Université de Guelma
Département Informatique

# Chapitre 3 : Les certificats de sécurité

Cours - Sécurité Informatique

3 année LMD SI & ISIL

Par : Dr. M. A. Ferrag

# Plan du cours

- **IPSec**
- **Certificat numérique X.509**
- **VPN**

# Rappels

Un système cryptographique repose sur deux éléments fondamentaux:

- Des primitives cryptographiques
  - Chiffrement symétrique/asymétrique
  - Calcul d'empreinte
  - Signatures
- Des protocoles
  - Signatures numériques
  - Gestion de clés
  - Communications sécurisées
  - Authentification
  - ...

# Rappels

Un système cryptographique fournit un ensemble des propriétés suivantes:

- Confidentialité
- Intégrité
- Authenticité
- Non-répudiation

# Protocoles

Qu’est-ce qu’un protocole ?

*protocole (n.m.): Ensemble de règles définissant le mode de communication entre deux ordinateurs.*

De manière générale, cela peut s’appliquer à toutes communications entre

plusieurs entités, ainsi qu’à autre chose que des communications.

Lorsque l’on souhaite construire un protocole cryptographique, une fois l’ objectif précisé, on définit:

- L’ensemble des étapes nécessaires
- Le fond et la forme des échanges

# Protocoles

Construction:

- Un protocole cryptographique est basé sur des primitives, des algorithmes, et éventuellement d'autres protocoles.

Exemple: Station-to-Station est basé sur Diffie-Hellman, et utilise de la signature numérique (comme DSA ou ECDSA)

- Problème du maillon faible: le plus faible algorithme, ou une mauvaise combinaison, peut présenter un point de rupture…

# Internet Protocol Security (IPSec)

# Internet Protocol Security (IPSec) (1)

- IPsec (Internet Protocol Security), défini par l'IETF comme un cadre de standards ouverts pour assurer des communications privées et protégées sur des réseaux IP, par l'utilisation des services de sécurité cryptographiques

- IPsec se différencie des standards de sécurité antérieurs en n'étant pas limité à une seule méthode d'authentification ou d'algorithme et c'est la raison pour laquelle il est considéré comme un cadre de standards ouverts

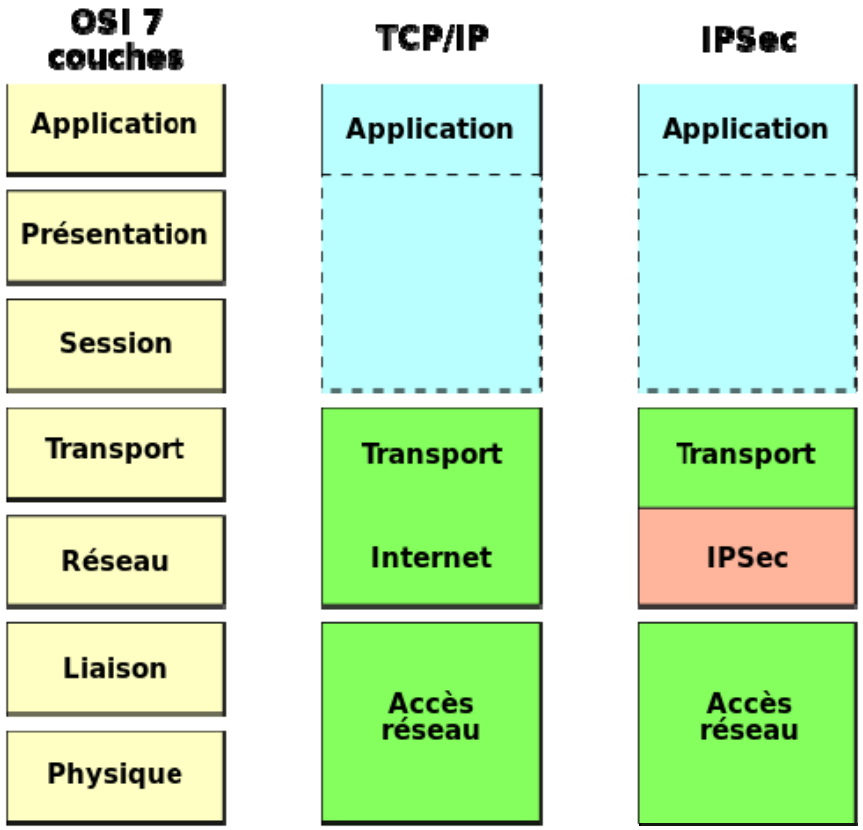
# Liste des RFC relatives à IPsec

| RFC | Description |
|---|---|
| **RFC 6071 [1]** | Feuille de route du document du IPsec et IKE |
| **RFC 4835 [2]** | Exigences de mise en œuvre de l'algorithme de cryptographie pour l'encapsulation de la charge utile de sécurité (ESP) et l'en-tête d'authentification (AH) |
| **RFC 4308 [3]** | Suites cryptographiques pour IPsec |
| **RFC 4305 [4]** | Extensions de protocole de statut de certificat en ligne (OCSP) sur IKEv2 |


1. Frankel, S., & Krishnan, S. (2011). *IP security (IPsec) and internet key exchange (IKE) document roadmap* (No. RFC 6071).
2. Manral, V. (2007). Cryptographic algorithm implementation requirements for encapsulating security payload (esp) and authentication header (ah).
3. Hoffman, P. (2005). Cryptographic suites for IPsec.
4. Myers, M., & Tschofenig, H. (2007). Online Certificate Status Protocol (OCSP) Extensions to IKEv2. RFC 4806.

