iTunes und der Fehler 54 (https://www.sugar-camp.com/itunes-und-der-fehler-54/)

Anleitung: In Proxmox vServern TUN/TAP bei openVZ Instanzen aktivieren (https://www.sugar-camp.com/anleitung-in-proxmox-vserver-tuntap-fuer-openvz-aktivieren/)

Mrz 26

Anleitung: openVPN Server auf Debian 7.8 installieren und anschließend mit Android, iOS oder Windows verbinden

- By Andre (https://www.sugar-camp.com/author/sugar/) in Allgemein (https://www.sugar-camp.com/allgemein/), Anleitungen (https://www.sugar-camp.com/anleitungen/), OpenVPN (https://www.sugar-camp.com/openvpn/)

OpenVPN ist ein wirklich Klasse Tool und immer wieder werde ich gefragt wie man ein virtuelles Netzwerk einrichtet und ob ich dabei helfen kann.

Natürlich kann ich das! Und deswegen schreibe ich hier eine kleine Anleitung mit den einzelnen Schritten um am Ende ein virtuelles Netzwerk zu haben.

Ich gehe davon aus, dass Grundkenntnisse mit Debian vorhanden sind.

Ziel ist es ein virtuelles Netzwerk einzurichten in dem man nur mittels Zertifikat hinein kommt. Somit werden keine Logins benötigt und man kann einen User jederzeit sperren.

Inhalt:

Voraussetzungen:

1. ein Server mit mindestens 512 MB Ram, mindestens eine 800 Mhz CPU (Mehr ist natürlich besser) und mindestens 5 GB freien Festplattenspeicher
2. TUN / TAP Unterstützung aktiviert
3. installiertes Debian System
4. SSH Zugang mit Root Rechten

Das sind die minimalen Voraussetzungen die euer Server erfüllen muss. Solltet Ihr einen besseren Server haben, sollte dies kein Problem sein.

Wenn der Server kein TUN/TAP aktiviert hat, müsst Ihr euch zu erst an euren Hoster wenden und um die Aktivierung bitten. Einige Hoster erlauben auch eine Aktivierung im Control Panel des jeweiligen Hosters.

OpenVPN installieren und konfigurieren

1. Verbindung zum Server aufbauen und Updates einspielen

Stellt mittels Putty (http://www.putty.org/) oder ähnlichem Client eine Verbindung zu eurem Server her.

Ist die Verbindung erfolgreich hergestellt werden erst mal eventuelle Updates installiert.

Dazu einfach in der Konsole folgenden Befehl ausführen:

```
root@vpn:~# apt-get update && apt-get upgrade
```

2. Prüfen ob TUN/TAP aktiviert ist

Um zu prüfen ob das TUN/TAP Device aktiv ist und korrekt arbeitet einfach folgenden Befehl in der Konsole eingeben:

```
root@vpn:~# cat /dev/net/tun
```

Die Ausgabe sollte dann so aussehen:

```
cat: /dev/net/tun: File descriptor in bad state
```

Hinweis

Wenn in der Ausgabe eine Meldung der Art “File descriptor in bad state” erscheint, ist alles in Ordnung und TUN/TAP ist aktiviert. Wenn in der Ausgabe hingegen eine Meldung der Form “No such device” erscheint, sollte man den Hoster mit der Bitte um Aktivierung des TUN/TAP Devices kontaktieren.

3. Installation von openVPN und udev

Einfach den Befehl eingeben und Entern

```
root@vpn:~# apt-get install openvpn udev
```

4. Kopieren der Beispielkonfigurationen von openVPN

Bei der Installation hat openVPN bereits alles mitgeliefert was wir benötigen. Die entsprechenden Dateien müssen lediglich kopiert werden.

