PocketPC.ch

Deine Windows Mobile Community

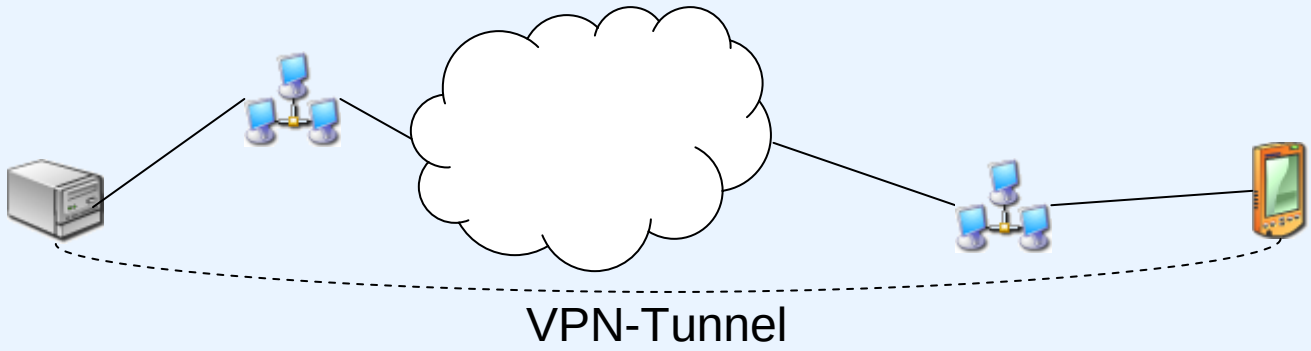
Virtual Private Network (VPN)

Yves Jeanrenaud

yjeanrenaud, pocketpc.ch

VPN-Grundlagen

- Geräte aus einem Netz in ein anderes, inkompatibles, Netz einbinden:



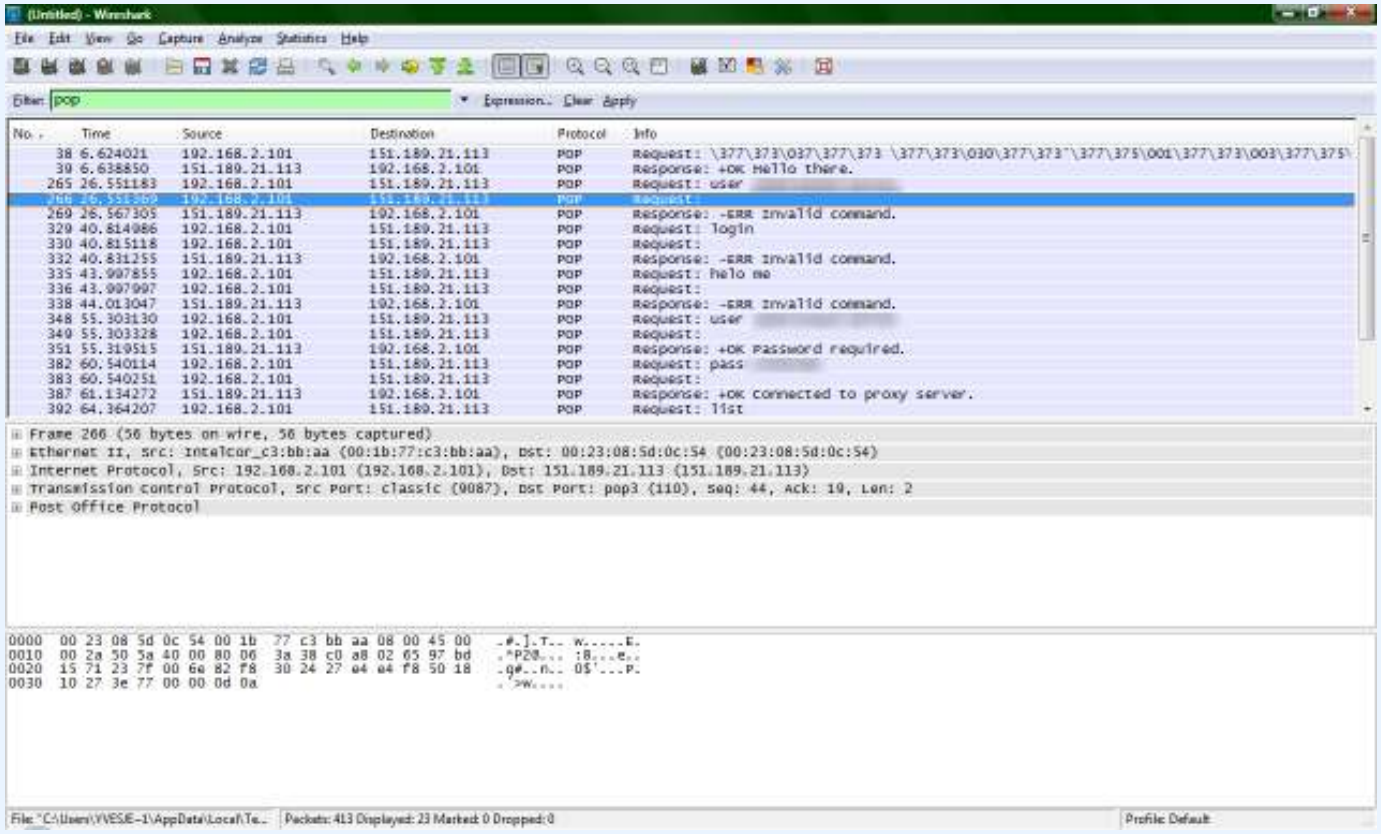
- Verschiedene Subnetze / Topologien / Protokolle
- Verschiedene Standorte
- Sicherheit (Verschlüsselung, Zugang)

