SSV Web ConfigTool

for Remote Access Gateways

User Manual

SSV Software Systems GmbH
Dünenweg 5
D-30419 Hannover
Phone: +49 (0)511/40 000-0
Fax: +49 (0)511/40 000-40
E-mail: sales@ssv-embedded.de

Document Revision: 1.0
Date: 2013-04-30

CONTENT

1 INTRODUCTION 4

1.1 Conventions 4

1.2 GUI Layout & Elements 4

1.3 Important Information 5

2 MENU ITEMS 7

2.1 Status 7

2.2 System 8

2.2.1. System Identification 8

2.2.2. System Management 8

2.2.2.1. System Management 8

2.2.2.2. System Configuration 8

2.2.3. Time and Date 9

2.2.3.1. Local Time zone Configuration 9

2.2.3.2. Time and Date Configuration 9

2.2.4. Com Ports 10

2.2.4.1. COM1 Properties 10

2.2.5. Remote Access 11

2.2.5.1. OpenSSH configuration 11

2.2.5.2. Change password for user "root" 11

2.2.6. Administration 12

2.2.6.1. Change web configuration password 12

2.2.6.2. Change web configuration master password 12

2.2.6.3. Session timeout 12

2.2.7. Logging 13

2.3 Network 14

2.3.1. LAN 14

2.3.1.1. Network configuration for LAN1 14

2.3.1.2. Network configuration for LAN2 14

2.3.1.3. DNS configuration 15

2.3.1.4. Default gateway configuration 15

2.3.2. Modem 16

2.3.2.1. Modem configuration 16

2.3.2.2. ISP settings 16

2.3.2.3. Connection settings 17

2.3.2.4. DNS server and gateway configuration 17

2.4 Services 18

2.4.1. General 18

2.4.1.1. General service configuration 18

2.4.2. OpenVPN 18

2.4.2.1. OpenVPN configuration 18

2.4.2.2. OpenVPN client configuration 18

2.4.2.3. OpenVPN server configuration 19

2.4.2.4. OpenVPN certificates and keys 19

2.4.2.5. OpenVPN create certificates 20

2.4.2.6. OpenVPN export certificates 20

2.4.3. IPsec 21
2.4.3.1. IPsec configuration 21
2.4.3.2. Connection protocol 21
2.4.3.3. IPsec shared keys 21
2.4.3.4. IPsec certificates and keys 22
2.4.3.5. Configuration of this side (right) 22
2.4.3.6. Configuration of other side (left) 22
2.4.4. DynDNS 23
2.4.4.1. DynDNS configuration 23
2.4.4.2. Change DynDNS username and password 23
2.4.4.3. Notification to webserver after ipaddress changes 23
2.4.5. DHCP Server 24
2.4.5.1. General configuration 24
2.4.5.2. Address range 24
2.4.6. Firewall and NAT 25
2.4.6.1. Firewall configuration 25
2.4.6.2. Firewall and NAT rules preconfigured sets 25
2.4.6.3. System specific ports allowed on WAN interface 25
2.4.6.4. User specific ports allowed on WAN interface 26
2.4.6.5. ICMP protocols 26
2.4.6.6. Forwarding with IP-Masquerading and NAT 26
2.4.6.7. Firewall and NAT rules script 26
2.5 Proxies 27
2.5.1. Web 27
2.5.1.1. General configuration 27
2.5.1.2. Proxy redirections 27
2.5.1.3. Create/Edit a redirection entry 27
2.5.1.4. SSL certificate 27
2.5.2. DNS 28
2.5.2.1. General configuration 28
2.5.3. Filetransfer 29
2.5.3.1. General configuration 29
2.5.3.2. Proxy redirections 29
2.5.3.3. Create/Edit a redirection entry 29
2.5.4. Telnet/SSH/others 30
2.5.4.1. General configuration 30
2.5.4.2. Proxy redirections 30
2.5.4.3. Create/Edit a redirection entry 30
2.6 Logout 31
3 HELPFUL LITERATURE 32
CONTACT 32
DOCUMENT HISTORY 32

1 INTRODUCTION

This document describes the Web ConfigTool for the Remote Access Gateways IGW/92x with the DIL/NetPC (A)DNP/9200. With its intuitively operable GUI (Graphical User Interface) all important system settings can be configured.

1.1 Conventions

The following conventions are used in this document:

Convention	Usage
[Button]	Name of a button like **[Apply]** or **[Info]**
<Item>	Name of a dropdown menu item like **<Analog>**
`monospace`	Passwords or IP addresses like `root` or `192.168.0.1`

Table 1: Conventions used in this document

1.2 GUI Layout & Elements

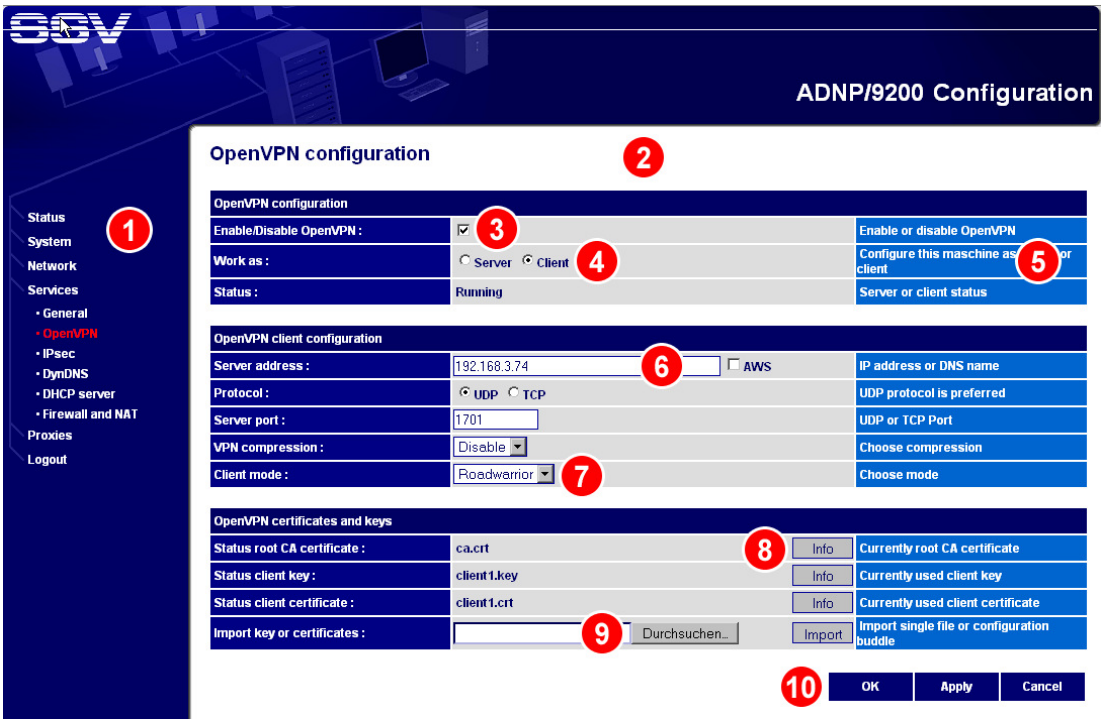

Figure 1: GUI layout of the SSV Web ConfigTool

1: Menu
2: Main content
3: Checkbox
4: Radio button
5: Short description
6: Text field
7: Dropdown menu
8: Button
9: Import/upload button
10: Main buttons

1.3 Important Information

To open the login page of the SSV ConfigTool in a Web browser enter this URL: **`http://192.168.0.126:7777`**. The following passwords can be used to login:

- The default Web ConfigTool password is "**`adnp`**". This is the standard user and has an idle timeout. The password and the timeout can be changed in the menu over "System > Administration".
- The default Web ConfigTool master password is "**`ssvadmin`**". This is the master user and has no idle timeout. The password can be changed in the menu over "System > Administration".

