

ALL-VPN10

VPN Tunnel aufbauen mit dem ALLNET VPN Client (IPSec)



Hilfestellung

In dieser Hilfestellung wird Ihnen Schritt für Schritt erklärt wie Sie einen VPN Tunnel zwischen dem ALLNET VPN Client und dem ALL-VPN10 aufbauen.

Den ALLNET VPN Client können Sie sich auf <u>www.allnet.de</u> im Downloadbereich herunterladen.

In diesem Beispiel wird der ALLNET VPN Client v4.70 verwendet, diesen können Sie direkt unter folgendem Link herunterladen:

ftp://212.18.29.48/ftp/pub//allnet/vpn/all1294vpnclient/ALL1294VPN Client Ver 4.70.zip

Grundsätzlich können Sie unsere Clients 30 Tage lang kostenlos testen. Nach Ablauf dieser Frist müssen Sie die Software mit einem Lizenzschlüssel freischalten, um ihn weiterhin nutzen zu können.

A Konfiguration des ALL-VPN10

Navigieren Sie auf der Weboberfläche des Routers zu VPN -> Client to Gateway

Iumnel(s) No Iumnel(s) No Interface: WAN 1 Interface: WAN 1 Enabled : V Icocal Security Gateway Type: IP Address: 188 192 188 192 193 192 192 193 192 193 194 194 195 195 198 199 <t< th=""><th>lunnel(s</th><th></th><th></th></t<>	lunnel(s		
Image(a) Name : allnet Imbordance: WAN 1 Enabled : Importance Importance: WAN 1 Enabled : Importance Importance: Importance Importance: </th <th></th> <th>) NO. 1</th> <th></th>) NO. 1	
Interface: WAN 1 * Enabled: Image: Control of Co	Tunnel(s) Na	me: allnet	
Enabled: ▼ Icocal VPN Group Setting Die IP Addresse wird automatisch vom Router ausgefüllt IP Address: 188 174 185 74 bitte nicht ändern - Icocal Security Group Type: Subnet ▼ • bitte nicht ändern - IP Address: 192 168 1 0 Stellen Sie hier das LAN-seitige Subnet Mask: Subnet Mask: 265 255 0 Stellen Sie hier Ads LAN-seitige Subnet Ihres ALL-VPN10 ein Remote VPN Group Setting Dynamic IP + E-mail(User FODN) Authentication ▼ E-mail: test @ alinet.de IPSec Setting Keying Mode: KE with Preshared Key ▼ Phase1 Encryption: DES ▼ Phase1 SA LIfe Time: 28800 seconds Phase2 SA Life Time: 28800 seconds Phase2 Authenticator: MD5 ▼ Phase2 Authenticator: MD5 ▼ Phase2 Authenticator: MD5	Interf	ace: WAN 1	
 Local VPN Group Setting Die IP Adresse wird automatisch vom Router ausgefüllt	Enab	led :	
 Local VPN Group Setting Die IP Adresse wird automatisch vom Router ausgefüllt			
Local Security Gateway Type: IP Only vom Router ausgefüllt IP Address: 188 174 185 74 Local Security Group Type: Subnet * • bitte nicht ändern - Local Security Group Type: 192 168 1 0 Stellen Sie hier das LAN-seitige Subnet * Subnet Mask: 255 255 0 Stellen Sie hier das LAN-seitige Subnetz Ihres ALL-VPN10 ein Remote VPN Group Setting Remote Security Gateway Type: Dynamic IP + E-mail(User FQDN) Authentication * • E-mail: test @ alinet de • • Phase1 DHGroup : Group 1 ~ • • Phase1 SA Life Time: 28800 seconds • • Phase2 DHGroup: Group 1 ~ • • Phase2 DHGroup: Group 1 ~ • • Phase2 DHGroup: Group 1 ~ • • Phase2 Authentication: MD5 ~ • • Phase2 Authentication: MD5 ~ • • Phase2 SA Life Time: 3600 seconds • • Phase2 SA Life Time: 3600 seconds <	Local VPN Group Setting		Die IP Adresse wird automatisch
IP Address: 188 174 185 74 - bitte nicht ändern - Local Security Group Type: Subnet I 92 188 1 0 Stellen Sie hier das LAN-seitige Subnet Mask: 255 255 0 Stellen Sie hier das LAN-seitige Subnet Mask: 255 255 0 Stellen Sie hier das LAN-seitige Subnet VPN Group Setting Remote Security Gateway Type: Dynamic IP + E-mail(User FQDN) Authentication ▼ Email: est @ alinet de IP Sec Setting Keying Mode: KE with Preshared Key ▼ Phase1 DhGroup: Group 1 ▼ Phase1 DhGroup: Group 1 ▼ DES ▼ Phase1 Authentication: MD5 ▼ Phase1 SA Life Time: 28800 seconds Perfect Forward Secrecy Ø Phase2 DhGroup: Group 1 ▼ Phase2 Seconds Phase2 Seconds Phase2 Seconds Phase2 Authentication: MD5 ▼ Phase2 Seconds Phase2 Seconds Phase2 Seconds Phase2 SA Life Time: 3600 seconds Seconds Phase2 Seconds	Local Security Gateway	Type: IP Only	vom Bouter ausgefüllt
