Geneko

GWG

USER MANUAL

GWG Gateway

Document version: 1.0.2
Date: March 2017

Document History

Date	Description	Author	Comments
24.12.2015	User Manual	Tanja Savić	Firmware version: 1.0.10
28.07.2016	User Manual	Tanja Savić	Firmware version: 1.1.0
02.03.2017	User Manual	Tanja Savić	Firmware version: 1.2.2

Document Approval

The following report has been accepted and approved by the following:

Signature	Printed Name	Title	Date
	Dragan Marković	Executive Director	24.12.2015
	Dragan Marković	Executive Director	28.07.2016
	Dragan Marković	Executive Director	02.03.2017

Trademark

Content

List of Figures

List of Tables

SAFETY WARNINGS:

The power to use an adapter (with output voltage from 9 to 36 VDC) that is certified EN 60950:2005-1+A1:2010+A2:2013+A11:2009+A12:2011 and in confirmation with article 2.5-LPS (Limited Power Source).

All pinout (GPIO, Ignition etc.) must be SELV (Safety Extra Low Voltage).

Description of the GWG-30/40 Gateway

Geneko GWG gateway is compact and cost effective communications solution that provides cellular capabilities for fixed and mobile applications such as data acquisition, smart metering, remote monitoring and management. GWG supports a variety of radio bands options, on 2G, 3G, 4G cellular technologies. It is reliable solution thanks to high performance hardware platform and VPN/Security powerful options. When coupled with the rich embedded intelligence, it is the perfect choice for a broad set of M2M solutions.

GWG comes with numerous connectivity options and multiple configuration methods. It allows you to connect your existing Ethernet and serial devices using basic configuration. Besides Ethernet, RS-232 and RS-485 serial ports, the device is equipped with USB port as well as 3 configurable input/output pins. Its small size and easy installation makes it suitable for challenging and size-constrained applications. GWG gateway can be used on either desktop or mounted on a DIN rail.

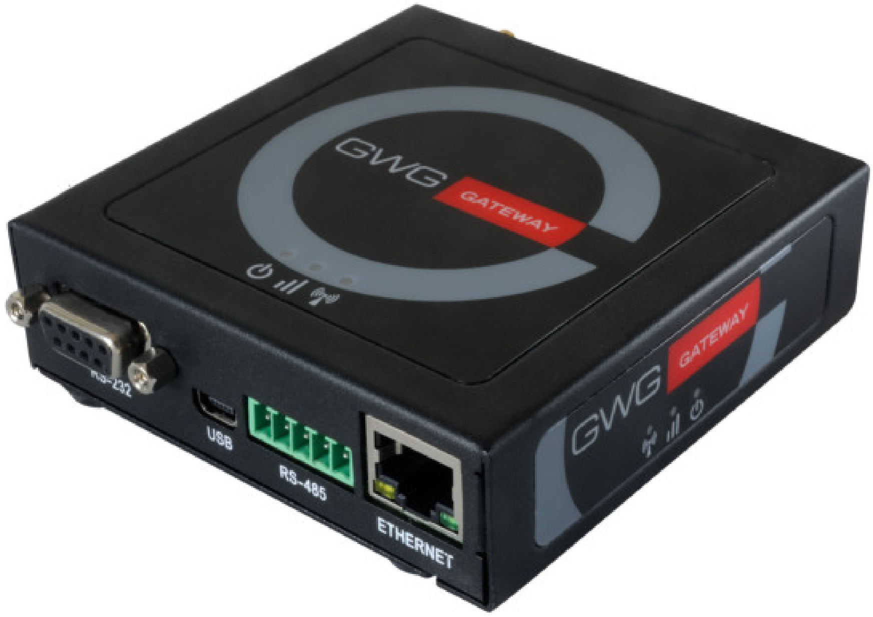


Figure 1 – GWG Gateway

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 GWG support team behind you.

