

KB Name	Server on Endian-DMZ		
Type	Config Example		
Since revision	NA		
KB Number	KB-0032-0)	Build	6
Mod date	9. Sep. 2009		

Knowledge Base Information

Server on Endian-DMZ

1 Purpose

By design, Endian-for-eWON “bridges” the LAN corporate network and all VPN Clients. For usual Road Warriors usage, this bridge is not a problem, but for eWON permanently connected by GPRS to the Endian-for-eWON, this bridge implies that all broadcast messages travelling on the LAN corporate network will be sent also on each VPN Client through GPRS connections. As you pay for any GPRS traffic, these broadcast messages could cost a lot of money (one broadcast message will generate several GPRS communications).

VPN Clients on GPRS-EDGE connection don't want to be "bridged" with the LAN corporate network. Then, placing the Application Server on the ENDIAN-DMZ blocks all broadcast messages from the LAN.

2 Application Server placed on Endian-for-eWON DMZ

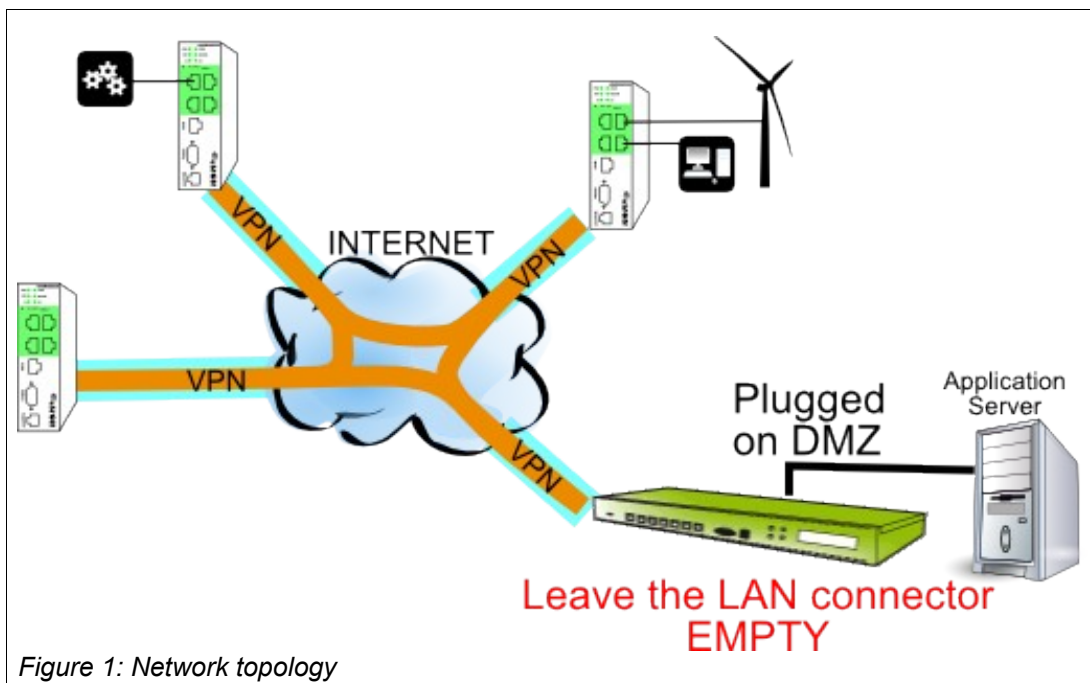


Figure 1: Network topology

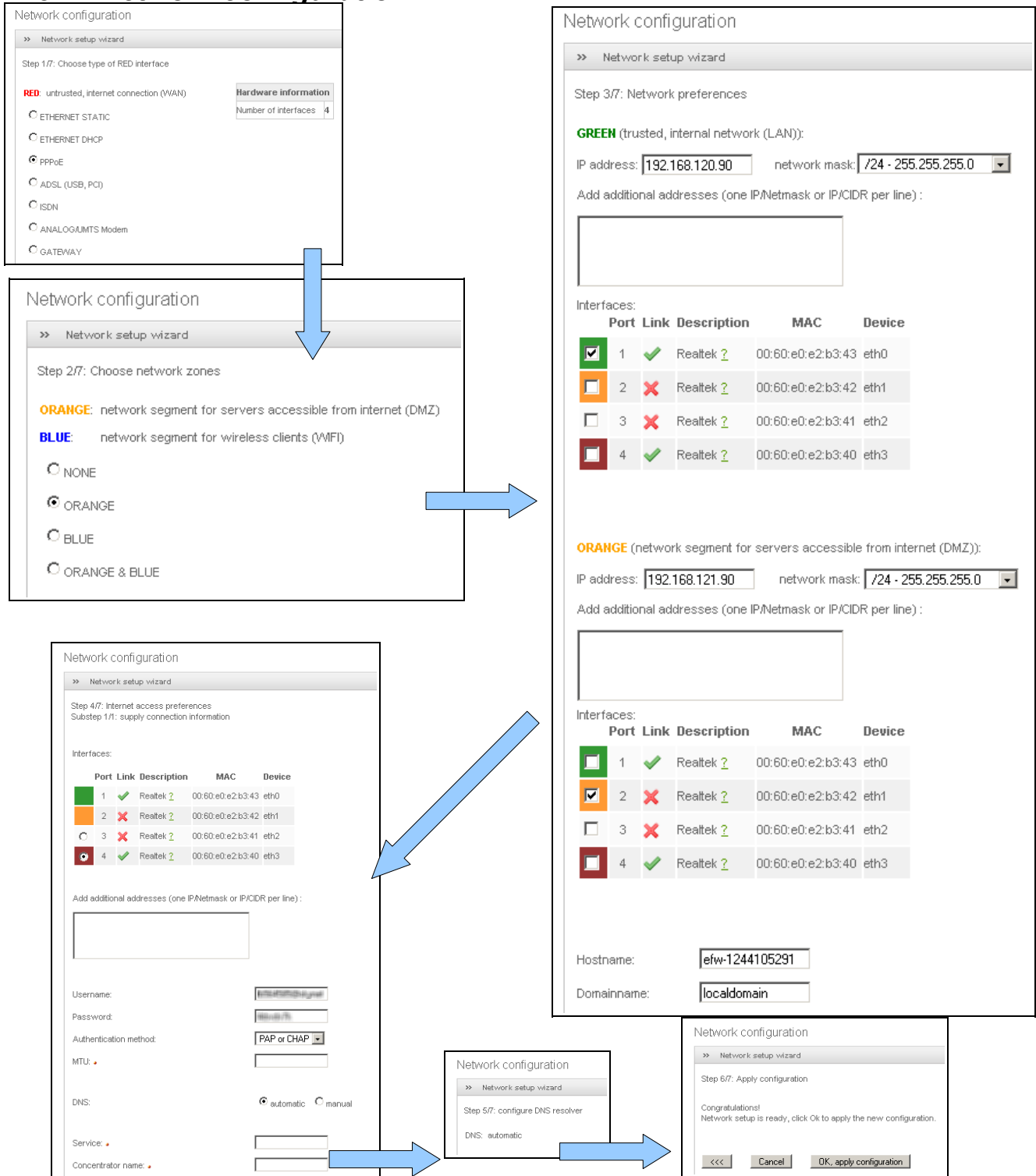
In this topology, the Application Server is connected on DMZ interface of the Endian-for-eWON and there is nothing plugged in the LAN interface.

