



USER MANUAL

GWR Cellular Router Series

Device firmware version: 3.0
Document version: 3.16
Date: March 2016

Content

LIST OF FIGURES	4
LIST OF TABLES	7
DESCRIPTION OF THE GPRS/EDGE/HSPA/HSPA+/LTE ROUTER SERIES	8
TYPICAL APPLICATION	9
TECHNICAL PARAMETERS	10
PROTOCOLS AND FEATURES.....	12
PRODUCT OVERVIEW.....	15
Front panel.....	15
Back panel.....	15
Top Panel.....	16
PUTTING INTO OPERATION	17
DECLARATION OF CONFORMITY	18
DEVICE CONFIGURATION	19
DEVICE CONFIGURATION USING WEB APPLICATION.....	19
ADD/REMOVE/UPDATE MANIPULATION IN TABLES	20
SAVE/RELOAD CHANGES.....	20
STATUS INFORMATION	21
Status - General	21
Status - Network Information	21
Status - DHCP.....	22
Status - WAN Information.....	22
Status - Firewall.....	23
Status - Router Monitoring	23
SETTINGS – NETWORK.....	26
SETTINGS – DHCP SERVER.....	27
SETTINGS – WAN SETTING.....	29
SETTINGS – ROUTING	34
Port translation.....	35
SETTINGS – DYNAMIC ROUTING PROTOCOL.....	36
Routing Information Protocol (RIP).....	36
<i>RIP routing engine for the GWR Router</i>	<i>37</i>
SETTINGS – VPN SETTINGS.....	39
Generic Routing Encapsulation (GRE)	39
<i>GRE Keepalive.....</i>	<i>40</i>
Internet Protocol Security (IPSec).....	41
OpenVPN.....	47
SETTINGS – FIREWALL – MAC FILTERING	52
SETTINGS – DYNDNS.....	53
SETTINGS – SERIAL PORT.....	55
Serial port over TCP/UDP settings.....	55
Modbus Gateway settings	58
SMS(SHORT MESSAGE SERVICE)	60
SMS – SEND SMS	61
MAINTENANCE	62
Maintenance – System Control	62
Maintenance – Device Identity Settings	62
Maintenance – Administrator Password.....	63
Maintenance – Date/Time Settings.....	64
Maintenance – Diagnostics.....	66
Maintenance – Update Firmware	66
Maintenance – Settings Backup	67
<i>Import Configuration File</i>	<i>67</i>
<i>Export Configuration File</i>	<i>67</i>

Maintenance – Default Settings	68
Maintenance – System Reboot	68
MANAGEMENT – COMMAND LINE INTERFACE.....	69
MANAGEMENT – REMOTE MANAGEMENT	70
MANAGEMENT – CONNECTION MANAGER.....	71
Getting started with the Connection Wizard.....	71
MANAGEMENT – SIMPLE MANAGEMENT PROTOCOL (SNMP)	75
MANAGEMENT – LOGS	76
LOGOUT	77
CONFIGURATION EXAMPLES.....	78
GWR ROUTER AS INTERNET ROUTER	78
GRE TUNNEL CONFIGURATION BETWEEN TWO GWR ROUTERS	79
GRE TUNNEL CONFIGURATION BETWEEN GWR ROUTER AND THIRD PARTY ROUTER	83
IPSEC TUNNEL CONFIGURATION BETWEEN TWO GWR ROUTERS	86
Scenario #1.....	87
Scenario #2.....	93
Scenario #3.....	100
IPSEC TUNNEL CONFIGURATION BETWEEN GWR ROUTER AND CISCO ROUTER	105
IPSEC TUNNEL CONFIGURATION BETWEEN GWR ROUTER AND JUNIPER SSG FIREWALL	109
APENDIX	120
A. HOW TO ACHIEVE MAXIMUM SIGNAL STRENGTH WITH GWR ROUTER?	120
Antenna placement.....	120
Antenna Options.....	120

List of Figures

Figure 1 - GWR Router.....	8
Figure 2 - GWR Router front panel	15
Figure 3 - GWR Router back panel (GPRS and EDGE)	15
Figure 4 - GWR Router back panel (HSPA, HSPA+ and LTE)	16
Figure 5 - GWR Router top panel side.....	16
Figure 6 - Declaration of conformity	18
Figure 7 - User authentication.....	19
Figure 8 - General router information.....	21
Figure 9 - Network Information	22
Figure 10 - DHCP Information.....	22
Figure 11 - WAN Information.....	23
Figure 12 - Firewall Information.....	23
Figure 13 - Router Monitoring #1.....	24
Figure 14 - Router Monitoring #2.....	25
Figure 15 - Network parameters configuration page.....	26
Figure 16 - DHCP Server configuration page	28
Figure 17 - WAN Settings configuration page.....	29
Figure 18 - Routing configuration page.....	34
Figure 19 - RIP configuration page.....	36
Figure 20 - GRE tunnel parameters configuration page.....	40
Figure 21 - IPSec Summary screen	41
Figure 22 - IPSec Settings.....	43
Figure 23 - OpenVPN example	47
Figure 24-Open VPN Summary screen	47
Figure 25 - OpenVPN configuration page.....	50
Figure 26- Firewall configuration page.....	51
Figure 27- MAC filtering configuration page	53
Figure 28 - DynDNS settings.....	53
Figure 29 - Serial Port Settings initial menu	55
Figure 30 - Serial Port configuration page.....	57
Figure 31 - Modbus gateway configuration page.....	59
Figure 32 - SMS remote control configuration.....	60
Figure 33- Send SMS.....	61
Figure 34- System Control	62
Figure 35 - Device Identity Settings configuration page	62
Figure 36 - Administrator Password configuration page.....	63
Figure 37 - Date/Time Settings configuration page	64
Figure 38 - Diagnostic page.....	66
Figure 39 - Update Firmware page.....	66
Figure 40 - Export/Import the configuration on the router.....	67
Figure 41 - File download	67
Figure 42 - Default Settings page.....	68
Figure 43 - System Reboot page.....	68
Figure 44 - Command Line Interface	69
Figure 45 - Remote Management.....	70
Figure 46 - Connection Manager	71
Figure 47 - Connection Wizard - Initial Step	72
Figure 48 - Connection Wizard - Router Detection	73
Figure 49 - Connection Wizard - LAN Settings	73
Figure 50 - Connection Wizard - WAN Settings.....	74
Figure 51 - SNMP configuration page	75
Figure 52 - Syslog configuration page.....	76

Figure 53 – GWR Router as Internet router	78
Figure 54 – GRE tunnel between two GWR Routers	79
Figure 55 – Network configuration page for GWR Router 1.....	79
Figure 56 – GRE configuration page for GWR Router 1	80
Figure 57 – Routing configuration page for GWR Router 1	80
Figure 58 – Network configuration page for GWR Router 2.....	81
Figure 59 – GRE configuration page for GWR Router 2	81
Figure 60 – Routing configuration page for GWR Router 2	82
Figure 61 – GRE tunnel between Cisco router and GWR Router	83
Figure 62 – Network configuration page	84
Figure 63 – GRE configuration page.....	85
Figure 64 – Routing configuration page.....	85
Figure 65 – IPSec tunnel between two GWR Routers.....	86
Figure 66 – Network configuration page for GWR Router 1.....	87
Figure 67 – IPSEC configuration page I for GWR Router 1.....	88
Figure 68 – IPSEC configuration page II for GWR Router 1	88
Figure 69 – IPSEC configuration page III for GWR Router 1	89
Figure 70 – IPSEC start/stop page for GWR Router 1	89
Figure 71 – Network configuration page for GWR Router 2.....	89
Figure 72 – IPSEC configuration page I for GWR Router 2.....	91
Figure 73 – IPSEC configuration page II for GWR Router 2	91
Figure 74 – IPSEC configuration page III for GWR Router 2	91
Figure 75 – IPSEC start/stop page for GWR Router 2	92
Figure 76 – Network configuration page for GWR Router 1.....	93
Figure 77 – IPSEC configuration page I for GWR Router 1	94
Figure 78 – IPSEC configuration page II for GWR Router 1	95
Figure 79 – IPSEC configuration page III for GWR Router 1	95
Figure 80 – IPSEC start/stop page for GWR Router 1	95
Figure 81 – Network configuration page for GWR Router 2.....	96
Figure 82 – IPSEC configuration page I for GWR Router 2.....	97
Figure 83 – IPSEC configuration page II for GWR Router 2.....	98
Figure 84 – IPSEC configuration page III for GWR Router 2	98
Figure 85 – IPSEC start/stop page for GWR Router 1	98
Figure 86 – IPSEC configuration page I for GWG Gateway 1.....	101
Figure 87 – IPSEC configuration page II for GWG Gateway 1.....	101
Figure 88 – IPSEC start/stop page for GWG Gateway 1	102
Figure 89 – IPSEC configuration page I for GWG Gateway 2.....	103
Figure 90 – IPSEC configuration page II for GWG Gateway 2.....	103
Figure 91 – IPSEC start/stop page for GWG Gateway 1	104
Figure 92 – IPSEC tunnel between GWR Router and Cisco Router.....	105
Figure 93 – Network configuration page for GWR Router.....	105
Figure 94 – IPSEC configuration page I for GWR Router	107
Figure 95 – IPSEC configuration page II for GWR Router	107
Figure 96 – IPSEC configuration page III for GWR Router.....	107
Figure 97 – IPSEC start/stop page for GWR Router	108
Figure 98 – IPSEC tunnel between GWR Router and Cisco Router.....	110
Figure 99 – Network configuration page for GWR Router.....	110
Figure 100 – IPSEC configuration page I for GWR Router	112
Figure 101 – IPSEC configuration page II for GWR Router	112
Figure 102 – IPSEC configuration page III for GWR Router.....	113
Figure 103 – IPSEC start/stop page for GWR Router	113
Figure 104 – Network Interfaces (list).....	114
Figure 105 – Network Interfaces (edit)	114
Figure 106 – AutoKey Advanced Gateway.....	115
Figure 107 – Gateway parameters.....	115

Figure 108 - Gateway advanced parameters116
Figure 109 - AutoKey IKE.....116
Figure 110 - AutoKey IKE parameters117
Figure 111 - AutoKey IKE advanced parameters.....117
Figure 112 - Routing parameters118
Figure 113 - Policies from untrust to trust zone119
Figure 114 - Policies from trust to untrust zone119

List of Tables

Table 1 - Technical parameters.....	11
Table 2 - GWR Router features	14
Table 3 - Network parameters.....	26
Table 4 - DHCP Server parameters	28
Table 5 - WAN parameters.....	31
Table 6 - Advanced WAN Settings.....	33
Table 7 - Routing parameters	35
Table 8 - RIP parameters.....	37
Table 9 - GRE parameters	40
Table 10 - IPSec Summary for first firmware version.....	42
Table 11 - IPSec Parameters for first firmware version	46
Table 14 - OpenVPN parameters	50
Table 22 - Firewall parameters.....	52
Table 23 - MAC filtering parameters	53
Table 16 - DynDNS parameters	54
Table 17 - Serial Port over TCP/UDP parameters.....	56
Table 19 - Modbus gateway parameters.....	58
Table 20 - Device Identity parameters	62
Table 21 - Administrator password.....	64
Table 22 - Date/time parameters.....	65
Table 23 - Command Line Interface parameters	69
Table 24 - Remote Management parameters.....	70
Table 25 - SNMP parameters.....	75
Table 26 - Syslog parameters.....	77

Description of the GPRS/EDGE/HSPA/HSPA+/LTE Router Series

GWR routers represent a robust solution designed to provide remote connectivity across cellular networks. Low transmission delay and very high data rates offered by existing cellular networks completely eliminate the need for expensive wired infrastructure. GWR series brings scalability of even most demanding corporate networks on highest possible level. Installing a reliable, high performance backup solution for existing land lines or satellite networks is now a simple task thanks to modern cellular networks. Therefore, no matter if the goal is to provide primary internet access or backup solution for already existing network GWR router series represents a top rated solution.



Figure 1 – GWR Router

There are practically no limits when it comes to possible application of GWR routers. Wired infrastructure is no longer necessary for building scalable and high performance systems. GWR routers will reduce the costs and speed up the ROI process for each one of possible applications. The list of most common GWR router applications is presented bellow.

Typical application

Data collection and system supervision

- Extra-high voltage equipment monitoring,
- Running water, gas pipe line supervision,
- Centralized heating system supervision,
- Environment protection data collection,
- Flood control data collection,
- Alert system supervision,
- Weather station data collection,
- Power Grid,
- Oilfield,
- Light Supervision,
- Solar PV Power Solutions.

Financial and department store

- Connection of ATM machines to central site,
- Vehicle based bank service,
- POS,
- Vending machine,
- Bank office supervision.

Security

- Traffic control,
- Video Surveillance Solutions,

Other

- Remote Office Solution,
- Remote Access Solution.

There are numerous variations of each and every one of above listed applications. Therefore GENEKO formed highly dedicated, top rated support team that can help you analyze your requirements and existing system, chose the right topology for your new system, perform initial configuration and tests and monitor the complete system after installation. Enhance your system performance and speed up the ROI with high quality cellular routers and all relevant knowledge of GWR support team behind you.

Technical Parameters

Wireless Interfaces - 3G GSM Huawei MU609 (available on 3G models)	
UMTS/HSPA+	Band 1 (2100 MHz), Band 2 (1900 MHz), Band 5 (850 MHz), Band 8 (900 MHz) Transfer rate (max): 14.4 Mbps down, 5.76 Mbps up Note: UMTS/HSPA+ transfer rate limited to 12 MBps due to USB 1.1 Full Speed interface limitations
GSM/GPRS/EDGE	850/900/1800/1900 MHz Transfer rate (max): 236.8 Kbps down, 236.8 Kbps up
Antenna Connector	2 x 50 Ω SMA (Center pin: female)
SIM Slots	2, Mini-SIM (2FF), Drawer
Wired Interfaces - RS232	
Ports	1
Standard	EIA/TIA-232, RS-232, V.28/ V.24
Data Rate	250 kbps (Note 2)
DTE/DCE	DCE
Signal Support	TXD, RXD, RTS, CTS, DTR, DSR
Flow Control	Software XON/XOFF, Hardware CTS/RTS or DTR/DSR
Connector	RJ-45, 8p8c, Shielded
Pinout	1: RTS, 2: DTR, 3: TXD, 4: GND, 5: GND, 6: RXD, 7: DSR, 8: CTS
Wired Interfaces - USB	
Ports	1
Standard	USB 1.1 Host
Signaling	Full Speed, 12 Mbps
Connector	Type A
Wired Interfaces -Ethernet	
Ports	1
Standard/Physical Layer	IEEE 802.3; 10/100 Base-T
Data Rate/Mode/Interface	10/100 Mbit/s; Full or Half duplex; Auto MDI/MDIX
Connector	RJ-45, 8p8c, Shielded, with integrated Link and Activity LED's
Power	
Input	9-12 VDC
Input Protection	Transients, overcurrent (internal 1 A time-lag fuse)
Consumption at 9 VDC	Typical: TBD mA

Physical	
Dimensions (L x W x H)	135 mm x 95 mm x 35 mm
Weight	380g
Status LEDs	Reset, Power, Link, Signal (5 LED's), LAN (on Ethernet connector: Link, Activity)
Pushbuttons	1 - Device Reset (short press)/Factory Default (long press)
Material	Steel sheet 0.8 mm
Mounting	Desktop (optional: DIN Rail Mounting Kit)
Environmental	
Operating Temperature	-10° C to +55° C
Storage Temperature	-20° C to +85° C
Relative Humidity	5% to 95% (non-condensing)
IP rating	IP40
Ethernet Isolation	1.5 kV RMS
Serial Ports Protection (ESD)	+/- 15 kV (IEC 61000-4-2 Air Gap)
Approvals	
Safety	EN 60950-1:2006 + A1:2010 + A2:2013 + A11:2009 + A12:2011
EMC	EN 301 489-1 V1.9.2, EN 301 489-7 V1.3.1, EN 301 489-17 V2.1.1, EN 301 489-24 V1.5.1
Radio Spectrum	EN 301 511 v9.0.2, EN 301 908-2 v5.2.1, EN 301 908-13 v5.2.1, EN 300 328 v1.8.1

Table 1 – Technical parameters

Notes

- 1) Supported by hardware but currently not implemented in firmware. Feature might be available with future firmware upgrades.
- 2) Currently maximum of 115200 bps supported.

Protocols and features

Features	Short description
Ethernet	
LAN	<ul style="list-style-type: none"> • Static
DHCP Server: <ul style="list-style-type: none"> • Static lease reservation • Address exclusions 	DHCP Server support.
Network	
Routing	Static
RIP	The Routing Information Protocol provides great network stability, guarantying that if one network connection goes down the network can quickly adapt to send packets through another connection.
DMZ support	Demilitarized Zone (DMZ) allows one local IP Address to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open, DMZ provides this function by forwarding all the ports to one computer at the same time.
SNMP	SNMP (<i>Simple Network Management Protocol</i>) is a network protocol that provides network administrators with the ability to monitor the status of the Geneko Router and receive notification of any critical events as they occur on the network. The Router supports SNMP v1/v2c and all relevant Management Information Base II (MIBII) groups. The appliance replies to SNMP Get commands for MIBII via any interface (Mobile, LAN, WAN/DSL, Wireless) and supports a custom MIB for generating trap messages.
NTP(RFC1305)	The Network Time Protocol is a protocol for synchronizing the clocks of router.
DynDNS	Client for various dynamic DNS services.
Firewall: <ul style="list-style-type: none"> • IP filtering • MAC filtering 	IP address / Network filtering
Serial over TCP/UDP	Serial to Ethernet converter
Modbus serial/IP gateway	Translation between Modbus/TCP or Modbus/RTU.
SMS	SMS Remote Control Send SMS
VPN (Virtual Private Network)	
GRE	GRE is a tunneling protocol which is used to transport packets from one network to another by opening a tunnel.
GRE keepalive	<ul style="list-style-type: none"> • Keepalive for GRE tunnels, • Cisco compliant.
IPSec pass-through	ESP tunnels.
IPsec	IPsec (<i>Internet Protocol Security</i>) is a protocol suite for securing IP communication.
Key Exchange Mode	<ul style="list-style-type: none"> • IKE with Preshared key
Data integrity	<ul style="list-style-type: none"> • HMAC-MD5, SHA-1, • Authentication and key management.
Authenticate Mode	<ul style="list-style-type: none"> • Pre-shared key
Encryption	<ul style="list-style-type: none"> • 3DES • AES (128/192/256) • Blowfish (128/192/256) • SERPENT (128/192/256)

	<ul style="list-style-type: none"> TWOFISH (128/256)
IPSec IKE failover	Defines number of failed IKE negotiation attempts before failover.
IPSec tunnel failover	This option will failover to other tunnel in case that selected one fails to established connection
IPSec - max. number of tunnels	5
OpenVPN	OpenVPN is a full-featured SSL VPN solution for securing communications via the Internet. Implements OSI layer 2 or 3 secure network extension using the industry standard SSL/TLS protocol.
OpenVPN - max. number of tunnels	5
GSM/UMTS features	
2G/3G/4G	Support with dual SIM capability.
Dual SIM support	For operator backup.
SIM PIN locking	Enable locking of SIM card with PIN code.
Roaming protection	By enabling this option router will be able to connect to roaming network.
Authentication	PAP, CHAP, PAP-CHAP
SIM keepalive	Make some traffic periodically in order to maintain connection alive.
SIM Priority	SIM1, SIM2
Reboot after failed connections	Reboot gateway after 'n' consecutive failed connection attempts.
Persistent connection	Keep connection alive, try to reopen the connection if it is broken.
Management	
User-friendly WEB GUI	HTTP based.
CLI: <ul style="list-style-type: none"> SSH telnet serial 	Remote management over SSH. Remote management over Telnet. Custom AT scripting to modem
Traffic and event log	Log tracing.
Connection Manager	Enabling Connection Manager will allow Connection Wizard (located on setup CD that goes with the router) to guide you step-by-step through the process of device detection on the network and setup of the PC-to-device communication. Thanks to this utility user can simply connect the router to the local network without previous setup of the router. Connection Wizard will detect the device and allow you to configure some basic functions of the router. Connection Manager is enabled by default on the router and if you do not want to use it you can simply disable it.
Remote Management	Remote Management Utility is a standalone Windows application with many useful options for configuration and monitoring of Geneko Routers.
Maintenance	
Diagnostics	Ping utility
Date/Time Settings	Current Date and Time Date and Time Setup: <ul style="list-style-type: none"> Manually Automatically
Device Identity Settings	There is an option to define name, location of device and description of device function. These data are kept in device permanent memory.
Import/Export settings	Import or Export of configuration (Possibility of selecting type of configuration to export).

Factory default settings	External taster and configuration application.
Update Firmware	<ul style="list-style-type: none">• Over WEB interface

Table 2 - GWR Router features

Product Overview

Front panel

On the front panel (*Figure 2*) the following connectors are located:

- one RJ45 connector – Ethernet port for connection into local computer network,
- one RJ45 connector for RS232 serial communication,
- reset button,
- one USB connector for connection of additional device,
- Power supply connector.

Ethernet connector LED:

- ACT (yellow) on – Network traffic detected (off when no traffic detected),
- Network Link (green LED) on – Ethernet activity or access point engaged.

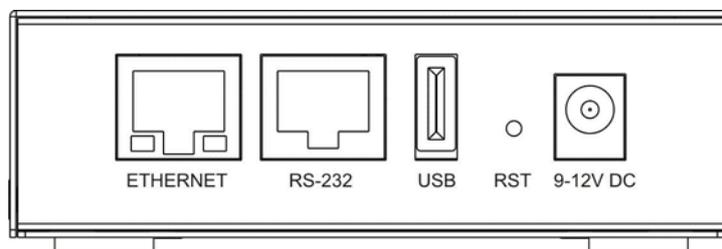


Figure 2 – GWR Router front panel

The Reset button can be used for a warm reset or a reset to factory defaults.

Warm reset: If the GWR Router is having problem connecting to the Internet, press and hold the reset button for a second using the tip of a pen.

Reset to Factory Defaults: To restore the default settings of the GWR Router, hold the RESET button pressed for a few seconds. Restoration of the default configuration will be signaled by blinks of the first and last signal strength LED on the top panel. This will restore the factory defaults and clear all custom settings of the GWR Router. You can also reset the GWR Router to factory defaults using the Maintenance > Default Settings screen.

Back panel

On the back panel of device (*Figure 3* and *Figure 4*) the following connectors are located:

- slot for SIM cards,
- 2 SMA connectors for connection of the GSM/UMTS antenna (main, aux).

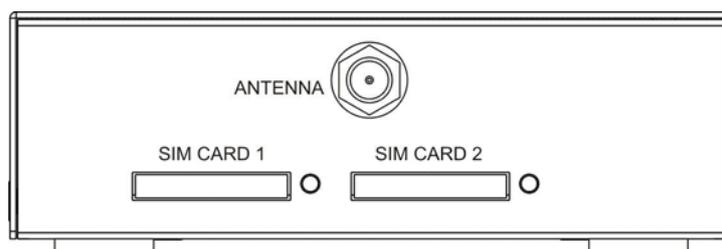


Figure 3 – GWR Router back panel (GPRS and EDGE)

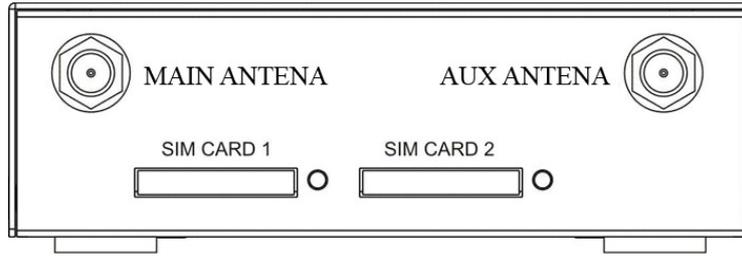


Figure 4 - GWR Router back panel (HSPA, HSPA+ and LTE)

Top Panel

There is a sequence of 8 LED indicators on the top of this device by which the indication of the system current state, device power supply and presence of GSM/UMTS network as well as signal level is performed.

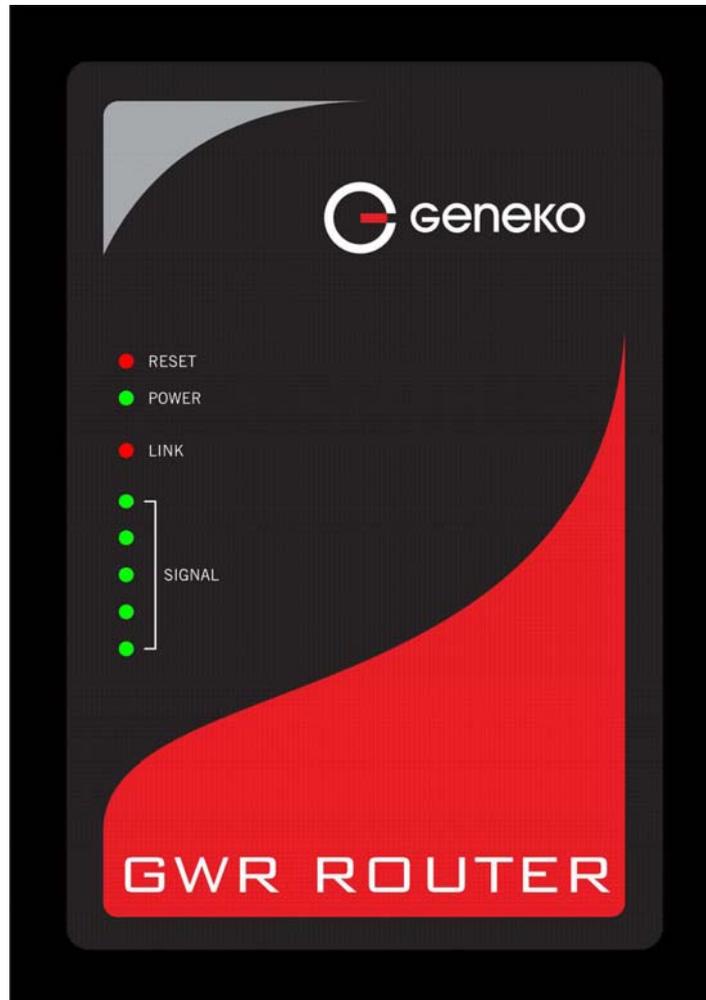


Figure 5 - GWR Router top panel side

LED Indicator Description:

1. Reset (red LED) on – the GWR Router reset state.
2. Power status (green LED) on – Power supply. Power status LED will blink when the GWR Router is in initializing state.
3. Link (red LED) will blink when connection is active.
4. Signal strength LED indicator:
 - -107 or less dBm = Unacceptable (1 LED),
 - -107 to -98 dBm = Weak (2 LED),
 - -98 to -87 dBm = Moderate (3 LED),
 - -87 to -76 dBm = Good (4 LED),
 - -76 or better dBm = Excellent (5 LED).
 - 0 is not known or not detectable (running LED).

Signal strength LED will blink when GPRS/EDGE/HSPA/HSPA+/LTE connection is not active. When connection is active Signal strength LED is on. Reset condition will be indicated by blinks of the first and last Signal strength LED. When signal quality is not known or not detectable there will be running LED indication.

Putting Into Operation

Before putting the GWR Router in operation it is necessary to connect all components needed for the operation:

- GSM antenna,
- Ethernet cable and
- SIM card must be inserted.

And finally, device should have powered up using power supply adaptor.

SIM card must not be changed, installed or taken out while device operates. This procedure is performed when power supply is not connected.

Declaration of conformity



RB General Ekonomik
HARDWARE · SOFTWARE · ENGINEERING



DECLARATION OF CONFORMITY

We hereby declare, that following product
COMMUNICATION EQUIPMENT WIRELESS ROUTER

Model/Type reference	Trade Mark	Ratings
GWR202-XXXXXX, GWR252-XXXXXX GWR302-XXXXXX, GWR352-XXXXXX*	GENEKO GWR ROUTER	Input: 9-12 V ~, 1A

* Where x can be any combination of numbers or characters, and represents non-safety relevant information

are in conformity with standards harmonised with directives:

LVD	IEC 60950-1:2005 (Second Edition), Am 1: 2009 Test report No. T223-0258/11
EMC	EN 301 489-1 V1.8.1 (2008-04) EN 301 489-7 V1.3.1 (2005-11) Test report No. T251-0689/11
R&TTE	Article 10 (5) and Annex IV of R&TTE Directive 1999/5/EC EN 60950-1:2006+A11:2009 EN 301 489-1 V1.8.1, EN 301 489-7 V1.3.1 EN 301 511 V9.0.2, EN 301 908-1 V3.2.1, EN 301 908-2 V3.2.1. Statement of Opinion No. 1304-R&TTE-C251-0119/11
RoHS	EU Directive 2002/95/EC EU Commission Decision 2005/618/EC, 2005/717/EC 2005/747/EC, 2006/310/EC, 2006/690/EC 2006/691/EC and 2006/692/EC Test report No. T211-0129/08

CE 1304

Year of affixing of CE mark:
2008

Place and date:
Belgrade, December 30, 2011

Director
Borisav Bojkovic



RB GeneralEkonomik

Bul Despota Sefana 59a · 11000 Belgrade · Serbia · Phone: +381 11 3340-591, 3340-178 · Fax: +381 11 3224-437 · office@geneko.rs · www.geneko.rs

Figure 6 – Declaration of conformity

Device Configuration

There are two methods which can be used to configure the GWR Router. Administrator can use following methods to access router:

- Web browser,
- Command line interface.

Default access method is by web interface. This method provides administrator full set of privileges for configuring and monitoring the router. Configuration, administration and monitoring of the GWR Router can be performed through the web interface. The default IP address of the router is 192.168.1.1. Another method is by command line interface. This method has limited options for configuring the GWR Router but still represents a very powerful tool when it comes to router setup and monitoring. Another document deals with CLI commands and instructions.

Device configuration using web application

The GWR Router's web-based utility allows you to set up the Router and perform advanced configuration and troubleshooting. This chapter will explain all of the functions in this utility.

For local access to the GWR Router's web-based utility, launch your web browser, and enter the Router's default IP address, 192.168.1.1, in the address field. A login screen prompts you for your User name and Password. Default administration credentials are admin/admin.

If you want to use web interface for router administration please enter IP address of router into web browser. Please disable *Proxy server* in web browser before proceed.

geneko
HARDWARE

GWR ROUTER - CONFIGURATION CONSOLE

Login

Username

Password

Login

Copyright © 2008 Geneko. All rights reserved.
<http://www.geneko.co.rs/>

Figure 7 - User authentication

After successfully finished process of authentication of *Username/Password* you can access *Main Configuration Menu*.

You can set all parameters of the GWR Router using web application. All functionalities and parameters are organized within few main tabs (windows).

Add/Remove/Update manipulation in tables

To **Add** a new row (new rule or new parameter) in the table please do following:

- Enter data in fields at the bottom row of the table (separated with a line).
- After entering data in all fields click **Add** link.

