

HowTo: Einrichtung einer IPSec Verbindung mit einem IPSEC VPN Client zum DWC-1000 am Beispiel der "Shrewsoft" VPN Clientsoftware

[Voraussetzungen]

1. DWC-1000 mit Firmware Version: 4.2.0.3_B502 und höher 2. VPN Lizenz

[Szenario]

Ein Client soll sich per "Shrewsoft" VPN Client mit IPSec auf den DWC-1000 verbinden.





[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/DWC-1000_HowTo/</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>)
- ⇒ Bitte lesen Sie vorab das Handbuch und die bereits vorhandenen Anleitungen um die grundlegende Konfiguration des DWC-1000 zu erledigen.
- ⇒ Den "Shrewsoft" VPN Client können Sie unter folgender Adresse herunterladen <u>https://www.shrew.net/</u>
- ⇒ Der "Shrewsoft" VPN Client ist eine kostenfreie Alternative zu einem NCP-Client



- 1.) Einrichtung der IPsec Policies
- 2.) Konfiguration der IPsec Mode Konfiguration
- 3.) Anlegen einer Benutzerdatenbank
- 4.) Anlegen eines IPsec Benutzers
- 5.) Konfiguration des Shrewsoft Client
- 1.) Einrichtung der IPsec Policies
 Öffen Sie die Menüpunkt IPsec Policies:
 (>Setup > VPN Settings > IPsec > IPsec Policies:

Product Page: DWC-1000							Ha	rdware Versio	n: A1 Firn	ware Version: 4.2.0.3_B604_WW
D-Li	nk									
DWC-1000	SETU	IP	ADVANCED		тоо	LS		STATUS		HELP
Wizard •										Helpful Hints
WLAN Global Settings	IPSEC POLICIES	\$							LOGOUT	An IPsec VPN can be established over the
AP Management	This page shows the policies from this p	he list of config	ured IPsec VPN policies on the	router. A us	ser can also a	add, delete, er	dit, enable an	d disable IPse	C VPN	internet by configuring the appropriate policy here.
WLAN Visualization 🕨									_	You need to have matching parameters for
Internet Settings	List of VPN Policies both the connecting peers. Some important peers for a set of the connecting peers of the formation of th									
Network Settings	Status	Name	Backup Tunnel Name	Type	TReec M	ode Lo	ral Rem	ote Aut	Encr	connection, Encryption
QoS 🕨	Manual Policy	name	backup runner wante	Type	Irsec H	ode Lo	Lai Kelli	ole Aut	Elicr	communication etc.) are displayed here.
GVRP	r turiaur r olicy	5 In .								More
Captive Portal	ļ	Edit	Enable Disab	le l	Jelete	Add	Expo	ort		
External	List of back up	Policies								
Authentications	Status	Name	Primary Tunnel Nam	ie	Туре	Local	Remote	Auth	Encr	
VPN Settings D	IPsec	IPsec	Policies							
VLAN Settings	PPTP	▶ IPsec	ModeConfig							
DMZ Setup	L2TP	► DHCF	P Range							
USB Settings	SSL VPN Server	•								
WIRELESS CO	SSL VPN Client	•								
	OpenVPN	•	Copyright	© 2012 D-Lir	nk Corporatio	on.				

Erstellen Sie eine neue Policy über die Schaltfläche "Add":

froducer age. Dive 1000				<u> </u>				and the second	UN AL TIN	Marc version: 1.2.0.5_0001_000
D-Liı	nk									
DWC-1000	SE	rup	ADVANCED		тос	DLS		STATUS		HELP
Wizard +										Helpful Hints
WLAN Global Settings	IPSEC POLICI	ES							LOGOUT	An IPsec VPN can be established over the
AP Management 🕨	This page shows	the list of confi	igured IPsec VPN policies on the	router. A us	er can also	add, delete,	edit, enable an	d disable IPse	ec VPN	internet by configuring the appropriate policy here.
WLAN Visualization 🔸	You need to have matching parameters for									
Internet Settings	List of VPN Policies both the connecting peers. Some important									
Network Settings	Auto Policy parameters (Type of the cornection, Encryption									
QoS 🕨	Manual Policy	name	backup runnername	Type	If Sec 1		ocar Ren	INCE AN	ai Elici	communication etc.) are displayed here.
GVRP		E In								More
Captive Portal		Edit	Enable Disab	D D	Jerete	Add	Exp	ort		
External	List of back u	p Policies				A	dd			
Autrentications	Status	Name	Primary Tunnel Nam	e	Туре	Local	Remote	Auth	Encr	
VPN Settings										
VLAN Settings										
DMZ Setup										
USB Settings										
WIRELESS CO	NTROLLER	२								



Konfigurieren Sie die allgemeinen Einstellungen wie folgend:

Vergeben Sie der Policy einen Namen.

Wichtiger Hinweis: Der Policy Name kann nachträglich nicht geändert werden.

General		
Policy Name:	IPSec-Shrewsoft	Namen eintragen
Policy Type:	Auto Policy 🗸	
IP Protocol Version:	IPv4 IPv6	
IKE Version:	IKEv1 IKEv2	
IPsec Mode:	Tunnel Mode 👻	
Select Local Gateway:	Option1 👻	
Remote Endpoint:	FQDN 👻	
	0.0.0.0	
Enable Mode Config:		
Enable NetBIOS:		
Enable RollOver:		
Protocol:	ESP 👻	
Enable DHCP:		
Local IP:	Subnet 👻	
Local Start IP Address:	192.168.10.0	
Local End IP Address:		
Local Subnet Mask:	255.255.255.0	
Local Prefix Length:		
Remote IP:	Any 👻	
Remote Start IP Address:		
Remote End IP Address:		
Remote Subnet Mask:		
Remote Prefix Length:		
Enable Keepalive:		
Source IP Address:		
Destination IP Address:		
Detection Period:	10	
Reconnect After Failure Count:	3	

