

Kopplung zweier TP-II über das Internet

Vorraussetzung:

- Firmware \geq 7.46
- Betriebs-System \geq 0.38
- Feste IP-Adresse auf der Endkundenseite, ansonsten sich eine feste IP-Adresse besorgen (Siehe Kapitel DynDNS)



Aktuelle Firmware sowie Betriebssystem können unter www.tpa-partner.de/ftp/pub/demos/TP-II-Internet-Kopplung.zip

runtergeladen werden. Das Passwort zum Entpacken der Datei lautet: tp2
Anschließend Setup.exe starten und den Prof-II-Manager installieren.

Nach dem der Manager gestartet wurde, IP-Adresse des TP-II einstellen und durch Drücken des Buttons „Firmware & OS Senden“ wird beides im TP-II aktualisiert. Der ganze Vorgang ist beendet, wenn der Manager „Action OK“ meldet.

Aufbau:

Es werden hierzu beide Geräte mit der passenden Ethernet-IP-Adresse an das jeweilige Netzwerk angeschlossen. Die Subnet-Maske sollte hierbei ebenfalls verwendet werden. Bitte auch das Standard-Gateway für Verbindungen in das Internet korrekt konfigurieren.

Allgemeines zur Sicherheit:

Im TELE-PROF-II haben wir das populäre unter Opensource veröffentlichte OpenVPN implementiert. Detaillierte Information finden Sie unter <http://www.openvpn.net>.

Hier möchte ich kurz die Funktion des OpenVPN, wie es im TELE-PROF-II implementiert ist, erläutern.

Grundsätzlich gibt es zwei Betriebsarten des OpenVPN: *Server* oder *Client*.

Als *Server* wird normalerweise das Gerät an der Anlage (AG-TELE) konfiguriert. Mit OpenVPN stellen wir im TeleProf ein neues Netzwerkinterface zur Verfügung. Dieses Interface wird quasi mit einer Leitung (virtuelle Leitung) mit dem OpenVPN-Interface des Partnergerätes verbunden. Die Leitung wird mit Software realisiert. Dabei werden sämtliche Protokolle für dieses Interface über einen eigenen UDP-Kanal ausgetauscht. Man kann sagen es wird eine Telefonverbindung zwischen den Geräten per UDP hergestellt. Selbstverständlich ist die Verbindung verschlüsselt. Die Schlüssel sind im TELE-PROF-II hinterlegt.

Verwenden von DynDNS

TELE-PROF II	DynDNS Konfig
Netzwerk	verwende DynDNS: Ja <input type="checkbox"/>
Net-Konfig	DynDNS Hostname: tprof2.dynalias.com
Hostliste	DynDNS Username: TpDynDNS
DynDNS Konfig	DynDNS Passwort: MyPass
Internet	Änderungen übernehmen: <input type="checkbox"/>
Firewall	Daten neu laden: <input type="checkbox"/>
Open VPN	
VPN-Verbindungen	
PSK-Schlüssel	
erzeuge PSK	

Wir setzen voraus, dass wir vom Provider eine öffentliche IP-Adresse bekommen. Nun stellt sich die Frage, wie kann das TELE-PROF-II-Gerät nach der Einwahl ins Internet erreicht werden?

Für dieses Problem gibt es bereits eine Lösung im Internet. Der Dienstleister DynDNS (DynDNS = Dynamic DomainName Server) (<http://www.dyndns.org>) bietet hier einen Service an. Dazu müssen Sie sich bei DynDNS anmelden. Näheres auf der Homepage von DynDNS. Bis zu 5 dynamische IP-Adressen sind frei. Sollten Sie mehr benötigen, können Sie bei DynDNS gegen Bezahlung eine entsprechende Anzahl Namen buchen.

Im Groben geht das so:



Sie registrieren bei DynDNS den gewünschten Hostnamen. z.B. meineanlage.dynalias.com. Für Ihren Zugang erhalten Sie Benutzername und Passwort. Tragen Sie diese Daten in die Einstellung **DynDNS-Konfig** ein und setzen Sie „verwende DynDNS“ auf ja. Bei der nächsten Interneteinwahl registriert das TELE-PROF-II die ihm zugeteilte IP-Adresse bei DynDNS unter meineanlage.dynalias.com.