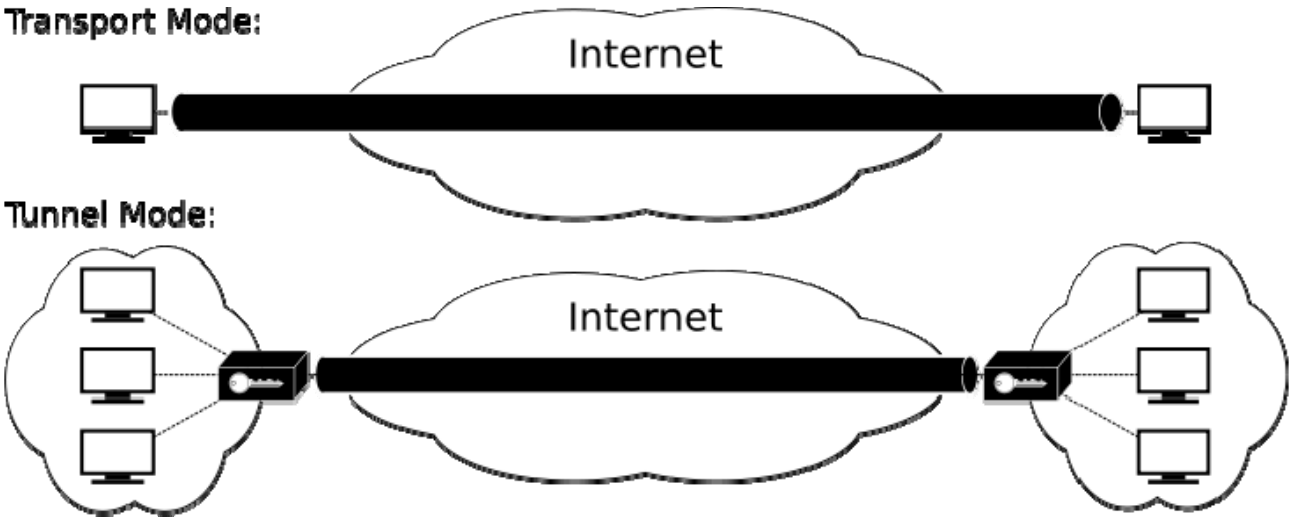
# Internet Protocol Security (IPSec) (2)

- IPsec opère à la couche réseau (couche 3 du modèle OSI) contrairement aux standards antérieurs qui opéraient à la couche application (couche 7 du modèle OSI), ce qui le rend indépendant des applications, et veut dire que les utilisateurs n'ont pas besoin de configurer chaque application aux standards IPsec.



# IPSec - Modes de fonctionnement

- **Mode transport :** Dans le mode transport, ce sont uniquement les données transférées (la partie payload du paquet IP) qui sont chiffrées et/ou authentifiées.
- **Mode tunnel :** En mode tunnel, c'est la totalité du paquet IP qui est chiffré et/ou authentifié.



# Le protocole SSL/TLS (1)

- Secure Socket Layer est un protocole légèrement supérieur à la couche 4 du modéle OSI. Il a pour objectif, tel qu'il est définit dans la RFC 2246, de fournir la confidentialité et l'intégrité des données entre deux applications en communication.

- La version actuelle de SSL est la 3.1, connue sous le nom de TLS (Transport Layer Security). Ce changement de nom marque le rachat du brevet SSL par l'IETF, appartenant initialement à Netscape. Nous parlerons donc plutôt de TLS que de SSL, cette nouvelle appelation risquant fort de supplanter la première dans les années qui viennent.

# TLS

TLS: Transport Layer Security

Il s'agit du successeur de SSL. TLS version 1 est fortement basé sur SSL version 3.

Principaux objectifs de sécurité:

- Authenticité du serveur
- Confidentialité et intégrité des échanges
- En option, authentification du client par certificat numérique

En principe, fournit une grande flexibilité d'usage: les protocoles applicatifs peuvent fonctionner de façon transparente derrière une connexion TLS.

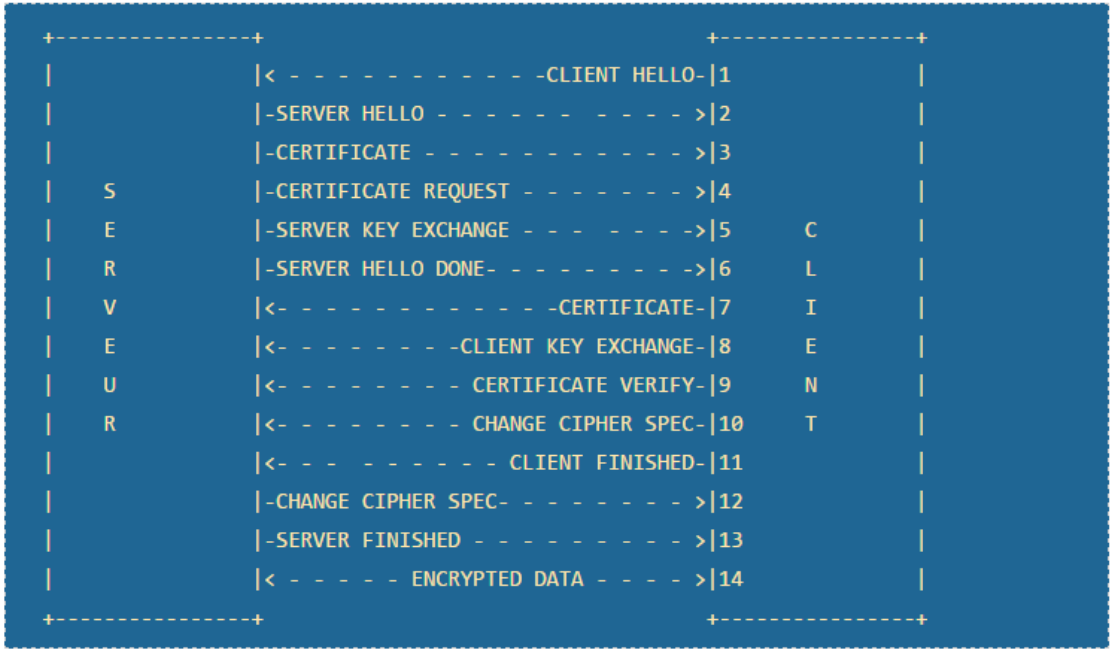
# TLS

- Le protocole se découpe en deux étapes:
  - Négociation (handshake)
  - Chiffrement (Record Protocol)
- La première phase met en place et vérifie les éléments de sécurité
- La deuxième utilise ces éléments afin de fournir les propriétés de sécurité.

