

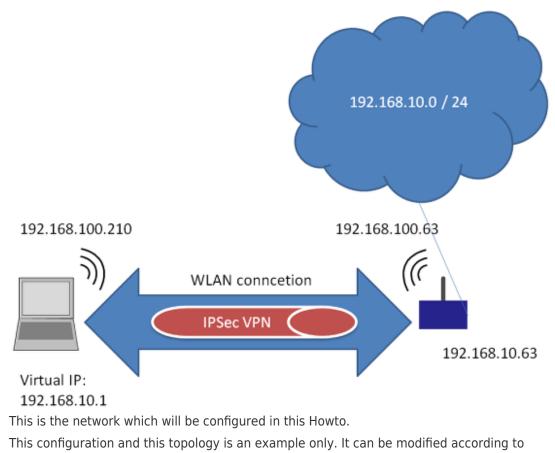
Wissensdatenbank > Produkte > BAT > BAT, WLC (HiLCOS) > Howto configure a VPN between an OpenBAT and freeware Shrewsoft VPN Client (IPSec)

Howto configure a VPN between an OpenBAT and freeware Shrewsoft VPN Client (IPSec)

- 2018-02-21 - BAT, WLC (HILCOS)

This lesson describes how to use a VPN between a OpenBAT and a WIN7 Shrewsoft Client over a WLAN connection

Network Topology



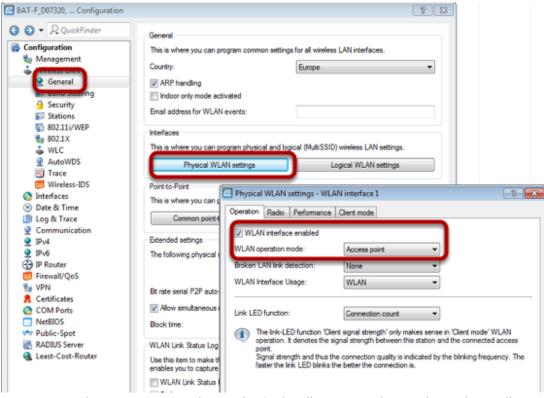
customers needs.

Assign IP-address

HiDiscovery							
Datei Bearbeiten Optio	2 🔳 🤉		stellungen 192.1	168. 10.4: ASIX AX887	728 US82.0 to Fast Ethern	•]	
Id MAC-Adresse	Schreibbar	IP-Adresse A	Netzmaske	Default Gateway	Produkt		Name
6 EC:E5:55:D0:73:20	V.		0.0.0.0		BAT-F		BAT-F_D07320
7 EC:E5:55:42:F3:00	1	192.168.10.11	255.255.255.0	0.0.0.0	MAR 1040-4C4C4C4C99995M	HRHH	MACH-42F300
5 00:80:63:39:2E:A2		192 168 10 28	255 255 255 0	0.0.0.0	DS30-3407T1T1S0AFHH	6	RS-392EA2
1 EC:E5:55:1E:64:26	Eigenschaft	en			×		RSP-ECE5551E6426
4 EC:E5:55:01:4B:C0	MAC-Adresse	: EC:E5:55:D0:73	:20				RSP-ECE555014BC0
2 EC:74:BA:35:FD:9A	Name:	BAT-F_D07320				8S	RSP-EC74BA36FD9A
8 EC:E5:55:68:1F:27	IP-Konfigura	tion					RSB-681F27
3 EC:E5:55:A4:B6:00	IP-Adresse:	6 192 .	168 . 10	. 63 Defa	lt setzen (192.168.10.23)		MSP-ECE555A4B600
	Netzmaske: Default Gat		255 . 255 0 . 0	. 0 D	it setzen (255.255.255.0) efault setzen (0.0.0.0)		
			Als Voreinste	lung speichern			
			Ok	Abbrechen			
4			IT				•
-							

Use HiDiscovery to assign a IP-address to the BAT. The PC is locally connected.

Configure physical WLAN settings

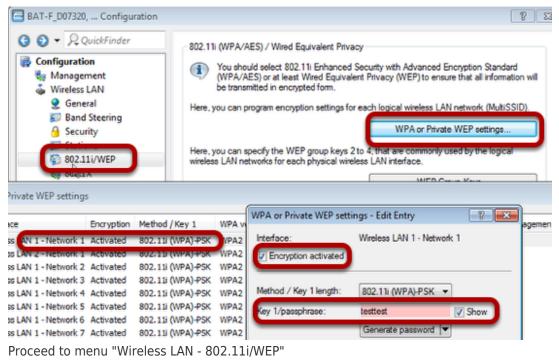


Use Access-Point as WLAN operation mode. Optionally you can choose alternative Radio settings etc.

