Autor: Benjamin Wagner linux@ben-wagner.de

Dieses Dokument beschreibt kurz, wie man unter Debian Linux einen VPN-Zugang einrichtet. Im Gegensatz zu OpenVPN wird hier nicht mit Rechnerzertifikaten die Userauthentifizierung durchgeführt, sondern rein über Benutzername und Kennwort. Über diesen Zugang können sich andere Rechner aus dem Internet mit der Maschine verbinden. So können dienste wie http, CIFS oder ftp genutzt werden, ohne dass dies explizit über die Firewall des Servers freigegeben werden muss.

Hinweis:

Dieses Dokument ist gültig für Debian Sarge 3.1.

Als Testrechner diente ein Pentium3 500Mhz als Server mit 256 MB RAM. Als Kernel läuft Kernel 2.6.8-3-686, die interne IP-Adresse ist 192.168.10.11. Der Server hängt hinter einem Netgear Router. Der Router ist über dyndns im Internet erreichbar.

Als Client diente ein Windows XP Pro SP2, das über Internet mit dem Rechner verbunden sein sollte.

Installation von PPTP

Mit dem Befehl "apt-get install pptpd" wird der PPTP-Dienst installiert.

Anschließend müssen folgende Dateien editiert werden:

/etc/pptp.conf

Hier werden die IP-Adresse des lokalen VPN-Devices sowie der Nummernpool der Clients definiert:

localip 192.168.10.20 remoteip 192.168.10.30-40

/etc/ppp/pptp-options

refuse-pap refuse-chap refuse-mschap # Require the peer to authenticate itself using MS-CHAPv2 [Microsoft # Challenge Handshake Authentication Protocol, Version 2] authentication. Require-mschap-v2 # Require MPPE 128-bit encryption # (note that MPPE requires the use of MSCHAP-V2 during authentication) require-mppe-128 # }} nobsdcomp auth name pptpgate #(pptpgate ist hier der Name des VPN-Servers)

/etc/ppp/chap-secrets

#Benutzername	VPN-Serve	rdienst	Passwort	IP-Adresse
z.B. VPN-USER1	pptpgate	VPN-	PASSWORT1	192.168.10.31

Kernelanpassung

Anschließend muss sichergestellt sein, dass der aktuelle Kernel mppe (MPPE Encryption) unterstützt. Dies ist bei allen Kernel ab 2.6.17 der Fall. Falls der eigene Kernel älter ist, muss der Kernel neu kompiliert werden.

Dazu werden die aktuellen Kernelsourcen von <u>www.kernel.org</u> heruntergeladen, und im Verzeichnis /usr/src/ entpackt:

cd /usr/src wget <u>http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.18.tar.bz2</u> bunzip2 -c linux-2.6.18.tar.bz2 | tar x ln -s linux2.6.18 linux

Nun wird der Kernel neu kompiliert. Dazu werden die Settings des aktuellen Kernel als Grundlage genommen. Hierdurch ist sichergestellt, dass der neue Kernel die gleichen Features hat wie der gerade laufende.

cp /boot/config-2.6.8-3-686 /usr/src/linux/.config

Als nächstes startet man das Tool menuconfig, mit dem man die Kernelparameter konfigurieren kann.

cd /usr/src/linux make menuconfig

Unter dem Punkt **"Device Drivers" - "Network Device Support" - "PPP" den Punkt PPP MPPe Compression"** aktivieren.

Mit "exit" das Programm beenden, und die Konfiguration abspeichern. In der Datei /etc/kernel-pkg.conf kann man nun diverse Parameter ändern, z.B: die eigene eMailadresse und den Revisionsstand des Kernels. Dies sollte man machen, damit man den eigenen Kernel leichter von offiziellen Debian-Kerneln unterscheiden kann. Mit dem Befehl

make-kpkg kernel_image --initrd -revision=mppe1.0

startet man dann das Kompilieren des neuen Kernels. Dies kann je nach der verfügbaren Rechenpower zwischen mehreren Minuten und mehreren Stunden dauern. Anschließend wird das fertige Paket als kernel-image-2.6.18_mppe1.0_i386.deb im Ordner /usr/src abgespeichert. Mit dem Befehl

dpkg -i kernel-image-2.6.18_mppe1.0_i386.deb

wird der Kernel installiert, und als Defaultkernel eingerichtet. Nun wird der Rechner mit shutdown -r now neu gestartet.

