

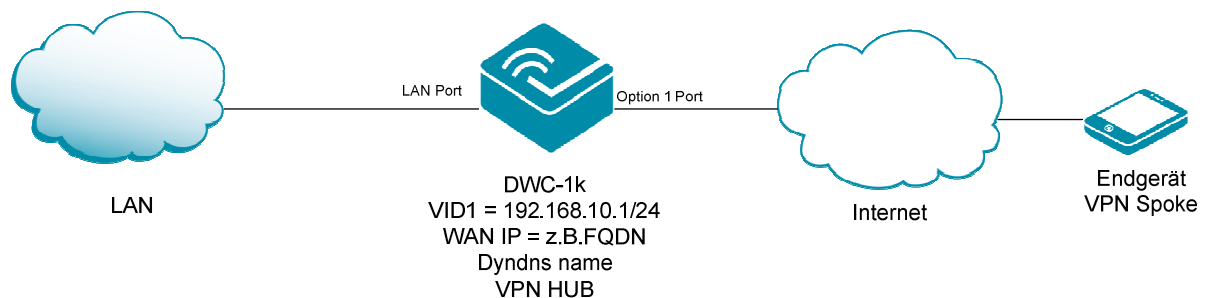
# HowTo: Einrichtung von L2TP over IPSec VPN

## [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.

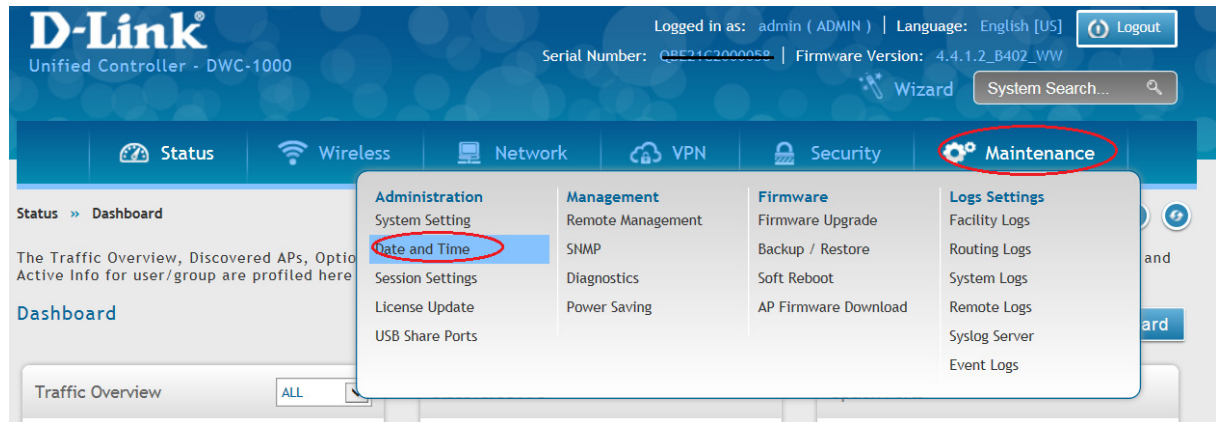


[Vorbereitung]

- ⇒ 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 (<ftp://ftp.dlink.de/dwc/dwc-1000/documentation/> ) nach
- ⇒ Stellen Sie bitte sicher, dass Sie die aktuellste Firmware für den DWC-1000 installiert haben ([ftp://ftp.dlink.de/dwc/dwc-1000/driver\\_software/](ftp://ftp.dlink.de/dwc/dwc-1000/driver_software/) )
- ⇒ 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