Please note: If a standard user is already logged in, he will be automatically logged out when the master user logs in. In contrast to the standard user it is possible to log in more then once at the same time with the master password. **Although it is possible it is not recommended!**

- The default root password for Telnet, SSH and FTP access is "`root`". This password does not work with the Web ConfigTool. The root password can be changed in the menu over "System > Remote access".

The three main buttons are on every page always in the lower right corner of the main content. They have the following functions:

- **[OK]:** Saves changed settings, but the system needs to be rebooted.
- **[Apply]:** Saves changed settings and applies them immediately. The changes can not be canceled afterwards! A reboot is not necessary.
- **[Cancel]:** Restores old settings, but only if the changes were not already saved!

Figure 2: Main buttons of the SSV Web ConfigTool

Please note: Some settings are only visible if the appending function is enabled. The figures 3 and 4 illustrate this behaviour:

The OpenVPN service is disabled, so no settings are shown.

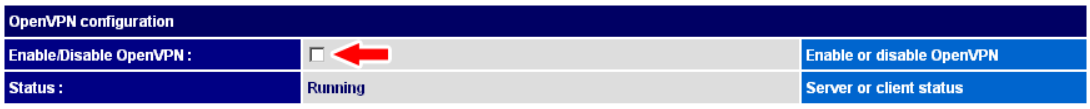

Figure 3: OpenVPN service is disabled

After enabling the OpenVPN service with the checkbox the settings appear. If you switch between server and client mode with the radio buttons the offered settings will change.

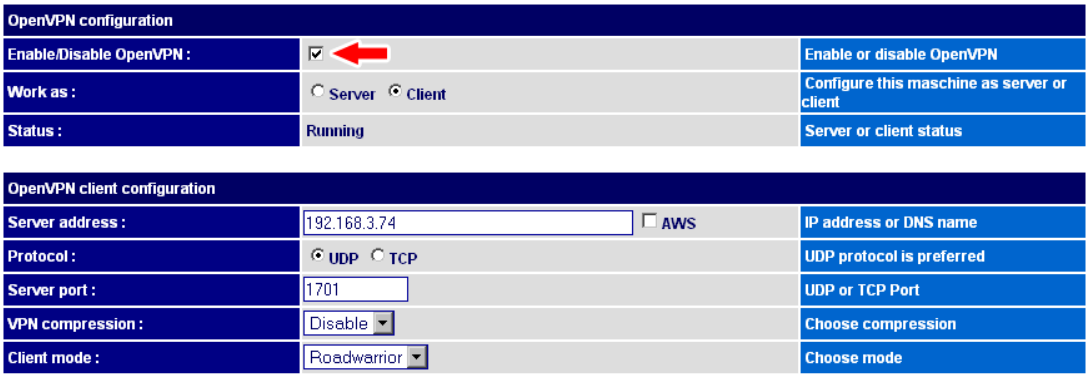

Figure 4: OpenVPN client configuration

2 MENU ITEMS

The following chapters describe the particular menu items and their functions.

2.1 Status

The Status page shows some information about the device like name, time or IP addresses.

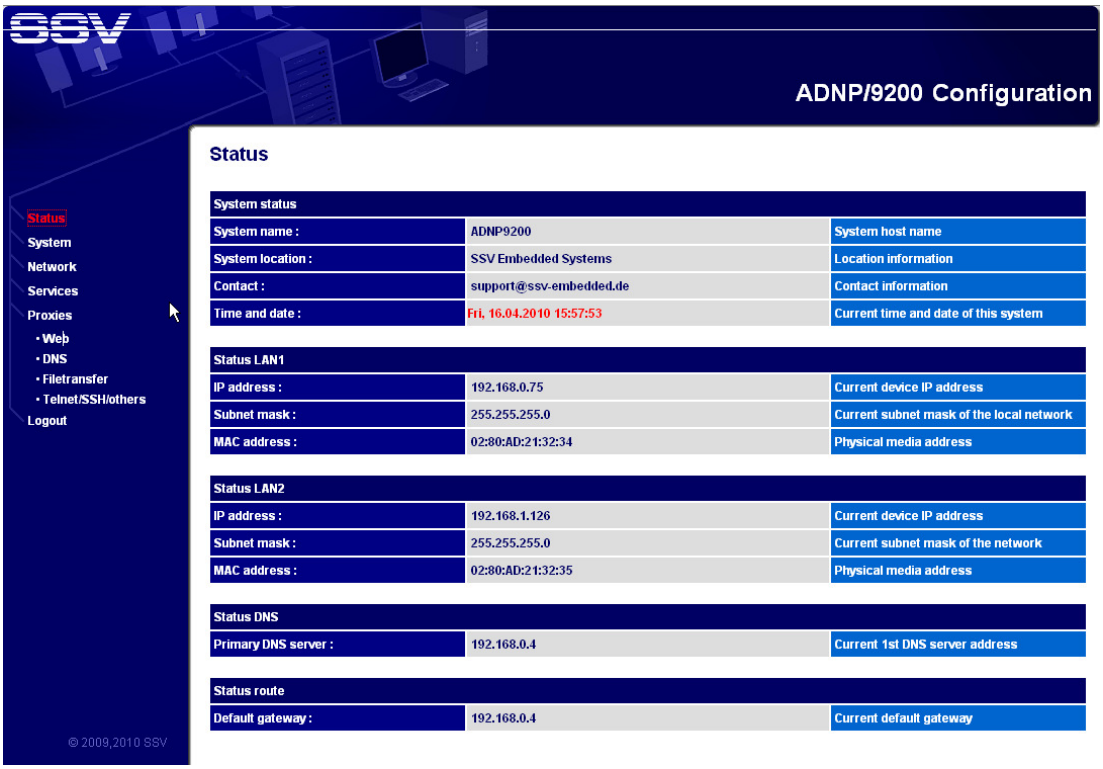

Figure 5: Status page of the SSV Web ConfigTool

2.2 System

In this section you can configure the basic settings of the device like host name, time and administration.

2.2.1. System Identification

Enter a host name and the location of the device and some contact information. The settings in this section are used for certificates.

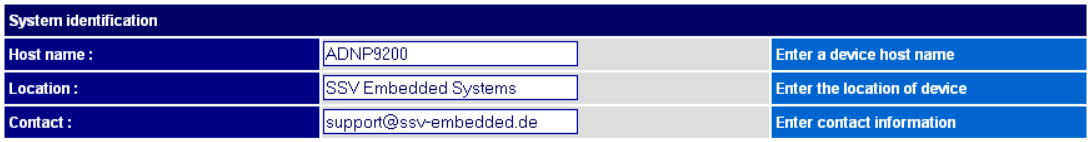

Figure 6: System identification settings

2.2.2. System Management

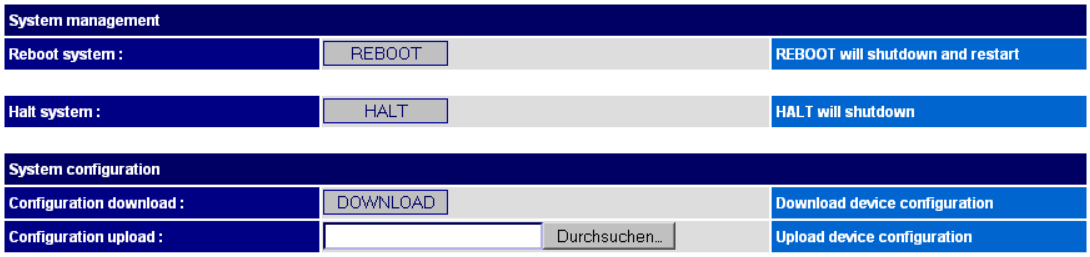

Figure 7: System management settings

2.2.2.1. System Management

- **Reboot System:** Click on [REBOOT] to shutdown and restart the system.