Belassen Sie den Policy Type auf: "Auto Policy" IP Protocol Version auf: IPv4 IKE Version: IKEv1 IPsec Mode: Tunnel Mode Select Local Gateway: Option 1



Als Remote Endpoint wählen Sie bitte "FQDN" aus und tragen "0.0.0.0" ein:

General	
Policy Name:	IPSec-Shrewsoft
Policy Type:	Auto Policy 👻
IP Protocol Version:	IPv4 IPv6
IKE Version:	IKEv1 IKEv2
IPsec Mode:	Tunnel Mode 🗸
Select Local Gateway:	Option1 -
Remote Endpoint:	FQDN FQDN FUlly Qualified Domain Name
	0.0.0.0 stellen und "0.0.0.0" eintragen
Enable Mode Config:	
Enable NetBIOS:	
Enable RollOver:	
Protocol:	ESP 👻
Enable DHCP:	
Local IP:	Subnet 👻
Local Start IP Address:	192.168.10.0
Local End IP Address:	
Local Subnet Mask:	255.255.255.0
Local Prefix Length:	
Remote IP:	Any 🗸
Remote Start IP Address:	
Remote End IP Address:	
Remote Subnet Mask:	
Remote Prefix Length:	
Enable Keepalive:	
Source IP Address:	
Destination IP Address:	
Detection Period:	10
Reconnect After Failure Count:	3



Aktivieren Sie "Enable Mode Config":

General	
Policy Name:	IPSec-Shrewsoft
Policy Type:	Auto Policy 👻
IP Protocol Version:	IPv4 IPv6
IKE Version:	IKEv1 KEv2
IPsec Mode:	Tunnel Mode 🗸
Select Local Gateway:	Option1 -
Remote Endpoint:	FQDN -
	0.0.0.0
Enable Mode Config:	Enable Mode Config aktivieren
Enable NetBIOS:	
Enable RollOver:	
Protocol:	ESP 👻
Enable DHCP:	
Local IP:	Subnet 👻
Local Start IP Address:	192.168.10.0
Local End IP Address:	
Local Subnet Mask:	255.255.255.0
Local Prefix Length:	
Remote IP:	Any 🗸
Remote Start IP Address:	
Remote End IP Address:	
Remote Subnet Mask:	
Remote Prefix Length:	
Enable Keepalive:	
Source IP Address:	
Destination IP Address:	
Detection Period:	10
Reconnect After Failure Count:	3



Wählen Sie bitte bei Local IP: "Subnet", tragen Sie als Local Start IP Address: "192.168.10.0" ein, und als Local Subnet Mask tragen Sie die "255.255.255.0" ein.(*)

General		
Policy Name:	IPSec-Shrewsoft	
Policy Type:	Auto Policy 🗸	
IP Protocol Version:	IPv4 IPv6	
IKE Version:	IKEv1 IKEv2	
IPsec Mode:	Tunnel Mode 🗸	
Select Local Gateway:	Option1 👻	
Remote Endpoint:	FQDN -	
	0.0.0.0	
Enable Mode Config:		
Enable NetBIOS:		
Enable RollOver:		
Protocol:	ESP 👻	
Enable DHCP:		0.0000000000000000000000000000000000000
Local IP:	Subnet - Angabe des L hier: 192.168.	okalen Subnetzes, 10.0/24
Local Start IP Address:	192.168.10.0	
Local End IP Address:		
Local Subnet Mask:	255.255.255.0	
Local Prefix Length:		
Remote IP:	Any 👻	
Remote Start IP Address:		
Remote End IP Address:		
Remote Subnet Mask:		
Remote Prefix Length:		
Enable Keepalive:		
Source IP Address:		
Destination IP Address:		
Detection Period:	10	
Reconnect After Failure Count:	3	

(*) Sollte der DWC-1000 ein anderes lokales Subnetz verwenden, ändern Sie bitte die Local Start IP Address sowie die Local Subnet Mask entsprechend.



Als Remote IP wählen Sie bitte "Any":

General	
Policy Name:	IP Sec-Shrewsoft
Policy Type:	Auto Policy 🗸
IP Protocol Version:	ІРv4 Прv6 Ірv6
IKE Version:	IKEv1 IKEv2
IPsec Mode:	Tunnel Mode 🗸
Select Local Gateway:	Option 1 👻
Remote Endpoint:	FQDN -
	0.0.0.0
Enable Mode Config:	
Enable NetBIOS:	
Enable RollOver:	
Protocol:	ESP -
Enable DHCP:	
Local IP:	Subnet 👻
Local Start IP Address:	192.168.10.0
Local End IP Address:	
Local Subnet Mask:	255.255.255.0
Local Prefix Length:	
Remote IP:	Any 🗸 Remote IP auf "Any" stellen
Remote Start IP Address:	
Remote End IP Address:	
Remote Subnet Mask:	
Remote Prefix Length:	
Enable Keepalive:	
Source IP Address:	
Destination IP Address:	
Detection Period:	10
Reconnect After Failure Count:	3



Übersicht der allgemeinen Einstellungen:

eneral	
Policy Name:	IPSec-Shrewsoft
Policy Type:	Auto Policy 👻
IP Protocol Version:	IPv4 IPv6
IKE Version:	IKEv1 KEv2
IPsec Mode:	Tunnel Mode 🛛 👻
Select Local Gateway:	Option1 👻
Remote Endpoint:	FQDN 👻
	0.0.0.0
Enable Mode Config:	
Enable NetBIOS:	
Enable RollOver:	
Protocol:	ESP 👻
Enable DHCP:	
Local IP:	Subnet 👻
Local Start IP Address:	192.168.10.0
Local End IP Address:	
Local Subnet Mask:	255.255.255.0
Local Prefix Length:	
Remote IP:	Any 🗸
Remote Start IP Address:	
Remote End IP Address:	
Remote Subnet Mask:	
Remote Prefix Length:	
Enable Keepalive:	
Source IP Address:	
Destination IP Address:	
Detection Period:	10
Reconnect After Failure Count:	3



Konfiguration der Phase1:

Wählen Sie als Local Identifier Type: "Local Wan IP" aus.