Sofort haben Sie auf die Maschine über den Namen meineanlage.dynalias.com Zugriff. Da Sie jedoch mit der Firewall arbeiten und die Zugänge über Modem (außer OpenVPN) gesperrt haben, wird kein Ping oder ähnliches funktionieren. Zum Test können Sie den Pingservice über Modem freigeben. Nun sollten Sie bei „ping meineanlage.dynalias.com“ auch eine Antwort bekommen. Deaktivieren Sie den Ping über Modem wieder (Internetverbindung muß nicht beenden werden) und Sie bekommen keine Antwort mehr. Nun wissen Sie, Ihr Gerät im Internet ist.

Fortan bauen Sie eine Verbindung über OpenVPN zum Gerät auf und schon können Sie Ihre Anlage warten. Auch OpenVPN verwendet den Eintrag meineanlage.dynalias.com.

Konfiguration des OpenVPN-Server:

Anbei die Beispielseinstellung.

TELE-PROF II	Open VPN
Netzwerk	OVPN-Mode: Server (UDP) ▼
Net-Konfig	IP-Pool (nur Server): 10.111.111.0
Hostliste	IP-Pool Netmask (nur Server): 255.255.255.0
DynDNS Konfig	Port: 1194
Internet	Server-Adr (nur Client):
Firewall	Benutzer (nur Client):
Open VPN	Passwort (nur Client):
VPN-Benutzer	Änderungen übernehmen: 
VPN-Verbindungen	Daten neu laden: 
HAUPTAUSWAHL	
© Copyright 1994 - 2004 by TIS & PI	

Im Serverbetrieb geben Sie an, welche IP-Adresse das Netzwerkinterface des OpenVPN-Servers erhält. Diese legen Sie über den IP-Pool fest.

Bei der Angabe im Beispiel erhält der Server die Adresse 10.111.111.1 und 10.111.111.2. Diese beiden Adressen reserviert sich OpenVPN automatisch, da später darüber eine PPP-Verbindung realisiert wird.

Über die IP-Pool-Netmask legen Sie fest, aus welchem IP-Bereich den Clients, die sich mit dem TeleProf über OpenVPN verbinden, eine IP-Adresse für Ihr virtuelles Netzwerkinterface zur Verfügung gestellt wird



Bei der Auswahl der Adressen beachten Sie, dass sie einen Adressbereich verwenden, der weder von Ethernet-Interface des Prof II noch von den Modems (Analog oder ISDN) verwendet wird.

Die virtuellen Tunneladressen sind (fast) beliebig, es müssen aber **private Adressen** sein. Die virtuellen Adressen sollten auch aus einem anderen Block stammen als die realen Adressen, da somit das **Routing** einfacher wird -- reales und virtuelles Netz sind leicht zu unterscheiden.



Private Adresse: *Normale, öffentliche IP-Adressen sind weltweit eindeutig. Nur so kann ein Paket den Weg zum richtig Ziel finden. Im Gegensatz dazu sind die privaten IP-Adressen nur im lokalen Netz gültig,*

sie werden nicht in das öffentliche Internet geroutet. Dadurch können mehrere Netze die selben privaten Adressen nutzen. Für diesen Zweck sind einige IP-Bereiche reserviert: 10.x.x.x und 192.168.z.z sowie 172.16.y.y bis 172.31.y.y.

Die Kommunikation wird grundsätzlich über UDP abgehandelt: Sie geben hier lediglich den Port an, über welchen kommuniziert werden soll. Die Ports 9999 und 9998 sollten nicht verwendet werden, da diese vom TELE-PROF-II intern genutzt werden. Als Standard wird 1194 eingestellt. Falls Sie die Geräte an einer Firewall betreiben, sorgen Sie dafür, dass dieser Port weitergeleitet werden bzw. offen ist (z.B. hier im Beispiel UDP 1194).

Zugangsberechtigung

Wer darf nun eine OpenVPN-Verbindung aufbauen?

Wie kann der Zugang kontrolliert werden.



ACHTUNG: Prinzipiell kann jede der das Zertifikat hat und die IP-Adresse des TELE-PROF-II hat eine VPN-Verbindung aufbauen und auf das Gerät zugreifen. Das damit zu vergleichen, wenn Sie das Gerät an die Telefonleitung anschließen und kein Passwort für die Modemeinwahl vergeben.

So schützen Sie das Gerät vor unberechtigtem Zugang

TELE-PROF II						
VPN-Benutzer						
	Nr.	vollständiger Name	Benutzer	Passwort	Passwort (wiederholen)	aktiv
<input type="checkbox"/>	1	Otto Telemeister	Otto	••••••	••••••	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2			*****	*****	

Tragen Sie unter VPN-Benutzer die Teilnehmer ein, welche sich mit OpenVPN verbinden dürfen.