Das geschieht mittels:

```
root@vpn:~# cp -R /usr/share/doc/openvpn/examples/easy-rsa/ /etc/openvpn/
```

5. OpenVPN Beispielkonfiguration bearbeiten

Als erstes editieren wir die Datei “vars” mit vi oder nano oder was Ihr sonst gern verwendet. Die Werte für “KEY_COUNTRY”, “KEY_PROVINCE”, “KEY_CITY”, “KEY_ORG” und “KEY_EMAIL” einfach mit den eigenen Werten anpassen. Kein muss aber eine ganz klare Empfehlung ist die 1024-Bit Verschlüsselung zu erhöhen da diese heutzutage durchaus zu knacken ist.

Dazu einfach “KEY_SIZE” auf 4096 stellen.

Nun die Datei einfach speichern und schließen.

```
root@vpn:~# vi /etc/openvpn/easy-rsa/2.0/vars
```

Die Datei sieht so aus mit entsprechenden Stellen die editiert werden müssen:

```
# These are the default values for fields

# which will be placed in the certificate.#

Don’t leave any of these fields blank.

export KEY_COUNTRY=”DE”

export KEY_PROVINCE=”B oder euer Bundesland”

export KEY_CITY=”Berlin oder sonst etwas”

export KEY_ORG=”Organisation oder Domain”

export KEY_EMAIL=”eure@mailadresse.de”

export KEY_SIZE=4096
```

6. OpenVPN Zertifikat erstellen

Dazu einfach nachfolgende Befehle, nacheinander in die Shell eingeben.

Wir wechseln in das korrekte Verzeichnis mit:

```
root@vpn:~# cd /etc/openvpn/easy-rsa/2.0/
```

Hier laden wir die vorhin erstellte “vars” Datei

```
root@vpn:~# . /etc/openvpn/easy-rsa/2.0/vars
```

Mit diesem Befehl werden alle Altlasten und bereits erstellten Schlüssel gelöscht

```
root@vpn:~# . /etc/openvpn/easy-rsa/2.0/clean-all
```

Jetzt erstellen wir ein Server Zertifikat. Dabei werden einige Eingaben erforderlich die Ihr einfach ausfüllen könnt

```
root@vpn:~# . /etc/openvpn/easy-rsa/2.0/build-ca
```

Wichtig!

Die beiden Fragen bzw. Werte müssen einzigartig sein und dürfen nicht doppelt vergeben werden!

Common Name (eg, your name or your server's hostname) [changeme]:vpn.euer-host.com

Name [changeme]:einmaliger-name

7. OpenVPN privaten Server Schlüssel erstellen

Nun gilt es wieder, wie so oft, einen Befehl in der Shell ein zutippen um damit den privaten Schlüssel für den Server zu erstellen. Im Zuge dessen wird man auch wieder aufgefordert einige Daten einzugeben. Die Eingaben bitte auf eure persönlichen Bedürfnisse anpassen. Das "challenge password" und den "company name" kann man in diesem Fall leer lassen. Die Eingaben muss man im Anschluss noch 2x mit der Taste "y" oder der "j" Taste (engl.: yes, dt.: ja) bestätigen.

```
root@vpn:/etc/openvpn/easy-rsa/2.0# . /etc/openvpn/easy-rsa/2.0/build-key-server vpn-server
```

8. OpenVPN Schlüssel für einen Client erstellen

Um einen Schlüssel für einen Client zu erstellen einfach den nachfolgenden Shell Befehl eintippen wobei dabei das "windowspc" in diesem Befehl unbedingt durch eine eigene Bezeichnung ersetzt werden sollte. Es darf weiterhin keine 2 Clients geben die mit genau der gleichen Bezeichnung arbeiten. Sie müssen vom Namen her paarweise also immer verschieden sein.