To **Update** the row in the table:

- Change data directly in fields you want to change.

To **Remove** the row from the table:

- Click **Remove** link to remove selected row from the table.

Save/Reload changes

To save all the changes in the form press **Save** button. By clicking **Save** data are checked for validity. If they are not valid, error message will be displayed. To discard changes press the **Reload** button. By clicking **Reload**, previous settings will be loaded in the form.

Status Information

The GWR Router’s Status menu provides general information about router as well as real-time network information. Status information is divided into following categories:

- General Information,
- Network Information (LAN),
- DHCP,
- WAN Information,
- Firewall,
- Router Monitoring

Status – General

General Information Tab provides general information about device type, device firmware version, kernel version, CPU vendor, Up Time since last reboot, hardware resources utilization and MAC address of LAN port. Screenshot of General Router information is shown at *Figure 8*. Data in Status menu are read only and cannot be changed by user. If you want to refresh screen data press *Refresh* button.

SIM Card detection is performed only at time booting the system, and you can see the status of SIM slot by checking the Enable SIM Card Detection option.

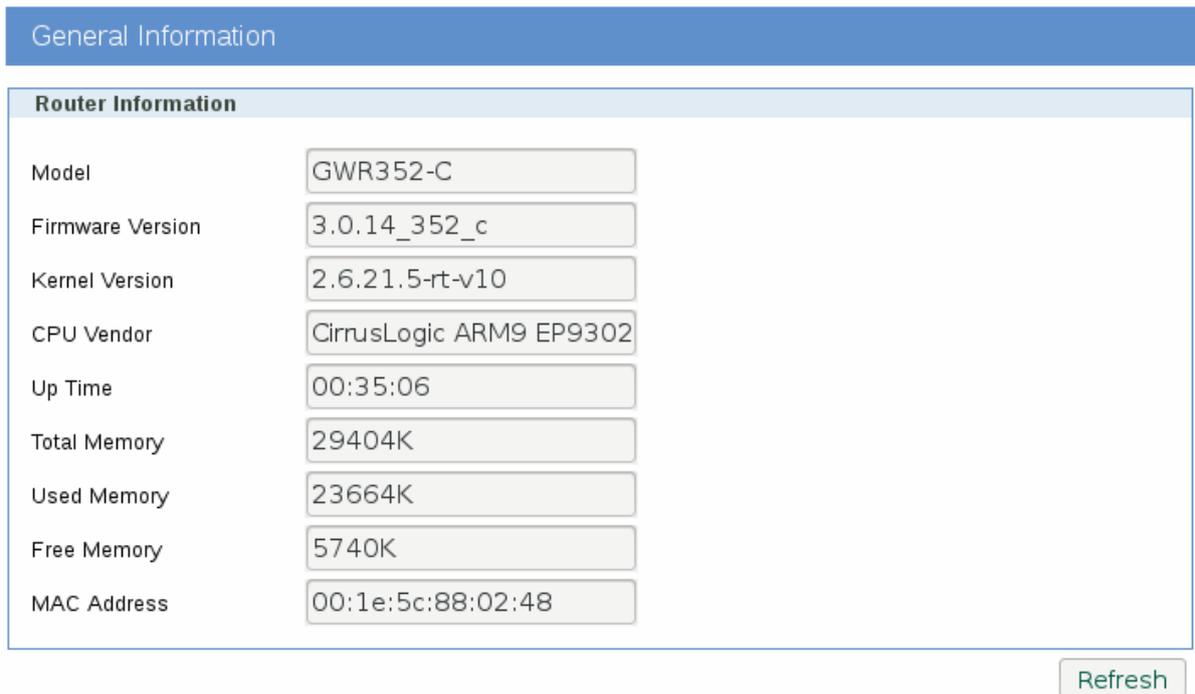


Figure 8 – General router information

Status – Network Information

Network Information Tab provides information about Ethernet port and Ethernet traffic statistics. Screenshot of Network Router information is shown in *Figure 9*.

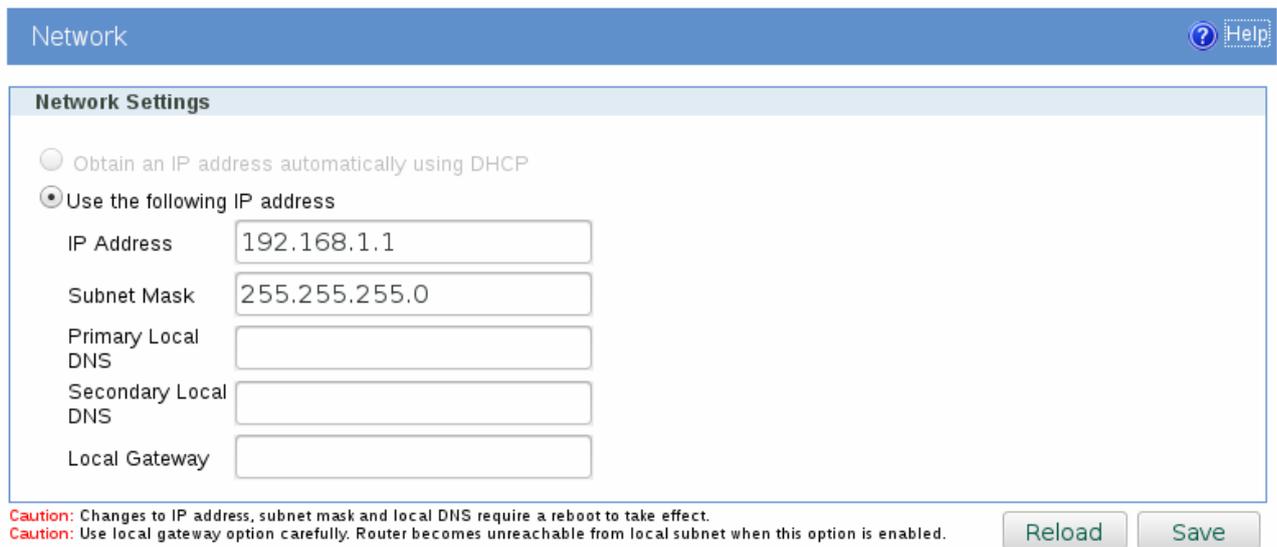


Figure 9 – Network Information

Status – DHCP

DHCP Information Tab provides information about DHCP clients with IP addresses gained from DHCP server, MAC addresses, expiration period, and lease status. Screenshot of DHCP information from the router is shown in *Figure 11*.

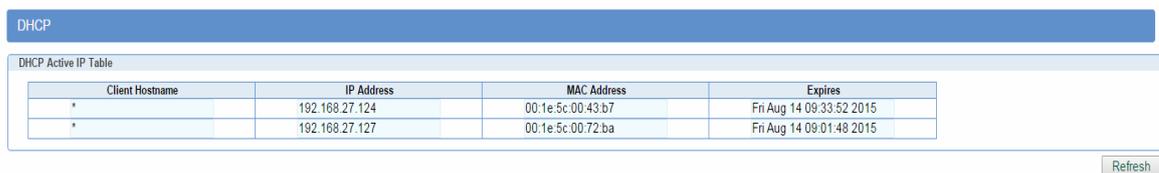


Figure 10 – DHCP Information

Status – WAN Information

WAN Information Tab provides information about GPRS/EDGE/HSPA/HSPA+/LTE connection and traffic statistics. *WAN information menu* has three submenus which provide information about:

- GPRS/EDGE/HSPA/HSPA+/LTE mobile module(manufacturer and model),
- Mobile operator and signal quality,
- Mobile traffic statistics.

Screenshot of WAN information from the router is shown in *Figure 111*.

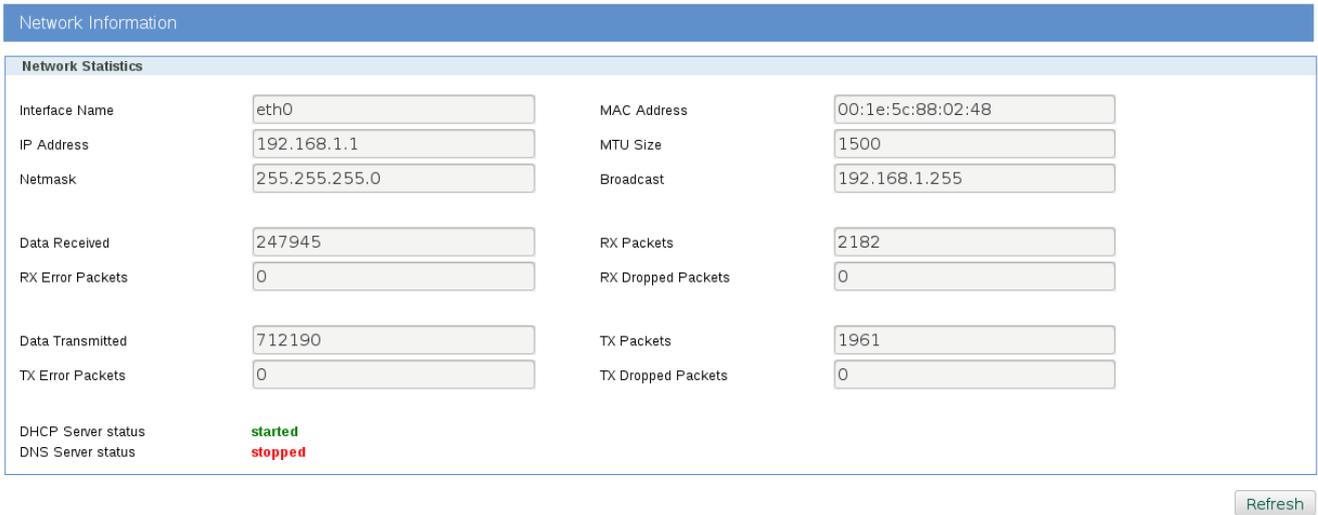


Figure 11 – WAN Information

Status – Firewall

Firewall Information Tab provides information about active firewall rules divided in three groups: INPUT, FORWARD and OUTPUT chain. Each of these groups has packet counter which can be cleared with one of three displayed button: Reset INPUT, Reset FORWARD and Reset OUTPUT. Screenshot of Firewall Information from the router is shown in Figure 12.

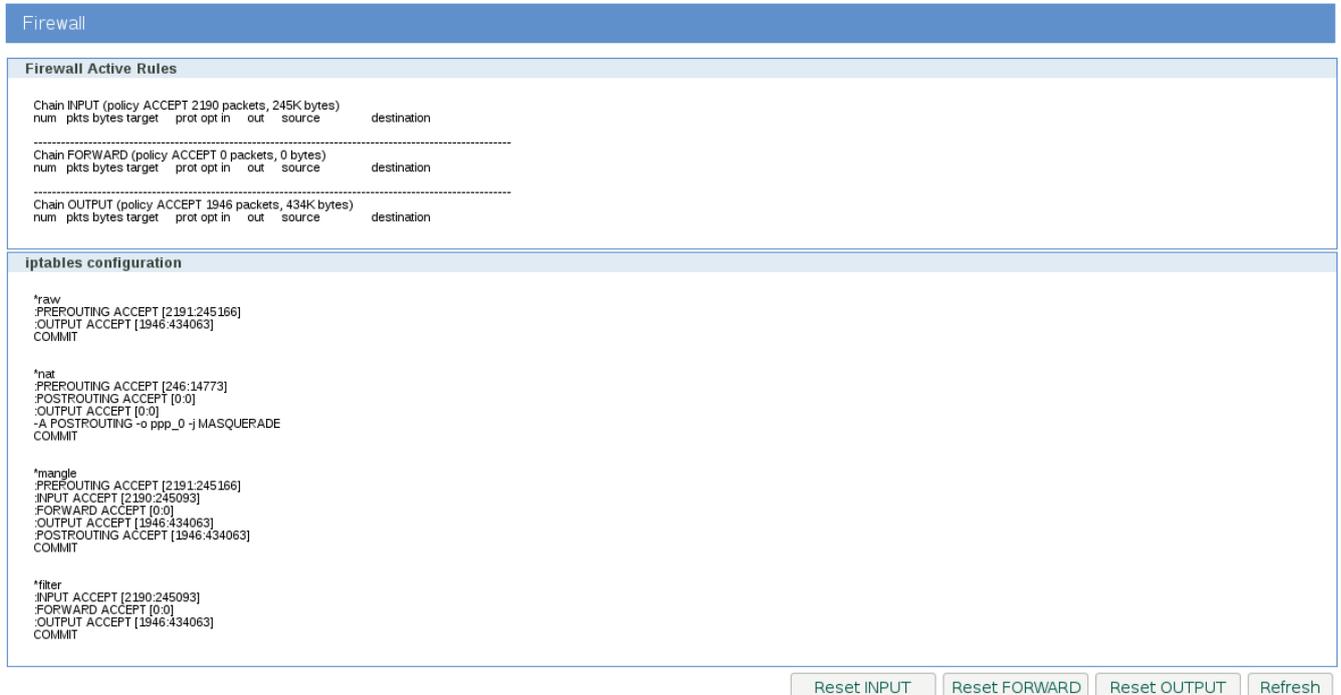


Figure 12 – Firewall Information

Status – Router Monitoring

Router Monitoring tab provides Base information, LAN and WAN real-time information. You can activate Automatic refresh after 5, 10, 15, 30 or 60 seconds. Screenshot of Router Monitoring Information from the router is shown in Figure 13.

Router Monitoring			
<input checked="" type="checkbox"/> Base Information			
Model	GWR352-C	Firmware version	3.0.14_352_c
Kernel version	2.6.21.5-rt-v10	Up time	00:15:44
Total memory	29404K	Used memory	24004K
Free memory	5400K		
<input checked="" type="checkbox"/> LAN Information			
IP address	192.168.1.1	Netmask	255.255.255.0
Broadcast	192.168.1.255	MTU	1500
Primary local DNS		Secondary local DNS	
DHCP server status	started	DNS server status	stopped
<input checked="" type="checkbox"/> LAN Statistics			
Data received(bytes)	303757	Received packet	2402
Error packet	0	Dropped packet	0
Data transmitted(bytes)	490702	Transmitted packet	2131
Error packet	0	Dropped packet	0

Figure 13 – Router Monitoring #1

<input checked="" type="checkbox"/> WAN Information			
Modem manufacturer	<input type="text" value="Cinterion"/>	Modem model	<input type="text" value="PH8-P"/>
Modem serial number	<input type="text" value="359628040349776"/>	Revision	<input type="text" value="03.001"/>
<input checked="" type="checkbox"/> WAN Connection			
Operator	<input type="text" value="Vip SRB"/>	Cell ID	<input type="text" value="0354"/>
Signal strength	<input type="text" value="-71 dBm"/>	Radio access technology	<input type="text" value="EDGE"/>
Connection status	<input type="text" value="connected"/>	Activity time	<input type="text" value="00:06:26"/>
WAN address	<input type="text" value="10.81.243.160"/>	PPP address	<input type="text" value="10.64.64.64"/>
Primary DNS address	<input type="text" value="212.91.97.3"/>	Secondary DNS address	<input type="text" value="212.91.97.4"/>
<input checked="" type="checkbox"/> WAN Statistics			
Data received(bytes)	<input type="text" value="76"/>	Received packet	<input type="text" value="10"/>
Error packet	<input type="text" value="0"/>	Dropped packet	<input type="text" value="0"/>
Data transmitted(bytes)	<input type="text" value="205"/>	Transmitted packet	<input type="text" value="11"/>
Error packet	<input type="text" value="0"/>	Dropped packet	<input type="text" value="0"/>
<input type="checkbox"/> Automatic refresh after <input type="text" value="10"/> sec			
<input type="button" value="Refresh"/>			

Copyright © 2008 - 2014 Geneko. All rights reserved.
<http://www.geneko.rs>

Figure 14 – Router Monitoring #2

Settings – Network

Click *Network* Tab, to open the LAN network screen. Use this screen to configure LAN TCP/IP settings.

Network Tab Parameters	
Label	Description
<i>Use the following IP address</i>	Choose this option if you want to manually configure TCP/IP parameters of Ethernet port.
<i>IP Address</i>	Type the IP address of your GWR Router in dotted decimal notation. 192.168.1.1 is the factory default IP address.
<i>Subnet Mask</i>	The subnet mask specifies the network number portion of an IP address. The GWR Router support sub-netting. You must specified subnet mask for your LAN TCP/IP settings.
<i>Primary Local DNS</i>	IP address of your primary local DNS server
<i>Secondary Local DNS</i>	IP address of your secondary local DNS server.
<i>Local Gateway</i>	Type the IP address of your local gateway. Use Local Gateway option carefully. Router becomes unreachable from local subnet when this option enabled.
<i>Reload</i>	Click <i>Reload</i> to discard any changes and reload previous settings.
<i>Save</i>	Click <i>Save</i> button to save your changes back to the GWR Router. Whether you make changes or not, router will reboot every time you click <i>Save</i> .

Table 3 - Network parameters

In the *Figure 155* you can see screenshot of *Network* Tab configuration menu.



Figure 15 - Network parameters configuration page

Settings – DHCP Server

The GWR Router can be used as a DHCP (Dynamic Host Configuration Protocol) server on your network. A DHCP server automatically assigns available IP addresses to computers on your network. If you choose to enable the DHCP server option, all of the computers on your LAN must be set to obtain an IP address automatically from a DHCP server. (By default, Windows computers are set to obtain an IP automatically.)

To use the GWR Router as your network’s DHCP server, click **DHCP Server** Tab for DHCP Server setup. The GWR Router has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

DHCP Server Parameters	
Label	Description
<i>Enable DHCP Server</i>	DHCP (Dynamic Host Configuration Protocol) allows individual clients (workstations) to obtain TCP/IP configuration at startup from a server. When configured as a server, the GWR Router provides TCP/IP configuration for the clients. To activate DHCP server, click check box Enable DHCP Server . To setup DHCP server fill in the IP Starting Address and IP Ending Address fields. Uncheck Enable DHCP server check box to stop the GWR Router from acting as a DHCP server. When Unchecked, you must have another DHCP server on your LAN, or else the computers must be manually configured. Uncheck Enable DHCP server check box to stop the GWR Router from acting as a DHCP server. When Unchecked, you must have another DHCP server on your LAN, or else the computers must be manually configured.
<i>IP Starting Address (From)</i>	This field specifies the first of the contiguous addresses in the IP address pool.
<i>IP Ending Address (To)</i>	This field specifies last of the contiguous addresses in the IP address pool.
<i>Lease Duration</i>	This field specifies DHCP session duration time.
<i>Primary DNS, Secondary DNS</i>	This field specifies IP addresses of DNS server that will be assigns to systems that support DHCP client capability. Select None to stop the DHCP Server from assigning DNS server IP address. When you select None, computers must be manually configured with proper DNS IP address. Select Used by ISP to have the GWR Router assigns DNS IP address to DHCP clients. DNS address is provided by ISP (automatically obtained from WAN side). This option is available only if mobile connection is active. Please establish mobile connection first and then choose this option. Select Used defined to have the GWR Router assigns DNS IP address to DHCP clients. DNS address is manually configured by user.
<i>Static Lease Reservation</i>	This field specifies IP addresses that will be dedicated to specific DHCP Client based on MAC address. DHCP server will always assign same IP address to appropriate client.
<i>Address Exclusions</i>	This field specifies IP addresses that will be excluded from the pool of DHCP IP address. DHCP server will not assign this IP to DHCP clients.
<i>Add</i>	Click Add to insert (add) new item in table to the GWR Router.
<i>Remove</i>	Click Remove to delete selected item from table.
<i>Save</i>	Click Save to save your changes back to the GWR Router.
<i>Reload</i>	Click Reload to discard any changes and reload previous settings.

Table 4 - DHCP Server parameters

DHCP Server
[? Help](#)

DHCP Server Settings

Enable DHCP server

IP Address range Lease duration days hrs mins

From

To

Network

Netmask

Primary DNS Secondary DNS

None None

Used by ISP Used by ISP

User defined User defined

Static Lease Reservations

IP addresses that will be dedicated to specific DHCP Client based on MAC address

Enable	IP Address	MAC Address	Action
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Add

Address Exclusions

Exclude these address from the DHCP IP address pool

Enable	Start Address	End Address	Action
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Add

Status

DHCP Server status started

DNS Server status stopped

* MAC Address format: xx:xx:xx:xx:xx:xx

* The IP address pool must specify addresses that are in the subnetwork of the GWR Router. The DHCP server will not operate if this configuration does not meet this requirement.

* A reservation IP address must not be the same as the IP address of the DHCP server itself. It must be a valid IP address in the subnetwork of the DHCP server. The DHCP server will ignore a reservation that does not meet these requirements.

* An IP address exclusion range must specify valid IP addresses in the subnetwork of the DHCP server. The DHCP server will ignore an exclusion that does not meet this requirement.

Reload
Save

Copyright © 2008 - 2014 Geneko. All rights reserved.
<http://www.geneko.rs>

Figure 16 - DHCP Server configuration page

Settings – WAN Setting

Click *WAN Settings* Tab, to open the Wireless screen. Use this screen to configure the GWR Router GPRS/EDGE/HSPA/HSPA+/LTE parameters (Figure 177).

Figure 17 – WAN Settings configuration page

WAN Settings	
Label	Description
<i>Provider</i>	This field specifies name of GSM/UMTS ISP. You can setup any name for provider.
<i>Authentication</i>	This field specifies password authentication protocol. Select the appropriate protocol from drop down list. (PAP, CHAP, PAP – CHAP).
<i>Username</i>	This field specifies Username for client authentication at GSM/UMTS network. Mobile provider will assign you specific username for each SIM card.
<i>Password</i>	This field specifies Password for client authentication at GSM/UMTS network. Mobile provider will assign you specific password for each SIM card.

APN	This field specifies APN.
Dial String	This field specifies Dial String for GSM/UMTS modem connection initialization. In most cases you have to change only APN field based on parameters obtained from Mobile Provider. This field cannot be altered.
Number of retry	This field specifies number of attempts to establish connection.
PIN enabled	This field enables you to enter PIN code for SIM card if it is enabled on the SIM.
Enable Failover	Mark this option in order to enable failover feature. This feature is used when both SIM have been enabled. You specify the amount of time after which Failover feature brings down current WAN connection (SIM2) and brings up previous WAN connection (SIM1).
Enable network locking	A network lock forces your device only supporting SIM cards which are locked on a predefined set of networks. This lock is defined by a list of PLMNs.
Persistent connection	Keep connection alive, after Do not exit after a connection is terminated. Instead try to reopen the connection.
Reboot after failed connections	Reboot after n consecutive failed connection attempts.
Enable SIM1/SIM2 keepalive	Make some traffic periodically in order to maintain connection active. You can set keepalive interval value in minutes.
Ping target	This field specifies the target IP address for periodical traffic generated using ping in order to maintain the connection active.
Ping interval	This field specifies ping interval for keepalive option.
Advanced ping interval	This field specifies the time interval for advanced ping proofing.
Advanced ping wait for a response	This field specifies the timeout for advanced ping proofing.
Maximum number of failed packets	This field specifies maximum number of failed packets in percent before keepalive action is performed.
Keepalive action	This menu provides a choice between two possible keepalive actions in case maximum number of failed packets is exceeded. If Switch SIM option is selected router will try to establish the connection using the other SIM card after the maximum number of failed packets is exceeded. If Current SIM option is selected router will only restart the PPP connection.
Enable SIM1/SIM2 data limit	Enable traffic data limit per SIM.
Traffic limit	Defines maximum data amount transferred over SIM card. When traffic limit is reached SIM card cannot be longer used for network connection. Traffic limit can be defined in units of KB (from 1 to 1024), MB (from 1 to 1024) or GB (from 1 to 1024).
SIM1/SIM2 data limit action	In case of reaching defined data traffic limit one of two possible actions will be performed: 1) Switch SIM – switches network connection from the SIM card on which data traffic limit has been reached to another SIM card, 2) Disconnect – disconnects network connection over the SIM card on which data traffic limit has been reached.

Current traffic	Displays amount of traffic that has been transferred over SIM card from the moment of enabling "SIM data limit" option. In order to refresh the displayed value in the "Current traffic" field please click on <i>Refresh</i> .
Reset current traffic value	Click on <i>Reset</i> resets a value of the current traffic to zero.
Reset current traffic value on specified day of the month	Every month, on the specified day, a value of the current traffic will be reset to zero. The day of reset is specified by ordinal number.
Connection type	Specifies the type of connection router will try to establish. There are three available options: only GSM, only UMTS and AUTO. For example, if you select Only GSM option, router will not try to connect to UMTS, instead router will automatically try to connect to GSM. By selecting AUTO option, router will first try to establish UMTS connection and if it fails, router will go for GSM connection.
Reload	Click <i>Reload</i> to discard any changes and reload previous settings.
Save	Click <i>Save</i> to save your changes back to the GWR Router.
Switch SIM	Click Switch SIM try to establish the connection using the other SIM card.
Refresh	Click <i>Refresh</i> to see updated mobile network status.
Connect/Disconnect	Click <i>Connect/Disconnect</i> to connect or disconnect from mobile network.

Table 5 - WAN parameters

Figure 177 shows screenshot of GSM/UMTS tab configuration menu. GSM/UMTS menu is divided into two parts.

- Upper part provides all parameters for configuration GSM/UMTS connection. These parameters can be obtained from Mobile Operator. Please use exact parameters given from Mobile Operator.
- Bottom part is used for monitoring status of GSM/UMTS connection (create/maintain/destroy GSM/UMTS connection). Status line show real-time status: connected/disconnected.

If your SIM Card credit is too low, the GWR Router will performed periodically connect/disconnect actions.

WAN Settings(advanced)	
Label	Description
Enable	This field specifies if Advanced WAN settings is enabled at the GWR Router.
Accept Local IP Address	With this option, pppd will accept the peer's idea of our local IP address, even if the local IP address was specified in an option.
Accept Remote IP Address	With this option, pppd will accept the peer's idea of its (remote) IP address, even if the remote IP address was specified in an option.
Idle time before disconnect (sec)	Specifies that pppd should disconnect if the link is idle for <i>n</i> seconds. The link is idle when no data packets are being sent or received.
Refuse PAP	With this option, pppd will not agree to authenticate itself to the peer using PAP.

<i>Require PAP</i>	Require the peer to authenticate using PAP (Password Authentication Protocol) authentication.
<i>Refuse CHAP</i>	With this option, pppd will not agree to authenticate itself to the peer using CHAP.
<i>Require CHAP</i>	Require the peer to authenticate using CHAP (Challenge Handshake Authentication Protocol) authentication.
<i>Max. CHAP challenge transmissions</i>	Set the maximum number of CHAP challenge transmissions to n (default 10).
<i>CHAP restart interval sec</i>	Set the CHAP restart interval (retransmission timeout for challenges) to n seconds (default 3).
<i>Refuse MS-CHAP</i>	With this option, pppd will not agree to authenticate itself to the peer using MS-CHAP.
<i>Refuse MS-CHAPv2</i>	With this option, pppd will not agree to authenticate itself to the peer using MS-CHAPv2.
<i>Refuse EAP</i>	With this option, pppd will not agree to authenticate itself to the peer using EAP.
<i>Connection debugging</i>	Enables connection debugging facilities. If this option is selected, pppd will log the contents of all control packets sent or received in a readable form.
<i>Maximum Transmit Unit (bytes)</i>	Set the MTU (Maximum Transmit Unit) value to n . Unless the peer requests a smaller value via MRU negotiation, pppd will request that the kernel networking code send data packets of no more than n bytes through the PPP network interface.
<i>Maximum Receive Unit (bytes)</i>	Set the MRU (Maximum Receive Unit) value to n . Pppd will ask the peer to send packets of no more than n bytes. The value of n must be between 128 and 16384; the default is 1500.
<i>VJ-Compression</i>	Disable Van Jacobson style TCP/IP header compression in both directions.
<i>VJ-Connection-ID Compression</i>	Disable the connection-ID compression option in Van Jacobson style TCP/IP header compression. With this option, pppd will not omit the connection-ID byte from Van Jacobson compressed TCP/IP headers.
<i>Protocol Field Compression</i>	Disable protocol field compression negotiation in both directions.
<i>Address/Control Compression</i>	Disable Address/Control compression in both directions.
<i>Predictor-1 Compression</i>	Disable or enable accept or agree to Predictor-1 compression.
<i>BSD Compression</i>	Disable or enable BSD-Compress compression.
<i>Deflate Compression</i>	Disable or enable Deflate compression.
<i>Compression Control Protocol negotiation</i>	Disable CCP (Compression Control Protocol) negotiation. This option should only be required if the peer is buggy and gets confused by requests from pppd for CCP negotiation.
<i>Magic Number negotiation</i>	Disable magic number negotiation. With this option, pppd cannot detect a looped-back line. This option should only be needed if the peer is buggy.
<i>Passive Mode</i>	Enables the "passive" option in the LCP. With this option, pppd will attempt to initiate a connection; if no reply is received from the peer, pppd will then just wait passively for a valid LCP packet from the peer, instead of exiting, as it would without this option.
<i>Silent Mode</i>	With this option, pppd will not transmit LCP packets to initiate a connection until a valid LCP packet is received from the peer (as for the "passive" option).

	with ancient versions of pppd).
Append domain name	Inserts the entered domain name to the local host name for authentication purposes.
Show PAP password in log	When logging the contents of PAP packets, this option causes pppd to show the password string in the log message.
Time to wait before re-initiating the link (sec)	Specifies how many seconds to wait before re-initiating the link after it terminates. The holdoff period is not applied if the link was terminated because it was idle.
LCP-Echo-Failure	If this option is given, pppd will presume the peer to be dead if <i>n</i> LCP echo-requests are sent without receiving a valid LCP echo-reply. If this happens, pppd will terminate the connection. This option can be used to enable pppd to terminate after the physical connection has been broken (e.g., the modem has hung up) in situations where no hardware modem control lines are available.
LCP-Echo-Interval	If this option is given, pppd will send an LCP echo-request frame to the peer every <i>n</i> seconds. Normally the peer should respond to the echo-request by sending an echo-reply. This option can be used with the <i>lcp-echo-failure</i> option to detect that the peer is no longer connected.
Use Peer DNS	With this option enabled, router resolves addresses using ISP's DNS servers.
Modem Initialization String	This field provides an option to directly specify AT commands.
Roaming Mode	By enabling this option router will be able to connect to roaming network.
Reset Location Information	By enabling this option router will erase LOCI Elementary File in SIM card. This will cause SIM card to scan all available networks when registering.

Table 6 - Advanced WAN Settings

Settings – Routing

The static routing function determines the path that data follows over your network before and after it passes through the GWR Router. You can use static routing to allow different IP domain users to access the Internet through the GWR Router. Static routing is a powerful feature that should be used by advanced users only. In many cases, it is better to use dynamic routing because it enables the GWR Router to automatically adjust to physical changes in the network’s layout.

