

# HowTo: Einrichtung von L2TP over IPSec VPN

#### [Voraussetzungen]

- 1. DWC-1000/2000 mit Firmware Version: 4.4.1.2 und höher mit aktivierter VPN-Lizenz
- 2. DSR-150N,250N,500N,1000N,1000AC mit Firmware Version 2.x und höher

#### [Szenario]

Remote Clients sollen per L2TP over IPSec VPN auf den Router eine VPN Verbindung aufbauen. Diese Konstellation wird u.a. auch Hub-Spoke genannt.





## [Vorbereitung]

- ⇒ Der DWC-1000 hat im Auslieferungszustand die Standard IP 192.168.10.1/24 sowie den Benutzernamen "admin" & Passwort "admin"
- ⇒ Bitte ändern Sie dies bei der Ersteinrichtung (Integration in Ihre bestehende Infrastruktur) des DWC-1000 in Ihrem Netzwerk, für die genaue Vorgehensweise der Einstellung der IP & des Benutzernamens schlagen Sie bitte im Handbuch (<u>ftp://ftp.dlink.de/dwc/dwc-1000/documentation/</u>) nach
- Stellen Sie bitte sicher, dass Sie die aktuellste Firmware f
  ür den DWC-1000 installiert haben (<u>ftp://ftp.dlink.de/dwc/dwc-1000/driver\_software/</u>)
- ⇒ Die VPN Lizenz ist korrekt auf dem DWC-1000 aktiviert
- ⇒ Der WAN-Zugang ist korrekt konfiguriert und das Gerät hat Internetzugriff
- ⇒ Sollten sie keine statische WAN IP besitzen, so muss das Gerät bei Ihrem z.B. DynDNS Anbieter registriert sein um eine entsprechende Namensauflösung zu nutzen



#### [Einrichtung der korrekten Systemzeit]

1.) Bitte passen Sie die Zeitsynchronisierung des Gerätes an, gehen Sie hierzu auf "Maintenance -> Date and Time"

<b>D-Link</b> Unified Controller - DWC-1000		Logged in Serial Number: <u>QBE21C24</u>	as: admin (ADMIN)   Lan 200055-   Firmware Version: Wiz	guage: English [US]	Logout Q
🙆 Status 🛜 Win	reless 📃 Net	work 🙆 VPN	Security	<b>O</b> Maintenance	
atus » Dashboard he Traffic Overview, Discovered APs, Opt ctive info for user/group are profiled her	Administration System Setting Oate and Time Session Settings	Management Remote Management SNMP Diagnostics	Firmware Firmware Upgrade Backup / Restore Soft Reboot	Logs Settings Facility Logs Routing Logs System Logs	and
ashboard	License Update USB Share Ports	Power Saving	AP Firmware Download	Remote Logs Syslog Server Event Logs	ard

Passen Sie die bei Ihnen gültigen Zeiteinstellungen an

a.	Time Zone	= z.B. GMT +1 Berlin (in Deutschland)
b.	Daylight Saving	= aktivieren Sommer/Winterzeit
c.	NTP Server	= Network Time Server aktivieren
	i. Default	= vorgegebene Server
	ii. Custom	= hier haben Sie die Möglichkeit 2 eigene Zeitserver
		einzutragen
d.	Time to Synchronize	= Zeit zwischen 2 Synchronisierungsabläufen (eine zu
	· 7 <sup>-</sup> · 1	

**d.** Time to Synchronize = Zeit zwischen 2 Synchronisierungsabläufen (eine zu geringe Zeitspanne kann je nach Konfiguration des Servers zu Fehlern/Sperrungen des Client führen)

Maintenance » Administration » Date and Time	
This page allows us to set the date, time and NTP a network of computers. Accurate time across a network of computers.	servers. Network Time Protocol (NTP) is a protocol that is used to synchronize computer clock time in etwork is important for many reasons.
Date and Time	
Current Device Time	Wed Oct 28 10:28:38 GMT+0100 2015
Time Zone	(GMT+01:00) Amsterdam Berlin 🔽
Daylight Saving	ON III
NTP Servers	ON THE
NTP Server Type	● Default ○ Custom
Time to re-synchronize	60 [Default: 120, Range: 5 - 1440] Minutes
	Save Cancel

Mittels Save speichern Sie Ihre Eingaben.