Das "challenge password" und den "company name" kann man in diesem Fall auch leer lassen. Die Eingaben muss man im Anschluss noch 2x mit der Taste "y" oder der "j" Taste (engl.: yes, dt.: ja) bestätigen.

```
root@vpn:/etc/openvpn/easy-rsa/2.0# . /etc/openvpn/easy-rsa/2.0/build-key windowspc
```

Möchte man später noch weitere Clients hinzufügen so muss man dieses Prozedere einfach mit folgenden Befehlen wiederholen und die Bezeichnung "linuxpc" wieder entsprechend ändern:

```
root@vpn:~# cd /etc/openvpn/easy-rsa/2.0/
```

```
root@vpn:/etc/openvpn/easy-rsa/2.0# . /etc/openvpn/easy-rsa/2.0/vars
```

```
root@vpn:/etc/openvpn/easy-rsa/2.0# . /etc/openvpn/easy-rsa/2.0/build-key linuxpc
```

9. Diffie-Hellman-Parameter erstellen

Einfach folgenden Befehl ausführen:

```
root@vpn:/etc/openvpn/easy-rsa/2.0# . /etc/openvpn/easy-rsa/2.0/build-dh
```

10. OpenVPN Dateien auf den Client kopieren

Ich kopiere die Dateien per scp auf meinen Rechner und verteile diese von da aus an meine Clients per USB Stick oder als verschlüsseltes Archiv über eine verschlüsselte https Verbindung.

Hinweis

Wichtig ist, dass Ihr das eben nicht einfach nur unverschlüsselt per Browser, E-Mail, FTP oder ähnliches übertragt. Dann ist die Sicherheit eurer VPN-Verbindung, die ihr später einmal nutzen wollt, gegebenfalls bereits mitunter schon nicht mehr gewährleistet.

Benötigt wird für jeden Client die ca.cert. Weiterhin gibt es für jeden Client 2 Dateien die mit obigen Befehlen erstellt werden. In meinem Beispiel also die windowspc.crt und windowspc.key

Die Dateien liegen unter:

```
/etc/openvpn/easy-rsa/2.0/keys
```

11. OpenVPN Server Dateien kopieren

Hinweis

Beachtet bitte die “server.crt”, “server.key”, “server.conf” und “windowspc.conf” hat bei euch gegebenenfalls einen anderen Namen. Je nachdem wie ihr euren Server bzw. Client einige Schritte zuvor genannt habt.

Zuerst wechseln wir ins openvpn Verzeichnis, wo unsere Zertifikate und Keys gespeichert sind:

```
root@vpn:/etc/openvpn/easy-rsa/2.0# cd /etc/openvpn/easy-rsa/2.0/keys
```

Nun kopieren wir die erstellten Serverkeys und Serverzertifikate

```
root@vpn:/etc/openvpn/easy-rsa/2.0/keys# cp ca.crt ca.key dh4096.pem server.crt server.key /etc/openvpn
```

Jetzt holen wir uns die Server Konfigurationsdateien

```
root@vpn:/etc/openvpn/easy-rsa/2.0/keys# cd /usr/share/doc/openvpn/examples/sample-config-files
```

```
root@vpn:/usr/share/doc/openvpn/examples/sample-config-files# gunzip -d server.conf.gz
```

```
root@vpn:/usr/share/doc/openvpn/examples/sample-config-files# cp server.conf /etc/openvpn/server.conf
```

```
root@vpn:/usr/share/doc/openvpn/examples/sample-config-files# cp client.conf ~/windowspc.conf
```

12. Server Konfiguration editieren

Hinweis

In der “server.conf” muss kontrolliert werden ob die Bezeichnungen und Pfade für “ca”, “cert”, “key” und “dh” stimmen. Wenn der Server zum Beispiel anders genannt wurde, dann die Bezeichnungen an dieser Stelle einfach anpassen.

```
root@vpn:/usr/share/doc/openvpn/examples/sample-config-files# cd /etc/openvpn
```

```
root@vpn:/etc/openvpn# vi server.conf
```

```
# Any X509 key management system can be used.
# OpenVPN can also use a PKCS
#12 formatted key file
# (see “pkcs12” directive in man page).
ca ca.crt
cert server.crt
key server.key
# This file should be kept secret
# Diffie hellman parameters.
# Generate your own with:
# openssl dhparam -out dh1024.pem 1024
# Substitute 2048 for 1024 if you are using
# 2048 bit keys.
dh dh4096.pem
```

