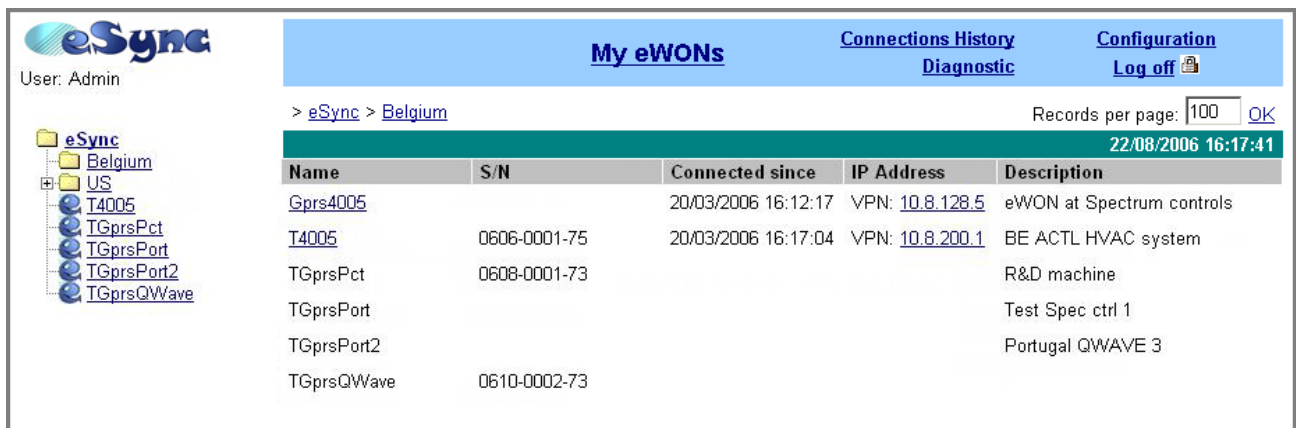


eSync VPN Server Configuration

The screenshot shows the eSync web interface. On the left is a navigation tree with folders for 'Belgium' and 'US', and sub-items like 'T4005', 'TGprsPct', 'TGprsPort', 'TGprsPort2', and 'TGprsQWave'. The main area is titled 'My eWONs' and shows a table of connected devices. The table has columns for Name, S/N, Connected since, IP Address, and Description. The current view is for the 'Belgium' folder, showing a list of devices connected on 20/03/2006.

Name	S/N	Connected since	IP Address	Description
Gprs4005		20/03/2006 16:12:17	VPN: 10.8.128.5	eWON at Spectrum controls
T4005	0606-0001-75	20/03/2006 16:17:04	VPN: 10.8.200.1	BE ACTL HVAC system
TGprsPct	0608-0001-73			R&D machine
TGprsPort				Test Spec ctrl 1
TGprsPort2				Portugal QWAVE 3
TGprsQWave	0610-0002-73			

Contents

This application user guide explains step by step how to configure eSync and the eWON in order to link them by a VPN network using the eWON as VPN-client and eSync as VPN-Server.

Important: The VPN solution presented in this document is superseded by newer technologies and products including Talk2M and eFive.

1	Hardware and software requirements.....	3
1.1	Hardware requirements.....	3
1.2	Software requirements.....	3
1.3	eWON Firmware Version.....	3
2	What is a VPN for ?.....	4
3	eWONs as VPN routers.....	5
4	VPN : general topology.....	5
4.1	VPN server.....	6
4.2	Local User Connection and Remote.....	9
4.3	eWON dial-up on VPN.....	11
4.4	eWON GPRS as VPN Gateway.....	14
4.5	eWON2005CD as broadband VPN router.....	17
4.6	Appendix - eWON with C configuration.....	22
	Revision history.....	23

1 Hardware and software requirements

1.1 Hardware requirements

In order to follow this guide you will need:

- 1 eWON with a second Ethernet interface (for example : eWON 2005CD, 4005CD)

1.2 Software requirements

eWON configuration software:

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

Additionally we suggest you to download the eBuddy utility on our website : <http://support.ewon.biz>. 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 backup/restore your configuration or upgrade the firmware of your eWON (if required).

eGorbit:

To establish the VPN connection you need to install eGorbit on your PC. This software will act as VPN Client for the VPN connection to the VPN server (eWON).

eGorbit can be downloaded for free from our website: <http://support.ewon.biz>.

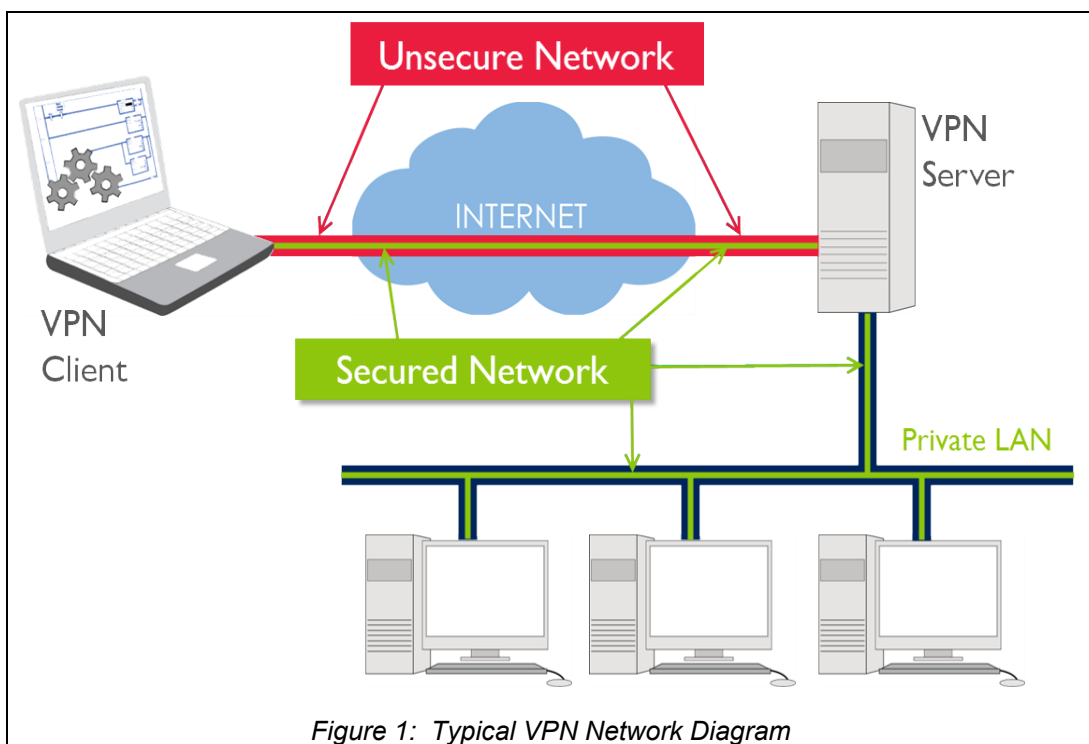
1.3 eWON Firmware Version

To be able to follow this guide your eWON needs a firmware version 5.2s0 or higher. A simple way to realize the eWON firmware upgrade is to use eBuddy, the eWON software companion.

2 What is a VPN for ?

A Virtual Private Network (VPN) is a private communication network usually used within a company, or between companies or organizations, in order to establish secured communication using the public network.

A good compromise is to use the *Internet* as carrier with a *tunneling* protocol (encapsulating the encrypted data). This network is called **virtual** because it links two physical networks (LAN) with a untrusted link (Internet). This network is called **private** because only the computers (or devices) connected on this particular VPN can understand the encrypted data.



In brief, a VPN provide you a global secured link at low cost.

Advantages of VPN:

- low cost
as compared to a real Wide Area Network based on expensive leased lines.
- scalability
It is easy to add/remove a computer from the VPN.

Disadvantages of VPN:

- VPNs require an in-depth understanding of public network security issues and taking proper precautions in VPN deployment.
- The availability and performance of an organization's wide-area VPN (over the Internet in particular) depends on factors largely outside of their control.
- VPN technologies from different vendors may not work well together due to immature standards.
- VPN need to accommodate protocols other than IP and existing ("legacy") internal network technology.



The purpose of this document is to show you how to setup your VPN (Virtual Private Network) with eWONs.

3 eWONs as VPN routers

To build your VPN, all connected devices need to *speak* the same encrypted language. On recent computers, the VPN software handles the VPN layer. In the case of older computers or other Ethernet devices like PLCs, it is impossible to include these devices into the VPN network.

You need to build a Network in a way completely transparent for the participants. This job is done by using **VPN Routers**. Not all eWON models are able to act as VPN Routers.

On the computer side, you have two software companions :

	eGabit : the VPN connection tool
	eSync Connect : the VPN Server application

Today, there are many VPN technologies available, we choose to build VPN on the

OpenVPN standard see <http://openvpn.net>.

In eSync Connect, we need WebServer, DataBase and ServerSide technologies, we choose to use

Apache see <http://www.apache.org>
MySQL see <http://www.mysql.com>
PHP see <http://www.php.net>

4 VPN : general topology

With a VPN, you generally build a network like the one in Figure 2.