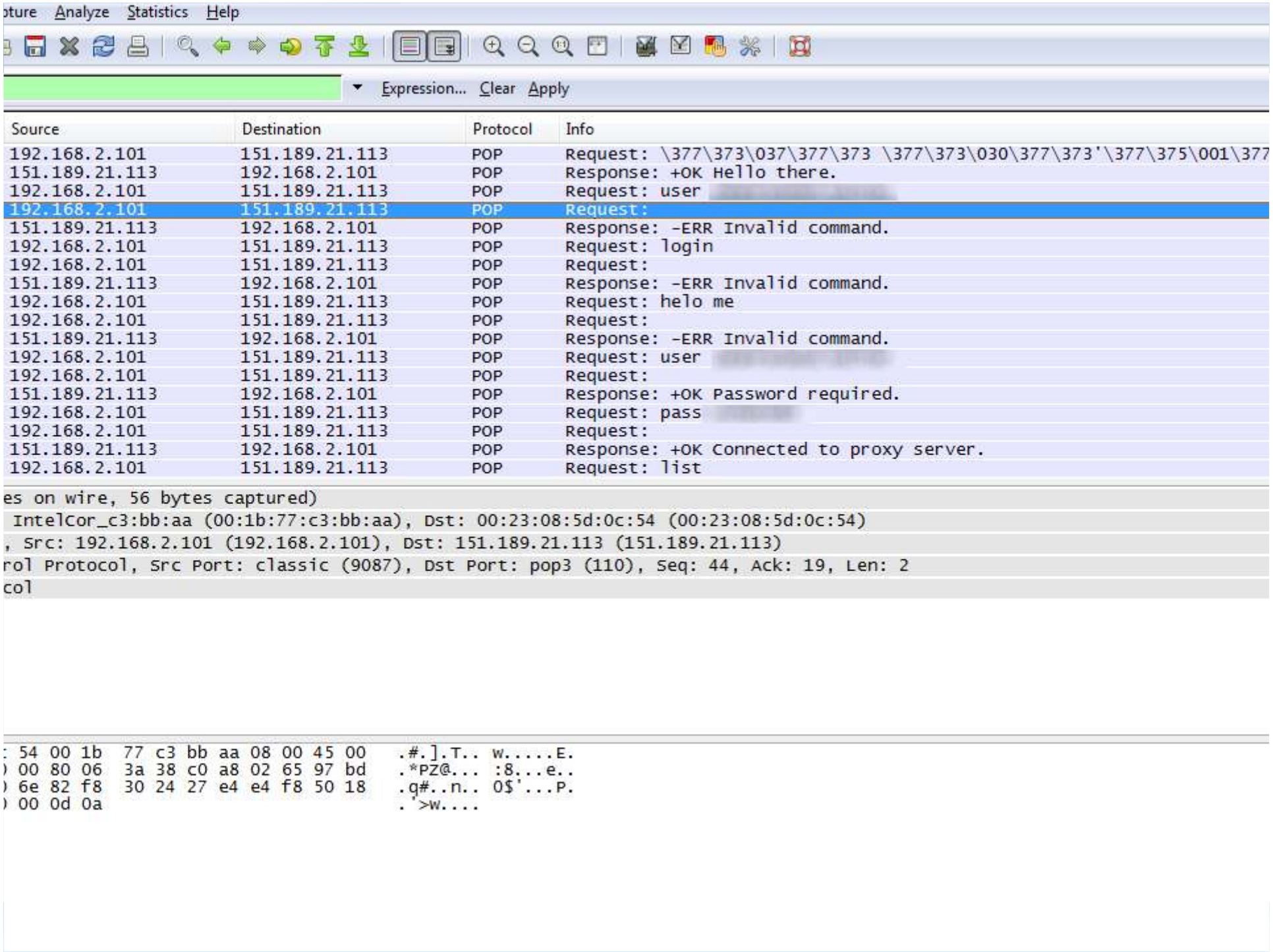
VPN-Grundlagen – Wozu?

- Anwendungsbeispiele:
  - Internetzugang an vielen Unis: WLAN unverschlüsselt, Authentifizierung **und** Verschlüsselung via VPN
  - Zugang zum Firmen-Netzwerk von Unterwegs/Zuhause
  - Sichern **aller** übertragener Daten (Passwörter!) in einem public Hotspot

VPN-Grundlagen – Wozu?

- Daten verschlüssen. Warum?