The GWR Router is a fully functional router with static routing capability. *Figure 188* shows screenshot of Routing page.

Figure 18 – Routing configuration page

Use this menu to setup all routing parameters. Administrator can perform following operations:

- Create/Edit/Remove routes (including default route),
- Reroute GRE and IPSEC packet to dedicated destination at inside network,
- Port translation – Reroute TCP and UDP packets to desired destination inside the network.

Routing Settings	
Label	Description
<i>Routing Table</i>	
<i>Enable</i>	This check box allows you to activate/deactivate this static route.
<i>Dest Network</i>	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
<i>Netmask</i>	Subnet mask for allowed IP subnet.
<i>Gateway</i>	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.

Metric	Metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Interface	Interface represents the "exit" of transmission for routing purposes. In this case <i>Eth0</i> represents LAN interface and <i>ppp0</i> represents GSM/UMTS mobile interface of the GWR Router.
TCP/UDP Traffic forwarding	
Enable	This field specifies IP address of the VPN server on local area network. VPN tunnel ends at this VPN server. You must use VPN tunnel option when configuring VPN connection, because of NAT.
Protocol	This is the IP protocol type.
Source IP	This field specifies address from which portforwarding is allowed, all other traffic is denied.
Source Netmask	This field specifies netmask for allowed IP subnet.
Destination IP	This field specifies IP address of the incoming traffic.
Destination Netmask	This field specifies netmask for the previous address.
Destination Port	This is the TCP/UDP port of incoming traffic.
Forward to IP	This field specifies IP address where packets should be forwarded.
Forward to port	Specify TCP/UDP port on which the traffic is going to be forwarded.
Interface	Select interface where portforwarding is done. Portforwarding from outside (WAN) interface to inside (LAN) interface is done on PPP, and in reverse direction on Ethernet interface.
Add	Click Add to insert (add) new item in table to the GWR Router.
Remove	Click Remove to delete selected item from table.
Reload	Click Reload to discard any changes and reload previous settings.
Save	Click Save to save your changes back to the GWR Router. After pressing Save button it make take more than 10 seconds for router to save parameters and become operational again.

Table 7 - Routing parameters

Port translation

For incoming data, the GWR Router forwards IP traffic destined for a specific port, port range or GRE/IPsec protocol from the cellular interface to a private IP address on the Ethernet "side" of the GWR Router.

Settings – Dynamic Routing Protocol

Dynamic routing performs the same function as static routing except it is more robust. Static routing allows routing tables in specific routers to be set up in a static manner so network routes for packets are set. If a router on the route goes down the destination may become unreachable. Dynamic routing allows routing tables in routers to change as the possible routes change.

Routing Information Protocol (RIP)

The Routing Information Protocol (RIP) is a dynamic routing protocol used in local and wide area networks. As such it is classified as an interior gateway protocol (IGP) using the distance-vector routing algorithm. The Routing Information Protocol provides great network stability, guaranteeing that if one network connection goes down the network can quickly adapt to send packets through another connection.

Click **RIP** Tab, to open the Routing Information Protocol screen. Use this screen to configure the GWR Router RIP parameters (Figure 19).

The screenshot shows the configuration interface for the Routing Information Protocol (RIP). It is titled "Routing Information Protocol" and includes a "Help" icon. The interface is organized into three main sections:

- Routing Manager:** Contains fields for "Hostname" (Router), "Password" (zebra), "Enable log" (checkbox), and "Port to bind at" (radio buttons for "User defined" and "Default [2601]").
- RIPD:** Contains fields for "Hostname" (ripd), "Password" (zebra), and "Port to bind at" (radio buttons for "User defined" and "Default [2602]").
- Routing Information Protocol Status:** Shows the current status as "stopped" in red text, with "Start", "Stop", and "Restart" buttons below it.

At the bottom right of the configuration area, there are "Reload" and "Save" buttons.

Figure 19 – RIP configuration page

RIP Settings	
Label	Description
<i>Routing Manager</i>	
<i>Hostname</i>	Prompt name that will be displayed on telnet console.
<i>Password</i>	Login password.
<i>Port to bind at</i>	Local port the service will listen to.
<i>RIPD</i>	
<i>Hostname</i>	Prompt name that will be displayed on telnet console of the Routing Information Protocol Manager.
<i>Password</i>	Login password.
<i>Port to bind at</i>	Local port the service will listen to.
<i>Routing Information Protocol Status</i>	
<i>Start</i>	Start RIP.
<i>Stop</i>	Stop RIP.
<i>Restart</i>	Restart RIP.
<i>Save</i>	Click <i>Save</i> to save your changes back to the GWR Router.
<i>Reload</i>	Click <i>Reload</i> to discard any changes and reload previous settings.

Table 8 - RIP parameters

RIP routing engine for the GWR Router

Use telnet to enter in global configuration mode.

```
telnet 192.168.1.1 2602 // telnet to eth0 at TCP port 2602///
```

To enable RIP, use the following commands beginning in global configuration mode:

```
router# router rip
```

To associates a network with a RIP routing process, use following commands:

```
router# network [A.B.C.D/Mask]
```

By default, the GWR Router receives RIP version 1 and version 2 packets. You can configure the GWR Router to receive and send only version 1. Alternatively, you can configure the GWR Router to receive and send only version 2 packets. To configure GWR Router to send and receive packets from only one version, use the following command:

```
router# rip version [1|2] // Same as other router //
```

Disable route redistribution:

```
router# no redistribute kernel
router# no redistribute static
router# no redistribute connected
```

Disable RIP update (optional):

```
router# passive-interface eth0  
router# no passive-interface eth0
```

Routing protocols use several timer that determine such variables as the frequency of routing updates, the length of time before a route becomes invalid, an other parameters. You can adjust these timer to tune routing protocol performance to better suit your internetwork needs. Use following command to setup RIP timer:

```
router# timers basic [UPDATE-INTERVAL] [INVALID] [TIMEOUT] [GARBAGE-COLLECT]  
router# no timers basic
```

Configure interface for RIP protocol

```
router# interface greX  
router# ip rip send version [VERSION]  
router# ip rip receive version [VERSION]
```

Disable rip authentication at all interface.

```
Router(interface)# no ip rip authentication mode [md5|text]
```

Debug commands:

```
router# debug rip  
router# debug rip events  
router# debug rip packet  
router# terminal monitor
```

Settings – VPN Settings

Virtual private network (VPN) is a communications network tunneled through another network and dedicated to a specific network. One common application of VPN is secure communication through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features.

A VPN may have best-effort performance, or may have a defined Service Level Agreement (SLA) between the VPN customer and the VPN service provider. Generally, a VPN has a topology more complex than point-to-point. The distinguishing characteristics of VPNs are not security or performance, but that they overlay other network(s) to provide a certain functionality that is meaningful to a user community.

Generic Routing Encapsulation (GRE)

Originally developed by Cisco, generic routing encapsulation (GRE) is now a standard, defined in RFC 1701, RFC 1702, and RFC 2784. GRE is a tunneling protocol used to transport packets from one network through another network.

If this sounds like a virtual private network (VPN) to you, that’s because it theoretically is: Technically, a GRE tunnel is a type of a VPN – but it isn’t a secure tunneling method. However, you can encrypt GRE with an encryption protocol such as IPSec to form a secure VPN. In fact, the point-to-point tunneling protocol (PPTP) actually uses GRE to create VPN tunnels. For example, if you configure Microsoft VPN tunnels, by default, you use PPTP, which uses GRE.

Solution where you can use GRE protocol:

- You need to encrypt multicast traffic. GRE tunnels can carry multicast packets – just like real network interfaces – as opposed to using IPSec by itself, which can’t encrypt multicast traffic. Some examples of multicast traffic are OSPF, EIGRP. Also, a number of video, VoIP, and streaming music applications use multicast.
- You have a protocol that isn’t routable, such as NetBIOS or non-IP traffic over an IP network. You could use GRE to tunnel IPX/ AppleTalk through an IP network.
- You need to connect two similar networks connected by a different network with different IP addressing.

Click *VPN Settings* Tab, to open the VPN configuration screen. In the *Figure 2020* you can see screenshot of *GRE* Tab configuration menu.

VPN Settings / GRE Tunneling Parameters	
Label	Description
<i>Enable</i>	This check box allows you to activate/deactivate VPN/GRE traffic.
<i>Local Tunnel Address</i>	This field specifies IP address of virtual tunnel interface.
<i>Local Tunnel Netmask</i>	This field specifies the IP netmask address of virtual tunnel. This field is unchangeable, always 255.255.255.252
<i>Tunnel Source</i>	This field specifies IP address or hostname of tunnel source.
<i>Tunnel Destination</i>	This field specifies IP address or hostname of tunnel destination.
<i>Interface</i>	This field specifies GRE interface. This field gets from the GWR Router.
<i>KeepAlive Enable</i>	Check for keepalive enable.
<i>Period</i>	Defines the time interval (in seconds) between transmitted keepalive packets. Enter a number from 3 to 60 seconds.

Retries	Defines the number of times retry after failed keepalives before determining that the tunnel endpoint is down. Enter a number from 1 to 10 times.
Add	Click Add to insert (add) new item in table to the GWR Router.
Remove	Click Remove to delete selected item from table.
Reload	Click Reload to discard any changes and reload previous settings.
Save	Click Save to save your changes back to the GWR Router.

Table 9 – GRE parameters

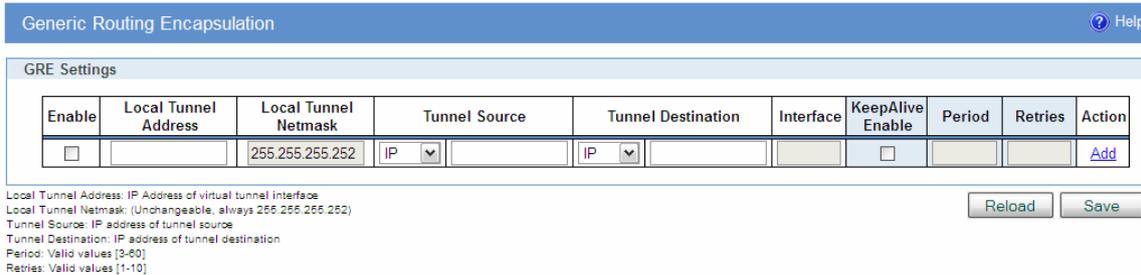


Figure 20 – GRE tunnel parameters configuration page

GRE Keepalive

GRE tunnels can use periodic status messages, known as keepalives, to verify the integrity of the tunnel from end to end. By default, GRE tunnel keepalives are disabled. Use the keepalive check box to enable this feature. Keepalives do not have to be configured on both ends of the tunnel in order to work; a tunnel is not aware of incoming keepalive packets. You should define the time interval (in seconds) between transmitted keepalive packets. Enter a number from 1 to 60 seconds, and the number of times to retry after failed keepalives before determining that the tunnel endpoint is down. Enter a number from 1 to 10 times.

Internet Protocol Security (IPSec)

Internet Protocol Security (IPSec) is a protocol suite for securing Internet Protocol communication by authenticating and encrypting each IP packet of a data stream.

Click *VPN Settings* Tab, to open the VPN configuration screen. At the Figure 21 *Figure 21 – IPSec Summary screen* you can see IPSec Summary screen. This screen gathers information about settings of all defined IPSec tunnels. Up to 5 IPSec tunnels can be defined on GWR router.

IPSec Summary and IPSec Settings are briefly displayed in following figures and tables.

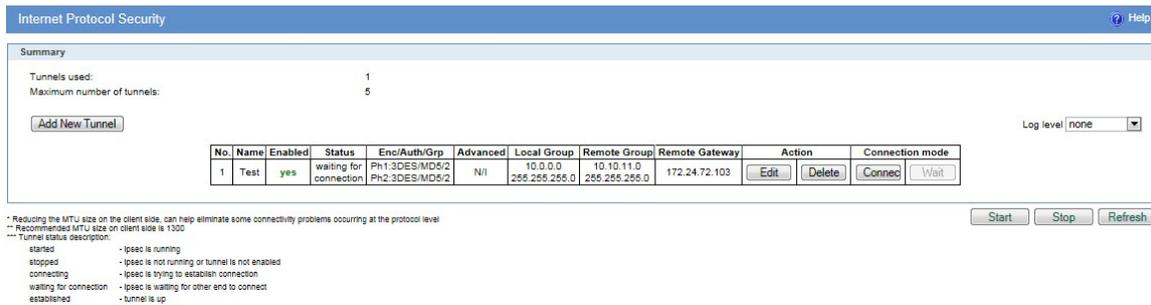


Figure 21 – IPSec Summary screen

VPN Settings / IPSec Summary	
Label	Description
<i>Tunnels Used</i>	This is the number of IPSec tunnels being defined.
<i>Tunnels Available</i>	This is the number of available, not yet defined, IPSec tunnels.
<i>No</i>	This field indicates the number of the IPSec tunnel.
<i>Name</i>	Field shows the Tunnel Name that you gave to the IPSec tunnel.
<i>Enabled</i>	This field shows if tunnel is enabled or disabled. After clicking on Start button, only enabled tunnels will be started
<i>Status</i>	Field indicates status of the IPSec tunnel. Click on <i>Refresh</i> button to see current status of defined IPSec tunnels.
<i>Enc/Auth/Grp</i>	This field shows both Phase 1 and Phase 2 details, Encryption method (DES/3DES/AES), Authentication method (MD5/SHA1), and DH Group number (1/2/5) that you have defined in the IPSec Setup section.
<i>Advanced Setup</i>	Field shows the chosen options from IPSec Advanced section by displaying the first letters of enabled options.
<i>Local Group</i>	Field shows the IP address and subnet mask of the Local Group.
<i>Remote Group</i>	Field displays the IP address and subnet mask of the Remote Group.
<i>Remote Gateway</i>	Field shows the IP address of the Remote Device.
<i>Connection mode</i>	Field displays connection mode of the current tunnel. <i>Connect</i> - IPSec tunnel initiating side in negotiation process. <i>Wait</i> - IPSec tunnel responding side in negotiation process.
<i>Log level</i>	Set IPSec log level.
<i>Delete</i>	Click on this link to delete the tunnel and all settings for that particular tunnel.
<i>Edit</i>	This link opens screen where you can change the tunnel's settings.

Add New Tunnel	Click on this button to add a new Device-to-Device IPSec tunnel. After you have added the tunnel, you will see it listed in the Summary table.
Start	This button starts the IPSec negotiations between all defined and enabled tunnels. If the IPSec is already started, Start button is replaced with Restart button.
Stop	This button will stop all IPSec started negotiations.
Refresh	Click on this button to refresh the Status field in the Summary table.

Table 10 - IPSec Summary for first firmware version

To create a tunnel click Add New Tunnel button. Depending on your selection, the Local Group Setup and Remote Group Setup settings will differ. Proceed to the appropriate instructions for your selection.

Device 2 Device Tunnel
Help

Add New Tunnel

Tunnel Number

Tunnel Name

Enable

Local Group Setup

Local Security Gateway Type

Local ID Type

IP Address From

Local Security Group Type

IP Address

Subnet Mask

Remote Group Setup

Remote Security Gateway Type

IP Address

Remote ID Type

Remote Security Group Type

IP Address

Subnet Mask

IPSec Setup

Key Exchange Mode: IKE with Preshared key ▾

Mode: main ▾

Phase 1 DH Group: Group2 (1024) ▾

Phase 1 Encryption: 3DES ▾

Phase 1 Authentication: MD5 ▾

Phase 1 SA Life Time: 28800 sec

Perfect Forward Secrecy:

Phase 2 Encryption: 3DES ▾

Phase 2 Authentication: MD5 ▾

Phase 2 SA Life Time: 3600 sec

Preshared Key: 0123456789

Failover

Enable IKE Failover

IKE SA Retry:

Restart PPP After IKE SA Retry Exceeds Specified Limit

Enable Tunnel Failover

Ping IP Or Hostname:

Ping Interval: sec

Packet Size:

Advanced Ping Interval: sec

Advanced Ping Wait For A Response: sec

Maximum Number Of Failed Packets: %

Advanced

Compress (Support IP Payload Compression Protocol (IPComp))

Dead Peer Detection (DPD) 20 sec

NAT Traversal

Send Initial Contact

Copyright © 2008 - 2014 Geneko. All rights reserved.
<http://www.geneko.rs>

Figure 22 – IPSec Settings

VPN Settings / IPSec Settings	
Label	Description
Tunnel Number	This number will be generated automatically and it represents the tunnel number.
Tunnel Name	Enter a name for the IPSec tunnel. This allows you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel.
Enable	Check this box to enable the IPSec tunnel.
Local Security Gateway Type	Select the type you want to use: IP Only - Only a specific IP address will be able to establish a tunnel. NOTE: The Local Security Gateway Type you select should match the Remote Security Gateway Type selected on the IPSec device at the other end of the tunnel
IP Address	The WAN (or Internet) IP address of the GWR Router automatically appears. If the GWR Router is not yet connected to the GSM/UMTS network this field is without IP address.

<i>Custom peer ID</i>	Authentication identity for one of the participant. Can be an IP address or a fully-qualified domain name preceded by @.
<i>Local Security Group Type</i>	Select the local LAN user(s) behind the GWR Router that can use this IPSec tunnel. Select the type you want to use: IP or Subnet. NOTE: The Local Security Group Type you select should match the Remote Security Group Type selected on the IPSec device at the other end of the tunnel.
<i>IP Address</i>	Only the computer with a specific IP address will be able to access the tunnel.
<i>Subnet Mask</i>	Enter the subnet mask.
<i>Remote Security Gateway Type</i>	Select the remote LAN user(s) behind the GWR Router at the other end that can use this IPSec tunnel. Select the type you want to use: IP or Subnet. NOTE: The Remote Security Group Type you select should match the Local Security Group Type selected on the IPSec device at the other end of the tunnel.
<i>IP Address</i>	Only the computers with a specific IP addressess will be able to access the tunnel. IP addressess should be separated by comma.
<i>Remote Security Group Type</i>	Select the remote LAN user(s) behind the GWR Router at the other end that can use this IPSec tunnel. Select the type you want to use: IP or Subnet. NOTE: The Remote Security Group Type you select, should match the Local Security Group Type selected on the IPSec device at the other end of the tunnel.
<i>IP Address</i>	Only the computer with a specific IP address will be able to access the tunnel.
<i>Subnet Mask</i>	Enter the subnet mask.
<i>IPSec Setup</i>	In order to establish an encrypted tunnel, the two ends of an IPSec tunnel must agree on the methods of encryption, decryption and authentication. This is done by sharing a key to the encryption code. For key management, the GWR Router uses only IKE with Preshared Key mode.
<i>Key Exchange Mode</i>	IKE with Preshared Key IKE is an Internet Key Exchange protocol used to negotiate key material for Security Association (SA). IKE uses the Preshared Key to authenticate the remote IKE peer. Both ends of IPSec tunnel must use the same mode of key management.
<i>Phase 1 DH Group</i>	Phase 1 is used to create the SA. DH (Diffie-Hellman) is a key exchange protocol used during Phase 1 of the authentication process to establish pre-shared keys. There are three groups of different prime key lengths. Group 1 is 768 bits, Group 2 is 1024 bits, Group 5 is 1536 bits and Group 14 is 2048 bits long. If network speed is preferred, select Group 1. If network security is preferred, select Group 5.
<i>Phase 1 Encryption</i>	Select a method of encryption: 3DES, AES-128 (128-bit), AES-192 (192-bit), AES-256 (256-bit), BLOWFISH-128 (128-bit), BLOWFISH-192 (192-bit), BLOWFISH-256 (256-bit), SERPENT-128 (128-bit), SERPENT-192 (192-bit), SERPENT-256 (256-bit), TWOFISH-128 (128-bit), TWOFISH-256 (256-bit). The method determines the length of the key used to encrypt or decrypt ESP packets. AES-128 is recommended because it is the most secure. Make sure both ends of the IPSec tunnel use the same encryption method.
<i>Phase 1 Authentication</i>	Select a method of authentication: MD5 or SHA1. The authentication method determines how the ESP packets are validated. MD5 is a one-way hashing algorithm that produces a 128-bit digest. SHA1 is a one-way hashing algorithm that produces a 160-bit digest. SHA1 is recommended because it is more secure. Make sure both ends of the IPSec tunnel use the same authentication method.
<i>Phase 1 SA Life Time</i>	Configure the length of time IPSec tunnel is active in Phase 1. The default value is 28800 seconds. Both ends of the IPSec tunnel must use the same Phase 1 SA Life Time setting.
<i>Perfect Forward</i>	If the Perfect Forward Secrecy (PFS) feature is enabled, IKE Phase 2 negotiation

<i>Secrecy</i>	will generate new key material for IP traffic encryption and authentication, so hackers using brute force to break encryption keys will not be able to obtain future IPSec keys. Both ends of the IPSec tunnel must enable this option in order to use the function.
<i>Phase 2 DH Group</i>	If the Perfect Forward Secrecy feature is disabled, then no new keys will be generated, so you do not need to set the Phase 2 DH Group. There are three groups of different prime key lengths. Group 1 is 768 bits, Group 2 is 1024 bits, Group 5 is 1536 bits and Group 14 is 2048 bits long. If network speed is preferred, select Group 1. If network security is preferred, select Group 5. You do not have to use the same DH Group that you used for Phase 1, but both ends of the IPSec tunnel must use the same Phase 2 DH Group.
<i>Phase 2 Encryption</i>	Phase 2 is used to create one or more IPSec SAs, which are then used to key IPSec sessions. Select a method of encryption: NULL, 3DES, AES-128 (128-bit), AES-192 (192-bit), AES-256 (256-bit), BLOWFISH-128 (128-bit), BLOWFISH-192 (192-bit), BLOWFISH-256 (256-bit), SERPENT-128 (128-bit), SERPENT-192 (192-bit), SERPENT-256 (256-bit), TWOFISH-128 (128-bit), TWOFISH-256 (256-bit). It determines the length of the key used to encrypt or decrypt ESP packets. AES-128 is recommended because it is the most secure. Both ends of the IPSec tunnel must use the same Phase 2 Encryption setting. NOTE: If you select a NULL method of encryption, the next Phase 2 Authentication method cannot be NULL and vice versa.
<i>Phase 2 Authentication</i>	Select a method of authentication: NULL, MD5 or SHA1. The authentication method determines how the ESP packets are validated. MD5 is a one-way hashing algorithm that produces a 128-bit digest. SHA1 is a one-way hashing algorithm that produces a 160-bit digest. SHA1 is recommended because it is more secure. Both ends of the IPSec tunnel must use the same Phase 2 Authentication setting. NOTE: If you select a NULL method of authentication, the previous Phase 2 Encryption method cannot be NULL.
<i>Phase 2 SA Life Time</i>	Configure the length of time an IPSec tunnel is active in Phase 2. The default is 3600 seconds. Both ends of the IPSec tunnel must use the same Phase 2 SA Life Time setting.
<i>Preshared Key</i>	This specifies the pre-shared key used to authenticate the remote IKE peer. Enter a key of keyboard and hexadecimal characters, e.g., Ay_%4222 or 345fa929b8c3e. This field allows a maximum of 1023 characters and/or hexadecimal values. Both ends of the IPSec tunnel must use the same Preshared Key. NOTE: It is strongly recommended that you periodically change the Preshared Key to maximize security of the IPSec tunnels.
<i>Enable IKE failover</i>	Enable IKE failover option which will try periodically to reestablish security association.
<i>IKE SA retry</i>	Number of IKE retries, before failover.
<i>Enable tunnel failover</i>	Enable tunnel failover. If there is more than one tunnel defined, this option will failover to other tunnel in case that selected one fails to established connection.
<i>Ping IP</i>	IP address on other side of tunnel which will be pinged in order to determine current state.
<i>Ping interval</i>	Specify time period in seconds between two ping.
<i>Maximum numbers of failed packets</i>	Set percentage of failed packets until failover action is performed.

<i>Compress (IP Payload Compression Protocol (IP Comp))</i>	IP Payload Compression is a protocol that reduces the size of IP datagram. Select this option if you want the Router to propose compression when it initiates a connection.
<i>Dead Peer Detection (DPD)</i>	When DPD is enabled, the GWR Router will send periodic HELLO/ACK messages to check the status of the IPSec tunnel (this feature can be used only when both peers or IPSec devices of the IPSec tunnel use the DPD mechanism). Once a dead peer has been detected, the GWR Router will disconnect the tunnel so the connection can be re-established. Specify the interval between HELLO/ACK messages (how often you want the messages to be sent). The default interval is 20 seconds.
<i>NAT Traversal</i>	Both the IPSec initiator and responder must support the mechanism for detecting the NAT router in the path and changing to a new port, as defined in RFC 3947. NOTE: If you select this mode the Aggressive mode will be automatically selected because it is obligatory option for NAT-T to work properly. NOTE: Keep-alive for NAT-T function is enabled by default and cannot be disabled. The default interval for keep-alive packets is 20 seconds.
<i>Send initial contact</i>	The initial-contact status message may be used when one side wishes to inform the other that this is the first SA being established with the remote system. The receiver of this Notification Message might then elect to delete any existing SA's
<i>Back</i>	Click <i>Back</i> to return on IPSec Summary screen.
<i>Reload</i>	Click <i>Reload</i> to discard any changes and reload previous settings.
<i>Save</i>	Click <i>Save</i> to save your changes back to the GWR Router. After that router automatically goes back and begin negotiations of the tunnels by clicking on the <i>Start</i> .

Table 11 - IPSec Parameters for first firmware version

OpenVPN

OpenVPN site to site allows connecting two remote networks via point-to-point encrypted tunnel. OpenVPN implementation offers a cost-effective simply configurable alternative to other VPN technologies. OpenVPN allows peers to authenticate each other using a pre-shared secret key, certificates, or username/password. When used in a multiclient-server configuration, it allows the server to release an authentication certificate for every client, using signature and Certificate authority. It uses the OpenSSL encryption library extensively, as well as the SSLv3/TLSv1 protocol, and contains many security and control features. The server and client have almost the same configuration. The difference in the client configuration is the remote endpoint IP or hostname field. Also the client can set up the keepalive settings. For successful tunnel creation a static key must be generated on one side and the same key must be uploaded on the opposite side.

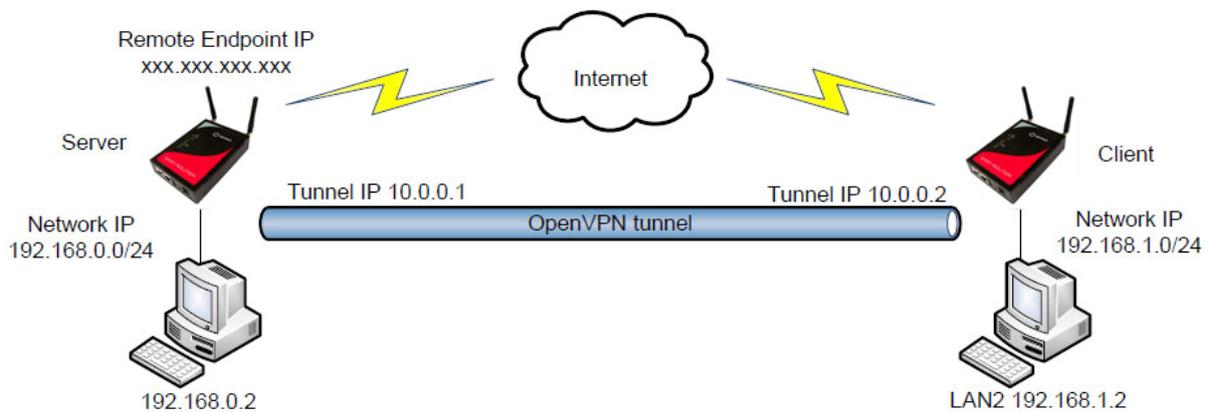


Figure 23 - OpenVPN example

Click **VPN Settings -OpenVPN**, to open the VPN configuration screen. At the Figure 24 you can see OpenVPN Summary. This screen gathers information about settings of all defined OpenVPN tunnels. Up to 3 OpenVPN tunnels can be defined on GWG Gateway.

OpenVPN Summary and OpenVPN Settings are briefly displayed in following figures and tables.

