

Inhalt:

0. Summary (English)
1. OpenVPN-Version
2. Authentifizierungsmethode
3. LZO-Kompression
4. Empfohlene Konfigurationsparameter
5. Vorsichtsmaßnahmen
6. Hinweise für Linux-Systeme
7. Hinweise für Windows-Systeme
8. Verwendung als Router
9. Anhang
 - 9.1 Das mdex-Zertifikat
 - 9.2 Eine Beispiel-Konfiguration
 - 9.3 Kontakt

0. Summary (English)

- Use OpenVPN version 2.0x or higher.
- Authentication method: Username/Password (compile binary with option '--enable-password-save')
- The OpenVPN binary needs to be built with support for LZO compression.
- Recommendation: Set configuration parameter "reneg-sec" to 86400 seconds to keep traffic volume low.
- On routers, please make NAT support on the OpenVPN virtual interface configurable. For "mdex fixed.IP" NAT is necessary, for "mdex managed.VPN" it isn't.
- You will find our certificate and a configuration example at the end of this document.

1. OpenVPN-Version

Geeignet ist ein OpenVPN-Client ab Version 2.0x

2. Authentifizierungsmethode

Der OpenVPN-Zugang von mdex benutzt als Authentifikationsmethode des Clients ausschliesslich "Username/Passwort".

Username und Passwort sollten in der Konfigurations-GUI einmalig eingegeben werden können und in eine Passwort-Datei unterhalb von /etc/openvpn geschrieben werden. Damit OpenVPN diese Datei einliest muss der OpenVPN-Client mit der Option '--enable-password-save' kompiliert werden.

Beispiel-Datei "password.txt":

m0001234@mdex.de

1te54hz6

3. LZO-Kompression

Das OpenVPN-Binary muss mit LZO-Support erstellt werden.

4. Empfohlene Konfigurationsparameter

- Wir empfehlen das Hochsetzen des "reneg-sec"-Parameters auf 86400 Sekunden, um das übertragene Datenvolumen gering zu halten.
- Eine Beispiel-Konfiguration mit weiteren Parametern finden Sie im Anhang (Abschnitt 9.2).

5. Vorsichtsmaßnahmen

- Bei unbeaufsichtigtem Betrieb des OpenVPN-Clients sind Maßnahmen vorzusehen, welche ein ungewolltes Gebührenaufkommen durch wiederholte, erfolglose Einwahlversuche unterbindet (Retry delay o.ä.)
- Bei unbeaufsichtigtem Betrieb des OpenVPN-Clients sind Maßnahmen vorzusehen, welche einer ungewollten Beendigung des OpenVPN-Service durch wiederholte, erfolglose Einwahlversuche unterbindet (Hardware restart alle 24h etc.)
- ~ Regelmäßiges Testen des Tunnels (z.B. ping auf ping.mdex.de) erhöht die Stabilität

6. Hinweise für Linux-Systeme

Auf UNIX/Linux wählt man im Rahmen des typischen Build-Dreisatzes alle gewünschten Optionen aus:

- 1.) ./configure --enable-password-save
- 2.) make
- 3.) make install

./configure --help gibt aus was OpenVPN an Konfigurationsoptionen anbietet und wie sie defaultmäßig gesetzt sind.

7. Hinweise für Windows-Systeme

OpenVPN Patchanleitung:

```
--- ../sources/openvpn-2.0.9/openvpn-2.0.9/options.c           Mon Dec 12 14:50:44 2005
+++ options.c           Tue Mar 20 15:16:52 2007
@@ -2231,6 +2231,7 @@
    msg (M_INFO|M_NOPREFIX, "%s", title_string);
    msg (M_INFO|M_NOPREFIX, "Developed by James Yonan");
    msg (M_INFO|M_NOPREFIX, "Copyright (C) 2002-2005 OpenVPN Solutions LLC ");
    msg (M_INFO|M_NOPREFIX, "With --enable-password-save for mdex by IC3S(elohmann)");
    openvpn_exit (OPENVPN_EXIT_STATUS_USAGE); /* exit point */
}
```

```
--- ../sources/openvpn-2.0.9/openvpn-2.0.9/config-win32.h      Sun Oct 1 04:18:54 2006
+++ config-win32.h      Tue Mar 20 15:40:41 2007
@@ -63,7 +63,7 @@
#define TAP_WIN32_MIN_MINOR 1

/* Allow --askpass and --auth-user-pass passwords to be read from a file */
/* #undef ENABLE_PASSWORD_SAVE */
#define ENABLE_PASSWORD_SAVE

/* Enable client/server capability */
#define ENABLE_CLIENT_SERVER 1
```

8. Verwendung als Router

fixed.IP:

Pakete welche über das OpenVPN-Device laufen, müssen für fixed.IP per NAT weitergeleitet werden.

managed.VPN:

Pakete welche über das OpenVPN-Device laufen, sollten für managed.VPN NICHT per NAT weitergeleitet werden.