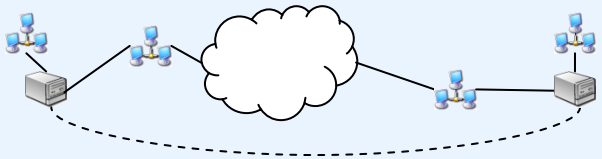

ture Analyze Statistics Help
Expression... Clear Apply
Source Destination Protocol Info
192.168.2.101 151.189.21.113 POP Request: \377\373\037\377\373 \377\373\030\377\373'\377\375\001\377
151.189.21.113 192.168.2.101 POP Response: +OK Hello there.
192.168.2.101 151.189.21.113 POP Request: user
192.168.2.101 151.189.21.113 POP Request:
151.189.21.113 192.168.2.101 POP Response: -ERR Invalid command.
192.168.2.101 151.189.21.113 POP Request: login
192.168.2.101 151.189.21.113 POP Request:
151.189.21.113 192.168.2.101 POP Response: -ERR Invalid command.
192.168.2.101 151.189.21.113 POP Request: helo me
192.168.2.101 151.189.21.113 POP Request:
151.189.21.113 192.168.2.101 POP Response: -ERR Invalid command.
192.168.2.101 151.189.21.113 POP Request: user
192.168.2.101 151.189.21.113 POP Request:
151.189.21.113 192.168.2.101 POP Response: +OK Password required.
192.168.2.101 151.189.21.113 POP Request: pass
192.168.2.101 151.189.21.113 POP Request:
151.189.21.113 192.168.2.101 POP Response: +OK Connected to proxy server.
192.168.2.101 151.189.21.113 POP Request: list
es on wire, 56 bytes captured)
IntelCor_c3:bb:aa (00:1b:77:c3:bb:aa), Dst: 00:23:08:5d:0c:54 (00:23:08:5d:0c:54)
, Src: 192.168.2.101 (192.168.2.101), Dst: 151.189.21.113 (151.189.21.113)
rol Protocol, Src Port: classic (9087), Dst Port: pop3 (110), Seq: 44, Ack: 19, Len: 2
col
: 54 00 1b 77 c3 bb aa 08 00 45 00 .#.].T.. w.....E.
) 00 80 06 3a 38 c0 a8 02 65 97 bd .*PZ@... :8...e..
) 6e 82 f8 30 24 27 e4 e4 f8 50 18 .q#..n.. 0$'...P.
) 00 0d 0a .'>w....

VPN-Grundlagen

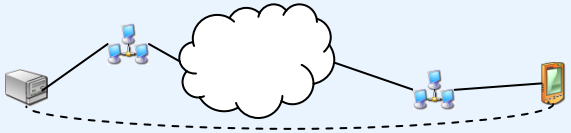
- OSI Layer 2 → mehrere Protokolle (OSI 4/5) parallel benutzbar

	OSI-Schicht	Einordnung	DoD-Schicht	Einordnung	Protokollbeispiel	Einheiten	Kopplungselemente
7	Anwendung (Application)	Anwendungs-orientiert	Anwendung	Ende zu Ende (Multihop)	HTTP FTP HTTPS SMTP LDAP NCP	Daten	Gateway, Content-Switch, Layer 4-7 Switch
6	Darstellung (Presentation)						
5	Sitzung (Session)						
4	Transport (Transport)	Transport-orientiert	Transport		TCP UDP SCTP SPX	Segmente	
3	Vermittlung (Network)		Internet	Punkt zu Punkt	ICMP IGMP IP IPX	Pakete	Router, Layer-3-Switch
2	Sicherung (Data Link)		Netzzugang		Ethernet Token Ring FDDI ARCNET	Rahmen (Frames)	Bridge, Switch
1	Bitübertragung (Physical)					Bits	Hub, Repeater

- Site-to-site:



- End-to-end:



- VPN ist ein reines Softwareprodukt
  Softwareunterstützung erforderlich

VPN Software auf Windows Mobile

1. PPTP (Point-to-Point Tunneling Protocol)

2. IPsec/L2TP (Internet Protocol Security/Layer-2-Tunneling-Protocol)

3. Drittanbieter, z.B. OpenVPN

VPN Software auf Windows Mobile

1. PPTP (Point-to-Point Tunneling Protocol)
   - 1996 implementiert durch ein Software-Konsortium (Microsoft, Ascend, 3Com, Cisco, etc.)
   - Vorinstalliert auf WM, WinXP, Vista, Win2003 etc. und vielen Linux-Distributionen
   - Vergleichsweise einfache Konfiguration der Software
   - Kryptoanalyse (Schneier) zeigt Sicherheitsprobleme in alten MS-Implementierungen und direkte Korrelation mit der Passwortlänge
   - Gratis

VPN Software auf Windows Mobile

2. IPsec/L2TP (Internet Protocol Security/Layer-2-Tunneling-Protocol)
   - 1998, kommerzielle Entwicklung von BBN
   - L2TP ist die Weiterentwicklung von PPTP
   - L2TP ist unverschlüsselt, stellt nur den Tunnel her
   - Reines IPsec kann auch zum Tunneln, aber nicht auf Windows ohne Drittsoftware (Cisco)
   - IPsec ist OSI Layer 3, also nicht protokollunabhängig
   - Derzeit höchste IP-Sicherheit
   - Erfordert zusätzliche, kostenpflichtige Software auf der Serverseite (ausser auf Linux z.B. OpenSwan, aber komplex einzurichten)

