Réseaux

Virtual Private Network

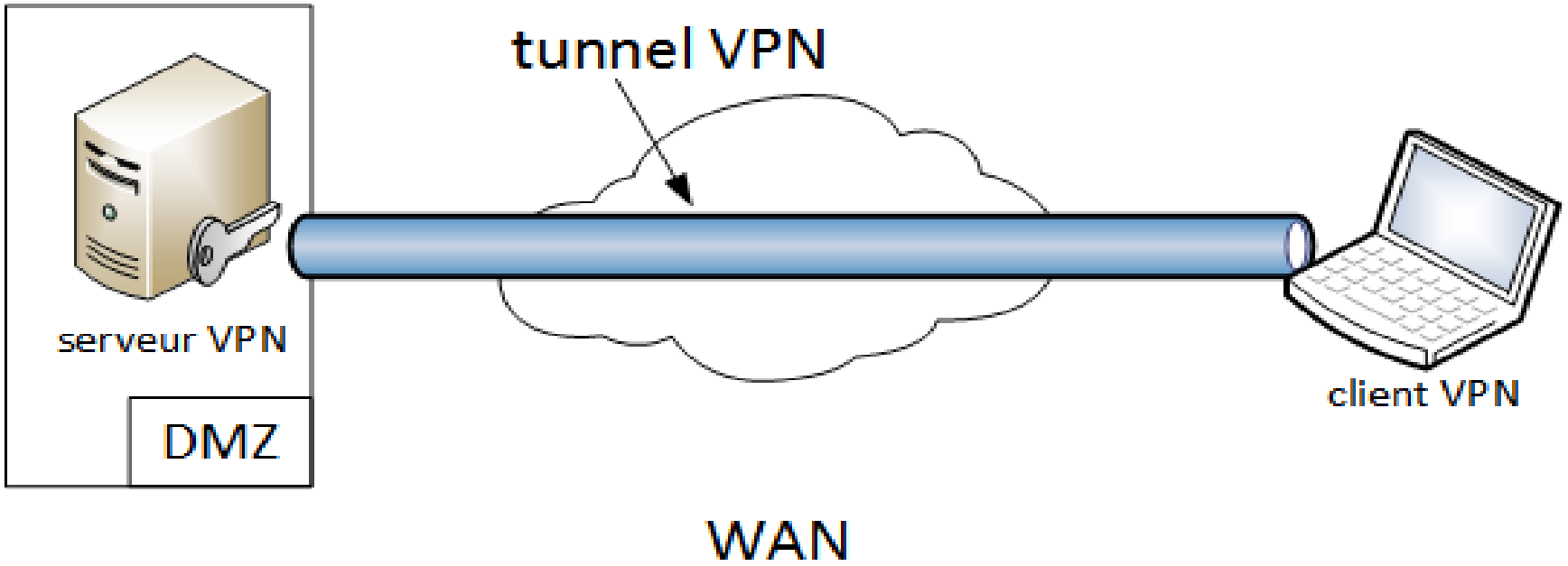
Sommaire

Généralités

Un réseau VPN repose sur un protocole appelé "protocole de tunneling".