Technical Parameters

Wireless Interfaces – 4G GSM Cinterion PLS8-E (available on 4G models)	
LTE FDD	Band 1 (2100 MHz), Band 3 (1800 MHz), Band 7 (2600 MHz), Band 8 (900 MHz), Band 20 (800 MHz) Transfer rate (max): 100 Mbps down, 50 Mbps up
UMTS/HSPA+/DC-HSPA+	Band 1 (2100 MHz), Band 3 (1800 MHz), Band 8 (900 MHz) Transfer rate (max): 42 Mbps down, 5.76 Mbps up
GSM/GPRS/EDGE	900/1800 MHz Transfer rate (max): 384 Kbps down, 384 Kbps up
Antenna Connector	2 x 50 Ω SMA (Center pin: female)
SIM Slots	1, Mini-SIM (2FF), Hinge
Wireless Interfaces – 3G GSM Cinterion PHS8-E (available on 3G models)	
UMTS/HSPA+	Band 1 (2100 MHz), Band 8 (900 MHz) Transfer rate (max): 14.4 Mbps down, 5.76 Mbps up
GSM/GPRS/EDGE	900/1800 MHz Transfer rate (max): 384 Kbps down, 384 Kbps up
Antenna Connector	1 or 2 x 50 Ω SMA (Center pin: female)
SIM Slots	1 Mini-SIM (2FF), Hinge
Wireless Interfaces – GNSS Cinterion PLS8-E/PHS8-E (available on automotive models	
GNSS Systems	GPS, GLONASS
GNSS Tracking Sensitivity	-159 dBm
GNSS Acquisition Sensitivity	-149 dBm
GNSS Cold Start Sensitivity	-145 dBm
GNSS Cold Start	< 32 seconds TTFF @ -130 dBm
GNSS Connector	1 x 50 Ω SMA (Center pin: female)
Wired Interfaces – RS232	
Ports	1
Standard	EIA/TIA-232, RS-232, V.28/ V.24
Data Rate	400 kbps (2)
DTE/DCE	DCE
Signal Support	TXD, RXD, CTS, RTS
Flow Control	Software XON/XOFF, Hardware CTS/RTS
Connector	D-SUB 9, female
Pinout	2: TX, 3: RX, 5: GND, 7: CTS, 8: RTS, remaining pins: NC
Wired Interfaces – RS-485/RS-422	
Ports	1
Standard	RS-422, 4 wires, Full-Duplex Note: can be externally wired as 2 wire RS-485 half-duplex

Data Rate	10 Mbps (2)
On-Board Termination	None
Connector	Phoenix 1844249
Pinout	1: RX+, 2: RX-, 3: TX-, 4: TX+, 5: GND Note: for RS-485 half-duplex mode connect 1 to 4 and use as A, and then connect 2 to 3 and use as B
Wired Interfaces – USB	
Ports	1
Standard	USB 2.0 Device
Signaling	Full Speed, High Speed
Connector	USB mini AB
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
Wired Interfaces – Digital Input/Output (available on GPIO Connector)	
Digital Inputs/Outputs	3 user selectable input or output
Digital Inputs	with internal weak pull-up, active when pulled down to GND
Digital Outputs	open-drain, 4-28V, no over-current protection
Connector	Phoenix 1844249
Pinout	1: +5VDC with 500mA resettable PTC fuse, 2: IO1, 3: IO2, 4: IO3, 5: GND
Wired Interfaces – Digital Input/Output (available on Power Connector)	
Digital Inputs/Outputs	1 output, 1 ignition sense input
Digital Output	open-drain, 4-28V, 350 mA ressetable PTC fuse
Ignition Sense Input	active when pulled up to 9-36 VDC
Connector	Molex 43045-0400
Pinout	1: +9..36VDC (also Analog Input), 2: GND, 3: Ignition Sense Input, 4: Digital Output
Wired Interfaces – Analog Input (available on Power Connector)	
Analog Input Range	9-36 VDC
Pinout	1: +9..36 VDC (also Analog Input), 2: GND, 3: Ignition Sense Input, 4: Digital Output
Power	
Input	9-36 VDC
Input Protection	Reverse polarity, transients, overcurrent (internal 1 A time-lag fuse)
Consumption at 12 VDC	Hibernation (GPS OFF, GSM OFF): 5 mA (1) Sleep (GPS OFF, GSM wake-up on SMS or call): TBD mA (1) Typical (GPS ON, GSM ON, idle): 148 mA Typical (GPS ON, GSM ON, data transfer): 165 mA Peak (GPS ON, GSM TX burst for 577 s every 4.615