Phase1(IKE SA Parameters)	
Exchange Mode:	Main 👻
Direction / Type:	Both
Nat Traversal:	
On:	۲
Off:	0
NAT Keep Alive Frequency (in seconds):	20
Local Identifier Type:	Local Wan IP Local Identifier Type auf: Local WAN IP" stellen
Local Identifier:	
Remote Identifier Type:	Remote Wan IP 🔻
Remote Identifier:	
Encryption Algorithm:	
DES:	
3DES:	
AES-128:	
AES-192:	
AES-256:	
BLOWFISH:	
CAST128:	
Authentication Algorithm:	
MD5:	
SHA-1:	
SHA2-256:	
SHA2-384:	
SHA2-512:	
Authentication Method:	Pre-shared key 🔻
Pre-shared key:	IPSecKey2013
Diffie-Hellman (DH) Group:	Group 5 (1536 bit) 👻
SA-Lifetime (sec):	28800
Enable Dead Peer Detection:	
Detection Period:	10
Reconnect after failure count:	3

Belassen Sie die voreingestellten Optionen für: Exchange Mode: "Main" Direction/Type: "Both" NAT Traversal "On" NAT Keep Alive "20"



Bei Remote Identifier Type wählen Sie "Remote Wan IP":

Phase1(IKE SA Parameters)	
Exchange Mode:	Main 👻
Direction / Type:	Both 💌
Nat Traversal:	
On:	۲
Off:	0
NAT Keep Alive Frequency (in seconds):	20
Local Identifier Type:	Local Wan IP 🔻
Local Identifier:	
Remote Identifier Type:	Remote Wan IP
Remote Identifier:	Remote WAN IP stellen
Encryption Algorithm:	
DES:	
3DES:	
AES-128:	
AES-192:	
AES-256:	
BLOWFISH:	
CAST128:	
Authentication Algorithm:	
MD5:	
SHA-1:	
SHA2-256:	
SHA2-384:	
SHA2-512:	
Authentication Method:	Pre-shared key 💌
Pre-shared key:	IPSecKey2013
Diffie-Hellman (DH) Group:	Group 5 (1536 bit) 🔹
SA-Lifetime (sec):	28800
Enable Dead Peer Detection:	
Detection Period:	10
Reconnect after failure count:	3



Als Encryption Algorithm wählen Sie bitte AES-256 aus:

Phase1(IKE SA Parameters)		
Exchange Mode:	Main 👻	
Direction / Type:	Both 💌	
Nat Traversal:		
On:	۲	
Off:	\odot	
NAT Keep Alive Frequency (in seconds):	20	
Local Identifier Type:	Local Wan IP 🔻	
Local Identifier:		
Remote Identifier Type:	Remote Wan IP 💌	
Remote Identifier:		_
Encryption Algorithm:		Encryption Algorithm
DES:		konfigurieren:
3DES:		
AES-128:		
AES-192:		Auswahl von AES-256
AES-256:		
BLOWFISH:		
CAST128:		
CAST128: Authentication Algorithm:		
CAST128: Authentication Algorithm: MD5:		
CAST128: Authentication Algorithm: MD5: SHA-1:		
CAST128: Authentication Algorithm: MD5: SHA-1: SHA2-256:		
CAST128: Authentication Algorithm: MD5: SHA-1: SHA2-256: SHA2-384:		
CAST128: Authentication Algorithm: MD5: SHA-1: SHA2-256: SHA2-384: SHA2-512:		
CAST128: Authentication Algorithm: MD5: SHA-1: SHA2-256: SHA2-384: SHA2-512: Authentication Method:	 ✓ Pre-shared key ▼ 	
CAST128: Authentication Algorithm: MD5: SHA-1: SHA2-256: SHA2-384: SHA2-512: Authentication Method: Pre-shared key:	Pre-shared key V IPSecKey2013	
CAST128: Authentication Algorithm: MD5: SHA-1: SHA2-256: SHA2-384: SHA2-384: SHA2-512: Authentication Method: Pre-shared key: Diffie-Hellman (DH) Group:	 ✓ ✓ Pre-shared key ▼ IPSecKey2013 Group 5 (1536 bit) ▼ 	
CAST128: Authentication Algorithm: MD5: SHA-1: SHA2-256: SHA2-384: SHA2-512: Authentication Method: Pre-shared key: Diffie-Hellman (DH) Group: SA-Lifetime (sec):	Pre-shared key V IPSecKey2013 Group 5 (1536 bit) V	
CAST128: Authentication Algorithm: MD5: SHA-1: SHA2-256: SHA2-384: SHA2-384: SHA2-512: Authentication Method: Pre-shared key: Diffie-Hellman (DH) Group: SA-Lifetime (sec): Enable Dead Peer Detection:	 ✓ ✓ Pre-shared key ▼ IPSecKey2013 Group 5 (1536 bit) ▼ 28800 	
CAST128: Authentication Algorithm: MD5: SHA-1: SHA2-256: SHA2-384: SHA2-384: SHA2-512: Authentication Method: Pre-shared key: Diffie-Hellman (DH) Group: SA-Lifetime (sec): Enable Dead Peer Detection: Detection Period:	 □ □	



Als Authentication Algorithm wählen Sie "SHA-1":

