ENDIAN Topologies
Setup of different Network topologies with Endian Firewalls
# Table of Contents

1. Hardware and software requirements.................................................................3
   Hardware requirements......................................................................................3
   Software requirements.......................................................................................3
   eWON Firmware Version..................................................................................3

2. Network Topologies .........................................................................................4
   Topology 1: Dedicated SA network.................................................................4
      ENDIAN Connectivity Setup.........................................................................4
      OpenVPN setup.............................................................................................7
      eWON setup..................................................................................................9
      Conclusions..................................................................................................10
   Topology 2a: SA in separate network.............................................................11
      ENDIAN connectivity setup.........................................................................11
      OpenVPN setup............................................................................................13
      eWON Setup................................................................................................13
      What ask to the Corporate IT......................................................................14
      Conclusions..................................................................................................15
   Topology 2b: SA in DMZ network.................................................................16
      ENDIAN connectivity setup.........................................................................16
      OpenVPN setup............................................................................................18
      eWON Setup................................................................................................18
      What ask to the Corporate IT......................................................................19
      Conclusions..................................................................................................20

Revisions.............................................................................................................21
Hardware and software requirements

Hardware requirements

In order to follow this guide you'll need:

- Minimum 1 eWON-VPN (several is better) with Internet connection for example: an eWON2005CD on your corporate LAN or an eWON2101-gprs with a SIMCard or an eWON2104 with an ADSL connection
- 2 Endian4ewon devices.
- One Broadband Internet connection without any port restrictions For example: an ADSL line with an ADSL modem

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 Explorer® or Firefox®.

Additionally we suggest you to download the eBuddy utility on our website: [http://support.ewon.biz](http://support.ewon.biz).

This utility allows you 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).

**Other programming software:**

ENDIAN Firewall is configurable through its web server. So, all you need is a standard Web Browser software like Internet Explorer® or Firefox®.

**eWON Firmware Version**

To be able to follow this guide your eWON needs a firmware version 5.6s2 or higher. A simple way to realize the eWON firmware upgrade is to use eBuddy, the eWON software companion.
Network Topologies

Topology 1: Dedicated SA network

SA stands for Supervisor Application.

This network topology is the simplest one, you have a dedicated Internet connection to your Supervisor Network.

Your Endian Device will do all the connectivity and security tasks to allow your remote eWONs to be connected to the LAN network.

**ENDIAN Connectivity Setup**

On this Endian, you need only to setup 2 interfaces, the GREEN and the RED. For that, simply use the Network Configuration wizard.

**NOTE**

With my ADSL Modem (D-LINK DSL-300T), if I use it as ADSL-Router, the internal D-Link firewall will block all ports excepts 80 and 21.

As the ENDIAN is firstly a Firewall and because I want to use OpenVPN (UDP1194), it’s required to setup the ADSL Modem in **Bridge mode** to disable the D-Link firewall.

Then, the PPPoE parameters will be setup in the ENDIAN.
2. Network Topologies

ENDIAN Topologies (Setup of different Network topologies with Endian Firewalls)
Now, the ENDIAN has the LAN IP address 192.168.120.16 and is connected to Internet by the ADSL Line.

To easily manage the “Supervisor Network”, configure the DHCP service with, for example, DHCP IP range from 120 to 254.

Then, our “Supervisor Network” is divided in two ranges:
- the lower IP addresses (till 119) reserved for fixed IP addresses
- the upper IP addresses (from 120) reserved for DHCP IP addresses.
With my ADSL line, the public IP address is dynamic, then, it is useful to setup a Dynamic DNS service to help eWONs to find the server.

On the Dynamic DNS page, click on the Add a host link and configure your dynamic DNS account (among dyndns.org, dyns.cx, easydns, no-ip, ...).

My Endian Firewall is now reachable at the address ewon.dynalias.net.

OpenVPN setup

To allow eWONs or computers to join the “Supervisor Network”, you need to configure the VPN of the ENDIAN.

Here above, we reserve the addresses from 192.168.120.20 to 40 for the pool of OpenVPN Clients (eWONs or computers).
We need to create one Account for each OpenVPN clients.

Here above, we defined 5 accounts, one for a User where we don't defined any remote nets behind this remote computer, and 4 accounts for eWON devices where we defined one remote network.

In the Advanced page, you can defined the Protocol/Port (UDP/1194) used by the OpenVPN and the authentication method (PSK username/password).