	ms): 1 A
Connector	Molex 43045-0400
Pinout	1: +9..36VDC (also Analog Input), 2: GND, 3: Ignition Sense Input, 4: Digital Output
Physical	
Dimensions (L x W x H)	101 mm x 88 mm x 30 mm (connectors and rubber stands included)
Weight	248 g
Status LEDs	Power, Signal, Network, LAN (on Ethernet connector: Link, Activity)
Pushbuttons	1 – Device Reset (short press)/Factory Default (long press)
Material	Steel sheet 0.8 mm
Mounting	desktop, wall, or DIN rail (DIN rail mounting kit sold separately)
Environmental	
Operating Temperature	-20° C to +70° C
Storage Temperature	-40° C to +85° C
Relative Humidity	5% to 95% (non-condensing)
IP rating	IP40
Ethernet Isolation	1.5 kV RMS
RS-485 Port Protection (ESD)	2 kV
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
Accessories (included)	
Power supply cable	Cable length: 1.2 m Cable connector: Molex 43025-0400 Wires: 4 wires, stranded, AWG-22 Pinout: 1 (red) POWER, 2 (black) GND, 3 (white) IGNITION, 4 (green) GPIO OUT
3G/GSM antenna	Frequency: 850/900/1800/1900/2100 MHz VSWR: ≤ 2.0 Gain: 4.5 dBi Connector: SMA (Center pin: male) Dimensions (L x W x H): 163 mm x 22 mm x 14 mm
Accessories (optional)	
AC/DC adapter	Input: 90-264 VAC, 47-63 Hz Output: 12 VDC, 2 A

GSM antenna extension cable with magnetic base	Cable length: 3 m Cable connector: SMA (Center pin: male) Magnet base connector: SMA (Center pin: female) Magnet base dimensions (D x H): 50 mm x 40 mm
Active uBlox GPS antenna with magnetic base	Cable length: 5 m Cable connector: SMA (Center pin: male) Frequency: 1575 ± 3 MHz LNA Gain: 27 dB VSWR: max. 2 Dimensions (L x W x H): 48 mm x 40 mm x 13 mm
DIN rail mounting kit	DIN rail clip 3 screws

Table 1 – Technical parameters

(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	Description
Ethernet	
LAN	• Static • DHCP Client
DHCP Server: • **Static lease reservation** • **Address exclusions**	DHCP Server support
Network	
Routing	Static, NAT, PAT
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.
VRRP	VRRP is a protocol which elects a master server on a LAN and the master answers to a 'virtual IP address'. If it fails, a backup server takes over the IP address.
Port forwarding, NAT	Port forwarding is an application of NAT (*Network Address Translation*) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway.
DMZ host	DMZ (*Demilitarized Zone*) allows one IP Address to be exposed to the Internet. DMZ provides this function by forwarding all the ports to one computer at the same time.
DynDNS	Client for various dynamic DNS services.
FIREWALL: • **IP Filtering** • **MAC Filtering**	IP address / Network filtering
GPS	GPS page will show a graphical view of router's location. Modem must provide capabilities of GPS, the router must be connected to GPS antenna, coordinates are connected and GPS support is enabled, GPS information will be displayed. ([1])
SMS : • **SMS Remote Control** • **Send SMS**	SMS remote control feature allows users to execute a short list of predefined commands by sending SMS messages to the GWG-30/40 gateway. 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.
Serial Port over TCP/UDP	Serial to Ethernet converter
USB Port	USB Port as Serial Port
Modbus serial/IP gateway	Translation between Modbus/TCP or Modbus/RTU.
RS-485	The Geneko Router is able to connect a Modbus RTU RS-485 device to a PC with Modbus TCP master via an Ethernet network. Maximum RS485 communication speed is 115 200 bps.
Certificate management	Certificate management is used to manage certificate files so they can be used for peer authentication. • CA Certificate