Phase1(IKE SA Parameters)		
Exchange Mode:	Main 🔻	
Direction / Type:	Both 🔻	
Nat Traversal:		
On:	۲	
Off:	0	
NAT Keep Alive Frequency (in seconds):	20	
Local Identifier Type:	Local Wan IP 🔻	
Local Identifier:		
Remote Identifier Type:	Remote Wan IP 💌	
Remote Identifier:		
Encryption Algorithm:		
DES:		
3DES:		
AES-128:		
AES-192:		
AES-256:	\checkmark	
BLOWFISH:		T
CAST128:		
Authentication Algorithm:		Authentication Algorithm
MD5:		konfigurieren:
SHA-1:		mer snærr auswamen
SHA2-256:		
SHA2-384:		
SHA2-512:		
Authentication Method:	Pre-shared key 💌	
Pre-shared key:	IPSecKey2013	
Diffie-Hellman (DH) Group:	Group 5 (1536 bit) 🔹	
SA-Lifetime (sec):	28800	
Enable Dead Peer Detection:		
Detection Period:	10	
Reconnect after failure count:	3	



Als "Authentication Method" wählen Sie "Pre-shared Key" und vergeben Sie einen Pre-shared Key, hier: "IPSecKey2013":

Phase1(IKE SA Parameters)	
Exchange Mode:	Main 💌
Direction / Type:	Both
Nat Traversal:	
On:	۲
Off:	0
NAT Keep Alive Frequency (in seconds):	20
Local Identifier Type:	Local Wan IP 👻
Local Identifier:	
Remote Identifier Type:	Remote Wan IP 💌
Remote Identifier:	
Encryption Algorithm:	
DES:	
3DES:	
AES-128:	
AES-192:	
AES-256:	
BLOWFISH:	
CAST128:	
Authentication Algorithm:	
MD5:	
SHA-1:	
SHA2-256:	
SHA2-384:	
SHA2-512:	
Authentication Method:	Pre-shared key Authentication Method auf "Pre-shared Key" stellen und
Pre-shared key:	IPSecKey2013 den Pre-shared Key eintragen
Diffie-Hellman (DH) Group:	Group 5 (1536 bit) 🗸
SA-Lifetime (sec):	28800
Enable Dead Peer Detection:	
Detection Period:	10
Reconnect after failure count:	3



Als Diffie-Hellman Group wählen Sie "Group 5 (1536 Bit)" und setzen die SA-Lifetime auf "28800" Sekunden:

Phase1(IKE SA Parameters)	
Exchange Mode:	Main 👻
Direction / Type:	Both 💌
Nat Traversal:	
On:	۲
Off:	0
NAT Keep Alive Frequency (in seconds):	20
Local Identifier Type:	Local Wan IP 🔻
Local Identifier:	
Remote Identifier Type:	Remote Wan IP 💌
Remote Identifier:	
Encryption Algorithm:	
DES:	
3DES:	
AES-128:	
AES-192:	
AES-256:	
BLOWFISH:	
CAST128:	
Authentication Algorithm:	
MD5:	
SHA-1:	
SHA2-256:	
SHA2-384:	
SHA2-512:	
Authentication Method:	Pre-shared key 💌
Pre-shared key:	IPSecKey2013
Diffie-Hellman (DH) Group:	Group 5 (1536 bit)
SA-Lifetime (sec):	28800 SA-Lifetime auf 28800 Sekunden
Enable Dead Peer Detection:	
Detection Period:	10
Reconnect after failure count:	3

Als Extended Authentication wählen Sie "Edge Device" und bei Authentication Type: "User Database":

Extended Authentication:	Edge Device 💌	Extended Authentication für XAuth
Authentication Type:	User Database 🔻	Authentication Type zeigt auf die
Username:		User Database (XAuth)
Password:		1



Konfiguration der Phase2:

Festlegen der SA Lifetime auf "3600" Sekunden:

SA Lifetime:	3600	Seconds -	SA Lifetime auf 3600
Encryption Algorithm:			Sekunden stellen
DES:			
NONE:			
3DES:			
AES-128:			
AES-192:			
AES-256:			
AES-CCM:			
AES-GCM:			
TWOFISH (128):			
TWOFISH (192):			
TWOFISH (256):			
BLOWFISH:			
CAST128:			
Integrity Algorithm:			
MD5:			
SHA-1:			
SHA2-224:			
SHA2-256:			
SHA2-384:			
SHA2-512:			
PFS Key Group:	DH Group	5 (1536 bit) 🔻	



Phase2-(Auto Policy Parameters) 3600 Seconds 💌 SA Lifetime: Encryption Algorith konfigurieren, hier auf: Encryption Algorithm: DES: NONE: 3DES: AES-128: AES-192: AES-256 stellen. AES-256: V AES-CCM: AES-GCM: TWOFISH (128): TWOFISH (192): TWOFISH (256): BLOWFISH: CAST128: Integrity Algorithm: MD5: V SHA-1: SHA2-224: SHA2-256: SHA2-384: SHA2-512: [1] ☑ DH Group 5 (1536 bit) ▼ PFS Key Group:

Konfiguration des Encryption Algorithm, auch hier wählen Sie "AES-256" aus:

Für den Integrity Algorithm wählen Sie "SHA-1":

A Lifetime:	3600 Seconds -
ncryption Algorithm:	
DES:	
IONE:	
BDES:	
AES-128:	
AES-192:	
AES-256:	
AES-CCM:	
ES-GCM:	
WOFISH (128):	
WOFISH (192):	
WOFISH (256):	
LOWFISH:	
AST128:	
ntegrity Algorithm:	Integrity Algorithm konfigurieren, hier
1D5:	SHA_1
SHA-1:	
HA2-224:	
HA2-256:	
HA2-384:	
SHA2-512:	
FS Key Group:	☑ DH Group 5 (1536 bit) ▼



Aktivieren Sie PFS (Perfect Forward Secrecy) und wählen Sie die Diffie Hellman Group "DH Group 5 (1536 Bit)":