Please note: You will see the message “Rebooting the system”. The reboot process takes about one minute. After that time open the login page and enter your password.

- **Halt System:** Click on [HALT] to shutdown the system.

Please note: If the device is shutdown, there is no possibility to boot the system from the distance!

2.2.2.2. System Configuration

- **Configuration download:** Click on [DOWNLOAD] to save the system configuration.
- **Configuration upload:** Click on the button to upload a system configuration. Click on [OK] to save the configuration. To use the new configuration the system must be rebooted.

Please note: You should download and save the system configuration before changing any settings! So the system can be restored if there was a problem.

2.2.3. Time and Date

In this section you can set the system time and date manually or automatically via NTP.

2.2.3.1. Local Time zone Configuration

- **Time zone:** Choose your time zone from the dropdown menu.

2.2.3.2. Time and Date Configuration

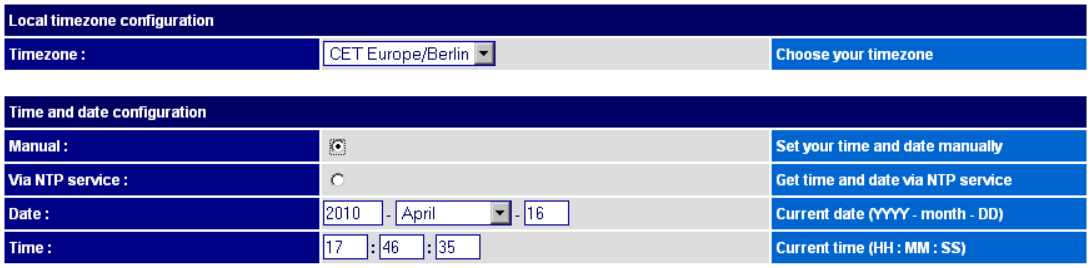

Figure 8: Manual time settings

- **Manual:** Click on this radio button to set your time and date manually.
- **Date:** Enter the current date (YYYY - <month> - DD).
- **Time:** Enter the current time (HH : MM : SS).

Figure 9: Time settings via NTP service

- **Via NTP service:** Click on this radio button to get time and date via an NTP service.
- **Primary NTP server:** Enter the address of an NTP server. You can leave this field empty and only use the secondary NTP server.
- **Secondary NTP server:** Choose an NTP server from the dropdown menu.
- **Time synchronize interval:** Choose the time synchronization interval.
- **NTP server test:** Click on [Synchronize now] to test the connection with the NTP server. If the test is successful, you should see the following message in the short description: “Time synchronization successful”.

Please note: Before enabling the NTP service it is recommended to set the network gateway and DNS correctly.

2.2.4. Com Ports

In this section you can configure with which application each of the three COM ports is used. The settings for each port are the same, so only the settings for COM1 are described.

COM1 is typically configured as <Remote console>. To use COM1 for other applications, you should remove the RCM jumper from the device (please refer to the hardware reference of the device).
If the device offers a GPRS/UMTS modem, it is connected to COM3. COM3 must then be set to <Modem>.

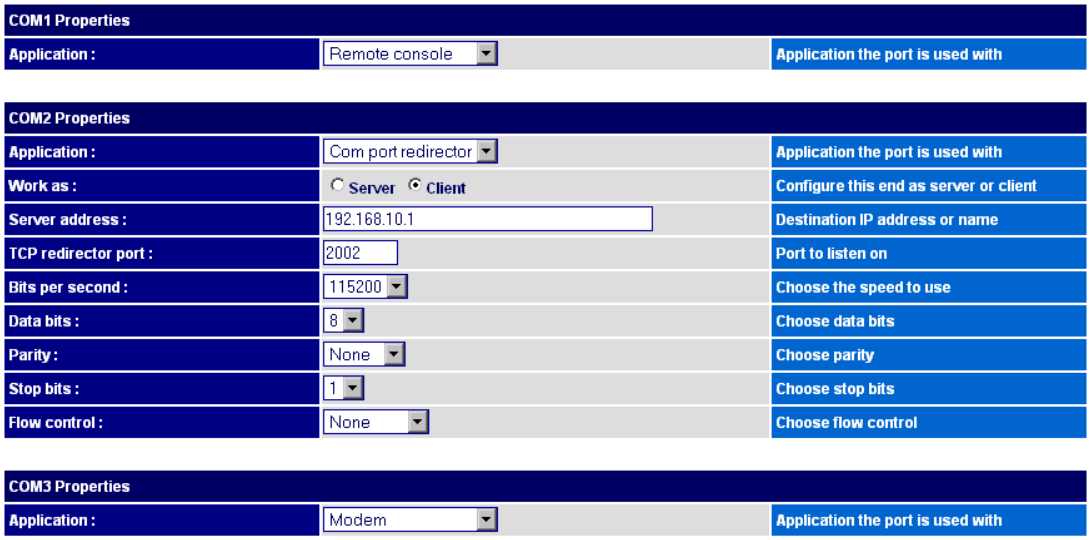

Figure 10: COM port settings

2.2.4.1. COM1 Properties

- **Application:** Application the port is used with.
- **Work as:** Configure this end as server or client.
- **Server address:** Destination IP address or name.
- **TCP redirector port:** Port to listen on.
- **Bits per second:** Choose the speed to use.
- **Data bits:** Choose the data bits.
- **Parity:** Choose the parity.
- **Stop bits:** Choose the stop bits.
- **Flow control:** Choose the flow control.

2.2.5. Remote Access

In this section you can configure the settings for the SSH server.

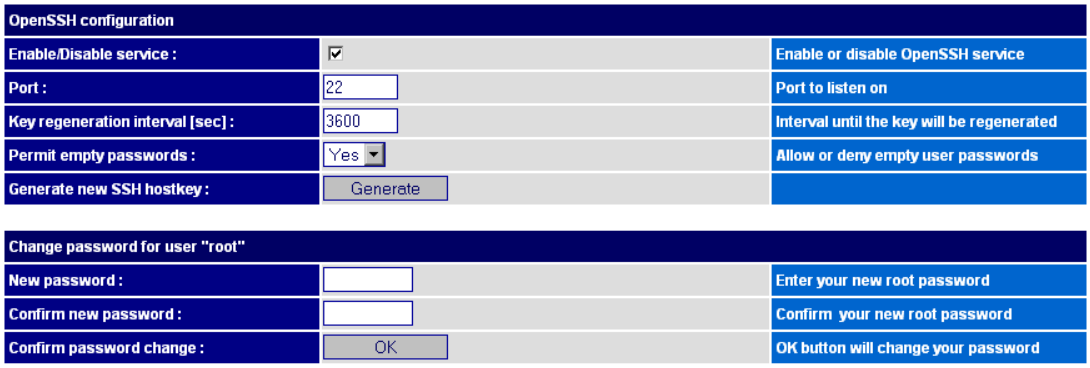

Figure 11: Remote access settings

2.2.5.1. OpenSSH configuration

- **Enable/Disable service:** Enable or disable the OpenSSH service.
- **Port:** Enter the port to listen on.
- **Key regeneration interval [sec]:** Enter the time interval in seconds for the key re-generation.
- **Permit empty passwords:** Allow or deny empty user passwords.
- **Generate new SSH host key:** Click on [Generate] to create a new SSH host key.

Please note: The key generation can take up to five minutes! Do not interrupt the process and wait until you see this message: “Key generation successful”!

2.2.5.2. Change password for user "root"

- **New password:** Enter your new root password.
- **Confirm new password:** Confirm your new root password.
- **Confirm password change:** Click on [OK] to save your new password.

Please note: The default password for root is “root”. It is highly recommended to change the password before using the device in unsafe environments like the Internet!

2.2.6. Administration

In this section you can set the login passwords for the Web ConfigTool and the idle time for a session.