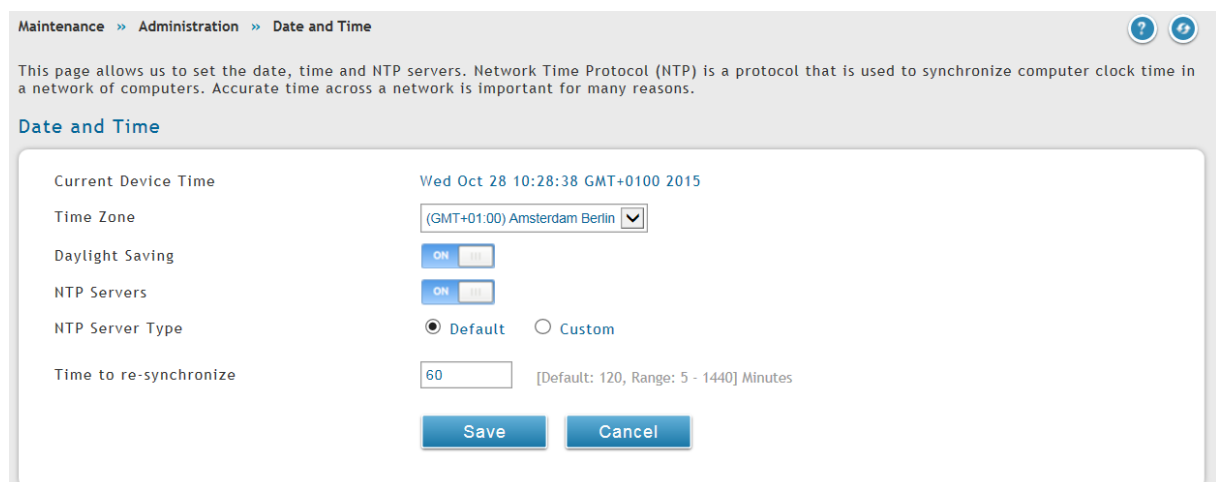
## [Einrichtung der korrekten Systemzeit]

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



Passen Sie die bei Ihnen gültigen Zeiteinstellungen an

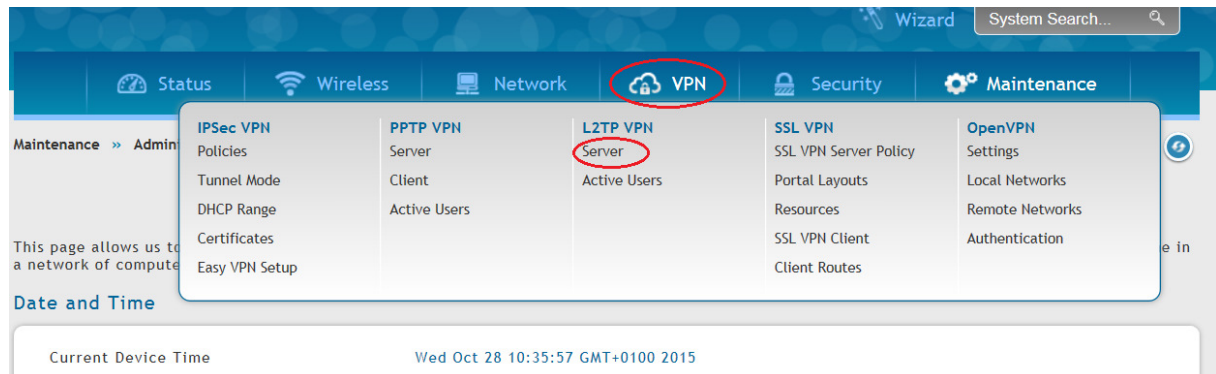
- a. Time Zone = z.B. GMT +1 Berlin (in Deutschland)
- b. Daylight Saving = aktivieren Sommer/Winterzeit
- c. NTP Server = Network Time Server aktivieren
  - i. Default = vorgegebene Server
  - ii. Custom = hier haben Sie die Möglichkeit 2 eigene Zeitserver einzutragen
- d. Time to Synchronize = Zeit zwischen 2 Synchronisierungsabläufen (eine zu geringe Zeitspanne kann je nach Konfiguration des Servers zu Fehlern/Sperrungen des Client führen)



Mittels Save speichern Sie Ihre Eingaben.