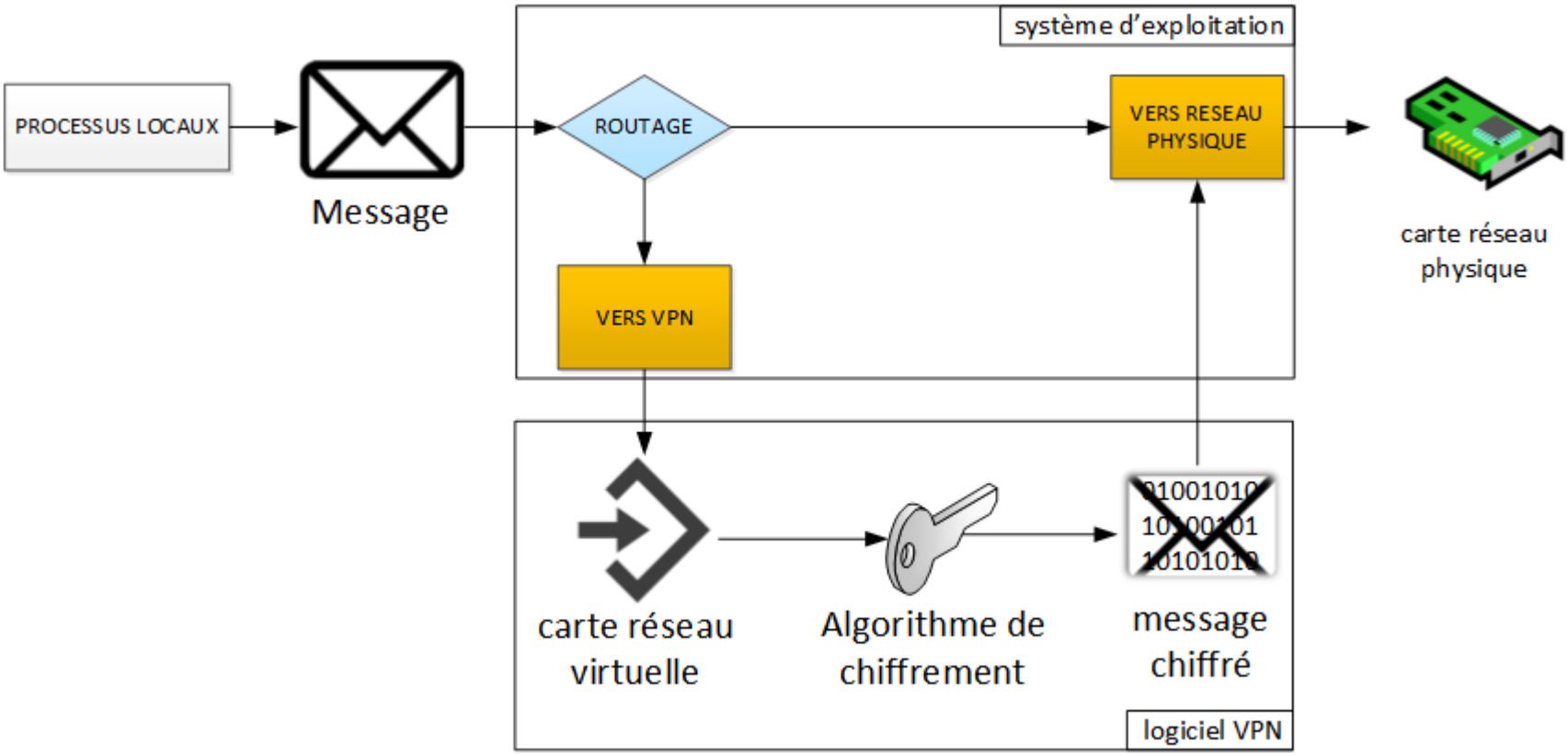
Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel.

Les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.



Le tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire.

La source chiffre les données et les achemine en empruntant ce chemin virtuel.



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.

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;
- Chiffrement des données : lors de leur transport sur Internet, les données doivent être protégées par un chiffrement efficace;
- Gestion de clés : les clés de chiffrement 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).

Suivant les besoins, on référence 3 types de VPN :

• Le VPN d'accès : permet à des utilisateurs itinérants d'accéder au réseau de leur entreprise (eg. Commerciaux)

• L'intranet VPN : 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

• L'extranet VPN : une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires

Les protocoles utilisés

Les protocoles utilisés dans le cadre d'un VPN sont de 3 types, suivant le niveau OSI:

- PPTP ou L2TP au niveau 2
- IPsec ou MPLS au niveau 3
- SSL/TLS au niveau 4

IPSec

- RFC240
- Sécurise l'échange de données au niveau de la couche réseau (OSI 3)
- IPSec = IP Security Protocols

IPSec est basé sur deux mécanismes:

- AH → Authentification Header
- ESP → Encapsulating Security Payload

Authentification Header

- Assure intégrité et authenticité des paquets IP.
- Ne fournit aucune confidentialité (données non chiffrées)

Encapsulating Security Payload

- Peut permettre l'authentification des données
- Surtout utilisé pour le chiffrement

Bien qu'indépendants, ces deux mécanismes sont presque toujours utilisés conjointement.