VPN Software auf Windows Mobile

3. Drittanbieter, z.B. OpenVPN
   - OpenSource (GNU GPL)
   - Entwickelt seit 2002 durch die OpenVPN Solutions LLC
   - OpenVPN for PocketPC ist derzeit alpha (1.4.2007)
   - Software muss auf beiden Seiten installiert werden
   - Konfiguration nicht ganz so simpel
   - Gratis
   - Plattformunabhängig

PPTP

I. Server auf Windows (z.B. Vista)
(analog auf XPpro, ME, Vista, 2003 Server etc.)

II. (Firewall konfigurieren)

III. Client auf Windows Mobile 6
(analog auf WM5)

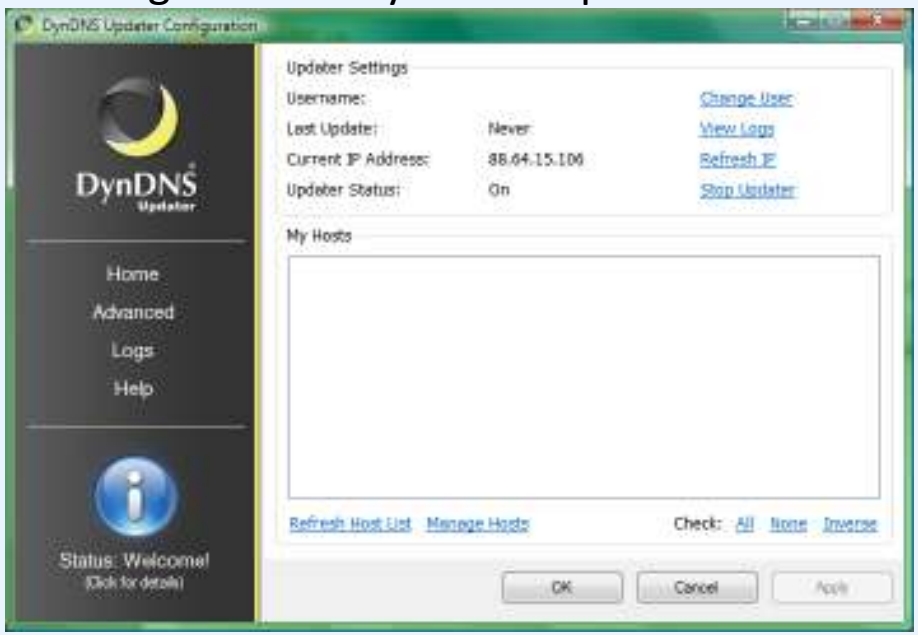
I. PPTP – Server auf Vista

Voraussetzung: Server muss via Internet erreichbar sein.

→DDNS-Account oder fixe IP:

Dynamische IP-Vergabe → DynDNS löst diesen auf einen global erreichbaren Namen auf.

z.B. www.dyndns.com Account gratis und DynDNS® Updater for Windows 4.0.8 Software für Windows:



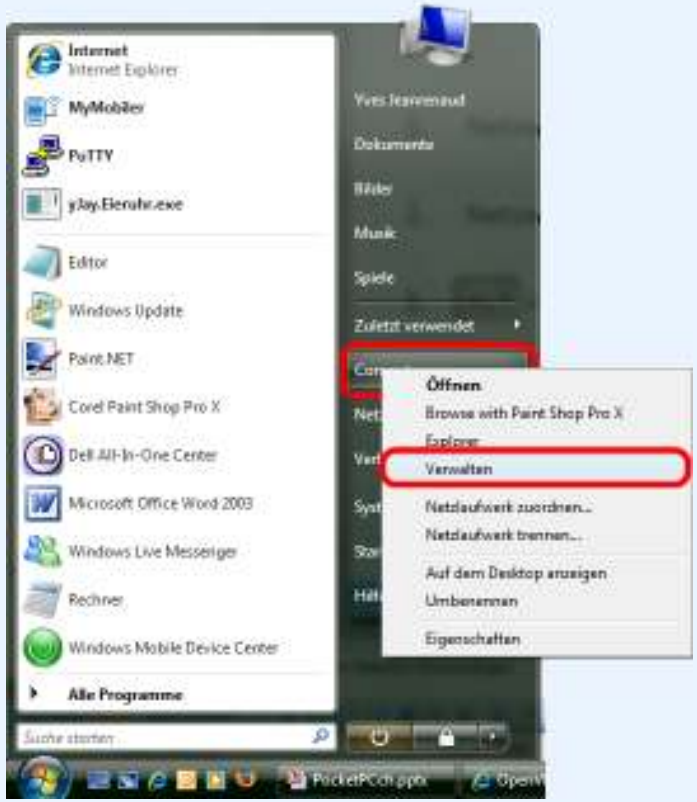
I. PPTP – Server auf Vista

1. *[optional]* Benutzerkonto/en einrichten:

   Start>Benutzerkonten>
   Anderes Konto verwalten>
   Neues Konto erstellen

WICHTIG: *Sicheres* Passwort

und > 12 Zeichen

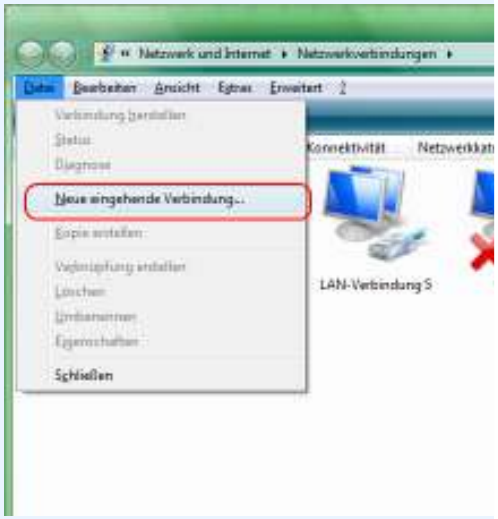


(natürlich immer die Aktionen im Rahmen der Benutzerkontensteuerung bestätigen)

Für Vista Business auch
über Computer
(8 Rechtsklick)> Verwalten>Lokale Benutzer und Gruppen

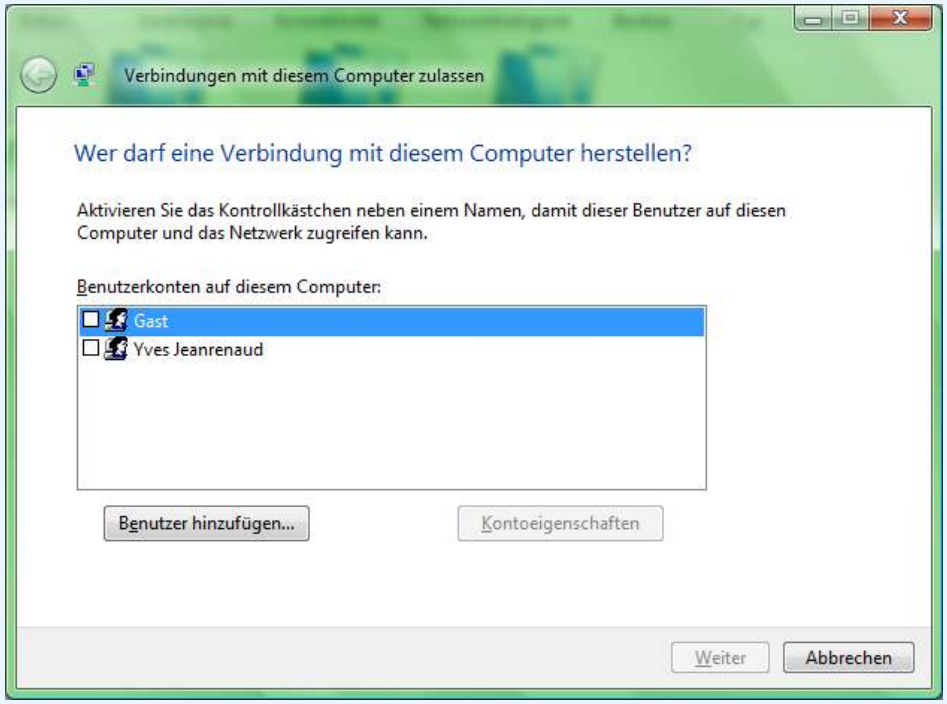
I. PPTP – Server auf Vista

1. Netzwerk und Freigabecenter
2. Netzwerkverbindungen verwalten