Möchte man zusätzlich noch das der Client auch auf das vLAN Netz hinter dem VPN Server zugegriffen werden kann (Client to Client), müssen folgende Zeilen in die “server.conf” eingefügt werden:

```
push “redirect-gateway def1 bypass-dhcp”
client-to-client
```

Zum konfigurieren bestimmter DNS Server einfach folgendes eintragen:

```
push “dhcp-option DNS 85.214.20.141”
push “dhcp-option DNS 8.8.8.8”
```

Man könnte auch weitere DNS Server eintragen. Ich nutze zum Beispiel einen DNS Server in meinem VPN Netzwerk. Damit ist es mir möglich Domains via Browser erreichbar zu machen die nur im VPN Netzwerk funktionieren und kein Geld kosten. Beispielsweise eine Domain wie vpn.netzwerk. Das hat nicht nur den Vorteil das man sich die Adressen leichter merken kann, sondern auch noch dass man für Entwicklungen keine zusätzlichen Domains kaufen muss.

Möchte man zusätzlich noch das heimische Netzwerk erreichbar machen, so fügt man einfach diese Zeile hinzu

```
push “route 192.168.0.0 255.255.255.0”
```

Die IP muss man natürlich an das heimische Netzwerk anpassen.

Eine Verschlüsselung und Kompression sollte man natürlich einbauen aber Achtung, dies treibt die CPU Auslastung natürlich etwas in die Höhe!

```
cipher AES-128-CBC
comp-lzo
```

Das wären die wichtigsten Funktionen, es gibt natürlich noch viele Parameter mehr aber das wäre dann schon für

spezielle Anwendungsbereiche.

13. Windows Client Datei für die Verbindung mit Server

Die Datei müssen wir natürlich auch editieren und mit unseren Daten Füttern.

Wichtig ist dabei nur dass die Pfade der ca.crt, windowspc.crt und windowspc.key stimmen, die IP Eures VPN Servers eingetragen ist und Ihr den Verschlüsselungsmechanismus eintragt.

In der Zeile “remote” bevorzuge ich persönlich eher Domain Namen. Da hat man weniger Probleme falls sich die IP mal ändern sollte.

```
# to load balance between the servers.
remote 192.168.0.1 1194
# SSL/TLS parms.
# See the server config file for more
# description. It’s best to use
# a separate .crt/.key file pair
# for each client. A single ca
# file can be used for all clients.
ca ca.crt
cert windowspc.crt
key windowspc.key
cipher AES-128-CBC
```

14. Anpassungen am Host Server

Damit das alles auch so funktioniert müssen noch Anpassungen am Host System vorgenommen werden.

In der “sysctl.conf” muss das IPv4-Forwarden aktiviert werden. Dazu das Semikolon vor “net.ipv4.ip_forward=1″ entfernen und die Datei speichern.

Die Datei liegt in /etc/

```
root@vpn:~# vi /etc/sysctl.conf
```

```
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

Nun müssen wir noch ein paar iptables Regeln anwenden.

Hinweis

Vor dem ausführen der Befehle mit “ifconfig” die eigenen Einstellungen und Netzwerkkarten Namen herausfinden und in den Befehlen entsprechend anpassen!! sonst funktionieren die Regeln nicht!

Hat man seinene Netzwerkkarten Bezeichnung mittels “ifconfig” herausgefunden, so muss man die einfach entsprechend in den Regeln ersetzen. Es kann also sein dass Ihr aus eth0 ein venet0 oder Ähnliches machen müsst.

Die Regeln, einzeln, einfach in die Konsole eingeben und Entern

```
iptables -A INPUT -i eth0 -m state --state NEW -p udp --dport 1194 -j ACCEPT
```

```
iptables -A INPUT -i tun+ -j ACCEPT
```

```
iptables -A FORWARD -i tun+ -j ACCEPT
```

```
iptables -A FORWARD -i tun+ -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
iptables -A FORWARD -i eth0 -o tun+ -m state --state RELATED,ESTABLISHED -j ACCEPT
```

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

Wichtig!

Bei den iptables Regeln unbedingt darauf achten, dass an den Stellen