SA Lifetime:	3600	Seconds 👻	
Encryption Algorithm:			
DES:			
NONE:			
3DES:			
AES-128:			
AES-192:			
AES-256:			
AES-CCM:			
AES-GCM:			
TWOFISH (128):			
TWOFISH (192):			
TWOFISH (256):			
BLOWFISH:			
CAST128:			
Integrity Algorithm:			
MD5:			
SHA-1:			
SHA2-224:			
SHA2-256:			
SHA2-384:			
SHA2-512:		DEC alute from	



2.) Konfiguration der IPsec Mode Konfiguration
 Öffnen Sie die Einstellungen zu IPsec Mode Config.
 >Setup >VPN Settings > IPsec > IPsec Mode Config

D-Li	nk				
DWC-1000	SETUP	ADVANCE	D	TOOLS	STATUS
Wizard					
WLAN Global Settings	IPSEC MODE CONFIG				LOGOUT
AP Management 🕨	This page allows you to de	fine the IP address range for o	lients connec	ting using Mode Config.	
WLAN Visualization 🕨	Save Settings	Don't Save Settings			
Internet Settings	Insec Mode Config Co	nfiguration			
Network Settings	Tunnel Mode	mgulation	Full Tr	innel 👻	
QoS 🕨	Start ID Addross		192.1	S8 12 100	
GVRP	Start IP Address.		102.1	0.12.100	
Captive Portal	End IP Address:		192.10	58.12.199	
External	Primary DNS(Option	ial):	8.8.8.	3	
VBN Cettinge	Secondary DNS(Opt	ional):			
VI AN Settings		Page Mode Config			
DMZ Setup					
LISE Settings	SSI V/PNI Server				
- oob octaings -	SSL VPN Client		Doma	inNames	
	Open//PN	Edit	Dele	te Add	
WIRELESS CO	INTROLLER				

Legen Sie über "Add" eine neue IPsec Mode Config Configuration an: Wählen Sie bei Tunnel Mode: "Full Tunnel" aus

D-Li	nk				
DWC-1000	SETUP	ADVANCED	τοοι	Ls	STATUS
Wizard	•				
WLAN Global Settings	IPSEC MODE CONFIG				LOGOUT
AP Management	This page allows you to define the	IP address range for clients connec	ting using Mode Cor	nfig.	
WLAN Visualization	Save Settings D	on't Save Settings			
Internet Settings	Ipsec Mode Config Configu	ration			
Network Settings	Tunnel Mode:	Full T	nnel 🚽 Tur	nnel Mode aut	F"Full Tunnel" stellen
QoS	Start ID Address	192.1	8 12 100		
GVRP	Start IF Address.	102.1	20 10 100		
Captive Portal	End IP Address:	192.1	58.12.199		
External	Primary DNS(Optional):	8.8.8.	3		
VRN Settings	Secondary DNS(Optional)):			
VEN Settings	Primary WINServer(Optio	nal):			
DMZ Setun	Secondary WINServer(Op	tional):			
LISB Settings	Split DNS Names				
		Doma	inNames		
		Edit Dele	te Add		
WIRELESS C	ONTROLLER				



Tragen Sie bei Start IP Address die IP Adresse ein mit der der Pool für die IPsec Clients beginnen soll, hier: "192.168.12.100".

Bei End IP Address tragen Sie die letzte zu vergebende IP Adresse des Pools ein, hier: 192.168.12.199.

Die Eingabe der DNS Server ist optional, hier wurde beispielsweise der Google-DNS "8.8.8" eingetragen.

D-Li	nk						
DWC-1000	SETUP	ADVANCED	TOOLS	STATUS			
Wizard 🕨							
WLAN Global Settings	IPSEC MODE CONFIG			LOGOUT			
AP Management 🕨	This page allows you to define the	IP address range for clients connec	ting using Mode Config.				
WLAN Visualization 🕨	Save Settings De	on't Save Settings					
Internet Settings	Insec Mode Config Configu	ration					
Network Settings	Tunnel Mode:	Turnel Meder					
QoS 🕨	Chart ID Address	102.10	IP Adress	sen Pool für die IPSec			
GVRP	Start IP Address:	152.10	Clients k	onbfigurieren. Hier:			
Captive Portal	End IP Address:	192.16	58.12.199 192.168.1	12.100-192.168.12.199			
External	Primary DNS(Optional):	8.8.8.8	В				
Authentications	Secondary DNS(Optional)):					
VPN Settings	Primary WINServer(Optio	nal):					
VLAN Settings	Secondary WINServer(On	tional):					
DMZ Setup	Contrary Transcitter(op	cionaly					
USB Settings	Split DNS Names						
		Doma	inNames				
		Edit Dele	te Add				
WIRELESS CC	INTROLLER						

3.) Anlegen einer Benutzerdatenbank
 Wechseln Sie in die Group Einstellungen
 > Advanced > Users > Groups

DWC-1000	SETUP	ADVANCED	TOOLS	STATUS	HELP
Global 🕨		·			Helpful Hints
Peer Controllers	GROUPS			LOGOUT	Login policies, Policies by Brow and Policies by IP can only be
AP Profile	This page shows the list of added	groups to the router. The user can	add, delete and edit the groups also		configured for groups having sslvpn privileges.
SSIDs	List of Groups				More
WIDS Security		Group	Descrij	otion	
Client		ADMIN	Admin G	Group	
WDS Configuration		GUEST	Guest G	iroup	
Application Rules		front	from	t	
Website Filter 🕨 🕨		φ	φ		
Firewall Settings	IP:	Sec-XAuth	IPSec-X	Auth	
IPv6		Ed it De l	ete Add		
Advanced Network	_			-	
Routing •		ogin Policies By	Browsers Policies By IP		
Certificates					
Users D	Get Users DB				
IP/MAC Binding	Groups				
Switch Settings	Users				
Intel [®] AMT					
WIRELESS CO	NTROLLER				



Fügen Sie hier über "Add" eine neue Gruppe für die IPsec-User hinzu. Vergeben Sie der Gruppe einen Namen, z.B. "IPSec-XAuth":

