### **Bitte beachten:**

Diese Anleitung bezieht sich auf die im folgenden Bild dargestellte Beispielkonfiguration. Diese kann natürlich entsprechend angepasst werden und ist nur als funktionsfähiges Beispiel zu verstehen.

Dabei werden der Allnet VPN-Client v2.03 und der ALL1294VPN-Router mit installierter Firmware v1.6 Rel. 1E verwendet.

Sollten sie den Router noch auf die aktuelle Firmware updaten wollen, bitte nach dem Update unbedingt einen Reset auf Werkseinstellungen durchführen (entweder über Konfig-Menü oder Reset-Taster für 20sec drücken).



#### Vorbereitung:

1.

Auf dem PC eine funktionsfähige Internetverbindung einrichten und testen. (z.B. t-online mit direktem Modemzugang zum Internet)

### 2.

Auf dem PC den Allnet VPN-Client (z.Zt. Version 2.03) installieren und neu booten. Das Symbol des VPN-Clients erscheint dann in der Taskleiste unten rechts.



3.

Den Router ALL1294VPN für die Internetverbindung einrichten (siehe Handbuch) und diese testen.

WAN Port Con	figuration	
Identification	Hostname:	SCEF6FE0
	Domain Name:	
	WAN Port MAC Addres	s: 00c002ef6fe1
		Default Copy from PC
IP Address	IP Address is ass	igned automatically (Dynamic IP Address)
	O Specified IP Addre	ess (Static IP Address)
NAT	Enable NAT, allow	v all LAN users to share WAN IP address.
	🔘 Disable NAT, perf	orm standard routing ONLY.
DNS	<ul> <li>Automatically obta</li> </ul>	in from Server
	O Use this DNS	
Login	Login Method: PPPo	E 🔽
	Login User Name:	2220#0001@t-online.de
	Login Password:	•••••
	RAS Plan:	512k Ethernet 🔽 (SingTel RAS only)
	Server Address (Not r	equired for PPPoE, SingTel RAS)
	IP Address:	
	🔘 Domain Name:	
	Connection behavior:	Keep alive(maintain connection)
		Auto-disconnect Idle Time-out: 0 min

Nach einer erfolgreichen Verbindung ergibt sich dann folgender Internet-Status:

Status		
internet	Connection Method:	PPPoE
	Broadband Modem :	Connection OK
	Internet Connection:	Active
	Internet IP Address:	217.228.228.165
		Connection Details
LAN	IP Address:	192.168.0.1
	Network Mask:	255.255.255.0
	DHCP Server:	ON
System	Device Name:	SCEF6FE0
	Firmware Version:	Version 1.6 Release 1E
		System Data
		Restart Router Refresh Screen Help

#### 4.

Auf dem Router einen DynDNS-Zugang einrichten (dazu ggfs. vorher bei <u>www.dyndns.org</u> einen kostenlosen Hostnamen registrieren lassen). Bei erfolgreicher Einwahl ergibt sich folgendes Bild (Status: Update ok):

DDNS (Dyr	amic DNS)			
DDNS Service	Dynamic DNS allows y of an IP Address) to ac	ou to provide Internet cess your Virtual Sei	users with a doma vers.	ain name (instead
DDNS Data	User name is set when y DDNS Service: d User Name: al Password: Domain Name: r	vou register; your pass yndns V Web Si Isupp rry	word is E-mailed to te	org
			Save Ca	ncel Help

#### 5.

In den folgenden Menüpunkten die entsprechenden Einstellungen vornehmen. DNS-Adresse und MTU-Wert sind providerabhängig und müssen eventuell angepasst werden.

Das Beispiel bezieht sich auf einen t-dsl Zugang von T-Online.

Backup	Backup DNS (1) IP Address:	194 25 2 129
	Backup DNS (2) IP Address:	
	These DNS (Domain Name Servers) are	e used only if the primary DNS is unavailable.
	MTU MTU (Maximum Transmission Unit): 1	492 (11500) bytes
	This setting only affects PPPoE and PPT	P connections.
Logs		
Logs Enable Logs	✓ DoS (Denial or Service) attacks	View Log Clear Log
Logs Enable Logs	<ul> <li>DoS (Denial or Service) attacks</li> <li>Internet connections</li> </ul>	View Log Clear Log View Log Clear Log
Logs Enable Logs	<ul> <li>DoS (Denial or Service) attacks</li> <li>Internet connections</li> <li>Access Control</li> </ul>	View Log Clear Log View Log Clear Log View Log Clear Log
Logs Enable Logs	<ul> <li>DoS (Denial or Service) attacks</li> <li>Internet connections</li> <li>Access Control</li> <li>Firewall Rules</li> </ul>	View Log Clear Log View Log Clear Log View Log Clear Log View Log Clear Log

