eWON Application User Guide

AUG 021 / Rev 1.0







This guide will explain in a few steps how to configure and use your ENDIAN to create a VPN network with eWONs.

1. Hardware and software requirements Hardware requirements Software requirements eWON Firmware Version	3 3 3 3
2. What is ENDIAN for eWON? What is ENDIAN? What is ENDIAN for eWON?	4 4 4
3. Network Setup	5
ENDIAN connection	э 5
Interfaces Configuration	6
OpenVPN Configuration	9
eWON Configuration	13
PC configuration	15
4. Network topologies	17
Only eWONs	17
ENDIAN Settings	17
Only eWONS + eWONS see eWONS	18
	10
ENDIAN Settings	19
5. Security	21
Revisions	23

Hardware and software requirements

Hardware requirements

In order to follow this guide you'll need:

- 1 ENDIAN server appliance (in this document, we use an ENDIAN-Mini)
- 1 (or several) eWON-VPN with an Internet access

Software requirements

eWON configuration software:

The eWON is configured through its web server. So all you need is a standard Web Browser software like Internet Explorerⁱ or Firefoxⁱⁱ.

Additionally we suggest you to download the eBuddy utility on our website : <u>http://support.ewon.biz.</u>

This utility allows to list all the eWONs on your network and to change the default IP address of an eWON to match your LAN IP address range. With eBuddy you can also easily upgrade the firmware of your eWON (if required).

eWON Firmware Version

To be able to follow this guide your eWON needs a firmware version 5.5 or higher. A simple way to do an eWON firmware upgrade is to use eBuddy, the eWON software companion.



What is ENDIAN for eWON?

What is ENDIAN?

ENDIAN is an Open Source Firewall UTM Appliance.

Website: http://www.endian.com

The Endian Firewall is an open source Linux distribution that specializes on Routing/Firewalling and Unified Threat Management. It is being developed by the Italian Endian SrI and the community.

The version of the Endian Firewall used in this document is version 2.2.1.

ENDIAN is mainly a Firewall (both directions), but also a "Virtual Private Network (VPN) Gateway with OpenVPN or IPsec".

Other features are: DHCP-Server, Hotspot/Wireless Security, Web Antivirus, Web Antispam, E-Mail Antivirus, E-Mail Antispam, Transparent HTTP-Proxy, Content Filter, SIP VoIP Support, Network Address Translation, Multi IP address (aliases), HTTPS web interface, Connection statistics, Log of networking traffic, Forwarding of logs to an external server, NTP-Server, Intrusion Detection System, ADSL-Modem Support

What is ENDIAN for eWON?

As eWON-VPN are based on OpenVPN too, it is easy to build a VPN network with an ENDIAN as OpenVPN Server and eWONs as OpenVPN Clients.





Network Setup

ENDIAN configuration

ENDIAN Connection

By default, you can access the ENDIAN appliance by its LAN Ethernet connector.

The default IP LAN address range is the 192.168.0.0/24 and the ENDIAN Firewall is at 192.168.0.15.



Figure 2: Endian Home page



Interfaces Configuration

ENDIANS are built to manage 4 hardware interfaces. In this document, we only need 2 hardware interfaces to build our VPN network.

In our simple VPN network, we need only a LAN and a WAN interfaces.

LAN: our private network LAN address range 192.168.0.0/24 ENDIAN-LAN: 192.168.0.15

WAN: the corporate network allowing us to access Internet WAN address range 10.0.0.0/16 ENDIAN-WAN: 10.0.120.9

Use the *Network configuration* menu and follow the wizard to define and configure the network interfaces.