3. ALT >Datei>Neue eingehende Verbindung…



I. PPTP – Server auf Vista

4. Zugelassene Benutzer auswählen oder Benutzer hinzufügen (auch auf Vista Home), Weiter

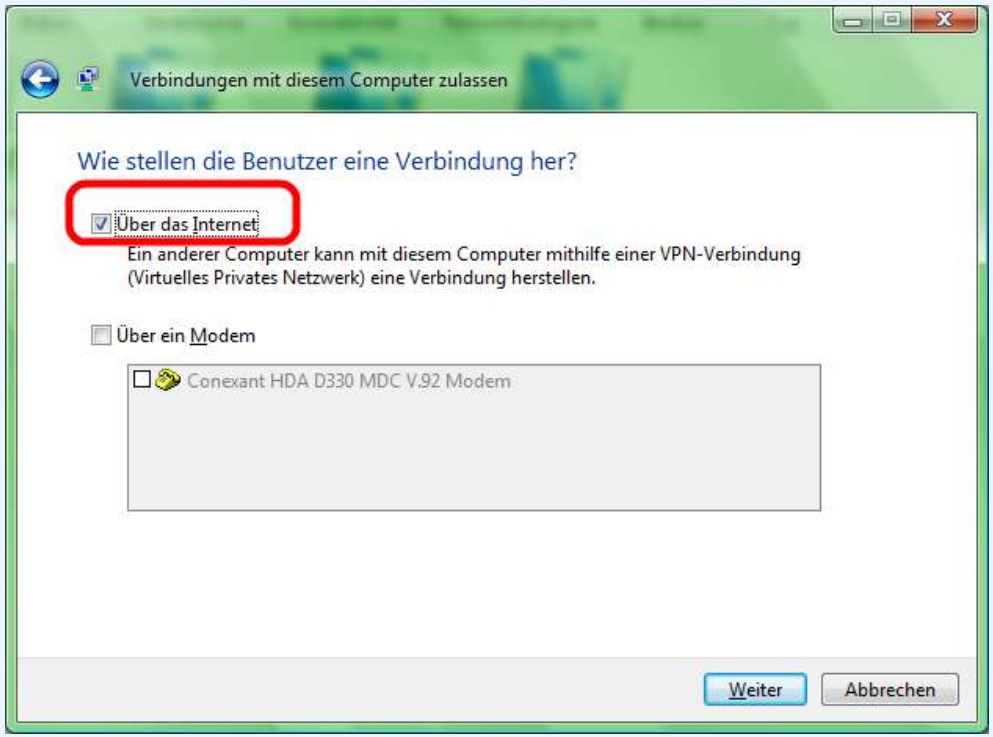


Empfehlung: neuen, dezidierten Benutzernamen für VPN anlegen

WICHTIG: *Sicheres* Passwort und > 12 Zeichen

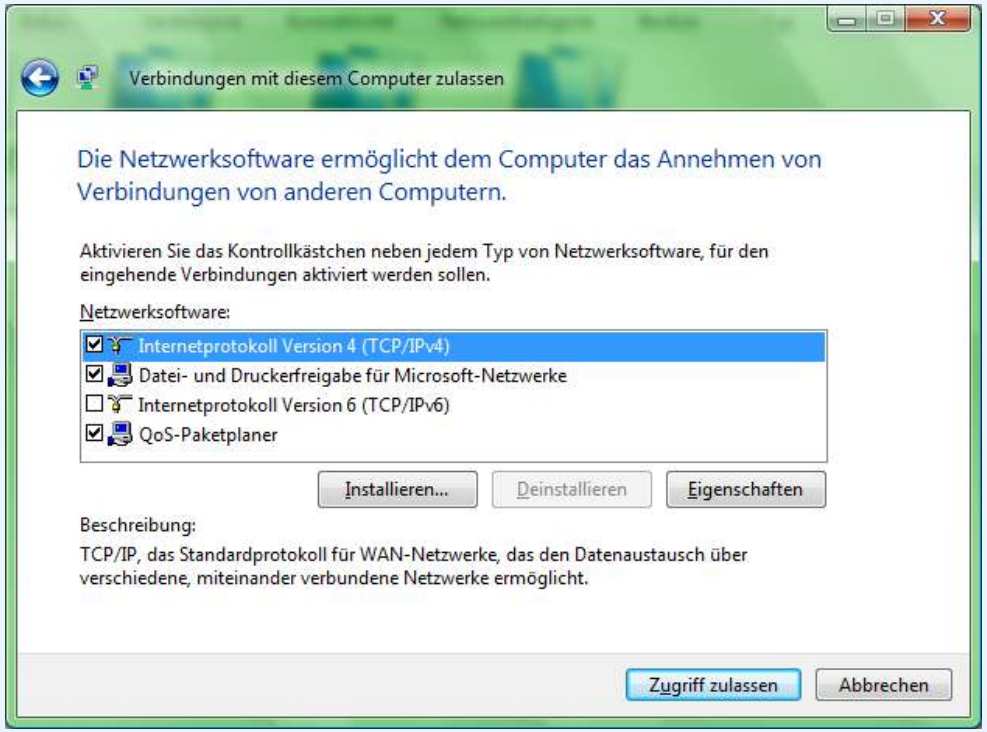
I. PPTP – Server auf Vista

5. Über das Internet, Weiter



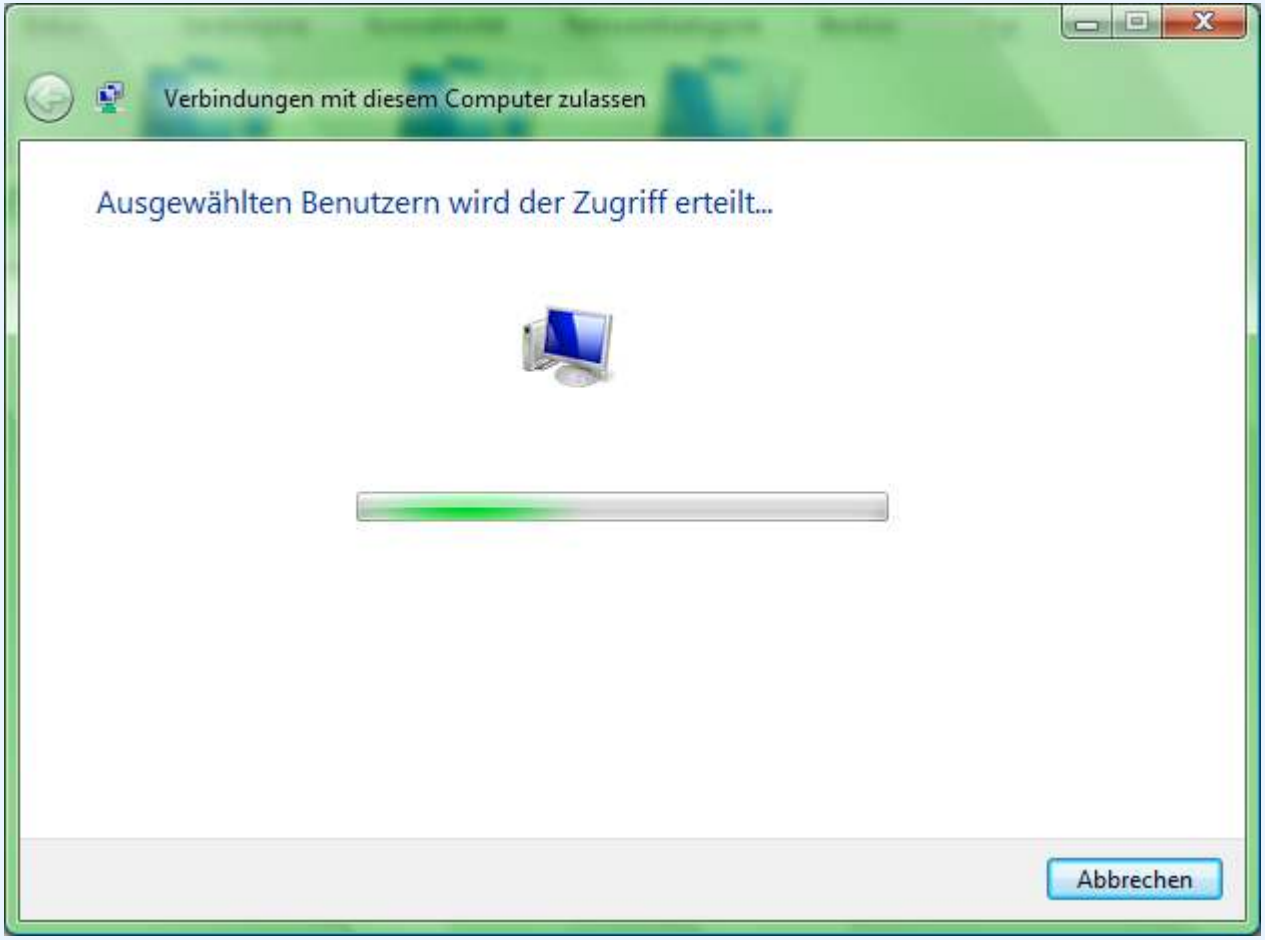
I. PPTP – Server auf Vista

6. Protokolle und Dienste auswählen, Zugriff zulassen