```
state --state NEW -p udp - -dport 1194
```

```
eth0 -m state --state RELATED
```

```
tun+ -m state --state RELATED
```

Zwei – Striche vor state und dport sind. Manche Browser machen aus diesen 2 – Zeichen ein längeres — Zeichen

Danke Jakob, ohne das Gespräch mit dir wäre mir das selbst so nie aufgefallen.

Sollten bei diesen Befehlen keinerlei Fehler auftauchen, speichert diese in die “rc.local” um die Befehle bei einem Restart des Server erneut auszuführen.

```
root@vpn:~# vi /etc/rc.local
```

```
# By default this script does nothing.

iptables -A INPUT -i eth0 -m state --state NEW -p udp --dport 1194 -j ACCEPT

iptables -A INPUT -i tun+ -j ACCEPT

iptables -A FORWARD -i tun+ -j ACCEPT

iptables -A FORWARD -i tun+ -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT

iptables -A FORWARD -i eth0 -o tun+ -m state --state RELATED,ESTABLISHED -j ACCEPT

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

Nun kann OpenVPN neugestartet werden. Dazu einfach den Befehl ausführen:

```
root@vpn:~# /etc/init.d/openvpn restart
```

Sollte dabei kein Fehler erscheinen kann mit der Client Konfiguration fortgefahren werden.

Erscheint bei Euch eine Fehlermeldung dann einfach die Schreibweise und Pfade in den Konfigurationen überprüfen, dort liegt oft der Fehler. Natürlich gebe ich gern Hilfe falls Ihr hängt.

15. Windows Client Einrichtung

In ein paar Schritten zuvor, habt Ihr euch ja 4 Dateien runter geladen.

- ca.cert
- windowspc.cert
- windowspc.key
- windowspc.conf

Mit diesen Dateien macht Ihr einfach an dieser Stelle hier weiter:

Windows VPN Einrichtung (https://www.sugar-camp.com/windows-8-vpn-mit-openvpn-einrichten/)

Den Artikel schrieb ich schon vor einer ganzen Weile mal ist aber nach wie vor aktuell.

16. Linux Client einrichten

Als erstes muss auch hier die OpenVPN Software installiert werden

```
root@vpn-client:~# apt-get install openvpn
```

Die 4 Dateien die Ihr runtergeladen habt, einfach in den Ordner

```
/etc/openvpn
```

kopieren und dann openvpn mittels

```
root@vpn-client:~# openvpn --config windowspc.conf
```

neustarten.

Hinweis

Auch auf einem Linux Client muss entsprechend das TUN/TAP Device vorhanden sein!

17. Client unter OS X einrichten

Ladet euch die Software Tunnelblick (https://code.google.com/p/tunnelblick/wiki/DownloadsEntry?tm=2) herunter. Öffnet und installiert die heruntergeladene Datei dann bei euch so wie im Prinzip jedes andere Programm. Im Anschluss wird ein Abfragefenster angezeigt bei dem man auf “Open configuration folder” klickt. In das sich daraufhin öffnende Fenster kopiert man die 4 Dateien hinein. Jetzt Tunnelblick aus dem Programmordner heraus starten und eine Verbindung mit dem OpenVPN-Server herstellen.

18. Client unter iOS einrichten

Benennt die Datei “windowspc.conf” in “windowspc.ovpn” um.

Ladet euch die OpenVPN App für iOS auf euer iPhone, iPad oder iPod touch (https://itunes.apple.com/de/app/openvpn-connect/id590379981?mt=8).

Startet dann die App und klickt rechts oben auf den Button “Help”. Ihr seht dann dort eine Vielzahl an Möglichkeiten eure OpenVPN-Verbindung damit einzurichten.