Security Option	ns	
SPI Firewall	💽 Enable DoS (D	enial of Service) Firewall
	Threshold:	● High (WAN bandwidth > 2 Mbps)
		🔘 Medium (WAN bandwidth 1 - 2 Mbps)
		○ Low (WAN bandwidth < 1 Mbps)
	If Enabled (recom affects invalid co	mended), invalid packets and connections are dropped. The "Threshold" nnections only.
Options	Respond to ICI	MP (ping) on WAN interface
	🗹 Allow IPsec	
	Allow PPTP	
	Allow L2TP	
	Allow TFTP firm	nware upgrade
		Save Cancel Help

### VPN-Einstellungen des ALL1294VPN Routers

Für einen (mobilen) VPN-Client mit dynamischer IP-Adresse folgendes Profil erstellen:

OK I	Policy Name 1]client1	Enable Remote VPN Endpoint	Key Type IKE	
				Ĵ

Router Setup		VPN Policy Definition	
Setup Wizard		Name: client1 Enable Policy	
LAN		Remote VPN endpoint	
Status		O Domain Name:	
🔻 Internet		Local IP addresses	
- Security		Type: Subnet address 🗹 IP address: 192, 168, 0 . 0 ~ 0	
▼ Security		Subnet Mask: 255, 255, 0	
▲ VPN (IPSec)		Remote IP addresses	
VPN Policies		Type: Single address 🕜 IP address: 0 0 0 0 ~ 0	
CRLs		Subnet Mask: 255, 255, 255, 0	
VPN Status		AH Authentication Algorithm: MD5	
▼ Microsoft VPN		ESP Encryption Algorithm: 3DES	
▲ Other			
Config File     Network Diag		Manual Key Exchange	
PC Database		IKE (Internet Key Exchange)	
Remote Admin		Direction Responder	
Dipgrade FW		Local Identity Data	
▶ UPnP	1	Remote Identity Type Remote WAN IP	
÷			
Router Setup		ESD Authentication	
	8		
Setup Wizard			
LAN		IKE (Internet Key Exchange)	
		Direction Responder	
Status		Local Identity Type	
		Local Identity Type Fully Qualified Domain Name	
▼ Internet		Local Identity Type Fully Qualified Domain Name Local Identity Data rrry.dyndns.org Remote Identity Type Remote WAN IP	
▼ Internet		Local Identity TypeFully Qualified Domain NameLocal Identity Datarmy.dyndns.orgRemote Identity TypeRemote WAN IPRemote Identity Datatest@allnet.de	
▼ Internet ▼ Security		Local Identity TypeFully Qualified Domain NameLocal Identity Datarrry.dyndns.orgRemote Identity TypeRemote WAN IPRemote Identity Datatest@allnet.deAuthenticationRSA Signature (requires certificate)	
<ul> <li>✓ Internet</li> <li>✓ Security</li> <li>▲ VPN (IPSec)</li> </ul>		Local Identity TypeFully Qualified Domain NameLocal Identity Datarrry.dyndns.orgRemote Identity TypeRemote WAN IPRemote Identity Datatest@allnet.deAuthenticationRSA Signature (requires certificate)Image: Pre-shared KeyPre-shared Key	
<ul> <li>✓ Internet</li> <li>✓ Security</li> <li>▲ VPN (IPSec)</li> <li>▶ VPN Policies</li> </ul>	100	Local Identity Type       Fully Qualified Domain Name         Local Identity Data       rrry.dyndns.org         Remote Identity Type       Remote WAN IP         Remote Identity Data       test@allnet.de         Authentication       RSA Signature (requires certificate)         Image: Pre-shared Key       abcdefgh	
<ul> <li>✓ Internet</li> <li>✓ Security</li> <li>▲ VPN (IPSec)</li> <li>&gt; VPN Policies</li> <li>&gt; Certificates</li> <li>&gt; CRLs</li> </ul>	100	Local Identity Type Fully Qualified Domain Name Local Identity Data rrry.dyndns.org Remote Identity Type Remote WAN IP Remote Identity Data test@allnet.de Authentication	