#### [Einrichtung der L2TP VPN]

1.) Bitte aktivieren Sie den L2TP Servermodus, gehen Sie hierzu auf "VPN => L2TP VPN => Server"

🐼 Sta	itus 🛜 Wi	ireless 📃 💻 Net	work 🕼 VPN	Security	😳 Maintenance
ntenance » Admin	IPSec VPN Policies	PPTP VPN Server	L2TP VPN Server	SSL VPN SSL VPN Server Policy	OpenVPN Settings
	Tunnel Mode	Client	Active Users	Portal Layouts	Local Networks
	DHCP Range	Active Users		Resources	Remote Networks
page allows us to	Certificates			SSL VPN Client	Authentication
atwork of compute	Easy VPN Setup			Client Routes	
te and Time					

Aktivieren und Konfigurieren Sie den L2TP Server

- **a.** Enable L2TP Server = Ein-/Ausschalten des Servermodus für L2TP **b.** L2TP Routing Mode
  - = NAT oder Klassisches Routing
- = IP Adressbereich der den Clients zugewiesen **c.** Range of IP Addresses wird, dieser IP Bereich darf in Ihrem Netzwerk noch nicht verwendet/vergeben sein
- **d.** Autenntication Support = die Möglichen angebotenen Authentifizierungsverfahren, prüfen Sie hier, welche von Ihren Clients benötigt werden
- e. User Time-Out = Zeit indem der Benutzer inaktiv sein darf, ohne dass die Verbindung getrennt wird (inaktiv = kein Datenfluss)
- **f.** Netbios = soll die Netbios Namensauflösung unterstützt werden (bei aktiviertem Netbios können Sie 2 WINS Server angeben)

VPN » L2TP VPN » Server		0
L2TP allows an external user to connect to yo define a range of IP addresses for clients con communicate with LAN hosts, access any serve	ur router through the internet, forming a VPN. This section allows you to necting to your router. The connected clients can function as if they are ers present etc.).	enable/disable L2TP server and on your LAN (they can
L2TP Server		
Server Setup Enable L2TP Server	OFF	
	Save Cancel	



VPN » L2TP VPN » Server	<ul> <li>(9)</li> </ul>
L2TP allows an external user to connect to define a range of IP addresses for clients o communicate with LAN hosts, access any s	your router through the internet, forming a VPN. This section allows you to enable/disable L2TP server and connecting to your router. The connected clients can function as if they are on your LAN (they can ervers present etc.).
L2TP Server	
Server Setup	
Enable L2TP Server	ON THE
L2TP Routing Mode	● Nat O Classical
Range of IP Addresses (Allocated t	o L2TP Clients)
Starting IP Address	192.168.100.10
Ending IP Address	192.168.100.20 ×
Authentication Supported	
PAP	ON THE
СНАР	ON
MS-CHAP	OFF
MS-CHAPv2	OFF
Secret Key	OFF
User Time-out	
Idle TimeOut	300 [Range: 300 - 1800] Seconds
Netbios Setup	
Netbios	OFF
	Save Cancel

Mittels Save speichern Sie Ihre Eingaben.

2.) Anlegen und Konfigurieren Sie den L2TP Benutzer, gehen Sie hierzu auf "Security => User Database"

	🕐 Status	🛜 Wireless	💻 Netw	vork 🚯 VPN	Security	🗘 Maintenance
				Authentication	Web Content Filter	Firewall
VPN » L21	FP VPN » Server			User Database	Static Filtering	Firewall Rules
L2TP allow	s an external user t	o connect to your route	er through the	External Auth Servers		Schedules
define a ra	nge of IP addresses	for clients connecting	to your router	Radius Accounting Glob	pal	Blocked Clients
communica	ILE WITH LAN HOSTS,	access any servers pres	ent etc.).	Settings		Custom Services
L2TP Ser	ver			Login Profiles		ALGs

Legen Sie eine neue L2TP Gruppe mittels "Add New Group" an und speichern Sie diese mittels Save.