Mein persönlicher Favorit ist der: schließt euer iPhone, iPad oder iPod touch an euren PC/Mac an, startet iTunes, wählt euer Gerät unter “GERÄTE links im Menü aus, klickt dann auf “Apps”, scrollt runter zum Abschnitt “Dateifreigabe”, klickt die App “OpenVPN” an und dann rechts auf “Hinzufügen…” und wählt nun die 4 Dateien zum Hochladen in die App aus.

Nachdem ihr das gemacht habt startet ihr die OpenVPN App für iOS auf eurem iPhone, iPad oder iPod touch und richtet euch ein Profil mit diesen Dateien ein. Wenn ihr innerhalb der App dann den Schalter unterhalb von “Disconnected” umschaltet wird eine Verbindung zu eurem OpenVPN-Server hergestellt.

19. Client unter Android einrichten

Benennt die Datei “windowspc.conf” in “windowspc.ovpn” um.

Nun ladet Euch die OpenVPN App für Android (https://play.google.com/store/apps/details?id=de.blinkt.openvpn&hl=de) auf das Android Gerät. Kopiert anschließend die 4 Dateien auf das Android Gerät und startet die OpenVPN App für Android. Klickt darin unten rechts auf das Ordnersymbol um die windowspc.ovpn Konfiguration für euren OpenVPN-Server auszuwählen. Im Anschluss werden einige Hinweise angezeigt die man in der Regel nicht zu beachten braucht es reicht dann auf das Diskettensymbol unten rechts zu klicken um den Import abzuschließen.

Im Hauptmenü sollte dann die Verbindung erscheinen die man mit einem Klick darauf starten kann.

Zum Schluss:

Es gibt einige gute Anleitungen auch im Netz aber mir fiel keine auf in der wirklich mal alles zusammen geschrieben wurde.

Ich hoffe die Anleitung ist Euch eine Hilfe und Ihr spart ein wenig Zeit und kommt damit ans Ziel!

LG

Share it! (https://www.facebook.com/sharer.php?u=https://www.sugar-camp.com/anleitung-openvpn-server-auf-debian-7-8-installieren-und-anschliessend-mit-android-ios-oder-windows-verbinden/) (mailto:?Subject=Anleitung: openVPN Server auf Debian 7.8 installieren und anschließend mit Android, iOS oder Windows verbinden&Body=Gesehen auf www.sugar-camp.com%20https://www.sugar-camp.com/anleitung-openvpn-server-auf-debian-7-8-installieren-und-anschliessend-mit-android-ios-oder-windows-verbinden/) (https://plus.google.com/share?url=https://www.sugar-camp.com/anleitung-openvpn-server-auf-debian-7-8-installieren-und-anschliessend-mit-android-ios-oder-windows-verbinden/) (https://twitter.com/share?url=https://www.sugar-camp.com/anleitung-openvpn-server-auf-debian-7-8-installieren-und-anschliessend-mit-android-ios-oder-windows-verbinden /&text=Anleitung%3A+openVPN+Server+auf+Debian+7.8+installieren+und+anschlie%C3%9Fend+mit+Android%2C+iOS+oder+Windows+verbinden+)

- Anleitung (https://www.sugar-camp.com/tag/anleitung/), Debian (https://www.sugar-camp.com/tag/debian/), OpenVPN (https://www.sugar-camp.com/tag/openvpn/)

(https://www.sugar-camp.com/author/sugar/)

Andre

Begeisterter Technik Fan der im Online Bereich bei Telefonica Germany arbeitet. Niemals aufgeben und immer eine Lösung finden, steht auf meiner Fahne denn nichts ist unmöglich! Man muss es sich nur selbst erarbeiten!

- (mailto:sugar@sugar-camp.com)

4 Kommentare

1 Ping

Zum Kommentar-Formular springen

1. 
   - Roland on 23. Mai 2016 at 12:07
   - Antworten (https://www.sugar-camp.com/anleitung-openvpn-server-auf-debian-7-8-installieren-und-anschliessend-mit-android-ios-oder-wind

   Vielen Dank für diese Anleitung!