Local Security Group Type: Subnet IP Address: 192 Subnet Mask: 255 255 255 0 Remote VPN Group Setting Remote Security Gateway Type: Dynamic IP + E-mail(User FQDN) Authentication E-mail: test @ allnet de	IP Addr	ess: 188 . 174 . 185 . 74	- hitte nicht ändern -
Local Security Group Type: Subnet IP Address: 192 Subnet Mask: 255 255 255 0 Stellen Sie hier das LAN-seitige Subnetz Ihres ALL-VPN10 ein Remote VPN Group Setting Remote Security Gateway Type: Dynamic IP + E-mail(User FODN) Authentication Phase Setting IPSec Setting Keying Mode: KE with Preshared Key Phase1 DHGroup: Group 1 Phase1 Sh Life Time: 28800 Phase2 Sh Life Time: 3600 Phase2 DHGroup: DES Phase2 Sh Life Time: 3600 Phase2 Sh Life Time: 3600 Phase2 Sh Life Time: 3600 Phase2 Sh Life Time: 3600	- 10 M (20 M (4))		
IP Address: 192 168 1 0 Stellen Sie hier das LAN-seitige Subnetz Ihres ALL-VPN10 ein Subnet Mask: 255 255 255 0 Stellen Sie hier das LAN-seitige Subnetz Ihres ALL-VPN10 ein Remote VPN Group Setting Remote Security Gateway Type: Dynamic IP + E-mail(User FQDN) Authentication E-mail: test @ allnet de IPSec Setting Keying Mode: KE with Preshared Key • Phase1 DHGroup: Group 1 • Phase1 DHGroup: Des • Phase1 Authentication: MD5 • Phase1 Authentication: MD5 • Phase2 Authent	Local Security Group	Type: Subnet 💌	
Subnet Mask: 255 255 0 Subnetz Ihres ALL-VPN10 ein Remote VPN Group Setting Remote Security Gateway Type: Dynamic IP + E-mail(User FODN) Authentication E-mail: E-mail: <td>IP Addr</td> <td>ess: 192 . 168 . 1 . 0</td> <td>Stellen Sie hier das LAN-seitige</td>	IP Addr	ess: 192 . 168 . 1 . 0	Stellen Sie hier das LAN-seitige
Remote VPN Group Setting Remote Security Gateway Type: E-mail: by alinet de IPSec Setting Keying Mode: IKE with Preshared Key ◆ Phase1 DHGroup: Group 1 ◆ Phase1 DHGroup: DES ◆ Phase1 Authentication: MD5 ◆ Phase2 Authentication: DES ◆ Phase2 Authentication: MD5 ◆ Phase2 Authentication: MD5 ◆ Phase2 Authentication: MD5 ◆ Phase2 Authentication: MD5 ◆ Phase2 Authentication: Phase2 Authentication: MD5 ◆ Phase2 Authentication: Phase2 Authentication: MD5 ◆ Phase2 Authentication: Phase2 Authentication: <td< td=""><td>Subnet M</td><td>ask: 255 . 255 . 255 . 0</td><td>Subnetz Ihres ALL-VPN10 ein</td></td<>	Subnet M	ask: 255 . 255 . 255 . 0	Subnetz Ihres ALL-VPN10 ein
Remote VPN Group Setting Remote Security Gateway Type: Dynamic IP + E-mail(User FQDN) Authentication ▼ E-mail test @ allnet.de Phase Setting Keying Mode: IKE with Preshared Key ▼ Phase1 DHGroup: Group 1 ▼ Phase1 DHGroup: Group 1 ▼ Phase1 SA Life Time: 28800 seconds Perfect Forward Secrecy ✓ Phase2 DHGroup: Group 1 ▼ Phase2 DHGroup: Group 1 ▼ Phase2 DHGroup: Group 1 ▼ Phase2 Authentication: MD5 ▼ Phase2 DHGroup: Group 1 ▼ Phase2 Authentication: MD5 ▼ Phase2 SA Life Time: 3600 seconds Phase2 SA Life Time: 3600 seconds Phase2 SA Life Time: 3600 seconds			
Remote Security Gateway Type: Dynamic IP + E-mail(User FQDN) Authentication E-mail: test @ allnet.de	Remote VPN Group Setting		