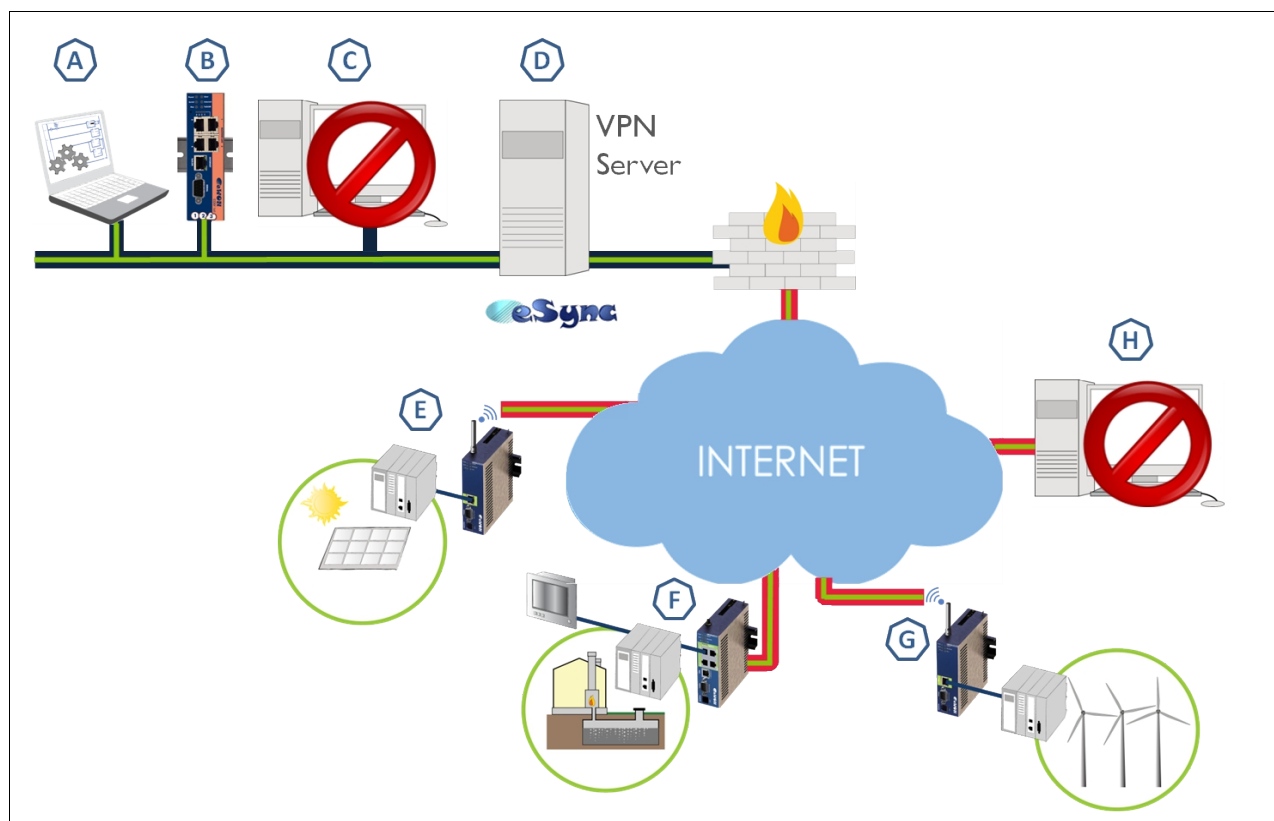


Figure 2: VPN general topology

Devices A, B, D, E, F and G are on the same Virtual Private Network. All devices on the VPN can connect to any other belonging to the same VPN network. The devices C and H have access to Internet but have no access to the VPN network.

4.1 VPN server

To build a VPN, you need a server acting as master of VPN communications. Every device has to ask the Server to enter on the VPN.

eWON developed the **eSync** application to make the installation, configuration and daily use of the VPN easier. The installation of your eSync is very simple (follow the installer) and eSync will install on your computer :

- An Apache WebServer listening on port 80
Even if you have already a Webserver running on your computer, but in this case, eSync will listen on port 81.
- A MySQL Database listening on port 3306
Even if you have already another one running on your computer, but in this case, MySQL will use the port 3307.
- An OpenVPN layer composed of Services listening the port UDP 1194
Even if you have already another OpenVPN running on your computer, but in this case, eSync will use the port 1195.

And you are ready to establish secured connections. You can view your VPN interface on your Network Connections window (renamed here in VPN connection).

LAN or High-Speed Internet			
VPN Connection	LAN or High-Speed Inter...	Connected	TAP-Win32 Adapter V8
Local Area Connection	LAN or High-Speed Inter...	Connected	Intel(R) PRO/1000 MT N...

Figure 3: Network connections

With the eSync application, you manage your VPN by opening a secure tunnel of communication between every VPN actors and the Server.
 The standard setup of eSync will build a VPN where all actors receive an IP address on the range 10.8.x.x.

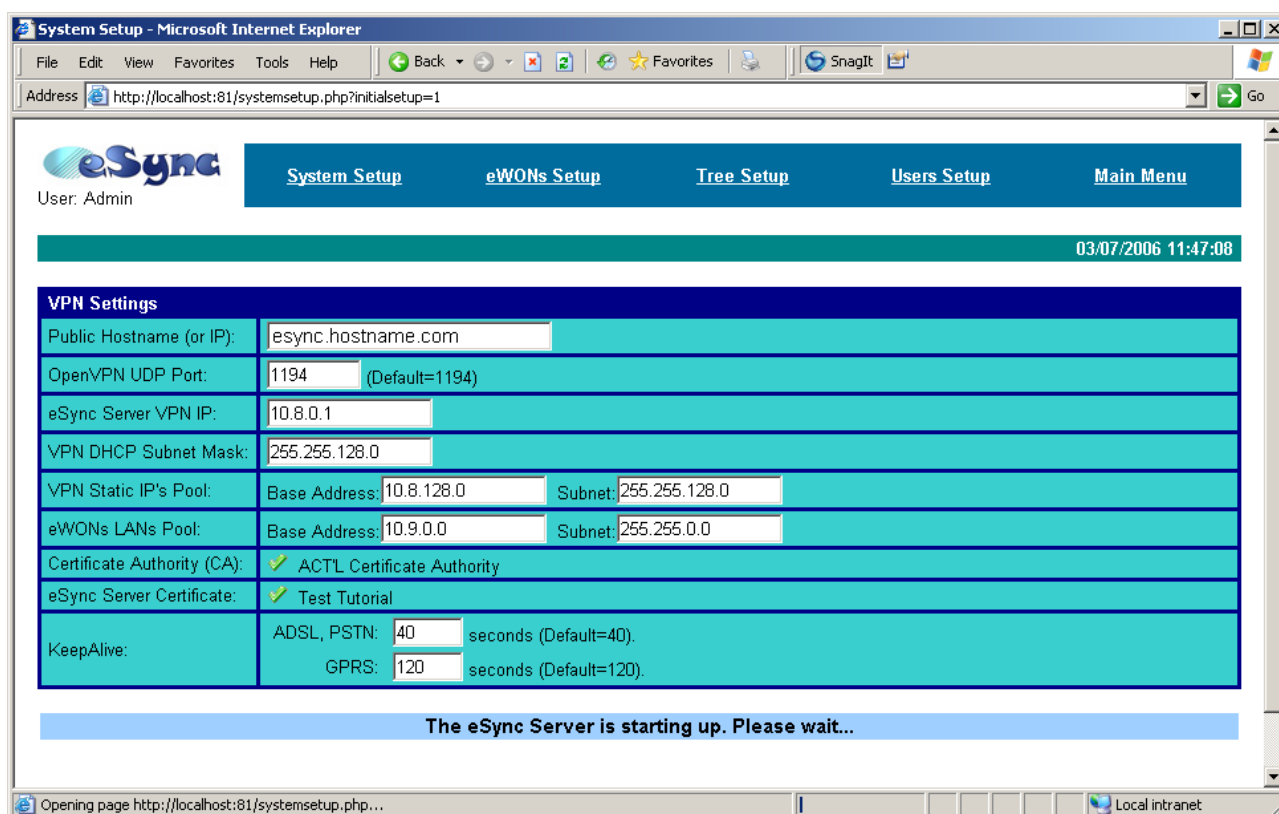


Figure 4: eSync VPN settings

These addresses could be assigned statically or dynamically.
 By default, the IP address ranges are divided in two, one half for the Static IP's and the other half for DHCP IP's.
 You can define also the Base Address of all devices placed on the LAN side of eWON-VPN.
 Then, in our default configuration (see Figure 4), all devices placed behind an eWON-VPN must have an address beginning by 10.9.x.x. to be accessible on the VPN.

After the installation, you configure eSync with your Browser, just connect you to the LAN IP address of the server (and use the right port if necessary).

The Admin account of eSync is by default :

login: **adm**
 password: **adm**

If your Server is accessible on your LAN, you can access to eSync from every computer.


Warning!

For security reasons, changing the default password **adm** is absolutely required. To change the **adm** password, from the menu bar, click on **Users Setup** and double click on the **adm** entry to edit its parameters. Enter the new password twice and click **Save**.

Server requirements:

- The Server must be *accessible from Internet*, generally through a fixed IP address.
- Port TCP 80 must be open for the HTTP traffic (or 81 if eSync was installed on 81)
- Port UDP 1194 must be open on the Server.

4.2 Local User Connection and Remote

If you want to go on the VPN from a computer, you need to use the VPN Client  eGrabit. You can download it freely from the www.ewon.biz website. The installation requires no parameters. Now, you need a VPN account. Go on eSync Configuration, select Users Setup and click on Create New User link.

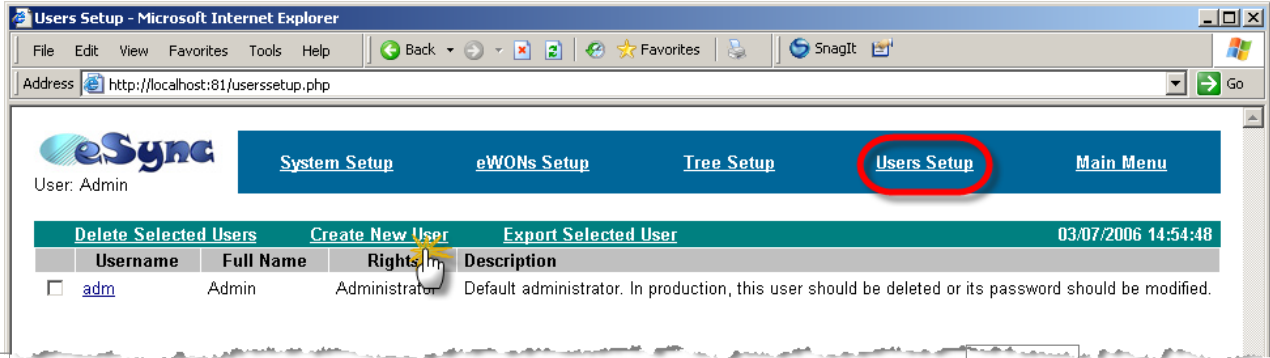
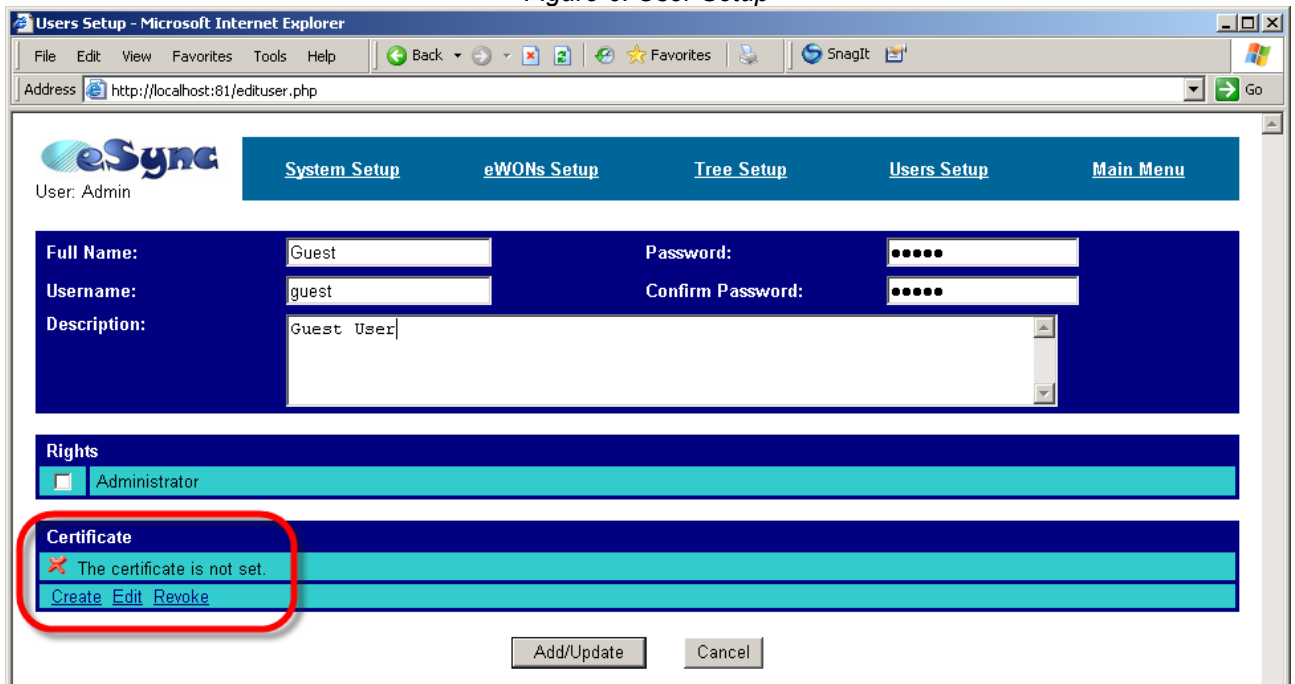