La gestion des clefs

- Les protocoles sécurisés ont recours à des algorithmes de chiffrement.
- Les algorithmes de chiffrement fonctionnent avec des clefs
- Comment gérer ces clés (génération, distribution, stockage et suppression) ?
- Des protocoles spécifiques s'en occupent :
  - ISAKMP (Internet Security Association and Key Management Protocol)
  - IKE (Internet Key Exchange)

Deux modes de fonctionnement:

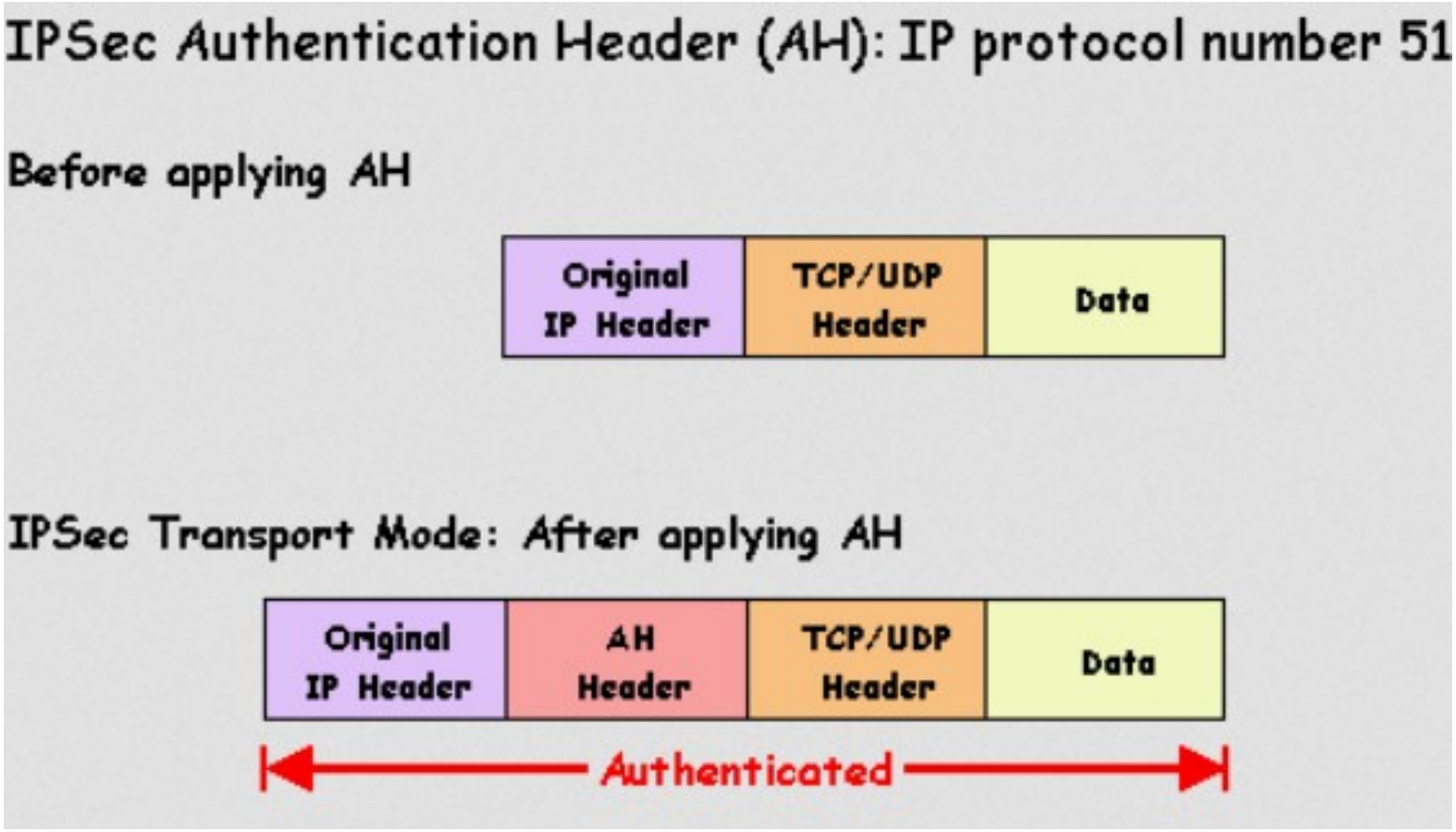
- transport
- tunnel

Mode transport

- Uniquement les données transférées (le payload du paquet IP) sont chiffrées et/ou authentifiées.

- Les adresses IP ne peuvent pas être modifiées sans corrompre l'en-tête AH = impossible de faire du NAT !