WICHTIG!

Es werden nur diese Benutzer zugelassen, welche mit dem „aktiv“-Kennzeichen versehen sind. Ist kein Benutzer eingetragen oder ist kein Benutzer aktiviert, so wird jeder Benutzer zugelassen egal welcher Benutzername, oder welches Passwort verwendet wird. Also der Zugang ist offen. ALSO: unbedingt mindestens einen Benutzer anlegen und diesen

aktivieren. Diese Option kann nur hilfreich sein, falls die Zugangsdaten verloren gehen und dringend auf die Anlage zugegriffen werden muß!

Konfiguration des Client (PG-Seite)

Für die Konfiguration des Clients (PG-Seite) gibt es zwei Möglichkeiten:

- Verbindung immer zum gleichen AG-TELE → Variante 1
- Verbindungen zu verschiedenen AG-TELE → Variante 2

Variante 1:

TELE-PROF II PI-ISDN -	Open VPN PI-ISDN -	
Netzwerk	OVPN-Mode:	Client (UDP) <input type="button" value="v"/>
Net-Konfig	IP-Pool (nur Server):	<input type="text"/>
Hostliste	IP-Pool Netmask (nur Server):	<input type="text"/>
DynDNS Konfig	Port:	1194
Internet	Server-Adr (nur Client):	192.168.0.14
Firewall	Benutzer (nur Client):	Otto
Open VPN	Passwort (nur Client):	Mein_Passwort
VPN-Benutzer	Änderungen übernehmen:	<input type="button" value="OK"/>
VPN-Verbindungen	Daten neu laden:	<input type="button" value="↻"/>
HAUPTAUSWAHL		
© Copyright 1994 - 2007 by TIS & PI		

Es wird als OVPN-Mode die Betriebsart „Client UDP“ ausgewählt. Die Menüpunkte „IP-Pool“ sowie „IP-Pool Netmask“ werden hier nicht benötigt und müssen leer sein! Als Port ist der selbe einzustellen, der auch im AG-TELE eingestellt wurde, hier im Beispiel der Port 1194.

„Benutzer“ und „Passwort“ sind von dem Benutzer, der auch im AG-TELE hinterlegt wurde. Nach Übernahme der Einstellungen versucht das Gerät automatisch über die Serveradresse die Gegenstelle zu erreichen und sich VPN-basierend verbinden.

Selbstverständlich kann anstatt einer IP-Adresse auch die DynDNS-Adresse meineanlage.dynalias.com eingetragen werden.

Variante 2:

TELE-PROF II PHISDN -		Open VPN PHISDN -	
OVPN-Mode:		kein OVPN	
IP-Pool (nur Server):		10.111.111.0	
IP-Pool Netmask (nur Server):		255.255.255.0	
Port:		1194	
Server-Adr (nur Client):			
Benutzer (nur Client):			
Passwort (nur Client):			
Änderungen übernehmen:			
Daten neu laden:			

Da in dieser Variante mit verschiedenen AG-TELE und somit mit verschiedenen VPN-Servern gearbeitet wird darf man hier in diesem Menu den automatischen Verbindungsaufbau zum VPN-Server nicht verwenden. Deshalb wird der OVPN-Mode auf „kein OVPN“ gesetzt und abgespeichert.

Dafür legen Sie unter „VPN-Verbindungen“ einen Eintrag an, der auf die feste IP-Adresse des Endkunden (z. Bsp: 192.168.0.14) oder die eventuelle DynDNS-Adresse zeigt.

Protokoll: UDP, Port: 1194 Benutzer wie am AG-TELE unter VPN-Benutzer anlegen.

TELE-PROF II		VPN-Verbindungen					
		Nr.	Name	Server-Adr (nur Client)	Protokoll	Port	Benutzer
		1	192.168.0.14	192.168.0.14	UDP	1194	
		2	teleprof.dyndns.org	teleprof.dyndns.org	UDP	1194	Otto Telemeister
		3			UDP	0	

Nun sorgen Sie dafür, dass das PG-Tele eine Verbindung zum Internet hat.

Dazu tragen Sie in den Netzeinstellungen als Standardgateway und DNS Ihren Router ein, dann wird die Verbindung per Ethernet TCP/IP über Ihren Router hergestellt. Hier die Firewallinstellungen beachten. Der Port UDP 1194 muß geöffnet sein bzw. die Rückmeldung muß von der Firewall über den Port 1194 an das TP-II weitergeleitet werden.