D-Lit	ık		_	
DWC-1000	SETUP	ADVANCED	TOOLS	STATUS
Global 🕨				
Peer Controllers	GROUP CONFIGURATION			LOGOUT
AP Profile	This page allows user to add a new	vuser group. Once this group is ac	ded, a user can then add system	users to it.
SSIDs	Save Settings Do	n't Save Settings		
WIDS Security	Group Configuration			
Client	Group Name:	IPSe	-XAuth	
WDS Configuration	Group Manie.	17.00	XA.th	
Application Rules	Description:	IP Se	c-XAUth	
Website Filter	User Type	_		
Firewall Settings	PPTP User:			
IPv6	L2TP User:			
Advanced Network 🕨	Xauth User:	V		
Routing	Admin:			
Certificates	Guest User (readonly):			
Users D	Captive Portal User:			
IP/MAC Binding	Front Desk User			
Switch Settings	Idle Timeout:	10	(Minutes)	
Intel [®] AMT				
WIRELESS CO	NTROLLER			

Wählen Sie als User Type "Xauth User" aus:

D.T.S.	1_0			
DWC-1000	SETUP	ADVANCED	TOOLS	STATUS
Global 🕨				
Peer Controllers	GROUP CONFIGURATION			LOGOUT
AP Profile	This page allows user to add a nev	v user group. Once this group is add	ed, a user can then add system u	sers to it.
SSIDs	Save Settings Do	on't Save Settings		
WIDS Security	Group Configuration			
Client	Group Name:	IP Care	XAuth	
WDS Configuration	Group Name.	1000	NA II	
Application Rules	Description:	IPSec-	XAuth	
Website Filter 🕨 🕨	User Type			
Firewall Settings	PPTP User:			
IPv6	L2TP User:		User Turne auf VAuth	lises steller
Advanced Network 🔸	Xauth User:	V	User Type aut XAutr	roserstellen
Routing +	SSLVPN User:			
Certificates	Guest User (readonly)			
Users D	Captive Portal User:			
IP/MAC Binding	Front Desk User			
Switch Settings	Idle Timeout:	10	(Minutes)	
Intel [®] AMT				
WIRELESS COM	NTROLLER			



4.) Anlegen eines IPsec Benutzers Wechseln Sie in die "Users" Einstellungen.> Advanced > Users > Users

D-Li	nk				
DWC-1000		SETUP	ADVANCED	TOOLS	STATUS
Global 🕨					
Peer Controllers	USERS				LOGOUT
AP Profile	This page	ge shows a list of available	users in the system. A user can add	d, delete and edit the users also. Th	is page can also be used for
SSIDs	betang				
WIDS Security	List of	Users	_		
Client		User Name	Group	Login Sta	tus
WDS Configuration 🕨		admin	ADMIN	Enabled (LAN) Enabl	ed (OPTION)
Application Rules		guest	GUEST	Disabled (LAN) Disab	led (OPTION)
Website Filter 🕨 🕨		front	mont	Enabled (LAN) Enabl	ed (OPTION)
Firewall Settings		ф	CP TDC-c VA.uth	Enabled (LAIN) Enabl	
IPv6		ipsec	IPSec-XAuth	Enabled (LAN) Enabl	
Advanced Network		ipsec125	IPSec-XAUU	Enabled (LAN) Enabl	ed (OPTION)
Routing ►			Edit Dele	Add	
Certificates					
Users D	GetUser	's DB			
IP/MAC Binding	Groups				
Switch Settings	Users				
Intel [®] AMT					
WIRELESS CO	INTRO	LLER			

Über "Add" können Sie einen neuen Benutzer erstellen: Vergeben Sie einen User Name, hier "IPSecUser1":

DI						
DWC-1000	SETUP	ADVANCED	TOOLS	STATUS		
Global	•					
Peer Controllers	USERS CONFIGURATION			LOGOUT		
AP Profile	This page allows a user to add r	This page allows a user to add new system users.				
SSIDs	Save Settings	Don't Save Settings				
WIDS Security	Users Configuration					
Client	User Name:	IPSec	User1 XA	uth Username		
WDS Configuration	First Name:	Vom	ma			
Application Rules		Volite				
Website Filter	Last Name:	Nach	name			
Firewall Settings	Select Group:	IPSed	⊳-XA⊔th 👻			
IPv6	MultiLogin :					
Advanced Network	Password:	••••	••••			
Routing	Confirm Password:	••••	••••			
Certificates						
Users	\triangleright					
IP/MAC Binding						
Switch Settings						
Intel [®] AMT						
WIRELESS C	ONTROLLER					



Weisen Sie dem Benutzer eine Gruppe zu, hier soll der eben angelegte User der vorher angelegten Xauth Gruppe zugewiesen werden. Wählen Sie daher bei Select Group "IPSec-XAuth" aus.

DI	1	1-*				
	,					
DWC-1000		SETUP	ADVANCED		TOOLS	STATUS
Global	►					
Peer Controllers	Þ	USERS CONFIGURATION				LOGOUT
AP Profile		This page allows a user to add new system users.				
SSIDs		Save Settings Don't Save Settings				
WIDS Security	۲	Users Configuration				
Client		User Name:	IPS	SecUser1		
WDS Configuration	►	First Name	Ve			
Application Rules	۲	First Name:	vo	mame		
Website Filter	۲	Last Name:	Na	ichname		
Firewall Settings	Þ	Select Group:	IP:	Sec-XAuth 👻	Zuweisung zur X	Auth User Datenbank
IPv6	Þ	MultiLogin :				
Advanced Network	Þ	Password:		•••••		
Routing	۲	Confirm Password:	••	•••••]	
Certificates						
Users	D					
IP/MAC Binding						
Switch Settings						
Intel [®] AMT						
WIRELESS C	:0	NTROLLER				

Vergeben Sie dem Benutzer ein Passwort: hier "ipsec123" und bestätigen Sie dieses durch erneute Eingabe.