	System	Status	Network	Services	Firewall	Proxy	VPN	Logs				
	Network	configura	ation									
Home	>> Netw	/ork setup wi	zard									
Network configuration	Shan 4 7. Channe huma of BED interface											
Support	Step 1/7: 0	Choose type	of RED interfac	e								
Endian Network	RED: unti	rusted intern	et connection (WANT	Hardward	e informatio	n					
Passwords	-				Number of	f interfaces	a					
SSH access	• ETHE	RNET STATIO	0			i intorracco	•					
GUI settings	O ETHE	RNET DHCP										
Backup		F										
Shutdown		L										
Credits	- C ADSL	USB, PCI)										
	C ISDN											
	C ANAL	LOG/UMTS N	lodem									
	O GATE	EWAY										
	Car	ncel	>>>									
Figure 3: Choose type	of RED	interfa	се									

	System	Status	Network	Services	Firewall		VPN	Logs
	Network	configura	ation					
Home	>> Netw	ork setup wi	zard					
Network configuration								
Support	- Step 2/7: 0	Choose netw	ork zones/					
Endian Network	ORANGE	network se	ament for serv	ers accessible	from internet (DMZ)		
Passwords	BLUE	network se	- oment for wire	less clients (18/1	FD	ŕ		
SSH access		network se	gineric for wre	1033 CIICI II.3 (Y M				
GUI settings	● NONE	-						
Backup	O ORAI	NGE						
Shutdown	0.000							
Credits								
	C ORAL	NGE & BLUE						
	<<<	Cancel	>>>					



3. Network Setup

	System	Stat	us Netw	ork Service:	s Firewal	Proxy	VPN	Logs	
								Logo	
	Networ	k conf	guration						
Home	>> Net	work set	up wizard						
Network configuration	Sten 4/7	. Internet	access prefe	rences					
Support			000000 proto	011000					
Endian Network	RED (ur	trusted,	nternet conne	ction (WAN)):					
Passwords	- IP addre	SS:			10.0.120.9		netw	ork mask:	/16 - 255.255.0.0 🔹
SSH access	0.44.04	dition of our	ldraaaaa (ana	Déletrock ex ID/C	IDD nex line) :				·
GUI settings	Auu au	allionarat	iuresses (one	IP/Netmask or IP/C	JDR per line).				
Backup									
Shutdown	_								
Credits									
	Interfac	es:							
	Р	ort Link	Description	MAC	Device				
		1 🖌	Realtek <u>?</u>	00:60:e0:e2:b3:4	13 eth0				
	0	2 🗙	Realtek <u>?</u>	00:60:e0:e2:b3:4	12 eth1				
	0	з 🗙	Realtek <u>?</u>	00:60:e0:e2:b3:4	11 eth2				
	۲	4 🖌	Realtek <u>?</u>	00:60:e0:e2:b3:4	40 eth3				
	Default	gateway			10.0.0.254				
	MTL								
	Spoof N	1AC addr	ess with: •		I				
	* This f	ield may	oe blank.						
	<<<	0	ancel	>>>					
ure 5: Internet acc	ess pref	eren	ces						

	System	Status	Network	Services	Firewall	Proxy	VPN	Logs
	Network	configura	ation					
Home	>> Netv	vork setup wi	zard					
Network configuration								
Support	Step 5/7:	configure DN	S resolver					
Endian Network	manual D	NS configura	tion:					
Passwords		-						
SSH access		10.0.0.13						
GUI settings	DNS 2:	10.0.0.13						
Backup								
Shutdown		Cancel		1				
Credits				I				

Figure 6: Configure DNS resolver



3. Network Setup

	System	Status	Network	Services	Firewall	Proxy	VPN	Logs
	Network	configura	ition					
Home	» Netwo	ork setup wiz	ard					
Network configuration								
Support	Step 6//: A	Apply configu	ration					
Endian Network	Coparatula	tional						
Passwords	Network s	etup is ready	, click Ok to ap	ply the new co	nfiguration.			
SSH access								
GUI settings								
Backup	_ <<<	Cancel	0K, a	apply configuration	on			
Shutdown								

		oratoro	INCLIVIOIN	Services	Firewall	Proxy	VPN	Logs
	Network	configura	ation					
Home	>> Netw	ork setup wi	zard					
Network configuration	0							
Support	- Step ///: E	nd						
Endian Network	Your conf	iguration has	been saved. P	Please wait unti	I the depender	t services ha	ave been re	eloaded. This may take up to 20 seconds. Enjoy!
Passwords								
SSH access	Remember	to check if I	P address bloc	ks of services	are still configi	ured as you v	wish. Mainl	y check the configuration of "Network based access control" o
GUI settings	the HITP F	roxy.						