Now, the ENDIAN firewall is well configured to manage the LAN, connect to Internet and handle the OpenVPN Clients.
2. Network Topologies

**eWON setup**

To configure an eWON, fill the VPN→Outgoing Page with one account defined in the ENDIAN firewall and with the certificate of it.

You can also use the eWON wizard to setup these parameters.
Your Supervisor Network holds 2 computers, one at fixed IP address 192.168.120.10, another using DHCP to get the address 192.168.120.153.

These 2 computers have access to Internet through the ENDIAN.

The ewon45 is connected to Internet and is linked to the Supervisor Network by the address ewon.dynalias.net. Its VPN interface receives the address 192.168.120.21.

1. From the Supervisor Network, ewon45 is reachable at 192.168.120.21 exactly like if it was on the same network.

2. From the Supervisor Network, devices connected on the ewon45 LAN are directly reachable because the ENDIAN Firewall routes all 10.0.45.x requests to the ewon45 VPN client.

3. From the ewon45, the Supervisor Network is reachable.
2. Network Topologies

**Topology 2a: SA in separate network**

SA stands for Supervisor Application.

With this network topology, you will place the Supervisor Network in an existing IT infrastructure but not directly on the Corporate IT LAN. The purpose is exactly the same as in Topology 1: Dedicated SA network (link eWONs to the SA Network) but you must pass through a corporate network.

**ENDIAN connectivity setup**

On this “SA Router”, you need only to setup 2 interfaces, the GREEN and the RED, and both are Ethernet connections.

As the DMZ network is controlled by the Corporate IT, ask the IP address your SA Router (RED interface) to them.

With the Network Setup Wizard, you will have the following configuration screens:
2. Network Topologies

**ENDIAN Topologies**

Setup of different Network topologies with Endian Firewalls
Now, the ENDIAN has the LAN IP address 192.168.120.16 and is WAN side is connected to Internet by another Ethernet link (192.168.220.x).

To easily manage the "Supervisor Network", configure the DHCP service with, for example, DHCP IP range from 120 to 254.

**OpenVPN setup**

The OpenVPN setup is exactly the same as in Topology 1.

see OpenVPN setup on page 7

**eWON Setup**

To configure an eWON, fill the VPN→Outgoing Page with one account defined in the ENDIAN firewall and with the certificate of it.

The only difference with the eWON setup from Topology 1 is that you need to reach the Public IP address of the Corporate Network where your SA Network is placed.

You can also use the eWON wizard to setup these parameters.
2. Network Topologies

**What ask to the Corporate IT**

The minimum you need to ask to IT Guys is:

- to forward the incoming UDP/1194 traffic to the Endian Router

Then, eWONs and Users could establish a VPN connection with the **Supervisor Network** placed inside the Corporate network.

---

**IMPORTANT**

As this is the Corporate Router securing the **Corporate LAN**, there is no security problem with this topology. The IT staff manages alone the security of his network.

---

**NOTE**

By default, you will not be able to go on Internet from the **SA Network**. Thus, if you need to go on Internet, you must ask to the IT Staff to allow it.

---

Common setup of the Corporate Firewall is to allow Corporate LAN to go on the DMZ but to disable the DMZ to go on the Corporate LAN.

Pay attention that DMZ is only addresses 192.168.220.0/24 (distinct than SA Network addresses).

By default, as the DMZ link of the Corporate router enters in the WAN (aka Internet) of the **SA Router**, all incoming connections are blocked.

Then, from the IT LAN, **you must open a VPN connection** to gain access to the **SA Network**.

Then, the **SA Router** controls all the security of its **SA Network** (by creating one VPN account for each user) and the **Corporate Router** controls all the security of its **Corporate Network**.

If you don't want to open a VPN between IT LAN and SA LAN, one simple way is, on the **SA Router**, to add a Firewall rule to forward the incoming TCP80 on the **Supervisor Application Computer**.

<table>
<thead>
<tr>
<th>Proto</th>
<th>Source</th>
<th>Destination</th>
<th>Remark</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>192.168.220.10 : 80(HTTP)</td>
<td>192.168.120.10 : 80(HTTP)</td>
<td>ROUTE TO 10</td>
<td></td>
</tr>
</tbody>
</table>

Then, from the **IT LAN**, you can access to the **Supervisor website** at the address http://192.168.220.10 . That allows **ALL** Users from the **IT LAN** to access to the **Supervisor**.
Your SA Network holds only the main Server and is isolated behind the Corporate Firewall.

The ewon45 is connected to Internet and is linked to the SA Network by the address of the Corporate Network, generally a fixed IP address like http://www.mycompany.com using the port UDP 1194. Its VPN interface receives the address 192.168.120.21.