Figure 5: Create new user

Fill all information

Figure 6: User Setup



You must have the following display when Certificate is generated.



Figure 7: User Certificate generated

Now, you need to export this Certificate to your local computer.

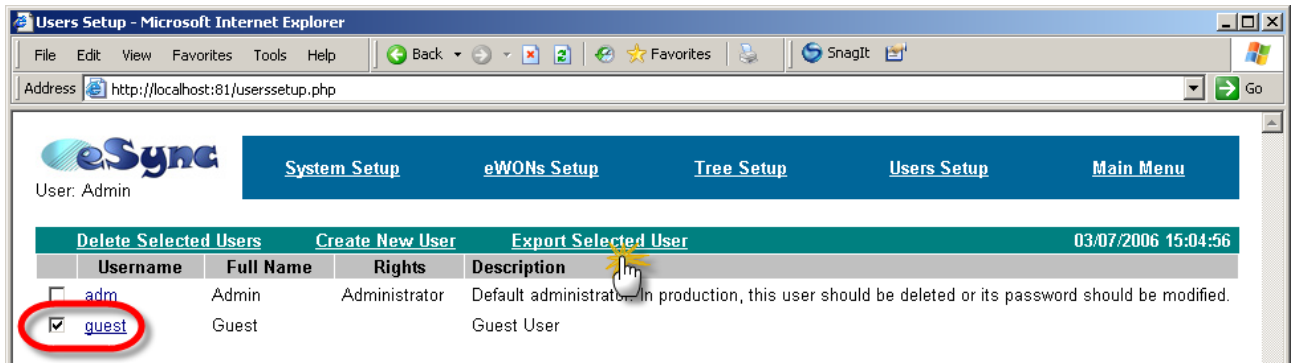
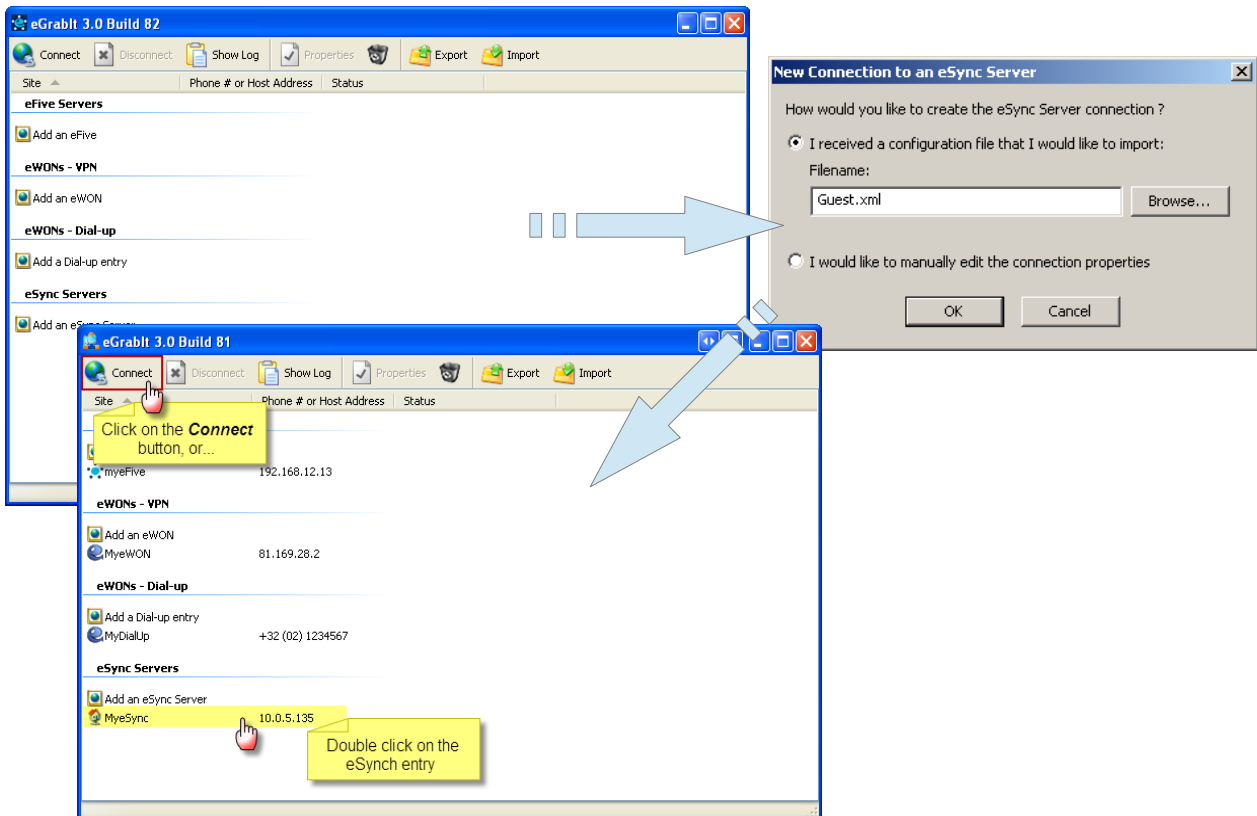


Figure 8: Export User Certificate

For that, select the User you want to export and click to the *Export Selected User* link. You will be prompted to give the location and name for this XML file.



In eGrabIt, click on the *Add an eSync Server* link and use your User Certificate file to create your VPN link.



If you double-click on the new eSync Server connection, you will enter in the VPN. Now, your computer has access to all the devices connected to the VPN.

For example, you can connect to eSync through the VPN connection if you go to <http://10.8.0.1:81> (my installation is on port 81).

4.3 eWON dial-up on VPN

To connect your eWON on the VPN, you need to create an account for it. Go on eSync Configuration, select eWONs Setup and click on the Add an eWON link.