	• Private Certificate • Private Key • Preshared Key Files CRL Certificate is used to manage Certificate Revocation List certificate files so they can be used for validating certificates.
VPN (Virtual Private Network)	
GRE	GRE (*Generic Routing Encapsulation*) is a tunneling protocol that can encapsulate a wide variety of network layer protocol packet types inside IP tunnels.
GRE keepalive	• Keepalive for GRE tunnels • Cisco compliant
GRE-max. number of tunnels	3
IPsec	IPSec (*Internet Protocol Security*) is a protocol suite for securing Internet Protocol communication by authenticating and encrypting each IP packet of a data stream.
Key Exchange Mode	• IKE with Preshared key • IKE with Preshared key file • IKE with X509 certificates and PSK • IKE with X509 certificates and PSK file
Data integrity	• HMAC-MD5, SHA1 • Authentication and key management
Authenticate Mode	• Pre-shared secret • Username / password • X.509 cert. (client) • X.509 cert. (server)
Encryption	• AES(128/192/256) • 3DES • Blowfish (128/192/256)
IKE features	• IKE with pre-shared key
IPSec IKE failover	Defines number of failed IKE negotiation attempts before failover.
IPSec tunnel failover	Switches to another provider when tunnel performance is bad or one provider is unavailable.
IPSec-max. number of tunnels	3
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	3
L2TP	L2TP is suitable for Layer-2 tunneling.
L2TP max. number of tunnels	5
PPTP	PPTP client
PPTP max. number of tunnels	5
GSM/UMTS features	
2G/3G/4G	Support with dual SIM capability. (2)
Authentication	PAP, CHAP, PAP-CHAP
SIM PIN locking	Enable locking of SIM card with PIN code.
Operator locking	This option forces your SIM card to register to predefined PLMN only.

Roaming protection	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.
SIM keepalive	Make some traffic periodically in order to maintain connection active.
SIM data limit	Enable traffic data limit per SIM.
Reboot after failed connection	Reboot gateway after 'n' consecutive failed connection attempts.
Maintenance	
Diagnostics	Ping utility
System control	Create a scheduled task to reboot the device at a regular interval.
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.
Authentication	Used for activating and deactivating device access system through Username and Password mechanism. It is possible to activate or deactivate function for authentication via remote radius server.
Date and time settings	Current Date and Time Date and Time Setup: • Manually • From time server • From mobile provider
NTP	NTP (*Network Time Protocol*) is a protocol for synchronizing the clocks of router.
Update Firmware	• Over WEB interface • Over CLI
Import/Export settings	Import or Export of configuration (Possibility of selecting type of configuration to export).
Factory default settings	Returns to factory default settings.
Reboot	System reboot
LED	LED Settings: • Top • Side • Both
GPIO	GPIO sends SMS when some certain event occur. Action executed when GPIO pin change its state to Low or High. On router's board are 5 GPIO generic pins which represent: 1. +5VDC with 500mA resettable PTC fuse 2. IO1 3. IO2 4. IO3 5. GND IO1, IO2, IO3 are 3 user selectable input or output. Input value is readable (high=1, low=0). Output value is writable (high=1, low=0).
Management	
User-friendly WEB GUI	HTTP based
Timed actions	Create a schedule of actions to be performed in a certain time of the day. There is a possibility to add more actions for each day of the

	week.
CLI: • **SSH** • **telnet** • **serial**	Remote management over SSH. Remote management over Telnet. Custom AT scripting to modem
SNMP v1,2c	SNMP (*Simple Network Management Protocol*) is a network protocol that provides network administrators with the ability to monitor the status of the GWG-30/40 gateway and receive notification of any critical events as they occur on the network. The GWG-30/40 gateway supports SNMP v1/v2c and all relevant Management Information Base II (MIBII) groups.
Traffic and event log	Log tracing.
Connection Manager	Enabling Connection Manager will allow Connection Wizard (located on setup CD that goes with the gateway) 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 gateway to the local network without previous setup of the gateway. Connection Wizard will detect the device and allow you to configure some basic functions of the router.
Remote Management	Remote Management Utility is a standalone Windows application with many useful options for configuration and monitoring of Geneko Routers. In order for it to work, it must be enabled on the router and installed on a Windows computer. It is a Geneko TM application.
Customization options	
Chroot environment	Support for shell scripts, LUA. Perl and compiled C/C++ executables. Allowed access to device peripherals from user space.

