Das Spiel Testdrive Unlimited hat jede Menge Bugs. Der schlimmstejedoch ist das es praktisch unmöglich ist das Spiel "durchzuspielen"also 100% zu erreichen. Das Problem: eine Mission verlangt das derSpieler in einem Rennen Club vs Club gegen einen anderen Clubmindestens 3 Siege erringt. Aber die Clubfunktionalität ist so kaputtdas dies nicht geht. Jedenfalls nicht ohne Tricks.

Problem: Clubrennen lassen sich nur starten wenn mindestens 2 Spieler desselben Clubs gleichzeitig online sind **UND**sich in der Club Lobby auch gegenseitig sehen. Wegen des Fehlers gehtgenau das nur wenn beide Spieler sich im selben LAN hinter einem Routerbefinden. Ansonsten meldet das Spiel störisch: "Kein weiteresClubmitglied online"
Lösung 1: Lan hinter einem Router.
4Spieler packen ihre Rechner ein und machen eine schöne Lanparty. Ok,hat was, da kann man gleich auch noch anstoßen und den ein oder anderenSchluck trinken. Aber das -=I.O.S=- TDU Team ist über ganz Deutschlandverteilt. Nur für die 100% 4 Spieler mit teilweise über 600KMEntfernung zueinander führen ist zu Heavy. Und überhaupt! Das Internetmuss doch noch für mehr als Fickbilder gut sein oder?
Also Lösung 2:
Lösung 2: VPN Tunnel
Nurkurz umrissen ist es möglich mit VPN ein virtuelles LAN zu erstellen.Und es funktioniert überraschenderweise mit TDU in ganz einfacherKonfiguration.

Ausgangspunkt: Ein Linux (Ubuntu) Server hinter einem Kabelmodem mit 25000/6000 UP/Downstrem Rate, Feste IP oder DynDnS Name.

1) OpenVPN auf dem Server installieren

Unter Debian-Like mit apt-get install openvpn

2) Zertifikate erstellen.

In der Defaultconfiguration liegt unter /usr/share/doc/openvpn/examples/easy-rsa/2.0/vars ein Template in dem einige Punkte angepasst werden können:

- export KEY_COUNTRY="US"
- export KEY_PROVINCE="CA"
- export KEY_CITY="SanFrancisco"
- export KEY_ORG="Fort-Funston"
- export KEY_EMAIL="me@myhost.mydomain"

Dies wird dann später im Certifikat angezeigt, ist ansonsten aber nicht von Belang. Die restlichen Default Vorgaben sind so erstmal in Ordnung.

cd **/usr/share/doc/openvpn/examples/easy-rsa/2.0/**
Die Datei ./vars editieren**.**

Der folgende Befehl veranlasst OpenVPN nun die editierte Vorlage beim Erstellen des Zertifikates zu benutzen:
source ./vars

Jetzt werden die Zertifikate für den Server und für jeden einzelnen Spieler erstellt:

- ./clean-all
- ./build-ca
- ./build-key-server server
- ./build-key Spieler1
- ./build-key Spieler2
- ./build-key Spieler3
- ./build-key Spieler4
- ./build-dh

Jetzt liegen die Zertifikate für den Server und für jeden Spieler unter dem Pfad /usr/share/doc/openvpn/examples/easy-rsa/2.0/keys/
Dort sind sie nicht so gut aufgehoben, deswegen kopiere ich sie nach /etc/openvpn/keys

- mkdir /etc/openvpn/keys/
- cp keys/dh1024.pem /etc/openvpn/keys/
- cp keys/server.* /etc/openvpn/keys/
- cp keys/Spieler* /etc/openvpn/keys/
- cp keys/ca.* /etc/openvpn/keys/