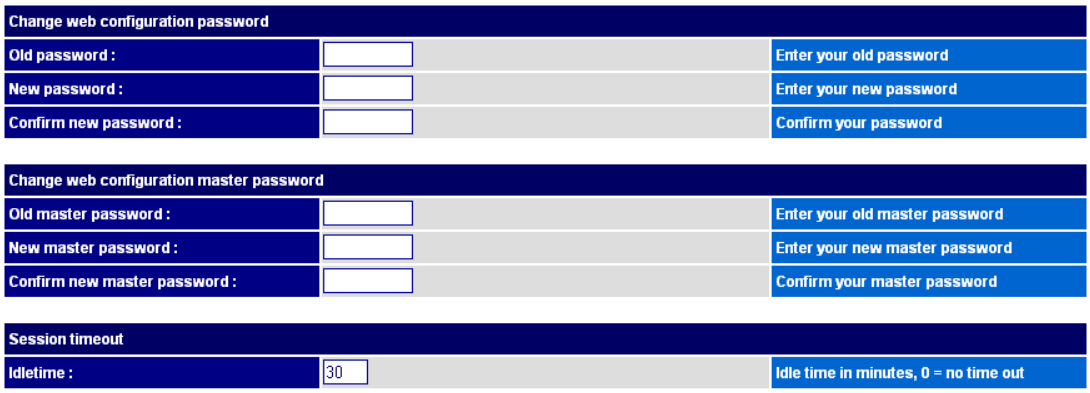

Figure 12: Administration settings

2.2.6.1. Change web configuration password

- **Old password:** Enter your old password.
- **New password:** Enter your new password.
- **Confirm new password:** Confirm your new password.

2.2.6.2. Change web configuration master password

- **Old master password:** Enter your old master password.
- **New master password:** Enter your new master password.
- **Confirm new master password:** Confirm your new master password.

Please note: The master password does not depend on a session timeout and can be used to revoke logins with the standard password.

2.2.6.3. Session timeout

- **Idle time:** Idle time in minutes, 0 = no time out.

2.2.7. Logging

In this section you can view and download the system log file. Click on [Download] to save the log as a file.

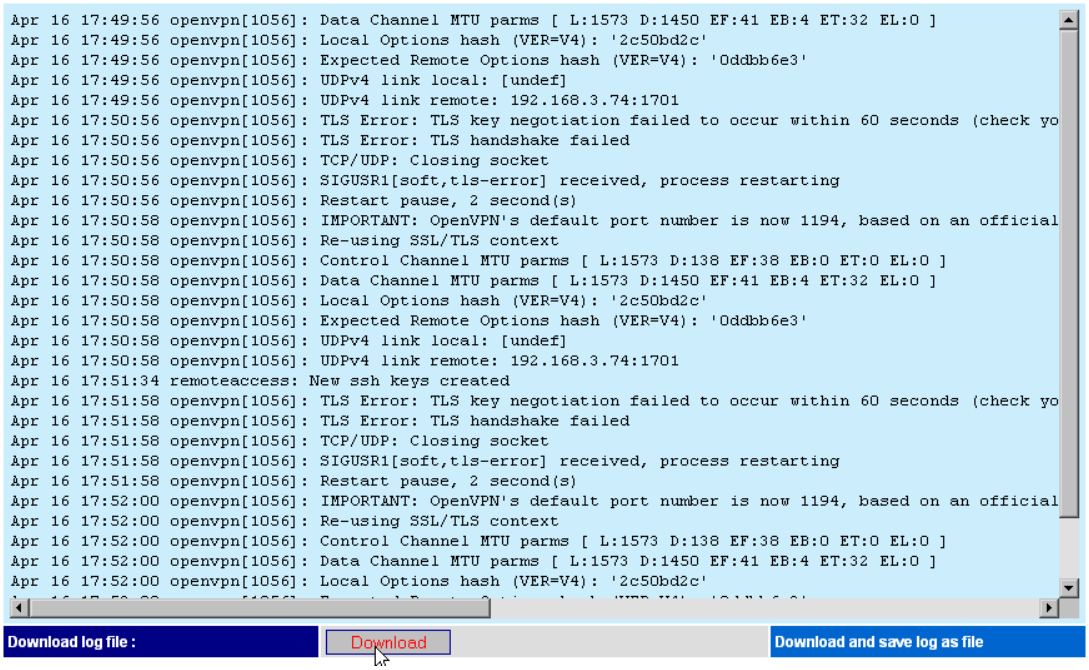

Figure 13: Log file view

2.3 Network

In this section you can configure the LAN and modem settings.

2.3.1. LAN

In this section you can configure the settings for LAN1 and LAN2.

2.3.1.1. Network configuration for LAN1

Network configuration for LAN1 (10/100 MBit)		
Enable/Disable interface LAN1 :	☑	Enable or disable interface LAN1
Obtain an IP address automatically :	○	Device configuration through DHCP server
Use the following IP address :	◉	Manual device configuration
IP address :	192 . 168 . 0 . 75	Device IP address
Subnet mask :	255 . 255 . 255 . 0	Subnet mask of the local network
Enable/Disable alias IP address :	☐	Enable or disable alias IP address

Figure 14: LAN1 settings

- **Enable/Disable interface LAN1:** Enable or disable interface LAN1.
- **Obtain an IP address automatically:** Device configuration through DHCP server.
- **Use the following IP address:** Manual device configuration.
- **IP address:** IP address of the device.
- **Subnet mask:** Subnet mask of the local network.
- **Enable/Disable alias IP address:** Enable or disable the alias IP address.
- **Alias IP address:** Secondary static IP address for the same interface.
- **Alias subnet mask:** Subnet mask of the alias network.

2.3.1.2. Network configuration for LAN2

Network configuration for LAN2 (10/100 Mbps)		
Enable/Disable interface LAN2 :	☑	Enable or disable interface LAN2
Use device for DSL :	○	Device used to connect to a DSL modem
Obtain an IP address automatically :	○	Device configuration through DHCP server
Use the following IP address :	◉	Manual device configuration
IP address :	192 . 168 . 1 . 126	Device IP address
Subnet mask :	255 . 255 . 255 . 0	Subnet mask of the local network

Figure 15: LAN2 settings

- **Enable/Disable interface LAN2:** Enable or disable interface LAN2.
- **Use device for DSL:** Device is used to connect with a DSL modem.
- **Obtain an IP address automatically:** Device configuration through DHCP server.
- **Use the following IP address:** Manual device configuration.
- **IP address:** IP address of the device.
- **Subnet mask:** Subnet mask of the local network.

2.3.1.3. DNS configuration

In this section you can configure the DNS server settings. These settings are only necessary, if the system is configured as a router on LAN1.

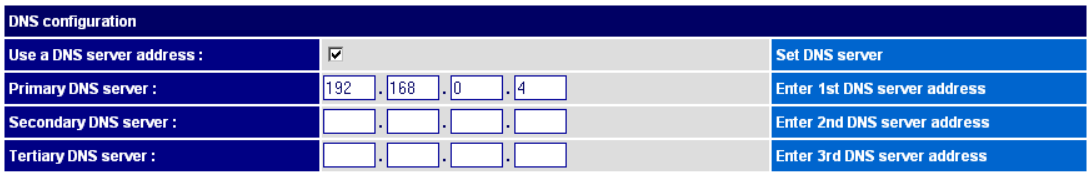

Figure 16: DNS configuration

- **Use a DNS server address:** Enable the DNS server.
- **Primary DNS server:** Enter the first DNS server IP address.
- **Secondary DNS server:** Enter the second DNS server IP address.
- **Tertiary DNS server:** Enter the third DNS server IP address.