1. From the SA Network, ewon45 is reachable at 192.168.120.21 exactly like if it was on the same network.
2. From the SA Network, devices connected on the ewon45 LAN are directly reachable because the SA Router routes all 10.0.45.x requests to the ewon45 VPN client.
3. From the SA Network, the Corporate Network is unreachable.
4. From the ewon45, the SA Network is reachable.
5. From the Corporate Network, the SA Network may be reachable:
   - either by opening a VPN Client connection to the SA Network.
   - either by adding port forwarding in the SA Router.
   But Corporate Firewall could block all traffic from Corporate Net to SA Net.
2. Network Topologies

Topology 2b: SA in DMZ network

This topology is similar to the Topology 2a: SA in separate network but theEndian4ewon only play the role of VPN Server (no Firewall). The Supervisor Server is placed on the DMZ (and not behind the DMZ like in Topology 2a).

The Supervisor Network is behind an existing IT infrastructure but not directly on the Corporate IT LAN.

The purpose is always the same as in other topologies (link eWONs from Internet to the SA Network).

ENDIAN connectivity setup

On this Endian4ewon configured as “VPN Server”, you need only one interface because you don't need to physically separate 2 networks.

In the Endian4ewon, you will need to “disable” the RED, in fact configure it on Gateway.

As you place your Supervisor Server and the VPN Server on a network fully controlled by the Corporate IT, you must ask which addresses you can use.

With the Network Setup Wizard, you will have the following configuration screens:
2. Network Topologies

ENDIAN Topologies (Setup of different Network topologies with Endian Firewalls)
Now, the Endian4ewon has the LAN IP address 192.168.120.16 (on two interfaces, see Step 3 of the wizard) and is connected to Internet by a Gateway (the Corporate Router).

As the Endian4ewon (VPN Server) is placed in the DMZ of the Corporate Network, disable the DHCP Service on your Endian4ewon.

**OpenVPN setup**

The OpenVPN setup is exactly the same as previous Topologies. see OpenVPN setup on page 7

**eWON Setup**

To configure an eWON, fill the VPN→Outgoing Page with one account defined in the ENDIAN firewall and with the certificate of it.

Encode the Public IP address of the Corporate Network where your SA Network is placed.

You can also use the eWON wizard to setup these parameters.
2. Network Topologies

What ask to the Corporate IT

In addition of the IP addresses, you must ask to the IT guys:

- to forward the incoming UDP/1194 traffic to the Endian Router

Then, eWONs and Users from Internet could establish a VPN connection with the Supervisor Network.

IMPORTANT

As this is the Corporate Router securing the Corporate LAN, there is no security problem with this topology. The IT staff manages alone all the security of his network.

NOTE

By default, you will not be able to go on Internet from the SA Network. Thus, if you need to go on Internet, you must ask to the IT Staff to allow it.

Common setup of the Corporate Firewall is to allow Corporate LAN to go on the DMZ but to disable the DMZ to go on the Corporate LAN.

In contrast to the Topology 2a: SA in separate network, the Endian4ewon doesn't act as Firewall, then Users from the Corporate LAN have a direct access to all devices on the DMZ Network.
2. Network Topologies

Conclusions

Your SA Network holds only the main Server and is the DMZ behind the Corporate Firewall.

The ewon45 is connected to Internet and is linked to the SA Network by the address of the Corporate Network, generally a fixed IP address like http://www.mycompany.com using the port UDP 1194. Its VPN interface receives the address 192.168.120.21.

1. From the SA Network, ewon45 is reachable at 192.168.120.21 exactly like if it was on the same network.

2. From the SA Network, devices connected on the ewon45 LAN are directly reachable because the SA Router routes all 10.0.45.x requests to the ewon45 VPN client.

3. From the SA Network, the Corporate Network is unreachable.

4. From the ewon45, the SA Network is reachable.

5. From the Corporate Network, the SA Network is reachable
But Corporate Firewall could block all traffic from Corporate Net to SA Net

**IMPORTANT**
The Supervisor Server must have the VPN Server as Gateway to allow communications with VPN Clients!
Other computers placed on the DMZ may have the Corporate Firewall as Gateway (normal configuration).
<table>
<thead>
<tr>
<th>Revision Level</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>23/04/08</td>
<td>First release.</td>
</tr>
</tbody>
</table>

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.

Microsoft, Internet Explorer, Windows and Windows XP are either registered trademarks or trademarks of Microsoft Corporation.

Firefox is a trademark of the Mozilla Foundation.