WireGuard

WireGuard® is an extremely simple yet fast and modern VPN that utilizes state-of-the-art cryptography. It aims to be faster, simpler, leaner, and more useful than IPsec, while avoiding the massive headache. It intends to be considerably more performant than OpenVPN. WireGuard is designed as a general purpose VPN for running on embedded interfaces and super computers alike, fit for many different circumstances. Initially released for the Linux kernel, it is now cross-platform (Windows, macOS, BSD, iOS, Android) and widely deployable.

Generating Keys

The communication protocols and cryptography is different than SSH but the concepts are the same where both public and private keys are generated by both the client and server and exchanged prior to communication.

All traffic to the server is encrypted with the `server-public-key` and can only be decrypted with the `server-private-key`. Similarly all traffic to the client is encrypted with the `client-public-key` and can only be decrypted wtih the `client-private-key`.

The steps for both server and client are similar

1. set the umask so all the files we're about to create to be 700 (rwx------)
2. use `wg` to generate a private key and write it to a file and pipe the content to `wg` to generate a public key that is also written to a file

Server

```
# umask 077
# wg genkey | tee server.key | wg pubkey > server.pub
# cat server.key
<server-private-key>
# cat server.pub
<server-public-key>
```

Client

```
# umask 077
# wg genkey | tee client.key | wg pubkey > client.pub
```

```
# cat client.key
<client-private-key>
# cat client.pub
<client-public-key>
```

Server Configuration

```
[Interface]
PrivateKey = <server-private-key>
Address = 10.0.99.1/24
ListenPort = 51820

[Peer]
PublicKey = <client-public-key>
AllowedIPs = 10.0.99.2/32
```

Client Configuration

```
[Interface]
PrivateKey = <client-private-key>
Address = 10.0.99.2/32
ListenPort = 51820

[Peer]
PublicKey = <server-public-key>
AllowedIPs = 0.0.0.0/0
```

Generate PresharedKey (optional)

If an additional layer of symmetric-key crypto is required (for, say, post-quantum resistance), WireGuard also supports an optional pre-shared key that is mixed into the public key cryptography. When pre-shared key mode is not in use, the pre-shared key value used below is assumed to be an all-zero string of 32 bytes.

```
# wg genpsk
<psk>
```

Add the same PresharedKey parameter to both `[Peer]` sections in server and client configuration files.

```
[Peer]
...
PresharedKey = <psk>
```

Revision #5
Created 22 February 2021 17:00:41 by dustin@swigg.net
Updated 22 February 2021 17:57:47 by dustin@swigg.net