3) Die Server Config erstellen

Die Datei /etc/openvpn/server.conf erstellen bzw editieren. Der Server bekommt die Adresse 10.8.0.0, wir möchten gern udp und auf Port 1194 lauschen. Außerdem muss der Pfad zu den Keys angegeben werden, die wurden im Schritt 2 ja nach /etc/openvpn/keys kopiert. (Unter anderem damit man hier nicht einen endlos Pfad eintippen muss) Die komplette Beispieldatei:

```
server 10.8.0.0 255.255.255.0
dev tun
port 1194
proto udp

push "redirect-gateway def1"
push "dhcp-option DNS 145.253.2.11" # DNS-Server 1
push "dhcp-option DNS 145.253.2.171" # DNS-Server 2 (falls vorhanden)

ping-timer-rem
keepalive 20 180

persist-key
persist-tun
verb 3
mute 50

dh /etc/openvpn/keys/dh1024.pem
ca /etc/openvpn/keys/ca.crt
key /etc/openvpn/keys/server.key
cert /etc/openvpn/keys/server.crt
duplicate-cn
```

```
client-config-dir /etc/openvpn/clients
```

4) Ready, Set GO!

Jetzt das erste mal Openvpn starten mit dem Befehl:

- openvpn --config /etc/openvpn/server.conf

Und Iptables anweisen das Pakete die über OpenVPN ankommen in die Weiten des Internets geschickt werden sollen (NAT-Maskiert weil 10.8.0.0 ein privates Netzwerksegment ist).

- iptables -t nat -A POSTROUTING -o eth0 -s 10.8.0.0/24 -j MASQUERADE

5) Authorisierte Clients freischalten

Der Server läuft jetzt, oder sollte es zumindest. Ansonsten geben die Fehlermeldungen hoffentlich einen Hinweis wo es hängt. Nun muss OpenVPN noch wissen wer sich verbinden darf, und welche Einstellungen für die Clients gültig sind.

Ein Verzeichnis /etc/openvpn/clients anlegen und dort für jeden Spieler eine Datei
spieler1 spieler2 spieler3 spielerx [...] mit dem Inhalt:

```
# Der Client wird angewiesen den OpenVPN-Server als Default-Gateway zu nutzen
# und alle Verbindungen über ihn abzuwickeln:
push redirect-gateway

# Der Server wird angewiesen dem Client eine feste IP zuzuweisen.
ifconfig-push 10.8.0.14 10.8.0.13
```

Die IP-Adresse muss für jeden Spieler individuell angepasst werden.

Passend zur Subnetzmaske 255.255.255.252 sind für die Spieler 1-4 folgende Kombinationen gültig:
Spieler1 10.8.0.6 10.8.0.5
Spieler2 10.8.0.10 10.8.0.9
Spieler3 10.8.0.14 10.8.0.13
Spieler4 10.8.0.18 10.8.0.17

Damit ist der Server einsatzbereit und wartet auf die ihm bekannten Clients.

6) Client Installation

Das OpenVPN GUI Paket auf den Clients installieren. Zur Zeit: openvpn-2.0.9-gui-1.0.3-install.exe
Den Ordner in dem openvpn Installiert wurde öffnen und zu dem Ordner config durchhangeln, also z.B. C:\Programme\OpenVPN\config
Dort einen Ordner keys erstellen und dort die

- ca.crt
- Spieler1.crt,
- Spieler1.key

die im Punkt 3 auf dem Server erstellt wurden und die wir nach/etc/openvpn/keys kopiert haben ablegen. Kann man z.B. über einensicheren Kanal (verschlüsselte E-Mail ;) den anderen Spielern zukommenlassen)
Im Ordner C:\Programme\OpenVPN\config eine Datei Spieler1.ovpn anlegen mit dem Inhalt:

```
client
ip-win32 manual
remote 192.168.1.1 1194 # Hostname/externe IP und Port des Servers
proto udp
dev tun

ca C:\\Programme\\OpenVPN\\config\\keys\\ca.crt
cert C:\\Programme\\OpenVPN\\config\\keys\\Spieler1.crt
key C:\\Programme\\OpenVPN\\config\\keys\\Spieler1.key

verb 3 # Zum Debugging erhöhen
mute 50 # Zum Debugging auskommentieren
```