OpenVPN Configuration

Global settings

To configure the VPN of the ENDIAN, use the VPN top menu, followed by the *OpenVPN server* in the left menu.

The only thing to do is to enable the OpenVPN server and to fix the Dynamic IP pool adresses used by VPN Clients.

	System	Status	Network	Services	Firewall	Proxy	VPN	Log
	OpenV	⊃N - Virtu	al Private	Networkin	g			
OpenVPN server	» Sei	ver configu	ration Acc	ounts Adva	nced VPN cl	ient downloa	d	
OpenVPN client (Gw2Gw)	» Glo	bal settings						
	OpenVP	N server ena	bled:		V			
	Dynamic	IP pool start	address:		192.16	68.0.20		
	Dynamic	IP pool end a	iddress:		192.16	68.0.254		
	Save	and restart			Downlo	oad CA certif	icate	

One practical feature of ENDIAN VPN is that all VPN-Clients will receive a VPN address compatible with the LAN network.

In our example, as the LAN (our GREEN interface) is 192.168.0.0/24, all the VPN clients will receive an address between 192.168.0.20 and 192.168.0.254.



Then, from any devices placed on the LAN, all the remote eWONs connected by VPN will be reachable the same way as if they were physically on the same LAN!



Accounts

Now, for each client, you need to create an account. For that, select the *Accounts* tab and use the *Add Account* button.

		System	Status	Network	Services	Firewall	Proxy	VPN	Logs
		OpenVPI	N - Virtual	Private N	etworking				
	OpenVPN server	» Serve	r configuratio	Accounts	Advanced	VPN client	download		
	OpenVPN client (Gw2Gw)								
	IPsec	>> Chang	je account ev	/on92					
		Account in	nformation			000000		_	
						ewonaz		_	
		Password:				•••••	••••		
		Verify pass	sword:			•••••	••••		
Figure	e 10: Add a VPN Acco	unt							

For now, just enter the *Username* and *Password* and save your account. Leave all the other parameters blank, we will discuss them later.

Create as much accounts as you need.



Advanced parameters

With the *Advanced* tab, you will set the *Port* and *Protocol* used for the VPN (UDP 1194 by default) and select the Authentication type (PSK).

Check the *Block DHCP responses coming from tunnel* parameter to avoid DHCP trafic between DHCP-Servers from different places.

Uncheck the *Don't block traffic between clients* to block communication between VPN Clients.

	System Status Network		The wait The xy	Cogo	
	OpenVPN - Virtual Private	e Networking			
N server	Server configuration Account	unts Advanced	VPN client download		
l client (Gw2Gw)	Advanced settings				
					-
	Port: [119	4	Block DHCP resp	onses coming from tunnel:	V
	Protocol: UDF	•	Don't block traffic	between clients:	
	Note: You may allow multiple ports by po	rt forward them			
	Save and restart				
	Global push options		and the second se		
	» Authentication settings				
	Authentication type				
	C PSK (username/password)				
	O X.509 certificate				
	O X.509 certificate & PSK (two fai	ctor)			
	Certificate management				
	Download CA certificate	U:	se this file as CA certifica	ate for clients.	
	Export CA as PKCS#12 file	U	se this file for import on C	OpenVPN fallback servers.	
	Import server certificate from primar	y OpenVPN server	or external Certification /	Authority (CA)	
	PKCS#12 file:			Browse	
	Challenge password:				
	Host certificate:		C=IT/O=efw/CN=127.0.0.	1	
	CA certificate:		C=IT/O=efw/CN=efw CA		

Use the *Download CA certificate* link to retrieve the certificate of the Firewall. You will need it to configure your eWONs.







eWON Configuration

Firstly, configure your eWON to access the Internet.

And then, go to the Wizard menu.