Configure Logical WLAN settings

IS		Physical WLAN settings	Logical WLAN settings
6	Logical WLAN settings - WLA	N interface 1 - Network 1	? 💌
	Network Transmission Alarms		
	Interface:	WLAN interface 1 - Network 1	-
	WLAN network enabled		
	Network name (SSID):	VPNtest	
	Suppress SSID broadcast:	No	·
	MAC filter enabled		
C	Maximum count of clients: onfigure the SSID	0	

Confiogure WPA PSK

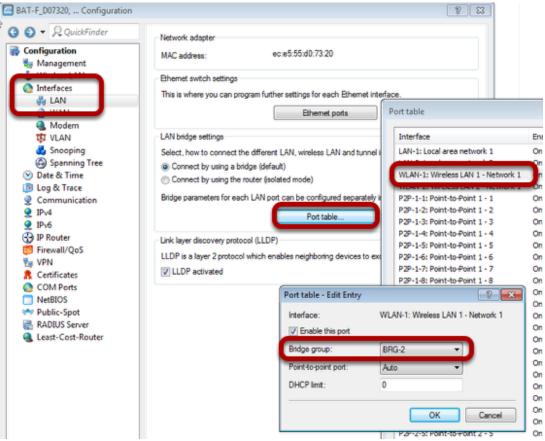


Use button "WPA or Private WEP settings...". A new window will open

Doubleclick on first line

Make sure that "encryption activated" is checked and enter a passphrase

Use Routing: Define separate bridge group for WLAN



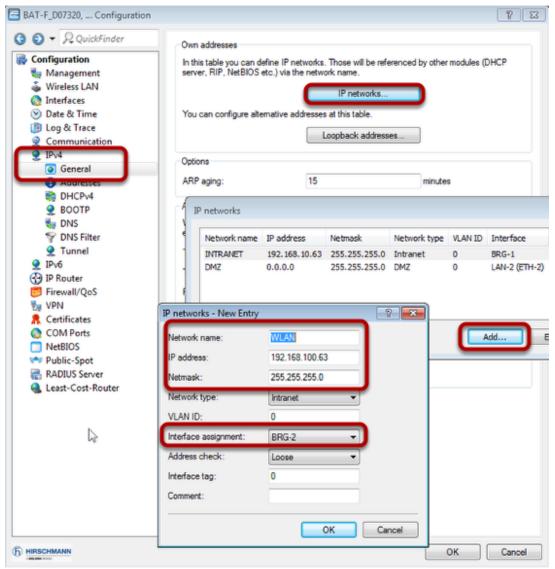
Proceed to menu "Interfaces - LAN"

Use button "Port table...". A new window will open.

Doubleclick on line "WLAN-1:..." A new window will open.

Choose "BRG-2" as Bridge group

Assign IP-address to BRG-2



Proceed to menu "IPv4 - General

Use button "IP networks...". A new window will open.

Use button "Add ... ". A new window will open.

Define IP parameters and make sure that BRG-2 is used.

Define DHCP for WLAN

	Mana Mirele Interfa Date 8 Log 8 Put IPv4 G Ge	gement Iss LAN aces & Time Trace		In	this table you o	an define (OHCP setting	Port table Port table s and select which DHCP networks onar comguration s DHCP options	network they as	pply to.
L	-	HCPv4		-4	ease time					
3. server	4. server	Buffer	Adapt	First address	Last address	Netmask	Broadcast	Default gateway	Primary DNS	Secondary D
0.0.0.0	0.0.0.0	No	No	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

name:	WLAN	Select Addresses for DH	CP clients
erver enabled:	Yes	First address:	192.168.100.200
te broadcast b	t	Last address:	192.168.100.220
P cluster		Netmask:	255.255.255.0
rding of DHCP q	ueries	Broadcast:	192.168.100.255
ver address:	0.0.0.0	Default gateway:	192.168.100.63
ver address:	0.0.0.0	Name server addr	05005
address:	0.0.0.0	Primary DNS:	0.0.0.0
er address:	0.0.0.0	Secondary DNS:	0.0.0.0
	in intermediate storage	Primary NBNS:	0.0.0
server replies	to the local network	Secondary NBNS	. 0.0.0