OpenVPN
Help

Summary

Tunnels used: 1

Maximum number of tunnels: 3

[Add New Tunnel](#)

No.	Name	Enabled	Status	Auth. Mode	Advanced	Remote Address	Statistics	Action	
1	geneko	yes	ready	none	NAT	172.27.234.24	Show	Edit	Delete

* Tunnel status description:
 started - openVPN is running
 stopped - openVPN is not running
 connecting - check chosen protocol on both side
 waiting - openVPN is trying to establish connection
 ready - tunnel interface is ready and up
 disabled - tunnel is not enabled

Start Stop Refresh

Figure 24-Open VPN Summary screen

OpenVPN	
Label	Description
<i>Tunnel Used</i>	This number will be generated automatically and it represents a number of configured tunnels.
<i>Maximum number of tunnels</i>	This is the maximum number of allowed OpenVPN tunnels
<i>No.</i>	This field indicates the number of the OpenVPN tunnel
<i>Name</i>	This field shows the Tunnel Name that you gave to the OpenVPN tunnel.
<i>Enabled</i>	This field shows if tunnel is enabled or disabled. After clicking on Start button, only enabled tunnels will be started.
<i>Status</i>	This field indicates status of the OpenVPN tunnel. Click on Refresh button to see current status of defined OpenVPN tunnels.
<i>Auth Mode</i>	This field shows authentication mode being used.
<i>Advanced</i>	This field shows the additional chosen options for OpenVPN tunnel.
<i>Remote Address</i>	This field displays the IP address of remote peer. If tunnel is in wait or client state, X letter will appear.
<i>Show</i>	This button opens a detailed statistics window for the tunnel.
<i>Delete</i>	Click on this link to delete the tunnel and all settings for that particular tunnel.
<i>Edit</i>	This link opens screen where you can change the tunnel's settings.
<i>Add New Tunnel</i>	Click on this button to add a new OpenVPN tunnel. After you have added the tunnel, you will see it listed in the Summary table.
<i>Start</i>	This button starts the OpenVPN negotiations between all defined and enabled tunnels. If the OpenVPN is already started, Start button is replaced with Restart button.
<i>Stop</i>	This button will stop all OpenVPN started negotiations.
<i>Refresh</i>	Click on this button to refresh the Status field in the Summary table.
OpenVPN Settings	
<i>Tunnel Number</i>	This number will be generated automatically and it represents a number of the tunnel.
<i>Tunnel Name</i>	Enter a name for the OpenVPN tunnel. This allows you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel.
<i>Enable</i>	Check this box to enable this particular OpenVPN tunnel.
<i>Interface Type</i>	Select TUN or TAP mode.
<i>Authenticate Mode</i>	Select a method of authentication, options are: NONE, Pre-Shared secret (PSK), Username/Password, X.509 client/server mode. The authentication method determines how the peers are authenticated to each other and to exchange cipher and HMAC keys to protect the data channel. Use NONE if you do not want authentication at all. Pre-Shared secret is a simple and easy way to authenticate your hosts. Username/Password can be used only in client mode where your server needs

	this kind of authentication. X.509 mode is full Transport Layer Security protocol with use of certificate/key pairs. Note that the designation of X.509 client or X.509 server is only for the purpose of negotiating the TLS control channel. Make sure both ends of the OpenVPN tunnel use the same authentication method. Certificate and key files must first be uploaded through web pages listed in the main menu under file management.
<i>Encryption Cipher</i>	Encrypt packets with cipher algorithm. The default is AES-128-CBC, an abbreviation for AES in Cipher Block Chaining mode. On the other hand, Blowfish has the advantages of being fast, very secure, and allowing key sizes of up to 448 bits. Blowfish is designed to be used in situations where keys are changed infrequently. OpenVPN supports the CBC cipher mode.
<i>Hash Algorithm</i>	Authenticate packets with HMAC using message digest algorithm. The default is SHA1. HMAC is a commonly used message authentication algorithm (MAC) that uses a data string, a secure hash algorithm and a key, to produce a digital signature. OpenVPN's usage of HMAC is to first encrypt a packet, then HMAC the resulting ciphertext. In TLS mode, the HMAC key is dynamically generated and shared between peers via the TLS control channel. If OpenVPN receives a packet with a bad HMAC it will drop the packet. HMAC usually adds 16 or 20 bytes per packet. Set none to disable authentication.
<i>Protocol</i>	Select a protocol you want to use for tunnel connection. UDP connect and TCP client will need the "Remote Host or IP Address" field in order to successfully establish a tunnel.
<i>UDP Port/TCP Port</i>	Enter a port number for a tunnel connection.
<i>LZO Compression</i>	Use fast LZO compression. This may add up to 1 byte per packet for incompressible data.
<i>NAT Rules</i>	NAT Rules is enabled by default.
<i>Keep Alive</i>	Use this mechanism to keep tunnel alive.
<i>Ping Interval</i>	Ping interval for sending pings over the TCP/UDP control channels. Number of seconds is specified in this field.
<i>Ping Timeout</i>	Defines a timeout interval in seconds after which a restart of OpenVPN tunnel will be triggered. This value must be twice as "Ping Interval" value.
<i>Max Fragment Size</i>	Enable internal datagram fragmentation so that no UDP datagrams are sent which are larger than max bytes. This option is available only when UDP protocol is being used. There are circumstances where using OpenVPN's internal fragmentation capability may be your only option, such as tunneling a UDP multicast stream which requires fragmentation.
<i>Pre-shared Secret</i>	Use Static Key encryption mode (non-TLS).
<i>Generate PSK</i>	Check this option and use "Generate" button to produce a pre-shared secret.
<i>Paste</i>	Use this option to manually paste a pre-shared secret from remote host's PSK file.
<i>CA Certificate</i>	Certificate authority (CA) file, also referred to as the root certificate.
<i>DH Group</i>	Choose a Diffie Hellman parameter group. This parameters may be considered public. Available only in X.509 server mode.
<i>Username</i>	Enter a username for authentication to the remote host server.
<i>Password</i>	Enter a password for authentication to the remote host server.
<i>Local Certificate</i>	Local peer's signed certificate, must be signed by a certificate authority whose

	certificate is in "CA Certificate" field.
Local Private Key	Local peer's private key.
Local/Remote Group Settings	
Remote Host or IP Address	Enter a remote peer IP address or host name. This field is available only in UDP connect and TCP client model.
Redirect Gateway	Check this option in order to use tunnel interface for default route.
Tunnel Interface Configuration	"Pull from server" mode is used when remote peer is an OpenVPN server and from where configuration will be pulled. In "Manual configuration" mode, you can enter tunnel interface IP addresses.
Local Interface IP Address	This is the IP address of the local VPN endpoint of local tunnel interface.
Remote Interface IP Address	This is the IP address of the remote VPN endpoint of remote tunnel interface.
Network Topology	Configure virtual addressing topology. net30 - use a point-to-point topology, by allocating one /30 subnet per client. p2p - use a point-to-point topology where the remote endpoint of the client's tunnel interface always points to the local endpoint of the server's tunnel interface. This mode allocates a single IP address per connecting client. Only use when none of the connecting clients are Windows systems. subnet - use a subnet rather than a point-to-point topology by configuring the tunnel interface with a local IP address and subnet mask. This mode allocates a single IP address per connecting client and works on Windows as well.

Table 12 - OpenVPN parameters

Figure 25 - OpenVPN configuration page

Settings – Firewall – IP Filtering

TCP/IP traffic flow is controlled over IP address and port number through router’s interfaces in both directions. With firewall options it is possible to create rule which exactly matches traffic of interest. Traffic can be blocked or forward depending on action selected. It is important when working with firewall rules to have in mind that traffic for router management should always be allowed to avoid problem with unreachable router. Firewall rules are checked by priority from the first to the last. Rules which are after matching rule are skipped.

The screenshot shows the 'Firewall' configuration page. At the top, there is a 'Firewall General Settings' section with an 'Enable' checkbox. Below it is the 'Firewall Rules' section, which contains a table of 17 rules. Each rule has a priority, a name, and various configuration parameters. At the bottom of the rules table, there is a 'Caution' note and an 'Apply Rules' button.

Priority	Name	Enabled	Chain	Service	Protocol	Port(s)	Input interface	Output interface	Source address	Destination address	Packet state	Policy	DoS	Action
1	Allow ALL from local LAN	no	INPUT	All	All	All/UnDef	br0	none	any	any	NEW	ACCEPT	no	Edit Delete
2	Allow already established traffic	no	INPUT	All	All	All/UnDef	any	none	any	any	ESTABLISHED,RELATED	ACCEPT	no	Edit Delete
3	Allow TELNET on ppp_0	no	INPUT	TELNET	TCP	23	ppp_0	none	any	any	NEW	ACCEPT	no	Edit Delete
4	Allow HTTP on ppp_0	no	INPUT	HTTP	TCP	80	ppp_0	none	any	any	NEW	ACCEPT	no	Edit Delete
5	Allow PING on ppp_0 - with DoS filter	no	INPUT	Custom	ICMP	All/UnDef	ppp_0	none	any	any	NEW	ACCEPT	yes	Edit Delete
6	Allow RIP on ppp_0	no	INPUT	Custom	TCP	2601,2602	ppp_0	none	any	any	NEW	ACCEPT	no	Edit Delete
7	Allow RIP on ppp_0 - route	no	INPUT	Custom	UDP	520	ppp_0	none	any	any	NEW	ACCEPT	no	Edit Delete
8	Allow GRE tunnels on ppp_0	no	INPUT	Custom	Custom	All/UnDef	ppp_0	none	any	any	NEW	ACCEPT	no	Edit Delete
9	Allow GRE Keepalive on ppp_0	no	INPUT	Custom	UDP	25162	ppp_0	none	any	any	NEW	ACCEPT	no	Edit Delete
10	Allow IPsec tunnels on ppp_0 - protocol	no	INPUT	Custom	ESP	All/UnDef	ppp_0	none	any	any	NEW	ACCEPT	no	Edit Delete
11	Allow IPsec tunnels on ppp_0 - IKE	no	INPUT	Custom	UDP	500	ppp_0	none	any	any	NEW	ACCEPT	no	Edit Delete
12	Allow IPsec tunnels on ppp_0 - IKE_NAT1	no	INPUT	Custom	UDP	4500	ppp_0	none	any	any	NEW	ACCEPT	no	Edit Delete
13	Allow OpenVPN tunnels on ppp_0 - UDP	no	INPUT	Custom	UDP	1194	ppp_0	none	any	any	NEW	ACCEPT	no	Edit Delete
14	Allow OpenVPN tunnels on ppp_0 - TCP	no	INPUT	Custom	TCP	1194	ppp_0	none	any	any	NEW	ACCEPT	no	Edit Delete
15	Allow SNMP on ppp_0	no	INPUT	Custom	UDP	161	ppp_0	none	any	any	NEW	ACCEPT	no	Edit Delete
16	Allow MOCBUS on ppp_0	no	INPUT	Custom	UDP	502	ppp_0	none	any	any	NEW	ACCEPT	no	Edit Delete
17	REJECT all other traffic	no	INPUT	All	All	All/UnDef	any	none	any	any	NEW	REJECT	no	Edit Delete

Figure 26– Firewall configuration page

Firewall	
Label	Description
<i>Firewall Rule Basic</i>	
Enable Firewall	This field specifies if Firewall is enabled at the router.
<i>Firewall Rule Settings</i>	
Priority	This field indicates the order in which the rule will be processed.
Name	Field shows the Rule Name that you gave to the firewall rule.
Enabled	This field shows if rule is enabled or disabled. After clicking on Apply rule button, only enabled rules will be applied.
Chain	Field displays chosen chain of the firewall rule.
Service	This field displays a service which is based on a predefined service protocol and service port. Also it can specifies a custom defined values.
Protocol	The protocol of the rule or of the packet to check. The specified protocol can be one of All, TCP, UDP, UDPLITE, ICMP, ESP, AH, SCTP or it can be a numeric value (from 0 to 255), representing one of these protocols or a different one. The

	number zero is equivalent to all. Protocol all will match with all protocols and is taken as default when this option is omitted.
<i>Port(s)</i>	This field specifies a service port with predefined or custom defined values.
<i>Input Interface</i>	Select the name of an interface via which a packet was received (only for packets entering the INPUT and FORWARD chains).
<i>Output Interface</i>	Select the name of an interface via which a packet is going to be sent (for packets entering the FORWARD and OUTPUT chains).
<i>Source address</i>	Field shows source IP address of the packet. It can be single IP address, range of IP addresses or "any".
<i>Destination address</i>	Destination IP address for the packet. It can be single IP address, range of IP addresses or "any".
<i>Packet state</i>	This option, when combined with connection tracking, allows access to the connection tracking state for this packet. Possible states are INVALID meaning that the packet could not be identified for some reason which includes running out of memory and ICMP errors which don't correspond to any known connection, ESTABLISHED meaning that the packet is associated with a connection which has seen packets in both directions, NEW meaning that the packet has started a new connection or otherwise associated with a connection which has not seen packets in both directions, and RELATED meaning that the packet is starting a new connection, but is associated with an existing connection, such as an FTP data transfer or an ICMP error.
<i>Policy</i>	Field shows selected firewall policy: ACCEPT, REJECT or DROP. If selected policy is REJECT field displays chosen reject type of the firewall rule.
<i>DDos</i>	This field shows if Distributed Denial of Service is disabled or enabled.
<i>Edit</i>	This link opens screen where you can change the rule's settings.
<i>Delete</i>	Click on this link to delete the rule and all settings for that particular rule.
<i>Add New Rule</i>	Click Add New Rule to add a new firewall rule. After you have added the rule, you will see it listed in the Summary table.
<i>Apply rules</i>	Click Add New Rule to add a new firewall rule. After you have added the rule, you will see it listed in the Summary table.

Table 13 - Firewall parameters

Settings – Firewall – MAC Filtering

MAC filtering can be used to restrict which Ethernet devices can send packets to the router. If MAC filtering is enabled, only Ethernet packets with a source MAC address that is configured in the MAC Filter table will be allowed. If the source MAC address is not in the MAC Filter table, the packet will be dropped.

MAC Filtering Settings	
Label	Description
<i>Enable MAC Filtering</i>	This field specifies if MAC Filtering is enabled at the router
<i>Enable</i>	Enable MAC filtering for a specific MAC address
<i>Name</i>	Field shows the Rule Name that is given to the MAC filtering rule.
<i>MAC address</i>	The Ethernet MAC source address to allow.

Reload	Click Reload to discard any changes and reload previous settings
Save	Click Save to save changes back to the GWR router

Table 14 - MAC filtering parameters

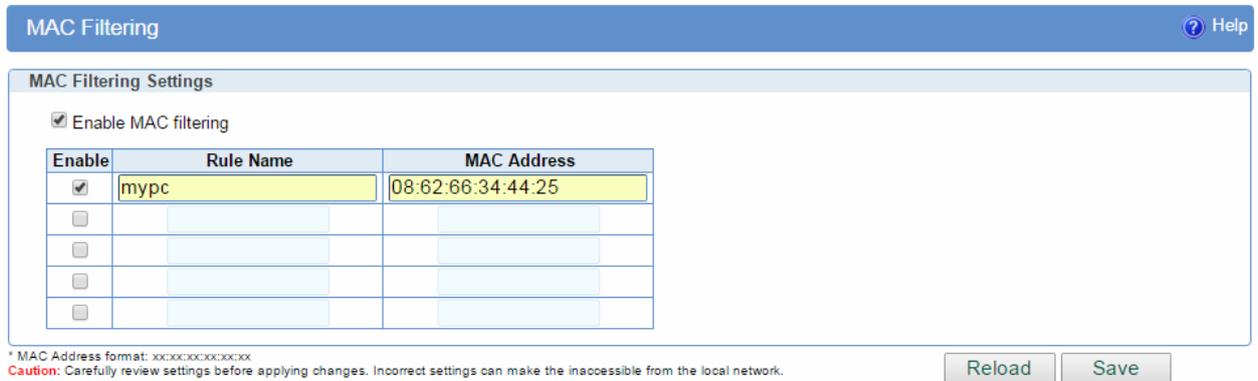


Figure 27- MAC filtering configuration page

Settings – DynDNS

Dynamic DNS is a domain name service allowing to link dynamic IP addresses to static hostname. To start using this feature firstly you should register to DDNS service provider. Section of the web interface where you can setup DynDNS parameters is shown in *Figure 288*.

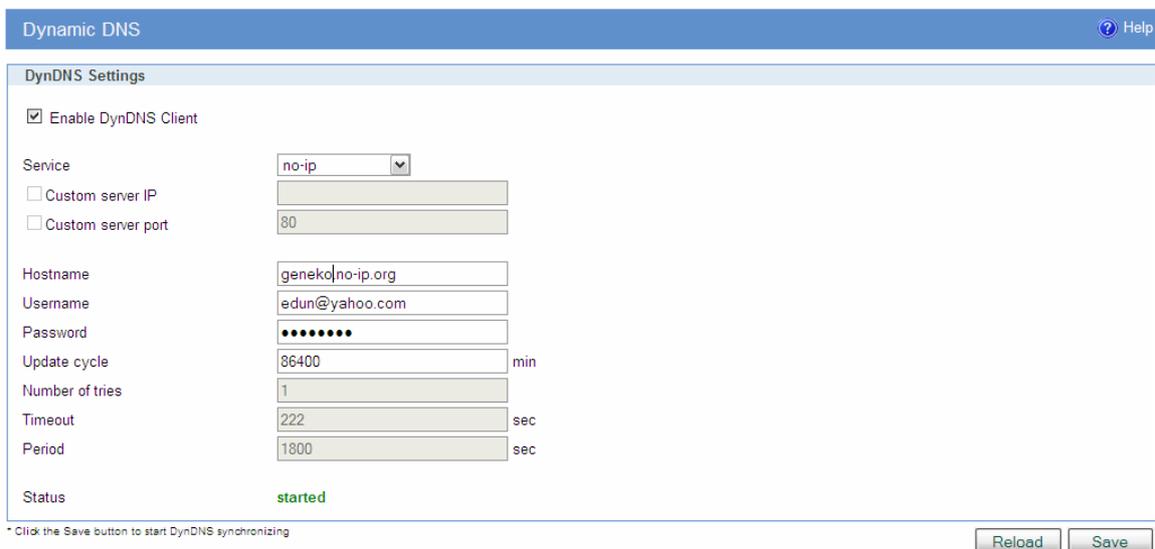


Figure 28 – DynDNS settings

DynDNS	
Label	Description
<i>Enable DynDNS Client</i>	Enable DynDNS Client.
<i>Service</i>	The type of service that you are using, try one of: no-ip, dhs, pggow, dyndns, dyndns-static, dyndns-custom, ods, easydns, dyns, justlinux and zoneedit.
<i>Custom Server IP</i>	The server IP to connect to.
<i>Custom Server port</i>	The server port to connect to.
<i>Hostname</i>	String to send as host parameter.
<i>Username</i>	User ID.
<i>Password</i>	User password.
<i>Update cycle</i>	Defines interval between updates of the DynDNS client. Default and minimum value for all DynDNS services, except No-IP service, is 86400 seconds. Update cycle value for No-IP service is represented in minutes and minimum is 1 minute.
<i>Number of tries</i>	Number of tries (default: 1) if network problem.
<i>Timeout</i>	The amount of time to wait on I/O (network problem).
<i>Period</i>	Time between update retry attempts, default value is 1800.
<i>Reload</i>	Click Reload to discard any changes and reload previous settings.
<i>Save</i>	Click Save to save your changes back to the GWR Router.

Table 15 - DynDNS parameters

Settings – Serial Port

Using the router’s serial port it is possible to perform serial-to-ethernet conversion (Serial port over TCP/UDP) and ModbusRTU-to-TCP conversion (Modbus gateway). Initial Serial Port Settings page is shown in figure bellow. By default above described features are disabled. Selecting one of two possible applications of Serial port opens up additional options available for configuration.

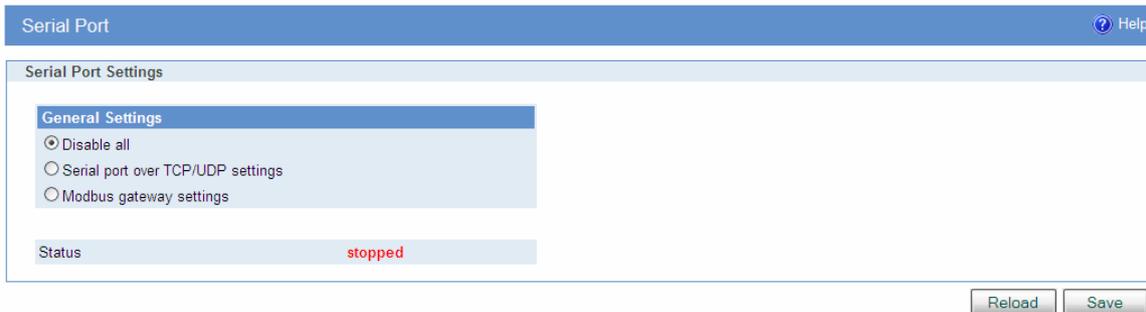


Figure 29 – Serial Port Settings initial menu

Serial port over TCP/UDP settings

The GWR Router provides a way for a user to connect from a network connection to a serial port. It provides all the serial port setup, a configuration file to configure the ports, a control login for modifying port parameters, monitoring ports, and controlling ports. The GWR Router supports RFC 2217 (remote control of serial port parameters).

Serial Port over TCP/UDP Settings	
Label	Description
<i>Bits per second</i>	The unit and attached serial device, such as a modem, must agree on a speed or baud rate to use for the serial connection. Valid baud rates are 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600 or 115200.
<i>Data bits</i>	Indicates the number of bits in a transmitted data package.
<i>Parity</i>	Checks for the parity bit. None is the default.
<i>Stop bits</i>	The stop bit follows the data and parity bits in serial communication. It indicates the end of transmission. The default is 1.
<i>Flow control</i>	Flow control manages data flow between devices in a network to ensure it is processed efficiently. Too much data arriving before a device is prepared to manage it causes lost or retransmitted data. None is the default.
<i>Protocol</i>	Choose which protocol to use [TCP/UDP].
<i>Mode</i>	Select server mode in order to listen for incoming connection, or client mode to establish one.
<i>Bind to TCP/UDP port</i>	Number of the TCP/UDP port to accept connections for this device. (Only on server side)

<i>Type of socket</i>	Either <i>raw</i> or <i>telnet</i> . Raw enables the port and transfers all data like between the port and the log. Telnet enables the port and runs the telnet protocol on the port to set up telnet parameters.
<i>Enable local echo</i>	Enable the local echo feature.
<i>Enable timeout</i>	Close connection after period of inactivity.
<i>Check TCP connection</i>	Enable connection checking.
<i>Keepalive idle time</i>	Set keepalive idle time in seconds.
<i>Keepalive interval</i>	Set time period between checking.
<i>Log level</i>	Set importance level of log messages.
<i>Reload</i>	Click <i>Reload</i> to discard any changes and reload previous settings.
<i>Save</i>	Click <i>Save</i> button to save your changes back to the GWR Router and activate/deactivate serial to Ethernet converter.

Table 16 – Serial Port over TCP/UDP parameters

Click *Serial Port* Tab to open the Serial Port Configuration screen. Use this screen to configure the GWR Router serial port parameters (*Figure 3030*).

Serial Port[? Help](#)

Serial Port Settings

General Settings

Disable all
 Serial port over TCP/UDP settings
 Modbus gateway settings

Serial Port Settings

Bits per second 57600 ▼
Data bits 8 ▼
Parity none ▼
Stop bits 1 ▼
Flow control none ▼

TCP/UDP Settings

Protocol TCP ▼
Mode server ▼

Bind to TCP port 2569
Type of socket raw ▼
 Enable local echo
 Enable timeout 3600 sec

Keepalive Settings

Check TCP connection
Keepalive idle time sec
Keepalive interval sec

Log Settings

Log level level 1 ▼

Status started

ReloadSave

Figure 30 – Serial Port configuration page

Modbus Gateway settings

The serial server will perform conversion from Modbus/TCP to Modbus/RTU, allowing polling by a Modbus/TCP master. The Modbus IPSerial Gateway carries out translation between Modbus/TCP and Modbus/RTU. This means that Modbus serial slaves can be directly attached to the unit's serial ports without any external protocol converters.

Click *Serial Port* Tab to open the Modbus Gateway configuration screen. Choose Modbus Gateway options to configure Modbus. At the *Figure 31 - Modbus gateway configuration* page you can see screenshot of Modbus Gateway configuration menu.

Modbus Gateway Parameters	
Label	Description
<i>TCP accept port</i>	This field determines the TCP port number that the serial server will listen for connections on. The value entered should be a valid TCP port number. The default Modbus/TCP port number is 502.
<i>Connection timeout</i>	When this field is set to a value greater than 0, the serial server will close connections that have had no network receive activity for longer than the specified period.
<i>Transmission response</i>	Select RTU, based on the Modbus slave equipment attached to the port.
<i>Response timeout</i>	This is the timeout (in milliseconds) to wait for a response from a serial slave device before retrying the request or returning an error to the Modbus master.
<i>Pause between request</i>	Set pause between requests in milliseconds. Valid values are between 1 and 10000. Default value is 100).
<i>Maximum number of retries</i>	Should no valid response be received from a Modbus slave, the value in this field determines the number of times the serial server will retransmit request before giving up.
<i>Log level</i>	Set importance level of log messages.
<i>Reload</i>	Click <i>Reload</i> to discard any changes and reload previous settings.
<i>Save</i>	Click <i>Save</i> button to save your changes back to the GWR Router and activate/deactivate serial to Ethernet converter.

Table 17 – Modbus gateway parameters

Serial Port ? Help

Serial Port Settings

General Settings

Disable all
 Serial port over TCP/UDP settings
 Modbus gateway settings

Serial Port Settings

Bits per second	57600	▼
Data bits	8	▼
Parity	none	▼
Stop bits	1	▼
Flow control	none	▼

Modbus Gateway Settings

TCP accept port	502	
Connection timeout	60	sec

Modbus Serial Settings

Transmission mode	RTU	▼
Response timeout	50	ms
Pause between request	100	ms
Maximum number of retries	3	

Log Settings

Log level	level 3	▼
-----------	---------	---

Status **started**

[Reload](#) [Save](#)

Figure 31 - Modbus gateway configuration page

SMS(Short Message Service)

SMS remote control feature allows users to execute a short list of predefined commands by sending SMS messages to the router. GWR router series implement following predefined commands:

1. In order to establish PPP connection, user should send SMS containing following string:
:PPP-CONNECT
 After the command is executed, router sends a confirmation SMS with "OK" if the command is executed without errors or "ERROR" if something went wrong during the execution of the command.

2. In order to disconnect the router from PPP, user should send SMS containing following string:
:PPP-DISCONNECT
 After the command is executed, router sends a confirmation SMS with "OK" if the command is executed without errors or "ERROR" if something went wrong during the execution of the command.

3. In order to reestablish (reconnect the router) the PPP connection, user should send SMS containing following string:
:PPP-RECONNECT
 After the command is executed, router sends a confirmation SMS with "OK" if the command is executed without errors or "ERROR" if something went wrong during the execution of the command.

4. In order to obtain the current router status, user should send SMS containing following string:
:PPP-STATUS
 After the command is executed, router sends one of the following status reports to the user:
 - CONNECTING
 - CONNECTED, WAN_IP: {WAN IP address or the router}
 - DISCONNECTING
 - DISCONNECTED

Remote control configuration page is presented on the following figure. In order to use this feature, user must enable the SMS remote control and specify the list of SIM card numbers that will be used for SMS remote control. The SIM card number should be entered in the following format: {Country Code}{Mobile Operator Prefix}{Phone Number} (for example **+38164111222**).

As presented on the figure 32 configuration should be performed for separately for both SIM cards. After the configuration is entered, user must click on *Save* button in order to save the configuration.

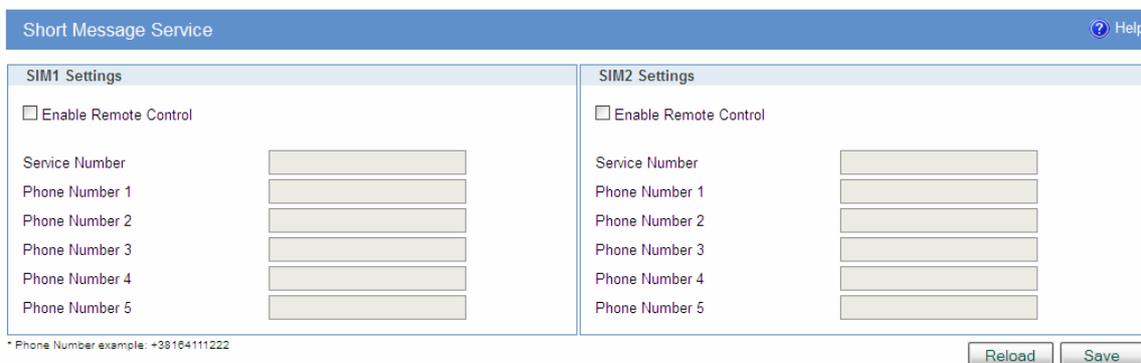


Figure 32 – SMS remote control configuration

SMS – Send SMS

SMS send feature allows users to send SMS message from WEB interface. In following picture is page where SMS can be sent. There are two required fields on this page: Phone number and Message. Sending SMS messages is possible with this application. The SMS message will be sent after entering Phone number and Message and by pushing button Send.

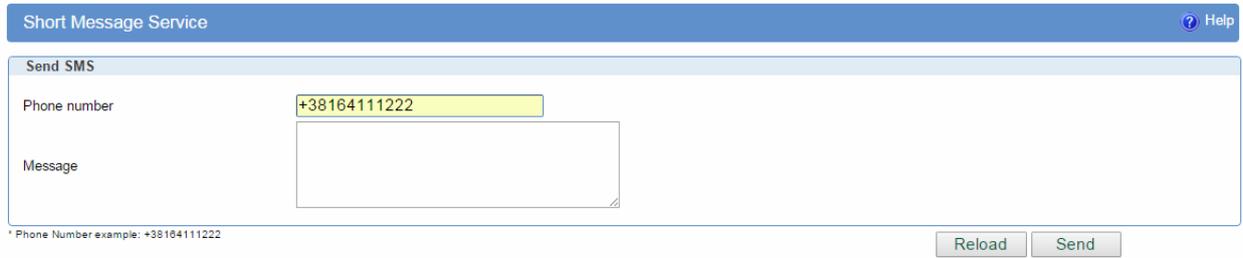


Figure 33– Send SMS

Maintenance

The GWR Router provides administration utilities via web interface. Administrator can setup basic router’s parameters, perform network diagnostic, update software or restore factory default settings.

Maintenance – System Control

Create a scheduled task to reboot the device at a regular interval.



Figure 34– System Control

Maintenance – Device Identity Settings

Within *Device Identity Settings Tab* there is an option to define name, location of device and description of device function. These data are kept in device permanent memory. *Device Identity Settings* window is shown on *Figure 3535*.

Device Identity Settings	
Label	Description
<i>Name</i>	This field specifies name of the GWR Router.
<i>Description</i>	This field specifies description of the GWR Router. Only for information purpose.
<i>Location</i>	This field specifies location of the GWR Router. Only for information purpose.
<i>Save</i>	Click <i>Save</i> button to save your changes back to the GWR Router.
<i>Reload</i>	Click <i>Reload</i> to discard any changes and reload previous settings.

Table 18 - Device Identity parameters



Figure 35 – Device Identity Settings configuration page

Maintenance – Administrator Password

By *Administrator Password* Tab it is possible to activate and deactivates device access system through *Username* and *Password* mechanism. Within this menu change of authorization data Username/Password is also done. *Administer Password* Tab window is shown on *Figure 366*.

NOTE: The password cannot be recovered if it is lost or forgotten. If the password is lost or forgotten, you have to reset the Router to its factory default settings; this will remove all of your configuration changes.

Figure 36 – Administrator Password configuration page

Administrator Password	
Label	Description
<i>Enable Password Authentication</i>	By this check box you can activate or deactivate function for authentication when you access to web/console application.
<i>Username</i>	This field specifies Username for user (administrator) login purpose.
<i>Old Password</i>	Enter the old password. The default is <i>admin</i> when you first power up the GWR Router.
<i>New Password</i>	Enter a new password for GWR Router. Your password must have 20 or fewer characters and cannot contain any space.
<i>Confirm Password</i>	Re–enter the new password to confirm it.
<i>WEB GUI port</i>	Bind HTTP or HTTPS to specified port.
<i>WEB GUI timeout</i>	WEB session timeout
<i>Save</i>	Click <i>Save</i> button to save your changes back to the GWR Router.
<i>Reload</i>	Click <i>Reload</i> to discard any changes and reload previous settings.

Table 19 – Administrator password

Maintenance – Date/Time Settings

To set the local time, select *Date/Time Settings* using the Network Time Protocol (NTP) automatically or Set the local time manually. Date and time setting on the GWR Router are done through window Date/Time Settings.

The screenshot displays the 'Date/Time Settings' configuration page. At the top, it shows the 'Current Date and Time' as 2012 / 10 / 03 and 13 : 46 : 33. Below this, the 'Date and Time Setup' section offers two options: 'Manually' (selected) and 'From time server'. The manual settings include date (2012 / 10 / 03) and time (13 : 46 : 33). The NTP section is configured with 'NTP (RFC-1305)' as the protocol, '195.176.208.1' as the time server address, and '(GMT +1.00 hours) CET (Central Europe Time), Belgrade, Copenhagen, Madrid, Paris' as the time zone. There is an unchecked checkbox for 'Automatically synchronize NTP' and a '15 min' interval for updates. At the bottom, there are options for 'Update for Daylight Saving Time' with start and stop dates set to January 01 at 00:00. Action buttons for 'Sync Clock', 'Reload', and 'Save' are located at the bottom right.