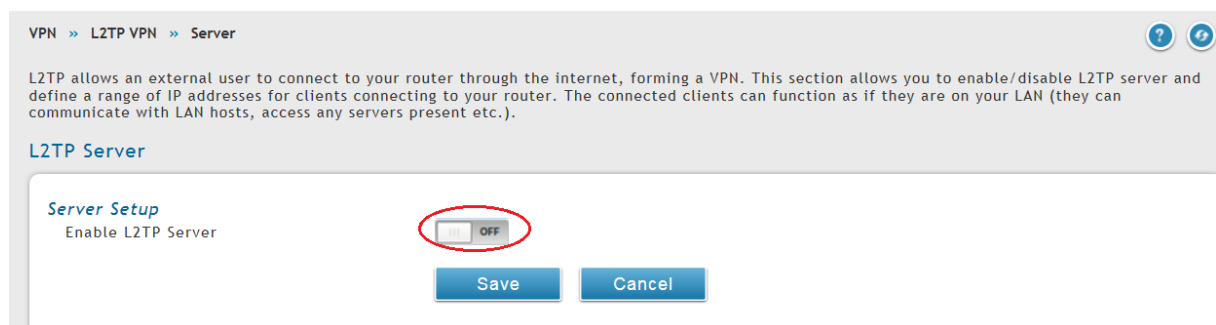
## [Einrichtung der L2TP VPN]

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



### 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
- c. Range of IP Addresses = IP Adressbereich der den Clients zugewiesen wird, dieser IP Bereich darf in Ihrem Netzwerk noch nicht verwendet/vergeben sein
- d. Authentication 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

L2TP allows an external user to connect to your router through the internet, forming a VPN. This section allows you to enable/disable L2TP server and define a range of IP addresses for clients connecting to your router. The connected clients can function as if they are on your LAN (they can communicate with LAN hosts, access any servers present etc.).

**L2TP Server**

**Server Setup**

Enable L2TP Server  ON  OFF

L2TP Routing Mode  Nat  Classical

**Range of IP Addresses (Allocated to L2TP Clients)**

Starting IP Address

Ending IP Address

**Authentication Supported**

PAP  ON  OFF

CHAP  ON  OFF

MS-CHAP  OFF

MS-CHAPv2  OFF

Secret Key  OFF

**User Time-out**

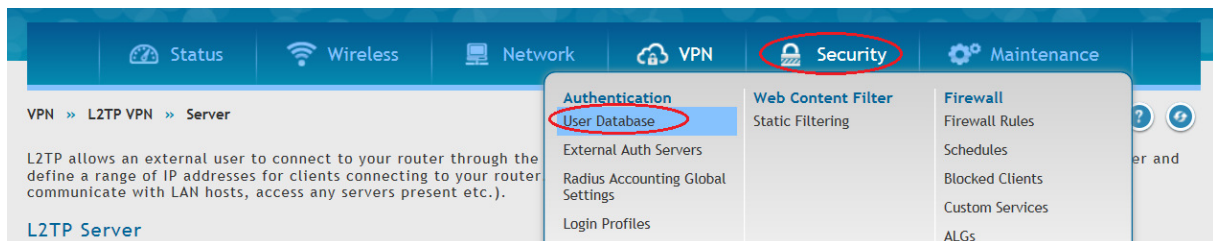
Idle TimeOut  [Range: 300 - 1800] Seconds

**Netbios Setup**

Netbios  OFF

Mittels Save speichern Sie Ihre Eingaben.