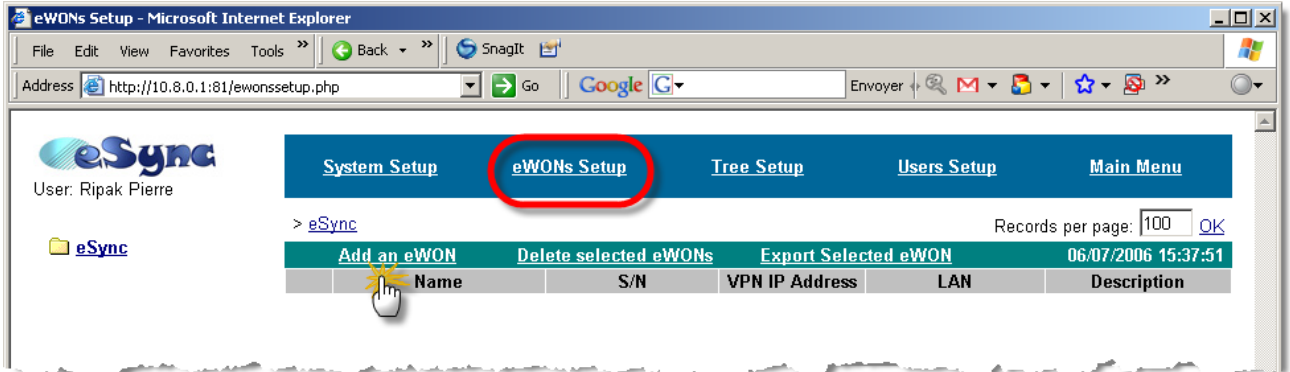


Figure 9: Create eWON VPN

Fill all information

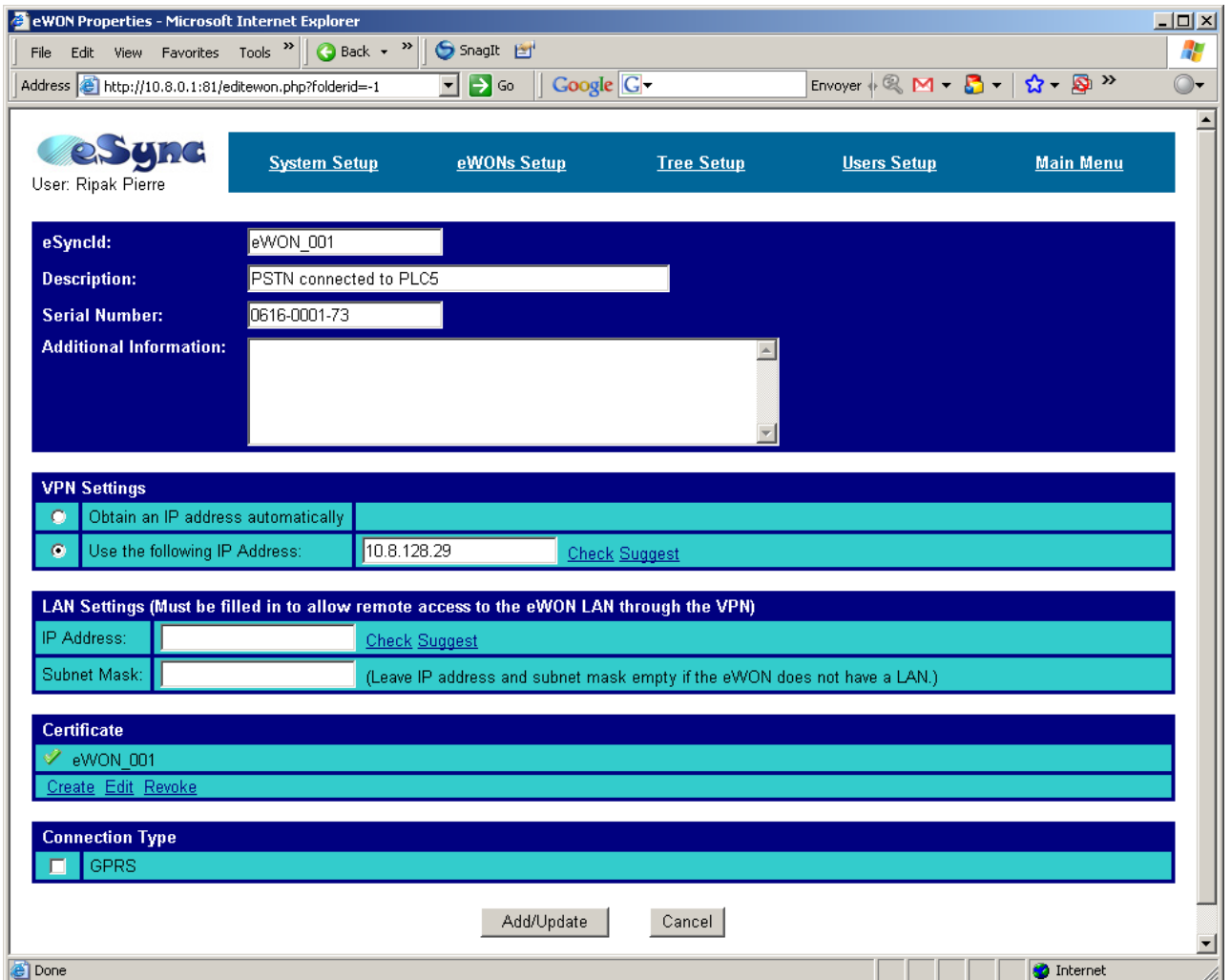


Figure 10: eWON setup

Use the *Suggest* link to select a free Fixed IP Address.
 Don't forget to create the Certificate!
 Now, you need to export this Certificate to your local computer.

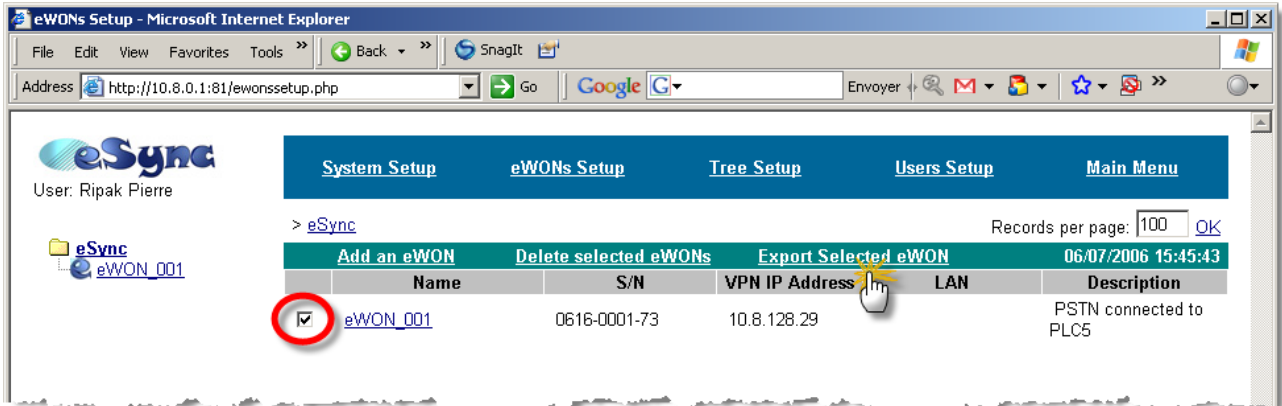
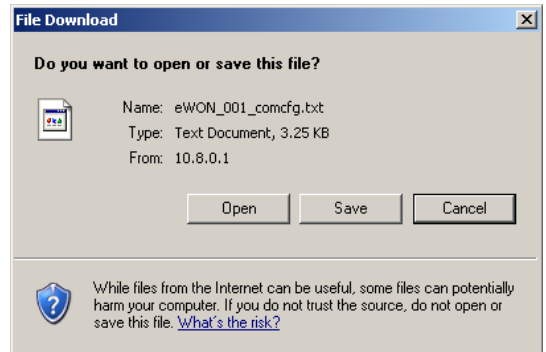


Figure 11: Export eWON Certificate

For that, select the eWON you want to export and click to the *Export Selected eWON* link.
 You will be prompted to give the location of the file.

This file is a Key to enter in your VPN !
 Store it to a secured place or destroy it after usage. you can re-export it if you need it again.



Note that suggested filename is "eWON_001_comcfg.txt", the VPN parameters are formatted in the file to be uploaded by FTP to configure the eWON. Just rename the file in "comcfg.txt" and send it to the eWON by FTP.

```

VPNcNxType:2
VPNKeyType:1
VPNSecretKey:-----BEGIN RSA PRIVATE KEY-----
MIICXA.....
-----END RSA PRIVATE KEY-----
VPNSecretCert:-----BEGIN CERTIFICATE-----
MIIDKj.....
-----END CERTIFICATE-----
VPNCACert:-----BEGIN CERTIFICATE-----
MIIDGT.....
-----END CERTIFICATE-----
VPNPortOut:1194
VPNA1ive:40
VPNSrv1:support.ewon.be
VPNSrv2:
VPN2PIpMode:0
    
```

Now, your eWON has the VPN configuration in place. At every connection of this eWON on Internet, it will setup the VPN tunnel with the server. For example, you can configure your eWON-pstn to use the Callback sequence to connect to Internet and VPN.

Once the eWON is on the VPN, the eSync main page shows you the eWON connected by displaying the IP address of it.

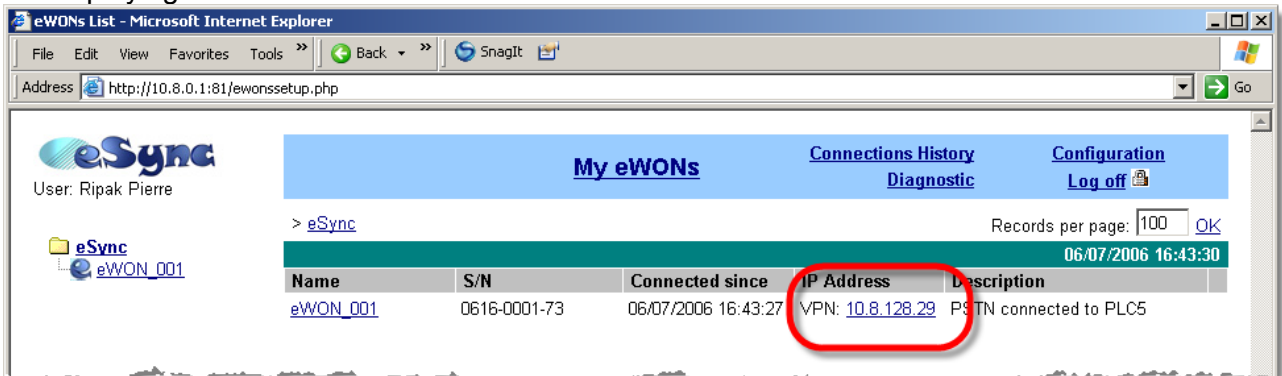


Figure 12: eSync shows eWON connected

If you open another Internet Browser and use this address (<http://10.8.128.29>), you will be connected on your eWON through the VPN.

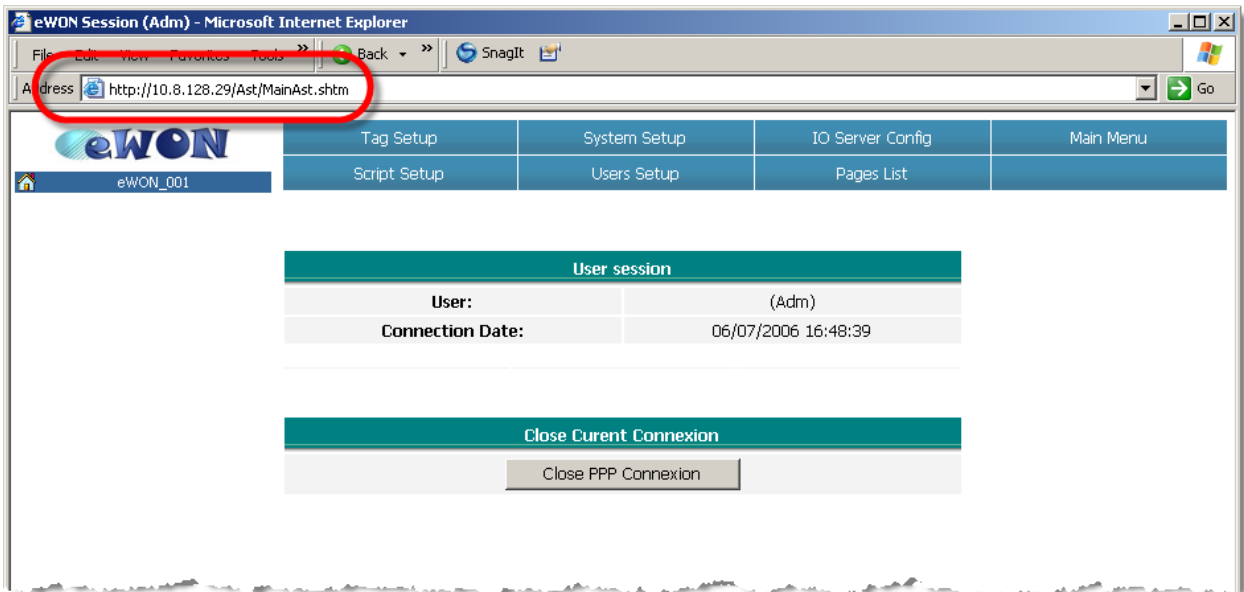


Figure 13: on eWON by VPN

If the WAN Protection (Security) is set to maximum (see Figure 14), the eWON website is accessible only through the VPN (the WAN address provided by the ISP will not answer).

