HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

Fête de la mobilité

SSLTunnel : un VPN tout-terrain

Alain Thivillon
<Alain.Thivillon@hsc.fr>

SSLTunnel – Buts

- Problème générique : monter un tunnel IP depuis n'importe où :
  - Derrière de la NAT
    - IPSEC difficile
  - Derrière un firewall n'autorisant que quelques ports
    - PPTP, Tunnels sur UDP impossibles
  - Derrière un relais HTTP
    - Vérification du contenu non SSL, vérification de l'établissement d'une session SSL
  - OpenSource
- Solutions partielles :
  - tunnels PPP sur SSH : le contrôle de contenu peut empêcher la connexion
  - VTun : utilise UDP, cryptographie critiquable
  - OpenVPN : peut utiliser TCP, mais pas de passage proxy

SSLTunnel – Principes

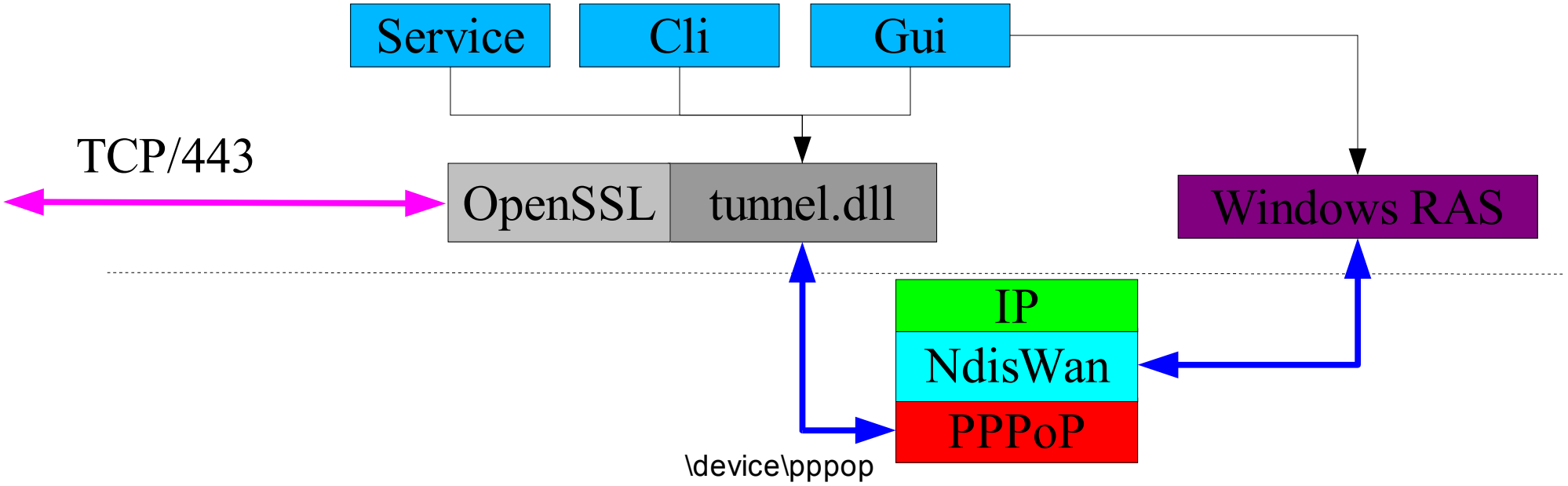
- Utilisation d'une session SSL/TLS sur TCP pour encapsuler PPP
  - Implémentation en utilisant les librairies OpenSSL : peu de code de cryptographie à réécrire.
  - Utilisation de PPP : criticable mais pas besoin de réécrire une couche de négociation IP, possibilité de passer d'autres protocoles.
- Authentification en utilisant des certificats clients X509
  - Plus sûr qu'un login/mot de passe
  - Authentification mutuelle : le client vérifie le certificat du serveur : pas de risque d'attaque Man in The Middle.
- Passage à travers les proxies HTTP
  - Utilisation du verbe CONNECT pour faire un tunnel TCP vers le serveur sur le port 443
  - Authentification en Proxy-Auth ou NTLM-Auth (MS-ISA server)