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



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

Security » Authentication » User Database » Groups

Get User DB  Users MAC Authentication

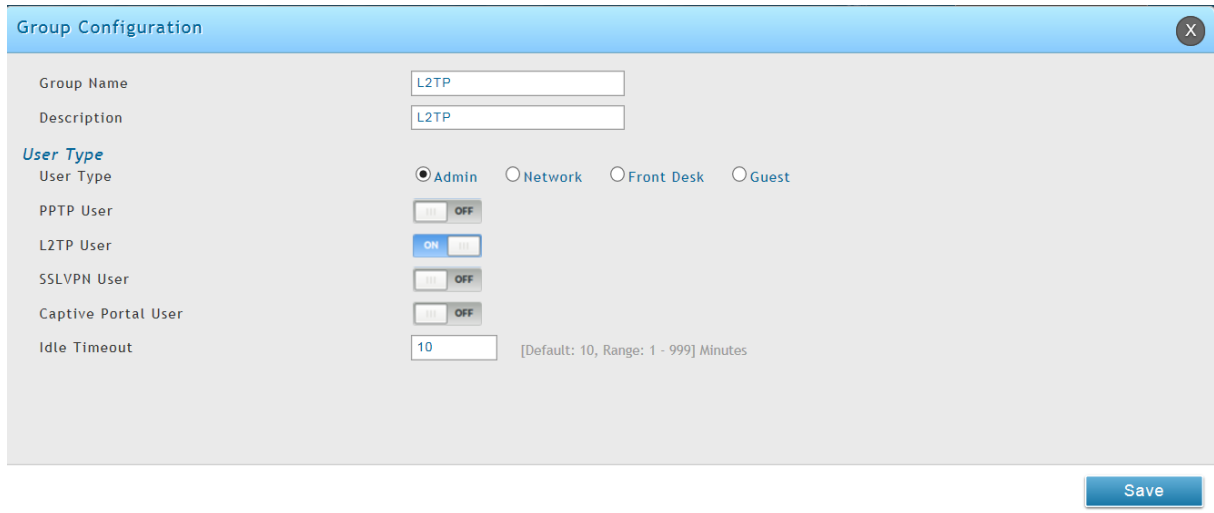
This page shows the list of added groups to the router. The user can add, delete and edit the groups also.

**Groups List**

Show  entries [Right click on record to get more options]

Group Name	Description
ADMIN	AdminGroup
GUEST	GuestGroup

Showing 1 to 2 of 2 entries



Group Configuration

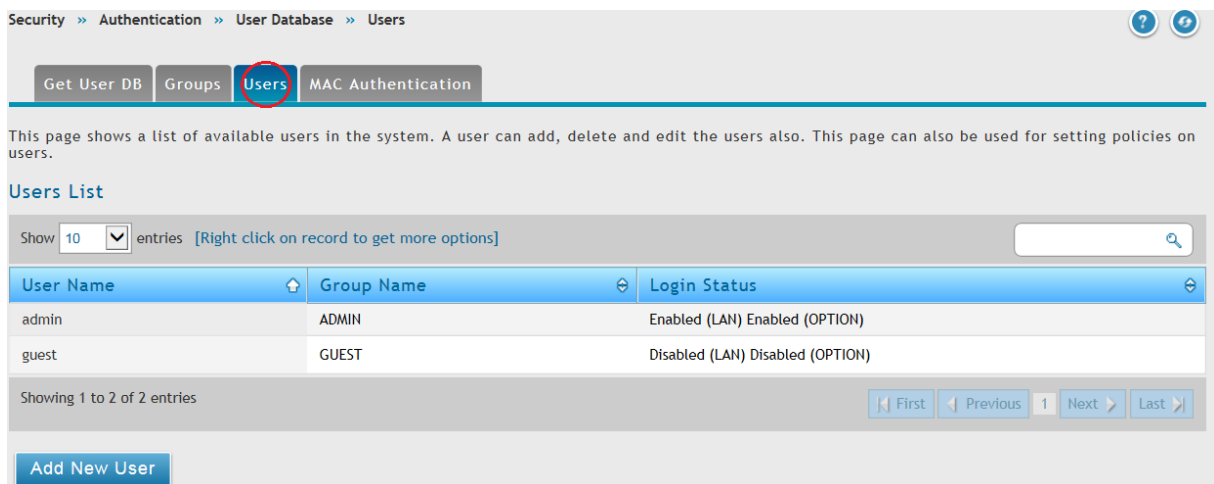
Group Name: L2TP  
Description: L2TP

User Type:  Admin  Network  Front Desk  Guest

PPTP User:  ON  OFF  
L2TP User:  ON  OFF  
SSLVPN User:  ON  OFF  
Captive Portal User:  ON  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 Database >> Users

Get User DB Groups **Users** MAC Authentication

This page shows a list of available users in the system. A user can add, delete and edit the users also. This page can also be used for setting policies on users.