Remote Security Gateway Type: Dynamic IP + E-mail(User FQDN) Authentication E-mail: test @ allnet.de IPSec Setting Keying Mode: KE with Preshared Key • Phase1 DHGroup: Group 1 • Organication Phase1 DHGroup: Group 1 • Organication Phase1 Authentication: MD5 • Organication Phase1 Authentication: MD5 • Organication Phase1 SA Life Time: 28800 seconds Organication Phase2 DHGroup: Group 1 • Organication Phase2 DHGroup: Group 1 • Organication Phase2 Authentication: MD5 • Organication Phase2 SA Life Time: 3600 seconds Organication Preshared Key: 12345 Organication	• Remote if it broup betting		
E-mail: test IPSec Setting Keying Mode: KE with Preshared Key Phase1 DHGroup: Group 1 Phase1 Encryption: DES Phase1 Authentication: MD5 Phase1 SA Life Time: 28800 Seconds Perfect Forward Secrecy Phase2 DHGroup: Group 1 Phase2 DHGroup: Group 1 Phase2 Authentication: MD5 Phase2 SA Life Time: 3600 seconds Phase2 SA Life Time: 3600 seconds	Remote Security Gateway	Dynamic IP + E-mail(User FQDN) Authenti	cation 💌
IPSec Setting Keying Mode: KE with Preshared Key ▼ Phase1 DHGroup: Group 1 ▼ Phase1 DHGroup: DES ▼ Phase1 Authentication: MD5 ▼ Phase1 SA Life Time: 28800 seconds Perfect Forward Secrecy ✓ Phase2 DHGroup: Group 1 ▼ Phase2 Authentication: MD5 ▼ Phase2 Authentication: MD5 ▼ Phase2 Authentication: MD5 ▼ Phase2 Authentication: MD5 ▼ Phase2 SA Life Time: 3600 seconds Phase2 SA Life Time: 3600 seconds	E4	nail: test @ allnet.de	
IPSec Setting Keying Mode: IKE with Preshared Key ↓ Phase1 DHGroup: Group 1 ↓ Phase1 DHGroup: DES ↓ Phase1 Authentication: MD5 ↓ Phase1 SA Life Time: 28800 seconds Perfect Forward Secrecy ✓ Phase2 DHGroup: Group 1 ↓ Phase2 DHGroup: Group 1 ↓ Phase2 DHGroup: Group 1 ↓ Phase2 Authentication: MD5 ↓ Phase2 SA Life Time: 3600 seconds Preshared Key: 12345			
Phase1 EncryptionDESPhase1 AuthenticationMD5Phase1 SA Life Time28800Perfect Forward SecredIPhase2 DHGroupGroup 1Phase2 EncryptionDESPhase2 AuthenticationMD5Phase2 SA Life Time3600Seconds12345	Phase1 DHGr	oup: Group 1 -	
Phase1 Authentication:MD5Phase1 SA Life Time:28800 secondsPerfect Forward SecrecyIPhase2 DHGroup:Group 1Phase2 Encryption:DESPhase2 Authentication:MD5Phase2 SA Life Time:3600 secondsPreshared Key:12345	Phase1 Encryp	tion: DES 👻	
Phase1 SA Life Time:28800 secondsPerfect Forward SecrecyImage: Comp and the secondsPhase2 DHGroup:Group 1 Image: Comp and the secondsPhase2 Encryption:DES Image: Comp and the secondsPhase2 SA Life Time:3600 secondsPreshared Key:12345	Phase1 Authentica	tion: MD5 👻	
Perfect Forward SecrecImage: Comparison of the second of the	Discussion of the T	20000	
Phase2 DHGroup:Group 1 Phase2 Encryption:DES Phase2 Authentication:MD5 Phase2 SA Life Time:3600 secondsPreshared Key:12345	Pliaset SA Life I	ime: 28800 seconds	
Phase2 Encryption: DES Phase2 Authentication: MD5 Phase2 SA Life Time: 3600 Preshared Key: 12345	Priaset SA Life I Perfect Forward Sec	recy V	
Phase2 Authentication: MD5 < Phase2 SA Life Time: 3600 seconds Preshared Key: 12345	Phaset SA Life 1 Perfect Forward Sec Phase2 DHGr	recy V Group 1 V	
Preshared Key: 12345	Phaset SA Life 1 Perfect Forward Sec Phase2 DHGr Phase2 Encryp	recy ♥ oup: Group 1 tion: DES UDS	
Preshared Key: 12345	Phase1 SA Life 1 Perfect Forward Sec Phase2 DHGr Phase2 Encryp Phase2 Authentica	recy ♥ oup: Group 1 ♥ tion: DES ♥ tion: MD5 ♥	
	Phase1 SA Life 1 Perfect Forward Sec Phase2 DHGr Phase2 Encryp Phase2 Authentica Phase2 SA Life 1	recy ♥ oup: Group 1 tion: DES ime: 3600 seconds	