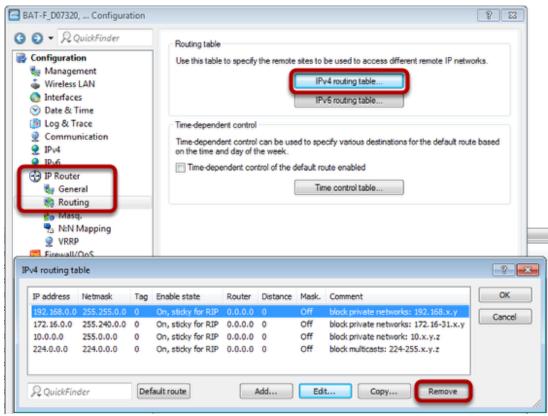
Proceed to menu "IPv4 - DHCPv4"

Use "DHCP networks...". A new window will open.

Use button "Add...". A new window will open.

Fill in relevant parameters.

Delete unused routes



Proceed to menu "IP Router - Routing"

Use button "IPv4 routing table". A new window will open.

Delete all entries by clicking button "Remove" several times.

Now send the configuration to the OpenBAT by clicking "OK" in all dialogs.

OPEN Wizard

Eile Edit Device Group	View Tools Help					
		Into	i Consumer			
**		· 🖉 😈	R QuickFind	er		
🏐 Hirschmann LANconfig	Name	Comment		Cluster Name	Address	Location
	BAT-F_D07320				102 169 10 62	
			Configure			Ctrl+O
			Setup/Wizard			Ctrl+W
			Quick Rollback	c		Ctrl+Q

In LANconfig right-click on the device and choose SetupWizard

Use Wizard for VPN / Remore access

Setup Wizard for BAT-F_D0	7320	×
	Setup Wizard for BAT-F_D07320	
	With this wizard you can comfortably configure your device for specific applications.	
	What do you want to do?	
	Manually edit the configuration	*
	Basic settings	
	Public Spot setup	E
	Provide remote access (RAS, VPN)	
	Configure Dynamic DNS	-
	< Back Next > Cano	el

Choose relevant wizard and press "Next"



Coose "VPN client with user-defines parameters" and click "Next"

🎾 Setup Wizard for BAT	-F_D07320		x
Provide remote acce Settings for this con	ess (RAS. VPN) nection's remote station		
First, enter a name f	or this access:		
VPN Name:	NOTEBOOK		
		_	
	2		
	<	Back Next >	Cancel

Choose VPN Name and click "Next"

Setup Wizard for BAT-F_D07320	
Provide remote access (RAS, VP VPN Authentication and Exchange	
Two kinds of VPN connection auth Select the used VPN connection a Preshared Key and Aggressive Centricates (NOA Signature) and	Authentication as well as the exchange mode: Mode
	Generate password
to the X.509 standard are no client. The device certificate	nat for RSA Signatures, digital certificates according becessary for both this device and for the remote e must be uploaded via HTTP(S) before establishing dition, when using certificates, it is necessary for the em time.
	< Back Next > Cancel

Choose "Preshared Key and Aggressive Mode" Choose a Preshared Key Click "Next"

Setup Wizard for BAT-F_D07320								
Provide remote access (RAS, VPN) Default IKE parameters for all incoming aggressive mode connections								
The following default IKE parameters for all incoming aggressive mode connections are already defined:								
Default IKE proposal list: IKE_PRESH_KEY								
Default IKE proposal group: 2								
These settings are used collectively by all incoming connections. Therefore, we recommend that you do not change them.								
Nevertheless, edit default IKE parameters for this and any future aggressive mode connections.								
Attention: Please take into account that if you change these settings, existing connections may no longer work!								
< Back Next > Cancel								

Use default settings and click "Next"

🎾 Se	etup Wizard for BAT-F_D0732	0
P	rovide remote access (RAS Which "Identities" should be	5. VPN) used for this VPN connection?
	To establish an encrypted VP both sides.	N connection, the given identities must be recognized by
		n sides and a corresponding unique identity for the ntity is required at a minimum in order to identify the right tion.
	Local identity type:	IP Address 🔹
	Local identity:	192.168.100.63
	Remote identity type:	IP Address 🔹
	Remote identity:	192.168.100.210
		< Back Next > Cancel

Coose "IP Address" as identifier (local and remote).

Enter IP-addresses. The remote IP address must be known. Probably you have to connect to the WLAN with your client first.