T T C	1_0				
DWC-1000	SETUP	ADVANCED	т	DOLS	STATUS
Global 🔸					
Peer Controllers	USERS CONFIGURATION				LOGOUT
AP Profile	This page allows a user to add new	system users.			
SSIDs	Save Settings Do	n't Save Settings			
WIDS Security	Users Configuration				
Client	User Name:	IPS	ecUser1		
WDS Configuration	First Name:	Vor			
Application Rules	First Name:	Vor	iame		
Website Filter 🕨 🕨	Last Name:	Nac	chname		
Firewall Settings	Select Group:	IPS	ec-XAuth 👻		
IPv6	MultiLogin :			XAuth Passwo	ort vergeben und
Advanced Network 🕨	Password:	•••			0
Routing	Confirm Password:	•••	•••••	bestätigen	
Certificates					
Users D					
IP/MAC Binding					
Switch Settings					
Intel [®] AMT					
WIRELESS COM	NTROLLER				



5.) Konfiguration des "Shrewsoft" Clients Als IP Address geben Sie die WAN IP des DWC-1000 ein, hier: "10.20.0.100"(*)

	esolution A	luthen	ticatic
Remote Host WAN	IP des DW	/C-10	00
Host Name or IP Addres	S		Port
10.20.0.100			500
Auto Configuration	ike config	pull	-
Adapter Mode	nd assigned	addras	~ •
Adapter Mode Use a virtual adapter an	nd assigned	addres	:s ▼
Adapter Mode Use a virtual adapter an MTU 1380 Address	nd assigned 🔽 Obtain A	addres Automa	s ▼ tically

(*) Geben Sie hier bitte Ihre WAN IP Adresse des DWC-1000 oder z.B. den DynDNS Namen ein.

Wählen Sie bei Auto Configuration "ike config pull" aus, damit die Client die Konfiguration vom Server zieht.

	t Name R	esolution	Authe	nticatic
Remote Hos	ł			
Host Name	or IP Addres	s		Port
10.20.0.10	D			500
Auto Config	uration	ike confi	g pull	•
- Local Host Adapter Mo Use a virtu	de al adapter ar	nd assigne	d addre	ess 🔻
мти		🔽 Obtair	Auton	natically
1380	Address		- 22	
	Materials		-	12



Wählen Sie bei Adapter Mode: "use a virtual adapter and assigned address" aus und aktivieren Sie "Obtain Automatically".

ieneral Clie	ent Name Resolution	Authenticatic
Remote H	ost	
Host Nam	e or IP Address	Port
10.20.0.1	00	500
Auto Conf	figuration ike con	fig pull 👻
Adapter M	t 1ode	
Adapter M Use a vir	t fode tual adapter and assign	ed address 💌
Adapter M Use a vir MTU	t fode tual adapter and assign V Obta	ed address 👻
Adapter M Use a vir MTU 1380	t fode tual adapter and assign V Obta Address	ed address 👻
Adapter M Use a vir MTU 1380	t tual adapter and assign V Obta Address Netmask	ed address 👻
Adapter M Use a vir MTU 1380 Virtuel	t tual adapter and assign v Obta Address Netmask Ilen Adapter und a	ed address 💌 in Automatically uutomatisch
Adapter M Use a vir MTU 1380 Virtuel zugewi	t tual adapter and assign	ed address

Auf dem Reiter "Client" sind keine Änderungen notwendig

chorai - Alta Antanio In	esolution Authenticatic
Firewall Options	
NAT Traversal	enable 🔻
NAT Traversal Port	4500
Keep-alive packet rate	15 Secs
IKE Fragmentation	enable 💌
Maximum packet size	540 Bytes
Other Options	
📝 Enable Dead Peer D	etection
📝 Enable ISAKMP Failu	ure Notifications
📝 Enable Client Login B	Banner



/PN Site Configuration	VPN Site Configuration
General Client Name Resolution Authenticatic DNS WINS Image: Client Obtain Automatically Server Address #1 Server Address #2 Server Address #3 Server Address #4 Image: With the server Addreserver Address #4	General Client Name Resolution Authenticatic DNS WINS Image: Client Enable WINS Image: Obtain Automatically Server Address #1 Image: Client Image: Client Server Address #2 Image: Client Image: Client
Save Cancel	Save Cancel

Auf dem Reiter "Name Resolution" sind ebenfalls keine Änderungen notwendig

Auf dem Reiter "Authentication" wählen Sie als Authentication Method: "Mutual PSK + Auth":

uthentication N	fethod Mutual PSK + XAuth
Local Identity	Remote Identity Credentials
Identification	Туре
IP Address	•
Address Strin	g
🔽 Use a dis	covered local host address
PS	ithentication auf Mutual K und XAuth stellen



Unter Local Identity wählen Sie bitte als Identification Type "IP Address" aus und aktivieren Sie "use a discovered local host address":

VPN Site Configuration	VPN Site Configuration
Client Name Resolution Authentication Phase	Client Name Resolution Authentication Phase Authentication Method Mutual PSK + XAuth Local Identity Remote Identity Credentials Identification Type IP Address Address Address Image: Comparison of the second sec
Save Cancel	Save Cancel

Unter Remote Identity wählen Sie bitte als Identification Type "IP Address" aus und aktivieren Sie "use a discovered local host address":

VPN Site Configuration	VPN Site Configuration
Client Name Resolution Authentication Phase Authentication Method Mutual PSK + XAuth Local Identity Remote Identity Credentials Identification Type IP Address Address String Use a discovered remote host address Remote Identity Identification Type auf "IP Address" stellen	Client Name Resolution Authentication Phase Authentication Method Mutual PSK + XAuth Local Identity Remote Identity Credentials Identification Type IP Address Address String Use a discovered remote host address Use a discovered remote host address verwenden
Save Cancel	Save Cancel