	Phaset SA Life I Perfect Forward Sec Phase2 DHGr Phase2 Encryp Phase2 Authentica Phase2 SA Life T Preshared	recy ♥ oup: Group 1 ↓ tion: DES ↓ tion: MD5 ↓ ime: 3600 seconds Key: 12345	
	Phaset SA Life I Perfect Forward Sec Phase2 DHGr Phase2 Encryp Phase2 Authentica Phase2 SA Life T Preshared	recy ♥ oup: Group 1 ↓ tion: DES ↓ tion: MD5 ↓ Time: 3600 seconds Key: 12345 Advanced -	
Advanced	Phase1 SA Life 1 Perfect Forward Sec Phase2 DHGr Phase2 Encryp Phase2 Authentica Phase2 SA Life 1 Preshared	Inte: 28800 seconds recy ✓ oup: Group 1 ↓ tion: DES ↓ tion: MD5 ↓ Time: 3600 seconds Key: 12345	
Advanced	Phase1 SA Life 1 Perfect Forward Sec Phase2 DHGr Phase2 Encryp Phase2 Authentica Phase2 SA Life 1 Preshared Advanced	Inne: 28800 seconds recy ♥ oup: Group 1 ↓ tion: DES ↓ tion: MD5 ↓ ime: 3600 seconds Key: 12345 Advanced -	
Advanced Aggressive Mode	Phase1 SA Life 1 Perfect Forward Sec Phase2 DHGr Phase2 Encryp Phase2 Authentica Phase2 SA Life 1 Preshared Advanced	Inne: 28800 seconds recy V bup: Group 1 v tion: DES v tion: MD5 v ime: 3600 seconds Key: 12345 Advanced -	
Advanced Aggressive Mode Compress (Support IP Payload Compression Protocol(IPComp))	Advanced Phaser SA Life I Perfect Forward Sec Phase2 DHGr Phase2 Encryp Phase2 Authentica Phase2 SA Life I Preshared Advanced Compress (Support I	Imme: 28800 seconds recy Imme: Group 1 oup: Group 1 Imme: ition: DES Imme: 3600 seconds Key: 12345	
Advanced Aggressive Mode Compress (Support IP Payload Compression Protocol(IPComp)) Keep-Alive	Advanced Advanced Aggressive Mode Compress (Support I Keep-Alive	Imme: 28800 seconds recy Imme: Group 1 Imme: Oup: Group 1 Imme: Group 1 Imme: 3600 seconds Key: 12345 Advanced -	
Advanced Aggressive Mode Compress (Support IP Payload Compression Protocol(IPComp)) Keep-Alive AH Hash Algorithm MD5	Advanced Advanced Advanced Keep-Alive Aligorithm 1	Inte: 28800 seconds recy rec	
Advanced Aggressive Mode Compress (Support IP Payload Compression Protocol(IPComp)) Keep-Alive AH Hash Algorithm MD5 NAT Traversal Double Automatic Version Check Form 10	Advanced Advanced Advanced Advanced Aggressive Mode Compress (Support I Keep-Alive AH Hash Algorithm I NAT Traversal Dect Base Dects for	Imme: 28800 seconds recy Imme: Group 1 Imme: oup: Group 1 Imme: Group 1 Imme: imme: 3600 seconds Key: 12345 Advanced - P Payload Compression Protocol(IPComp)) MD5 Imme: Topological Compression Protocol(IPComp)) MD5 Imme: Feable Automatic Version Obertion Complexity Topological Compression Protocol(IPComp))	
 Advanced Aggressive Mode Compress (Support IP Payload Compression Protocol(IPComp)) Keep-Alive AH Hash Algorithm MD5 AH Traversal Dead Peer Detection(DPD) Enable Automatic Version Check Every 10 seconds 	Advanced Advanced Advanced Advanced Advanced Aggressive Mode Compress (Support I Keep-Alive AH Hash Algorithm VAT Traversal Dead Peer Detectione	Imme: 28800 seconds recy Imme: Group 1 Imme: Joup: Group 1 Imme: Group 1 Imme: Jacobia Jacobia Jacobia Imme: Jacobia Jacobia Key: 12345 Jacobia P Payload Compression Protocol(IPComp)) Jacobia Jacobia ID5 Imme: Jacobia Jacobia DPD) Enable Automatic Version Check Every 10	seconds
 Advanced Aggressive Mode Compress (Support IP Payload Compression Protocol(IPComp)) Keep-Alive AH Hash Algorithm MD5 NAT Traversal Dead Peer Detection(DPD) Enable Automatic Version Check Every 10 seconds 	Advanced Advanced Advanced Compress (Support I Keep-Alive AH Hash Algorithm Dead Peer Detectione	Inte: 28800 seconds recy rec	seconds