# TLS

**1 - Négociation**

- Le client envoie la liste des algorithmes de chiffrement qu'il supporte
- Le serveur prend le "meilleur" algorithmes de cette liste qu'il supporte, et renvoi une valeur aléatoire S (identifiant de session) ainsi que son certificat
- Optionnellement, le client peut alors envoyer son propre certificat (si demandé par le serveur)
- Le client génère une clé "pré-maitre" aléatoire, la chiffre avec la clé publique du serveur, et lui envoit
- Le serveur et le client utilisent cette clé pour générer une première clé de session
- Le client envoi une notification au serveur indiquant qu'il commence à utiliser cette clé de session.

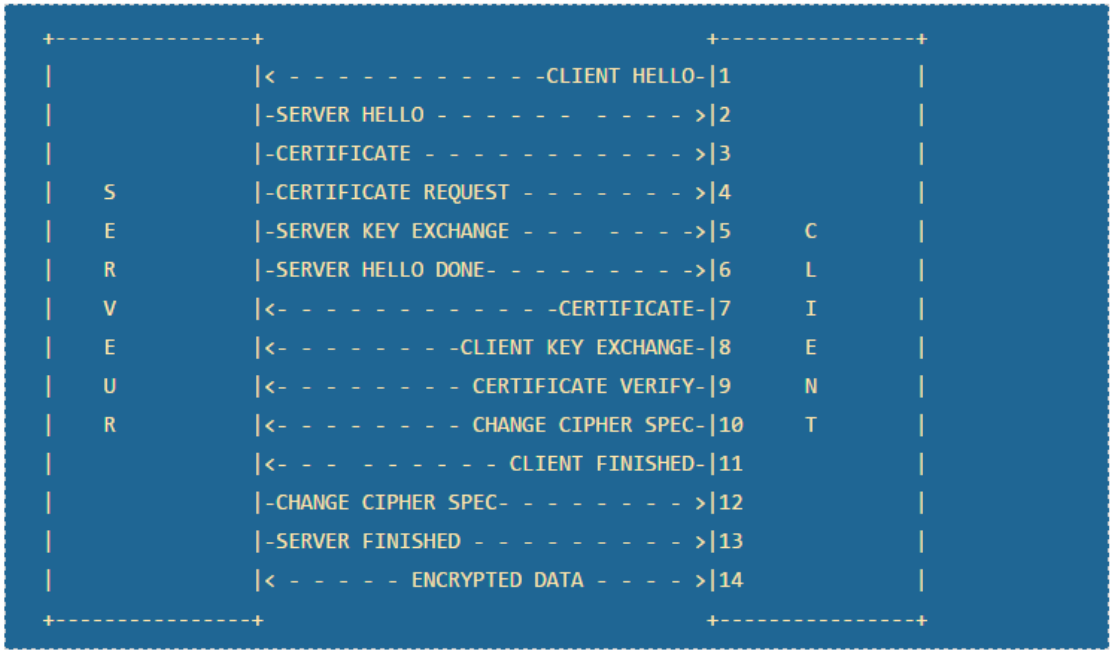


# TLS

## 1bis - Reprise de l'échange

TLS permet de reprendre un échange interrompu sans reproduire l'intégralité de la négociation:

- Le client envoi l'identifiant d'une session précédemment établie
- Si le serveur la retrouve, il renvoi cet identifiant au client
- Le client génère une nouvelle clé de session à partir de la clé maître, et notifie le serveur de l'utilisation de cette nouvelle clé
- L'échange reprend avec le chiffrement

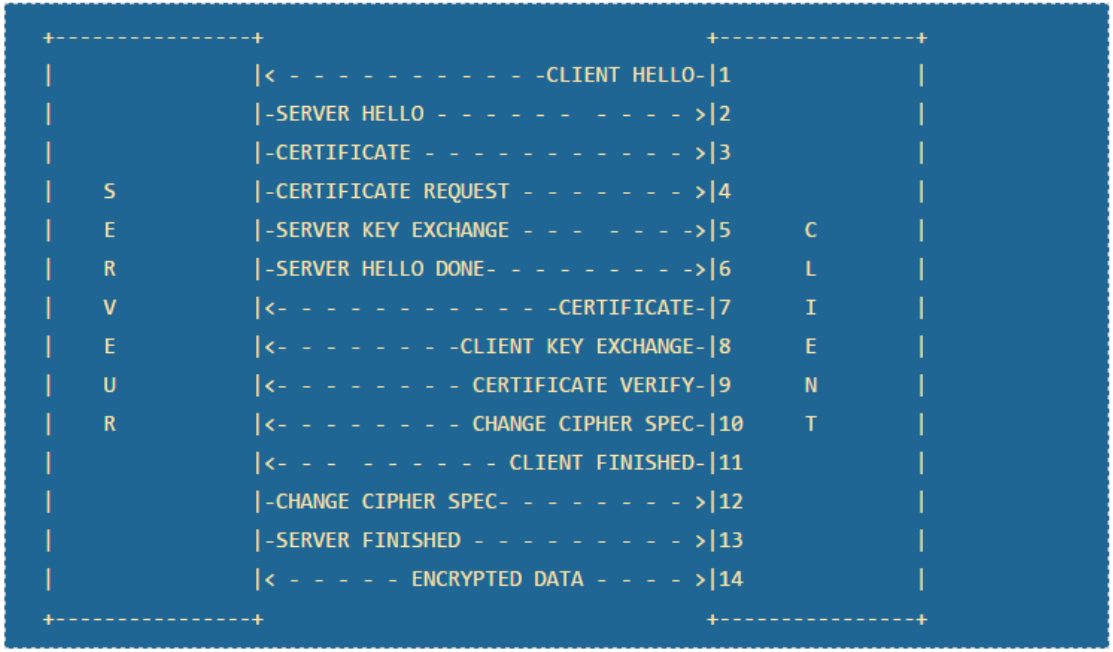


# TLS

## 2 - Chiffrement

Une fois la clé de session déterminée, TLS chiffre toutes les communications

- Découpage des données en blocs de taille compatibles avec le chiffrement utilisé
- Utilisation d'un MAC pour l'intégrité
- Chiffrement
- Envoi