<ul> <li>✓ Internet</li> <li>✓ Security</li> <li>▲ VPN (IPSec)</li> <li>▶ VPN Policies</li> <li>&gt; Certificates</li> <li>&gt; CRLs</li> <li>&gt; VPN Status</li> </ul>		Local Identity Type Fully Qualified Domain Name Local Identity Data rrry.dyndns.org Remote Identity Type Remote WAN IP Remote Identity Data test@allnet.de Authentication Remote Key abcdefgh Authentication Algorithm: SHA-1 Encryption: 3DES Exchange Mode	
<ul> <li>✓ Internet</li> <li>✓ Security</li> <li>▲ VPN (IPSec)</li> <li>&gt; VPN Policies</li> <li>&gt; Certificates</li> <li>&gt; CRLs</li> <li>&gt; VPN Status</li> </ul>		Local Identity Type       Fully Qualified Domain Name         Local Identity Data       rrry.dyndns.org         Remote Identity Type       Remote WAN IP         Remote Identity Data       test@allnet.de         Authentication       RSA Signature (requires certificate)         Pre-shared Key       abcde f gh         Authentication:       3DES         Encryption:       3DES         Exchange Mode       Aggressive Mode         IKE SA Life Time:       28800 (secs)	
<ul> <li>✓ Internet</li> <li>✓ Security</li> <li>▲ VPN (IPSec)</li> <li>&gt; VPN Policies</li> <li>&gt; Certificates</li> <li>&gt; CRLs</li> <li>&gt; VPN Status</li> <li>✓ Microsoft VPN</li> </ul>		Local Identity Type Fully Qualified Domain Name Local Identity Data rrry.dyndns.org Remote Identity Type Remote WAN IP Remote Identity Data test@allnet.de Authentication RSA Signature (requires certificate) Pre-shared Key abcdefgh Authentication Algorithm: SHA-1 V Encryption: 3DES  Exchange Mode Aggressive Mode  IKE SA Life Time: 28800 (secs) I IKE Keep Alive Ping IP Address: 0 0 0 0 0	
<ul> <li>✓ Internet</li> <li>✓ Security</li> <li>▲ VPN (IPSec)</li> <li>&gt; VPN Policies</li> <li>&gt; Certificates</li> <li>&gt; CRLs</li> <li>&gt; VPN Status</li> <li>✓ Microsoft VPN</li> <li>▲ Other</li> </ul>		Local Identity TypeFully Qualified Domain NameLocal Identity Datarrry.dyndns.orgRemote Identity TypeRemote WAN IPRemote Identity Datatest@allnet.deAuthenticationRSA Signature (requires certificate)Pre-shared Key abcde f ghabcde f ghAuthentication:3DES Encryption:3DES Exchange ModeAggressive Mode IKE SA Life Time:28800 (secs)IKE Keep AlivePing IP Address: 0.0.0.0IPSec SA Life Time:28800 (secs)	8
<ul> <li>✓ Internet</li> <li>✓ Security</li> <li>▲ VPN (IPSec)</li> <li>&gt; VPN Policies</li> <li>&gt; Certificates</li> <li>&gt; CRLs</li> <li>&gt; VPN Status</li> <li>✓ Microsoft VPN</li> <li>▲ Other</li> <li>&gt; Config File</li> <li>&gt; Network Diag</li> </ul>		Local Identity TypeFully Qualified Domain NameLocal Identity Datarrry.dyndns.orgRemote Identity TypeRemote WAN IPRemote Identity Datatest@allnet.deAuthenticationRSA Signature (requires certificate)Pre-shared Key abcdefghabcdefghEncryption:3DESExchange ModeAggressive ModeIKE SA Life Time:28800 (secs)IKE Keep AlivePing IP Address:DH GroupGroup 1 (768 Bit)	10