Configuration \rightarrow



Choose the "Configure Endian For eWON connectivity" button

Set the parameters for the ENDIAN connection. eWON configuration wizard / ENDIAN A user account must be created for your on the Endian4eWON firewall before you can use this wizard. The same account parameters must be entered here. eWON Account parameters Enter the information entered in the Endian Firewall configuration Server Address: 81.82.83.84 VPN Username: ewon92 VPN Password: CA Certificate: ----BEGIN CERTIFICATE--------- BEGIN CERTIFICATE ----MIID0jCCAkKgAwIBAgIBADANBgkghk HT 1DVgCCAAKgAw IB Ag IB ADABB gk ghà 14 HA= 6A,DVE CARD DVC HOT= 0 (TOVQCDE=01 HgC=Ha=AHED 0.107H00gA=HC==C07DV000 MA-6A1UECHMDZWZ3MQ8mDQYDVQQDEm ϺϳͺϨϣϲͶϺϧϭͶͶϺϧϒͶϽϨϨϢϳϪϧϺϨϧϣϹͺϨϒϽϓϨ VQQDEw21Znc gQ0EwggEiMA06C3q63I 💌 Important: Your eWON must have a working Internet Connection Before using the wizard, the eWON Internet access must be correctly configured. This wizard supposes that the VPN server uses port 1194 and UDP protocol (otherwise configure your VPN connection manually). << Previous Next >> Figure 12: eWON ENDIAN wizard

The VPN Username/Password comes from one of the Accounts created in the ENDIAN.

Copy the Certificate downloaded from the ENDIAN.

The Server Address is usually the Internet Public IP address behind which the ENDIAN is placed.

Click on the *Next* button and the eWON will do the VPN connection.



eWON configuration wizard / ENDIAN.	Connection test & configuration
Current operation	
Finished	11
Results	
VVAN connection	
✓ Test VPN connection	
Diagnosis	
SUCCESS: ENDIAN 4 eWON VPN connection wor	king
1	
<< Previous	Done
Figure 13: ENDIAN wizard success	

If the connection succeeds, you will have the following screen.

If you look at the ENDIAN website, you can view that the eWON92 is well connected.

	System Status	Network	Services	Firewall Proxy	VPN Logs									
	OpenVPN - Virtual Private Networking													
OpenVPN server	» Server config	uration Accou	nts Advance	d VPN client downloa	id									
OpenVPN client (Gw2Gw)	_													
IPsec	>> Global settings													
	OpenVPN server en Dynamic IP pool star Dynamic IP pool end Save and restart	abled: t address: address:		192.168.0.20 192.168.0.254 Download CA certificate										
	» Connection sta	tus and control												
	User	Assigned IP	Real IP	RX / TX	Connected	since Uptime	Actions							
	ewon92	192.168.0.2	25 10.0.120.92	1.6 KiB / 10 KiB	Thu Dec 4 15	5:31:13 2008 < 1m	kill ban							
	prk	192.168.0.2	24 10.0.120.1	46.6 KiB / 33.5 k	(iB Thu Dec 4 15	5:30:36 2008 1m	kill ban							



PC configuration

The ENDIAN Servers are mainly designed to build the PC's network. To connect a PC to your VPN network, you need to install a piece of software on your computer.

From the ENDIAN website, download and install the 😪 EndianVPNClient-setup

software.

Once installed, you have your *ENDIAN VPN Dialer* to connect your PC to the OpenVPN network.

Endian VPN Dialer
<u>Adiàn</u>
Profile: Endian VPN Profile 🔹 + 🖉
Username: prk
Password:
Connect
Figure 14: ENDIAN VPN Dialer

To join a VPN Network, create or edit a Profile.

Endian Profile Editor				×
Endian VPN ADSL Endian VPN Profile	Connection Adva	nced Global		
	Description:	Endian VPN Profile	•	
	Server:	10.0.120.9		
	Port:	1194		
	Certificate:	• CA Certificate	efw-test.pem.cer	
		O Pkcs #12		
	Authentication:	Username prk		
		Password .	•••	
	Owner:	The only in the users of the second secon	this computer	
	Connect:	manual	this compater	
		C on user logon	tart.	
		 on compacer s 	uan c	
+ -				?
			Ok Ok	Iancel

You need the same certificate as the one used to configure the eWON.



Г

Once connected, your PC has access to the whole corporate network (connected to the ENDIAN LAN interface).