2.3.1.4. Default gateway configuration

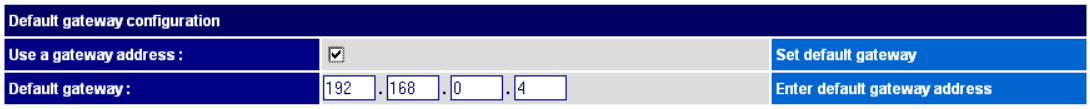

Figure 17: Default gateway configuration

- **Use a gateway address:** Enable the default gateway.
- **Default gateway:** Enter the default gateway IP address.

2.3.2. Modem

In this section you can configure the modem settings.

Please note: This section is only usable, if a modem is configured in COM ports or network (on LAN2)!

2.3.2.1. Modem configuration

- **Modem type:** The dropdown menu offers six different operation modes: <None>, <Analog>, <ISDN>, <GPRS>, <UMTS> and <DSL>.
- **Check modem:** Click on [Check modem] to test the connection with an existing modem. In case of a GPRS/UMTS modem the SIM card and the Quality of Service (QoS) are also tested.

2.3.2.2. ISP settings

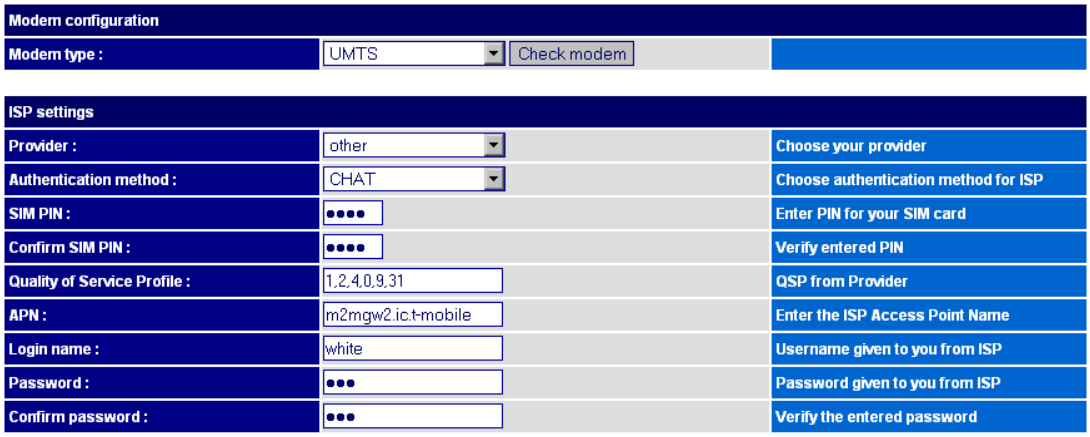

Figure 18: ISP settings for UMTS modem

Please note: The ISP settings depend on the choice of the modem type!

- **Provider:** Choose your Internet Service Provider (ISP).
- **Authentication method:** Choose an authentication method for the ISP.
- **MSN number:** Enter your ISDN MSN phone number.
- **Dialing phone number:** Enter the phone number to the ISP.
- **SIM PIN:** Enter the PIN for your SIM card.
- **Confirm SIM PIN:** Verify the entered SIM PIN.
- **Quality of Service Profile:** QSP from the ISP.
- **APN:** Enter the ISP Access Point Name.
- **Login name:** Enter the username given to you from the ISP.
- **Password:** Enter the password given to you from the ISP.
- **Confirm password:** Verify the entered password.

2.3.2.3. Connection settings

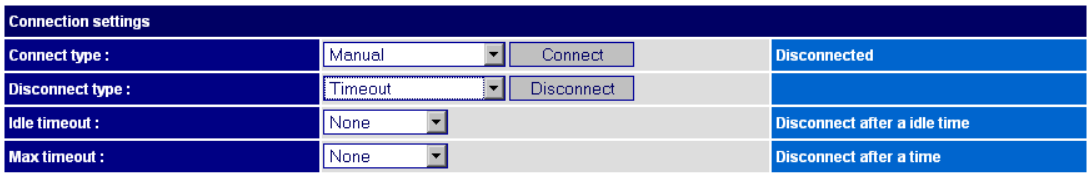

Figure 19: Connection settings

- **Connect type:** The dropdown menu offers following connection types: <Manual>, <System start> and <on demand>.
- **Disconnect type:** The dropdown menu offers following disconnection types: <Manual>, <Timeout> and <Always reconnect>.
- **Idle timeout:** Disconnect the system after a certain idle time.
- **Max timeout:** Disconnects the system after a certain time.

Please note: Connections over a GPRS/UMTS modem can be very cost intensive. Please refer to the prices of your provider, before connecting the modem for a long time or with high volume traffic.

2.3.2.4. DNS server and gateway configuration

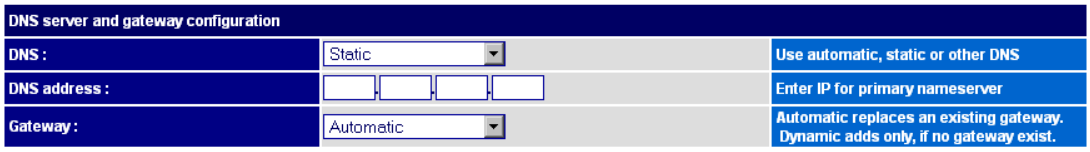

Figure 20: DNS configuration

- **DNS:** The dropdown menu offers following settings: <Automatic>, <Static> and <None>.
- **DNS address:** Enter the IP address for the primary name server.
- **Gateway:** <Automatic> replaces an existing gateway. <Dynamic> adds a new gateway only, if no other gateway exists.

2.4 Services

In this section you can configure services like OpenVPN, IPsec and DynDNS.

2.4.1. General

In this section you can enable or disable the general services.

2.4.1.1. General service configuration

- **Telnet server:** Enable or disable the Telnet server.
- **FTP server:** Enable or disable the FTP server.
- **Time server:** Enable or disable the time server.
- **HTTPS Web server:** Enable or disable the HTTPS web server.
- **Webconfig:** Enable or disable Web ConfigTool.
- **SSV ConfigTool:** Enable or disable the external SSV ConfigTool. This tool is only available on demand. Please contact therefore our support team.

2.4.2. OpenVPN

In this section you can configure the OpenVPN settings.

2.4.2.1. OpenVPN configuration

- **Enable/Disable OpenVPN:** Enable or disable OpenVPN.
- **Work as:** Configure the device as server or client.
- **Status:** Server or client status.

2.4.2.2. OpenVPN client configuration

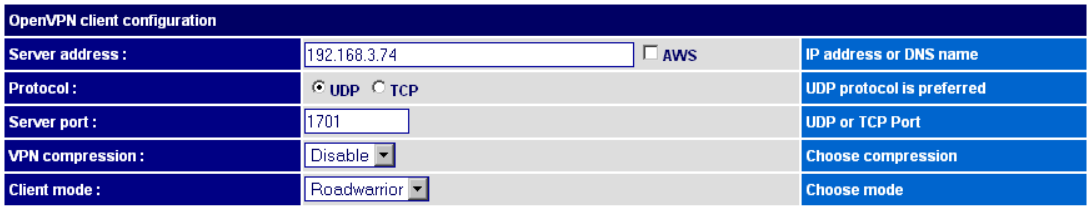

Figure 21: OpenVPN client configuration

- **Server address:** Enter the IP address or DNS name of the OpenVPN server. If you use a cloud service, you can activate the checkbox “AWS” and enter the bucket name in the text field instead of an IP address.
- **Protocol:** Choose the protocol. The UDP protocol is preferred.
- **Server port:** Enter the UDP or TCP port.
- **VPN compression:** Enable or disable the VPN compression.
- **Client mode:** Choose the client mode: <Roadwarrior> or <Bridging>.
- **OpenVPN bridge IP:** Establish a connection to the Web ConfigTool. It is recommended to use the same IP address like LAN1!