Unter Credentials tragen Sie als Pre-shared key, den im DWC-1000 vergebenen Preshared key ein, hier: "IPSecKey2013"

PN Site Configuration
Client Name Resolution Authentication Phase
Authentication Method Mutual PSK + XAuth
Local Identity Remote Identity Credentials
Server Certificate Autority File Unter Credentials
Client Certificate File
Client Private Key File
Pre Shared Key
Den Pre-shared Key, hier: "IPSecKey2013"
eintragen
Save

Konfiguration der Phase1, konfigurieren Sie die Proposals wie im DWC-1000 eingerichtet:

Proposal Parameters	Phase 1 konfig	gurieren	 Proposal Parameters 		
Exchange Type	main	•	Exchange Type	main	•
DH Exchange	group 5	-	DH Exchange	group 5	•
Cipher Algorithm	aes	•	Cipher Algorithm	aes	•
Cipher Key Length	256 🔹	Bits	Cipher Key Length	256 🔹	Bits
Hash Algorithm	sha1	•	Hash Algorithm	sha1	•
Key Life Time limit	28800	Secs	Key Life Time limit	28800	Secs
Key Life Data limit	0	Kbytes	Key Life Data limit	0	Kbytes
Enable Check Point	Compatible Vendor II	D	Enable Check Point C	Compatible Vendor II	D



Konfiguration der Phase2, konfigurieren Sie die Proposals wie im DWC-1000 eingerichtet:

Proposal Parameters P	hase 2 konfigu	rieren	Proposal Parameters	(
Transform Algorithm	esp-aes	•	Transform Algorithm	esp-aes	•
Transform Key Length	256 💌	Bits	Transform Key Length	256 💌	Bits
HMAC Algorithm	sha1	•	HMAC Algorithm	sha1	•
PFS Exchange	group 5	•	PFS Exchange	group 5	•
Compress Algorithm	disabled	•	Compress Algorithm	disabled	•
Key Life Time limit	3600	Secs	Key Life Time limit	3600	Secs
Key Life Data limit	0	Kbytes	Key Life Data limit	0	Kbytes
			Proposals wie im DV	VC 1000 konfig	urieren

Auf dem Reiter "Policy" wählen Sie für die IPSec Policy Configuration beim Policy Generation Level "require" aus. Tragen Sie zudem das Remote Network, also das lokale Subnetz des DWC-1000, ein.

VPN Site Configuration	VPN Site Configuration
Authentication Phase 1 Phase 2 Policy IPSEC Policy Configuration Policy Generation Level require Maintain Persistent Security Associations Obtain Topology Automatically or Tunnel All Remote Network Resource ↔ 192.168.10.0 / 255.255.255.0	Authentication Phase 1 Phase 2 Policy IPSEC Policy Configuration Policy Generation Level require Maintain Persistent Security Associations Obtain Topology Automatically or Tunnel All Remote Network Resource ++ 192.168.10.0 / 255.255.255.0
Add Modify Delete	Add Modify Delete



Verbindung herstellen, geben Sie als Username, den im DWC angelegten User an: "IPSecUser1" und als Passwort, das im DWC hinterlegte Passwort "ipsec123".

onnect Netv	vork
config loaded	l for site '10.20.0.100 (3)'
Credentials	
Credentials Username	IPSecUser1
Credentials Username Password	IPSecUser1
Credentials Username Password	IPSecUser1

Der Tunnel ist aufgebaut, wenn Sie "tunnel enabled" angezeigt bekommen, und unter Network sehen, dass der Tunnel "established" ist.

S VPN Connect - 10.20.0.100 (3)	S VPN Connect - 10.20.0.100 (3)
Connect Network	Connect Network
local id configured	Security Associations
remote id configured	Established - 1
bringing up tunnel	Expired - 0
network device configured	Failed - 0
	Tunnel
Credentials	Status - Connected
Username IPSecUser1	Remote Host - 10.20.0.100
Password	Transport Used - IKE ESP
	IKE Fragmentation - Disabled
Disconnect Cancel	Dead Peer Detection - Enabled

Die IP Adresse des Clients können Sie über ipconfig überpüpfen, der Client sollte eine IP Adresse des IPsec Pools des DWC-1000 erhalten. (192.168.12.100)





Sie können nun ein Device im Subnetz des DWC-1000 anpingen, oder den DWC-1000 selbst.

C:\Users\user>ping 192.168.10.1
Ping wird ausgeführt für 192.168.10.1 mit 32 Bytes Daten: Antwort von 192.168.10.1: Bytes=32 Zeit=21ms TTL=63 Antwort von 192.168.10.1: Bytes=32 Zeit=1ms TTL=63 Antwort von 192.168.10.1: Bytes=32 Zeit=1ms TTL=63
Antwort von 192.168.10.1: Bytes=32 Zeit=1ms TTL=63
Ping-Statistik für 192.168.10.1: Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
(0% Verlust), Ca. Zeitangaben in Millisek.: Minimum = 1ms, Maximum = 21ms, Mittelwert = 6ms

Im DWC-1000 sehen Sie die Übersicht der verbundenen Clients unter:

D-Link DWC-1000 SETUP ADVANCED TOOLS STATUS Dashboard . The page will auto-refresh in 5 seconds Global Info D ACTIVE VPN LOGOUT This page displays the active VPN connections, IPSEC as well as SSL. Access Point Info D Active IPsec SAs LAN Clients Info tx (KB) tx (Packets) State Policy Name Endpoint Action Wireless Client Info I. 192.168.12.100* 10.20.0.10 473.08 458 IPsec SA Established Drop WDS Managed APs Active SSL VPN Connections D User Name IP Address Local PPP Interface Peer PPP Interface IP Connect Status Traffic Monitor D Active PPTP VPN connections Active Sessions Connection Status Action Active VPNs Disconnected Connect Poll Interval: 10 (Seconds) Start Stop

> Status > Active VPNs