I. PPTP – Server auf Vista

7. Warten

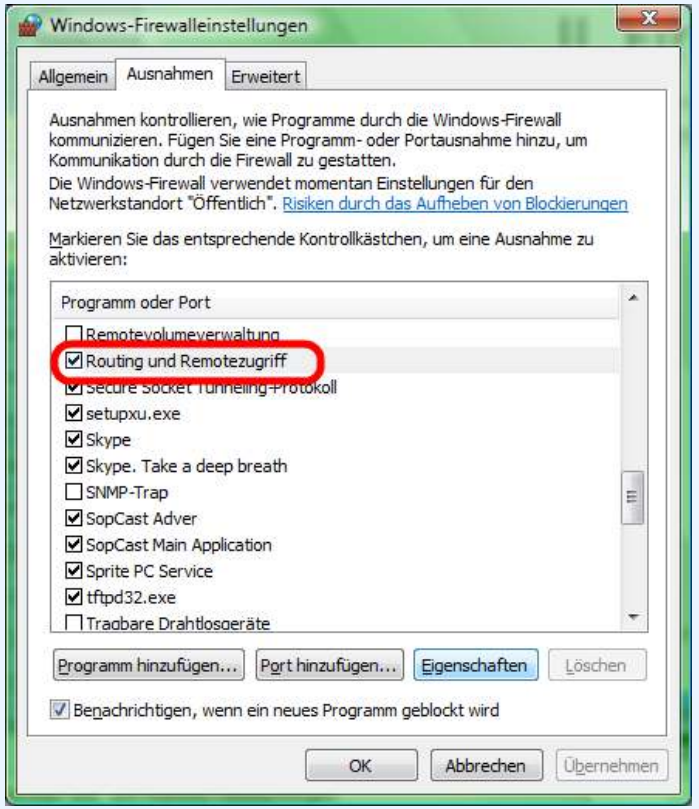


(II. Firewall)

1. Windows-Firewall wird automatisch konfiguriert:

2. Konfiguration für den Router:
   TCP Port 1723 und das
   Generic Routing
   Encapsulation-Protokoll (GRE) 47

   (meistens ist GRE nicht explizit aktivierbar, sondern eine Option namens VPN-Passthrough zu finden)



II. Client auf Windows Mobile 6

Voraussetzung: (Internetverbindung per 3G oder WLAN einrichten und testen)