<ul> <li>✓ Internet</li> <li>✓ Security</li> <li>▲ VPN (IPSec)</li> <li>&gt; VPN Policies</li> <li>&gt; Certificates</li> <li>&gt; CRLs</li> <li>&gt; VPN Status</li> <li>✓ Microsoft VPN</li> <li>▲ Other</li> <li>&gt; Config File</li> <li>&gt; Network Diag</li> <li>&gt; PC Database</li> </ul>		Local Identity TypeFully Qualified Domain NameLocal Identity Datarrry.dyndns.orgRemote Identity TypeRemote WAN IPRemote Identity Datatest@allnet.deAuthenticationRSA Signature (requires certificate)Pre-shared Key abcdefghabcdefghAuthentication3DES Encryption:3DES Exchange ModeAggressive Mode IKE SA Life Time:28800 (secs)IKE Keep AlivePing IP Address: 0 . 0 . 0 . 0DH GroupGroup 1 (768 Bit) IKE PFSGroup 1 (768 Bit)	
<ul> <li>✓ Internet</li> <li>✓ Security</li> <li>▲ VPN (IPSec)</li> <li>&gt; VPN Policies</li> <li>&gt; Certificates</li> <li>&gt; CRLs</li> <li>&gt; VPN Status</li> <li>✓ Microsoft VPN</li> <li>▲ Other</li> <li>&gt; Config File</li> <li>&gt; Network Diag</li> <li>&gt; PC Database</li> <li>&gt; Remote Admin</li> </ul>		Local Identity TypeFully Qualified Domain Name ♥Local Identity Datarrry.dyndns.orgRemote Identity TypeRemote WAN IPRemote Identity Datatest@allnet.deAuthenticationRSA Signature (requires certificate) ● Pre-shared Key abcdefghEncryption:3DES ♥Exchange ModeAggressive Mode ♥IKE SA Life Time:28800 (secs)IKE Keep AlivePing IP Address: 0.00.00IPSec SA Life Time:28800 (secs)DH GroupGroup 1 (768 Bit) ♥IPSec PFSGroup 1 (768 Bit) ♥	
<ul> <li>✓ Internet</li> <li>✓ Security</li> <li>▲ VPN (IPSec)</li> <li>&gt; VPN Policies</li> <li>&gt; Certificates</li> <li>&gt; CRLs</li> <li>&gt; VPN Status</li> <li>✓ Microsoft VPN</li> <li>▲ Other</li> <li>&gt; Config File</li> <li>&gt; Network Diag</li> <li>&gt; PC Database</li> <li>&gt; Remote Admin</li> <li>&gt; Routing</li> <li>&gt; Upgrade FW</li> </ul>		Local Identity TypeFully Qualified Domain NameLocal Identity Datarrry.dyndns.orgRemote Identity TypeRemote WAN IPRemote Identity Datatest@allnet.deAuthenticationRSA Signature (requires certificate)Pre-shared Key abcdefghabcdefghAuthentication Algorithm:SHA-1Encryption:3DESExchange ModeAggressive ModeIKE SA Life Time:28800 (secs)IKE Keep AlivePring IP Address:DH GroupGroup 1 (768 Bit)IKE PFSGroup 1 (768 Bit)IPSec PFSGroup 1 (768 Bit)	
<ul> <li>✓ Internet</li> <li>✓ Security</li> <li>▲ VPN (IPSec)</li> <li>&gt; VPN Policies</li> <li>&gt; Certificates</li> <li>&gt; CRLs</li> <li>&gt; VPN Status</li> <li>✓ Microsoft VPN</li> <li>▲ Other</li> <li>&gt; Config File</li> <li>&gt; Network Diag</li> <li>&gt; PC Database</li> <li>&gt; Remote Admin</li> <li>&gt; Routing</li> <li>&gt; Upgrade FW</li> <li>&gt; UPnP</li> </ul>		Local Identity Type       Fully Qualified Domain Name ♥         Local Identity Data       rrry.dyndns.org         Remote Identity Type       Remote WAN IP         Remote Identity Data       test@allnet.de         Authentication       RSA Signature (requires certificate)         Pre-shared Key       abcdefgh         Authentication Algorithm:       SHA-1 ♥         Encryption:       3DES ♥         Exchange Mode       Aggressive Mode ♥         IKE SA Life Time:       28800 (secs)         I IKE Keep Alive       Ping IP Address:       0.0.0.0         IPSec SA Life Time:       28800 (secs)         IKE PFS       Group 1 (768 Bit) ♥         IPSec PFS       Group 1 (768 Bit) ♥         IPSec PFS       Group 1 (768 Bit) ♥	