Nun unter den Netzwerkverbindungen die neu vorhandene virtuelleNetzwerkkarte (z.B. Lan Verbindung 2) Rechtsklick, Eigenschaften,TCP/IP, Eigenschaften eine Feste IP-Adresse zuweisen:

- Der erste Spieler 10.8.0.6 Mask 255.255.255.252 Gateway 10.8.0.5

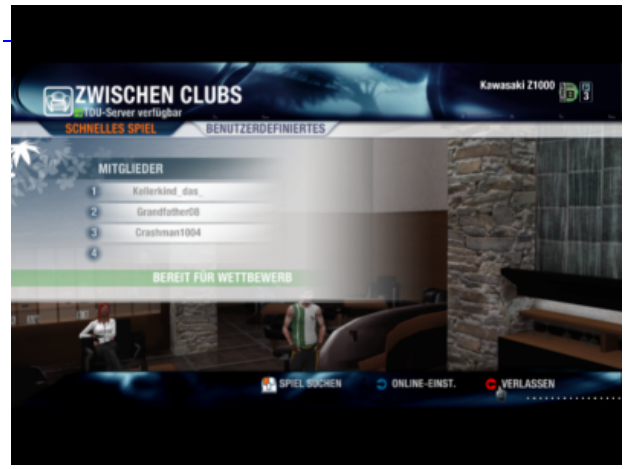
(Das ist die IP-Adresse die dem Server oben bei Schritt 5 unter /etc/openvpn/clients/Spielerx für diesen Spieler zugeteilt wurde)

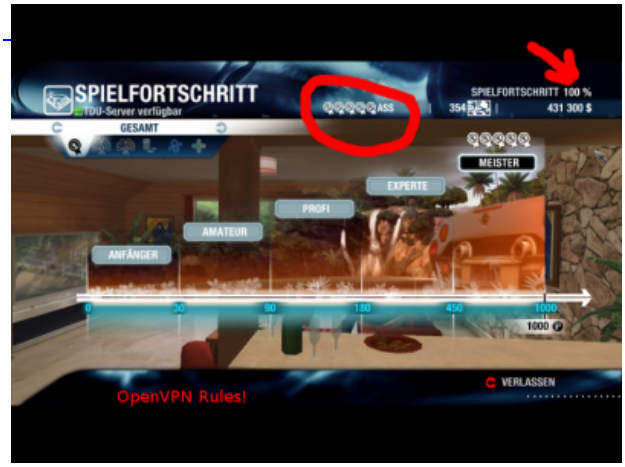
Beider Default Installation von OpenVPNGUI läuft der Prozess jetzt bereitsunten in der Taskleiste und wird durch ein rotes Netzwerksymbolangezeigt.
Dort Rechtsklick, verbinden und der Tunnel sollte stehen.
Ansonsten das Logfile des Server nach Fehlermeldungen durchsehen.

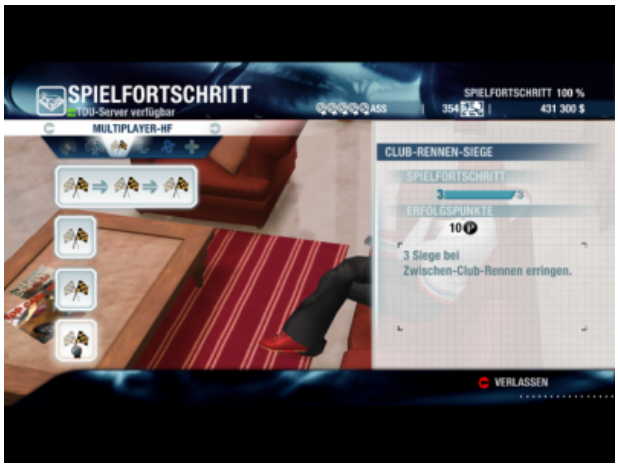
Vom Server aus sollte man in der Lage sein jeden einzelnen eingewählten Spieler anzupingen, der Spieler kann den Server anpingen. (Bei den Spielern untereinander klappt das nicht, dafür müsste man den OpenVPN-Modus TAP wählen)
Hat der Verbindungsaufbau geklappt werden alle Pakete ins Internet über den OpenVPNServer geleitet.Die Spieler befinden sich im selben LAN und gehen über dieselbe "Leitung"/ IP-Adresse auf den TDU Server.