Users List

Show 10 entries [Right click on record to get more options]

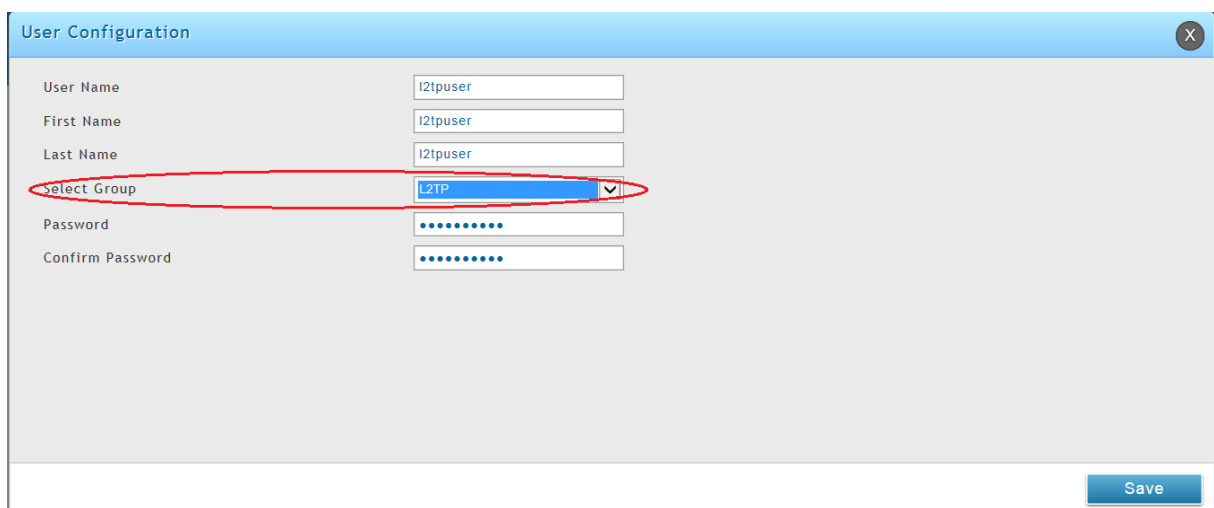
User Name	Group Name	Login Status
admin	ADMIN	Enabled (LAN) Enabled (OPTION)
guest	GUEST	Disabled (LAN) Disabled (OPTION)

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.



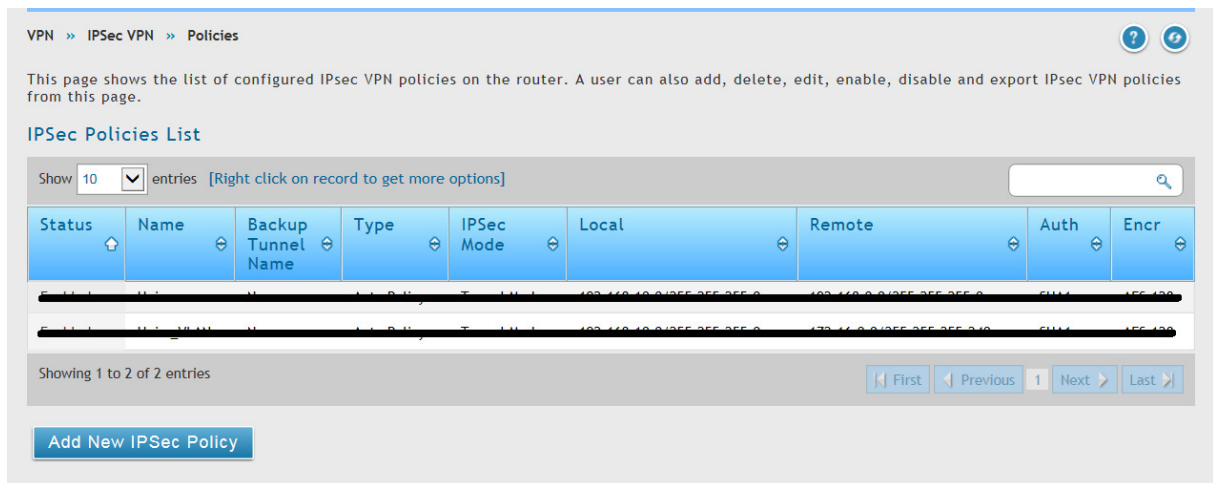
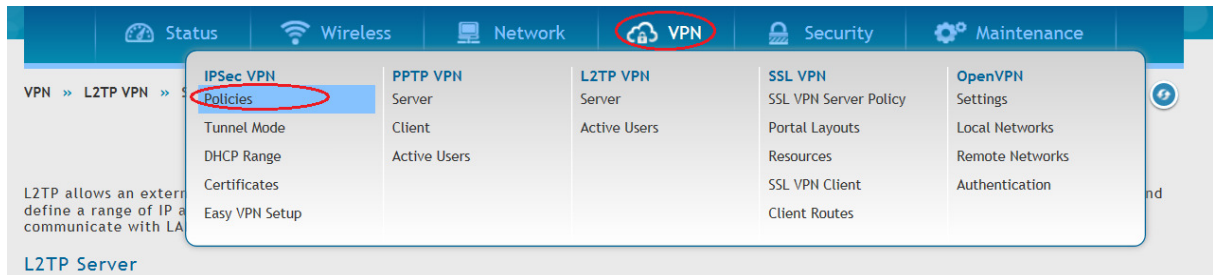
User Configuration