Figure 37 – Date/Time Settings configuration page

Date/Time Settings	
Label	Description
<i>Manually</i>	Sets date and time manually as you specify it.
<i>From time server</i>	Sets the local time using the Network Time Protocol (NTP) automatically.
<i>Time/Date</i>	This field species Date and Time information. You can change date and time by changing parameters.
<i>Sync Clock With Client</i>	Date and time setting on the basis of PC calendar.
<i>Time Protocol</i>	Choose the time protocol.
<i>Time Server Address</i>	Time server IP address.
<i>Time Zone</i>	Select your time zone.
<i>Automatically synchronize NTP</i>	Setup automatic synchronization with time server.
<i>Update time every</i>	Time interval for automatic synchronization.

<i>Update for Daylight Saving Time</i>	<p>Enables daylight saving time.</p> <p>On the date specified as start date, clock on the GWR router will be adjusted for one hour in advance.</p> <p>On the date specified as stop date, clock on the GWR router will be adjusted for one hour backward.</p>
<i>Save</i>	Click <i>Save</i> button to save your changes back to the GWR Router.
<i>Reload</i>	Click <i>Reload</i> to discard any changes and reload previous settings.

Table 20 – Date/time parameters

Maintenance – Diagnostics

The GWR Router provide built-it tool, which is used for troubleshooting network problems. The ping test bounces a packet of machine on the Internet back to the sender. This test shows if the GWR Router is able to connect the remote host. If users on the LAN are having problems accessing service on the Internet, try to ping the DNS server or other machine on network.

Click *Diagnostic* tab to provide basic diagnostic tool for testing network connectivity. Insert valid IP address in *Hostname* box and click *Ping*. Every time you click *Ping* router sends four ICMP packets to destination address.

Before using this tool make sure you know the device or host’s IP address.



Figure 38 – Diagnostic page

Maintenance – Update Firmware

You can use this feature to upgrade the GWR Router firmware to the latest version. If you need to download the latest version of the GWR Router firmware, please visit Geneko support site. Follow the on-screen instructions to access the download page for the GWR Router.

If you have already downloaded the firmware onto your computer, click *Browse* button, on *Update firmware* Tab, to look for the firmware file. After selection of new firmware version through *Browse* button, mechanism the process of data transfer from firmware to device itself should be started. This is done by *Upload* button. The process of firmware transfer to the GWR device takes a few minutes and when it is finished the user is informed about transfer process success.

NOTE: The Router will take a few minutes to upgrade its firmware. During this process, do not power off the Router or press the Reset button.

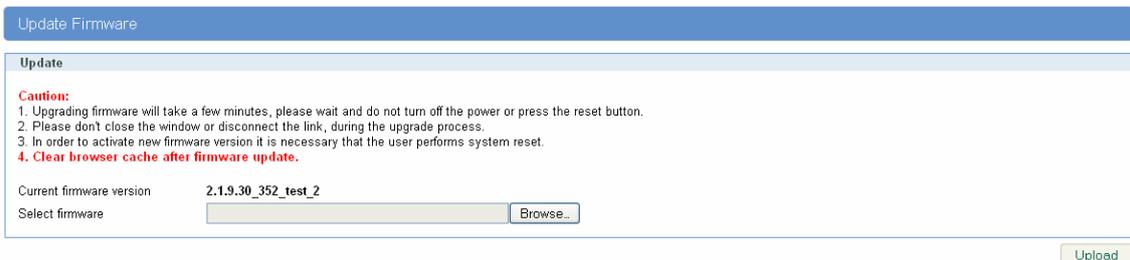


Figure 39 – Update Firmware page

In order to activate new firmware version it is necessary that the user performs system reset. In the process of firmware version change all configuration parameters are lost and after that the system continues to operate with default values.

Maintenance – Settings Backup

This feature allows you to make a backup file of complete configuration or some part of the configuration on the GWR Router. In order to backup the configuration, you should select the part of configuration you would like to backup. The list of available options is presented on the 40. To use the backup file, you need to import the configuration file that you previously exported.

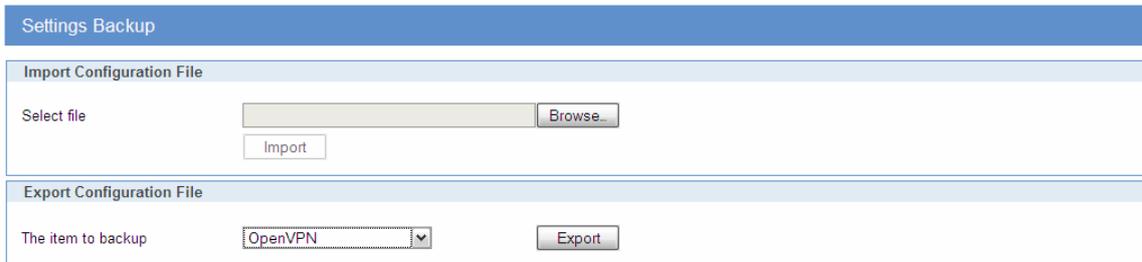


Figure 40 – Export/Import the configuration on the router

Import Configuration File

To import a configuration file, first specify where your backup configuration file is located. Click **Browse**, and then select the appropriate configuration file.

After you select the file, click **Import**. This process may take up to a minute. Restart the Router in order to changes will take effect.

Export Configuration File

To export the Router’s current configuration file select the part of the configuration you would like to backup and click **Export**.

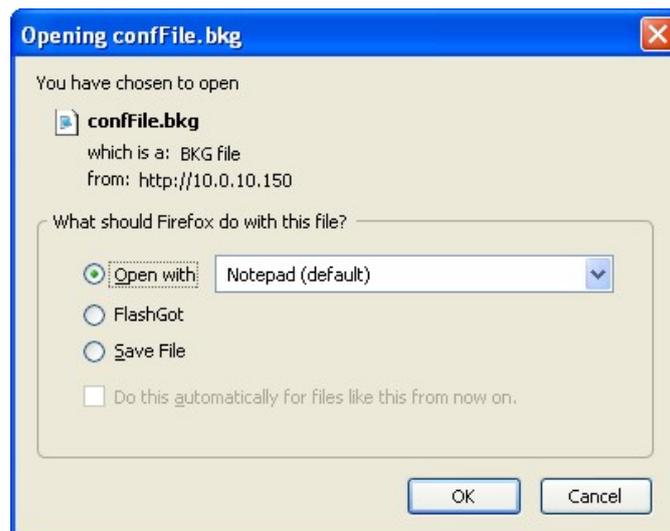


Figure 41 – File download

Select the location where you want to store your backup configuration file. By default, this file will be called *confFile.bkg*, but you may rename it if you wish. This process may take up to a minute.

Maintenance – Default Settings

Use this feature to clear all of your configuration information and restore the GWR Router to its factory default settings. Only use this feature if you wish to discard all the settings and preferences that you have configured.

Click *Default Setting* to have the GWR Router with default parameters. *Keep network settings* check-box allows user to keep all network settings after factory default reset. System will be reset after pressing *Restore* button.

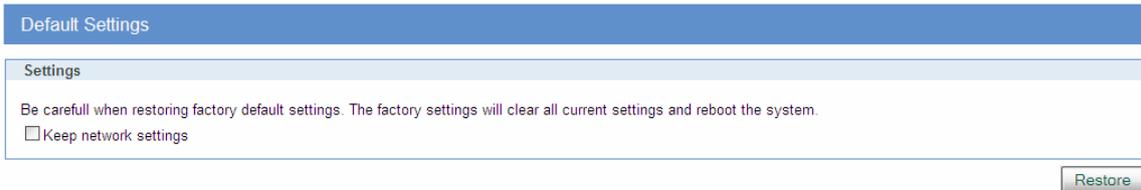


Figure 42 – Default Settings page

Maintenance – System Reboot

If you need to restart the Router, Geneko recommends that you use the Reboot tool on this screen. Click *Reboot* to have the GWR Router reboot. This does not affect the router’s configuration.

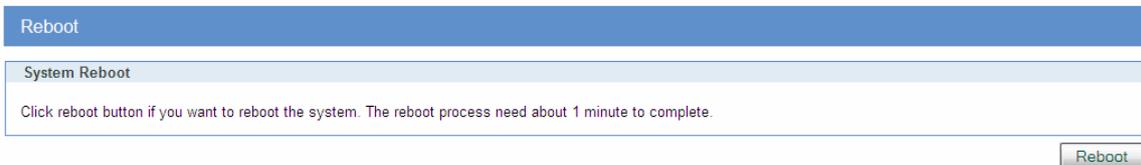


Figure 43 – System Reboot page

Management – Command Line Interface

CLI (command line interface) is a user text-only interface to a computer's operating system or an application in which the user responds to a visual prompt by typing in a command on a specified line and then receives a response back from the system.

In other words, it is a method of instructing a computer to perform a given task by "entering" a command. The system waits for the user to conclude the submitting of the text command by pressing the *Enter* or *Return* key. A command-line interpreter then receives, parses, and executes the requested user command.

On router's Web interface, in Management menu, click on Command Line Interface tab to open the Command Line Interface settings screen. Use this screen to configure CLI parameters *Figure 44 – Command Line Interface*.

Command Line Interface	
Label	Description
<i>CLI Settings</i>	
<i>Enable</i>	Enable or disable CLI
<i>CLI on</i>	Telnet, SSH, Serial
<i>View Mode Username</i>	Login name for View mode
<i>View Mode Password</i>	Password for View mode
<i>Confirm Password</i>	Confirm password for View mode
<i>View Mode Timeout</i>	Inactivity timeout for View mode in seconds. After timeout, user will be put in Main mode.
<i>Edit Mode Timeout</i>	Inactivity timeout for Edit mode in seconds. Note that Username and Password for Edit mode are the same as Web interface login parameters. After timeout, user will be put in Main mode.
<i>Console Type</i>	Windows, other.
<i>Save</i>	Click <i>Save</i> to save your changes back to the GWR Router.
<i>Reload</i>	Click <i>Reload</i> to discard any changes and reload previous settings.

Table 21 – Command Line Interface parameters

Figure 44 – Command Line Interface

Detailed instructions related to CLI are located in other document (Command_Line_Interface.pdf file on CD that goes with the router). You will find detailed specifications of all commands you can use to configure the router and monitor routers performance.

Management – Remote Management

Remote Management Utility is a standalone Windows application with many useful options for configuration and monitoring of GWR routers. More information about this utility can be found in other document (Remote_Management.pdf). In order to use this utility user has to enable Remote Management on the router *Figure 455*.

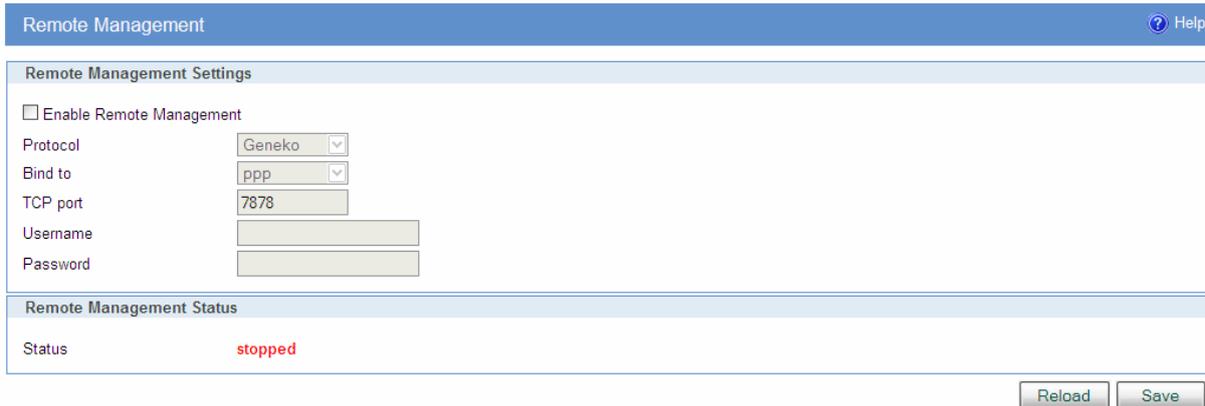


Figure 45 – Remote Management

Command Line Interface	
Label	Description
<i>Enable Remote Management</i>	Enable or disable Remote Management.
<i>Protocol</i>	Choose between Geneko and Sarian protocol.
<i>Bind to</i>	Specify the interface.
<i>TCP port</i>	Specify the TCP port.
<i>Username</i>	Specify the username.
<i>Password</i>	Specify the password.
<i>Save</i>	Click <i>Save</i> to save your changes back to the GWR Router.
<i>Reload</i>	Click <i>Reload</i> to discard any changes and reload previous settings.

Table 22 – Remote Management parameters

Management – Connection Manager

Enabling Connection Manager will allow Connection Wizard (located on setup CD that goes with the router) to guide you step-by-step through the process of device detection on the network and setup of the PC-to-device communication. Thanks to this utility user can simply connect the router to the local network without previous setup of the router. Connection Wizard will detect the device and allow you to configure some basic functions of the router. Connection Manager is enabled by default on the router and if you do not want to use it you can simply disable it *Figure 466*.



Figure 46 – Connection Manager

Getting started with the Connection Wizard

Connection Wizard is installed through few very simple steps and it is available immediately upon the installation. After starting the wizard you can choose between two available options for configuration:

- **GWR Router's Ethernet port** – With this option you can define LAN interface IP address and subnet mask.
- **GWR router's Ethernet port and GPRS/EDGE/HSPA/HSPA+/LTE network connection** – Selecting this option you can configure parameters for LAN and WAN interface



Figure 47 – Connection Wizard – Initial Step

Select one of the options and click *Next*. On the next screen after Connection Wizard inspects the network (whole broadcast domain) you'll see a list of routers present in the network, with following information:

- Serial number,
- Model,
- Ethernet IP,
- Firmware version,
- Pingable (if Ethernet IP address of the router is in the same IP subnet as PC interface then this field will be marked, i.e. you can access router over web interface).

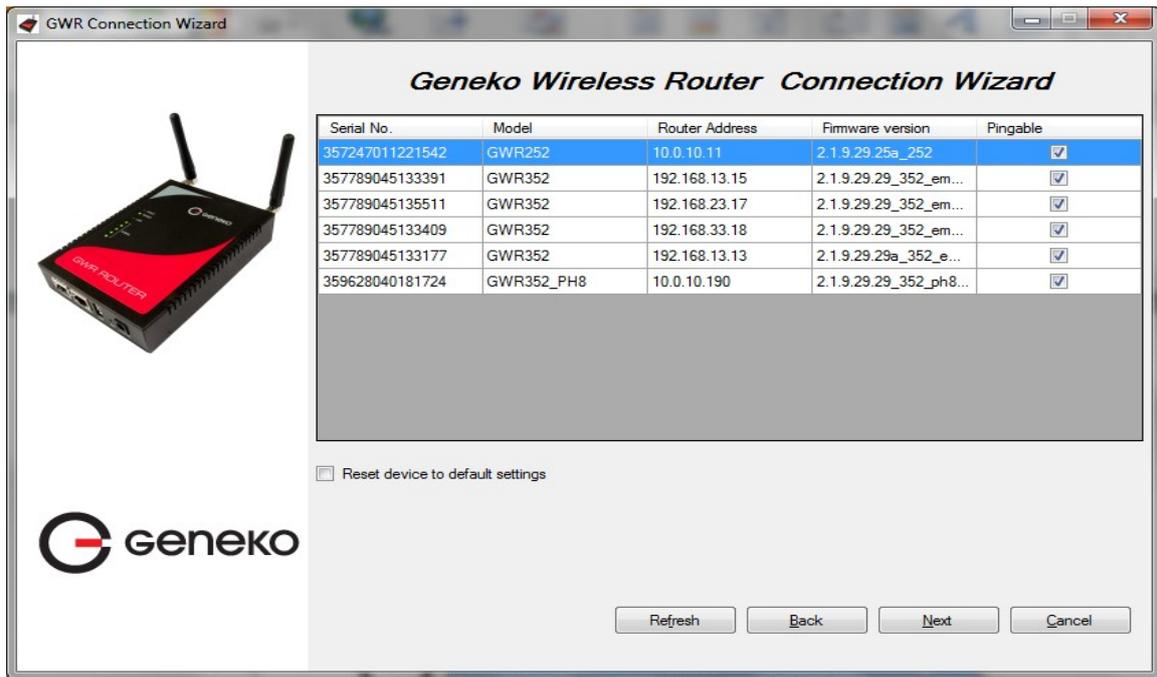


Figure 48 – Connection Wizard – Router Detection

When you select one of the routers from the list and click *Next* you will get to the following screen.



Figure 49 – Connection Wizard – LAN Settings

If you selected to configure LAN and WAN interface click, upon entering LAN information click *Next* and you will be able to setup WAN interface.



Figure 50 – Connection Wizard – WAN Settings

After entering the configuration parameters if you mark option *Establish connection* router will start with connection establishment immediately when you press *Finish* button. If not you have to start connection establishment manually on the router's web interface.

Management – Simple Management Protocol (SNMP)

SNMP, or Simple Network Management Protocol, is a network protocol that provides network administrators with the ability to monitor the status of the Router and receive notification of any critical events as they occur on the network. The Router supports SNMP v1/v2c and all relevant Management Information Base II (MIBII) groups. The appliance replies to SNMP Get commands for MIB II via any interface and supports a custom MIB for generating trap messages.

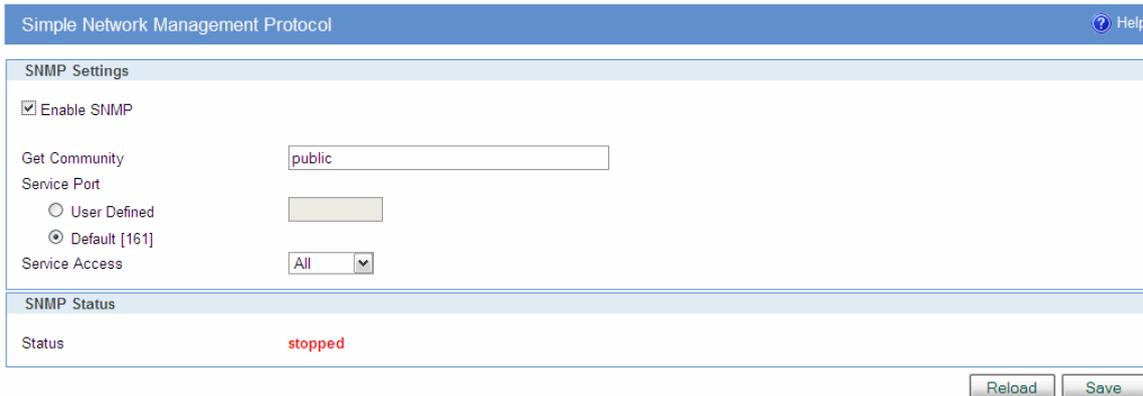


Figure 51 – SNMP configuration page

SNMP Settings	
Label	Description
<i>Enable SNMP</i>	SNMP is enabled by default. To disable the SNMP agent, click this option to unmark.
<i>Get Community</i>	Create the name for a group or community of administrators who can view SNMP data. The default is <i>public</i> . It supports up to 64 alphanumeric characters.
<i>Service Port</i>	Sets the port on which SNMP data has been sent. The default is 161. You can specify port by marking on user defined and specify port you want SNMP data to be sent.
<i>Service Access</i>	Sets the interface enabled for SNMP traps. The default is Both.
<i>Reload</i>	Click <i>Reload</i> to discard any changes and reload previous settings.
<i>Save</i>	Click <i>Save</i> button to save your changes back to the GWR Router and enable/disable SNMP.

Table 23 – SNMP parameters

Management – Logs

Syslog is a standard for forwarding log messages in an IP network. The term "syslog" is often used for both the actual syslog protocol, as well as the application or library sending syslog messages.

Syslog is a client/server protocol: the syslog sender sends a small (less than 1KB) textual message to the syslog receiver. Syslog is typically used for computer system management and security auditing. While it has a number of shortcomings, syslog is supported by a wide variety of devices and receivers across multiple platforms. Because of this, syslog can be used to integrate log data from many different types of systems into a central repository.

Figure 52 – Syslog configuration page

The GWR Router supports this protocol and can send its activity logs to an external server.

Syslog Settings	
Label	Description
<i>Disable</i>	Mark this option in order to disable Syslog feature.
<i>Local syslog</i>	Mark this option in order to enable Local syslog feature. Logs will remain on the router.
<i>Remote + local syslog</i>	Mark this option in order to enable remote and local syslog feature.
<i>Log to</i>	Set syslog storage to the router's internal buffer (local) or external to the USB flash. If you choose USB flash, drive must be formatted using the FAT32 file system.
<i>Syslog file size</i>	Set log size on one of the six predefined values. [10 / 20 / 50 / 128 / 256 / 512 / 1024]KB
<i>Event log</i>	Choose which events to be stored. You can store System, IPsec events or both of them.

<i>Enable syslog saver</i>	Save logs periodically on filesystem.
<i>Save log every</i>	Set time duration between two saves.
<i>Service server IP</i>	The GWR Router can send a detailed log to an external syslog server. The Router's syslog captures all log activities and includes this information about all data transmissions: every connection source and destination IP address, IP service, and number of bytes transferred. Enter the syslog server name or IP address.
<i>Service protocol</i>	Sets the protocol type.
<i>Service port</i>	Sets the port on which syslog data has been sent. The default is 514. You can specify port by marking on user defined and specify port you want syslog data to be sent.
<i>Reload</i>	Click Reload to discard any changes and reload previous settings.
<i>Save</i>	Click <i>Save</i> button to save your changes back to the GWG Gateway and enable/disable Syslog.

Table 24 - Syslog parameters

Logout

The *Logout* tab is located on the down left-hand corner of the screen. Click this tab to exit the web-based utility. (If you exit the web-based utility, you will need to re-enter your User Name and Password to log in and then manage the Router.)

Configuration Examples

GWR Router as Internet Router

The GWR Routers can be used as *Internet router* for a single user or for a group of users (entire LAN). NAT function is enabled by default on the GWR Router. The GWR Router uses Network Address Translation (NAT) where only the mobile IP address is visible to the outside world. All outgoing traffic uses the GWR Router mobile IP address.

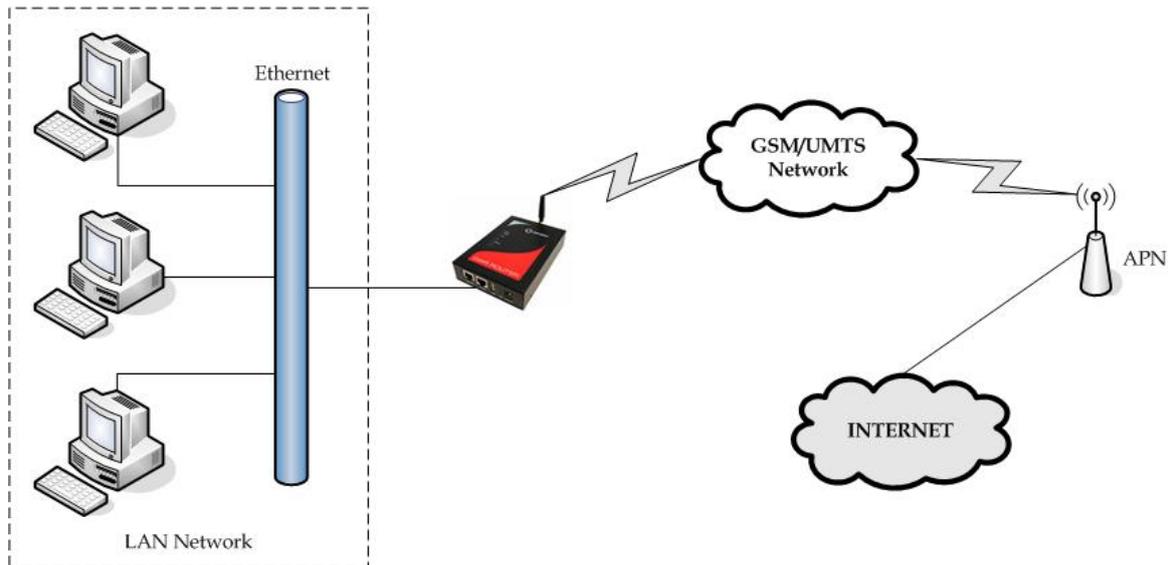


Figure 53 – GWR Router as Internet router

- Click **Network** Tab, to open the **LAN NETWORK** screen. Use this screen to configure LAN TCP/IP settings. Configure IP address and Netmask.
 - IP address: 10.1.1.1,
 - Netmask: 255.255.255.0.
- Press **Save** to accept the changes.
- Use SIM card with a dynamic/static IP address, obtained from Mobile Operator. (Note the default gateway may show, or change to, an address such as 10.0.0.1; this is normal as it is the GSM/UMTS provider's network default gateway).
- Click **WAN Settings** Tab to configure parameters necessary for GSM/UMTS connection. All parameters necessary for connection configuration should be provided by your mobile operator.
- Check the status of GSM/UMTS connection (**WAN Settings** Tab). If disconnected please click **Connect** button.
- Check **Routing** Tab to see if there is default route (should be there by default).
- Router will automatically add default route via *ppp0* interface.
- Optionally configure IP Filtering and TCP service port settings to block any unwanted incoming traffic.
- Configure the GWR Router LAN address (10.1.1.1) as a default gateway address on your PCs. Configure valid DNS address on your PCs.

GRE Tunnel configuration between two GWR Routers

GRE tunnel is a type of a VPN tunnel, but it is not a secure tunneling method. Simple network with two GWR Routers is illustrated on the diagram below (Figure 54). Idea is to create GRE tunnel for LAN to LAN (site to site) connectivity.

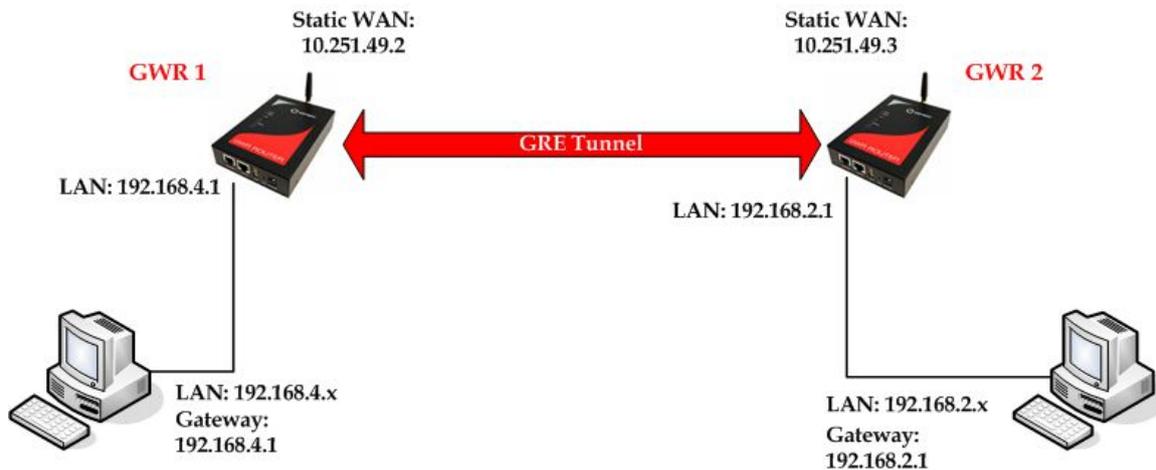


Figure 54 – GRE tunnel between two GWR Routers

The GWR Routers requirements:

- Static IP WAN address for tunnel source and tunnel destination address;
- Source tunnel address should have static WAN IP address;
- Destination tunnel address should have static WAN IP address;

GSM/UMTS APN Type: For GSM/UMTS networks GWR Router connections may require a Custom APN. A Custom APN allows for various IP addressing options, particularly static IP addresses, which are needed for most VPN connections. A custom APN should also support mobile terminated data that may be required in most site-to-site VPNs.

The GWR Router 1 configuration:

- Click **Network** Tab, to open the **LAN NETWORK** screen. Use this screen to configure LAN TCP/IP settings. Configure IP address and Netmask.
 - IP Address: 192.168.4.1,
 - Subnet Mask: 255.255.255.0,
 - Press **Save** to accept the changes.

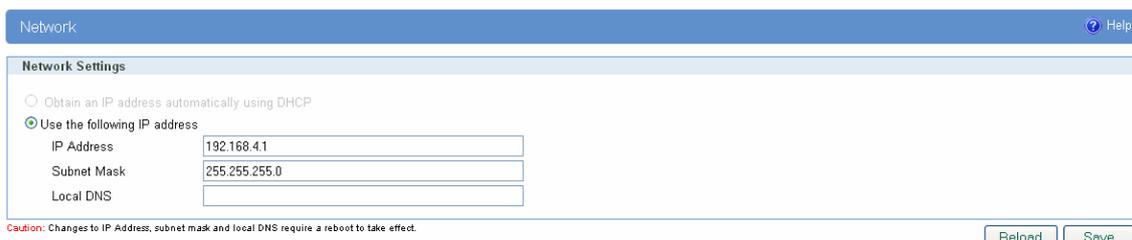


Figure 55 – Network configuration page for GWR Router 1

- Use SIM card with a static IP address, obtained from Mobile Operator. (Note the default gateway may show, or change to, an address such as 10.0.0.1; this is normal as it is the GSM/UMTS provider’s network default gateway).

- Click **WAN Settings** Tab to configure parameters necessary for GSM/UMTS connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS connection (**WAN Settings** Tab). If disconnected please click **Connect** button.
- Click **VPN Settings > GRE** to configure GRE tunnel parameters:
 - Enable: yes,
 - Local Tunnel Address: 10.10.10.1,
 - Local Tunnel Netmask: 255.255.255.252 (Unchangeable, always 255.255.255.252),
 - Tunnel Source: 10.251.49.2 (select HOST from drop down menu if you want to use host name as peer identifier),
 - Tunnel Destination: 10.251.49.3 (select HOST from drop down menu if you want to use host name as peer identifier),
 - KeepAlive enable: no,
 - Period:(none),
 - Retries:(none),
 - Press **ADD** to put GRE tunnel rule into GRE table.
 - Press **Save** to accept the changes.

