



Travail de Bachelor

25.07.2024

Table des matières

1 - Introduction	3
2 - Prérequis	3
2.1 - Installation de pcsd	3
2.2 - Modification du script <code>wg-quick</code>	3
2.3 - Ajout d'une capability à l'utilitaire de BoringTun	4
3 - Utilisation	4
3.1 - Modification de la configuration WireGuard	4
3.2 - Lancement du programme	4
3.3 - Arrêt du programme	4

1 - Introduction

Ce document permet à un utilisateur de Linux de comprendre comment installer BoringTun, configurer l'application et de l'utiliser avec un périphérique sécurisé (YubiKey, NitroKey, ...)

Ce mode d'emploi part du principe que l'utilisateur utilise WireGuard et est à l'aise avec la configuration de ce dernier. L'utilisateur doit aussi savoir comment utiliser son périphérique choisi avec OpenPGP afin de pouvoir générer une clé sur celui-ci. Les explications seront centrées sur les modifications apportées à BoringTun, ainsi que l'utilisation des périphériques sécurisés avec celui-ci.

2 - Prérequis

Les étapes qui suivent se font après avoir récupéré l'exécutable de BoringTun modifié soit en l'ayant directement compilé depuis le code source, soit via votre administrateur.

2.1 - Installation de pcsd

La première étape pour pouvoir utiliser une smartcard sur un système Linux est d'installer le daemon faisant le lien entre le matériel de votre machine et les cartes elles-mêmes.

```
1 sudo apt install pcsd
2 sudo service pcsd start
```

2.2 - Modification du script wg-quick

La seconde étape consiste à modifier le script `wg-quick` qui est installé par défaut avec WireGuard. Celui-ci ne peut pas être lancé par défaut avec un autre client WireGuard que l'original ou la version Go.

Utiliser un éditeur de texte afin de modifier le script se trouvant au chemin `/usr/bin/wg-quick`.

Il faut retrouver la fonction ci-dessous se trouvant à la ligne 90 du script.

```
1 add_if() {
2     local ret
3     if ! cmd ip link add "$INTERFACE" type wireguard; then
4         ret=$?
5         [[ -e /sys/module/wireguard ]] || ! command -v
6         "${WG_QUICK_USERSPACE_IMPLEMENTATION:-wireguard-go}" >/dev/null && exit $ret
7         echo "[!] Missing WireGuard kernel module. Falling back to slow userspace
8         implementation." >&2
9         cmd "${WG_QUICK_USERSPACE_IMPLEMENTATION:-wireguard-go}" "$INTERFACE"
10    fi
11 }
```

Celle-ci est à modifier par la fonction suivante afin que le script accepte notre version de WireGuard.

```

1  add_if() {
2      local ret
3      if [ ! -z "${WG_QUICK_USERSPACE_IMPLEMENTATION}" ]; then
4          echo "[!] Found WG_QUICK_USERSPACE_IMPLEMENTATION. Use userspace implementation
instead." >&2
5          cmd "${WG_QUICK_USERSPACE_IMPLEMENTATION:-wireguard-go}" "$INTERFACE"
6          elif ! cmd ip link add "$INTERFACE" type wireguard; then
7              ret=$?
8              [[ -e /sys/module/wireguard ]] || ! command -v
"${WG_QUICK_USERSPACE_IMPLEMENTATION:-wireguard-go}" >/dev/null && exit $ret
9              echo "[!] Missing WireGuard kernel module. Falling back to slow userspace
implementation." >&2
10             cmd "${WG_QUICK_USERSPACE_IMPLEMENTATION:-wireguard-go}" "$INTERFACE"
11         fi
12     }

```

2.3 - Ajout d'une capability à l'utilitaire de BoringTun

La dernière étape est d'ajouter la capability `CAP_NET_ADMIN` à l'exécutable de BoringTun. Pour les exemples de ce mode d'emploi, l'exécutable sera placé dans le chemin `/usr/bin/boringtun-cli`.

```

1  sudo setcap cap_net_admin+epi /usr/bin/boringtun-cli

```

3 - Utilisation

3.1 - Modification de la configuration WireGuard

Afin d'indiquer à la version modifiée de BoringTun que l'on souhaite utiliser un périphérique sécurisé, il faut utiliser une valeur spéciale pour la clé privée dans le fichier de configuration. Dans ce mode d'emploi, le fichier de configuration se trouve au chemin `/etc/wireguard/wg0.conf`.

Il faut donc remplacer la valeur de la clé privée que vous aviez précédemment lorsque vous utiliser le programme par l'indicateur ci-dessous.

```

1  [Interface]
2      ...
3      PrivateKey = AQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=
4      ...

```

3.2 - Lancement du programme

Le lancement du programme se fait avec l'exécutable `wg-quick` comme pour un WireGuard classique à la seule différence qu'il faut préciser quelques variables d'environnement.

```

1  sudo WG_QUICK_USERSPACE_IMPLEMENTATION="/usr/bin/boringtun-cli" WG_SUDO=1 wg-quick
up wg0

```

3.3 - Arrêt du programme

L'arrêt se passe exactement comme la version classique de WireGuard.

```

1  wg-quick down wg0

```