

OpenVPN startet nicht (ca md too weak)

Die folgende Lösung sollte nur ein kurzfristiger Workaround bleiben. Sicherer wäre es wenn auch der Serverteil aktualisiert und auf aktuelle Hashes und Cipher umgestellt wird!

Problem: OpenVPN Tunnel mag nicht starten. Im Log kommt folgende Meldung:

```
(OpenSSL: error:140AB18E:SSL routines:SSL_CTX_use_certificate:ca md too weak)
```

Neue OpenVPN Versionen haben veraltete Hashes und Ciphers deaktiviert. Es laufen aber noch ältere OpenVPN-Server zu denen man sich jetzt nicht mehr verbinden kann.

Die älteren Ciphers lassen sich mit einem Konfigurationsschalter wieder aktivieren.

Bei OpenVPN Configs direkt diese Zeile eintragen:

```
tls-cipher "DEFAULT:@SECLEVEL=0"
```

Bei Verbindungen mit dem NetworkManager kommt diese Zeile in den [vpn]-Teil:

```
tls-cipher=DEFAULT:@SECLEVEL=0
```

Danach muss der NetworkManager neu gestartet werden (Achtung, alle Verbindungen werden unterbrochen).
Achtung: Die Zeile verschwindet auch wieder aus der Config wenn in der GUI Änderungen vorgenommen wurden.

Revision #3

Created 2023-04-24 15:27:44 UTC by magenbrot

Updated 2024-04-04 07:17:20 UTC by magenbrot