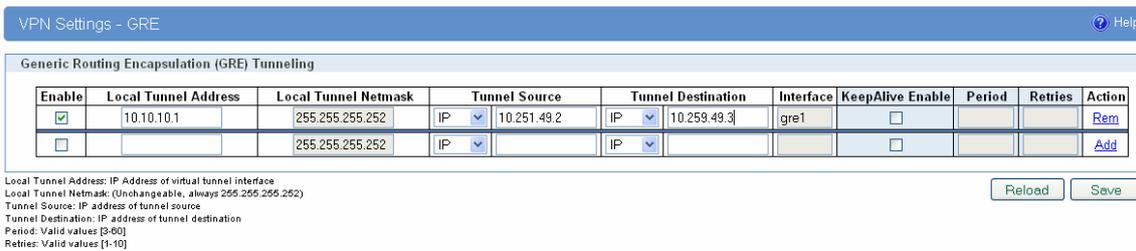


Figure 56 – GRE configuration page for GWR Router 1

- Click **Routing** on **Settings** Tab to configure GRE Route. Parameters for this example are:
 - Destination Network: 192.168.2.0,
 - Netmask: 255.255.255.0,
 - Interface: gre_x.

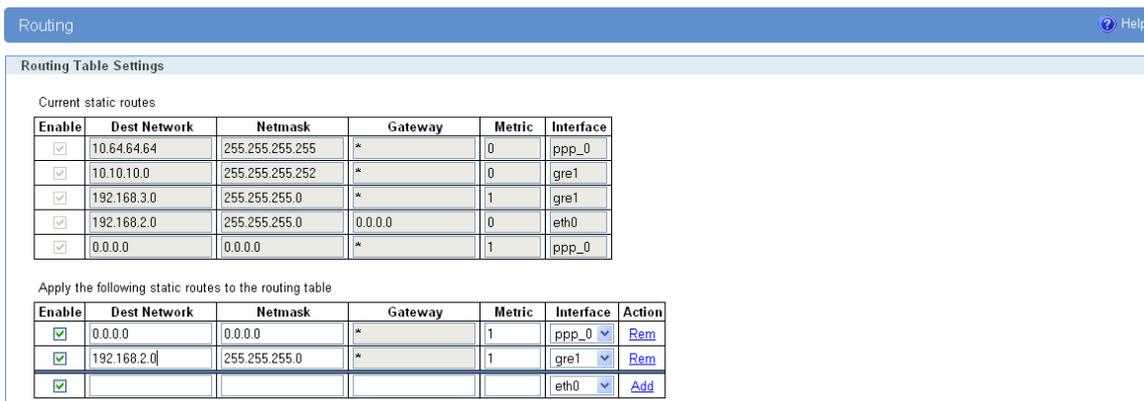


Figure 57 – Routing configuration page for GWR Router 1

- Optionally configure IP Filtering and TCP service port settings to block any unwanted incoming traffic.
- On the device connected on GWR router 1 setup default gateway 192.168.4.1

The GWR Router 2 configuration:

- Click **Network** Tab, to open the **LAN NETWORK** screen. Use this screen to configure LAN TCP/IP settings. Configure IP address and Netmask.

- IP Address: 192.168.2.1,
- Subnet Mask: 255.255.255.0,
- Press *Save* to accept the changes.

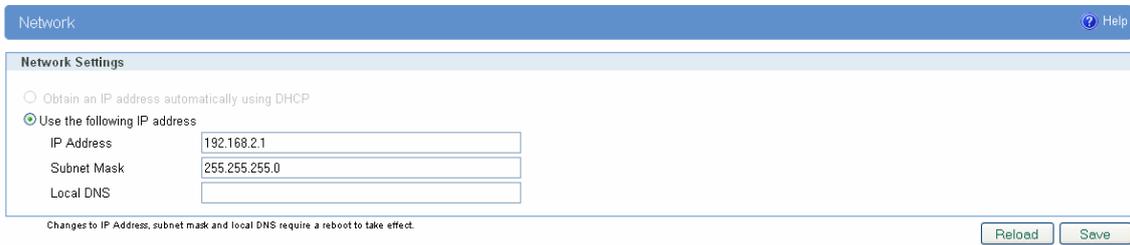


Figure 58 – Network configuration page for GWR Router 2

- Use SIM card with a static IP address, obtained from Mobile Operator. (Note the default gateway may show, or change to, an address such as 10.0.0.1; this is normal as it is the GSM/UMTS provider’s network default gateway).
- Click *WAN Settings* Tab to configure parameters necessary for GSM/UMTS connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS connection (*WAN Settings* Tab). If disconnected please click *Connect* button.
- Click *VPN Settings* > *GRE* to configure GRE tunnel parameters:
 - Enable: yes,
 - Local Tunnel Address: 10.10.10.2,
 - Local Tunnel Netmask: 255.255.255.252 (Unchangeable, always 255.255.255.252),
 - Tunnel Source: 10.251.49.3 (select HOST from drop down menu if you want to use host name as peer identifier),
 - Tunnel Destination: 10.251.49.2 (select HOST from drop down menu if you want to use host name as peer identifier),
 - KeepAlive enable: no,
 - Period:(none),
 - Retries:(none),
 - Press ADD to put GRE tunnel rule into GRE table,
 - Press *Save* to accept the changes.

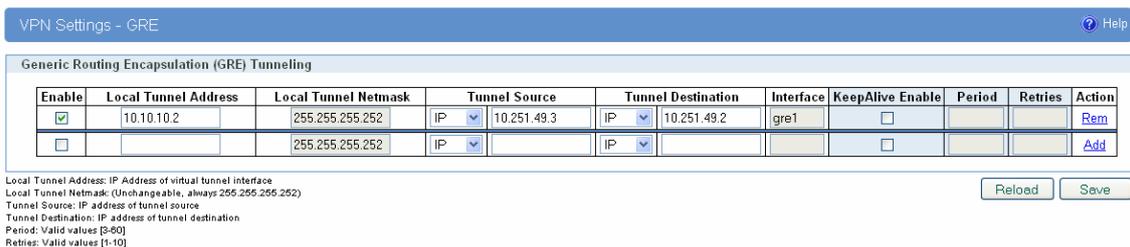


Figure 59 – GRE configuration page for GWR Router 2

- Configure GRE Route. Click *Routing* on *Settings* Tab. Parameters for this example are:
 - Destination Network: 192.168.4.0,
 - Netmask: 255.255.255.0.

Routing Help

Routing Table Settings

Current static routes

Enable	Dest Network	Netmask	Gateway	Metric	Interface
<input checked="" type="checkbox"/>	10.64.64.64	255.255.255.255	*	0	ppp_0
<input checked="" type="checkbox"/>	10.10.10.0	255.255.255.252	*	0	gre1
<input checked="" type="checkbox"/>	192.168.3.0	255.255.255.0	*	1	gre1
<input checked="" type="checkbox"/>	192.168.2.0	255.255.255.0	0.0.0.0	0	eth0
<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	*	1	ppp_0

Apply the following static routes to the routing table

Enable	Dest Network	Netmask	Gateway	Metric	Interface	Action
<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	*	1	ppp_0	Rem
<input checked="" type="checkbox"/>	192.168.4.0	255.255.255.0	*	1	gre1	Rem
<input checked="" type="checkbox"/>					eth0	Add

Figure 60 – Routing configuration page for GWR Router 2

- Optionally configure IP Filtering and TCP service port settings to block any unwanted incoming traffic.
- On the device connected on GWR router 2 setup default gateway 192.168.2.1.

GRE Tunnel configuration between GWR Router and third party router

GRE tunnel is a type of a VPN tunnels, but it isn't a secure tunneling method. However, you can encrypt GRE packets with an encryption protocol such as IPSec to form a secure VPN.

On the diagram below (61) is illustrated simple network with two sites. Idea is to create GRE tunnel for LAN to LAN (site to site) connectivity.

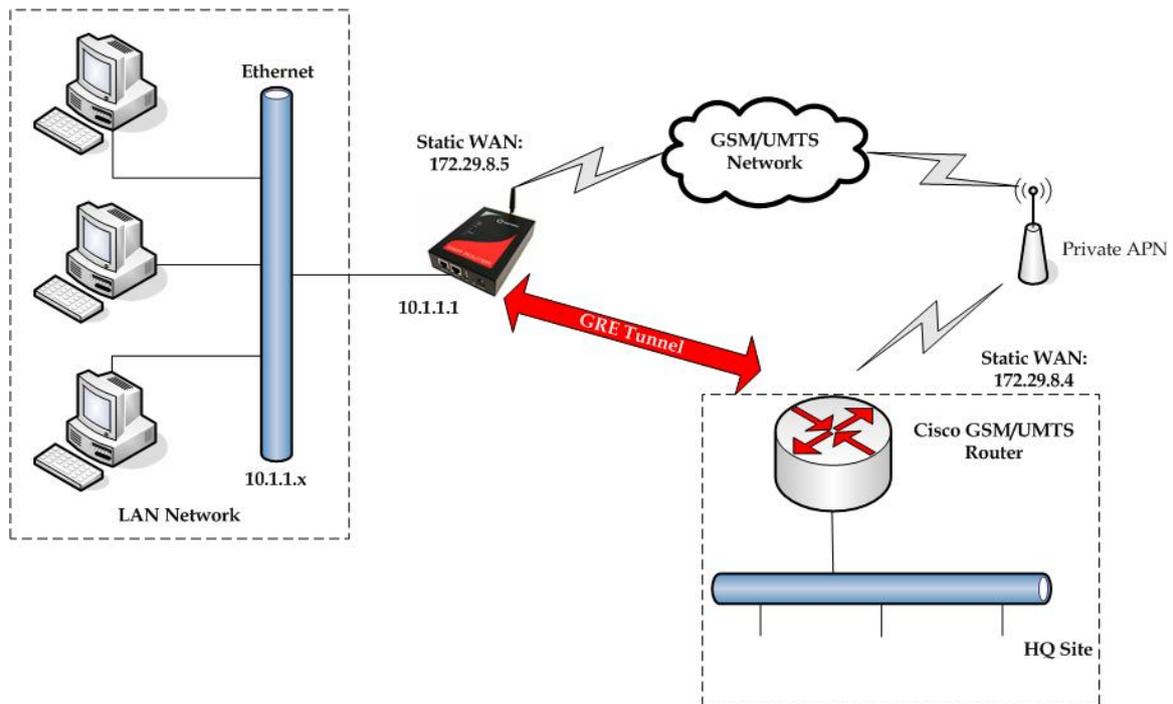


Figure 61 – GRE tunnel between Cisco router and GWR Router

GRE tunnel is created between Cisco router with GRE functionality on the HQ Site and the GWR Router on the Remote Network. In this example, it is necessary for both routers to create tunnel interface (virtual interface). This new tunnel interface is its own network. To each of the routers, it appears that it has two paths to the remote physical interface and the tunnel interface (running through the tunnel). This tunnel could then transmit unroutable traffic such as NetBIOS or AppleTalk.

The GWR Router uses Network Address Translation (NAT) where only the mobile IP address is visible to the outside. All outgoing traffic uses the GWR Router WAN/VPN mobile IP address. HQ Cisco router acts like gateway to remote network for user in corporate LAN. It also performs function of GRE server for termination of GRE tunnel. The GWR Router act like default gateway for Remote Network and GRE server for tunnel.

1. HQ router requirements:

- HQ router require static IP WAN address,
- Router or VPN appliance have to support GRE protocol,
- Tunnel peer address will be the GWR Router WAN's mobile IP address. For this reason, a static mobile IP address is preferred on the GWR Router WAN (GPRS) side,
- Remote Subnet is remote LAN network address and Remote Subnet Mask is subnet of remote LAN.

2. The GWR Router requirements:

- Static IP WAN address,

- Peer Tunnel Address will be the HQ router WAN IP address (static IP address),
- Remote Subnet is HQ LAN IP address and Remote Subnet Mask is subnet mask of HQ LAN.

GSM/UMTS APN Type: For GSM/UMTS networks GWR Router connections may require a Custom APN. A Custom APN allows for various IP addressing options, particularly static IP addresses, which are needed for most VPN connections. A custom APN should also support mobile terminated data that may be required in most site-to-site VPNs.

Cisco router sample Configuration:

```
Interface FastEthernet 0/1
ip address 10.2.2.1 255.255.255.0
description LAN interface

interface FastEthernet 0/0
ip address 172.29.8.4 255.255.255.0
description WAN interface

interface Tunnel0
ip address 10.1.1.1 255.255.255.0
tunnel source FastEthernet0/0
tunnel destination 172.29.8.5

ip route 10.1.1.0 255.255.255.0 tunnel0
```

The GWR Router Sample Configuration:

- Click **Network** Tab, to open the **LAN NETWORK** screen. Use this screen to configure LAN TCP/IP settings. Configure IP address and Netmask.
 - IP Address: 10.1.1.1,
 - Subnet Mask: 255.255.255.0,
 - Press **Save** to accept the changes.



Figure 62 – Network configuration page

- Use SIM card with a dynamic/static IP address, obtained from Mobile Operator. (Note the default gateway may show, or change to, an address such as 10.0.0.1; this is normal as it is the GSM/UMTS provider’s network default gateway).
- Click **WAN Settings** Tab to configure parameters necessary for GSM/UMTS connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS connection (**WAN Settings** Tab). If disconnected please click **Connect** button.
- Click **VPN Settings > GRE Tunneling** to configure new VPN tunnel parameters:
 - Enable: yes,
 - Local Tunnel Address: 10.1.1.1,
 - Local Tunnel Netmask: 255.255.255.252 (Unchangeable, always 255.255.255.252),
 - Tunnel Source: 172.29.8.5,

- Tunnel Destination: 172.29.8.4,
- KeepAlive enable: no,
- Period:(none),
- Retries:(none),
- Press **ADD** to put GRE tunnel rule into VPN table,
- Press **Save** to accept the changes.

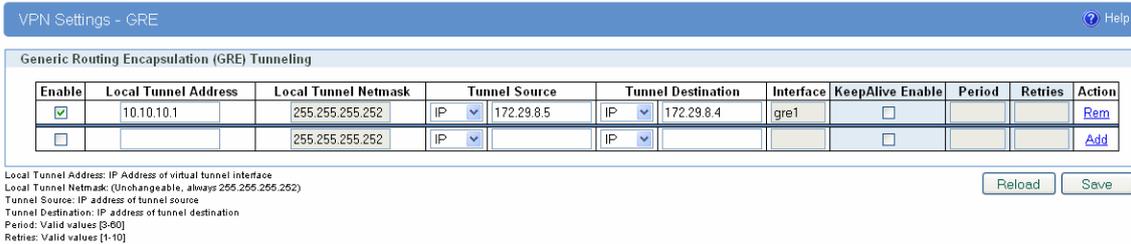


Figure 63 – GRE configuration page

- Configure GRE Route. Click **Routing** on **Settings** Tab. Parameters for this example are:
 - Destination Network: 10.2.2.0,
 - Netmask: 255.255.255.0.

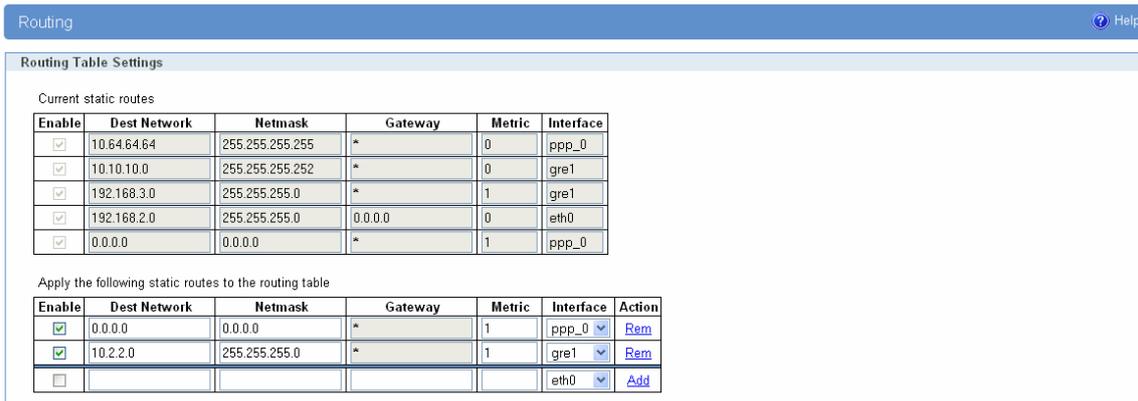


Figure 64 – Routing configuration page

- Optionally configure IP Filtering and TCP service port settings to block any unwanted incoming traffic.

User from remote LAN should be able to communicate with HQ LAN.

IPSec Tunnel configuration between two GWR Routers

IPSec tunnel is a type of a VPN tunnels with a secure tunneling method. Simple network with two GWR Routers is illustrated on the diagram below *Figure 65*. Idea is to create IPSec tunnel for LAN to LAN (site to site) connectivity.

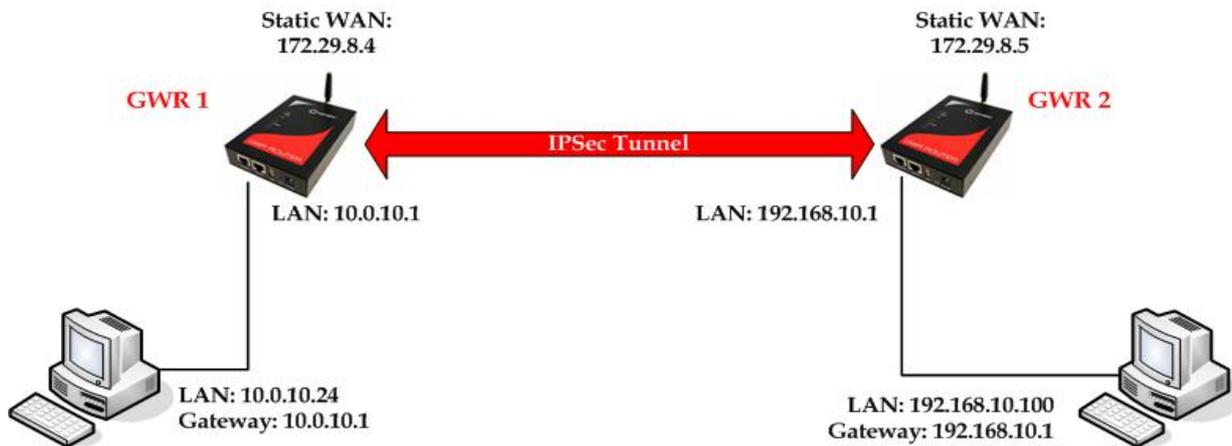


Figure 65 – IPSec tunnel between two GWR Routers

The GWR Routers requirements:

- Static IP WAN address for tunnel source and tunnel destination address,
- Dynamic IP WAN address must be mapped to hostname with DynDNS service (for synchronization with DynDNS server SIM card must have internet access),

GSM/UMTS APN Type: For GSM/UMTS networks GWR Router connections may require a Custom APN. A Custom APN allows for various IP addressing options, particularly static IP addresses, which are needed for most VPN connections. A custom APN should also support mobile terminated data that may be required in most site-to-site VPNs.

For the purpose of detailed explanation of IPSec tunnel configuration, two scenarios will be examined and network illustrated in the *Figure 62* will be used for both scenarios.

Scenario #1

Router 1 and Router 2, presented in the *Figure 66*, provides three modes of negotiation in IPSec tunnel configuration process:

- Aggressive,
- Main,

In this scenario, aggressive mode will be used. Configurations for Router 1 and Router 2 are listed below. The GWR Router 1 configuration:

Click *Network* Tab, to open the **LAN NETWORK** screen. Use this screen to configure LAN TCP/IP settings. Configure IP address and Netmask:

- IP Address: 10.0.10.1,
- Subnet Mask: 255.255.255.0,
- Press *Save* to accept the changes.

The screenshot shows the 'Network Settings' interface. At the top, there's a 'Network' header with a 'Help' icon. Below it, the 'Network Settings' section has two radio buttons: 'Obtain an IP address automatically using DHCP' (unselected) and 'Use the following IP address' (selected). Under the selected option, there are three input fields: 'IP Address' containing '10.0.10.1', 'Subnet Mask' containing '255.255.255.0', and 'Local DNS' which is empty. A red 'Caution' message at the bottom left states: 'Changes to IP Address, subnet mask and local DNS require a reboot to take effect.' At the bottom right, there are 'Reload' and 'Save' buttons.

Figure 66 – Network configuration page for GWR Router 1

- Use SIM card with a static IP address, obtained from Mobile Operator.
- Click *WAN Settings* Tab to configure parameters necessary for GSM/UMTS connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS connection (*WAN Settings* Tab). If disconnected please click *Connect* button.
- Click *VPN Settings* > *IPSEC* to configure IPSEC tunnel parameters. Click *Add New Tunnel* button to create new IPsec tunnel. Tunnel parameters are:
 - *Add New Tunnel*
 - Tunnel Name: test,
 - Enable: true,
 - *IPSec Setup*
 - Keying Mode: IKE with Preshared key,
 - Phase 1 DH group: Group 2,
 - Phase 1 Encryption: 3DES,
 - Phase 1 Authentication: MD5,
 - Phase 1 SA Life Time: 28800,
 - Perfect Forward Secrecy: true,
 - Phase 2 DH group: Group 2,
 - Phase 2 Encryption: DES,
 - Phase 2 Authentication: MD5,
 - Phase 2 SA Life Time: 3600,
 - Preshared Key: 1234567890.
 - *Local Group Setup*
 - Local Security Gateway Type: SIM card,
 - IP Address From: SIM 1 (WAN connection is established over SIM 1),
 - Local ID Type: IP Address,

- Local Security Group Type: Subnet,
- IP Address: 10.0.10.0,
- Subnet Mask: 255.255.255.0.
- **Remote Group Setup**
 - Remote Security Gateway Type: IP Only,
 - IP Address: 172.29.8.5,
 - Remote ID Type: IP Address,
 - Remote Security Group Type: IP,
 - IP Address: 192.168.10.1.
- **Failover**
 - Enable Tunnel Failover: false,
- **Advanced**
 - Negotiation Mode: Aggressive,
 - Compress(Support IP Payload Compression Protocol(IPComp)): false,
 - Dead Peer Detection(DPD): false,
 - NAT Traversal: true,
 - Send Initial Contact: true.

Figure 67 – IPSEC configuration page I for GWR Router 1

Figure 68 – IPSEC configuration page II for GWR Router 1

NOTE : If option NAT Traversal is selected Aggressive mode is predefined.

Figure 69 – IPsec configuration page III for GWR Router 1

Click **Start** button on *Internet Protocol Security* page to initiate IPSEC tunnel.

No.	Name	Enabled	Status	Enc/Auth/Grp	Advanced Setup	Local Group	Remote Group	Remote Gateway	Action
1	Test	yes	starting	Ph1: 3DES/MD5/2 Ph2: DES/MD5/2	A/N/I	10.0.10.0 255.255.255.0	192.168.10.1	172.29.8.5	Edit Delete

Figure 70 – IPsec start/stop page for GWR Router 1

- On the device connected on GWR router 1 setup default gateway 10.0.10.1

The GWR Router 2 configuration:

- Click **Network** Tab, to open the LAN NETWORK screen. Use this screen to configure LAN TCP/IP settings. Configure IP address and Netmask.
 - IP Address: 192.168.10.1,
 - Subnet Mask: 255.255.255.0,
 Press **Save** to accept the changes.

Figure 71 – Network configuration page for GWR Router 2

- Use SIM card with a static IP address, obtained from Mobile Operator.
- Click **WAN Settings** Tab to configure parameters necessary for GSM/UMTS connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS connection (**WAN Settings** Tab). If disconnected please click **Connect** button.

- Click *VPN Settings* > *IPSEC* to configure IPSEC tunnel parameters. Click *Add New Tunnel* button to create new IPsec tunnel. Tunnel parameters are:
 - *Add New Tunnel*
 - Tunnel Name: test,
 - Enable: true.
 - *IPSec Setup*
 - Keying Mode: IKE with Preshared key,
 - Phase 1 DH group: Group 2,
 - Phase 1 Encryption: 3DES,
 - Phase 1 Authentication: MD5,
 - Phase 1 SA Life Time: 28800,
 - Perfect Forward Secrecy: true,
 - Phase 2 DH group: Group 2,
 - Phase 2 Encryption: DES,
 - Phase 2 Authentication: MD5,
 - Phase 2 SA Life Time: 3600,
 - Preshared Key: 1234567890.
 - *Local Group Setup*
 - Local Security Gateway Type: SIM card,
 - IP Address From: SIM 1 (WAN connection is established over SIM 1),
 - Local ID Type: IP Address,
 - Local Security Group Type: IP,
 - IP Address: 192.168.10.1.
 - *Remote Group Setup*
 - Remote Security Gateway Type: IP Only,
 - IP Address: 172.29.8.4,
 - Remote ID Type: IP Address,
 - Remote Security Group Type: Subnet,
 - IP Address: 10.0.10.0,
 - Subnet: 255.255.255.0.
 - *Failover*
 - Enable Tunnel Failover: false.
 - *Advanced*
 - Negotiation Mode: Aggressive,
 - Compress(Support IP Payload Compression Protocol(IPComp)): false,
 - Dead Peer Detection(DPD): false,
 - NAT Traversal: true,
 - Send Initial Contact: true,
- Press *Save* to accept the changes.

Device to Device Tunnel Help

Add New Tunnel

Tunnel Number:
Tunnel Name:
Enable:

IPSec Setup

Keying Mode: IKE with Preshared key ▾
Phase 1 DH Group: Group2 ▾
Phase 1 Encryption: 3DES ▾
Phase 1 Authentication: MD5 ▾
Phase 1 SA Life Time: sec
Perfect Forward Secrecy:
Phase 2 DH Group: Group2 ▾
Phase 2 Encryption: DES ▾
Phase 2 Authentication: MD5 ▾
Phase 2 SA Life Time: sec
Preshared Key:

Figure 72 – IPSEC configuration page I for GWR Router 2

Local Group Setup

Local Security Gateway Type: SIM Card ▾
IP Address From: SIM 1 ▾
Local ID Type: IP Address ▾
Local Security Group Type: IP ▾
IP Address:

Remote Group Setup

Remote Security Gateway Type: IP Only ▾
IP Address:
Remote ID Type: IP Address ▾
Remote Security Group Type: Subnet ▾
IP Address:
Subnet Mask:

Figure 73 – IPSEC configuration page II for GWR Router 2

NOTE : If option NAT Traversal is selected Aggressive mode is predefined.

Failover

Enable Tunnel Failover
Ping IP:
Ping Interval: sec
Packet Size:
Advanced Ping Interval: sec
Advanced Ping Wait For A Response: sec
Maximum Number Of Failed Packets: %

Advanced

Negotiation Mode: Aggressive ▾
 Compression (IPComp)
 Dead Peer Detection (DPD): sec
 NAT Traversal
 Send Initial Contact

Figure 74 – IPSEC configuration page III for GWR Router 2

Click **Start** button on *Internet Protocol Security* page to initiate IPSEC tunnel

The screenshot shows the 'Internet Protocol Security' configuration page. At the top, there is a 'Summary' section with the following information:

- Tunnels used: 1
- Maximum number of tunnels: 5
- An 'Add New Tunnel' button is present.

Below the summary is a table with the following columns: No., Name, Enabled, Status, Enc/Auth/Grp, Advanced Setup, Local Group, Remote Group, Remote Gateway, and Action.

No.	Name	Enabled	Status	Enc/Auth/Grp	Advanced Setup	Local Group	Remote Group	Remote Gateway	Action
1	Test	yes	starting	Ph1: 3DES/MD5/2 Ph2: DES/MD5/2	A/N/I	192.168.10.1	10.0.10.0 192.168.10.1	172.29.8.4	Edit Delete

At the bottom right of the page, there are three buttons: 'Start', 'Stop', and 'Refresh'. Below the table, there is a legend for tunnel status:

- started - IPsec is running and tunnel's waiting for other end to connect
- established - tunnel is up
- stopped - IPsec is not running or tunnel is not enabled

Additional notes at the bottom left include:

- * Reducing the MTU size on the client side, can help eliminate some connectivity problems occurring at the protocol level
- ** Recommended MTU size on client side: 1300
- *** Press Refresh button to re-check IPsec tunnels' status
- **** Tunnel status description:

Figure 75 - IPsec start/stop page for GWR Router 2

- On the device connected on GWR router 2 setup default gateway 192.168.10.1.

Scenario #2

Router 1 and Router 2, presented in the *Figure 76*, will be in main mode.

Configurations for Router 1 and Router 2 are listed below.

The GWR Router 1 configuration:

Click *Network* Tab, to open the **LAN NETWORK** screen. Use this screen to configure LAN TCP/IP settings.

Configure IP address and Netmask:

- IP Address: 10.0.10.1
- Subnet Mask: 255.255.255.0
- Press *Save* to accept the changes.

Figure 76 – Network configuration page for GWR Router 1

- Use SIM card with a static IP address, obtained from Mobile Operator.
- Click *WAN Settings* Tab to configure parameters necessary for GSM/UMTS connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS connection (*WAN Settings* Tab). If disconnected please click *Connect* button.
- Click *VPN Settings* > *IPSEC* to configure IPSEC tunnel parameters. Click *Add New Tunnel* button to create new IPsec tunnel. Tunnel parameters are:
 - *Add New Tunnel*
 - Tunnel Name: test,
 - Enable: true.
 - *IPSec Setup*
 - Keying Mode: IKE with Preshared key,
 - Phase 1 DH group: Group 2,
 - Phase 1 Encryption: 3DES,
 - Phase 1 Authentication: MD5,
 - Phase 1 SA Life Time: 28800,
 - Perfect Forward Secrecy: true,
 - Phase 2 DH group: Group 2,
 - Phase 2 Encryption: DES,
 - Phase 2 Authentication: MD5,
 - Phase 2 SA Life Time: 3600,
 - Preshared Key: 1234567890.
 - *Local Group Setup*
 - Local Security Gateway Type: SIM card,
 - IP Address From: SIM 1 (WAN connection is established over SIM 1),
 - Custom Peer ID: false,

- Local Security Group Type: Subnet,
- IP Address: 10.0.10.0,
- Subnet Mask: 255.255.255.0.
- **Remote Group Setup**
 - Remote Security Gateway Type: IP Only,
 - IP Address: 172.29.8.5,
 - Custom Peer ID: false,
 - Remote Security Group Type: IP,
 - IP Address: 192.168.10.1.
- **Failover**
 - Enable IKE failover: false,
 - Enable Tunnel Failover: false.
- **Advanced**
 - Compress(Support IP Payload Compression Protocol(IPComp)): false,
 - Dead Peer Detection(DPD): false,
 - NAT Traversal: true,
 - Send Initial Contact: true.

