KB Name	Using eWON with OpenVPN		
Type	KB, Config Example		
Since revision	NA		
KB Number	KB-0018-0	Build	33
Mod date	11. Sep 2008		

Knowledge Base Information

Using eWON with OpenVPN

Table of Contents

1 OpenVPN configuration inside eWON

The OpenVPN configuration used by the eWON is described bellow. You must read this information like the concatenation of different blocs corresponding to conditions from the eWON COM configuration.

The UnderlinedGreen parameters come from the ComCfg.txt configuration.

The **Red** parameters are ComCfg.txt data which need additional data to pass them to the OpenVPN. The additional data can not be stored directly in the comcfg.txt configuration file . Instead a /usr/file should be used.

The **Black** parameters are explained in the footnotes.

Some examples are given at the end of this documents.

1.1 Depending on VPNKeyType

1.1.1 Using "shared key" (VPNKeyType=0)

plugin ewon

suppress-timestamps

rport VPNPortOut

ifconfig **CfgLocalIp CfgRemoteIp**[1]

secret **VPNSecretKey**

verb VPNDiag[2]

mute 10

comp-lzo

persist-key

up-delay

route-delay 0

---

1 If VPNP2PIpMode = 0 (automatic) and VPNCnxType **=** 2 (outgoing)
CfgLocalIp = 10.254.0.1
CfgRemoteIp = 10.254.0.2
If VPNP2PIpMode = 0 (automatic) and VPNCnxType **<>** 2 (outgoing)
CfgLocalIp = 10.254.0.2
CfgRemoteIp = 10.254.0.1
If VPNP2PIpMode **<>** 0 (automatic)
CfgLocalIp = VPNLocalIp
CfgRemoteIp = VPNRemoteIp

2 If VPNDiag < 0 then VPNDiag = 0
if VPNDiag > 11 then VPNDiag = 11

1.1.2 Using "PKI" (VPNKeyType=1)

plugin ewon
suppress-timestamps
client
ns-cert-type server
tls-exit
rport VPNPortOut
ca **VPNCACert**
cert **VPNSecretCert**
key **VPNSecretKey**
verb VPNDiag[3]
mute 10
comp-lzo
persist-key
up-delay
route-delay 0

1.1.3 Using "Password" (VPNKeyType=2)

plugin ewon
suppress-timestamps
client
tls-exit
rport VPNPortOut
ca **VPNCACert**
verb VPNDiag[4]
mute 10

3 If VPNDiag < 0 then VPNDiag = 0
if VPNDiag > 11 then VPNDiag = 11
4 If VPNDiag < 0 then VPNDiag = 0
if VPNDiag > 11 then VPNDiag = 11

comp-lzo

persist-key

up-delay

route-delay 0

auth-user-pass **USER_PASS_STRING**[5]

1.2 Depending on VPNDrvMode

1.2.1 TUN (VPNDrvMode=0)

```
dev-type tun
dev-node /tun/0
```

1.2.2 TAP (VPNDrvMode=1)

```
dev-type tap
dev-node /tap/0
```

1.3 Depending on VPNProto

1.3.1 UDP (VPNProto=0)

```
proto  udp
```

1.3.2 TCP (VPNProto=1)

5 The USER_PASS_STRING is a string built with the following format:<0xFF>VPNSecretCert<0xFF>VPNSecretKey.
Example: if VPNSecretCert if *joe* and VPNSecretKey is *pass* then the string is <0xFF>joe<0xFF>pass.
The <0xFF> is a single character with ascii value = 255.
REM: an editor is hard to use to build this string because the 0xFF character is not editable.

1.4 Depending on WANPxyMode

1.4.1 Standard proxy (WANPxyMode=1)

if (WANPxyUsr is empty)

```
http-proxy WANPxyAddr WANPxyPort
```

else

```
http-proxy WANPxyAddr WANPxyPort  USER_PASS_STRING[6] basic
```

1.5 Depending on VPNPortIn

1.5.1 local VPN IP Port not defined (VPNPortIn=0)

Important:

If VPNPortIn = 0 and VPNCnxType = 2 (Outgoing)

```
nobind
```

If VPNPortIn = 0 and VPNCnxType <> 2 (Not Outgoing)

Then VPNPortIn = 1194 and next paragraph applies

1.5.2 local VPN IP Port defined (VPNPortIn<>0)

6 The USER_PASS_STRING is a string built with the following format:<0xFF>WANPxyUsr<0xFF>WANPxyPass.
Example: if WANPxyUsr is *joe* and WANPxyPass is *pass* then the string is <0xFF>joe<0xFF>pass.
The <0xFF> is a single character with ascii value = 255.
REM: an editor is hard to use to build this string because the 0xFF character is not editable.

```
lport  VPNPortIn
```