Zur Anwahl bzw. Aufbau der Verbindung einfach mit der Maus auf den entsprechenden Eintrag der VPN-Verbindung klicken und die Verbindung sollte aufgebaut werden.

Nach Aufbau der VPN-Verbindung

Ist die VPN-Verbindung erfolgreich aufgebaut, so wird dem Client automatisch eine Route auf die IP-Adressen, welche über die Ethernetschnittstelle des Servers (AG-Tele) konfiguriert sind, eingerichtet. Beispiel:

SPS IP-Adresse: 192.168.1.99

AG-Tele-Ethernet-IP-Adresse: 192.168.1.54 Mask 255.255.255.0, (Routermode ein)

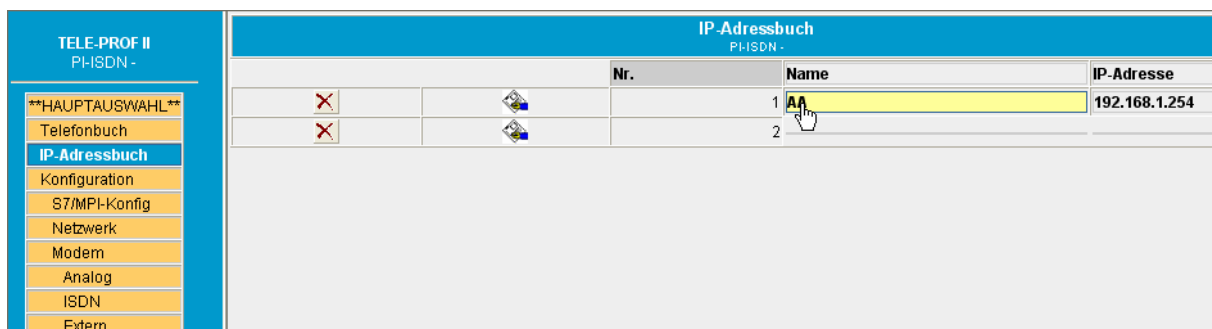
OpenVPN-Pool: 10.111.111.0 Mask 255.255.255.0

PG-Tele: Ethernet-IP-Adresse: 192.168.0.54 (Routermode ein)

PC: 192.168.0.1 (Standardgateway 192.168.0.54)

Ist die VPN-Verbindung aufgebaut können Sie z.B mit „ping 192.168.1.99“ die SPS erreichen oder auch programmieren.

Damit jetzt auch das PG-TELE „AG ist ONLINE“ meldet und der Zugriff auf die an der MPI/Profibus-Buchse angeschlossenen S7-SPS oder S5-SPS (AG-TTY) erfolgen kann, muß noch eine IP-Verbindung über das IP-Adressbuch erfolgen:



IP-Adressbuch PHISDN -		
Nr.	Name	IP-Adresse
1	AA	192.168.1.254
2		

Dazu wird ein Teilnehmer im Adressbuch mit seiner eigenen Ethernet-IP-Adresse angelegt und durch klicken mit der Maus auf den Namen oder IP-Adresse aufgebaut. Sobald dann beide Geräte verbunden sind, steht dem SPS-Zugriff nichts mehr im Weg.

Client PC-Seite

Um eine Verbindung mit einem PC herzustellen zu können benötigen Sie:

1. Eine Open-VPN-Installation auf Ihrem PC
(www.tpa-partner.de/ftp/pub/demos/OpenVPN.zip Passwort: tp2)
2. Die entsprechende Konfigurationsdatei und das zugehörige Zertifikat für das TELE-PROF-II
3. Die IP-Adresse des TELE-PROF-II-Gerätes im Internet. Dies kann eine feste sein, oder eine über DynDNS registrierte.

Wenn Sie unser OpenVPN-Install-Tool verwenden, wird Ihnen die Datei TProf2config.ovpn in /Programme/OpenVPN/Config installiert.

Tragen Sie in dieser Datei die entsprechenden Parameter ein für:

remote (= IP-Adresse des Zielgerätes: z.B. fest: xxx.yyy.nnn.xxx.) oder eben eine über DynDNS registrierte Domain. z.B. test.dyndns.org.

port (Wie am TELE-PROF-II konfiguriert, Standard = 1194)


Achten Sie darauf, dass Ihre Firewall UDP-Verbindungen über diesen Port zulässt.

