

Base de Conhecimentos > Products > 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							
Signal Eigenschaften V	Nen 2 S III (WWW Telnet P	ي ing Neu-Scan Eine	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		197 168 10 28	255 255 255 0	0.0.0.0	DS30-3407T1T1SDAFHH	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
	Default Gat	255 . eway: 0 .	0.0	. 0 Defau	efault setzen (0.0.0.0)		
			Als Voreinste	slung speichern			
			Ok	Abbrechen			
-							
							,

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
[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

		Configura Mana Wirele Date & Log 8 PV4 G Ge	ation gement ess LAN aces & Time t Trace		I D	HCP client/serv he interfaces wi this table you o HCP options ca	er hich should can define (n be used t	be applied to	o the DHCP server a Port table is and select which i DHCP networks DHCP options	network they as	ted in this table. oply to . e clients.
	L	in Di	HCPv4		-4	ease time					
3.	. server	4. server	Buffer	Adapt	First address	Last address	Netmask	Broadcast	Default gateway	Primary DNS	Secondary DNS

rk name:	WLAN	Addresses for DHCF	P clients
server enabled:	Yes	First address:	192.168.100.200
aluate broadcast b	ł	Last address:	192.168.100.220
HCP cluster		Netmask:	255.255.255.0
onwarding of DHCP q	ueries	Broadcast:	192.168.100.255
. server address:	0.0.0.0	Default gateway:	192.168.100.63
. server address:	0.0.0.0	Name server addres	1965
server address:	0.0.0.0	Primary DNS:	0.0.0.0
. server address:	0.0.0.0	Secondary DNS:	0.0.0.0
Place server replies	in intermediate storage	Primary NBNS:	0.0.0.0
Adapt server replies	to the local network	Secondary NBNS:	0.0.0.0

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

Hirschmann LANconfig							
Eile Edit Device Group	View Tools Help						
377 00 V	🖌 🖻 🖉 🖻 🗲 🗎 🗖	- 19 0	QuickFind	ler			
🏐 Hirschmann LANconfig	Name	Comment		Cluster Name	Address	Location	
	BAT-F_D07320	_			102 169 10 62		7
			Configure			Ctrl+O	
			Setup/Wizard			Ctrl+W	
			Quick Rollbac	k		Ctrl+Q	
			Charle			041-55	

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 Set up Internet pages	E
	Provide remote access (RAS, VPN)	
	Configure Dynamic DNS	Ŧ
	< 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	—
Provide remote acce Settings for this cor	ess (RAS. VPN) nection's remote station	
First, enter a name t	or this access:	
VPN Name:	NOTEBOOK	
	\swarrow	
	< Ba	ck Next > Cancel

Choose VPN Name and click "Next"

Setup Wizard for BAT-F_D07:	320						
Provide remote access (R/ VPN Authentication and Ex	AS. VPN) Inchange Mode Selection						
Two kinds of VPN connecting Select the used VPN connecting of the used value of the	on authentication are supported. action authentication as well as the exchange mode: ressive Mode are and main mode						
Preshared Key:	vpnpassword						
Information: Please take into account that for RSA Signatures, digital certificates according to the X.509 standard are necessary for both this device and for the remote client. The device certificate must be uploaded via HTTP(S) before establishing the VPN connection. In addition, when using certificates, it is necessary for the device to have a valid system 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
	Enter the identity type for both authorization. The remote iden preshared key for this connect	i 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	ec								
Additionally, it is recommende for key generation.	d for higher security to use PFS (Perfect-Forward-Secrecy)								
Use the PFS algorithm for	☑ Use 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	×
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 > Cance	el

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

Setup Wizard for BAT-F_D07	320		
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 a	Which AH authentication algorithms should be proposed to the client?		
Authentication:	No AH 🔹		
Additionally, you can specif	fy a IPCOMP compression algorithm:		
Compression:	No IPCOMP -		
You can change the pre-se	election however, it does meet most requirements.		
	< Back Next > Cancel		

Use default settings and press "Next"

🎾 Se	tup Wizard for BAT-	F_D07320		
Pr	rovide remote acce Settings for the TCP	ss (RAS. VPN) /IP protocol		
	Enter an unique IP a address from the add	ddress (Virtual IP) to be configured in your VPN client. Enter a free dress area of your network.		
	The network that your 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			
	You can omit the end as does the LANCO	ry 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	S. VPN) acol		
You may either allow all IP a VPN client (default) or you m	ddresses to be reached by the ay limit the access to a specific IF	network.	
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 stations mutual access to file and printer resources (For example, Microsoft Windows networks).
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 Acc	ess Mana	ger		_ 0 💌
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
Remote 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 🔻
Adapter Mode Use an existing adapter and current address MTU Obtain Automatically
Adapter Mode Use an existing adapter and current address MTU I380 Address Address
Adapter Mode Use an existing adapter and current address MTU I380 Address Netmask
Adapter Mode Use an existing adapter and current address MTU I380 Address Netmask

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	e 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 Authentication Phase	
Client Name Resolution Authentication Phase 4 Authentication Method Hybrid RSA + XAuth Image: Configuration Identification Type Image: Configuration Image: Client Identification Type Image: Client Name Resolution Identification Type Image: Client Name Resolution Image: Address String Image: Client Name Resolution Image: String Image: String Image: String Image: String Image: String Image: String Image: String	ES3 hentication Phase IBSA + XAuth VPN Site Configuration VPN Site Configuration Client Name Resolution Authentication Phase Interview Client Name Resolution Authentication Phase Interview Client Nemote Identity Credentials Server Certificate Autority File Client Certificate File
S	Client Private Key File
	Save Cancel

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

VP	N Site Configuration		×
4	Authentication Phase 1	Phase 2 Policy	4 >
	Proposal Parameters		
Н	Transform Algorithm	esp-aes	-
	Transform Key Length	256 🔹	Bits
	HMAC Algorithm	sha1	-
I	PFS Exchange	group 2	-
I	Compress Algorithm	disabled	-
I	Key Life Time limit	3600	Secs
I	Key Life Data limit	0	Kbytes
	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	8
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=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.