# Le protocole SSL/TLS

- SSL utilise le chiffrement symétrique conventionnel pour chiffrer les messages au cours d'une session. Il existe neuf choix possibles pour le chiffrement, y compris l'option du transfert non chiffré :
    - Pas de chiffrement
    - Chiffrement en continu (Stream Ciphers)

    RC4 avec clés de 40 bits
    RC4 avec clés de 128 bits
    - Chiffrement par blocs CBC (CBC Block Ciphers)

    RC2 avec clé de 40 bits
    DES avec clé de 40 bits
    DES avec clé de 56 bits
    Triple-DES avec clé de 168 bits
    Idea (clé de 128 bits)
    Fortezza (clé de 96 bits)

# Le protocole SSL/TLS

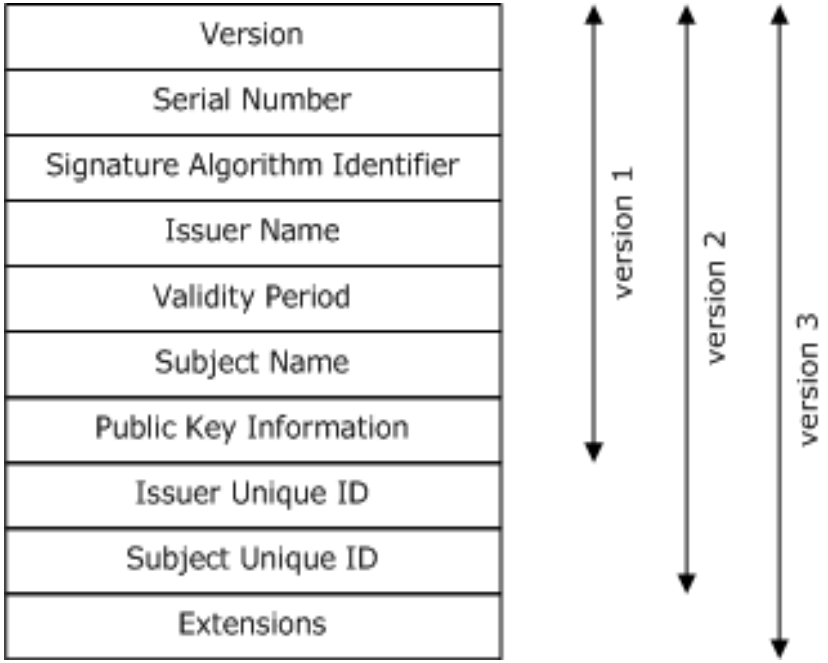
**En pratique, le SSL devrait être utilisé dans les cas suivants :**

- Pour sécuriser les transactions bancaires en ligne.
- Pour sécuriser les connexions et tout échange d'information confidentielle .
- Pour sécuriser les applications et les messageries web, telles que Outlook Web Access, Exchange et Office Communications Server.
- Pour sécuriser les flux de production et les applications de virtualisation tels que Citrix Delivery Platforms et les plates-formes sur le Cloud.
- Pour sécuriser les connexions entre un client de messagerie, tel que Microsoft Outlook et un serveur mail, tel que Microsoft Exchange.
- Pour sécuriser le transfert de fichiers au travers de services « https » et FTP, dans les cas de mise à jour de sites Internet par exemple.
- Pour sécuriser les connexions aux panneaux de contrôle et les activités d'hébergement, telles que Parallels, cPanel, et bien d'autres encore.
- Pour sécuriser les traffics intranet.
- Pour sécuriser les connexions aux réseaux et aux traffics de réseaux utilisant les VPNs SSL, tels que VPN Access Servers, et les applications, telles que Citrix Access Gateway.

# Certificat numérique X.509

# Version X. 509

- Depuis sa création en 1998, trois versions de la norme de certificat de clé publique X.509 ont évolué. Comme le montre la Figure, chaque version successive de la structure de données a conservé les champs qui existaient dans les versions précédentes et ajouté plus.



# Certificat numérique X.509

- Un certificat numérique est une sorte de “carte d'identité” d'une entité informatique.

**1.Version** la version de X.509
**2.Serial Number** un numéro de série
**3.Signature Algorithm** les algos qui ont signés le certificat
**4.Issuer** l'autorité qui a signé le certificat
**5.Validity** la période de validité
**6.Subject** le propriétaire du certificat
**7.Subject Public Key Info** des infos concernant la clé publique

```
Certificate:
 Data:
     Version: 3 (0x2)
     Serial Number: 3 (0x3)
     Signature Algorithm: sha1WithRSAEncryption
     Issuer: C=FR, ST=Indre-et-Loire, L=Tours, O=Resgate Security
Department, CN=authority.microgate.fr/emailAddress=security@microgate.fr
     Validity
         Not Before: May 13 15:33:45 2005 GMT
         Not After : May 11 15:33:45 2015 GMT
     Subject: C=FR, ST=Indre-et-Loire, L=Tours, O=Resgate Security
Department, CN=webmail.microgate.fr/emailAddress=security@microgate.fr
     Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
         RSA Public Key: (2048 bit)
             Modulus (2048 bit):
                 00:b4:bf:b6:d0:e6:af:30:5e:5f:a4:b8:6c:01:37:
                 0e:81:e4:c5:11:6e:08:e8:05:24:0d:30:ef:94:35:
```

# Version 3 Extensions

- Version 3 Extensions : Un certificat X.509 version 3 contient les champs définis dans la version 1 et la version 2 et ajoute des extensions de certificat. Les extensions standard de la version 3 et leurs identifiants d'objet (OID) sont répertoriés dans le Tableau.

```
-----------------------------------------------------------------
-- Extensions (beginning with version 3).
-----------------------------------------------------------------
Extensions ::= SEQUENCE OF Extension

Extension ::= SEQUENCE
{
  Id              OBJECT IDENTIFIER,
  critical          BOOLEAN DEFAULT FALSE,
  extnValue         OCTET STRING
}
```