Setup Wizard for BAT-F_D0732	20
Provide remote access (RAS Select the PFS group for IPS	
Additionally, it is recommende for key generation.	d for higher security to use PFS (Perfect-Forward-Secrecy)
Vse the PFS algorithm for	this connection
PFS group:	2 (MODP-1024)
A higher value for the PFS gro minor loss in connection time.	oup assures a higher level of security in exchange for a
You can change the pre-sele	ction however, it does meet most requirements.
	< Back Next > Cancel

Use default settings and press "Next"

Setup Wizard for BAT-F_D07320	٢.
Provide remote access (RAS. VPN) Which encryption and authentication algorithms should be proposed to the client for IPSec with ESP	
The device supports for data transmission (IPSec) with ESP different encryption and hash algorithms.	
Which encryption algorithms should be proposed to the client (at least one)?	
Blowfish (128bit)	
3DES (168bit)	
Which authentication algorithms should be proposed to the client for ESP (at least one)?	
MAC-SHA1-96	
You can change the pre-selection however, it does meet most requirements.	
< Back Next > Cancel]

Choose "AES 8256bit)" and "HMAC-SHA1-96" and press "Next"

Setup Wizard for BAT-F_D073	20		
Provide remote access (RAS. VPN) Which IPSec AH authentication algorithms should be proposed to the client?			
In addition, the device can propose a further authentication protocol (Authentication Header, short AH) for IPSec.			
Attention: This protocol will not work if your client is behind a masked connection (NAT/PAT)!			
Which AH authentication al	Which AH authentication algorithms should be proposed to the client?		
Authentication:	No AH		
Additionally, you can specify	Additionally, you can specify a IPCOMP compression algorithm:		
Compression:	No IPCOMP -		
You can change the pre-sel	ection however, it does meet most requirements.		
	< Back Next > Cancel		

Use default settings and press "Next"

🎾 Se	tup Wizard for BAT-	F_D07320		
Pr	Provide remote access (RAS, VPN) Settings for the TCP/IP protocol			
	Enter an unique IP address (Virtual IP) to be configured in your VPN client. Enter a free address from the address area of your network.			
	The network that yo	ur device belongs to:		
	IP network:	192.168.10.0		
	Netmask:	255.255.255.0		
	Legal addresses:	192.168.10.1 - 192.168.10.254		
	IP address:	192.168.10.1		
	(1) Information			
		try of an IP address if the VPN client in use supports Config Mode, M Advanced VPN Cli⊖t.		
		< Back Next > Cancel		

Choose a virtual IP address for the remote client in the local network. This will use proxy ARP automatically.

Press "Next"

Setup Wizard for BAT-F_D073.	20	X	
Provide remote access (RA Settings for the TCP/IP proto	-		
You may either allow all IP addresses to be reached by the VPN client (default) or you may limit the access to a specific IP network.			
Which IP addresses should b	Which IP addresses should be reachable for the VPN client:		
Allow all IP addresses to	be reachable for the VPN client		
The following IP network	should be reachable for the VPN	client:	
IP network:	192.168.10.0]	
Netmask:	255.255.255.0]	
Please remember to configure this IP network on VPN client as well. If you neglect to configure the same network there, a VPN connection will not be able to be established. Further networks and network relations or transmission properties can be configured in the corresponding new rule created on the firewall.			
	< Back	Next > Cancel	

Use default settings and press "Next"

Setup Wizard for BAT-F_D07320	×
Provide remote access (RAS, VPN) Settings for the TCP/IP protocol	
The NetBIOS protocol is used in some local networks to grant the individual stat mutual access to file and printer resources (For example, Microsoft Windows net	
You can also grant dial-in access to user access to networks of this type.	
Activate NetBIOS over IP routing	
< Back Next >	Cancel

Disable NetBIOS over IP routing Press "Next"



On Client side Shrewsoft VPN Clinet is used (freeware)



Install Shrewsoft VPN Client and start "VPN Access Manager"

Define new VPN

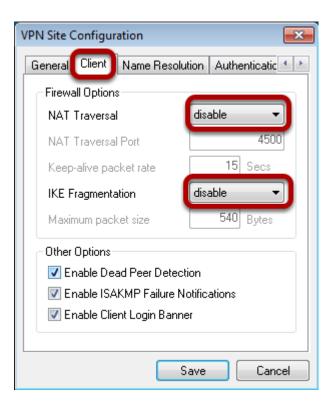
🚯 VPN Access Manager 📃 🗖 💌				
File Edit	View H	lelp		
Connect	Add	Object Control Cont	😑 Delete	
Connection	Name	-	Host Name	Authentication
(
•			III	•

Click "Add". A new window will open.