Die Punkte *Client to Gateway, Local VPN Group Setting* und *Remote VPN Group Setting* können bei Ihnen unter Umständen abweichen.

Bei *IPSec Setting* und *Advanced* stellen Sie bitte alles genauso ein wie in diesem Beispiel. **Ausnahme** ist der *Preshared Key*! Hier geben Sie bitte einen Schlüssel ein, der nur Ihnen bekannt ist.

Um die Einstellungen zu übernehmen klicken Sie auf "Apply".

Die Konfiguration des Routers ist somit abgeschlossen.

1. Parameter

AllNet VPN Client	1 DECEMBER OF		- X
Datei VPN Konfiguration	Ansicht Tools ?		
ALLNET		ALLNE	T VPN-Client
🔑 Konsole	Parameter		
Parameter	Ebensdauer (Sek.)		
🖙 Varbindungan	Standard	Minimal	Maximal
a verbindungen	Authentisierung (IKE) 28800	28800	28800
Root ⊡Sallnet	Verschlüsselung (IPSec) 3600	3600	3600
(® allnet	Dead Peer Detection (DPD) Intervall (Sek.) 30 Max. Wiederholungen 5 use zw. Wiederholungen (Sek.) 15		
	Verschiedenes Wiedeholungen 2 X-Auth 60	IKE Sek. NAT	Port
	🗖 Unverschlüsselten Netzwerkverkehr	blockieren Speich	ern & Anwenden
VPN Tunnel geöffnet			Tunnel 🔘

Stellen Sie unter Parameter exakt die gleichen Werte ein wie in diesem Screenshot.