# Les extensions standard de la version 3 du certificat X.509

| Extension | Description |
|---|---|
| Authority Key Identifier (2.5.29.19) | Identifie la clé publique de l'autorité de certification (CA) qui correspond à la clé privée du CA utilisée pour signer le certificat. |
| Basic Constraints (2.5.29.35) | Spécifie si l'entité peut être utilisée comme CA et, le cas échéant, le nombre de CA subordonnées qui peuvent exister dans la chaîne de certificats. |
| Certificate Policies (2.5.29.32) | Spécifie les règles sous lesquelles le certificat a été délivré et les fins pour lesquelles il peut être utilisé. |
| CRL Distribution Points(2.5.29.31) | Contient l'URI de la liste de révocation de certificat de base (CRL). |
| Enhanced Key Usage (2.5.29.46) | Spécifie la manière dont la clé publique contenue dans le certificat peut être utilisée. |
| Issuer Alternative Name (2.5.29.8) | Spécifie un ou plusieurs formulaires de nom alternatif pour l'émetteur de la demande de certificat. |
| Key Usage (2.5.29.15) | Spécifie les restrictions sur les opérations qui peuvent être effectuées par la clé publique contenue dans le certificat. |
| Name Constraints (2.5.29.30) | Spécifie l'espace de noms dans lequel tous les noms de sujet d'une hiérarchie de certificats doivent être localisés. L'extension n'est utilisée que dans un certificat CA. |
| Policy Constraints (2.5.29.36) | Limite la validation du chemin en interdisant le mappage des politiques ou en exigeant que chaque certificat de la hiérarchie contienne un identifiant de politique acceptable. L'extension n'est utilisée que dans un certificat CA. |
| Policy Mappings (2.5.29.33) | Spécifie les stratégies dans une autorité de certification subordonnée qui correspondent aux règles de l'autorité de certification émettrice. |
| Private Key Usage Period (2.5.29.16) | Spécifie une période de validité différente pour la clé privée que pour le certificat avec lequel la clé privée est associée. |
| Subject Alternative Name (2.5.29.17) | Spécifie un ou plusieurs formulaires de nom alternatif pour le sujet de la demande de certificat. Les exemples de formes alternatives incluent les adresses e-mail, les noms DNS, les adresses IP et les URI. |
| Subject Directory Attributes (2.5.29.9) | Transmet les attributs d'identification tels que la nationalité du sujet du certificat. La valeur d'extension est une séquence de paires OID-valeur. |
| Subject Key Identifier (2.5.29.14) | Se différencie entre plusieurs clés publiques détenues par le sujet du certificat. La valeur d'extension est généralement un hachage SHA-1 de la clé. |

# VPN – Virtual Private Network

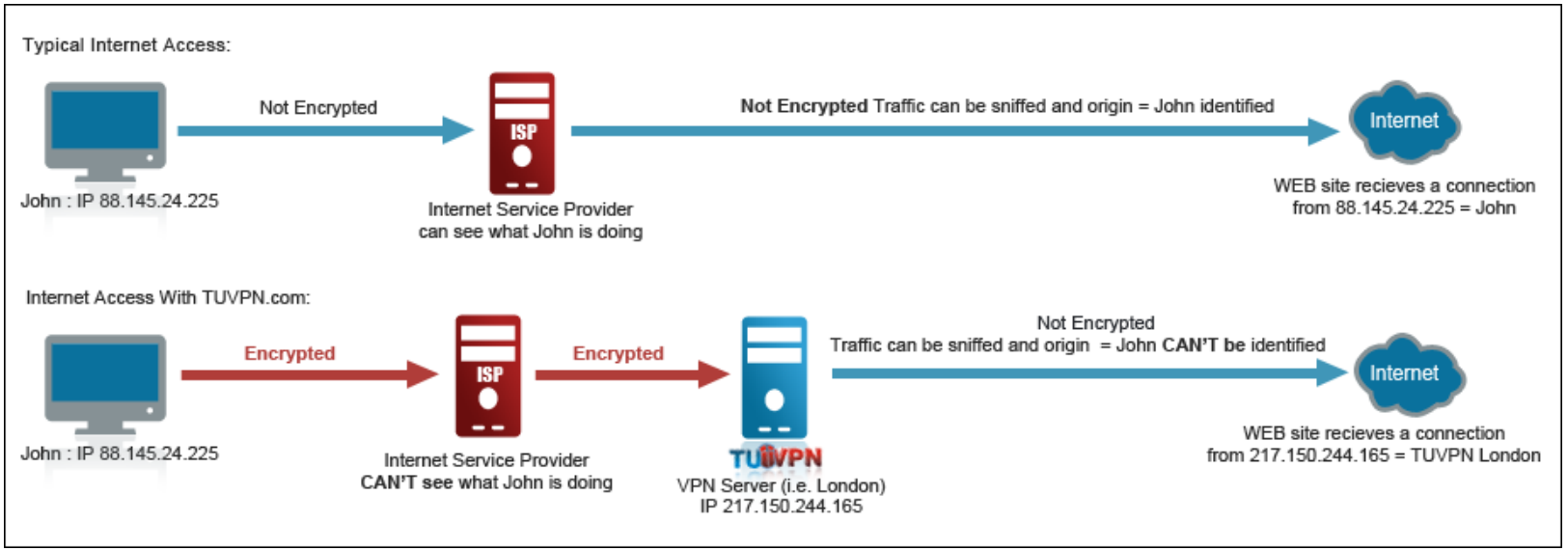
1. Généralités
2. Les différents types de VPN
3. Les protocoles utilisés
4. Les implémentations