2.4.2.3. OpenVPN server configuration

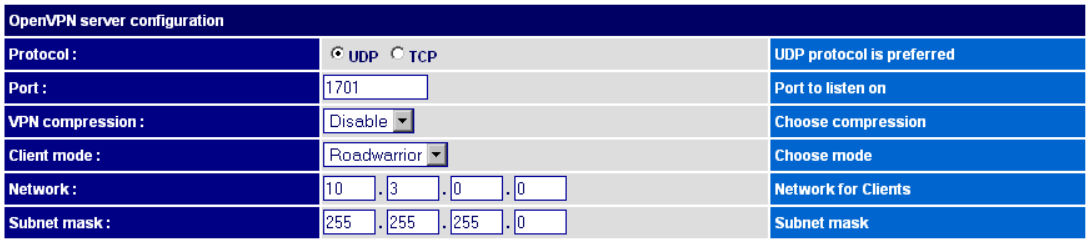

Figure 22: OpenVPN server configuration

- **Protocol:** The UDP protocol is preferred. TCP must be used if the server works behind a NAT router, e.g. a DSL modem with port forwarding.
- **Port:** Enter the port to listen on.
- **VPN compression:** Enable or disable the VPN compression.
- **Client mode:** Choose the client mode: <Roadwarrior> or <Bridging>.
- **Network:** Enter the IP address for Clients.
- **OpenVPN bridge IP:** Establish a connection to the Web ConfigTool. It is recommended to use the same IP address like LAN1!
- **Start IP address range:** Enter the start IP address of an IP address pool.
- **End IP address range:** Enter the end IP address of an IP address pool.
- **Subnet mask:** Enter the subnet mask of the IP address pool.

2.4.2.4. OpenVPN certificates and keys

The following settings are for the OpenVPN client mode.

Figure 23: OpenVPN client certificates and keys

- **Status root CA certificate:** Click on [Info] to see the currently used root CA certificate.
- **Status client key:** Click on [Info] to see the currently used client key.
- **Status client certificate:** Click on [Info] to see the currently used client certificate.
- **Import key or certificates:** Import a single file of a root certificate, a client key and a client certificate. You can also import a complete configuration archive (*.tar.gz).

The following settings are for the OpenVPN server mode.

Figure 24: OpenVPN server certificates and keys

- **Root CA certificate modification:** Click on [Info] to see the currently used root CA certificate.
- **Server key modification:** Click on [Info] to see the currently used server key.
- **Server certificate modification:** Click on [Info] to see the currently used server certificate.
- **Diffie hellman parameters modification:** Click on [Info] to see the currently used Diffie-Hellman parameters.

2.4.2.5. OpenVPN create certificates

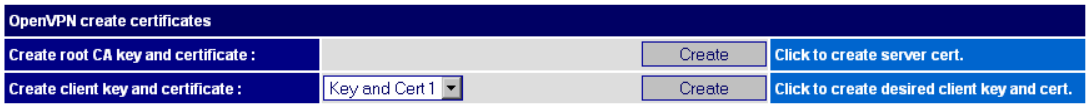

Figure 25: OpenVPN create certificates

- **Create root CA key and certificate:** Click on [Create] to generate a new server certificate.
- **Create client key and certificate:** Choose from the dropdown menu the desired client key and certificate. Then click on [Create] to generate a new key and certificate.

Please note: The generation of the OpenVPN certificates can take up to 30 minutes! Do not interrupt the process and wait until you have no **new timestamps** in "OpenVPN certificates and keys" overview! Click in the menu on "OpenVPN" to refresh this page.

2.4.2.6. OpenVPN export certificates

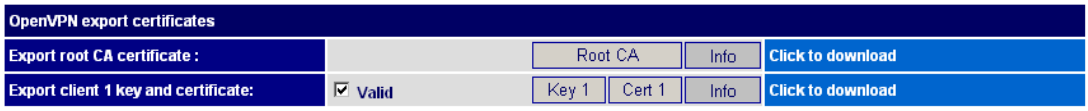

Figure 26: OpenVPN export certificates

- **Export root CA certificate:** Click on [Info] to see the currently used root CA certificate. Click on [Root CA] to download the current certificate.
- **Export client 1 key and certificate:** Click on [Info] to see the currently used client key and certificate. Click on [Key 1] to download the current key. Click on [Cert 1] to download the current client certificate.

2.4.3. IPsec

In this section you can configure the IPsec settings.

2.4.3.1. IPsec configuration

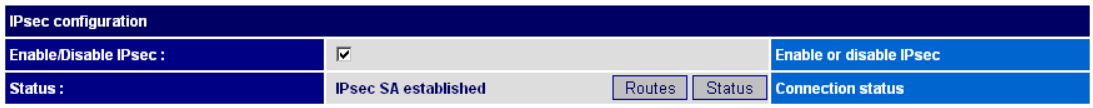

Figure 27: IPsec configuration

- **Enable/Disable IPsec:** Enable or disable IPsec.
- **Status:** Shows the current connection status. Click on [Routes] to see the routes. Click on [Status] to see all connection details.

2.4.3.2. Connection protocol

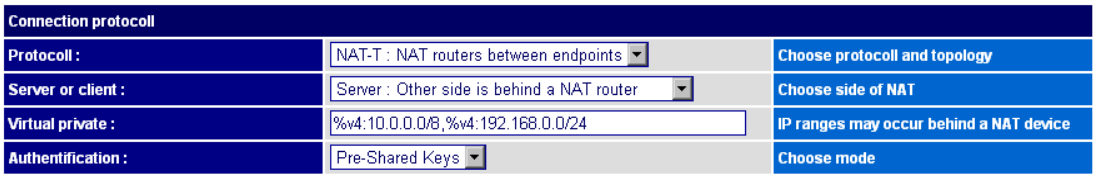

Figure 28: IPsec connection protocol

- **Protocol:** Choose the connection protocol and topology from the dropdown menu.
- **Server or client:** Choose the side of the NAT from the dropdown menu.
- **Virtual private:** Enter the IP ranges which may occur behind the NAT device.
- **Authentication:** Choose the authentication mode from the dropdown menu.

2.4.3.3. IPsec shared keys

Figure 29: IPsec shared keys

- **Pass phrase:** Enter the pass phrase for the secret shared key.
- **Confirm pass phrase:** Confirm the pass phrase for the secret shared key.

2.4.3.4. IPsec certificates and keys

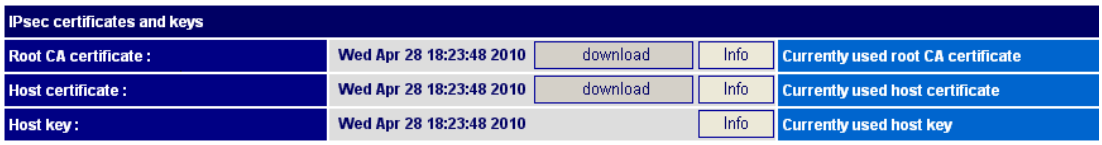

Figure 30: IPsec shared keys

- **Root CA certificate:** Click on [download] to save the currently used root CA certificate. Click on [Info] to see the currently used root CA certificate.
- **Host certificate:** Click on [download] to save the currently used host certificate. Click on [Info] to see the currently used host certificate.
- **Host key:** Click on [Info] to see the currently used host key.

2.4.3.5. Configuration of this side (right)

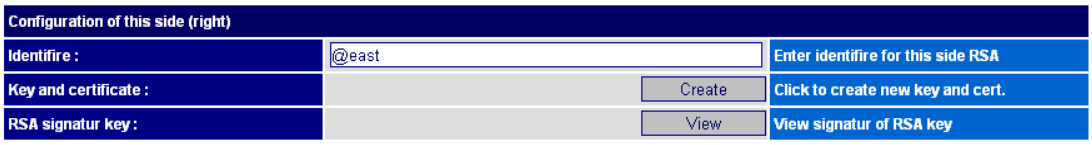

Figure 31: Configuration of this side (right)

- **Identifier:** Enter an identifier for this side.
- **Key and certificate:** Click on [Create] to generate a new key and certificate.
- **RSA signature key:** Click on [View] to see the signature of the RSA key.