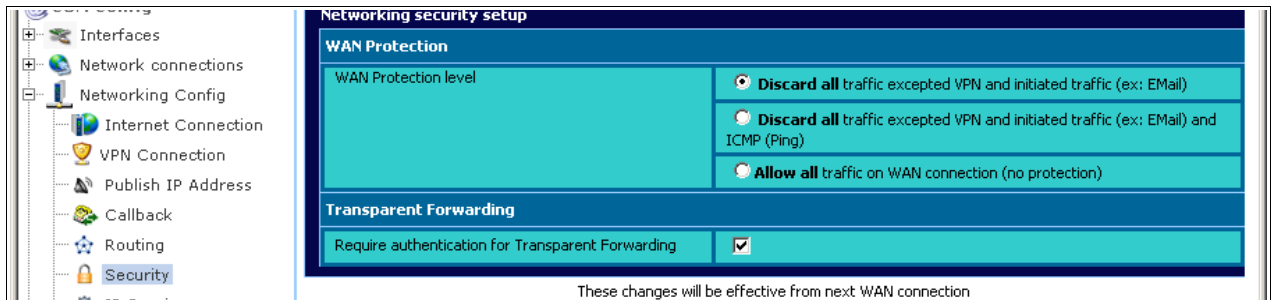


Figure 14: WAN Protection

If you have a PLC connected to this eWON and you want to access it with the corresponding software, simply use this VPN IP address.

4.4 eWON GPRS as VPN Gateway

The configuration of an eWON acting as VPN Gateway is the same as in the point “eWON dial-up on VPN“

The only things that change in this configuration are :

- eWON is used as Gateway to other ethernet devices
- eWON uses the built in GPRS modem to be connected (permanently) to Internet

Once you create the eWON in eSync, configure the LAN settings parameters (use the *Suggest* link).

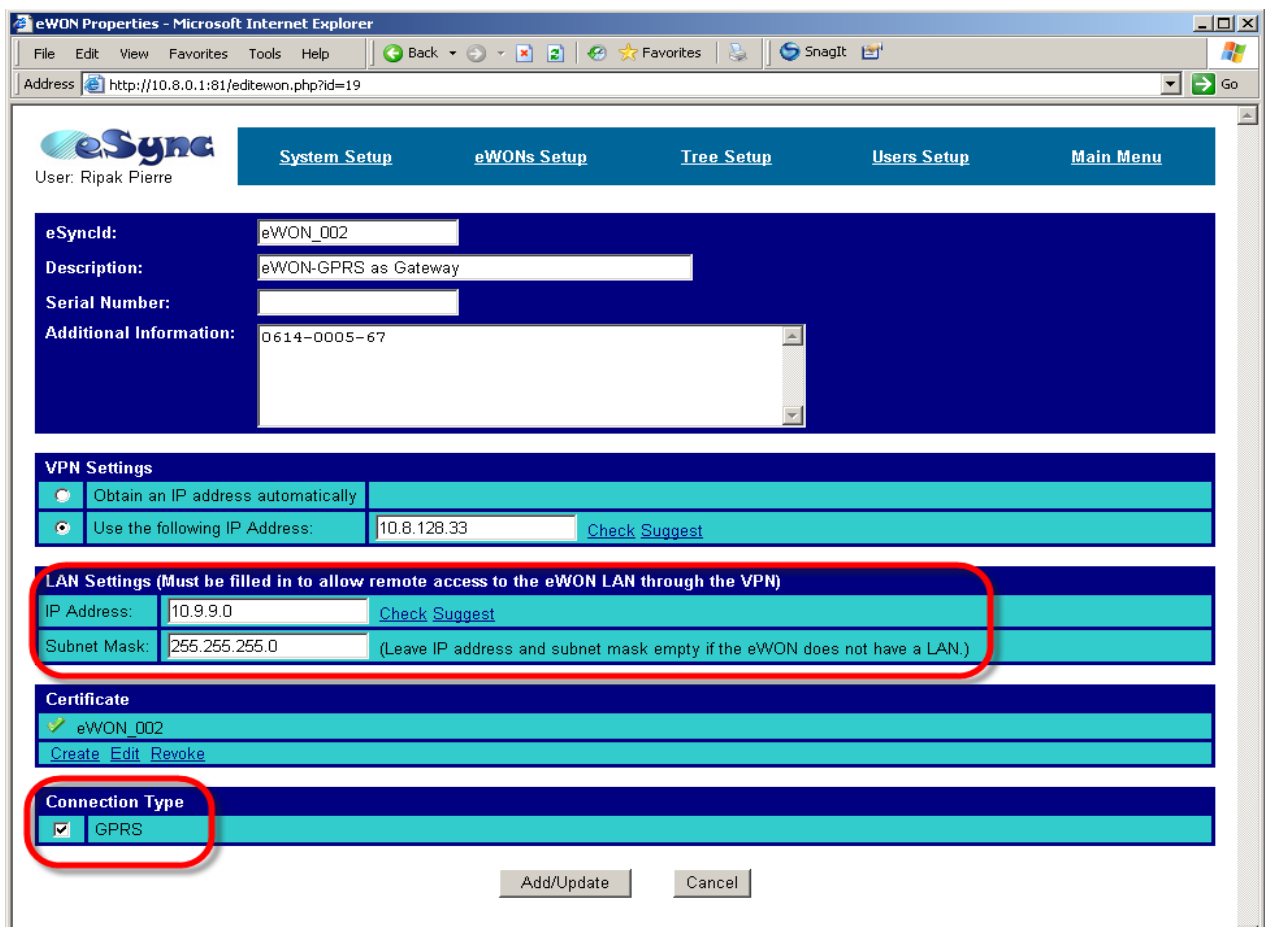


Figure 15: create eWON with a LAN

Then, all devices (and eWON) must have an IP address in this 10.9.9.x range to be part of the VPN.

If eWON has the 10.9.9.1 address, don't forget to set this address as Gateway in other devices. If your eWON is an GPRS one, you can check the *GPRS connection Type*. This option will send the KeepAlive frame slowly (in GPRS, you pay for the traffic not for the time connected).

Once the Certificate is in the eWON, you may configure the eWON to play the Gateway behavior you want. The Gateway function is always activated in eWON - VPN, you no longer have to check the “Enable IP Gateway” checkbox (like with firmware 4.x).

Go on the eWON *Routing page*, and set the option you need.

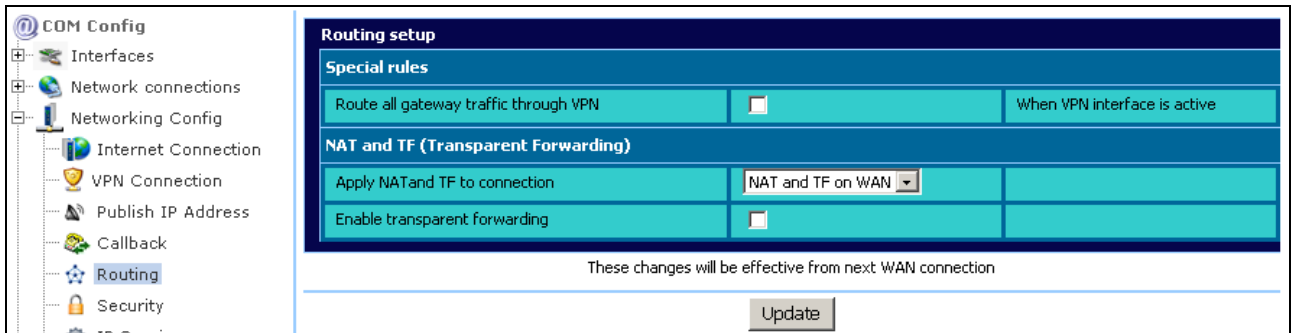


Figure 16: eWON Routing page

Usually, you need to set the NAT and TF (Transparent Forwarding) on WAN. This configuration allows your ethernet devices to use the both interfaces (WAN and VPN) to go outside. The WAN will be used if your device send an eMail to the ISP. The VPN connection will be use when the device needs to access another VPN participant or when it replies to a request coming from the VPN.

As you are in GPRS, you can stay connected permanently to Internet, check the *Maintain Connection* checkbox.

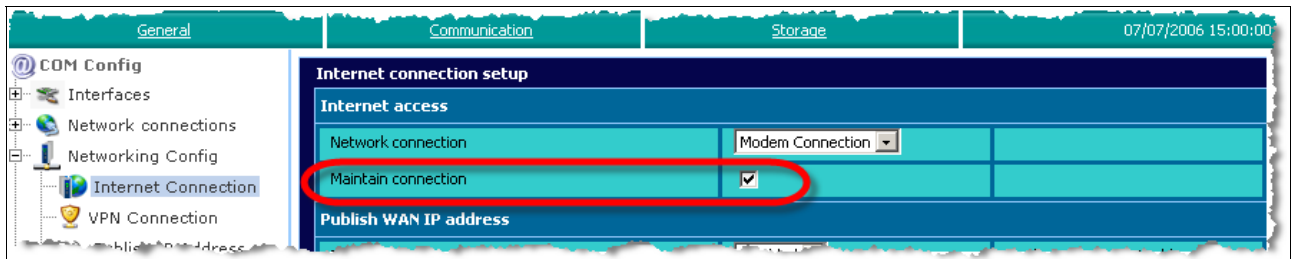


Figure 17: Maintain Connection parameter

Be aware that eWON and eSync will send small packets (ping) to maintain the connection open (KeepAlive). Then this permanent connection will cost some money (even if there is no usefull traffic). Once connected on GPRS, the eWON will establish its VPN connection and be accessible by other VPN participants.