# VPN - Généralités

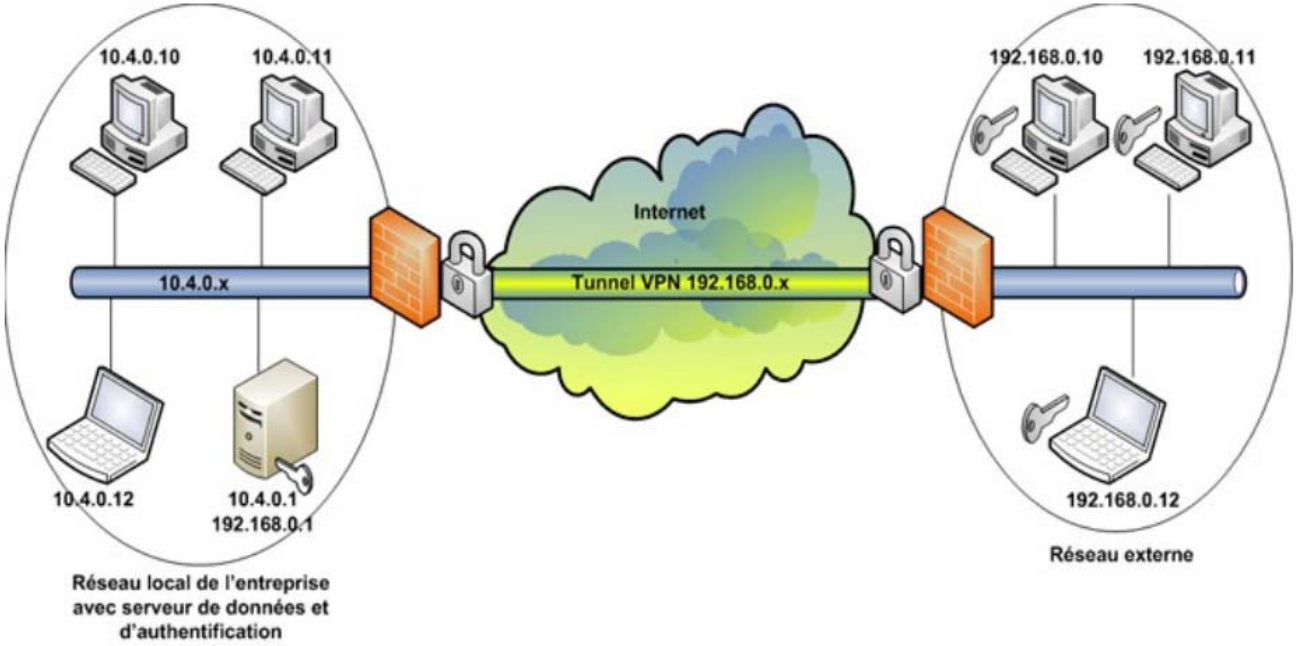
- Un VPN ou RPV (réseau privé virtuel) est une technique permettant à un ou plusieurs postes distants de communiquer de manière sure.

- Il permet d'utiliser les infrastructures publiques (Internet).

# VPN - Généralités



# VPN - Généralités




- Un réseau VPN repose sur un protocole appelé "protocole de tunneling". Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel. Les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

# VPN - Généralités

Les principaux avantages d'un VPN :

- Sécurité : assure des communications sécurisées et chiffrées;
- Simplicité : utilise les circuits de télécommunication classiques;
- Économie : utilise Internet en tant que média principal de transport, ce qui évite les coûts liés à une ligne dédiée.

# VPN - Généralités

Les contraintes d'un VPN :

- Le principe d'un VPN est d'être transparent pour les utilisateurs et pour les applications y ayant accès.
- Il doit être capable de mettre en oeuvre les fonctionnalités suivantes :
  - Authentification d'utilisateur : seuls les utilisateurs autorisés doivent avoir accès au canal VPN;
  - Cryptage des données : lors de leur transport sur Internet, les données doivent être protégées par un cryptage efficace;
  - Gestion de clés : les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées (pertes, vols, licenciement);
  - Prise en charge multi protocoles : la solution VPN doit supporter les protocoles les plus utilisés sur Internet (en particulier IP).

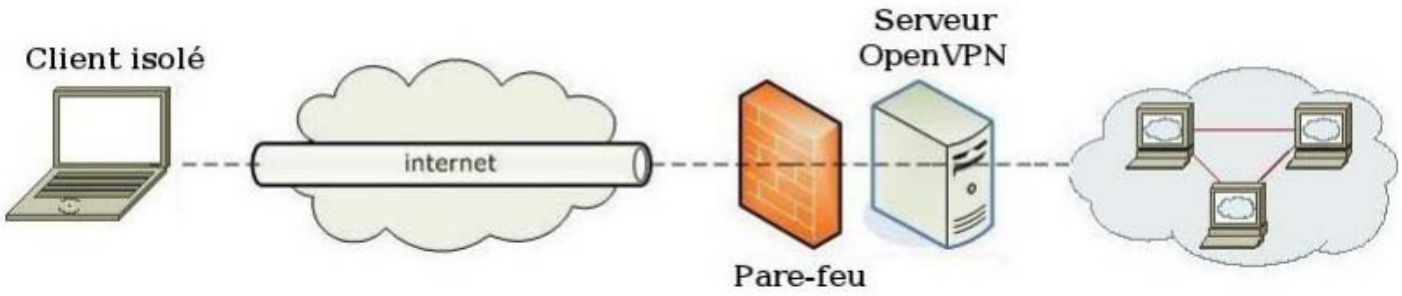
# VPN - Les différents types de VPN

Suivant les besoins, on référence 3 types de VPN :

- Le VPN d'accès;
- L'intranet VPN;
- L'extranet VPN.