٦

Endian VPN Manager						
Endian VPN Profile						
Disconnect Info View Log						
Image: Second connection Profile Editor	,					
Figure 16: PC VPN Client connected						



Network topologies

Only eWONs

Now, with the simple configuration of ENDIAN and eWONs done in the previous chapter (only with default settings), we have build a network like the one below:



With this topology:

- All the devices on the corporate LAN have access to all the eWONs
- All the eWONs have access to all the devices on the corporate LAN
- none of the eWONs have access to other eWONs

ENDIAN Settings

OpenVPN - Virtual Private Networking							
>> Server configuration Accounts	Advanced	VPN client download					
» Advanced settings							
Port: 1194		Block DHCP responses coming from tunnel:	7				
Protocol: UDP 💌		Don't block traffic between clients:					
Note: You may allow multiple ports by port forw	ard them						



Only eWONs + eWONs see eWONs

You can configure the ENDIAN firewall to allow each eWON (VPN Clients) to see all the others.



With this topology:

- · All the devices on the corporate LAN have access to all the eWONs
- All the eWONs have access to all the devices on the corporate LAN
- All the eWONs have access to other eWONs

ENDIAN Settings

To achieve this Global VPN inter-Clients communication, you need to allow it in the *Advanced* settings of the ENDIAN VPN Server.

I	OpenVPN - Virtual Private Networking							
	>> Server configuration	Accounts Advanced	VPN client download					
	» Advanced settings							
	Port:	1194	Block DHCP responses coming from tunnel:					
	Protocol:	UDP 💌	Don't block traffic between clients:					
	Note: You may allow multiple por	rts by port forward them						



eWONs + Local network of eWONs + eWONs see eWONs

Figure 19: Network: local network of eWONs

If you have a local network behind the eWONs, you can configure the ENDIAN Server to automatically handle the routes to these networks.

With this topology:

- All the devices on the corporate LAN have access to all the eWONs and to devices behind these eWONs
- All the devices on the corporate LAN have access to all the devices behind eWONs
- · All the eWONs have access to all the devices on the corporate LAN
- All the devices behind the eWONs have access to all the devices on the corporate LAN
- All the eWONs and devices behind have access to other eWONs and devices behind

ENDIAN Settings

In Advanced settings, allow trafic between clients.

OpenVPN - Virtual Private Networking							
 Server configuration 	ccounts Advanced	VPN client download					
Advanced settings							
Port:	1194	Block DHCP responses coming from tunnel:					
Protocol:		Don't block traffic between clients:					
Note: You may allow multiple ports by port forward them							



) DenVPN - Virti	ual Private I	Networking				
» Server configura		nts Advance	d VPN clier	beolowob tr		
Corror corrigan	Hecodi			il dofffiodd		
» Change account	ewon92					
Account informatio	n					
Username:			ewon92			
Password:			•••••	•••••		
Verify password:			•••••	•••••		
or						
Client routing	through the VP	N server:				
Doo't push any route:	s to client:					
Networks behind clier	nt:		10.1.1	10.0/04		
			10.1.1	.10.0/24		
Duch only these natu	vorke:				_	1
If this hox is empty mut	es to each of the	networks of the ot	ber			
clients will be pushed to	this client whenev	er it connects				
Custom push conf	iguration					
<u>Static ip addresses</u> :						
Push these nameserv	/ers:		,			
Duch domain:						
-uon uumain.			I			
Save						

And in each Accounts, you need to set the *Networks behind client*.

IMPORTANT

!

After changing the networks settings, the ENDIAN Server will invite you to restart the OpenVPN server.

This restart will disconnect all the VPN Clients (and they will automatically reconnect to the OpenVPN).

This OpenVPN reboot is required because when you change an account, maybe you have changed one of the Client Routing settings, and then the ENDIAN Server must send to <u>all the VPN clients</u> these new parameters.



Security

The previous chapter "Network topologies" allows you to globally design the shape of your network. For example, if you want the eWON_1 to have access to the corporate LAN and to one other eWON only, you cannot achieve that with the ENDIAN VPN configuration only.

To allow you to accurately define who has access to who in your VPN network, you need to use the Firewall functionality of the ENDIAN Server and more specifically the VPN Firewall.