1. Einstellungen>Verbindungen> Verbin-dungen

II. Client auf Windows Mobile 6

2. Nur bei der Büroverbindung möglich: Neue VPN-Serververbindung

II. Client auf Windows Mobile 6

3. Daten eingeben:
   Name der Verbindung, Hostname (DDNS)/IP
   VPN-Typ: PPTP

4. Weiter

II. Client auf Windows Mobile 6

5. Benutzerdaten eingeben:
   Benutzername und (optional) Kennwort wie bei der Einrichtung angegeben.
6. Als Domäne den Rechnernamen (z.B. GreenDay)

7. (Erweitert… ist nur zur Konfiguration der IP-Vergabe und der Header-Komprimierung, kann meistens auf Standardeinstellungen belassen werden)

8. Fertig

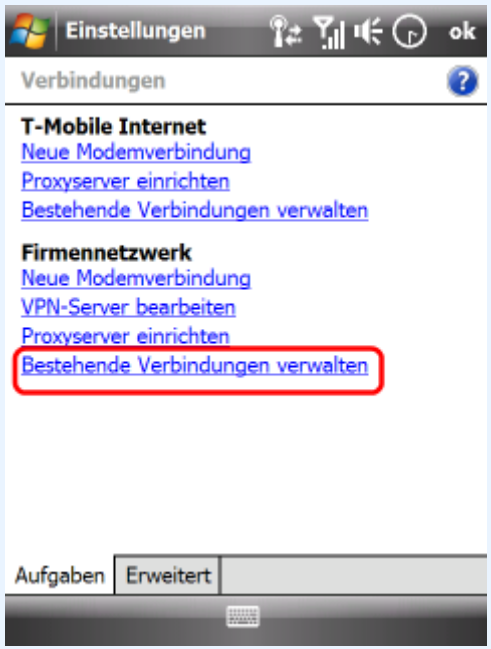
II. Client auf WM6 - Testen

9. Testen:

   Gerät in einem anderen Netz (zB. 3G), sonst Kollisionen

   (2 IPs des selben (Sub-) Netzes auf dem gleichem Gerät)

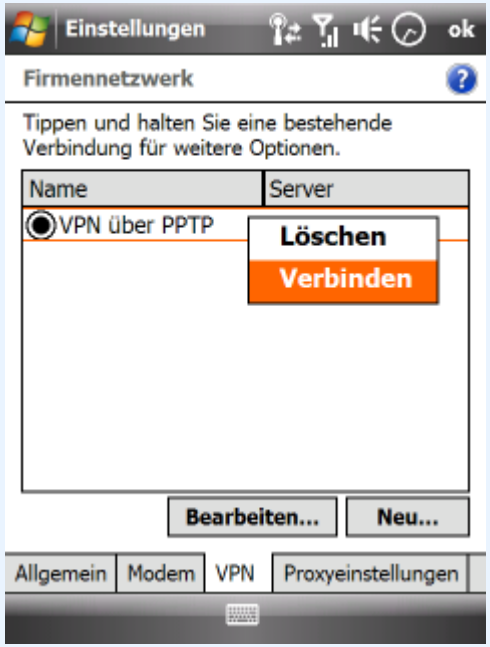
10. Bestehende Verbindungen verwalten



II. Client auf WM6 - Testen

11. VPN, Langes Antippen der soeben eingerichteten Verbindung>Verbinden

(ev. Kennwort eingeben, wenn zuvor nicht gespeichert)

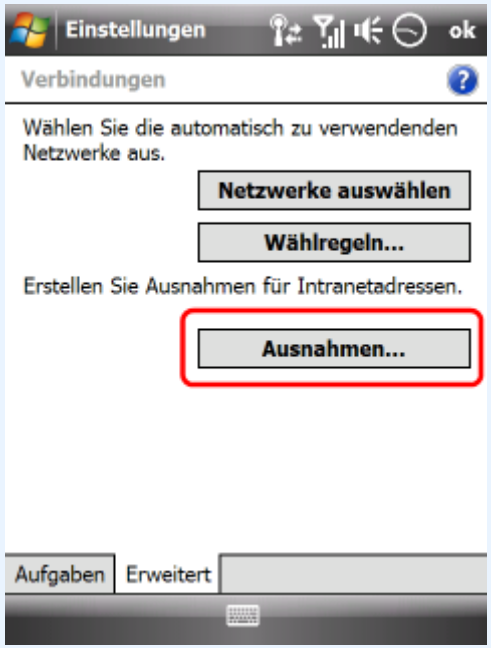


II. Client auf WM6 - Testen

12. Konnektivität prüfen

II. Client auf WM6 - Optional

13. (Optional) Ausnahme für die automatische Einwahl: Verbin-dungen>Erweitert>Ausnahmen…
14. Neuer URL… (sic)



II. Client auf WM6 - Optional

15. URL angeben und OK

II. Client auf WM6 - Trennen

16. Trennen

PocketPC.ch
Deine Windows Mobile Community

Vielen Dank für die Aufmerksamkeit

Yves Jeanrenaud
yjeanrenaud, pocketpc.ch