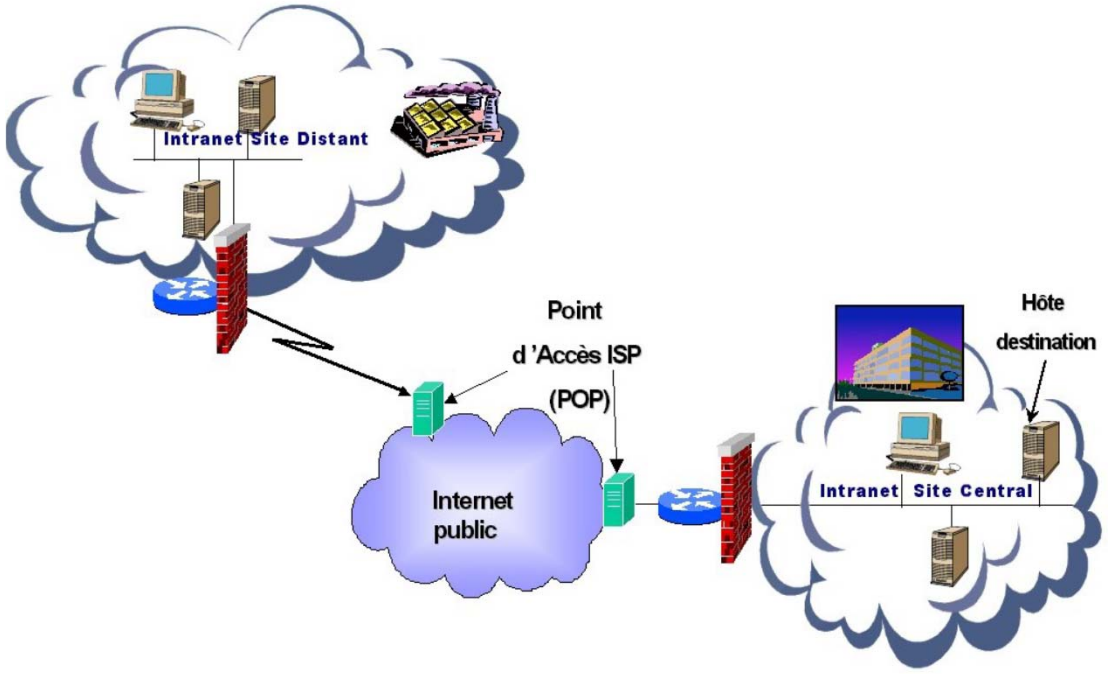
# VPN - Les différents types de VPN

Le VPN d'accès : il est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau de leur entreprise. L'utilisateur se sert d'une connexion Internet afin d'établir une liaison sécurisée.



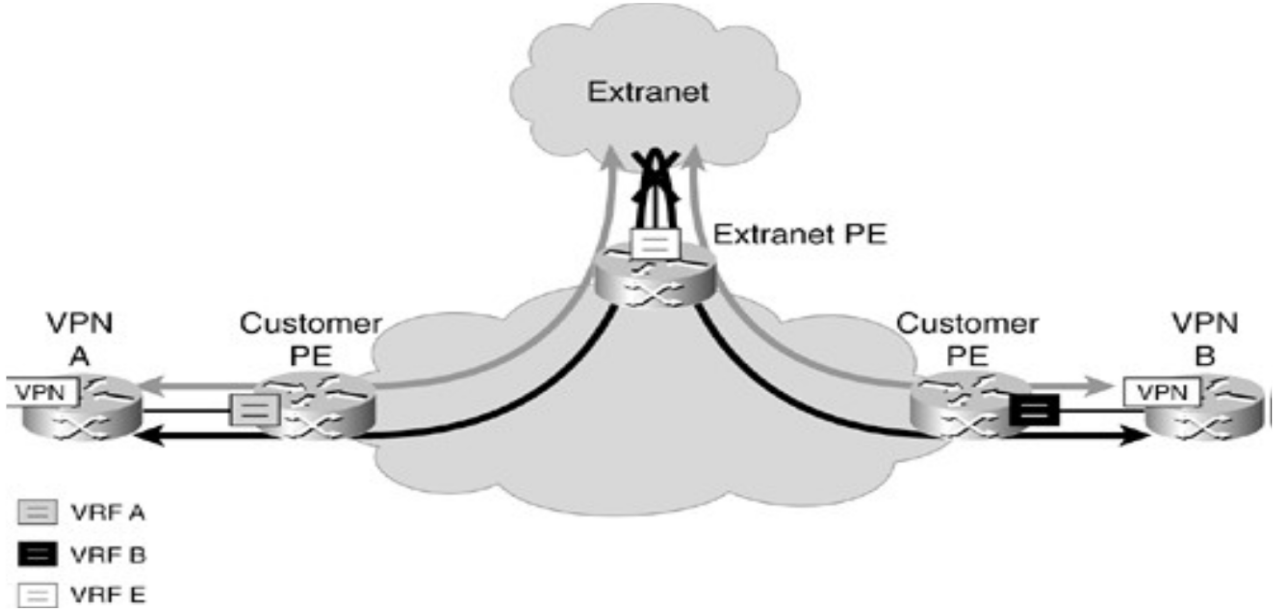
# VPN - Les différents types de VPN

- L'intranet VPN : il est utilisé pour relier deux ou plusieurs intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants.
- Cette technique est également utilisée pour relier des réseaux d'entreprise, sans qu'il soit question d'intranet (partage de données, de ressources, exploitation de serveurs distants …);



# VPN - Les différents types de VPN

- L'extranet VPN : une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires.
- Elle ouvre alors son réseau local à ces derniers et il est nécessaire d'avoir une authentification forte des utilisateurs, ainsi qu'une trace des différents accès.
- Souvent, seule une partie des ressources est partagée, ce qui nécessite une gestion rigoureuse des espaces d'échange.



# Les protocoles utilisés

## VPN

# VPN - Les protocoles utilisés

- Les protocoles utilisés dans le cadre d'un VPN sont de 2 types, suivant le niveau OSI:
    - Les protocoles de niveau 2 comme PPTP.
    - Les protocoles de niveau 3 comme Ipsec.

# Le protocol PPT (1/2)

PPTP
Point-to-Point Tunneling Protocol

- Fonctionnement

Le principe du protocole PPTP (RFC2637) (Point To Point Tunneling Protocol) est de créer des trames avec le protocole PPP et de les crypter puis de les encapsuler dans un paquet IP.

Cela permet de relier les deux réseaux par une connexion point à point virtuelle acheminée par une connexion IP sur Internet. Cela fait croire aux deux réseaux qu'ils sont reliés par une ligne directe.