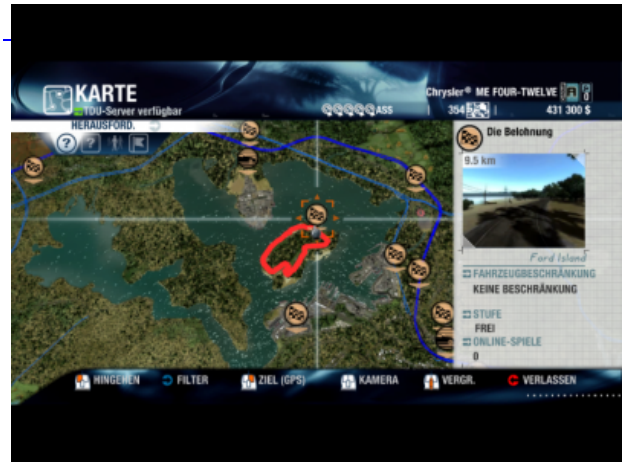
7) PROFIT!?

Sind jetzt alle Spieler imClub sehen sie sich nicht nur in der Club Lobby - womit das ganzeKonzept des Hauskaufes für den Club und die Features zurAvatargestaltung überhaupt erst einen Sinn ergibt - nein - jetzt kannman auch ein Club vs Club rennen fahren wenn sich jeweils Spieler 1 und2 bzw Spieler 3 und 4 in verschiedenen Clubs befinden.









Wieman sieht steht das dringend benötigte "Bereit für Wettbewerb" nunendlich da. Außerdem beachte man wie Crashman gelangweilt an der Barsteht, Kellerkind im Sessel darauf wartet das ein Gegner erscheint undganz hinten auf diesen Screenshot schwer zu erkennen lümmeltGrandfather auf der Couch rum....

Im Beispielwerden feste IP-Adressen benutzt - das lässt sich auch mit dhcpbenutzerfreundlicher gestalten. Mit dem tun Interface und derSubnetzmaske 255.255.255.252 (Eine Beschränkung von OpenVPN mitWindows) lassen sich andere LAN Spiele nicht gut spielen - dafür istdas TAP interface besser geeignet. Natürlich müssen alle FirewallLösungen bei den Spielern und auf dem Server entsprechendfreigeschaltet werden.
Einer unserer Spieler hatte Probleme mit derÜbernahme des DNS vom OpenVPN Server. Laut Wiki muss derBenutzerkontenschutz UAC bei Vista abgeschaltet werden und dieKonfigurationsschalter

route-method exe
route-delay 2

inder SpielerX.ovpn sollen helfen. Brachte aber nichts. Also von Hand denDNS beim Clienten eingetragen und Schwupps alles schick. Nach denersten AHA Effekt gibt es also noch jede Menge Möglichkeiten zumFinetuning. Gute Anlaufstellen dafür sind:
http://www.hs-esslingen.de/de/40044
http://arnowelzel.de/wiki/de/fli4l/openvpn

http://www.openvpn.net/index.php/documentation/howto.html
http://www.vpnforum.de/wiki/

und für Probleme
http://www.vpnforum.de/openvpn-forum/

oder fragt einfach bei uns im Board
http://www.internationaloldstars.de/board/index.php/topic,2128.75.html
http://www.internationaloldstars.de/board/index.php/topic,2607.0.html