DE LA RECHERCHE À L'INDUSTRIE

Master 2 SeCReTS
Concepts Sécurité et Réseaux

Introduction aux VPN

www.cea.fr

21 novembre 2019

Introduction aux VPN

Historique

La communication au sein d'une entreprise joue un rôle vital. A l'origine elles étaient composées d'une seule entité ou de plusieurs géographiquement proche. L'ouverture de son système d'information (SI) était alors assez limité.

Des besoins qui ont beaucoup évolué

Les entreprises sont aujourd'hui implantées sur plusieurs sites, que ce soit sur le territoire national ou à l'étranger. Il est devenu crucial d'ouvrir son système d'information non seulement entre les différents sites géographiques mais aussi à des employés devenus itinérants, des collaborateurs et des partenaires afin :

- de permettre une communication toujours plus rapide aux informations
- mutualiser un certain nombre de ressources

Introduction aux VPN

Besoins (suite)

- les besoins ont grandi tant sur le plan qualitatif que quantitatif : les échanges électroniques se développent au détriment du support papier (dématérialisation des échanges) et la quantité d'informations échangées augmente
- pour palier l'éloignement de certaines entités d'une même entreprise, l'organisation de réunions par visio conférence et leur multiplication est lui aussi devenu un besoin crucial pour son bon fonctionnement.

Besoins (suite)

- le télétravail s'est également développé ces dernières années, avec l'arrivée de connexions internet fiables et rapides dans les foyers
- l'entreprise doit également gérer l'itinérance des commerciaux et les astreintes à distance

L'ouverture du SI d'une entreprise est devenu une nécessité, celle-ci implique d'avoir des moyens de communication adaptés et sécurisés.

Introduction aux VPN

Besoins en terme de sécurité

- interceptions sur les réseaux ouverts (points d'accès, gares, hôtels)
  - une capture réseau donne aujourd'hui une mine d'informations
  - *tcpdump*, *aircrack-ng*
- de multiples points de passage
  - *traceroute*
- révélations de Snowden, écoutes des services de renseignement nationaux et étrangers
- espionnage économique.

Introduction aux VPN

Diverses solutions pour une entreprise

- ligne physique avec un lien dédié
  - idéal pour raccorder deux sites d'une même entreprise
  - ne répond pas au problème des salariés itinérants
- lignes dédiées louées auprès d'un opérateur
  - coût
  - confiance dans l'opérateur
  - utilisation de boitiers de chiffrement
- utilisation des réseaux publics.
  - VPN

Chacune a ses avantages et inconvénients : son coût, le temps de mise en œuvre, ses performances, sa disponibilité et sa sécurité sont à prendre en compte.

Introduction aux VPN

Réseau Privé Virtuel

- Réseau : support pour des échanges de données entre plusieurs sites distants. Problématiques d'adressage, de routage, de filtrage
- Privé : répondre aux contraintes de sécurité que l'on veut imposer
  - authenticité
  - confidentialité
  - intégrité
  - disponibilité
- Virtuel : sa mise en place ne dépend pas d'une infrastructure physique dédiée mais est construite par dessus une infrastructure existante qui peut être publique.

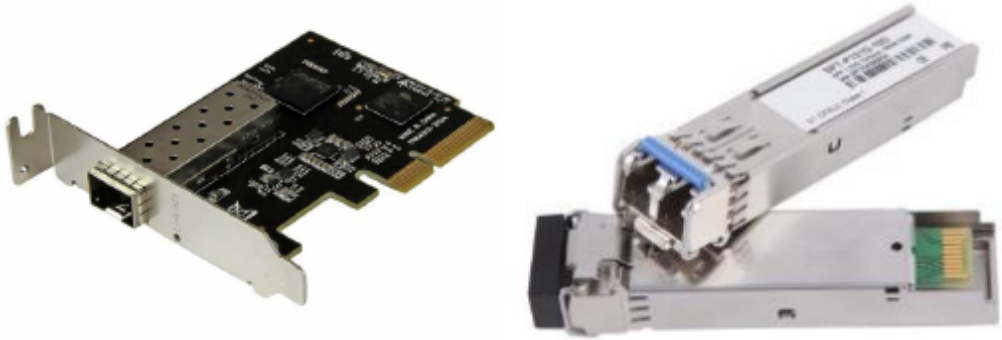
Construction d'un réseau Privé par dessus un réseau public.