Danach klicken Sie auf "Speichern & Anwenden".

2. Phase 1

atei VPN Konfiguration	Ansicht Tools ?
ALLNET	ALLNET VPN-Clie
A Konsole	Phase 1 (Authentisierung)
Parameter	Name allnet
S Verbindungen	Interface Alle
Root	Remote Gateway .dyndns.org Preshared Key ***** Bestätigen: ***** C Zertifikat Zertifikatsmanagement
	IKE Verschlüsselung DES P1 Erweitert Authentisierung MD5 Image: Comparison of the second s

Geben Sie bei *Name* die gleiche Bezeichnung ein wie in Ihrem ALL-VPN10.

Bei *Remote Gateway* tragen Sie die DDNS Adresse bzw. die feste WAN IP-Adresse Ihres ALL-VPN10 ein.

Geben Sie Ihren Preshared Key ein und zur Bestätigung wiederholen Sie die Eingabe.

Unter *IKE* tragen Sie bitte wieder die identischen Werte ein.

Danach klicken Sie auf "P1 Erweitert...".

3. Phase 1 Erweitert

				ALLNE
Erweiterte Einste	ellungen			
🔲 Config Mod	le	Redund.GW		
🔽 Agressive N	1ode	NAT-T	Automatic	-
X-Auth				
🔲 X-Auth Pop	up	Login		
🔲 Hybrid Mod	le	Passwort		
Lokale und Entf	ernte ID —			
	ID Typ auswä	ihlen:	ID Wert eintrage	n:
Lokale ID	eMail	•	test@allnet.de	
Entfernte ID	IP Adresse	•	.dyndns.org	

Tragen Sie bei *Lokale ID*, die Werte ein, welche Sie im ALL-VPN10 unter *Remote VPN Group Setting* hinterlegt haben.

Als *Entfernte ID* wählen Sie 'IP Adresse' und geben die DDNS Adresse bzw. die feste WAN IP-Adresse Ihres ALL-VPN10 ein.

Klicken Sie auf "OK" und danach auf "Speichern & Anwenden".

4. Phase 2

AllNet VPN Client Datei VPN Konfiguration	n Ansicht Tools ?
ALLNET	ALLNET VPN-Client
🔑 Konsole	Phase 2 (IPSec Konfiguration)
🎯 Parameter	Name allnet
😽 Verbindungen	VPN Client Adresse 178 . 27 . 2 . 253
⊡ <mark>G</mark> Root ⊡SG allnet 	Adresstyp Subnetz Adresse Remote LAN Adresse 192 . 168 . 1 . 0 Subnetz Maske 255 . 255 . 0
	ESP Verschlüsselung DES P2 Erweitert Authentisierung MD5 Skripte
	Modus Tunnel
	PFS Gruppe DH1 (768) Tunnel schliessen
	Speichern & Anwenden
VPN Tunnel geöffnet	Tunnel 🔘

Geben Sie bei *Name* wieder die gleiche Bezeichnung ein wie in Ihrem ALL-VPN10.

Bei *VPN Client Adresse* geben Sie eine IP Adresse ein, welche nicht zu dem Subnetz Ihres lokalen Netzwerkes, noch zum LAN-seitigen Netzwerk des ALL-VPN10 passt.

Wählen Sie 'Subnetz Adresse', tragen bei *Remote LAN Adresse* das LAN-seitige Subnetz Ihres ALL-VPN10 und bei *Subnetz Maske* die entsprechende Subnetz Maske ein.

Die korrekten Werte von ESP übernehmen Sie wieder eins zu eins aus dem Screenshot.

Zum Bestätigen der Eingaben klicken Sie auf "Speichern & Anwenden".

5. Tunnel öffnen

Abschließend machen Sie einen Rechtsklick auf Ihren Tunnelnamen (im Bsp. *allnet*) und wählen "Tunnel öffnen".