Das Konzept

Multihop

Mullvad bietet ein Multihop Feature, bei welchem der Traffic durch einen weiteren Entry Server geleitet wird. Dabei besteht nur eine VPN Verbindung, nämlich mit dem Exit Server, während der Entry lediglich den Traffic weiterleitet. Das funktioniert, da jeder Mullvad Server einen eindeutigen "Multihop Port" hat, welcher auf allen Servern gleich ist. So hat bspw. der Server `de-fra-wg-001` den Multihop Port `3053`. Konfiguriert man im Client nun den VPN Endpoint `se-sto-wg-005:3053`, weiß der Server `se-sto-wg-005` dass der Traffic zu `de-fra-wg-001` geleitet werden soll.

Wir packen auf dieses Setup noch einen drauf und fügen unseren eigenen Server *Sentinel* als "vor-Entry" ein. Dadurch ergibt sich folgendes Bild:

```
Client --1--> Sentinel --2--> Mullvad Entry --2--> Mullvad Exit --> Internet
```

Mullvad sieht somit zu keinem Zeitpunkt die wahre Client IP und der Mullvad Exit zu keinem Zeitpunkt beides: Traffic und Sentinel IP.

Eigenes Netz vs Weiterleiten

Wir hätten ebenfalls den Traffic einfach weiterleiten können, ähnlich wie es Mullvad implementiert. Das hätte jedoch die folgenden Nachteile gehabt:

- Änderungen am Setup (bspw. Mullvad Server wechsel) hätten im Client **und** Sentinel Anpassungen benötigt. Denn der Client benötigt den richtigen (Exit Server) Public Key und Sentinel die richtige IP:Port des Entry Servers.
- 1 Client = 1 Mullvad Slot

Ein eigenes Wireguard Netz zwischen Client und Sentinel bietet folgende Vorteile:

- Einfaches Wechseln der Mullvad Server
  - Keine Client Anpassung nötig
  - Kann im Hintergrund passieren ohne dass der Client etwas davon mitbekommt
- Eigener DNS Server im VPN Netz
  - Dieser ist optional. In der Client Config kann ein eigener oder auch der Mullvad DNS Server eingetragen werden.
- N Clients auf 1 Mullvad Slot

Revision #20
Created 17 May 2024 06:41:31 by Mike
Updated 25 May 2024 19:12:09 by Mike