On garde, ainsi les adresses des réseaux physiques dans la trame PPP cryptées et cette trame est acheminée normalement sur Internet vers l'autre réseau

# Le protocole PPTP (2/2)


Il permet les opérations suivantes :

- L'authentification se fait par le protocole MSCHAP (Challenge Handshake Authentification Protocol) version 2 ou avec le protocole PAP (Password Authentification Protocol)
- L'encryption se fait par le procotole MPPE (Microsoft PointtoPoint Encryption). Cela crée un tunnel de niveau 3 (Réseau) géré par le protocole GRE (Generic Routing Encapsulation).
- La compression peut se faire avec le protocole MPPC (Microsoft Point to Point Compression)
- On peut ajouter autant de protocole que l'on veut dans le protocole PPTP pour l'encryption et la compression des données

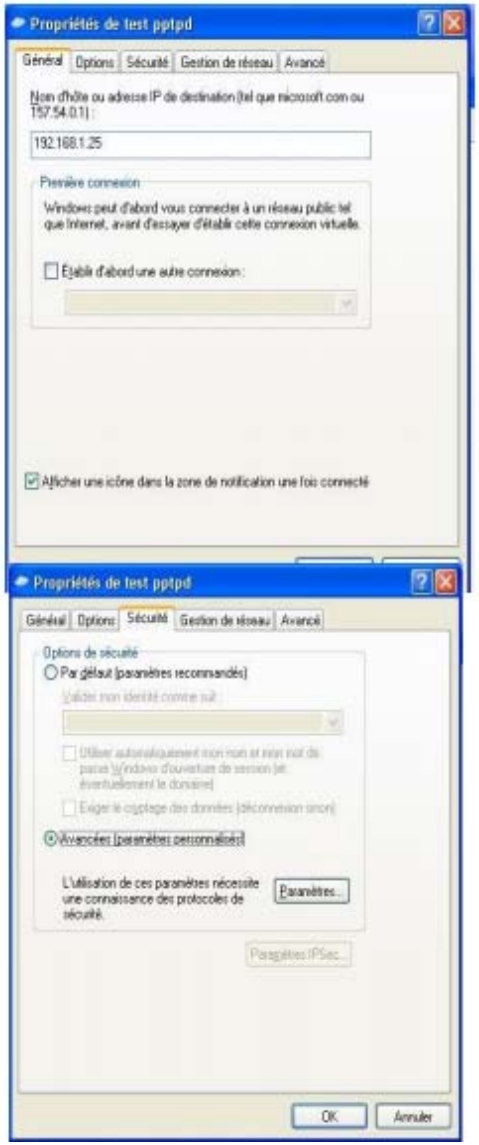
# Le protocole PPTP
# Configurer un client PPTP sous Windows

- Panneau de configuration
- Connexions réseaux et accès à distance
- Créez une nouvelle connexion à distance :

  - Réseau d'entreprise/Réseau Privé Virtuel

  - Remplir avec l'IP du serveur PPTP et les logins/mots de passes que l'on vous a attribués

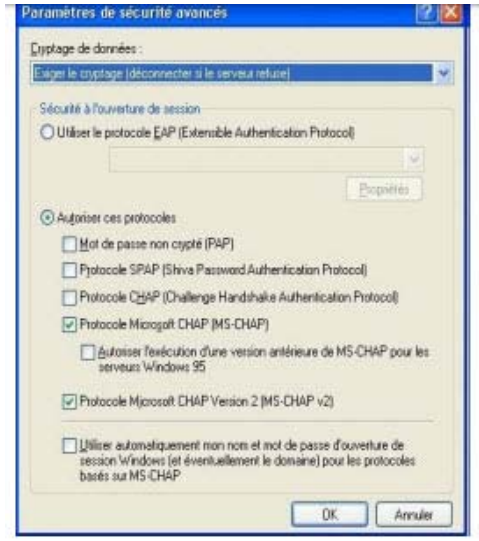
- Editer les propriétés de la connexion afin d'obtenir quelque chose comme ceci :

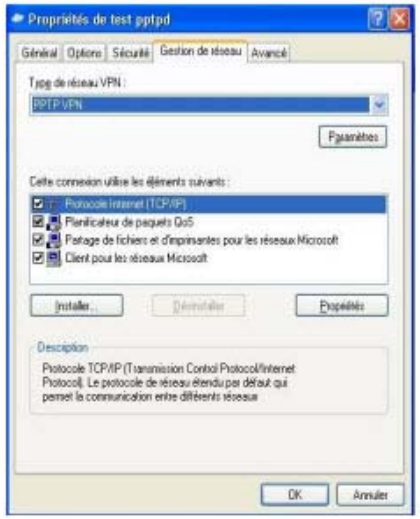




PPTP

Point-to-Point Tunneling Protocol





PPTP

Point-to-Point Tunneling Protocol

# Les implementations

## VPN

# VPN - Les implementations Logicielles (1)

Racoon, s'intègre au noyau Linux et permet de gérer les authentifications suivantes:

- Mot de passe de groupe (tous les utilisateurs ont le même mdp)
- Login / password
- Certificats x509

OpenVPN, s'installe comme paquetage et permet de gérer les authentifications suivantes:

- Certificats SSL
- Login / password

# VPN - Les implementations Logicielles (2)

**EJBCA (Enterprise Java Bean Certificates Authority**), est certainement la PKI la plus aboutie (gratuite) et permet de gerer :

- La creation de certificats;
- Le renouvellement ;
- Certificats x509 ;
- SCEP (Simple Certificates Enrollment Protocol)
- OCSP (Open Certificates Status Protocol)

# VPN - Les implementations materials

Plusieurs marques proposent des passerelles VPN:

Zyxel USG100


Cisco ASA5505

Sonicwall VPN2000

# VPN - Distributions dédiées et gratuites

Plusieurs marques proposent des passerelles VPN:

Monowall

PfSense

IpCop

# Reference

- Dieter Gollmann "Computer Security" (3ème édition, mais 2ème est également bien)

Http://www.amazon.com/Computer-Security-Dieter-Gollmann/dp/0470741155

- Ross Anderson " Security Engineering "

Http://www.amazon.com/Security-Engineering-Building-Dependable-Distributed/dp/0470068523/

(Également disponible en ligne à: http://www.cl.cam.ac.uk/~rja14/book.html)

- Avoine, G., Junod, P., & Oechslin, P. (2015). Sécurité informatique-Cours et exercices corrigés. (3ème édition, mais 2ème est également bien)

Disponible à la bibliothèque de l'Université de Guelma