Auszug aus der Configdatei:

```
#####  
# client-side OpenVPN 2.0 config file      #  
# for connecting to TeleProf II          #  
#                                         #  
# On Windows, you might want to rename this #  
# file so it has a .ovpn extension       #  
#####  
  
# hier die Remote IP-Adresse für TELE-PROF-II eingeben  
# here set the remote ip address of TELE-PROF-II  
# e.g. remote tprof2.dynalias.org  
# replace xxxx with the ip-address  
remote tprof2.dynalias.com  
  
# hier den Port für OpenVPN eingeben  
# here set port of TELE-PROF-II, standard is 1194  
# if you change it, you have to change it on both sides  
port 1194
```

Diese Datei können Sie nach Bedarf für jede Ihrer Anlagen erzeugen und dann am besten nach Anlagenname umbenennen.

Aufbau der Verbindung mit der OpenVPN GUI

Nach Installation sollte in der Taskleiste das OVPN-GUI Symbol  erscheinen. Bewegen Sie die rechte Maustaste über das Icon, die entsprechende Configdatei auswählen und „Connect“ starten. Der Rest dürfte automatisch ablaufen. Gibt es nur eine Configdatei, so gehen Sie direkt auf Connect.

Bei Problemen studieren Sie bitte die Log-Datei. Dort finden Sie Hinweise, was nicht funktioniert hat.

OpenVPN installiert den sogenannten TAP-Netzwerkadapter unter Windows. Das ist ein virtueller Netzwerkadapter. Dieser Adapter erhält nach erfolgreichem Connect eine IP-Adresse aus dem IP-Pool, der im TELE-PROF-II-OpenVPN-Server konfiguriert wurde.

Haben Sie am TELE-PROF-II-Gerät den „Routermode“ eingeschaltet, so wird Ihnen automatisch zu diesem Ethernet-IP-Netzwerk des TELE-PROF-II die entsprechende Route gesetzt.

Beispiel:

IP-Pool: 10.111.111.0

IP-Pool-Mask: 255.255.255.0

Ethernet-IP des TELE-PROF-II: 192.168.100.1

Ethernet-IP-Maske: 255.255.255.0

IP-Adresse Ihres PC: 192.168.1.1

Zugewiesene Adresse Ihres TAP-Adapters: 10.111.111.16

Nach Verbindungsaufbau werden alle IP-Pakete die ins Netz 10.111.111.0 und ins Netz 192.168.100.0 geschickt werden über die IP-Adresse 10.111.111.16 des TAP-Adapters geroutet. Nach einem Disconnect wird diese Route automatisch entfernt.

Betrieb von WinTELEPROF über VPN

Bitte so vorgehen:

1. VPN-Verbindung herstellen
2. im IP-Adressbuch einen Eintrag auf die erste IP-Adresse des IP-Pools des Ziel-TELE-PROF-II (z.B: 10.111.111.1) oder auf die Ethernet IP-Adresse des Ziel-TELE-PROF-II (im Beispiel: 192.168.100.1) erzeugen und Verbindung aufnehmen

Wichtiges zum Betrieb

Das als Server betriebene Gerät (es wird von Ihnen angewählt!) muß auf jeden fall über eine feste IP-Adresse ansprechbar sein.

Dazu ist folgendes zu beachten:

1.) Wenn Sie am Anschluß (Router) des TP-II keine feste IP-Adresse besitzen, dann bringt es nichts, wenn Sie sich bei DynDNS mit dem TP-II anmelden. Denn Ihr Gerät meldet sich dann bei DynDNS mit der momentanen IP-Adresse des Routers an und dann kann es passieren, daß Sie keine Verbindung zu dem Gerät bekommen. Denn wenn sich die Router-Adresse geändert hat, ist das Gerät bzgl. DynDNS nicht mehr auffindbar!

Dann müssen Sie Ihren Router so parametrieren, da er sich selbst bei DynDNS anmeldet und Sie dadurch über den Anlagenname immer den Router erreichen und somit das Gerät.

2.) Wenn sie hingegen eine feste IP-Adresse besitzen, dann benötigen Sie für die Kopplung/Kommunikation keinen Eintrag bei DynDNS, wobei Sie den gerne machen dürfen. Der Zugriff erfolgt dann über diese feste IP-Adresse.



Was auf jeden Fall immer gemacht werden muß ist, daß der Router bzgl. dem Port von OpenVPN auf das dahinterliegende TP-II verweist. Das heißt, in unserem Beispiel wird der Port 1194 für die OpenVPN-Kommunikation verwendet. Somit muß jetzt der Router wissen, daß er bei **UDP**-Zugriffen auf den **Port 1194** automatisch an das TP-II weiterleitet und dessen Rückantworten wiederum über den Port 1194 abwickelt.