User Name: i2tpuser  
First Name: i2tpuser  
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“



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
  - a. **Tunnel** = Tunnel verbindet zwei Netze über zwei Router
  - 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
  - b. FQDN = Full Qualified Domain Name, z.B. DynDNS Name der 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 RollOver: OFF

Save

- 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**

Enable NetBIOS: OFF

Enable RollOver: OFF

Protocol: ESP

Enable DHCP: OFF

Local IP: Any

Remote IP: Any

Enable Keepalive: OFF

**Phase 1(IKE SA Parameters)**

Exchange Mode: Main

Direction / Type: Both

Nat Traversal: ON

Local Identifier Type: Local Wan IP

Save

## PHASE 1

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



- l. Local Identifier Type = Indetifikator**
  - a. Local WAN IP** = lokale WAN IP, wird automatisch eingetragen
  - b. FQDN** = lokaler FQDN, bei Site-to-Site VPN Notwendig
  - c. User FQDN** = lokaler eigener FQDN
  - d. DER ASN1 DN** = DER ASN1 DN Zertifikat
- m. Remote Identifier**
  - a. Remote WAN IP** = remote WAN IP, wird automatisch eingetragen
  - b. FQDN** = remote FQDN, bei Site-to-Site VPN Notwendig
  - c. User FQDN** = remote eigener FQDN
  - d. DER ASN1 DN** = DER ASN1 DN Zertifikat

The screenshot shows the 'IPSec Policy Configuration' window. Under 'Phase 1 (IKE SA Parameters)', the 'Exchange Mode' is set to 'Main', 'Direction / Type' is 'Both', 'Nat Traversal' is 'ON', 'Local Identifier Type' is 'Local Wan IP', and 'Remote Identifier Type' is 'Remote Wan IP'. Under 'Encryption Algorithm', the following algorithms are listed with their status: DES (OFF), 3DES (OFF), AES-128 (ON), AES-256 (OFF), BLOWFISH (OFF), and CAST128 (OFF). A red oval highlights the right side of the configuration area.

- 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

The screenshot shows the 'IPSec Policy Configuration' window. Under 'Remote Identifier Type', it is set to 'Remote Wan IP'. Under 'Encryption Algorithm', the following algorithms are listed with their status: DES (OFF), 3DES (ON), AES-128 (ON), AES-256 (OFF), BLOWFISH (OFF), and CAST128 (OFF). Under 'Authentication Algorithm', the following algorithms are listed with their status: MD5 (OFF), SHA-1 (ON), SHA2-256 (OFF), SHA2-384 (OFF), and SHA2-512 (OFF). The 'Authentication Method' is set to 'Pre-Shared Key'. A red oval highlights the right side of the configuration area.