### Konfiguration des VPN-Clients

#### Einstellungen bei Phase 1

	Client	Networks based on Information Success, Friendsh	i, ip and n
Konsole	Authentisierun	ig	
Parameter	Name (Phase 1)	client1	
Verbindungen	Interface	× 💌	
J Konfiguration	Zieladresse	rrry.dyndns.org	
⊡ 🛃 dient1 ⊙ client1	<ul> <li>Preshared Key</li> <li>Bestätigen</li> </ul>	NEWNENNEN NEWNENNEN	
	C Zertifikat	Zertifikat Verwaltung	
	IKE Verschlüsselung	3DES  Mehr	1
	Schlüssel	DH768	

Bei "Preshared Key" denselben Schlüssel eingeben wie beim Router!

(hier: abcdefgh)

### Auf "Mehr" klicken und eingeben:

1 Oggies		
NAT Port		
Lokale ID —		-
Wert	test@allnet.de	
Туре	Email	
Entfernte ID		
Wert	rrry.dyndns.org	
Туре	DNS	

Die Einstellungen bei "**Parameter**" wurden für diesen Testaufbau nicht verändert. Hier kann man allerdings sinnvollerweise die Zeitspannen für "**Verschlüsselung** (**IPSec**)" entsprechend heraufsetzen. Üblich sind hier Werte im Bereich von mehreren Stunden für den Schlüsselwechsel.

### Einstellungen bei Phase 2

VPN	Client	Networks ba	sed on Information, Success, Friendship and n
Konsole	IPSec Konfigu	uration	
Parameter	Name (Phase 2)	client1	
Verbindungen	Lokale Adresse	192 . 168 . 1	10 . 10
🛃 Konfiguration	Netzwerk Adresse	192 . 168 .	0.0
client1	Vetzwerk Masl	< 255 . 255 . 2	255 . 0
	ESP		
	Verschlüsselung	3DES 💌	Aktiv während Systemstart
	Authentisierung	SHA 💌	
	Mode		
	PFS Gruppe	DH768 💌	Tunnel Öffnen
	12		Regeln anwenden

Wenn der Tunnel aufgebaut wird (auf "**Tunnel öffnen**" klicken) gibt es folgenden Status bei "**Verbindungen**"

	Client		
ateien <u>K</u> onfiguration <u>T</u>	ools <u>?</u>		
	N Client	Networks	based on Information, Success, Friendship and mo
Ronsole	Verbindungen		
Parameter	Host	Mode	Crypto
S Verbindungen	Sclient1-client1-P2	Tunnel	ESP 3DES SHA
			Löschen

Bei der Anzeige von "**Konsole**" sollte folgendes Protokoll bei einer funktionsfähigen VPN-Verbindung zu sehen sein:

🐵 VPN Konsole ACTIV	
105606 Default [SA client1-P1] SEND phase 1 Aggressive Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID]         105607 Default [SA client1-P1] SEND phase 1 Aggressive Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID]         105607 Default [SA client1-P1] SEND phase 1 Aggressive Mode [HASH]         105607 Default [SA client1-P1] SEND phase 2 Aggressive Mode [HASH]         105607 Default [SA client1-P1] SEND phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]         105607 Default [SA client1-client1-P2] SEND phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]         105607 Default [SA client1-client1-P2] SEND phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]         105607 Default [SA client1-client1-P2] SEND phase 2 Quick Mode [HASH]         105607 Default [SA client1-client1-P2] SEND phase 2 Quick Mode [HASH]         105607 Default [SA client1-client1-P2] SEND phase 2 Quick Mode [HASH]         105607 Default [SA client1-client1-P2] SEND phase 2 Quick Mode [HASH]         105608 Default RECV Informational [HASH] [DELETE]	
2	×
Misc Trpt Mesg Cryp Timr SDep SA       Exch Negt Plcy All       Current line :         0 • 0 • 0 • 0 • 0 • 0 • 0 • 0 • 0 • 0 •	31 10000
Stop Clear Stop File Save File Report	Close

### Auf der Seite des Routers kann man ebenfalls den VPN-Status überprüfen:

Policy Name	SPI	Type (IVE or IPSec)	VPN Endpoint	Data Transfered
INclient1-1	cd01ad9a	ESP	217.228.228.165	6900
client1-1	197d1623	ESP	80.128.92.133	6900

und das Logfile sollte ungefähr so aussehen:



Es ist jetzt möglich, vom Client-PC aus durch den VPN-Tunnel die entfernten PC's anzupingen bzw. das LAN-Interface des Routers (hier 192.168.0.1) zu erreichen.

### Der Tunnel wurde erfolgreich aufgebaut! (Quod erat demonstrandum ©)