Konfiguration der Windows XP-Clients

Unter Windows XP muss nun eine VPN-Verbindung eingerichtet werden. In der Systemsteuerung findet man dazu unter "Systemsteuerung" - "Netzwerkverbindungen" einen Assistenten: "neue Verbindung erstellen". Als Typ wählt man "Verbindung mit dem Netzwerk am

eneral Options Security Networking Advanced Dialing options Display progress while connecting Prompt for name and password, certificate, etc. Include Windows logon domain Redialing options Bedial attempts: 3 1 Time between redial attempts: 1 minute 1 Idle time before hanging up: never 1 Redial if line is dropped OK Cance optiplex.homedns.org Properties 0 0 Security options Otions 4 Validate my identity as follows: Require secured password 1 Automatically use my Windows logon name and password (and domain if any) I and domain if any) I action these settings Using these settings requires a knowledge of security protocols. Settings Settings	op				
Dialing options Display progress while connecting Prompt for name and password, certificate, etc. Include Windows logon domain Redialing options Redial attempts: Itime between redial attempts: Itime between redi	neral Option	s Security	Networking	Advanced	
Redialing options Bedial attempts: Image: Security Networking Advanced Security options Typical (recommended settings) Validate my identity as follows: Require secured password Automatically use my Windows logon name and password (and domain if any) Require data encryption (disconnect if none) Advanced (custom settings) Using these settings requires e knowledge: Security protocols. Security protocols. Require Security Security Security	Dialing option Display p Display p Prompt fo	is rogress while co or name and pas Vindows locion (onnecting ssword, certific domain	ate, etc.	
Redial attempts: 3 Time between redial attempts: 1 minute Idle time before hanging up: never Redial if line is dropped OK Cance optiplex.homedns.org Properties neral Options Security Networking Advanced Security options Typical (recommended settings) Validate my identity as follows: Require secured password Automatically use my Windows logon name and password (and domain if any) Require data encryption (disconnect if none) Advanced (custom settings) Using these settings requires a knowledge Settings	Bedialing opti	ions			
Image:	Redial attem	nts:	3		•
Idle time before hanging up: Redial if line is dropped OK Cance optiplex.homedns.org Properties meral Options Security Networking Advanced Security options Typical (recommended settings) Validate my identity as follows: Require secured password Automatically use my Windows logon name and password (and domain if any) Require data encryption (disconnect if none) Advanced (custom settings) Using these settings requires a knowledge of security protocols.	Time betwee	en redial attempt	·s· 1	minute	
Image: Control of the instrument of	Idle time bef	ve banging up:		ever	•
OK Cancel optiplex.homedns.org Properties Image: Conceleration of the security is a conceleration of the security is a conceleration of the security is a conceleration of the security as follows: Image: Conceleration of the security is a conceleration of the security of the secure of		bie nanging up.		0101	
Image: Provide and Control of Security Protocols Networking Advanced Security options Image: Provide and Control of Security as follows: Image: Provide and Control of Security as follows: Image: Provide and Control of Security Protocols Image: Provide and Control of Security Protocols Image: Provide and Control of Security Protocols Image: Provide and Provide and Provide and Control of Security Protocols Image: Provide and P				ok (Cance
 Security options Typical (recommended settings) Validate my identity as follows: Require secured password Automatically use my Windows logon name and password (and domain if any) Require data encryption (disconnect if none) Advanced (custom settings) Using these settings requires a knowledge settings 	ор	tiple×.homedr	ns.org Prope	DK C	Cance
 Automatically use my Windows logon name and password (and domain if any) Require data encryption (disconnect if none) Advanced (custom settings) Using these settings requires a knowledge of security protocols. 	op neral Optior	tiplex.homedr ₁₈ Security	ns.org Prope Networking	DK rties Advanced	Cance
Require secured password Automatically use my Windows logon name and password (and domain if any) Require data encryption (disconnect if none) Advanced (custom settings) Using these settings requires a knowledge of security protocols.	op neral Option Security option	tiplex.homedr ₁₅ Security ns	ns.org Prope Networking	DK rties Advanced	Cance
 Automatically use my Windows logon name and password (and domain if any) Require data encryption (disconnect if none) Advanced (custom settings) Using these settings requires a knowledge Settings 	op neral Optior Security optio OTypical (re Validate r	tiplex.homedr ns Security ns ecommended se ny identity as fol	Networking ttings)	DK rties Advanced	Cance
 Require data encryption (disconnect if none) Advanced (custom settings) Using these settings requires a knowledge <u>Settings</u>) 	op neral Option Security option OTypical (re Validate r Require	tiplex.homedr ns Security ns ecommended se ny identity as fol secured passwo	Networking ttings) lows:	DK rties Advanced	Cance
O Advanced (custom settings) Using these settings requires a knowledge <u>Settings</u>)	op neral Optior Security optio OTypical (re Validate r Require Auton passw	tiplex.homedr ns Security ns ecommended se ny identity as fol secured passwo natically use my vord (and domai	Networking Networking (lows: ord Windows logo n if any)	on name and	Cance
Using these settings requires a knowledge <u>Settings</u>)	op neral Option Security option Validate r Require Auton passw	tiplex.homedr ns Security ns ecommended se ny identity as fol secured passwo natically use my vord (and domai ire data encrypti	Networking Networking Ittings) Iows: ord Windows logo n if any)	on name and et if none)	Cance
	op neral Option Security option Validate r Require Auton passw M Requi	tiplex.homedr ns Security ns ecommended se ny identity as fol secured passwo natically use my vord (and domai ire data encrypti d (custom setting	Networking Networking Ittings) Ilows: ord Windows logo n if any) ion (disconneo	on name and et if none)	Cance
(IPSec Settings)	op neral Option Security option Validate r Require Auton passw M Requi Requi	tiplex.homedr ns Security ns ecommended se ny identity as fol secured passwo vord (and domai ire data encrypti d (custom setting se settings requ y protocols.	ns.org Prope Networking (ttings) lows: ord Windows logo n if any) ion (disconneo gs) ifres a knowle	on name and at if none)	Cance