- p. Authentication Method = Authentifizierungsmethode
  - a. PSK = Standard ist Passwort (PreSharedKey)
  - b. RSA Signature = 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 = definiert die Zeit bis ein neuer Schlüssel generiert wird
- s. Extended Authentication = weitergehende Authentifizierungsmethoden, wie z.B. Benutzername/Passwort

The screenshot shows the 'IPsec Policy Configuration' window. It includes the following settings:

- 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)

## PHASE 2

- t. SA Lifetime = definiert die Zeit bis ein neuer Schlüssel generiert wird
- u. Encryption Algorithm = Verfügbare Verschlüsselungsmechanismen, 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

The screenshot shows the 'IPsec Policy Configuration' window with the following settings:

- Extended Authentication: None
- Phase2-(Auto Policy Parameters) SA Lifetime: 3600 Seconds
- Encryption Algorithm:
  - DES: OFF
  - 3DES: OFF
  - AES-192: OFF
  - AES-CCM: OFF
  - TWOFISH (128): OFF
  - TWOFISH (256): OFF
  - BLOWFISH: OFF
  - CAST128: OFF
  - NONE: OFF
  - AES-128: ON
  - AES-256: OFF
  - AES-GCM: OFF
  - TWOFISH (192): OFF

**IPSec Policy Configuration** X

3DES <input type="checkbox"/>	AES-128 <input type="checkbox"/>
AES-192 <input type="checkbox"/>	AES-256 <input type="checkbox"/>
AES-CCM <input type="checkbox"/>	AES-GCM <input type="checkbox"/>
TWOFISH (128) <input type="checkbox"/>	TWOFISH (192) <input type="checkbox"/>
TWOFISH (256) <input type="checkbox"/>	
BLOWFISH <input type="checkbox"/>	
CAST128 <input type="checkbox"/>	
<i>Integrity Algorithm</i>	
MD5 <input type="checkbox"/>	SHA-1 <input type="checkbox"/>
SHA2-224 <input type="checkbox"/>	SHA2-256 <input type="checkbox"/>
SHA2-384 <input type="checkbox"/>	SHA2-512 <input type="checkbox"/>
PFS Key Group <input type="checkbox"/>	

**Save**

Mittels Save speichern Sie Ihre Eingaben.

VPN » 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 Policies List**

Show  entries [\[Right click on record to get more options\]](#)

Status	Name	Backup Tunnel Name	Type	IPSec Mode	Local	Remote	Auth	Encr
Enabled	VPN-HUB*	None	Auto Policy	Tunnel Mode	Any	Any	SHA1	3DES AES-128

Showing 1 to 3 of 3 entries First Previous 1 Next Last

Konfigurieren Sie nun Ihr Endgerät nach den Herstellervorgaben des Endgerätes.

## Prüfung am DWC-1000

⇒ Aktiver L2TP User

The screenshot shows the D-Link VPN configuration interface. The 'VPN' menu is selected, and the 'L2TP VPN' sub-menu is active. The 'Active Users' option is highlighted. Below the navigation menu, a table displays the active L2TP users. A red circle highlights the table header and the first row.

User Name	Remote IP	L2TP IP
l2tpuser	192.168.100.11	192.168.100.10

Showing 1 to 1 of 1 entries

⇒ Aktive SSLVPN Session

The screenshot shows the D-Link Status page. The 'Status' menu is selected, and the 'Active VPNs' option is highlighted. Below the navigation menu, a table displays the active VPN sessions. A red circle highlights the table header and the first row.

Policy Name	Endpoint	Lx (KB)	Lx (Packets)	Configuration State
109.84.1.234*	109.84.1.234	2.15	21	IPsec SA Established
...	...	0.59	4	IPsec SA Established
...	...	2.81	24	IPsec SA Established

Showing 1 to 3 of 3 entries