Security » Authentication » User Database » Groups	<b>0</b>
Get User DB Groups Users MAC Authentication	
This page shows the list of added groups to the router. The user can add, dele	te and edit the groups also.
Groups List	
Show 10 vertices [Right click on record to get more options]	٩
Group Name 🗘	Description $\Theta$
ADMIN	AdminGroup
GUEST	GuestGroup
Showing 1 to 2 of 2 entries	First     Previous     1     Next     Last
Add New Group	



Group Configuration		X
Group Name	L2TP	
Description	L2TP	
<b>User Type</b> User Type	Admin ONetwork OFront Desk OGuest	
PPTP User	OFF	
L2TP User	ON III	
SSLVPN User	OFF	
Captive Portal User	III OFF	
Idle Timeout	10 [Default: 10, Range: 1 - 999] Minutes	
	Save	

Wechseln Sie nun in die Benutzerverwaltung und fügen mittels "Add New User" einen neuen Benutzer hinzu.

Security » Authentication » User Datab	oase » Users	
Get User DB Groups Users	MAC Authentication	
This page shows a list of available use users.	rs in the system. A user can add, delete ar	d edit the users also. This page can also be used for setting policies on
Users List		
Show 10 v entries [Right click on r	ecord to get more options]	م
User Name 🔂	Group Name ⊖	Login Status $\Theta$
admin	ADMIN	Enabled (LAN) Enabled (OPTION)
guest	GUEST	Disabled (LAN) Disabled (OPTION)
Showing 1 to 2 of 2 entries		First     Previous     1     Next     Last
Add New User		

Definieren Sie für diesen Benutzer den Benutzernamen und das Passwort. Zudem weisen Sie diesen Benutzer der soeben angelegten Gruppe L2TP zu. Mittel Save speichern Sie Ihre Eingabe.

User Configuration			X
User Name	l2tpuser		
First Name	l2tpuser	]	
Last Name	I2tpuser	]	
Select Group	L2TP		
Password	••••	]	
Confirm Password	•••••	]	
		Save	•



### [Einrichtung der IPSEC VPN Policy]

1.) Bitte aktivieren Sie den L2TP Servermodus, gehen Sie hierzu auf "VPN => IPSEC VPN => Policies"

CA Sta	atus 🛜 Wirei	less 📃 Network	CâS VPN	Security	• Maintenance
N » L2TP VPN » S	IPSec VPN	PPTP VPN	L2TP VPN	SSL VPN	OpenVPN
	Policies Turned Made	Client	Server	SSL VPN Server Poucy	Securitys
	Tunnet Mode	Client	Active Users	Portal Layouts	Local Networks
	DHCP Kange	Active Users		Kesources	Remote Networks
TP allows an extern	Certificates			SSL VPN Client	Authentication nd
mmunicate with LA	Easy VPN Setup			Client Routes	
TP Server					
N » IPSec VPN »	Policies				
N » IPSec VPN » is page shows the m this page. Sec Policies Li how 10 v entri	Policies List of configured IPsec St es [Right click on record	VPN policies on the router to get more options]	. A user can also add, del	lete, edit, enable, disa	able and export IPsec VPN policience
N » IPSec VPN » is page shows the om this page. Sec Policies Li how 10 v entri- status Name	Policies List of configured IPsec St es [Right click on record $\ominus$ Backup $\ominus$ T Name	VPN policies on the router to get more options] Type $\Rightarrow$ IPSec Mode $\Rightarrow$	. A user can also add, del	lete, edit, enable, disa	able and export IPsec VPN policient Able and export IPsec VPN policient Auth ⊖ Encr
N » IPSec VPN » is page shows the om this page. Sec Policies Lis how 10 v entri- status Name	Policies ist of configured IPsec st es [Right click on record $\Rightarrow$ Backup Tunnel $\Rightarrow$ T Name	VPN policies on the router to get more options] Type $\Rightarrow$ IPSec Mode $\Rightarrow$	. A user can also add, del Local	ete, edit, enable, disa	Able and export IPsec VPN policie  Auth  Auth  Find  Find Find
N » IPSec VPN » is page shows the m this page. Sec Policies Li: how 10 v entri itatus Name	Policies ist of configured IPsec st es [Right click on record ⊕ Backup Tunnel ⊕ T Name	VPN policies on the router to get more options] Type ⊕ IPSec Mode ⊕ t 0 11 7 T 11 1	Local	ete, edit, enable, disa	€ Auth € Encr
N » IPSec VPN » is page shows the im this page. Sec Policies Li how 10 V entri itatus Name Name howing 1 to 2 of 2 entri	Policies ist of configured IPsec st as [Right click on record ⊖ Backup Tunnel ⊖ T Name → T ries	VPN policies on the router to get more options] <sup>•</sup> ype ⊕ IPSec Mode ⊕ · O.V., T	Local	ete, edit, enable, disa	Auth Auth Auth Auth For are are and fully Auth Auth For are are are are are are are are are ar
N » IPSec VPN » is page shows the in this page. Sec Policies Li: how 10 v entric tatus Name ii i i i i i i i i i i i i i i i i i i	Policies iist of configured IPsec st as [Right click on record ⊕ Backup Tunnel ⊕ T Name IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	VPN policies on the router to get more options]	Local	ete, edit, enable, disa Remote a too too enore a a too too enore a c too too enore a c too too enore a c too too enore a	Auth Auth Auth Previous 1 Next > Last ;