2.4.3.6. Configuration of other side (left)

Figure 32: Configuration of other side (left)

- **Address:** Enter an IP address or full hostname for the other side.
- **Identifier:** Enter an identifier for the other side.
- **RSA signature key:** Enter the signature of the RSA key from the output of the command "`ipsec show host key -left`" on the IPsec server.

Please note: The signature key is a very long text file. Please put it in as one single line without any line breaks!

2.4.4. DynDNS

In this section you can configure the DynDNS settings.

2.4.4.1. DynDNS configuration

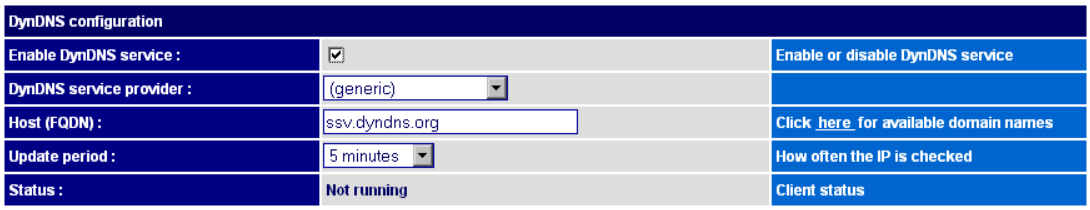

Figure 33: DynDNS configuration

- **Enable DynDNS service:** Enable or disable the DynDNS service.
- **DynDNS service provider:** Choose a DynDNS service provider from the dropdown menu.
- **Host (FQDN):** Enter the full hostname. Click on the link "here" for available domain names.
- **Update period:** Choose from the dropdown menu how often the IP address is checked.
- **Status:** Shows the current client status.

2.4.4.2. Change DynDNS username and password

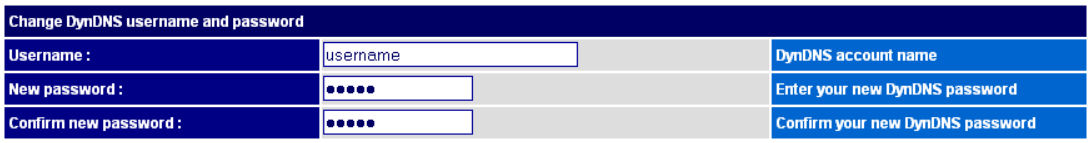

Figure 34: DynDNS username and password

- **Username:** Enter a DynDNS username.
- **New password:** Enter your new DynDNS password.
- **Confirm new password:** Confirm your new DynDNS password.

2.4.4.3. Notification to webserver after ipaddress changes

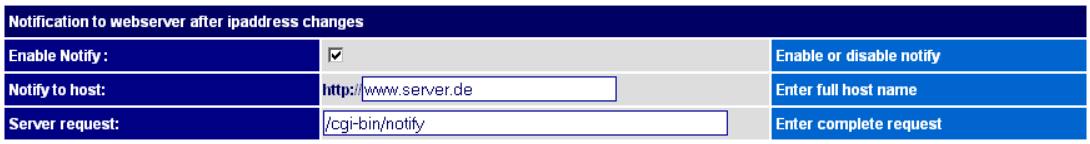

Figure 35: Notification to web server after IP address changes

- **Enable Notify:** Enable or disable the notification.
- **Notify to host:** Enter the full host name.
- **Server request:** Enter a complete GET request for the URL, e.g. a PHP script.

2.4.5. DHCP Server

In this section you can configure the DHCP server settings.

2.4.5.1. General configuration

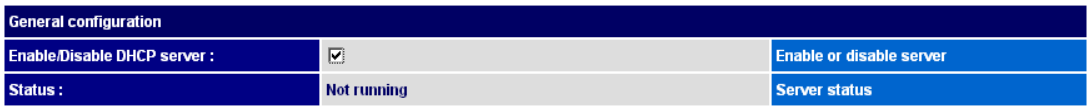

Figure 36: General configuration

- **Enable/Disable DHCP server:** Enable or disable the DHCP server.
- **Status:** Shows the current server status.

2.4.5.2. Address range

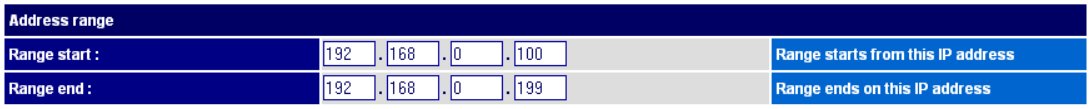

Figure 37: Address range

- **Range start:** Enter the start IP address for the IP address range.
- **Range end:** Enter the end IP address for the IP address range.

Please note: The DHCP server works on LAN1. So no other DHCP servers should exist there. All hosts in the network of LAN1 will use this device as gateway!

2.4.6. Firewall and NAT

In this section you can configure the firewall and NAT settings.

2.4.6.1. Firewall configuration

- **Enable/Disable firewall:** Enable or disable the firewall.

2.4.6.2. Firewall and NAT rules preconfigured sets

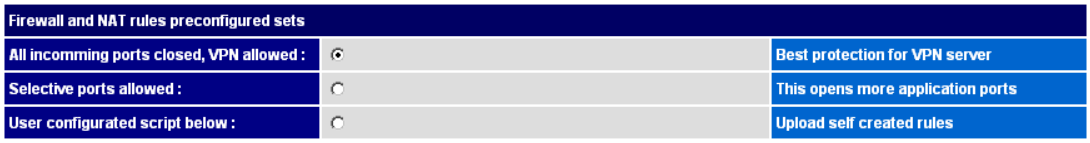

Figure 38: Firewall and NAT rules preconfigured sets

- **All incoming ports closed, VPN allowed:** Best protection for the VPN server.
- **Selective ports allowed:** This configuration opens more application ports.
- **User configured script below:** Upload own firewall rules.

2.4.6.3. System specific ports allowed on WAN interface

In this subsection you can simply allow or disallow which services may be accessed from unsafe WANs like Internet or GPRS/UMTS.

- **VPN server:** VPN server.
- **SSH access:** Remote access with SSH.
- **Telnet access:** Remote access with Telnet.
- **HTTP server:** Web server access.
- **HTTPS server:** Secure web server access.
- **Web proxy:** Access to HTTP proxy ports.
- **FTP proxy:** Access to FTP proxy ports.
- **TCP proxy:** Access to TCP proxy ports. (Telnet/SSH/others).
- **Web ConfigTool:** This web configuration site.
- **IPsec:** IPsec connection.

2.4.6.4. User specific ports allowed on WAN interface

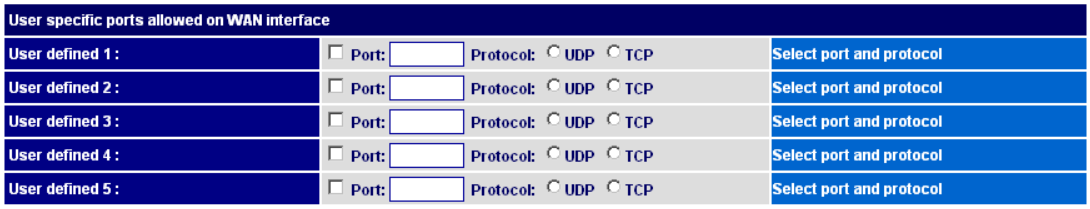

Figure 39: Firewall and NAT rules preconfigured sets

It is possible to define up to five specific ports for the WAN interface.

- **User defined X:** Click on the checkbox to enable the port. Enter the port number and choose the protocol.