Arbeitzplatz herstellen". Anschließend wählt man "VPN-Verbindung". Als Firmenname gibt man nun einen Aussagekräftigen Namen ein. Anschließend wird der Name bzw. die IP-Adresse des Rechners angegeben, mit dem man eine VPN-Verbindung aufnehmen möchte. Es empfiehlt sich, dass dieser Server entweder über eine statische IP oder bei einer Wahlleitung ins Internet über einen DYNDNS-Account erreichbar ist. Falls der Server hinter einem Router hängt, muss der Port 1723 weitergeleitet werden. Abschließend kann noch angegeben werden, für wen die neue Verbindung erreichbar ist.

Es startet nun das Eingabefenster für Benutzernamen und Passwort. Hier klickt man auf "Eigenschaften". Hier werden folgende Einstellungen laut der beigefügten Screenshots eingetragen:

Achtung: Bei den Eigenschaften des TCP/IP-Protokolls muss der Haken "Standardgateway für das Remotenetzwerk verwenden" deaktiviert werden, da ansonsten die VPN-Verbindung als Defaultgateway eingetragen wird.

Beim ersten Aufruf muss nun ein Benutzername und ein Kennwort eingetragen werden, hier wird der in der Datei /etc/ppp/chap-secrets eingetragene Benutzer verwendet. Pro VPN-Verbindung kann hier jeweils ein User verwendet werden.

Viel Erfolg beim austesten!

	optip	lex.homed	ns.org Prope	rties	0
∋eneral	Options	Security	Networking	Advanced	
Typ <u>e</u> of	VPN:				
PPTP	VPN				•
					tings
This c <u>o</u>	nnection u	ses the follo	wing items:		
V 7	Internet Pr	otocol (TCF	VIP)		
	QoS Pack File and Pr	et Schedule inter Sharin	er g for Microsoft	Networks	
	Client for M	licrosoft Ne	- tworks		
(Ir	stall		Ininstall	Prope	rties
Descr	iption	ontrol Protos	al (Internet Pre	taaal Tha da	fourth
wide	area netwo ss diverse i	ork protocol nterconnect	that provides of that provides of	cocoi. The de communicatio	n
			0	ok (Cancel
	,	Advanced	TCP/IP Setting	gs	(
eneral	DNS V	MNS			
This che network that can	ckbox only and a dial- not be seni	v applies wh up network t on the loca	en you are cor simultaneously al network is foi	nected to a li . When chec warded to the	ocal ked, data e dial-up
	default gati	eway on rer	note network		