KB Name	Server on Endian-DMZ		
Type	Config Example		
Since revision	NA		
KB Number	KB-0032-0)	Build	6
Mod date	9. Sep. 2009		

Knowledge Base Information

3 Endian-for-eWON configuration

3.1 Network configuration



KB Name	Server on Endian-DMZ		
Type	Config Example		
Since revision	NA		
KB Number	KB-0032-0)	Build	6
Mod date	9. Sep. 2009		

Knowledge Base Information

3.2 VPN configuration

OpenVPN - Virtual Private Networking

>> **Server configuration** Accounts Advanced VPN client download

>> Global settings

OpenVPN server enabled:

Dynamic IP pool start address:

Dynamic IP pool end address:

[Download CA certificate](#)

OpenVPN - Virtual Private Networking

>> Server configuration **Accounts** Advanced VPN client download

>> Change account ewonprk

Account information

Username:

Password:

Verify password:

Client routing

Direct all client traffic through the VPN server:

Don't push any routes to client:

Push route to orange zone:

[Networks behind client:](#)

[Push only these networks:](#)

If this box is empty routes to each of the networks of the other clients will be pushed to this client whenever it connects

Custom push configuration

[Static ip addresses:](#)

In each *Accounts*, check the “Push route to orange zone” to allow eWON and devices behind to reach the Application Server.

Also, defines the “Network behind client”.

OpenVPN - Virtual Private Networking

>> Server configuration Accounts **Advanced** VPN client download

>> Advanced settings

Port: Block DHCP responses coming from tunnel:

Protocol: Don't block traffic between clients:

Note: You may allow multiple ports by port forward them

>> Global push options

Push these networks: Enable

Push these nameservers: Enable

Push domain: Enable

KB Name	Server on Endian-DMZ		
Type	Config Example		
Since revision	NA		
KB Number	KB-0032-0)	Build	6
Mod date	9. Sep. 2009		

Knowledge Base Information

3.3 Firewall configuration

The screenshot shows the Endian Firewall configuration interface for eWON25. The 'Firewall' tab is selected, and the 'Inter-Zone firewall configuration' page is displayed. A table of current rules is shown, with rule 6 highlighted by a red oval. The table has columns for #, Source, Destination, Service, Policy, Remark, and Actions.

#	Source	Destination	Service	Policy	Remark	Actions
1	GREEN	GREEN	<ANY>	→		↓ ✓ ✎ 🗑
2	GREEN	BLUE	<ANY>	→		↑ ↓ ✓ ✎ 🗑
3	GREEN	ORANGE	<ANY>	→		↑ ↓ ✓ ✎ 🗑
4	BLUE	BLUE	<ANY>	→		↑ ↓ ✓ ✎ 🗑
5	ORANGE	ORANGE	<ANY>	→		↑ ↓ ✓ ✎ 🗑
6	ORANGE	GREEN	<ANY>	→		↑ ✓ ✎ 🗑

Legend: Enabled (click to disable) Disabled (click to enable) ✎ Edit 🗑 Remove

Show rules of system services >>

Inter-Zone Firewall Settings

Enable Inter-Zone firewall

Log accepted Inter-Zone connections

Save

To allow the DMZ (orange) zone to get access to the VPN, you need to add a rule to allow “Orange to Green traffic”.

The screenshot shows the Endian Firewall configuration interface for eWON25. The 'Firewall' tab is selected, and the 'VPN firewall configuration' page is displayed. The 'VPN Firewall Settings' section is shown, with the 'Enable VPN firewall' checkbox circled in red.

VPN Firewall Settings

Enable VPN firewall

Use the switch above to enable the VPN firewall. The VPN firewall gives the ability to globally DENY VPN traffic and explicitly configure VPN firewall rules.

Don't use the “VPN firewall”.

Knowledge Base Information

KB Name	Server on Endian-DMZ		
Type	Config Example		
Since revision	NA		
KB Number	KB-0032-0)	Build	6
Mod date	9. Sep. 2009		

4 Application Server configuration

You need to tell to the Application Server where the LAN network is.

Either use the Endian-for-eWON as default Gateway or add a route to the Endian-LAN.