/PN Site Configuration
General Client Name Resolution Authenticatic
Bemote Host
Host Name or IP Address Port 192.168.100.63 500
Auto Configuration ike config pull 👻
Local Host
Adapter Mode Use an existing adapter and current address
Use an existing adapter and current address 👻
Use an existing adapter and current address MTU MTU Dbtain Automatically
Use an existing adapter and current address MTU Image: Strain Address Address

Enter the IP-address of the VPN Gateway (OpenBAT)

Choose "Use existing adapter and current address" as "Adapter Mode"



In "Client" tab disable nat-T and Fragmentation.

VPN Site Configuration	×
General Client Name	Resolution Authenticatic
DNS WINS	
Enable DNS	✓ Obtain Automatically
Server Address #1	
Server Address #2	
Server Address #3	
Server Address #4	
DNS Suffix	Obtain Automatically
	Save Cancel

Disable DNS

VPN Site Configuration		
Client Name Resolution Authenticat	ation Phase 4	
Authentication Method Hybrid RSA +		53 56 4 4 •
	Saw Client Private Key File	
	Save	ancel

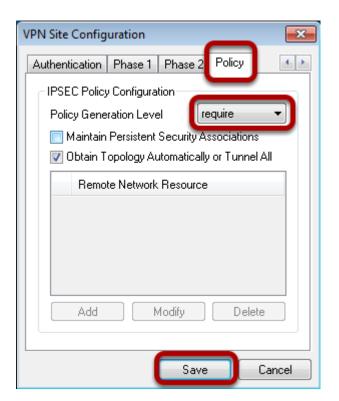
For authentication use" IP-Adress" as identifier and enter the addresses . In the "Credentials" tab enter the "Pre Shared Key" (vpnpassword)

VPN Site Configuration	×
Name Resolution Author	entication Phase 1 Pha:
- Proposal Parameters -	
Exchange Type	aggressive 🔻
DH Exchange	group 2 👻
Cipher Algorithm	aes 🔻
Cipher Key Length	256 🔻 Bits
Hash Algorithm	sha1 🔹
Key Life Time limit	2880¢ Secs
Key Life Data limit	0 Kbytes
Enable Check Point	Compatible Vendor ID
	Save Cancel

For phase1 use relevant parameters

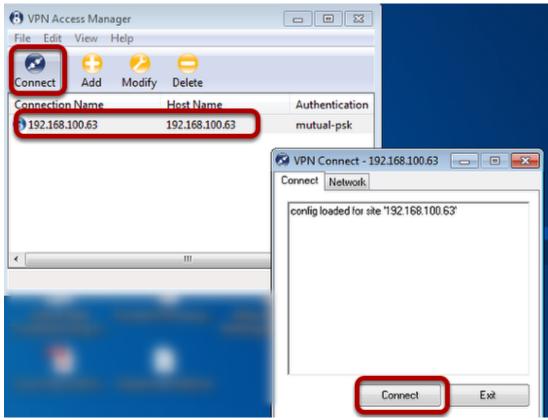
VPN	N Site Configuration		×
A	uthentication Phase 1	Phase 2 Policy	4 >
1	Proposal Parameters		
H	Transform Algorithm	esp-aes	-
	Transform Key Length	256 🔹	Bits
	HMAC Algorithm	sha1	-
I	PFS Exchange	group 2	-
H	Compress Algorithm	disabled	-
I	Key Life Time limit	3600	Secs
I	Key Life Data limit	0	Kbytes
l			
1			
	l	Save	Cancel

For phase2 use relevant parameters



In "Policy" tab user "require" as "Policy Generation Level" Press button "Save"

Start VPN



Mark the new created Vpn and press "Connect". A new window will open. Press "Connect".

Test VPN

Administrator: C:\Windows\system32\cmd.exe
Ping-Statistik für 192.168.10.28: Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust), Ca. Zeitangaben in Millisek.: Minimum = 26ms, Maximum = 64ms, Mittelwert = 36ms
C:\Users\jxs05012.DENEC1LT0360>ping 192.168.10.4 Ping wird ausgeführt für 192.168.10.4 mit 32 Bytes Daten: Antwort von 192.168.10.4: Bytes=32 Zeit=15ms TTL=127 Antwort von 192.168.10.4: Bytes=32 Zeit=17ms TTL=127
Antwort von 192.168.10.4: Bytes=32 Zeit=23ms TTL=127 Antwort von 192.168.10.4: Bytes=32 Zeit=17ms TTL=127
Ping-Statistik für 192.168.10.4: Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust), Ca. Zeitangaben in Millisek :

Open a DOS window and ping an IP-address of the remote network.