Mittels "Add New IPSec Policy" können Sie eine neue IPSec Policy anlegen

Aktivieren und Konfigurieren Sie den L2TP Server

**a.** Policy Name = Name für Ihre Policy **b.** Policy Type = Auto oder Manuell (Auto = Standard) **c.** IKE Version = IVEv1 oder IKEv2 (IKEv1 = Standard) **d.** IPSec Mode = Tunnel oder Transport Mode = Tunnel verbindet zwei Netze über zwei Router a. Tunnel **b.** Transport = Transport stellt eine Punkt-zu-Punkt-Kommunikation zwischen zwei Endpunkten her e. Local Gateway = definiert das WAN Interface auf dem das VPN aufgebaut wird **f.** Remote Endpoint = Adresse der Gegenstelle **a.** IP Adresse = statische IP Adresse der Gegenstelle = Full Qualified Domain Name, z.B. DynDNS Name der **b.** FQDN Gegenstelle, bei HUB-SPOKE Konstellation muss hier 0.0.0.0 am HUB eingetragen werden



IPSec Policy Configuration		
General		
Policy Name	VPN-HUB	
Policy Type	Auto Policy	
IP Protocol Version	IPv4	
IKE Version	IKEv1	
IPSec Mode	Tunnel Mode	
Select Local Gateway	Option1	
Remote Endpoint	FQDN	
IP Address / FQDN	0.0.0.0	
Enable Mode Config	OFF	
Enable NetBIOS	OFF	
Enable PollOver	000	

- **g.** Lokale IP = Lokale IP Einstellungen
  - **a.** ANY = ALLES, für Hub-Spoke an der HUB Seite
  - **b.** SINGLE = locale einzelne IP Adresse
  - **c.** RANGE = lokaler IP-Adressbereich
  - **d.** SUBNET = lokales IP-Subnetz, für Site-to-Site VPN
- **h.** Remote IP = Lokale IP Einstellungen
  - **a.** ANY = ALLES, für Hub-Spoke an der HUB Seite
  - **b.** SINGLE = remote einzelne IP Adresse
  - **c.** RANGE = remote IP-Adressbereich
  - **d.** SUBNET = remote IP-Subnetz, für Site-to-Site VPN
- i. Enable Keepalive = Einstellungen um einen Site-to-Site VPN auch bei nichtbenutzung aktiv zu halten

IPSec Policy Configuration		X
Enable NetBIOS	OFF	A
Enable RollOver	OFF	$\int$
Protocol	ESP	
Enable DHCP	OFF	1
Local IP	Any	
Remote IP	Any	( -
Enable Keepalive	OFF	
Phase1(IKE SA Parameters)		
Exchange Mode	Main 🗸	
Direction / Type	Both	
Nat Traversal	ON III	
Local Identifier Type	Local Wan IP	
		Save

#### PHASE 1

j.	Exchange Mode	= wie die SA Parameter ausgetauscht werden
	a. Main	= verschlüsselt
	<b>b.</b> Agressive	= unverschlüsselt (z.B. Standard bei AVM Gegenstelle)
k.	NAT Traversal	= aktiv. wenn z.B. eine NAT überwunden werden muss