Introduction aux VPN

Rappel sur les couches OSI

Couche 1 : physique

son rôle est de véhiculer les données reçus en les transformant en signaux adaptés au média physique utilisé (fibre, câble Ethernet). Casse-tête dans certains cas (fibre par ex)



Rappel sur les couches OSI

Couche 2 : liaison de données

cette couche fourni les moyens pour acheminer les données à travers les différents éléments du réseau. On retrouve des protocoles comme *Ethernet*, *IEEE 802.11 wireless LAN*, *Token Ring*.

Couche 3 : réseau

couche qui gère les communications entre les machines. Le routage se fait à ce niveau. On retrouve des protocoles comme *IP* et *IPX*

Rappel sur les couches OSI

Couche 4 : transport

son rôle est de gérer les communications entre programmes, assurer une communication stable, gérer la correction d'erreurs, etc...

Couches supérieures

- Session
- Présentation
- Application

Objectifs des VPN

La technologie des VPN repose sur la possibilité d'émettre des données privées sur un réseau public. Cette technologie doit répondre à plusieurs objectifs.

Tunnellage

Les informations échangées entre 2 entités internes sont rarement routables sur internet. Les VPN utilisent le tunnelage pour encapsuler un paquet non routable dans un paquet routable. Peut se faire à différents niveaux :

- niveau 2 : pptp, l2tp
- niveau 3 : ipsec
- niveaux supérieurs : SSL/TLS, SSH

Objectifs des VPN

Authentification

Garantir l'identité des extrémités d'un VPN avec par exemple l'utilisation :

- de clefs partagées
- de certificats
- d'OTP (One time Password)
- de Tokens d'authentification

Il faut également savoir gérer le vol t'authentifiants et de matériels

Chiffrement et signature

Garantir la confidentialité et l'intégrité des données transférées

Objectifs des VPN

Contrôle d'accès

Tous les membres d'un VPN n'ont pas nécessairement les même besoins en terme d'accès.

- mail
- astreinte
- documentation

Plusieurs protocoles peuvent être utilisés pour faire du VPN, certains d'entre eux visent uniquement à établir un tunnel, d'autres ajoutent une composante sécurité.