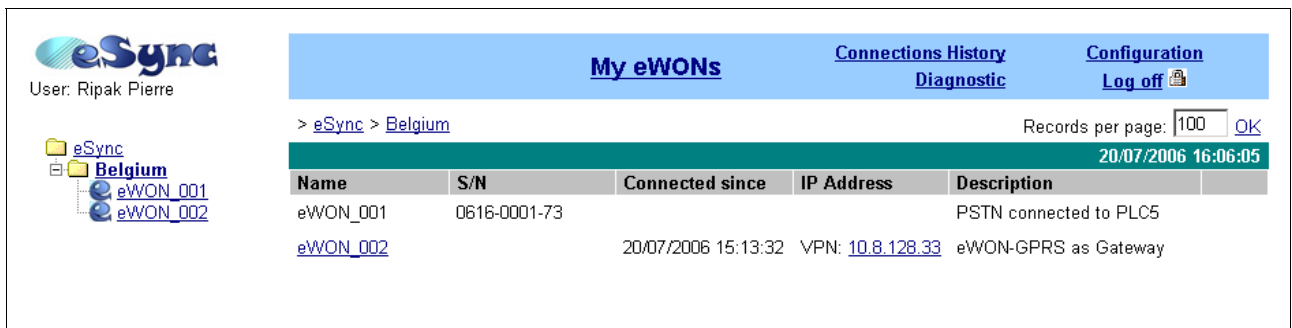
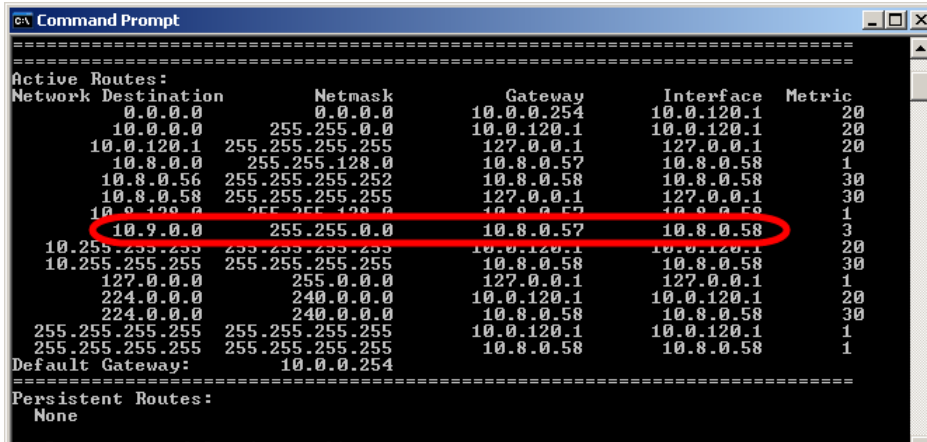


Figure 18: eWON-Gateway connected

The eWON is accessible at the address 10.8.128.33 (address on the VPN) or at the address 10.9.9.1 (address on the eWON LAN). The devices placed on the LAN of the eWON are accessible by their address 10.9.9.x directly from your computer.

If you display the *IP Routes* of your computer (command `ROUTE PRINT` in a DOS box), you will see that VPN has automatically add a Route to the 10.9.0.0 (Base Address of eWONS LAN pools in the eSync Setup).



```
=====  
Active Routes:  
Network Destination    Netmask          Gateway          Interface        Metric  
-----  
0.0.0.0                0.0.0.0          10.0.0.254       10.0.120.1       20  
10.0.0.0                255.255.0.0      10.0.120.1       10.0.120.1       20  
10.0.120.1             255.255.255.255  127.0.0.1        127.0.0.1        1  
10.8.0.0                255.255.128.0    10.8.0.57        10.8.0.58        1  
10.8.0.56              255.255.255.252  10.8.0.58        10.8.0.58        30  
10.8.0.58              255.255.255.255  127.0.0.1        127.0.0.1        30  
10.0.120.0             255.255.128.0    10.8.0.57        10.8.0.58        1  
10.9.0.0                255.255.0.0      10.8.0.57        10.8.0.58        3  
10.255.255.255         255.255.255.255  10.0.120.1       10.0.120.1       20  
10.255.255.255         255.255.255.255  10.8.0.58        10.8.0.58        30  
127.0.0.0              255.0.0.0        127.0.0.1        127.0.0.1        1  
224.0.0.0              240.0.0.0        10.0.120.1       10.0.120.1       20  
224.0.0.0              240.0.0.0        10.8.0.58        10.8.0.58        30  
255.255.255.255        255.255.255.255  10.0.120.1       10.0.120.1       1  
255.255.255.255        255.255.255.255  10.8.0.58        10.8.0.58        1  
Default Gateway:      10.0.0.254  
=====  
Persistent Routes:  
None
```

Figure 19: IP Routes

4.5 eWON2005CD as broadband VPN router

In this configuration, you may want to use an ADSL router because you need to transmit a lot of data.

The setup of this eWON is very similar than those from point 4.3 and 4.4.

The only thing that differs from point 4.4 is :

- the eWON use its WAN interface to connect on Internet.

Once you create the eWON in eSync, configure the LAN parameters like following.

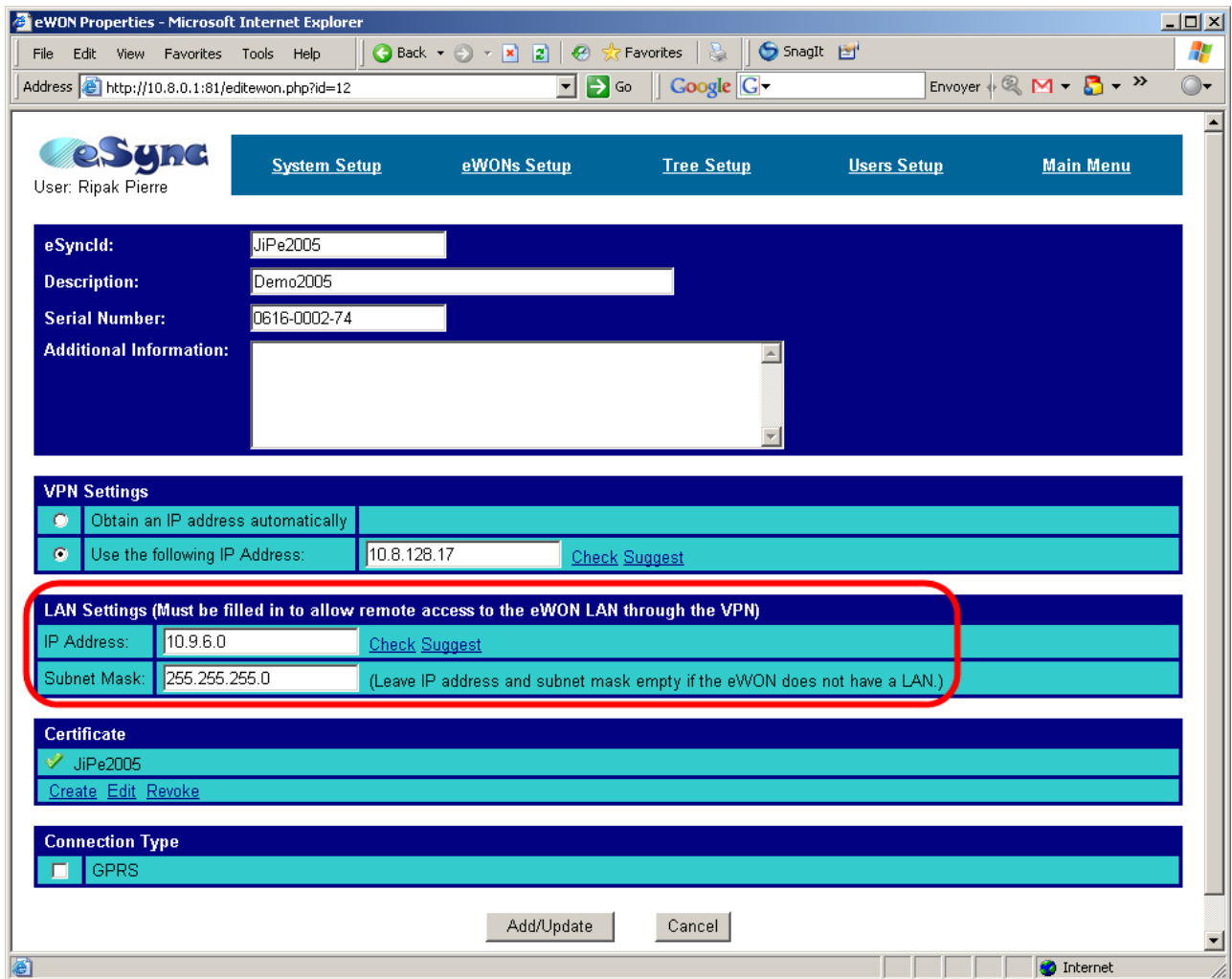


Figure 20: setup eWON2005CD in eSync

Then, all devices must have an IP address in the 10.9.6.x range to be part of the VPN.

On the eWON2005CD, you have two Ethernet interfaces to configure, the LAN and the WAN.

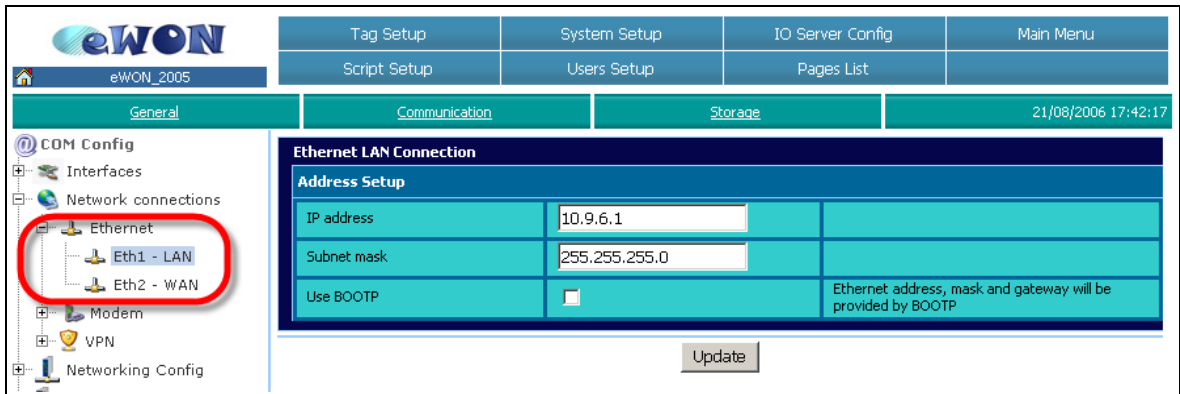


Figure 21: eWON2005CD - LAN setup

Then, if your eWON2005CD has the 10.9.6.1 LAN IP address, don't forget to set this address as Gateway in the devices you want to access.

And the WAN Ethernet interface must be configured with parameters compatible with your ADSL device.