1.6 Depending on VPNAlive

1.6.1 Keep Alive is used (VPNAlive<>0)

If VPNAlive < 10

Then VPNAlive = 10

```
keepalive  VPNAlive/4 VPNAlive
```

If VPNCnxType <> 2 (Not Outgoing)

```
ping-timer-rem
```

1.7 Depending on VPNCnxType

1.7.1 Connection type is set to “establish outgoing” (VPNCnxType=2)

If VPNSrv1 <> “”

```
remote VPNSrv1
```

If VPNSrv2 <> “”

```
remote VPNSrv2
```

```
resolv-retry infinite
```

1.8 Depending on VPNRedirect

1.8.1 Redirect all traffic through VPN enabled (VPNRedirect<>0)

```
redirect-gateway
```

1.9 Using or adding a "User defined config file"

The *VPNCfgFile* parameter can be defined to either **add** or **use** a VPN configuration file to the VPN configuration described above.

1.9.1 VPNCfgFile first character is '+': configuration file ADDED

If the configuration file is added, it will be added at the end of the above eWON configuration.

```
config VPNCfgFile[7]
```

1.9.2 VPNCfgFile first character is <> from '+': configuration file REPLACE config

If the configuration file replaces the above eWON configuration, then the following minimal configuration will be set:

```
plugin ewon
suppress-timestamps
config VPNCfgFile
```

2 Examples

2.1 Endian router configuration

7 The + character at the beginning of the file name is skipped.

VPNKeyType=2

```
plugin ewon
suppress-timestamps
client
tls-exit
rport VPNPortOut
ca VPNCACert
verb VPNDiag1
mute 10
comp-lzo
persist-key
up-delay
route-delay 0
auth-user-pass <0xFF>VPNSecretCert<0xFF>VPNSecretKey
dev-type tap[8]
dev-node /tap/0
proto  udp
nobind[9]
keepalive  VPNAlive/4 VPNAlive
ping-timer-rem
remote VPNSrv1
resolv-retry infinite
redirect-gateway[10]
```

2.2 Mdex configuration example

Considering this configuration proposed by Mdex

```
##############################################################################
# MDEX GmbH, fixed.IP Konfiguration                          ....................
..............................................................................
.............................................................................. #
# $Id: mdex fixed.IP.ovpn 42669 2008-04-18 09:45:03Z eike $ #
##############################################################################

#Falls mehr als ein Tunnel existiert TapWin32 Adaptername hier eintragen
;dev-node Interfacename

# IP Tunnelkonfiguration
dev tun
client
cipher BF-CBC
remote fixedip.mdex.de
rport 9300
proto udp
```

8 Because VPNDrvMode = 1
9 If VPNPortIn = 0
10 If VPNRedirect <> 0

```
tun-mtu 1500
fragment 1300
mssfix
float
reneg-sec 86400

# Sourceport dynamisch
nobind
#bind

# stabile Windowsrouten
route-method exe
route-delay 6 6

# Autorisierungseinstellungen
ca IC3S-CA.crt
ns-cert-type server
auth-user-pass
# Optional User/pwd in Datei
# auth-user-pass filename

# Kompression, Logging
comp-lzo
verb 4
```

The following configuration should be used in eWON

VPNKeyType=2 (password)

VPNDrvMode = 0 (dev tun)

VPNProto=0 (udp)

VPNSrv1=fixedip.mdex.de (remote fixedip.mdex.de)

VPNPortOut = 9300 (rport 9300)

VPNPortIn = 0 (nobind)

VPNCnxType = 2 (establish Cnx)

VPNCACert =

```
-----BEGIN CERTIFICATE-----
MIIFITCCBIqgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBujELMAkGA1UEBhMCREUx
..................... TRUNCATED ..............................
cDwJclaPsniDwKfCWOeobgh0frinSuWplemIuc+Ayi4MFZlzpbhQKyP0dZ3Xp1X+
l5Lm3825aD6ZXhZJdLEr8i2LoF5ee2i/5oa+9tybEL7qA81rqAP6Mx4bLCwYzhat
imunc43ySHf45rydk09IAGGNfSyw
-----END CERTIFICATE-----
```

VPNDiag = 4 (verb 4)

Then you need to create a **/usr/mdexcfg.txt** filewith the following content:

```
tun-mtu 1500
fragment 1300
mssfix
float
reneg-sec 86400
ns-cert-type server
```

VPNCfgFile = +/usr/mdexcfg.txt (add some VPN config from the file)

VPNSecretCert = *MdexUserName*

VPNSecretKey = *MdexPassword*

2.2.1 Remark:

These paramters are not required on eWON (windows dependent)

```
route-method exe
route-delay 6 6
```