# Tunnel SSH inversé vers RDP / VNC / SSH via un serveur tiers

La mise en place d'un tunnel SSH inversé se fait dans le contexte suivant:

- On veut accéder à un poste dit "client" qui a un service SSH, RDP ou VNC activé mais pas disponible à l'extérieur de son réseau local
- On dispose d'un serveur SSH disponible sur Internet
- Le poste "client" peut se connecter sur un serveur SSH sur Internet
- Le poste a partir duquel on veut accéder au "client" peut se connecter sur un serveur SSH sur Internet

# Sur le serveur SSH tiers

- On accepte les connections via authentification par clés publiques seulement
- Un compte utilisateur assigné au poste "client" est configuré, sans shell. La clé publique correspondant au poste "client" y est installée.
- Un compte "technicien" est configuré, sans shell (ou avec, selon). La clé publique correspondant au poste "technicien" y est installée.
- Un compte "administrateur" est configuré, avec shell. La clé publique correspondant au poste "administrateur" y est installée.

# Sur un client GNU/Linux

- Les applications ssh et ssh-keygen disponibles lorsque le paquet openssh-client est installé
- gSTM pour activer le tunnel sur demande (via le paquet ayant le même nom)
- openssh-server installé et configuré pour accepter uniquement les connections par authentification par clés publiques
- La clé publique du poste "technicien" est ajoutée à la fin du fichier .ssh/authorized\_keys

Installation des applications:

sudo apt install openssh-server openssh-client gstm

Configuration du service SSH:

1. Dans /etc/ssh/sshd\_config:

PasswordAuthentication no RSAAuthentication yes PubkeyAuthentication yes

# À partir de Windows

Pour mettre en place un tunnel SSH vers un poste Windows (RDP) il faut:

- Puttygen.exe (générateur de clés SSH) pour générer la paire de clés publique / privée permettant la connection
- Putty.exe (client SSH) pour activer le tunnel sur demande
- RDP actif et l'utilisateur configuré pour accepter les connections

Putty est disponible ici (prendre les versions 64-bit de préférence): https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

# Génération de paire de clés SSH

#### GNU/Linux - SSH

1. À partir du compte utilisateur:

mkdir ~/.ssh
chmod 700 ~/.ssh
ssh-keygen -t rsa -b 4096

Vous pourrez indiquer une phrase secrète pour la paire de clés et confirmer leur emplacement. Cette phrase secrète protégera votre clé privée pendant son stockage:

```
Generating public/private rsa key pair.
Enter file in which to save the key (/home/b/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/b/.ssh/id_rsa.
Your public key has been saved in /home/b/.ssh/id rsa.pub.
```

La clé publique sera disponible dans le fichier .ssh/id\_rsa.pub dans le dossier de l' utilisateur.

#### Windows - Putty

- 1. Démarrer puttygen.exe
- 2. Accepter l'avertissement d'installation Windows
- 3. \*Parameters > Type of key\*: RSA
- 4. \*Parameters > Number of bits\*: 4096
- 5. \*Actions > Generate\* Important: il faut bouger la souris dans la région blanche!
- 6. Une fois terminé, assigner un mot de passe
  - 1. À partir d'un poste GNU/Linux, générer un mot de passe (avec pwqgen par exemple)

- 2. Mettre le mot de passe dans \*Key passphrase\* et \*Confirm passphrase\*
- 7. Cliquer dans la section \*Key > Public key\*, choisir \*Tout sélectionner\* et coller cette information dans un nouveau fichier \*PCXXX-NOM Client SSH-pub.txt\* mettre dans \*Documents\*
- 8. Actions > Save the generated key > Save private key > PCXXX-NOM\_Client\_SSH mettre dans Documents, l'extension est .ppk par défaut (note: pour fins de backup)
- 9. Demander à un administrateur d'ajouter l'accès au compte SSH correspondant sur \$GW\_HOSTNAME à l'aide de la clé publique SSH enregistrée dans \*Documents\*

### Configuration du tunnel SSH (session Putty)

- 1. Démarrer putty.exe
- 2. Dans \*Basic settings\*:
  - 1. \*Host Name\*: \$GW\_HOSTNAME (nom de domaine de la passerelle SSH cible)
  - 2. \*Port\*: 22 (ou autre)
  - 3. \*Save Sessions\*: PCXXX-NOM\_Tunnel\_RDP (caractères de soulignement importants)
  - 4. Click \*Save\*
- 3. Dans \*Connection\*:
  - 1. \*Seconds between keepalives (0 to turnoff)\*: 30
  - 2. \*Data > Login Details > Auto-login username\*: \$USERNAME (nom d'utilisateur GNU/Linux fourni par l'admin)
  - 3. \*SSH > Protocol options > Don't start a shell or command at all\* (cocher)
  - 4. \*SSH > Protocol options > Enable compression\*
  - 5. \*SSH > Tunnels > Add new forwarded port > Source port\*: 2000 (ou autre)
  - \*SSH > Tunnels > Add new forwarded port > Destination\*: 192.168.X.XXX:3389 (IP du système Windows 7 cible, port RDP)
- 4. Click \*Add\*
- 5. Click sur \*Session\* et enregistrer la session
- SSH > Auth > Private key file for authentication > Pointer vers Documents/fichier .ppk de la clé privée
- 7. Retourner à Session, clicker 1 fois sur le profil et sauvegarder

## **Tester le tunnel et la connection RDP**

- 1. Démarrer putty.exe
- Session > Load, save or delete a stored session > Saved sessions, click 1 fois sur le profil, ensuite click Load
- 3. Click Open, accepter l'avertissement clé SSH
- 4. Une fenêtre noire Putty devrait s'ouvrir, entrer le mot de passe de la clé SSH
- 5. Ouvrir l'outil RDP de Windows
- 6. Spécifier 127.0.0.1:2000 (ou autre port au lieu de 2000) comme adresse, tester avec les informations RDP du poste serveur

## Faire le raccourci mRemoteNG

Installer "mRemoteNG":https://mremoteng.org/

- 1. Ajouter le tunnel (connection SSH2): \*Fichier > Nouvelle connection\* (ou Ctrl-N)
  - 1. Affichage > Nom: PCXXX-NOM SSH Tunnel
  - 2. Affichage > Panneau: PCXXX-NOM SSH Tunnel
  - 3. Connexion > Nom d'hôte/IP: \$GW\_HOSTNAME (nom du serveur passerelle)
  - 4. Connexion > Nom d'utilisateur: fourni par l'admin système
  - 5. Connexion > Mot de passe: celui qui protégeait la clé SSH
  - 6. Protocole > Protocole: SSH2
  - 7. Protocole > Port: 22 (ou autre)
- 2. Session Putty > choisir celle enregistrée lors de la création de session
- 1. Ajouter la connection RDP: \*Fichier > Nouvelle connection\* (ou Ctrl-N)
  - 1. Affichage > Nom: PCXXX-NOM accès RDP
  - 2. Affichage > Panneau: PCXXX-NOM accès RDP
  - 3. Connexion > Nom d'hôte/IP: 127.0.0.1
  - 4. Connexion > Nom d'utilisateur: celui sur le PC Windows cible
  - 5. Connexion > Mot de passe: celui sur le PC Windows cible
  - 6. Protocole > Protocole: RDP
  - 7. Protocole > Port: 2000 (ou autre)
  - 8. Session Putty > choisir celle enregistrée lors de la création de session

From: https://dulib.re/wiki/ - Le Goût du Libre

Permanent link: https://dulib.re/wiki/doku.php/sshrdp

Last update: 2018/02/28 09:05