- **I.** Local Identifier Type = Indetifikator
  - a. Local WAN IP
  - b. FQDN
  - c. User FQDN
  - d. DER ASN1 DN
- m. Remote Identifier
  - a. Remote WAN IP
  - b. FQDN
  - c. User FQDN
  - d. DER ASN1 DN

- = lokale WAN IP, wird automatisch eingetragen
  - = lokaler FQDN, bei Site-to-Site VPN Notwendig
- = lokaler eigener FQDN
- = DER ASN1 DN Zertifikat
- = remote WAN IP, wird automatisch eingetragen
- = remote FQDN, bei Site-to-Site VPN Notwendig
- = remote eigener FQDN
- N1 DN = DER ASN1 DN Zertifikat

IPSec Policy Configuration					X
Phase1(IKE SA Parameters) Exchange Mode Direction / Type	Main	<b>&gt;</b>			ſ
Nat Traversal	ON				
Local Identifier Type	Local Wan IP	~			
Remote Identifier Type	Remote Wan IP	$\checkmark$			
Encryption Algorithm					
	DES	OFF	3DES	OFF	
	AES-128	ON	AES-192	OFF	
	AES-256	OFF			
	BLOWFISH	OFF			
	CAST128	OFF			ł
					Save

- n. Encryption Algorithm = Verfügbare Verschlüsselungsmechanismen, prüfen Sie bitte die bei Ihren Endgeräten benötigten Mechanismen
   a. z.B. Iphone/Ipad/Windows benötigt den 3DES Algorithmus
- o. Authentication Algorithm = Verfügbare Authentifizierungsmechanismen, prüfen Sie bitte die bei Ihren Endgeräten benötigten Mechanismen

IPSec Policy Configuration					X
Remote Identifier Type	Remote Wan IP	$\checkmark$			Δ
Encryption Algorithm	DES AES-128 AES-256 BLOWFISH CAST128	OR OFF	3DES AES-192	ON OFF	
Authentication Algorithm Authentication Method	MD5 SHA2-256 SHA2-512 Pre-Shared Key	III OFF	SHA-1 SHA2-384	ON OFF	Ų



- p. Authentication Method
  - a. PSK
  - b. RSA Signature
- = Authentifizierungsmethode
- = Standard ist Passwort (PreSharedKey)
- = RSA Zertifikat
- q. Diffie-Hellmann Group = Protokoll wie die Schlüssel ausgetauscht werden sollen, prüfen Sie bitte die bei Ihren Endgeräten benötigten Mechanismen
- r. SA Lifetime generiert wird
- = definiert die Zeit bis ein neuer Schlüssel
- s. Extended Authentication = weitergehende Authentifizierungsmethoden, wie z.B.Benutzername/Passwort

IPSec Policy Configuration		X
	SHA2-256 OFF SHA2-384 OFF	
	SHA2-512 OFF	
Authentication Method	Pre-Shared Key	
Pre-Shared Key	1234567890 [Length: 8 - 49]	
Diffie-Hellman (DH) Group	Group 2 (1024 bit)	
SA-Lifetime	28800 [Default: 28800, Range: 300 - 2147483647] Seconds	
Enable Dead Peer Detection	OFF	
Extended Authentication	None	
Phase2-(Auto Policy Parameters)		
SA Lifetime	3600 Seconds	
Encryption Algorithm		
	DES OFF NONE OFF	A
		Save

#### PHASE 2

- t. SA Lifetime
- = definiert die Zeit bis ein neuer Schlüssel
- generiert wird
  - = Verfügbare Verschlüsselungsmechanismen,
- u. Encryption Algorithm prüfen Sie bitte die bei Ihren Endgeräten benötigten Mechanismen a. z.B. Iphone/Ipad/Windows benötigt den 3DES Algorithmus
- v. Integrity Algorithm = Verfügbare Authentifizierungsmechanismen, prüfen Sie bitte die bei Ihren Endgeräten benötigten Mechanismen