Table 2 – GWG Gateway functional features

[1] Future functionality

[2] LTE is available at GWG-40

Product Overview

Front panel

On the front panel the following connectors are located:

- One RJ45 connector Ethernet port for connection into local computer network
- One RJ45 connector for RS232 serial communication
- One RS-485 connector
- One USB connector for connection to the PC

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.

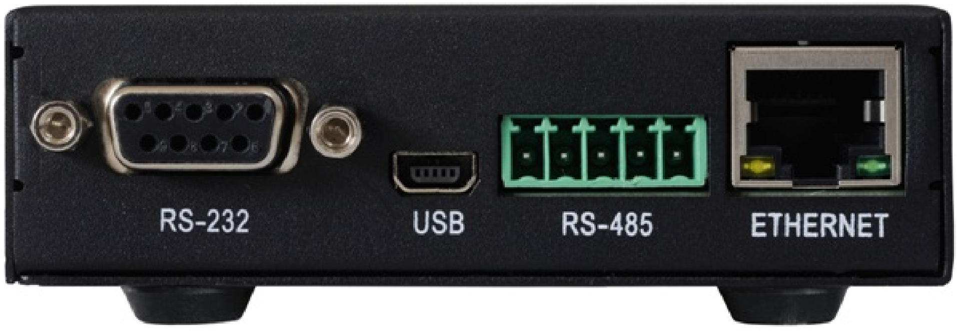


Figure 2– GWG Gateway front panel

Back panel

On the back panel of device the following connectors are located:

- Power supply connectors
- SMA connector for connection of the GSM/UMTS/LTE antenna (main)
- Reset button
- GPIO connector

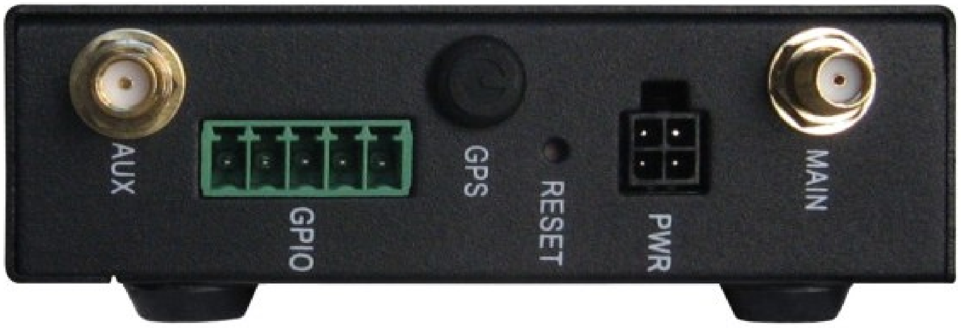


Figure 3– GWG Gateway rear panel

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

Warm reset: If the GWG Gateway 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 GWG Gateway, hold the RESET button pressed for a few seconds. Restoration of the default configuration will be signaled by blinks of the power LED on the top panel and the side. This will restore the factory defaults and clear all custom settings of the GWG Gateway. You can also reset the GWG Gateway to factory defaults using the Maintenance > Default Settings screen.

Top Panel

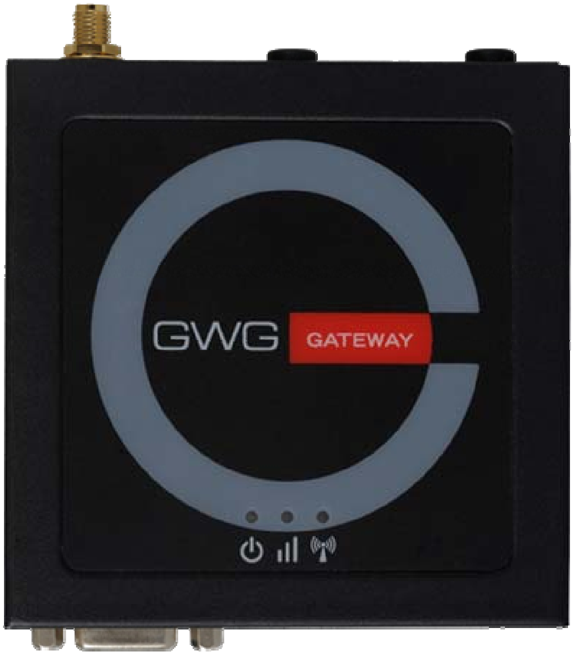


Figure 4 – GWG Gateway top panel side

LED Indicator Description:

Power LED- This monitors the input power.