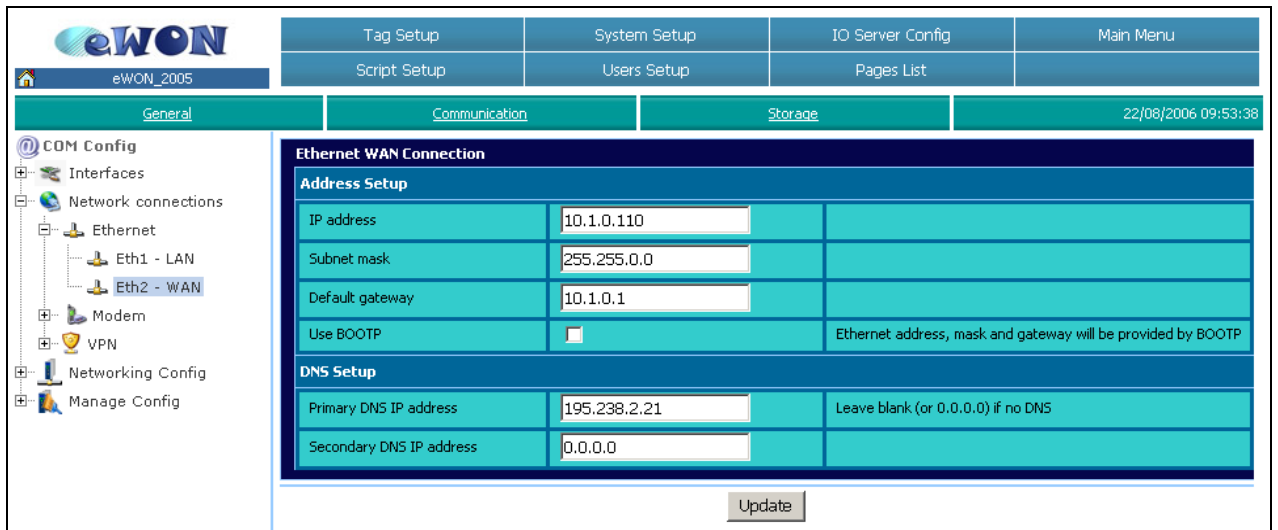


Figure 22: eWON2005CD WAN setup

Here, you can see that we have an ADSL router on the 10.1.0.1 (eWON default gateway).

The IP addresses of your Remote Site will be as shown on the right.

There is no MODEM configuration to set. You can disable the Modem Outgoing Connection.

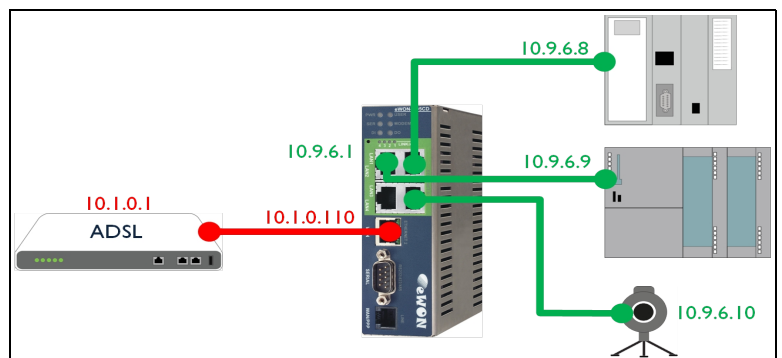


Figure 23: eWON2005CD remote site IP addresses

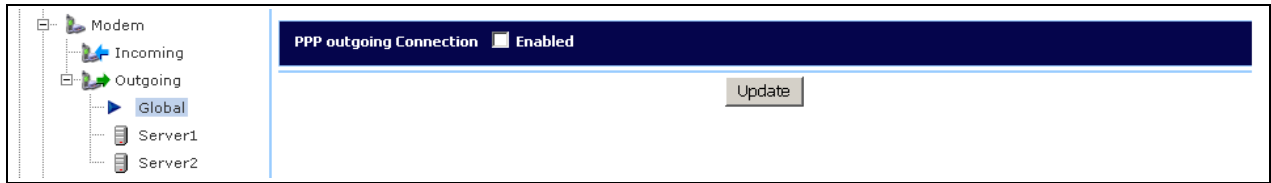


Figure 24: eWON2005CD Outgoing connection disable

The VPN configuration is always the same. Put the certificate generate by eSync in the eWON.

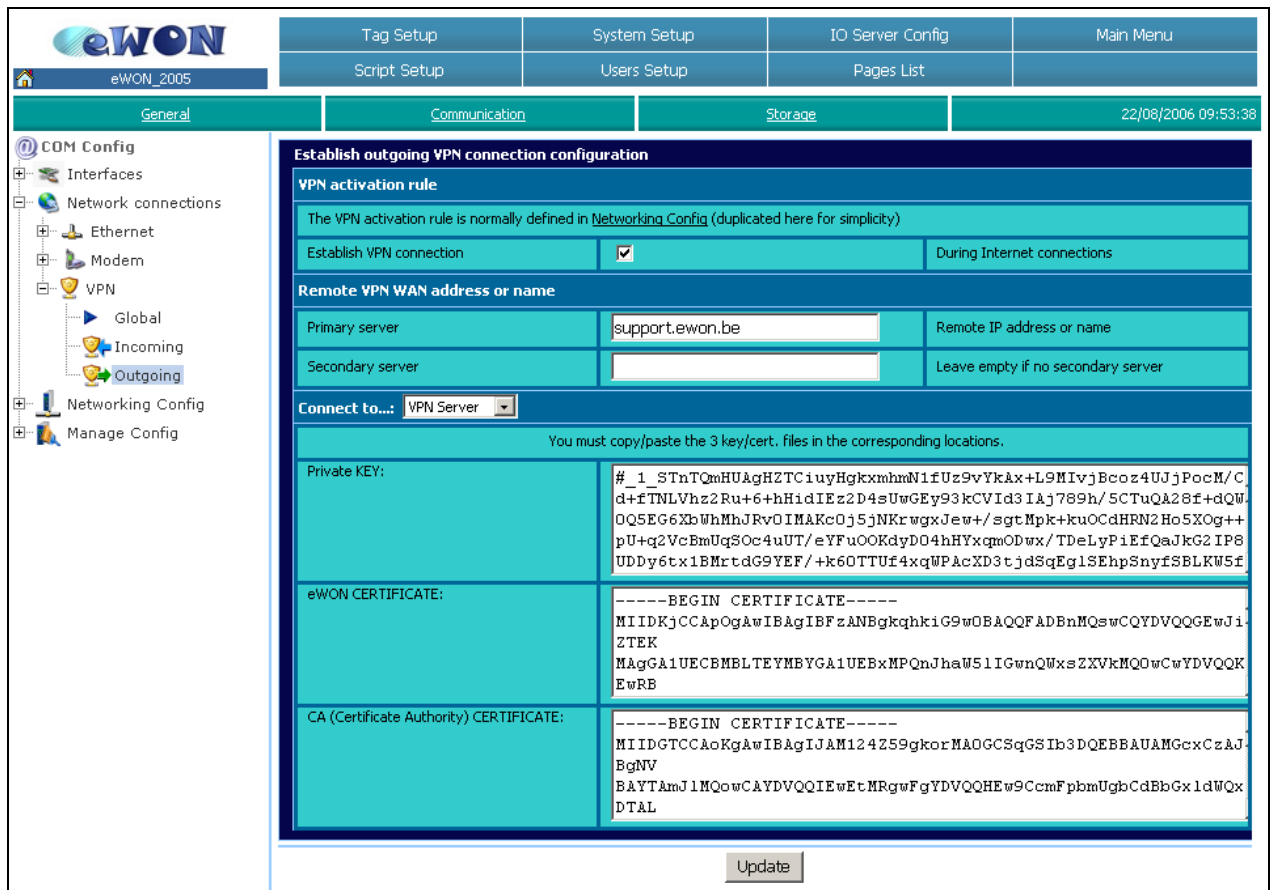


Figure 25: eWON2005CD VPN certificate setup

In the Networking Config branch, the *Internet Connection* must be set on the WAN interface.

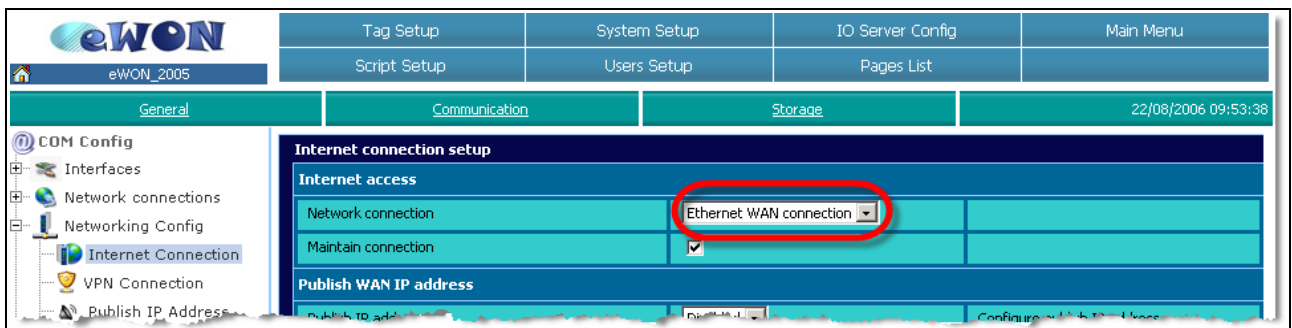


Figure 26: eWON2005CD Internet Connection

If you need a permanent access to Internet, use the *Maintain Connection* checkbox (as shown).

VPN Connection must be enable.

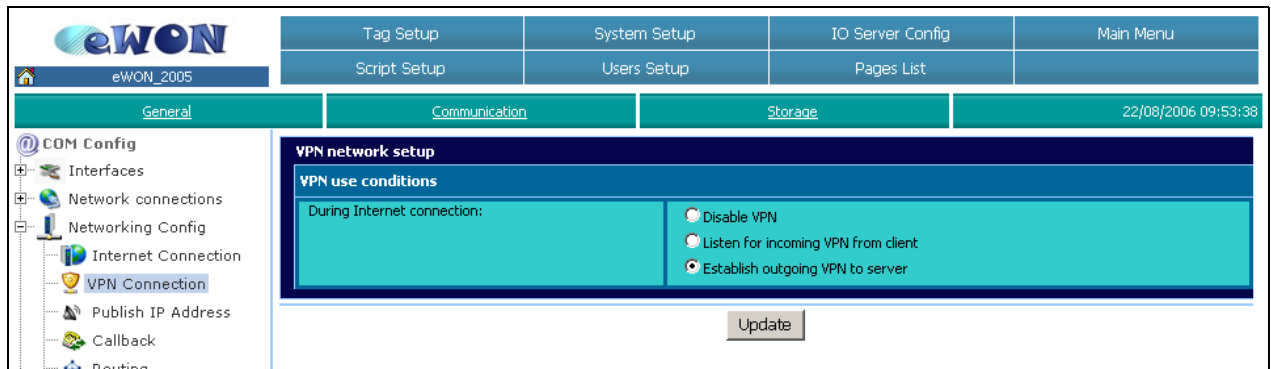


Figure 27: eWON2005CD VPN connection

Set the *Routing* configuration if you need to allow devices on LAN to go outside.