The screenshot displays the configuration interface for a Device 2 Device Tunnel. It is organized into three main sections:

- Add New Tunnel:**
 - Tunnel Number: 1
 - Tunnel Name: test
 - Enable:
- Local Group Setup:**
 - Local Security Gateway Type: SIM Card
 - Custom Peer ID
 - IP Address From: SIM 1
 - Local Security Group Type: Subnet
 - IP Address: 10.0.10.0
 - Subnet Mask: 255.255.255.0
- Remote Group Setup:**
 - Remote Security Gateway Type: IP Only
 - IP Address: 172.29.8.5
 - Custom Peer ID
 - Remote Security Group Type: IP
 - IP Address: 192.168.10.1

Figure 77 - IPSEC configuration page I for GWR Router 1

IPSec Setup

Keying Mode: IKE with Preshared key
 Phase 1 DH Group: Group2
 Phase 1 Encryption: 3DES
 Phase 1 Authentication: MD5
 Phase 1 SA Life Time: 28800 sec
 Perfect Forward Secrecy:

Phase 2 DH Group: Group2
 Phase 2 Encryption: DES
 Phase 2 Authentication: MD5
 Phase 2 SA Life Time: 3600 sec
 Preshared Key: 1234567890

Failover

Enable IKE Failover
 IKE SA Retry:
 Restart PPP After IKE SA Retry Exceeds Specified Limit

Enable Tunnel Failover
 Ping IP:
 Ping Interval: sec
 Packet Size:
 Advanced Ping Interval: sec
 Advanced Ping Wait For A Response: sec
 Maximum Number Of Failed Packets: %

Figure 78 – IPSEC configuration page II for GWR Router 1

Advanced

Compress (Support IP Payload Compression Protocol (IPComp))
 Dead Peer Detection (DPD) sec
 NAT Traversal
 Send Initial Contact

Back
Reload
Save

Figure 79 – IPSEC configuration page III for GWR Router 1

NOTE: Firmware version used in this scenario also provides options for Connection mode of IPsec tunnel. If connection mode Connect is selected that indicates side of IPsec tunnel which sends requests for establishing of the IPsec tunnel. If connection mode Wait is selected that indicates side of IPsec tunnel which listens and responses to IPsec establishing requests from Connect side.

Internet Protocol Security Help

Summary

Tunnels used: 1
Maximum number of tunnels: 5

[Add New Tunnel](#) Log level: lifecycle

No.	Name	Enabled	Status	Enc/Auth/Grp	Advanced	Local Group	Remote Group	Remote Gateway	Action	Connection mode
1	Test	yes	connecting	Ph1:3DES/MD5/2 Ph2:DES/MD5/2	N/I	10.0.10.0 255.255.255.0	192.168.10.1	172.29.8.5	Edit Delete	Connect Wait

* Reducing the MTU size on the client side, can help eliminate some connectivity problems occurring at the protocol level
 -- Recommended MTU size on client side is 1300
 -- Tunnel status description:
 started - ipsec is running
 stopped - ipsec is not running or tunnel is not enabled
 connecting - ipsec is trying to establish connection
 waiting for connection - ipsec is waiting for other end to connect
 established - tunnel is up

Start
Stop
Refresh

Figure 80 – IPsec start/stop page for GWR Router 1

Click **Connect** button and after that **Start** button on **Internet Protocol Security** page to initiate IPSEC tunnel

- On the device connected on GWR router 1 setup default gateway 10.0.10.1.

The GWR Router 2 configuration:

- Click **Network** Tab, to open the **LAN NETWORK** screen. Use this screen to configure LAN TCP/IP settings. Configure IP address and Netmask.
 - IP Address: 192.168.10.1,
 - Subnet Mask: 255.255.255.0.
 Press **Save** to accept the changes.

Network ? Help

Network Settings

Obtain an IP address automatically using DHCP

Use the following IP address

IP Address

Subnet Mask

Local DNS

Local Gateway

Caution: Changes to IP Address, subnet mask and local DNS require a reboot to take effect.

Figure 81 – Network configuration page for GWR Router 2

- Use SIM card with a static IP address, obtained from Mobile Operator.
- Click **WAN Settings** Tab to configure parameters necessary for GSM/UMTS connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS connection (**WAN Settings** Tab). If disconnected please click **Connect** button.
- Click **VPN Settings > IPSEC** to configure IPSEC tunnel parameters. Click **Add New Tunnel** button to create new IPsec tunnel. Tunnel parameters are:
 - **Add New Tunnel**
 - Tunnel Name: test,
 - Enable: true.
 - **IPSec Setup**
 - Keying Mode: IKE with Preshared key,
 - Phase 1 DH group: Group 2,
 - Phase 1 Encryption: 3DES,
 - Phase 1 Authentication: MD5,
 - Phase 1 SA Life Time: 28800,
 - Perfect Forward Secrecy: true,
 - Phase 2 DH group: Group 2,
 - Phase 2 Encryption: DES,
 - Phase 2 Authentication: MD5,
 - Phase 2 SA Life Time: 3600,
 - Preshared Key: 1234567890.
 - **Local Group Setup**
 - Local Security Gateway Type: SIM card,
 - IP Address From: SIM 1 (WAN connection is established over SIM 1),
 - Custom Peer ID: false,
 - Local Security Group Type: IP,
 - IP Address: 192.168.10.1.
 - **Remote Group Setup**
 - Remote Security Gateway Type: IP Only,
 - IP Address: 172.29.8.4,
 - Custom Peer ID: false,

- Remote Security Group Type: Subnet,
 - IP Address: 10.0.10.0,
 - Subnet: 255.255.255.0.
 - **Failover**
 - Enable IKE failover: false,
 - Enable Tunnel Failover: false.
 - **Advanced**
 - Compress(Support IP Payload Compression Protocol(IPComp)): false,
 - Dead Peer Detection(DPD): false,
 - NAT Traversal: true,
 - Send Initial Contact: true.
- Press *Save* to accept the changes.

Device 2 Device Tunnel
Help

Add New Tunnel

Tunnel Number

Tunnel Name

Enable

Local Group Setup

Local Security Gateway Type

Custom Peer ID

IP Address From

Local Security Group Type

IP Address

Remote Group Setup

Remote Security Gateway Type

IP Address

Custom Peer ID

Remote Security Group Type

IP Address

Subnet Mask

Figure 82 - IPSEC configuration page I for GWR Router 2

IPSec Setup

Keying Mode: IKE with Preshared key ▼

Phase 1 DH Group: Group2 ▼

Phase 1 Encryption: 3DES ▼

Phase 1 Authentication: MD5 ▼

Phase 1 SA Life Time: 28800 sec

Perfect Forward Secrecy:

Phase 2 DH Group: Group2 ▼

Phase 2 Encryption: DES ▼

Phase 2 Authentication: MD5 ▼

Phase 2 SA Life Time: 3600 sec

Preshared Key:

1234567890

Failover

Enable IKE Failover

IKE SA Retry:

Restart PPP After IKE SA Retry Exceeds Specified Limit

Enable Tunnel Failover

Ping IP:

Ping Interval: sec

Packet Size:

Advanced Ping Interval: sec

Advanced Ping Wait For A Response: sec

Maximum Number Of Failed Packets: %

Figure 83 – IPSEC configuration page II for GWR Router 2

Advanced

Compress (Support IP Payload Compression Protocol (IPComp))

Dead Peer Detection (DPD) sec

NAT Traversal

Send Initial Contact

Back
Reload
Save

Figure 84 – IPSEC configuration page III for GWR Router 2

Internet Protocol Security Help

Summary

Tunnels used: 1

Maximum number of tunnels: 5

Log level: lifecycle ▼

No.	Name	Enabled	Status	Enc/Auth/Grp	Advanced	Local Group	Remote Group	Remote Gateway	Action	Connection mode
1	Test	yes	waiting for connection	Ph1:3DES/MD5/2 Ph2:DES/MD5/2	N/A	192.168.10.1	10.0.10.0 255.255.255.0	172.29.8.4	Edit	Delete Connect Wait

Start
Stop
Refresh

* Reducing the MTU size on the client side, can help eliminate some connectivity problems occurring at the protocol level
 ** Recommended MTU size on client side is 1300
 *** Tunnel status description:
 started - ipsec is running
 stopped - ipsec is not running or tunnel is not enabled
 connecting - ipsec is trying to establish connection
 waiting for connection - ipsec is waiting for other end to connect
 established - tunnel is up

Figure 85 – IPsec start/stop page for GWR Router 1

Click *Wait* button and after that *Start* button on *Internet Protocol Security* page to initiate IPSEC tunnel.

- On the device connected on GWR router 2 setup default gateway 192.168.10.1.

Scenario #3

Gateway 1 and Gateway 2, are configured with IPsec tunnel in Main mode. Configurations for Router 1 and Router 2 are listed below.

- Click *VPN Settings* > *IPSEC* to configure IPSEC tunnel parameters. Click *Add New Tunnel* button to create new IPsec tunnel. Tunnel parameters are:
 - *Add New Tunnel*
 - Tunnel Name: test,
 - Enable: true.
 - *IPSec Setup*
 - Keying Mode: IKE with Preshared key,
 - Mode: main
 - Phase 1 DH group: Group 2,
 - Phase 1 Encryption: AES-128,
 - Phase 1 Authentication:MD5,
 - Phase 1 SA Life Time: 28800,
 - Perfect Forward Secrecy: false,
 - Phase 2 DH group: Group 2,
 - Phase 2 Encryption: AES-128,
 - Phase 2 Authentication:MD5,
 - Phase 2 SA Life Time: 3600,
 - Preshared Key: 1234567890,
 - *Local Group Setup*
 - Local Security Gateway Type: IP Only,
 - IP Address: 172.27.234.26
 - Local ID Type: User FQDN
 - Local User FQDN ID: alexander@zeitgeist.se,
 - IP Address: 192.168.223.0,
 - Subnet Mask: 255.255.255.0.
 - *Remote Group Setup*
 - Remote Security Gateway Type: IP Only,
 - IP Address: 172.27.234.56,
 - Remote ID Type: FQDN,
 - Remote FQDN ID: @vpn.zeitgeist.se,
 - IP Address: 192.168.222.0,
 - Subnet Mask: 255.255.255.0

Device 2 Device Tunnel
Help

Add New Tunnel

Tunnel Number:

Tunnel Name:

Enable:

Local Group Setup

Local Security Gateway Type:

IP Address:

Local ID Type:

Local User FQDN ID:

Local Security Group Type:

IP Address:

Subnet Mask:

Remote Group Setup

Remote Security Gateway Type:

IP Address:

Remote ID Type:

Remote FQDN ID:

Remote Security Group Type:

IP Address:

Subnet Mask:

Figure 86 – IPSEC configuration page I for GWG Gateway 1

IPSec Setup

Keying Mode:

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Life Time: sec

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Life Time: sec

Preshared Key:

Failover

Enable IKE Failover

IKE SA Retry:

Restart PPP After IKE SA Retry Exceeds Specified Limit

Enable Tunnel Failover

Ping IP:

Ping Interval: sec

Packet Size:

Advanced Ping Interval: sec

Advanced Ping Wait For A Response: sec

Maximum Number Of Failed Packets: %

Figure 87 – IPSEC configuration page II for GWG Gateway 1

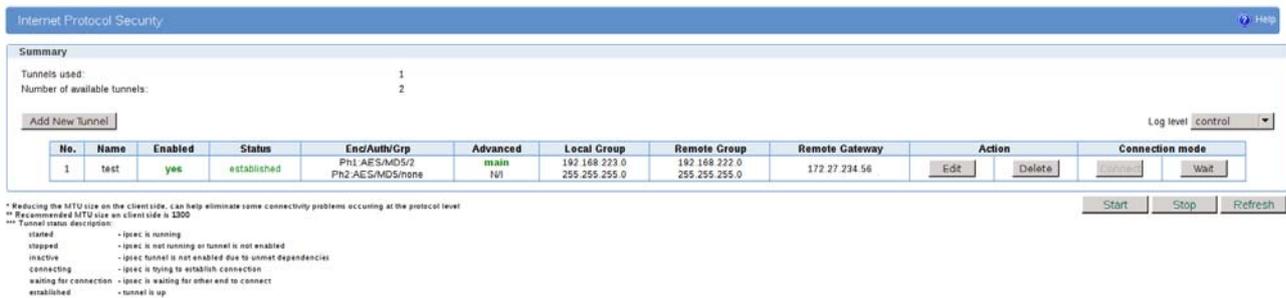


Figure 88 – IPSec start/stop page for GWG Gateway 1

Click **Start** button and after that **Connect** button on **Internet Protocol Security** page to initiate IPSEC tunnel.

The GWG Gateway 2 configuration:

- Click **VPN Settings > IPSEC** to configure IPSEC tunnel parameters. Click **Add New Tunnel** button to create new IPsec tunnel. Tunnel parameters are:
 - **Add New Tunnel**
 - Tunnel Name: test
 - Enable: true
 - **IPSec Setup**
 - Keying Exchange Mode: IKE with X509 certificates and PSK file
 - Mode: main
 - Phase 1 DH group: Group 2
 - Phase 1 Encryption: AES-128
 - Phase 1 Authentication: MD5
 - Phase 1 SA Life Time: 28800
 - Perfect Forward Secrecy: false
 - Phase 2 Encryption: AES-128
 - Phase 2 Authentication: MD5
 - Phase 2 SA Life Time: 3600
 - Preshared Key: 1234567890
 - **Local Group Setup**
 - Local Security Gateway Type: IP Only
 - IP Address: 172.27.234.56
 - Local ID Type: FQDN
 - Local FQDN ID: @VPNzeitgeist.se
 - IP Address: 192.168.222.0
 - Subnet Mask: 255.255.255.0
 - **Remote Group Setup**
 - Remote Security Gateway Type: IP Only
 - IP Address: 172.27.234.26
 - Remote ID Type: User FQDN
 - Remote User FQDN ID: alexander@zeitgeist.se
 - IP Address: 192.168.223.0
 - Subnet: 255.255.255.0

Device 2 Device Tunnel Help

Add New Tunnel

Tunnel Number:
 Tunnel Name:
 Enable:

Local Group Setup

Local Security Gateway Type:
 IP Address:
 Local ID Type:
 Local FQDN ID:
 Local Security Group Type:
 IP Address:
 Subnet Mask:

Remote Group Setup

Remote Security Gateway Type:
 IP Address:
 Remote ID Type:
 Remote User FQDN ID:
 Remote Security Group Type:
 IP Address:
 Subnet Mask:

Figure 89 – IPSEC configuration page I for GWG Gateway 2

IPSec Setup

Keying Mode:
 Phase 1 DH Group:
 Phase 1 Encryption:
 Phase 1 Authentication:
 Phase 1 SA Life Time: sec
 Perfect Forward Secrecy:

Phase 2 DH Group:
 Phase 2 Encryption:
 Phase 2 Authentication:
 Phase 2 SA Life Time: sec

Preshared Key:

Failover

Enable IKE Failover
 IKE SA Retry:
 Restart PPP After IKE SA Retry Exceeds Specified Limit

Enable Tunnel Failover
 Ping IP:
 Ping Interval: sec
 Packet Size:
 Advanced Ping Interval: sec
 Advanced Ping Wait For A Response: sec
 Maximum Number Of Failed Packets: %

Figure 90 – IPSEC configuration page II for GWG Gateway 2

Internet Protocol Security
Help

Summary

Tunnels used: 1
 Number of available tunnels: 2

Log level: control

[Add New Tunnel](#)

No.	Name	Enabled	Status	Enc/Auth/Grp	Advanced	Local Group	Remote Group	Remote Gateway	Action		Connection mode	
1	test	yes	established	Ph1 AES/MD5/2 Ph2 AES/MD5/none	main	192.168.222.0 255.255.255.0	192.168.233.0 255.255.255.0	172.27.234.26	Edit	Delete	Connect	Wait

* Reducing the MTU size on the client side, can help eliminate some connectivity problems occurring at the protocol level
 ** Recommended MTU size on Client side is 1300
 *** Tunnel status description:
 started - ipsec is running
 stopped - ipsec is not running or tunnel is not enabled
 inactive - ipsec tunnel is not enabled due to unmet dependencies
 connecting - ipsec is trying to establish connection
 waiting for connection - ipsec is waiting for other end to connect
 established - tunnel is up

[Start](#) [Stop](#) [Refresh](#)

Figure 91 – IPsec start/stop page for GWG Gateway 1

Click *Start* button and after that *Wait* button on *Internet Protocol Security* page to initiate IPSEC tunnel.

IPSec Tunnel configuration between GWR Router and Cisco Router

IPSec tunnel is a type of a VPN tunnels with a secure tunneling method. On the diagram below **Error! Reference source not found.** is illustrated simple network with GWR Router and Cisco Router. Idea is to create IPSec tunnel for LAN to LAN (site to site) connectivity.

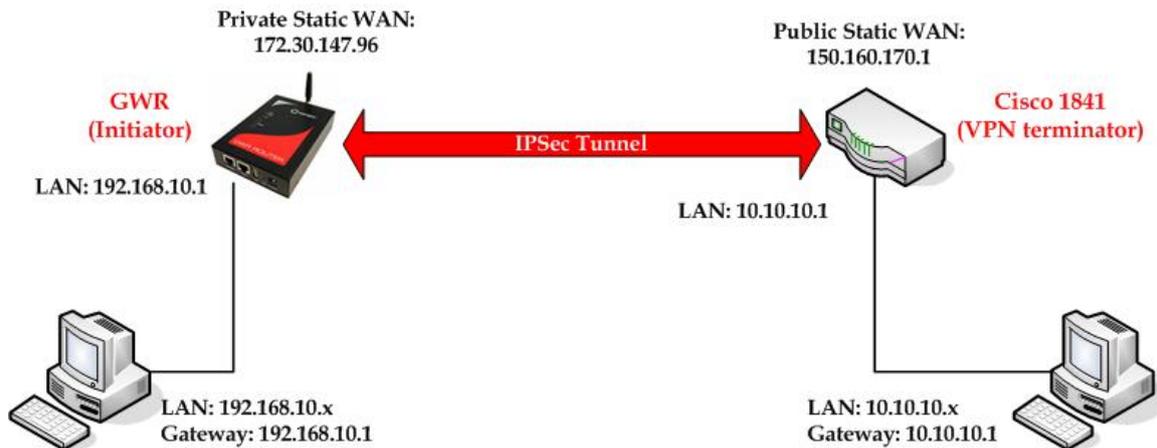


Figure 92 – IPSec tunnel between GWR Router and Cisco Router

The GWR Routers requirements:

- Static IP WAN address for tunnel source and tunnel destination address,
- Dynamic IP WAN address must be mapped to hostname with DynDNS service (for synchronization with DynDNS server SIM card must have internet access).

GSM/UMTS APN Type: For GSM/UMTS networks GWR Router connections may require a Custom APN. A Custom APN allows for various IP addressing options, particularly static IP addresses, which are needed for most VPN connections. A custom APN should also support mobile terminated data that may be required in most site-to-site VPNs.

The GWR Router configuration:

- Click **Network** Tab, to open the **LAN NETWORK** screen. Use this screen to configure LAN TCP/IP settings. Configure IP address and Netmask.
 - IP Address: 192.168.10.1,
 - Subnet Mask: 255.255.255.0.
 Press **Save** to accept the changes.



Figure 93 – Network configuration page for GWR Router

- Click *WAN Settings* Tab to configure parameters necessary for GSM/UMTS connection. All parameters necessary for connection configuration should be required from mobile operator.
 - Check the status of GSM/UMTS connection (*WAN Settings* Tab). If disconnected please click *Connect* button.
 - Click *VPN Settings > IPSEC* to configure IPSEC tunnel parameters. Click *Add New Tunnel* button to create new IPsec tunnel. Tunnel parameters are:
 - *Add New Tunnel*
 - Tunnel Name: test,
 - Enable: true.
 - *IPSec Setup*
 - Keying Mode: IKE with Preshared key,
 - Phase 1 DH group: Group 2,
 - Phase 1 Encryption: 3DES,
 - Phase 1 Authentication: SHA,
 - Phase 1 SA Life Time: 28800,
 - Phase 2 Encryption: 3DES,
 - Phase 2 Authentication: SHA1,
 - Phase 2 SA Life Time: 3600,
 - Preshared Key: 1234567890.
 - *Local Group Setup*
 - Local Security Gateway Type: SIM card,
 - IP Address From: SIM 1 (WAN connection is established over SIM 1),
 - Local ID Type: IP Address,
 - Local Security Group Type: Subnet,
 - IP Address: 192.168.10.0,
 - Subnet Mask: 255.255.255.0.
 - *Remote Group Setup*
 - Remote Security Gateway Type: IP Only,
 - IP Address: 150.160.170.1,
 - Remote ID Type: IP Address,
 - Remote Security Group Type: Subnet,
 - IP Address: 10.10.10.0,
 - Subnet Mask: 255.255.255.0.
 - *Failover*
 - Enable Tunnel Failover: false.
 - *Advanced*
 - Negotiation Mode: Aggressive,
 - Compress(Support IP Payload Compression Protocol(IPComp)): false,
 - Dead Peer Detection(DPD): false,
 - NAT Traversal: true,
 - Send Initial Contact Notification: true.
- Press *Save* to accept the changes.

IPSec Setup

Keying Mode: IKE with Preshared key

Phase 1 DH Group: Group2

Phase 1 Encryption: 3DES

Phase 1 Authentication: SHA1

Phase 1 SA Life Time: 28800 sec

Perfect Forward Secrecy:

Phase 2 Encryption: 3DES

Phase 2 Authentication: SHA1

Phase 2 SA Life Time: 3600 sec

Preshared Key: 1234567890

Figure 94 – IPSEC configuration page I for GWR Router

Local Group Setup

Local Security Gateway Type: SIM Card

IP Address From: SIM 1

Local ID Type: IP Address

Local Security Group Type: Subnet

IP Address: 192.168.10.0

Subnet Mask: 255.255.255.0

Remote Group Setup

Remote Security Gateway Type: IP Only

IP Address: 150.160.170.1

Remote ID Type: IP Address

Remote Security Group Type: Subnet

IP Address: 10.10.10.0

Subnet Mask: 255.255.255.0

Figure 95 – IPSEC configuration page II for GWR Router

Failover

Enable Tunnel Failover

Ping IP: [text box]

Ping Interval: [text box] sec

Packet Size: [text box]

Advanced Ping Interval: [text box] sec

Advanced Ping Wait For A Response: [text box] sec

Maximum Number Of Failed Packets: [text box] %

Advanced

Negotiation Mode: Aggressive

Compression (IPComp)

Dead Peer Detection (DPD) [text box] sec

NAT Traversal

Send Initial Contact

[Back] [Reload] [Save]

Figure 96 – IPSEC configuration page III for GWR Router

- Click **Start** button on **Internet Protocol Security** page to initiate IPSEC tunnel.

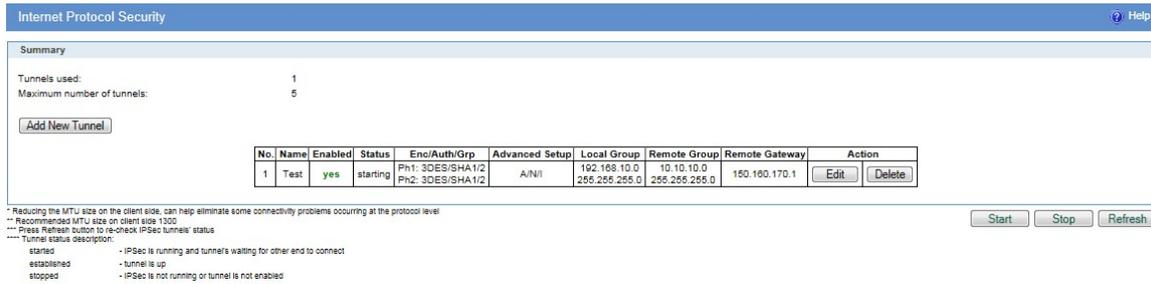


Figure 97 – IPSec start/stop page for GWR Router

- On the device connected on GWR router setup default gateway 192.168.10.1.

The Cisco Router configuration:

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Cisco-Router
!
boot-start-marker
boot-end-marker
!
username admin password 7 *****
!
enable secret 5 *****
!
no aaa new-model
!
no ip domain lookup
!
!--- Keyring that defines wildcard pre-shared key.
!
crypto keyring remote
  pre-shared-key address 0.0.0.0 0.0.0.0 key 1234567890
!
!--- ISAKMP policy
!
crypto isakmp policy 10
  encr 3des
  authentication pre-share
  group 2
  lifetime 28800
!
!--- Profile for LAN-to-LAN connection, that references
!--- the wildcard pre-shared key and a wildcard identity
!
crypto isakmp profile L2L
  description LAN to LAN vpn connection
  keyring remote
  match identity address 0.0.0.0
!
!
crypto ipsec transform-set testGWR esp-3des esp-sha-hmac
!
!--- Instances of the dynamic crypto map
!--- reference previous IPsec profile.
!
crypto dynamic-map dynGWR 5
  set transform-set testGWR
  set isakmp-profile L2L
  match address 121
!
!--- Crypto-map only references instances of the previous dynamic crypto map.
!
crypto map GWR 10 ipsec-isakmp dynamic dynGWR
!
interface FastEthernet0/0
  description WAN INTERFACE
  
```

```

ip address 150.160.170.1 255.255.255.252
ip nat outside
no ip route-cache
no ip mroute-cache
duplex auto
speed auto
crypto map GWR
!
interface FastEthernet0/1
description LAN INTERFACE
ip address 10.10.10.1 255.255.255.0
ip nat inside
no ip route-cache
no ip mroute-cache
duplex auto
speed auto
!
ip route 0.0.0.0 0.0.0.0 150.160.170.2
!
ip http server
no ip http secure-server
ip nat inside source list nat_list interface FastEthernet0/0 overload
!

