Les commandes Wireguard

Générer une paire de clé privé/public

Vous utiliserez les commandes intégrées `wg genkey` et `wg pubkey` pour créer les clés, puis ajouterez la clé privée au fichier de configuration de WireGuard.

Génération de la clé privée

```
wg genkey >> private.key
```

Une fois la clé privé généré, il faut lui enlever les droits des utilisateurs et des groupes :

La `sudo chmod go=...` commande supprime toutes les autorisations sur le fichier pour les utilisateurs et les groupes autres que l'utilisateur root afin de s'assurer que lui seul peut accéder à la clé privée.

```
chmod go= private.key
```

Génération de la clé publique

```
cat private.key | wg pubkey >> public.key
```

Ajouter un nouveau peer dans la configuration

```
wg set <interface_name> peer <public_key_client> allowed-ips <adress_ip_vpn_client>
```

/!\ Ne pas oublier d’enregistrer les modifications effectuées sur la configuration serveur : `wg-quick save <interface_name>`

Prendre en compte des modifications de la configuration

```
wg-quick save <interface_name>
```

Afficher la configuration prise en compte

```
wg show <interface_name>
```

Supprimer un peer sur le serveur

Pour supprimer un peer de la configuration serveur on a besoin :

- du nom de l'interface
- de la clé public du peer à supprimer

```
wg set <interface_name> peer <public_key_peer> remove
```

Si le serveur se trouve dans un conteneur

```
docker exec <container_name> wg set <interface_name> peer <public_key_peer> remove
```

/!\ Ne pas oublier d’gistrer les modifications effectuées sur la configuration serveur : `wg-quick save <interface_name>`

Comment surveiller qui se connecter à votre VPN Wireguard ?

La chose la plus simple que vous puissiez faire est de vous connecter en SSH à chacun des hôtes WireGuard sur votre réseau, et d'utiliser l'affichage d'état intégré de WireGuard pour vérifier l'état actuel de chaque interface et de chaque pair. Cela peut être faisable si vous n'avez que quelques serveurs VPN primaires à travers lesquels vos points de terminaison se connectent (plutôt qu'un réseau de points de terminaison connectés point à point).

Si vous vous connectez en SSH à un hôte exécutant WireGuard, vous pouvez obtenir un affichage en ligne de commande de chaque interface WireGuard active sur l'hôte, ainsi qu'une liste de chaque pair configuré pour l'interface, via la commande `wg` :

```
sudo wg show
```

```
interface: wg1
  public key: /TOE4TKtAqVsePRVR+5AA43HkAK5DSntkOCO7nYq5xU=
  private key: (hidden)
  listening port: 51821

peer: fE/wdxzl0klVp/IR8UcaoGUMjqaWi3jAd7KzHKFS6Ds=
  endpoint: 172.19.0.8:51822
  allowed ips: 10.0.0.2/32
  latest handshake: 1 minute, 22 seconds ago
  transfer: 3.48 MiB received, 33.46 MiB sent

peer: jUd41n3XYa3yXBzyBvWqlLhYgRef5RiBD7jwo70U+Rw=
  endpoint: 172.19.0.7:51823
  allowed ips: 10.0.0.3/32
  latest handshake: 2 hours, 3 minutes, 34 seconds ago
```

```
  transfer: 1.40 MiB received, 19.46 MiB sent
```

Chaque pair répertorié comprendra la clé publique utilisée par le pair, ainsi que quatre autres champs :

point final
Adresse IP publique actuelle (et port UDP) utilisée par l'homologue. Cette valeur est mise à jour à partir de la valeur initialement configurée pour l'homologue chaque fois que l'interface locale reçoit un nouveau paquet de l'homologue avec une adresse source (ou un port) différente.

ips autorisés
Adresses IP que l'interface WireGuard locale acheminera vers le pair.

dernier handshake
Si l'interface locale s'est connectée avec succès au pair distant depuis que l'interface a été démarrée, ceci indique la dernière fois que la connexion a été recodée. La "poignée de main" de reconnexion se produit toutes les 2 ou 3 minutes lorsque la connexion est activement utilisée (et uniquement lorsqu'elle est utilisée), ce qui vous donne une bonne approximation de la dernière fois que la connexion a été active. Ce champ sera omis si l'interface n'a pas réussi à se connecter à l'homologue depuis le démarrage de l'interface.

transfert
Si l'interface locale a tenté de se connecter à l'homologue distant depuis le démarrage de l'interface, ce champ indique la quantité de données reçues et envoyées à l'homologue. Ce champ sera omis si l'interface n'a pas tenté de se connecter à l'homologue depuis le démarrage de l'interface.

Les inconvénients évidents de l'utilisation de cette interface comme seul outil de surveillance sont que vous devez garder une session SSH ouverte sur chaque hôte que vous souhaitez surveiller, et que vous ne pouvez voir que ce qui se passe actuellement (ou la dernière fois que chaque pair était actif) - et non ce qui s'est passé aux moments spécifiques que vous pourriez vouloir examiner ou analyser.

Revision #7
Created 12 June 2023 15:58:58 by gpatruno
Updated 16 June 2023 11:13:14 by gpatruno