IPSec Policy Configuration					
Extended Authentication	None	~			λ
Phase2-(Auto Policy Parameters) SA Lifetime	3600	Seconds			
Encryption Algorithm					
	DES	OFF	NONE	OFF	
	3DES	OFF	AES-128	ON III	
	AES-192	OFF	AES-256	OFF	
	AES-CCM	OFF	AES-GCM	OFF	_
	TWOFISH (128)	OFF	TWOFISH (192)	OFF	
	TWOFISH (256)	OFF			
	BLOWFISH	OFF			
	CAST128	OFF			۷
					Save



IPSec Policy Configuration					×
	3DE5	ON III	AES-128	ON	
	AES-192	OFF	AES-256	OFF	1
	AES-CCM	OFF	AES-GCM	OFF	
	TWOFISH (128)	OFF	TWOFISH (192)	OFF	
	TWOFISH (256)	OFF			
	BLOWFISH	OFF			
	CAST128	OFF			
Integrity Algorithm					
	MD5	OFF	SHA-1	ON III	
	SHA2-224	OFF	SHA2-256	OFF	
	SHA2-384	OFF	SHA2-512	OFF	
	PFS Key Group	OFF			V
					Save

# Mittels Save speichern Sie Ihre Eingaben.

VPN » IPSec	PN » IPSec VPN » Policies								
	Operation Succeeded								
This page shows the list of configured IPsec VPN policies on the router. A user can also add, delete, edit, enable, disable and export IPsec VPN policies from this page.									
IPSec Poli	cies List								
Show 10	✓ entries [Ri	ght click on rec	cord to get mor	e options]					٩
Status 🕁	Name ⊖	Backup Tunnel ⊖ Name	Туре ⊖	IPSec Mode ⊖	Local 🕀	Remote	θ	Auth ⊖	Encr ⊖
Enabled	Hoim	Hone	Hate Folicy	Tannet Hode	·//E//08/18/0/195/195/195/195/0	17211001010/2551	199129918	511/1	
			inin Palla,	T	192-142-10-0/200-200-200-200-200-200-200-200-200-	1721101010/20012	55.255.2 10	2020	ALS 120
Enabled	VPN-HUB*	None	Auto Policy	Tunnel Mode	Any	Any		SHA1	3DES AES-128
Showing 1 to	Showing 1 to 3 of 3 entries								

Konfigurieren Sie nun Ihr Endgerät nach den Herstellervorgaben des Endgerätes.



# Prüfung am DWC-1000

⇒ Aktiver L2TP User

🙆 Sta	atus 🛜 Wirele	ss 📃 Network	VPN	Security	ǰ Maintenance
VPN » L2TP VPN » A Active L2TP tunnels c L2TP Active User Show 10 🕑 entrie	IPSec VPN Policies Tunnel Mode DHCP Range Certificates Easy VPN Setup	PPTP VPN Server Client Active Users	L2TP VPN Server	SSL VPN SSL VPN Server Policy Portal Layouts Resources SSL VPN Client Client Routes	OpenVPN Settings Local Networks Remote Networks Authentication
User Name Dipuser Showing 1 to 1 of 1 entr	ies	• Remote IP 192.168.100.11		E2TP IP           192.168.100.10	Previous 1 Next > Last >

### ⇒ Aktive SSLVPN Session

	🕜 Status	🛜 Wireless	💻 Network 🛛 🖌	S VPN 🔒	Security 🔅 🍄 Mainte	enance
Status » Act	Dashboard Dashboard	System Information Device All Logs USB Status	Network Information DHCP Clients Captive Portal Sessions Active Sessions	Wireless Information Radius Accounting Stastistics Controller Status Access Point	ACL & DiffServ IP ACL IP ACL Rules MAC ACL	00
This pag Active Show 1			Interfaces IPv6 Tunnels Status	Associated Clients Clustering WDS Groups Status	MAC ACL Rules DiffServ Class DiffServ Policy DiffServ Policy Attribute	٩
Policy	Name 🔗	Endpoint	- → - tx (KB) - ↔	tx (Packets)	Configuration State	θ
109.84.1	1.234*	109.84.1.234	2.15	21	IPsec SA Established	
-	-	dinianai,minang	0.59	4	IPsec SA Established	
	<u></u>	يستغر بالمطلقة	2.81	24	IPsec SA Established	
Showing	1 to 3 of 3 entries				First Previous 1	Next > Last >