ip access-list extended nat_list
deny ip 10.10.10.0 0.0.0.255 192.168.10.0 0.0.0.255
permit ip 10.10.10.0 0.0.0.255 any
ip access-list extended 121 permit ip 10.10.10.0 0.0.0.255 192.168.10.0 0.0.0.255
!
access-list 23 permit any
!
line con 0
line aux 0
line vty 0 4
access-class 23 in
privilege level 15
login local
transport input telnet ssh
line vty 5 15
access-class 23 in
privilege level 15
login local
transport input telnet ssh
!
end

```

Use this section to confirm that your configuration works properly. Debug commands that run on the Cisco router can confirm that the correct parameters are matched for the remote connections.

- **show ip interface** – Displays the IP address assignment to the spoke router.
- **show crypto isakmp sa detail** – Displays the IKE SAs, which have been set-up between the IPsec initiators.
- **show crypto ipsec sa** – Displays the IPsec SAs, which have been set-up between the IPsec initiators.
- **debug crypto isakmp** – Displays messages about Internet Key Exchange (IKE) events.
- **debug crypto ipsec** – Displays IPsec events.
- **debug crypto engine** – Displays crypto engine events.

IPSec Tunnel configuration between GWR Router and Juniper SSG firewall

IPSec tunnel is a type of a VPN tunnels with a secure tunneling method. On the diagram below *Figure 98* is illustrated simple network with GWR Router and Cisco Router. Idea is to create IPSec tunnel for LAN to LAN (site to site) connectivity.

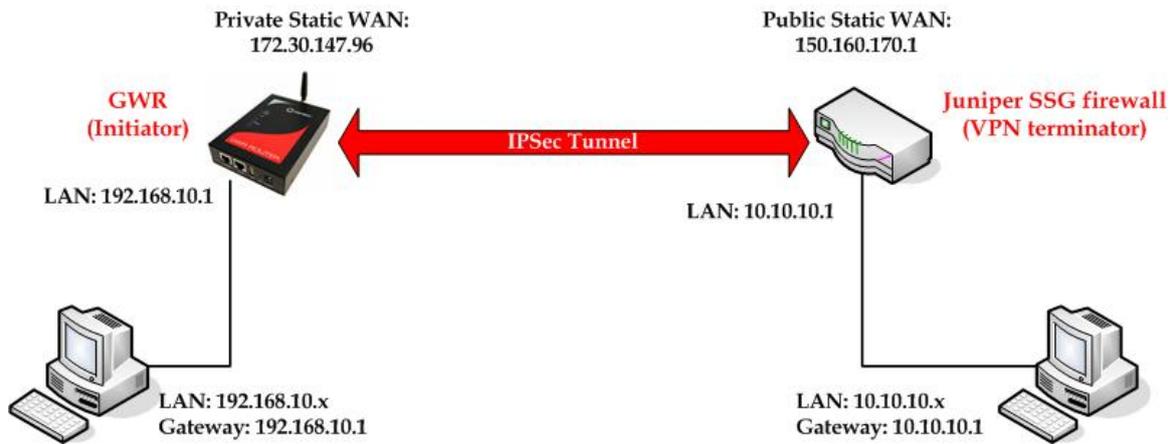


Figure 98 – IPsec tunnel between GWR Router and Cisco Router

The GWR Routers requirements:

- Static IP WAN address for tunnel source and tunnel destination address,
- Source tunnel address should have static WAN IP address,
- Destination tunnel address should have static WAN IP address.

GSM/UMTS APN Type: For GSM/UMTS networks GWR Router connections may require a Custom APN. A Custom APN allows for various IP addressing options, particularly static IP addresses, which are needed for most VPN connections. A custom APN should also support mobile terminated data that may be required in most site-to-site VPNs.

The GWR Router configuration:

- Click *Network* Tab, to open the **LAN NETWORK** screen. Use this screen to configure LAN TCP/IP settings. Configure IP address and Netmask.
 - IP Address: 192.168.10.1,
 - Subnet Mask: 255.255.255.0,
 - Press *Save* to accept the changes.

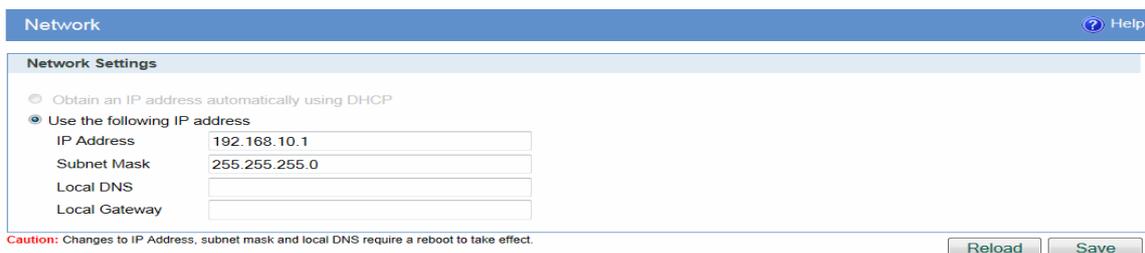


Figure 99 – Network configuration page for GWR Router

- Use SIM card with a static IP address, obtained from Mobile Operator.
- Click *WAN Settings* Tab to configure parameters necessary for GSM/UMTS connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS connection (*WAN Settings* Tab). If disconnected please click *Connect* button.
- Click *VPN Settings > IPSEC* to configure IPSEC tunnel parameters. Click *Add New Tunnel* button to create new IPsec tunnel. Tunnel parameters are:
 - *Add New Tunnel*
 - Tunnel Name: test,

- Enable: true.
- **Local Group Setup**
 - Local Security Gateway Type: IP Only,
 - IP Address: 172.30.147.96,
 - Local ID Type: Custom,
 - Custom Peer ID: 172.30.147.96,
 - Local Security Group Type: Subnet,
 - IP Address: 192.168.10.0,
 - Subnet Mask: 255.255.255.0.
- **Remote Group Setup**
 - Remote Security Gateway Type: IP Only,
 - IP Address: 150.160.170.1,
 - Remote ID Type: Custom,
 - Custom Peer ID: 150.160.170.1,
 - Remote Security Group Type: IP,
 - IP Address: 10.10.10.0,
 - Subnet Mask: 255.255.255.0.
- **IPSec Setup**
 - Keying Mode: IKE with Preshared key,
 - Phase 1 DH group: Group 2,
 - Phase 1 Encryption: 3DES,
 - Phase 1 Authentication: SHA1,
 - Phase 1 SA Life Time: 28800,
 - Perfect Forward Secrecy: true,
 - Phase 2 DH group: Group 2,
 - Phase 2 Encryption: 3DES,
 - Phase 2 Authentication: SHA1,
 - Phase 2 SA Life Time: 3600,
 - Preshared Key: 1234567890.
- **Advanced**
 - Aggressive Mode: true,
 - Compress(Support IP Payload Compression Protocol(IPComp)): false,
 - Dead Peer Detection(DPD): false,
 - NAT Traversal: true,
 - Press *Save* to accept the changes.

Device to Device Tunnel
Help

Add New Tunnel

Tunnel Number:

Tunnel Name:

Enable:

IPSec Setup

Keying Mode:

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Life Time: sec

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Life Time: sec

Preshared Key:

Figure 100 – IPSEC configuration page I for GWR Router

Local Group Setup

Local Security Gateway Type:

IP Address:

Local ID Type:

Custom Peer ID:

Local Security Group Type:

IP Address:

Subnet Mask:

Remote Group Setup

Remote Security Gateway Type:

IP Address:

Remote ID Type:

Custom Peer ID:

Remote Security Group Type:

IP Address:

Subnet Mask:

Figure 101 – IPsec configuration page II for GWR Router

Failover

Enable Tunnel Failover
 Ping IP
 Ping Interval sec
 Packet Size
 Advanced Ping Interval sec
 Advanced Ping Wait For A Response sec
 Maximum Number Of Failed Packets %

Advanced

Negotiation Mode Aggressive ▾
 Compression (IPComp)
 Dead Peer Detection (DPD) sec
 NAT Traversal
 Send Initial Contact

Figure 102 - IPsec configuration page III for GWR Router

- Click **Start** button on **Internet Protocol Security** page to initiate IPSEC tunnel.

Internet Protocol Security ? Help

Summary

Tunnels used: 1
 Maximum number of tunnels: 5

No.	Name	Enabled	Status	Enc/Auth/Grp	Advanced Setup	Local Group	Remote Group	Remote Gateway	Action
1	Test	yes	starting	Ph1: 3DES/SHA1/2 Ph2: 3DES/SHA1/2	A/N/I	192.168.10.0 255.255.255.0	10.10.10.0 255.255.255.0	150.160.170.1	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

* Reducing the MTU size on the client side, can help eliminate some connectivity problems occurring at the protocol level

** Recommended MTU size on client side: 1300

*** Press Refresh button to re-check IPSEC tunnels' status

**** Tunnel status description:

started - IPsec is running and tunnel is waiting for other end to connect

established - tunnel is up

stopped - IPsec is not running or tunnel is not enabled

Figure 103 - IPsec start/stop page for GWR Router

- On the device connected on GWR router setup default gateway 192.168.10.1.

The Juniper SSG firewall configuration:

Step1 - Create New Tunnel Interface

- Click Interfaces on Network Tab.

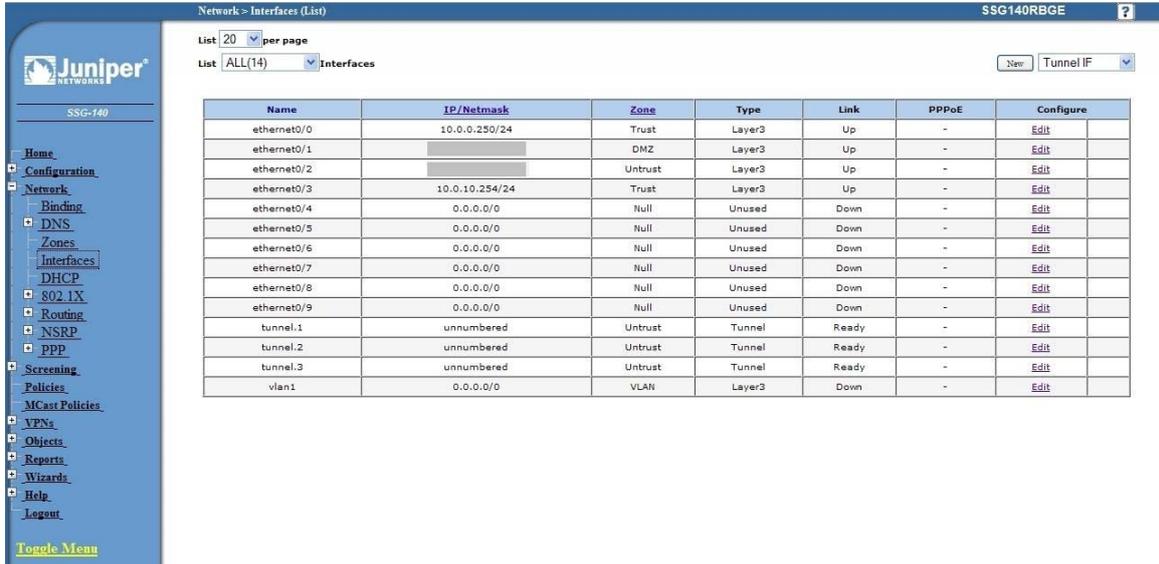


Figure 104 – Network Interfaces (list)

- Bind New tunnel interface to Untrust interface (outside int – with public IP address).
- Use unnumbered option for IP address configuration.

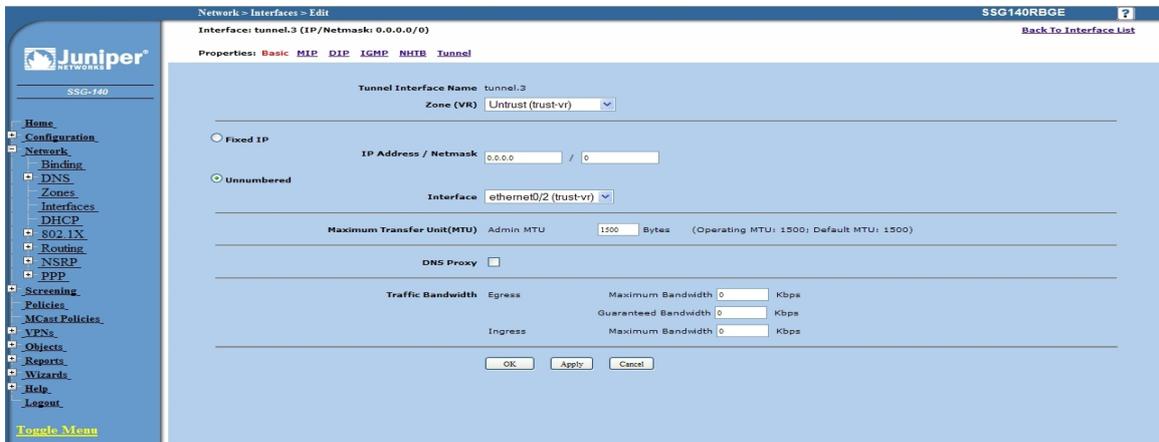


Figure 105 – Network Interfaces (edit)

Step 2 – Create New VPN IPSEC tunnel

- Click *VPNs* in main menu. To create new gateway click *Gateway* on *AutoKey Advanced* tab.

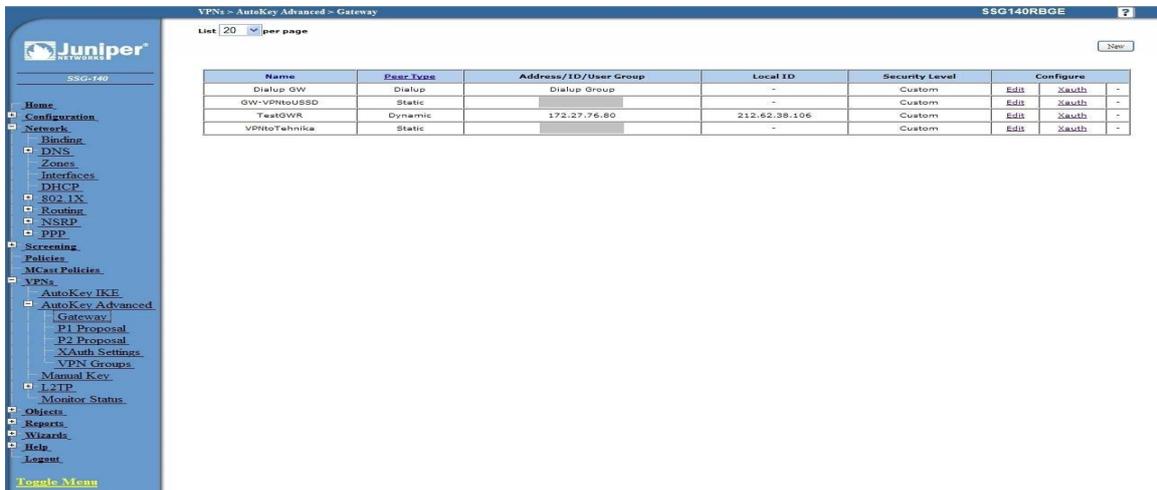


Figure 106 – AutoKey Advanced Gateway

- Click *New* button. Enter gateway parameters:
 - **Gateway name:** TestGWR,
 - **Security level:** Custom,
 - **Remote Gateway type:** Dynamic IP address(because your GWR router are hidden behind Mobile operator router’s (firewall) NAT),
 - **Peer ID:** 172.30.147.96,
 - **Presharedkey:** 1234567890,
 - **Local ID:** 150.160.170.1.

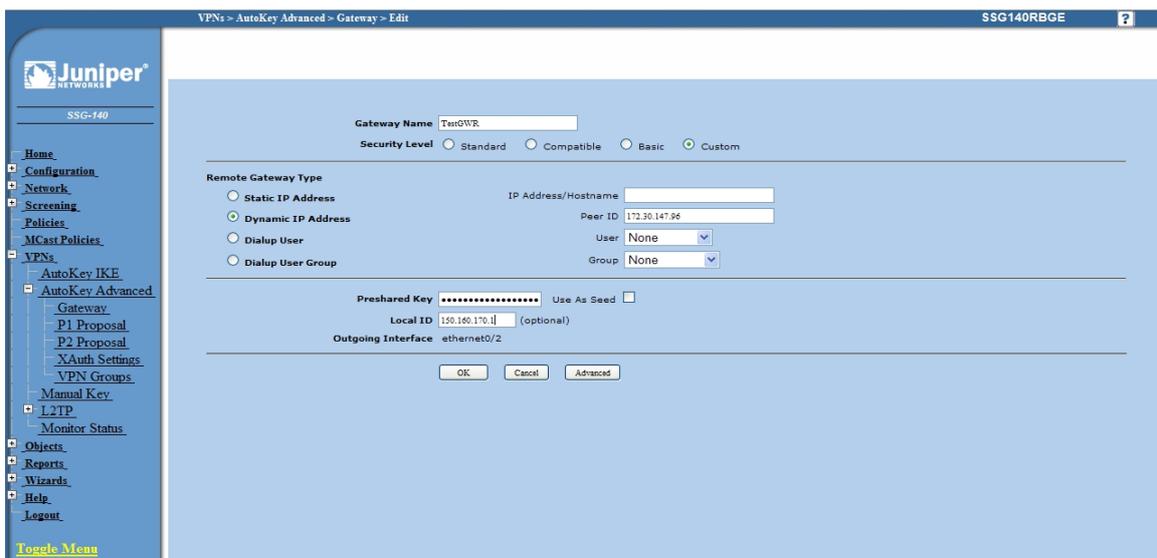


Figure 107 – Gateway parameters

- Click *Advanced* button.
 - **Security level – User Defined:** custom,

- **Phase 1 proposal:** pre-g2-3des-sha,
- **Mode:** Aggressive(must be aggressive because of NAT),
- **Nat-Traversal:** enabled,
- Click *Return* and *OK*.

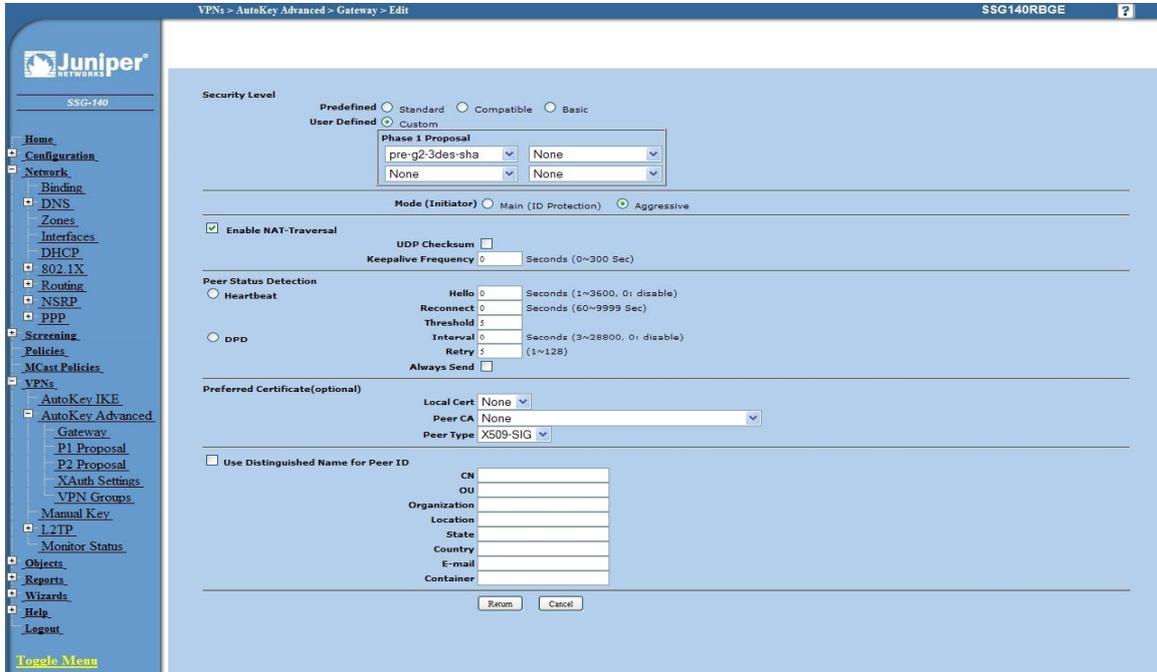


Figure 108 - Gateway advanced parameters

Step 3 - Create AutoKey IKE

- Click *VPNs* in main menu. Click *AutoKey IKE*.
- Click *New* button.

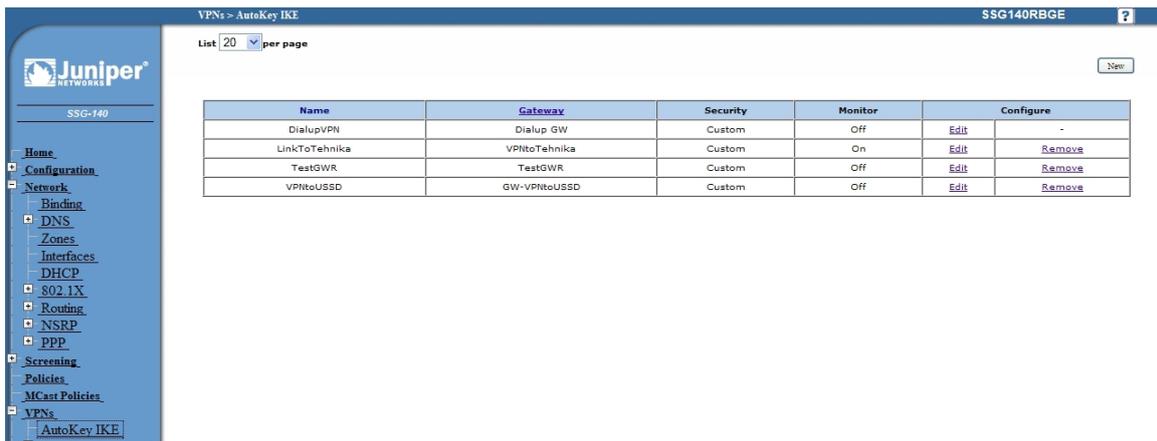


Figure 109 - AutoKey IKE

AutoKey IKE parameters are:

- **VPNname:** TestGWR,
- **Security level:** Custom,

- Remote Gateway: Predefined,
- Choose VPN Gateway from step 2.

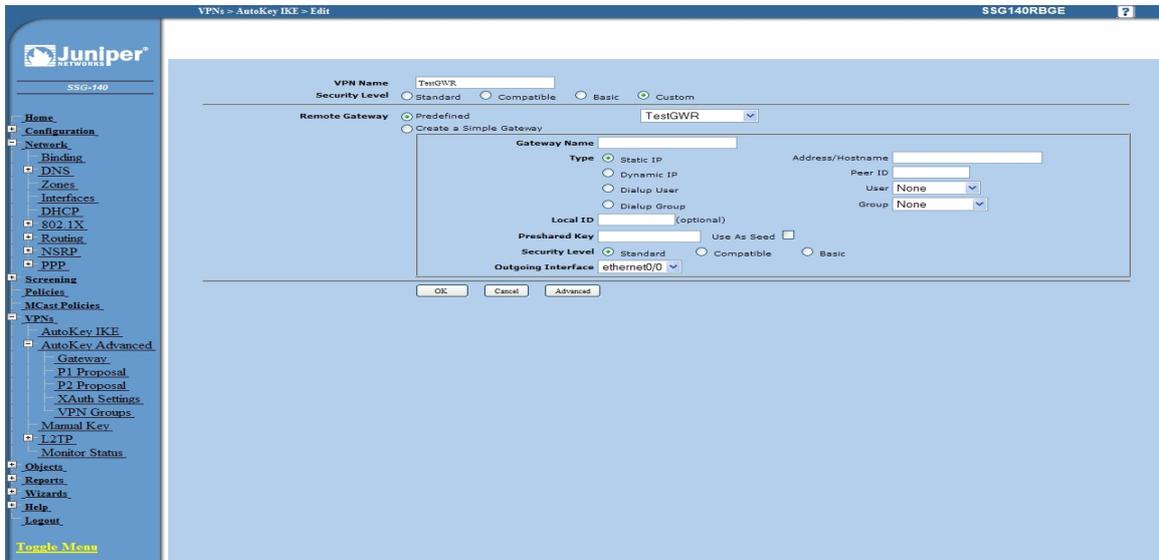


Figure 110 – AutoKey IKE parameters

- Click *Advanced* button.
 - Security level - User defined: custom,
 - Phase 2 proposal: pre-g2-3des-sha,
 - Bind to - Tunnel interface: tunnel.3(from step 1),
 - Proxy ID: Enabled,
 - LocalIP/netmask: 10.10.10.0/24,
 - RemoteIP/netmask: 192.168.10.0/24,
 - Click *Return* and *OK*.

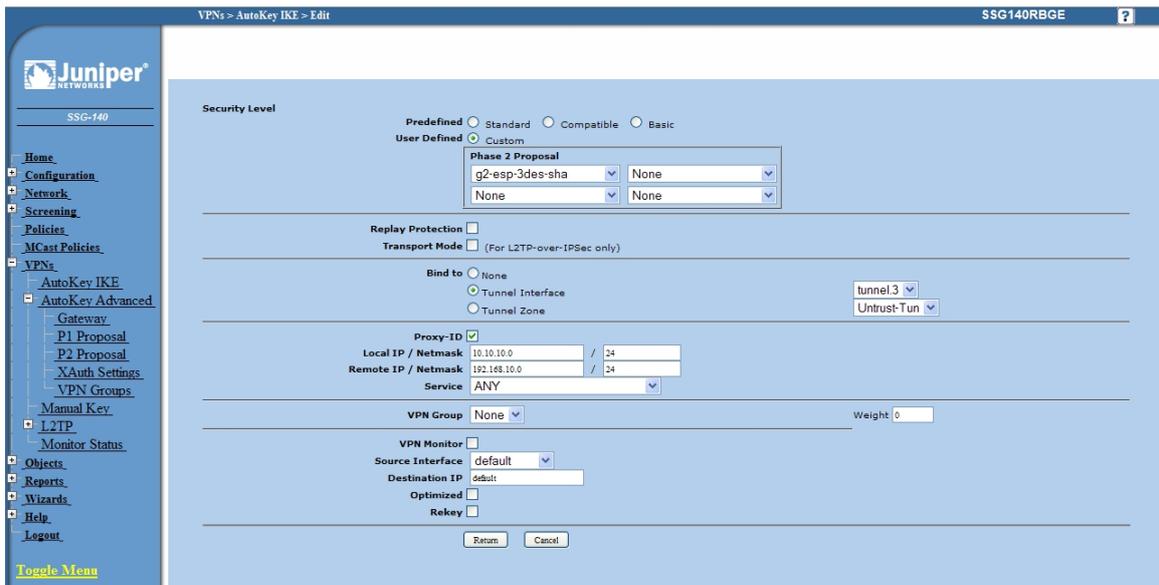


Figure 111 – AutoKey IKE advanced parameters

Step 4 - Routing

- Click *Destination* tab on *Routing* menu.
- Click *New* button. Routing parameters are:
 - **IP Address:** 192.168.10.0/24,
 - **Gateway:** tunnel.3(tunnel interface from step 1),
 - Click *OK*.

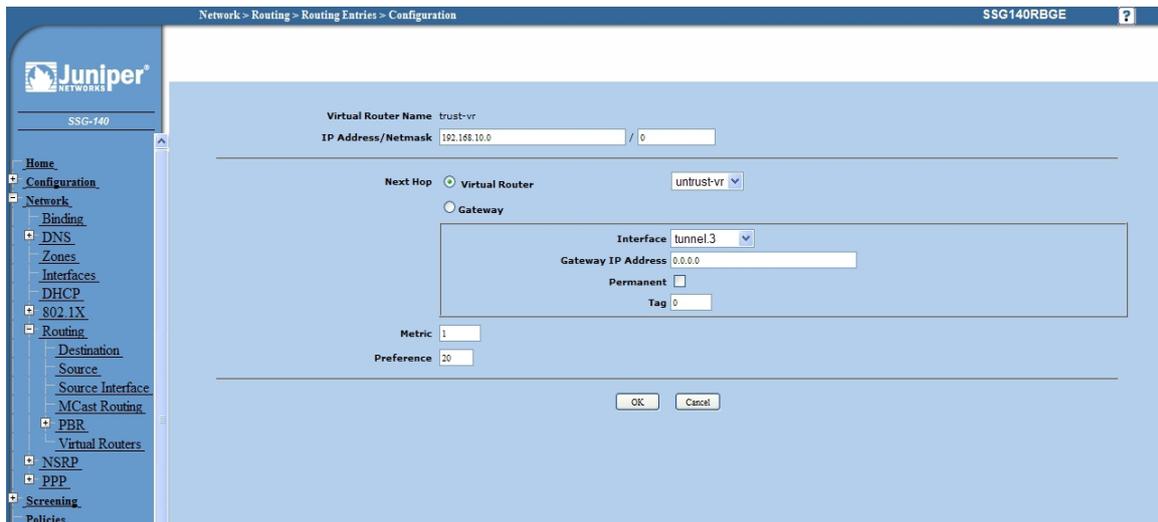


Figure 112 - Routing parameters

Step 5 - Policies

- Click *Policies* in main menu.
- Click *New* button (from Untrust to trust zone),
 - **Source Address:** 192.168.10.0/24,
 - **Destination Address:** 10.10.10.0/24,
 - **Services:** Any.
- Click *OK*.

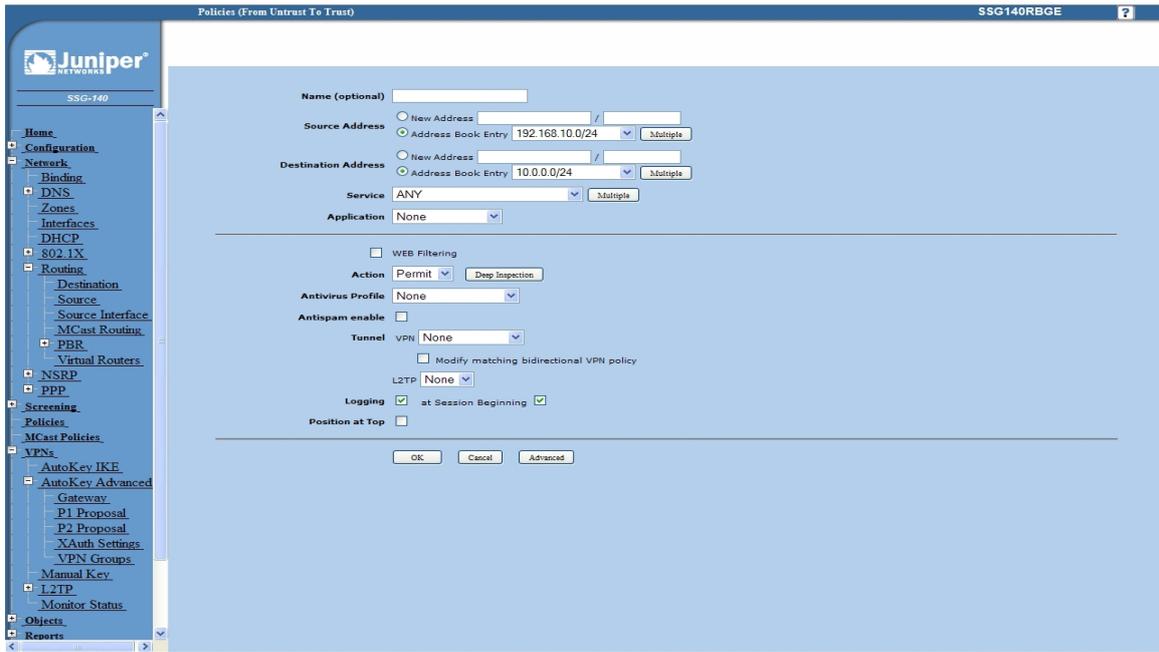


Figure 113 – Policies from untrust to trust zone

- Click *Policies* in main menu.
- Click *New* button (from trust to untrust zone),
 - **Source Address:** 10.10.10.0/24,
 - **Destination Address:** 192.168.10.0/24,
 - **Services:** Any.
- Click *OK*.

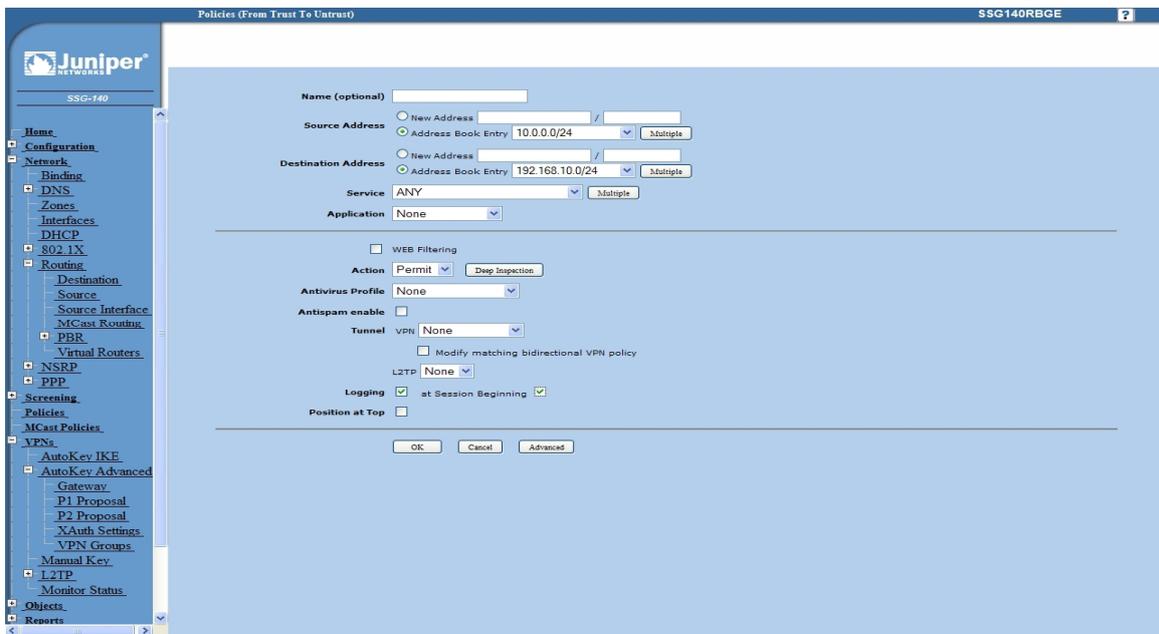


Figure 114 – Policies from trust to untrust zone

Appendix

A. How to Achieve Maximum Signal Strength with GWR Router?

The best throughput comes from placing the device in an area with the greatest Received Signal Strength Indicator (RSSI). RSSI is a measurement of the Radio Frequency (RF) signal strength between the base station and the mobile device, expressed in dBm. The better the signal strength, the less data retransmission and, therefore, better throughput.

RSSI information is available from several sources:

- The LEDs on the device give a general indication.
- Via the GWR Router local user interface.

Signal strength LED indicator:

- -101 or less dBm = Unacceptable (running LED),
- -100 to -91 dBm = Weak (1 LED),
- -90 to -81 dBm = Moderate (2 LED),
- -80 to -75 dBm = Good (3 LED),
- -74 or better dBm = Excellent (4 LED),
- 0 is not known or not detectable (running LED).

Antenna placement

Placement can drastically increase the signal strength of a cellular connection. Often times, just moving the router closer to an exterior window or to another location within the facility can result in optimum reception.

Another way of increasing throughput is by physically placing the device on the roof of the building (in an environmentally safe enclosure with proper moisture and lightning protection).

- Simply install the GWR Router outside the building and run an RJ-45 Ethernet cable to your switch located in the building.
- Keep antenna cable away from interferers (AC wiring).

Antenna Options

Once optimum placement is achieved, if signal strength is still not desirable, you can experiment with different antenna options. Assuming you have tried a standard antenna, next consider:

- Check your antenna connection to ensure it is properly attached.
- High gain antenna, which has higher dBm gain and longer antenna. Many cabled antennas require a metal ground plane for maximum performance. The ground plane typically should have a diameter roughly twice the length of the antenna.

NOTE: Another way of optimizing throughput is by sending non-encrypted data through the device. Application layer encryption or VPN put a heavy toll on bandwidth utilization. For example, IPsec ESP headers and trailers can add 20-30% or more overhead.

GENEKO

Bul. Despota Stefana 59a
11000 Belgrade • Serbia

Phone: +381 11 3340-591, 3340-178

Fax: +381 11 3224-437

e-mail: gwrsupport@geneko.rs

www.geneko.rs