Terminologie

Le protocole porteur

celui sur lequel on s'appuie pour échanger des données

Le protocole d'encapsulation

- gre
- l2tp
- ipsec

Le protocole transporté

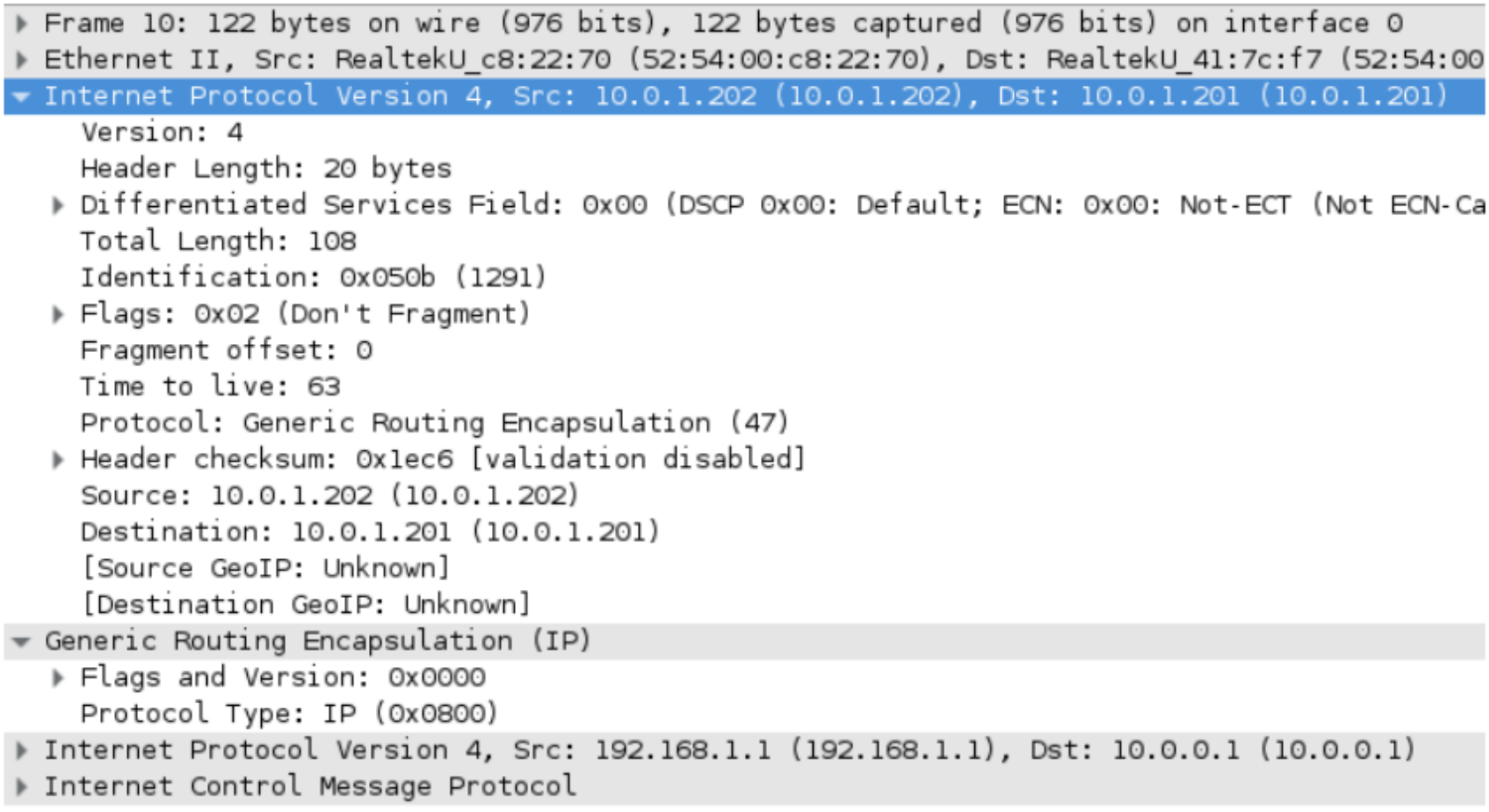
Terminologie

Generic Routing Encapsulation (GRE)

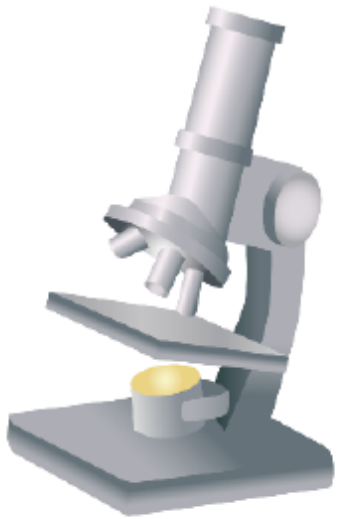
GRE est un protocole générique d'encapsulation de n'importe quel paquet dans un protocole de niveau 3 (couche réseau). Dans les faits, encapsulation généralement dans des paquets IP.

- utilise un code de protocole IP (47)
- structure assez simple essentiellement pour identifier le protocole transporté
- numéro de séquence
- contrôle d'erreurs (optionnel)

Generic Routing Encapsulation (GRE)



Generic Routing Encapsulation (GRE)



PPP, PPTP et L2TP

- PPP (Point to Point Protocol) est un protocole de liaison (couche 2 du modèle OSI) qui permet l'échange de paquets entre deux acteurs. Il est utilisé pour échanger des données entre deux ordinateurs reliés par un lien série ou téléphonique. PPP encapsule des paquets IP, IPX dans des trames PPP pour les transmettre à travers un lien point à point.
- PPTP (Point to Point Tunneling Protocol) est un protocole qui utilise une connexion PPP à travers un réseau IP. PPTP utilise deux canaux de communication : un canal de contrôle sur TCP (port 1723) et un tunnel GRE pour transporter les paquets PPP.

PPP, PPTP et L2TP

- L2TP (Layer 2 tunneling Protocol) est un protocole qui permettait initialement de transporter des connexions PPP à travers une connexion IP/UDP (port utilisé : 1701). Celui-ci a été ensuite généralisé pour transporter n'importe quel protocole de niveau 2. L2TP n'intègre en revanche pas de protocole de chiffrement.

```
▸ Frame 7: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits) on interface 0
▸ Ethernet II, Src: RealtekU_e5:dd:49 (52:54:00:e5:dd:49), Dst: RealtekU_ee:8a:3a (52:54:00:ee:8a
▸ Internet Protocol Version 4, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.1.202 (10.0.1.202)
▸ User Datagram Protocol, Src Port: 1701 (1701), Dst Port: 1701 (1701)
▸ Layer 2 Tunneling Protocol
▾ Point-to-Point Protocol
    Protocol: Internet Protocol version 4 (0x0021)
▸ Internet Protocol Version 4, Src: 11.0.100.20 (11.0.100.20), Dst: 192.168.1.1 (192.168.1.1)
▸ Internet Control Message Protocol
```

?