2.4.6.5. ICMP protocols

- **Enable/Disable ping:** Allow ping on WAN interface.

2.4.6.6. Forwarding with IP-Masquerading and NAT

- **Enable/Disable forwarding:** Full routing from internal (LAN1) to WAN interface.

Please note: With this option all hosts in the network of LAN1 may use this device as gateway. Be careful with this option, if using GPRS/UMTS or other modem connections. This can produce very high traffic!

2.4.6.7. Firewall and NAT rules script

Figure 40: Firewall and NAT rules script

- **Show current settings:** Click on [Script rules] to show the current rules. Click on [Active policies] to show the current policies.
- **Upload new rules:** Upload your own rules as a “Firewall Builder” output file.

Please note: A misconfigured firewall is often the reason for not working services. Please disable the firewall before enabling/changing services or ports. Enable the firewall afterwards. If any service does not run properly, try it without the firewall enabled.

Please note: LAN1 and VPN are defined as secure networks and all ports are usable there. The port selective options like enabling/disabling are only available for the WAN interface. The WAN interface can be a GPRS/UMTS modem, DSL modem or a network on LAN2. To change this definition, a full set of rules must be created and uploaded as a user script. As a template you can use the preconfigured script rules.

2.5 Proxies

In this section you can configure the proxy server settings.

2.5.1. Web

In this section you can configure the Web proxy server settings.

2.5.1.1. General configuration

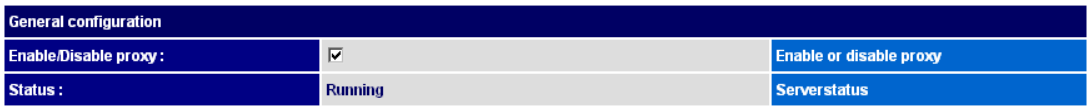

Figure 41: General configuration

- **Enable/Disable proxy:** Enable or disable the proxy server.
- **Status:** Shows the current server status.

2.5.1.2. Proxy redirections

Figure 42: Proxy redirections

This section shows the current HTTP or HTTPS proxy redirections. Click on [edit] to change the redirection settings or click on [delete] to remove the redirection.

2.5.1.3. Create/Edit a redirection entry

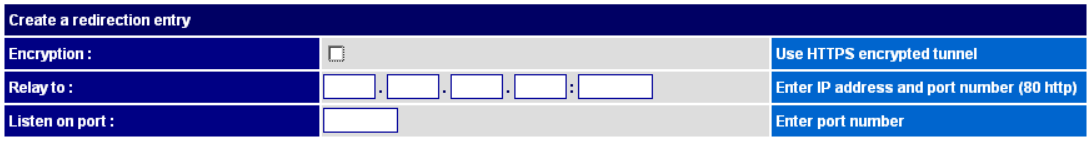

Figure 43: Create a redirection entry

Create a new redirection entry or change an existing redirection by clicking on [edit] in the section “Proxy redirections” above.

- **Encryption:** Enable or disable the HTTPS encrypted tunnel.
- **Relay to:** Enter an IP address and port number (e.g. port 80 for HTTP).
- **Listen on port:** Enter a port number.

2.5.1.4. SSL certificate

Figure 44: SSL certificate

- **Create SSL certificate:** Click on [Create] to generate a new SSL certificate.
- **Fingerprint MD5:** Shows the current MD5 fingerprint.
- **Fingerprint SHA1:** Shows the current SHA1 fingerprint.

2.5.2. DNS

In this section you can configure the DNS proxy server settings. These settings are only necessary, if the system is configured as a router on LAN1.

2.5.2.1. General configuration

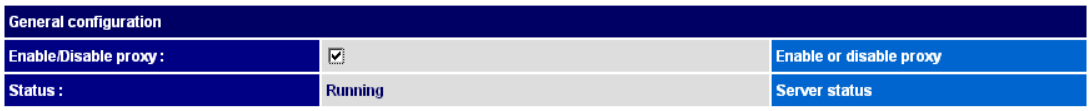

Figure 45: General configuration

- **Enable/Disable proxy:** Enable or disable the DNS proxy server.
- **Status:** Shows the current server status.

2.5.3. Filetransfer

In this section you can configure the FTP proxy server settings.

2.5.3.1. General configuration

- **Enable/Disable proxy:** Enable or disable the proxy server.

2.5.3.2. Proxy redirections

Figure 46: Proxy redirections

This section shows the current FTP proxy redirections. Click on [edit] to change the redirection settings or click on [delete] to remove the redirection.

2.5.3.3. Create/Edit a redirection entry

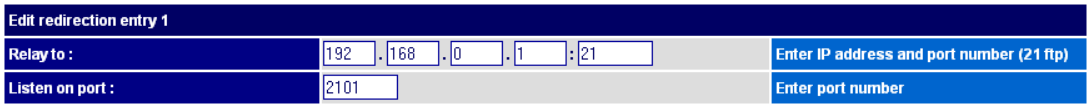

Figure 47: Editing a redirection entry

Create a new redirection entry or change an existing redirection by clicking on [edit] in the section “Proxy redirections” above.

- **Relay to:** Enter the IP address and port number (typ. port 21 for FTP).
- **Listen on port:** Enter the port number.

2.5.4. Telnet/SSH/others

In this section you can configure the Telnet, SSH or other TCP based proxy server settings.

2.5.4.1. General configuration

- **Enable/Disable proxy:** Enable or disable the proxy server.

2.5.4.2. Proxy redirections

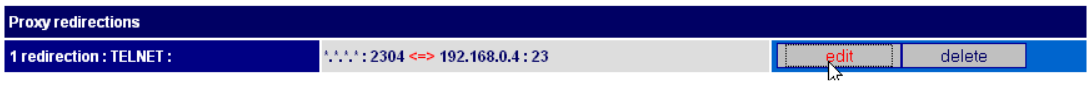

Figure 48: Proxy redirections

This section shows the current Telnet redirections. Click on [edit] to change the settings or click on [delete] to remove the Telnet redirection.

2.5.4.3. Create/Edit a redirection entry

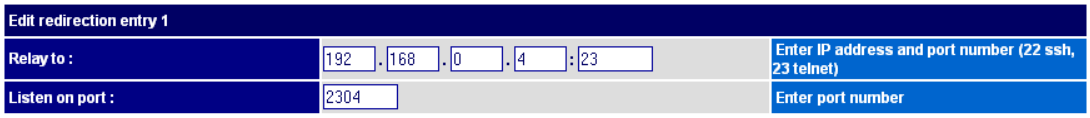

Figure 49: Editing a redirection entry

Create a new redirection entry or change an existing redirection by clicking on [edit] in the section "Proxy redirections" above.

- **Relay to:** Enter the IP address and port number (e.g. port 22 for SSH, port 23 for Telnet).
- **Listen on port:** Enter a port number.

2.6 Logout

Just click on Logout to finish the current session.

3 HELPFUL LITERATURE

- IGW/922 and IGW/925 hardware reference manual
- IGW/922 and IGW/925 first steps
- DIL/NetPC ADNP/9200 hardware reference manual

CONTACT

SSV Software Systems GmbH
Dünenweg 5
D-30419 Hannover

Phone: +49 (0)511/40 000-0
Fax: +49 (0)511/40 000-40
E-mail: sales@ssv-embedded.de

Internet: **www.ssv-embedded.de**
Forum: **www.ssv-comm.de/forum**

DOCUMENT HISTORY

Revision	Date	Remarks	Name
1.0	2013-04-30	First version	WBU

The content of this document can change any time without announcement. There is taken over no guarantee for the accuracy of the statements. The user assumes the entire risk as to the accuracy and the use of this document. Information in this document is provided 'as is' without warranty of any kind. Some names within this document can be trademarks of their respective holders.

© 2013 SSV Software Systems GmbH. All rights reserved.