SSLTunnel

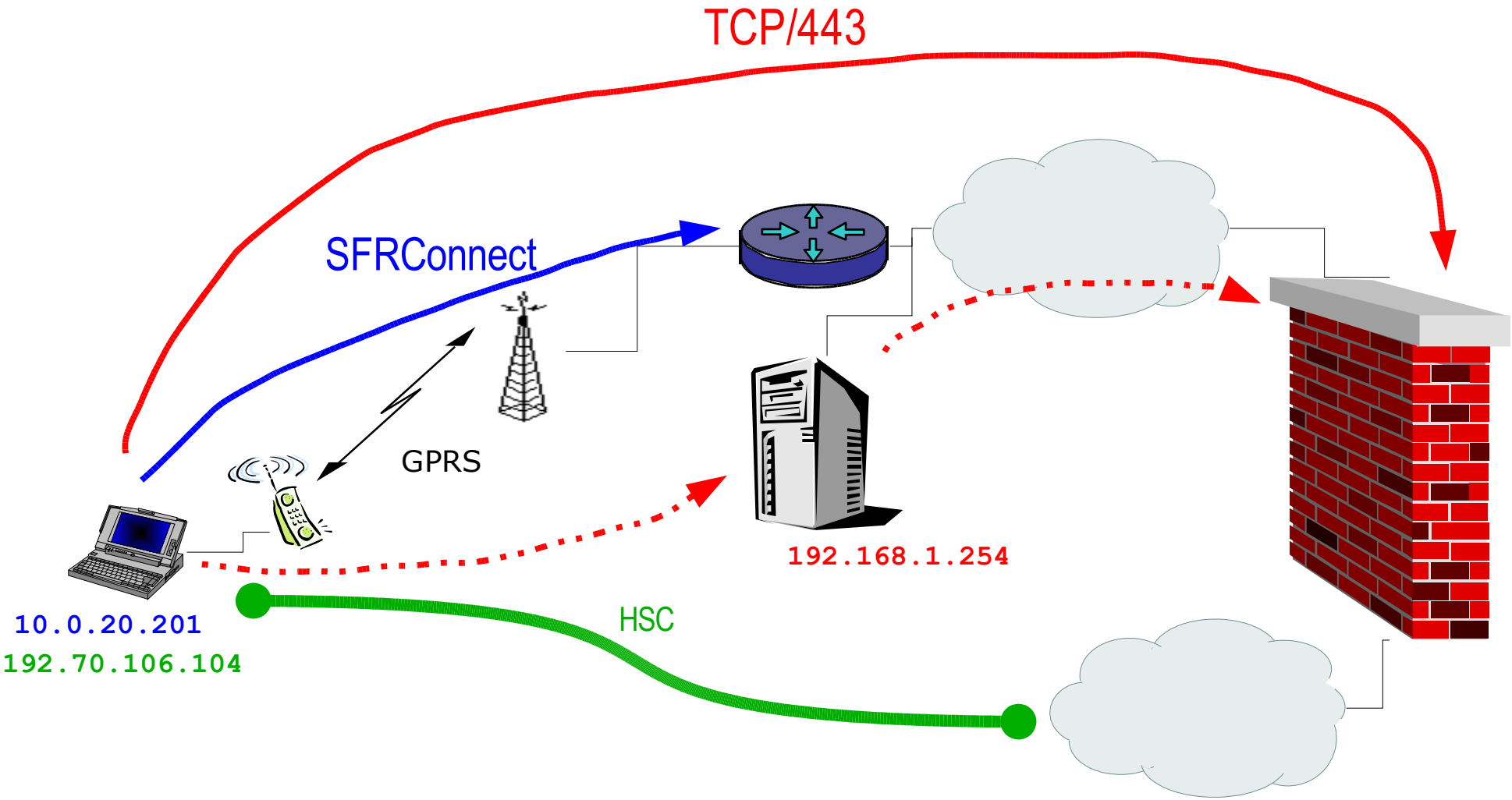
- Projet démarré au printemps 2003
  - Equipe HSC (AT, Denis Ducamp, Franck Davy)
  - Client Windows : AT & Nicolas Collignon (driver)
- Serveur : tourne uniquement sous Unix
  - BSD
  - Linux
  - Solaris
  - Utilise le pppd classique d'Unix
- Client
  - Unix
  - MacOS
  - Depuis hier, Windows (2000, XP, 2003)

Client Windows

- Trois parties :
  - Accès distant MS (RAS) : couche PPP
  - driver NDIS Wan Miniport : récupère les paquets PPP et les envoie dans un device \device\pppop (et vice-versa). Apparait comme une carte ISDN.
  - Programme userland : lecture/écriture des paquets dans le device driver, puis chiffrement/déchiffrement et communication avec le réseau.



Démo (et là, c'est le drame ...)



TODO

- Windows
  - Correction de bugs, retours d'expérience
  - Utilisation de CryptoApi au lieu de OpenSSL
  - Création automatique des connexions RAS (Wizard ?)
  - Fonctionner sans être administrateur ...
- Serveur Unix
  - Intégration dans un annuaire LDAP ?
  - Serveur d'administration HTTP (création des certificats, ...)
  - Filtres dynamiques
- Protocole
  - Envoi par le serveur des routes à mettre en place
  - Envoi par le serveur de règles de firewall

Liens

- Téléchargement : http://www.hsc.fr/ressources/outils/ssltunnel/
- Site du projet : http://sourceforge.net/projects/ssltunnel/
- Liste de diffusion : ssltunnel-users@lists.sourceforge.net (http://lists.sourceforge.net/lists/listinfo/ssltunnel-users)
- Cours PKI HSC : http://www.hsc.fr/ressources/cours/pki/index.html.fr
- OpenSSL : http://www.openssl.org/
- How-To CA : http://www.post1.com/home/ngps/m2/howto.ca.html , http://www.grennan.com/CA-HOWTO.html , Doc sur le site Sourceforge du projet.