Einrichtung einer Informatik-VPN-Verbindung mit Ubuntu-Linux

Verbinden Sie sich unter Ubuntu (13.04, unity-Desktop) über den "*NetworkManager*" mit dem unverschlüsselten WLAN *"UHH*" (oder alternativ *"eduroam*"):



Wählen Sie im "*NetworkManager*"-Menü den Punkt *"VPN-Verbindungen*" und dort im erscheinenden Kontext-Menü den Punkt *"VPN konfigurieren*":



Wählen Sie im Dialog "Netzwerkverbindungen" direkt "*Hinzufügen*", um einen neue VPN-Verbindung einzurichten, es erscheint eine Auswahl von möglichen Verbindungstypen, wählen Sie hier "*VPN – Point to Point Tunneling Protokol (PPTP*)":



In der erscheinenden Dialog-Box setzen Sie anschließend die Werte für

- 1.
- Einen sinnvollen Verbindungsnamen (z.B. *"Informatik-VPN*"), Die VPN-Server Zieladresse **"fbivpn.informatik.uni-hamburg.de**", Ihren Informatik-Anmeldenamen und das Kennwort, 2. 3.
- Sowie den Domänennamen "INFORMATIK" und wählen Sie abschließend 4.
- 5. den Auswahlpunkt "Erweitert" für die notwendige Schlüsselkonfiguration

Netzwerkverbindungen			De	(i;	* 🖂	K	◄)))	10:49	\$₽
٠									
	Se Informat	ik-VPN bearbeiten	1						
	Verbindungsname:	Informatik-VPN	1.						
	Allgemein VPN	IPv4-Einstellungen							
	Allgemein								
	Gateway: fbiv	pn.informatik.uni-hamburg.de 🧹	2.)					
				1.0					
	Optional								
	Benutzername:	1musterm							
	Passwort:	rspeichert	•						
1		Passwort zeigen							
	NT-Domäne:	INFORMATIK 4.) 5.)							
		🔀 Erweitert							
	(Burnethause)								
	Exportieren	Abbrechen Speicher	n						
		CONTRACTOR OF THE OWNER							

Für die Verbindungsaushandlung zum VPN-Server sind die entsprechend notwendigen Parameter anzupassen.

- deaktivieren Sie dafür alle Authentifizierungsmethoden bis auf "MSCHAPv2", 1.
- aktivieren Sie *"MPPE Verschlüsselung verwenden*", stellen Sie die Verschlüsselung auf *"128-Bit*" 2.
- 3.

Netzwerkverbindungen	De	((;	*	\bowtie	4))	10:50	ψ
Erweiterte PPTP-Optionen							
Verbin Die folgenden Methoden zur Legitimierung erlauben:							
Allae							
	1						
Mig Mischap	_						
1.) 🗹 MSCHAPv2							
Be Sicherheit und Komprimierung							
2.) 🖉 Point-to-Point Verschlüsselung (MPPE) verwenden	n I						
Sicherheit 128-Bit (am sichersten) - 3.)							
Stateful-Verschlüsselung erlauben							
BSD-Datenkomprimierung erlauben							
🖉 Deflate-Datenkomprimierung erlauben 🗤							
🔗 TCP-Header-Komprimierung verwenden	_						
Expo Echo]						
	-						
Abbrechen OK							

 ${\tt Best\" atigen Sie mit "OK", die VPN-Verbindung ist jetzt eingerichtet und kann genutzt werden.}$