<u>QUQIJU</u>	Endian Firewall Mini					
	System Status Network Services Firewall Proxy VPN Logs					
	VPN firewall configuration					
Port forwarding / NAT	>> VPN Firewall Settings					
Outgoing traffic						
nter-Zone traffic	Enable VPN firewall					
VPN traffic	(m)					
System access	Use the switch above to enable the VPN firewall. The VPN firewall gives the ability to globally DENY VPN traffic and explicitely configure VPN firewall rules.					

By default, this VPN Firewall is disabled. To enable it click on the switch button.

					21 Help			
endign					Endian Firewall Mini 📻			
	System Status	Network Services	Firewall Pro	oxy VPN L	ogs			
	VPN firewall cor	figuration						
Port forwarding / NAT	» Current rules							
Outgoing traffic	Califa and SON	financial inda						
Inter-Zone traffic	Add a new VPN	tirewall rule						
VPN traffic	# Source	Destination	Service	Policy Reman	k Actions			
	Legend M Enabl	ed (click to disable)	isabled (click to enable)	🦉 Edit 🎢 Rem	ove			
	VPN Firewall Settings Enable VPN firewall Log accepted VPN connections Save							
Figure 22: VPN Firew	vall enabled							



Now, the VPN Firewall is enabled and blocks all the VPN traffic because there is no rules defined. Click on the ③ Add a new VPN firewall rule link to create a rule.

Then, if you want to allow one user to access all the other VPN Clients, select the Source Type *User* and choose the name of the User in the list. In Destination, select the type User and choose *<ANY>* in the list. Don't forget to add a short description of your rule in the *Remark* field.

	System	orarus	NOLMOLY	JUNICES	THEWall	ноху	ALL N	Loga	
	VPN firev	vall con	figuration						
Port forwarding / NAT	» Current rules								
Outgoing traffic									
nter-Zone traffic	VPN firewall rule editor								
/PN traffic	C					D4:4:			
System access	Type *	User	•			Type *	Jser	•	
	select u ewon44 ewon44 ewon50 jcn prk Service Service	#Port *		ol * Des	tination port (d	ewon45 ewon46 ewon5 jcn ewon50 jcn		RL for multiselect)	
	Policy Action *	ALLOW	Remarkan	k PRK all VPN	access			Position * First 💌	
	Ena	bled	ΠLa	og all accepted p	ackets				
	Create	e rule or 9	Cancel						* This Field is require

And push the Create rule button.

PN fir	ewall con	figuration							
	rent rules	!	Fire to m Aț	wall rules ha nake the cha oply	ve been cł nges activ	nangei e	l and need to be ap	pplied in order	
 Cur Add 	a new VPN f	irewall rule							
» Cur <u>Add</u> # Sou	a new VPN f	irewall rule Des	tination	Servic	e F	Policy	Remark	Actions	

Use the Apply button to use immediately your new rule.

Create as many rules as required to build your *controlled* network.



Revisions		
Revision Level	Date	Description
1.0	2009-01-22	First release.

- i Microsoft, Internet Explorer, Windows and Windows XP are either registered trademarks or trademarks of Microsoft Corporation
- ii Firefox is a trademark of the Mozilla Foundation

Document build number: 37

Note concerning the warranty and the rights of ownership:

The information contained in this document is subject to modification without notice. The vendor and the authors of this manual are not liable for the errors it may contain, nor for their eventual consequences.

No liability or warranty, explicit or implicit, is made concerning quality, the accuracy and the correctness of the information contained in this document. In no case the manufacturer's responsibility could be called for direct, indirect, accidental or other damage occurring from any defect of the product or errors coming from this document.

The product names are mentioned in this manual for information purposes only. The trade marks and the product names or marks contained in this document are the property of their respective owners.

This document contains materials protected by the International Copyright Laws. All reproduction rights are reserved. No part of this handbook can be reproduced, transmitted or copied in any way without written consent from the manufacturer and/or the authors of this handbook

eWON sa, Member of ACT'L Group. Subject to change without notice.



ENDIAN with eWON (Getting started)