Gut wäre es, wenn man in der RouterGUI dieses Feature ein und abschalten kann, default sollte EIN sein.

Beispiel für NAT unter Linux:

```
*iptables -t nat -A POSTROUTING -o tun0 -j MASQUERADE*
```

9.1 Das Zertifikat IC3S–CA.CRT:

RootCA–cert.pem

=====

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 0 (0x0)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=DE, ST=Schleswig–Holstein, L=Quickborn, O=IC3S AG,
OU=Certification Authority, CN=Root Certification

Authority/Email=ca-admin@ic3s.de

Validity

Not Before: Dec 12 13:32:46 2002 GMT

Not After : Dec 7 13:32:46 2022 GMT

Subject: C=DE, ST=Schleswig–Holstein, L=Quickborn, O=IC3S AG,
OU=Certification Authority, CN=Root Certification

Authority/Email=ca-admin@ic3s.de

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:be:20:e0:83:53:6b:6a:de:bf:7f:34:cc:1f:dd:
76:10:36:9a:cd:2c:1c:60:b7:92:11:ad:a7:4d:5c:
88:a9:11:ea:53:f8:c5:ef:a7:4c:7d:a4:da:77:c9:
bb:47:80:2c:bc:9d:17:75:9e:2a:4b:ad:b3:c8:4d:
7a:f0:2c:7b:6d:da:f6:93:23:94:40:9e:cc:cf:5b:
83:21:5d:27:1f:55:e1:27:6a:cb:f1:bb:5a:15:89:
15:89:69:02:55:79:c0:8a:53:ff:ed:66:95:b0:25:
fe:2f:3d:60:0b:60:4b:b8:35:7c:bc:5f:d6:44:b6:
c7:b2:75:c3:93:84:a5:91:91

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:TRUE

X509v3 Subject Key Identifier:

F9:F3:34:39:03:EE:32:19:7E:FC:8C:F5:7D:53:0E:89:A5:EF:F7:DF

X509v3 Authority Key Identifier:

keyid:F9:F3:34:39:03:EE:32:19:7E:FC:8C:F5:7D:53:0E:89:A5:EF:F7:DF

DirName:/C=DE/ST=Schleswig-Holstein/L=Quickborn/O=IC3S

AG/OU=Certification Authority/CN=Root Certification

Authority/Email=ca-admin@ic3s.de

serial:00

X509v3 Key Usage:

Certificate Sign, CRL Sign

Netscape Cert Type:

SSL CA, S/MIME CA, Object Signing CA

X509v3 Subject Alternative Name:

email:ca-admin@ic3s.de

X509v3 Issuer Alternative Name:

email:ca-admin@ic3s.de

X509v3 CRL Distribution Points:

URI:http://ca.ic3s.de/RootCA.crl

Netscape Base Url:

<https://ca.ic3s.de/>

Netscape CA Policy Url:

<http://ca.ic3s.de/policy.html>

Netscape Comment:

This certificate is a Root CA Certificate

Signature Algorithm: md5WithRSAEncryption

b4:ce:2e:72:40:12:3b:3d:b5:ac:88:70:3c:09:72:56:8f:b2:
78:83:c0:a7:c2:58:e7:a8:6e:08:74:7e:b8:a7:4a:e5:a9:95:
e9:88:b9:cf:80:ca:2e:0c:15:99:73:a5:b8:50:2b:23:f4:75:
9d:d7:a7:55:fe:97:92:e6:df:cd:b9:68:3e:99:5e:16:49:74:
b1:2b:f2:2d:8b:a0:5e:5e:7b:68:bf:e6:86:be:f6:dc:9b:10:
be:ea:03:cd:6b:a8:03:fa:33:1e:1b:2c:2c:18:ce:16:ad:8a:
6b:a7:73:8d:f2:48:77:f8:e6:bc:9d:93:4f:48:00:61:8d:7d:
2c:b0

9.2 Eine Beispiel-Konfiguration

fixedip.conf:

```
client
dev tun
remote fixedip.mdex.de
rport 9300
proto udp
# 1500 hat sich bewährt
tun-mtu 1500
fragment 1300
# Einmal am Tag wg. Kosten
reneg-sec 86400
# keepalive wird gepusht ! (z.Zt. 27 sec.)
ns-cert-type server
ca /etc/openvpn/IC3S-CA.CRT
cipher BF-CBC
# muss auf 'auth-user-pass <filename>' gesetzt werden, wenn automatisches Login (Router)
erwünscht ist.
auth-user-pass password.txt
comp-lzo
# Optional: Default Gateway ersetzen, d.h. aller Internettraffic wird durch
# den openVPN Tunnel geroutet (experimental)
# redirect-gateway def1
```

9.3 Kontakt

Bitte wenden Sie sich bei Fragen an:

mdex GmbH
Bäckerbarg 6
22889 Tangstedt

Telefon: 04109-555 444
Telefax: 04109-555 101

E-Mail: support@mdex.de