trafic passe par là.
- LAN-to-LAN: tout le trafic passe par le tunnel établi par les passerelles TLS.