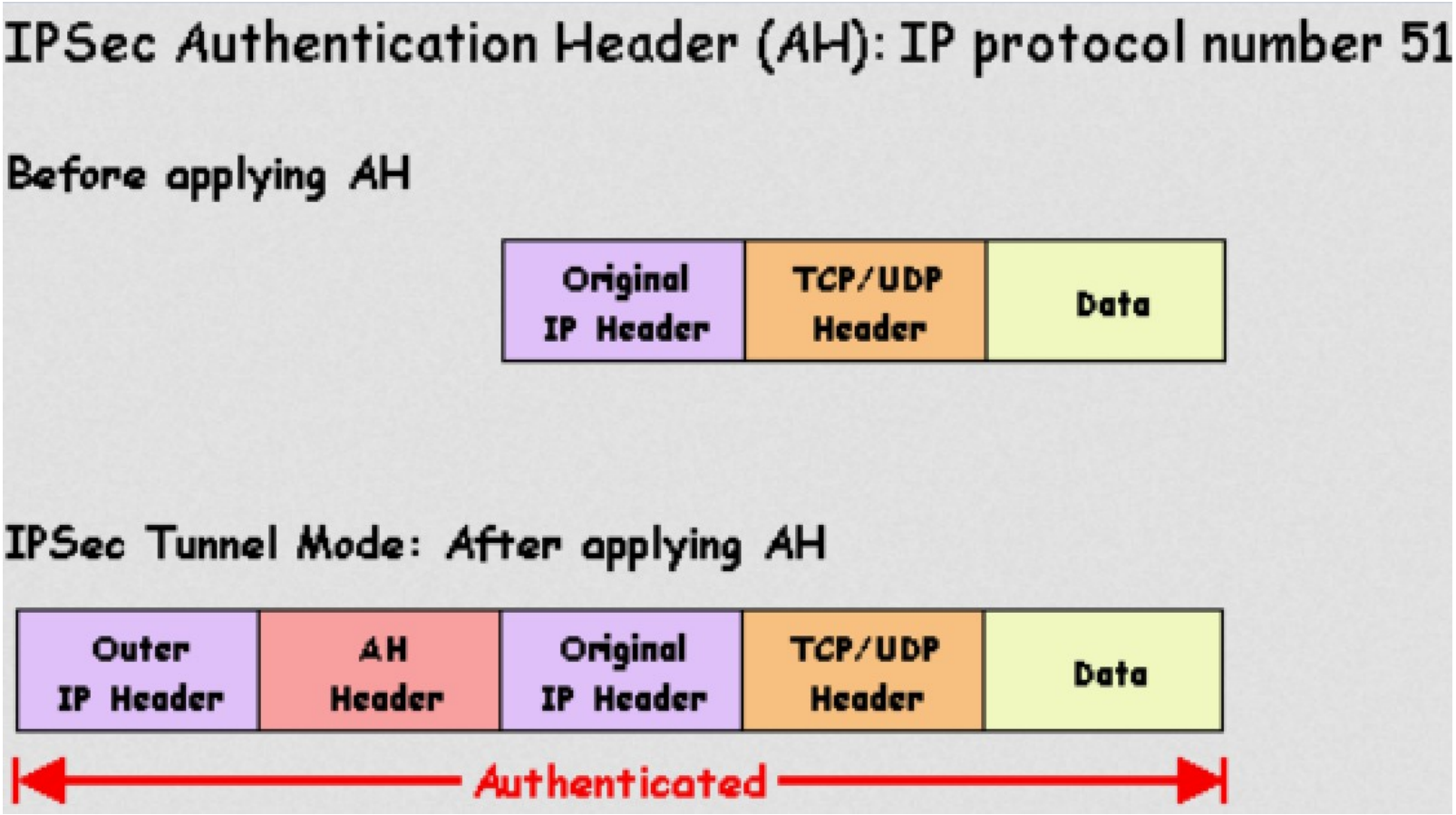
IPSec en mode transport



Mode tunnel

- la totalité du paquet IP est chiffré et/ou authentifié
- Le paquet est ensuite encapsulé dans un nouveau paquet IP
- Ce mode supporte la traversée de NAT
- utilisé pour créer des VPN permettant la communication de réseau à réseau (eg. entre deux sites distants).

Version avec NAT-T (NAT-Traversal)



SSL (Secure Socket Layer)

- protocole de niveau 4
- utilisé par une application pour établir un canal de communication sécurisé avec une autre application.

Deux grandes fonctionnalités :

- l'authentification du serveur et du client
- le chiffrement des données

Les implémentations

Implémentations logicielles:

IPSec

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

SSL/TLS

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

- Certificats SSL
- Login / password

Implémentations logicielles:

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

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

Implémentations matèrielles:

Plusieurs marques proposent des passerelles VPN:

- Zyxel USG100

- Cisco ASA5505

- Sonicwall VPN2000

Distributions dédiées et gratuites :

- Monowall

- PfSense

- IpCop