   Ich habe OpenVPN auf einem Vserver mit Debian installiert und möchte vom Client aus jeglichen Internet Verkehr über das VPN zum VServer leiten und von dort in das Internet gehen.

   Die Verbindung klappt auch, jedoch wird kein DNS gefunden, bzw. ich kann nur den Apache2 auf dem Vserver aufrufen bzw. dessen Seiten.
   Meine Iptables konfiguratiion habe ich auf venet0 geändert (Vserver).
   Hast du einen Tip zum Einlesen wie ich das Konfigurieren muß?

   viele Grüße
   Roland

   1. 
      - Andre (https://www.sugar-camp.com) on 23. Mai 2016 at 18:50
      - Author
      - Antworten (https://www.sugar-camp.com/anleitung-openvpn-server-auf-debian-7-8-installieren-und-anschliessend-mit-android-ios-od

      Hi Roland,

      freut mich wenn es dir geholfen hat 🙂

Ich würde mal vermuten, dass deine IP Tables nicht passen.
Hast du den Masquerade Eintrag angelegt? Klingt im ersten Moment als würde dieser fehlen (Die Tatsache dass dieser Kommentar mit einer 10.8.0.XX IP erstellt wurde würde das bestätigen)

```
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o venet0 -j MASQUERADE
```

Wie sieht denn die Server Config im Details aus?

Wie sieht denn deine client Config aus? und welches Betriebssystem verwendest du auf dem Client?
Kannst du einen MTR bei verbundenem VPN auf google.de machen und Posten?

Hat der Server eine funktionierende Internetverbindung?
Führst du Openvpn als Admin aus?

LG
André

2.
   - 
   - Michael on 29. November 2017 at 00:18
   - Antworten (https://www.sugar-camp.com/anleitung-openvpn-server-auf-debian-7-8-installieren-und-anschliessend-mit-android-ios-oder-wind

Vielen Dank für dieses tolle tut.
ich hätte mal eine eine Frage bezüglich ipv6. Ich habe natürlich einen eigenen vps und zuhause einen Kabel Deutschland Anschluss mit dual stack echte ipv4 und echte ipv6. Wie verhält sich nun der vpn server wechselt der nur die ipv4 und die echte ipv6 kommt trotzdem weiter durch oder blockiert die ipv6 der openvpn server? Man könnte natürlich auch am heimischen PC ipv6 blockieren aber leider geht das nicht direkt in der fritzbox da vodafone ihre Krüppel Firmware auf die Boxen installiert.

1.
   - 
   - Andre (https://www.sugar-camp.com) on 29. November 2017 at 07:25
   - **Author**
   - Antworten (https://www.sugar-camp.com/anleitung-openvpn-server-auf-debian-7-8-installieren-und-anschliessend-mit-android-ios-od

Hi,
gerne und danke für das Feedback!
Mir ist noch nicht ganz klar was dein Ziel ist? Wenn du mit dem VPN verbunden bist, hast du die IPv4/6 vom VPN Server und wenn du getrennt bist die IPv4/6 deines DSL Anschlusses.
Wenn du mit dem VPN verbunden bist, sieht niemand deine echte IP sondern nur die IP's vom Server.

1.
   - Anleitung:OpenVPN LDAP Authentifizierung beibringen (https://www.sugar-camp.com/anleitung-debian-openvpn-mit-ldap-auth-ohne-active-directory/) on 15. Mai 2015 at 22:41

[…] Sollte dies noch nicht der Fall sein, so könnt Ihr diese Anleitung dafür nutzen: Anleitung: openVPN Server auf Debian 7.8 installieren und anschließend mit Android, iOS oder Window… […]

Schreibe einen Kommentar

Your email address will not be published.

Your message

Name | Email | Website (optional)

Kommentar senden

☐ **Benachrichtige mich über nachfolgende Kommentare via E-Mail.**

☐ **Benachrichtige mich über neue Beiträge via E-Mail.**