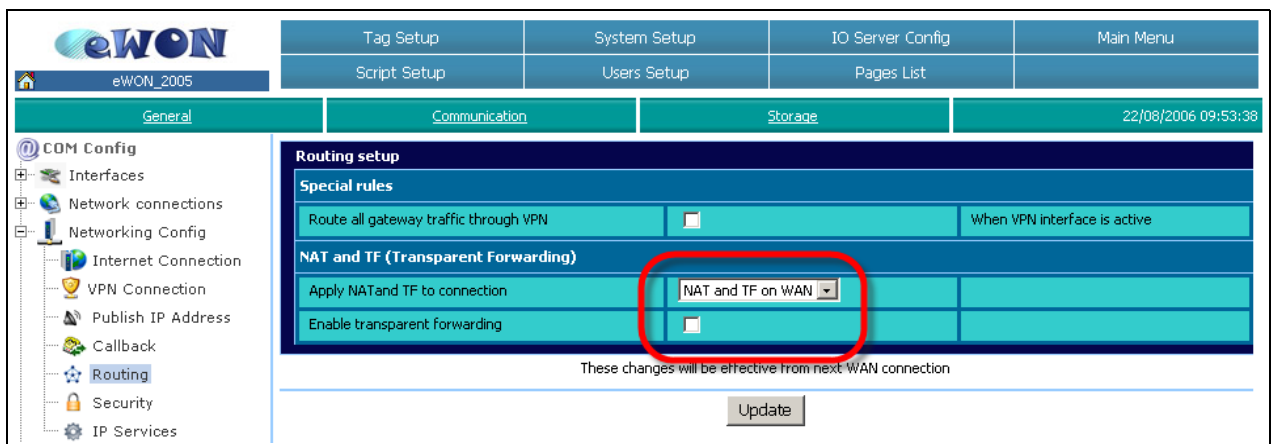


Figure 28: eWON2005CD Routing

Set the *Security* you need.

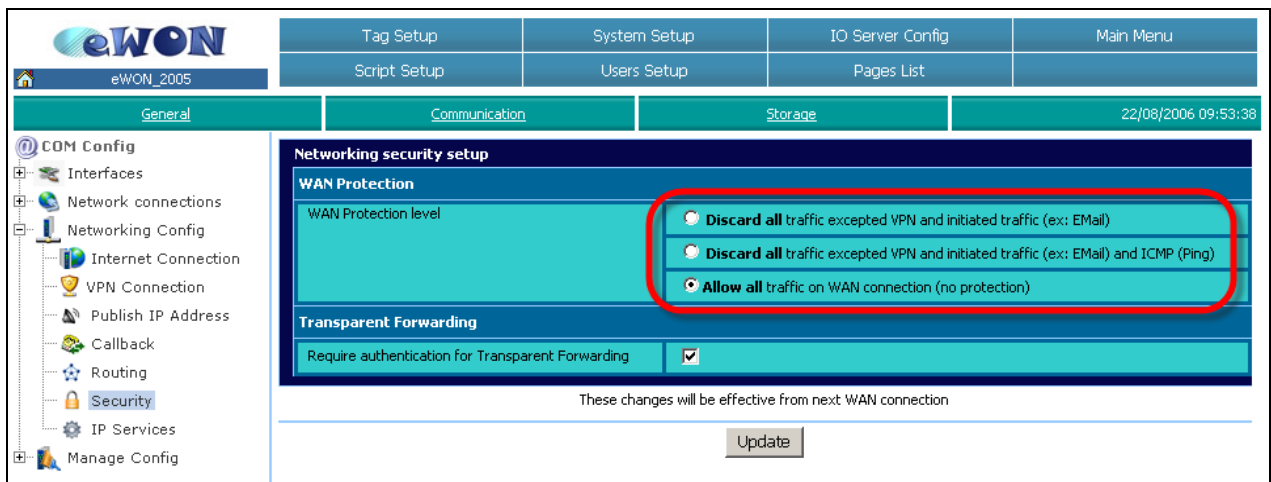


Figure 29: eWON2005CD Security

With a *WAN Protection Level* set to “Allow All”, your eWON accept also traffic coming from the “unsecured” world (not VPN).

With this configuration, you can access your eWON2005-VPN through the ADSL.

The screenshot shows the eSync web interface. The user is 'Ripak Pierre'. The location is 'Belgium'. A table lists the following eWON devices:

Name	S/N	Connected since	IP Address	Description
Gprs4005				eWON at Spectrum controls
T4005	0606-0001-75			BE ACTL HVAC syst
TGprsPct	0608-0001-73	22/08/2006 15:49:42	VPN: 10.8.128.17	R&D machine
TGprsPort				Test Spec ctrl 1
TGprsPort2				Portugal QWAVE 3
TGprsQWave	0610-0002-73			

Figure 30: eWON2005CD connected in eSync

The eWON2005CD is accessible at this VPN address 10.8.128.17 and at this LAN address 10.9.6.1 (eSync knows that all address belonging to 10.9.6.x must be routed to this eWON2005CD). You can PING your eWON at 10.9.6.1 and your LAN device at 10.9.6.8.

```

C:\>ping 10.9.6.1
Pinging 10.9.6.1 with 32 bytes of data:
Reply from 10.9.6.1: bytes=32 time=23ms TTL=255
Reply from 10.9.6.1: bytes=32 time=27ms TTL=255
Reply from 10.9.6.1: bytes=32 time=26ms TTL=255
Reply from 10.9.6.1: bytes=32 time=27ms TTL=255
Ping statistics for 10.9.6.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 23ms, Maximum = 27ms, Average = 25ms
C:\>
C:\>
C:\>ping 10.9.6.8
Pinging 10.9.6.8 with 32 bytes of data:
Reply from 10.9.6.8: bytes=32 time=27ms TTL=254
Reply from 10.9.6.8: bytes=32 time=25ms TTL=254
Reply from 10.9.6.8: bytes=32 time=26ms TTL=254
Reply from 10.9.6.8: bytes=32 time=23ms TTL=254
Ping statistics for 10.9.6.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 23ms, Maximum = 27ms, Average = 25ms
C:\>
    
```

Figure 31: ping through VPN

4.6 Appendix - eWON with C configuration

PPP outgoing Connection - Enabled

Global outgoing connections parameters

- Dial and connection timeout
- Enable protocol compression
- Delay between dialout retries
- Maximum connection time
- Idle time before hanging up
- Max outgoing call duration
- Hangup if no outgoing action after
- Error recovery**
 - Select next server in case of error
 - Reset modem after
- Calls budget management**
 - Allocated budget
 - Reset budget period: 168 hours
 - Current budget period: 00:00:00
 - Volume: IN: 92059, OUT: 116026, Last reset: 01/01/1970 00:00:00

PPP outgoing Connection - Server 1

Server access setup

- Server phone number: 0,090930199
- User name: am264240
- Password: [REDACTED]
- Require secure authentication (CHAP): (Otherwise allow PAP (password is sent in clear text))

Configuration common to all servers (summary) - editable in global outgoing configuration

- Dial and connection timeout: 180
- Enable protocol compression:
- Idle time before hanging up: 300

VPN Connection configuration

Advanced options

- Diagnosis level: Low
- Port In: 0
- Port Out: 1194
- Keep alive Interval: 40 seconds

Accept incoming VPN connection configuration

VPN activation rule

The VPN activation rule is normally defined in **Networking Config** (duplicated here for simplicity)

- Listen for incoming VPN connection: During Internet connections

Incoming VPN connection parameters

- Passphrase: [REDACTED]
- VPN IP addresses config: Automatic
- Local VPN IP address: 10.254.0.2
- Remote VPN IP address: 10.254.0.1

Establish outgoing VPN connection configuration

VPN activation rule

The VPN activation rule is normally defined in **Networking Config** (duplicated here for simplicity)

- Establish VPN connection: During Internet connections

Remote VPN WAN address or name

- Primary server: support.ewon.be Remote IP address or name
- Secondary server: [REDACTED] Leave empty if no secondary server

Connect to...: VPN Server

You must copy/paste the 3 key/cert. files in the corresponding local folder

Private KEY: # 1 sTnTQmUAgBETC1uyHqkxmbM...
 eWON CERTIFICATE: -----BEGIN CERTIFICATE-----
 MIIDFjOCCARgAwIBAgIBKDBANBgkqhkiG9w0BAQsF...
 CA (Certificate Authority) CERTIFICATE: -----BEGIN CERTIFICATE-----
 MIIDFTCCARgAwIBAgIBKDBANBgkqhkiG9w0BAQsF...
 BAYTAmJlMGoWCAVDVQVQIEwEtMRgwFg...
 DTAL

Internet connection setup

Internet access

- Network connection: Modem Connection
- Maintain connection:

Publish WAN IP address

- Publish IP address: Disabled
- Republish interval: 0 minutes

"On demand" Internet connection

- Accept dial on demand from **NO ONE EXCEPT** from:
- Accept dial on demand from **ANYONE EXCEPT** from:

IP Range	From: 0.0.0.0	To: 0.0.0.0
IP Range	From: 0.0.0.0	To: 0.0.0.0
IP Range	From: 0.0.0.0	To: 0.0.0.0
IP Range	From: 0.0.0.0	To: 0.0.0.0

VPN network setup

VPN use conditions

- During Internet connection:
 - Disable VPN
 - Listen for incoming VPN from client
 - Establish outgoing VPN to server

Routing setup

Special rules

- Route all gateway traffic through VPN: When VPN interface is active

NAT and TF (Transparent Forwarding)

- Apply NAT and TF to connection: NAT and TF disabled

These changes will be effective from next WAN connection

Networking security setup

WAN Protection

- WAN Protection level:
 - Discard all traffic excepted VPN and initiated traffic (ex: EMail)
 - Discard all traffic excepted VPN and initiated traffic (ex: EMail) and ICMP (Ping)
 - Allow all traffic on WAN connection (no protection)

Transparent Forwarding

- Require authentication for Transparent Forwarding:

These changes will be effective from next WAN connection

Revision history

Revision Level	Date	Description
1.0	2006	Initial version (formerly User Guide eWON - VPN).
1.1	19/12/13	Transfer into template and AUG structure + eGrabIt + new network diagrams + Superseded notice

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

Document build number: 32

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 ACTL Group.