- **OFF** –No power or input voltage ≥36VDC or ≤7.5VDC
- **Flashing Green**- The device is entering low power mode or system low level boot.
- **Green**- The device is connected to nominal power and is operating normally.
- **Green with a momentary red flash**- The device has a GPS fix.

Signal LED-This shows the cellular network's signal level.

- **OFF**-No signal is present. (RSSI>-110dBm)/ There is no network coverage at the location.
- **Flashing Green**- A bad or marginal signal is present. (RSSI> -85dBm or ≤ -110 dBm)
- **Green**- A good signal is present. (RSSI≤ -85dBm)

Network LED-This monitors the cellular network.

- **Off**-The device was unable to authenticate on the network.
- **Flashing green (slow)**- The cellular network is found and the device is connecting.

- **Green**- Connected to the cellular network.
- **Flashing Green (fast)-** The device is roaming.

Bottom Panel

SIM card holder is on the bottom of the GWG Gateway.

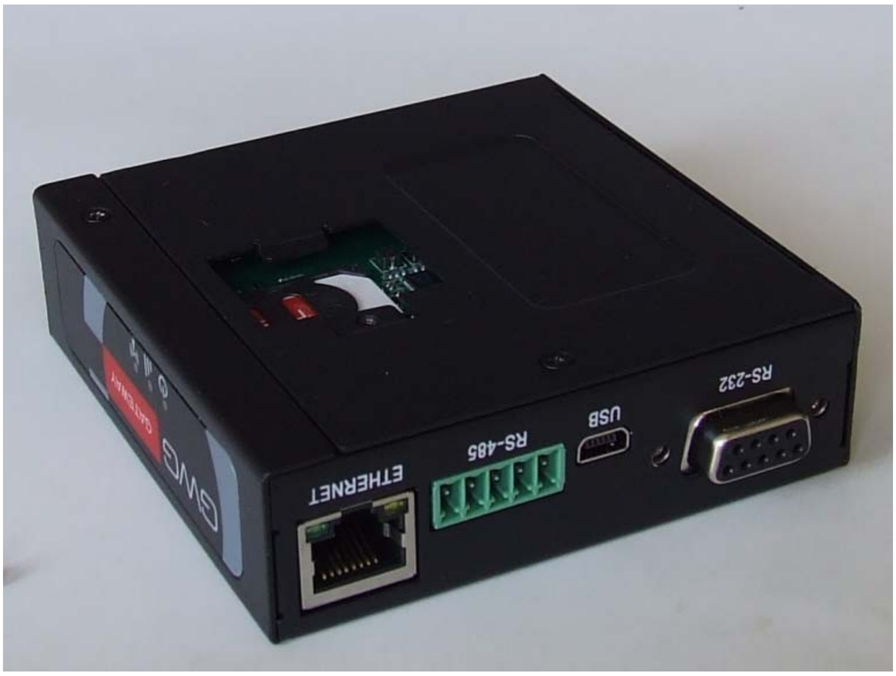


Figure 5– GWG Gateway bottom panel

Putting Into Operation

Before putting the GWG Gateway in operation it is necessary to connect all components needed for the operation:

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

And finally, device should have powered up using power supply adapter.
Power consumption of GWG Gateway is 2W in standby and 3W in burst mode.

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

Device Configuration

There are two methods which can be used to configure the GWG Gateway. 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 GWG Gateway. Configuration, administration and monitoring of the GWG Gateway 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 (CLI). This method has limited options for configuring the GWG Gateway but still represents a very powerful tool when it comes to gateway setup and monitoring. Another document deals with CLI commands and instructions.

Quick start

Inserting SIM Cards

Warning: do not insert or eject SIM cards while gateway is powered on. Make sure to disconnect gateway from AC/DC adapter (9-36VDC) before inserting or ejecting SIM cards.

- Use a screwdriver to remove the cover from the back of the GWG Gateway
-UNLOCK SIM card holder
-Lift the SIM card HOLDER and put SIM card in it
-LOCK SIM card holder
-Put the cover back and use screwdriver to tighten the screw

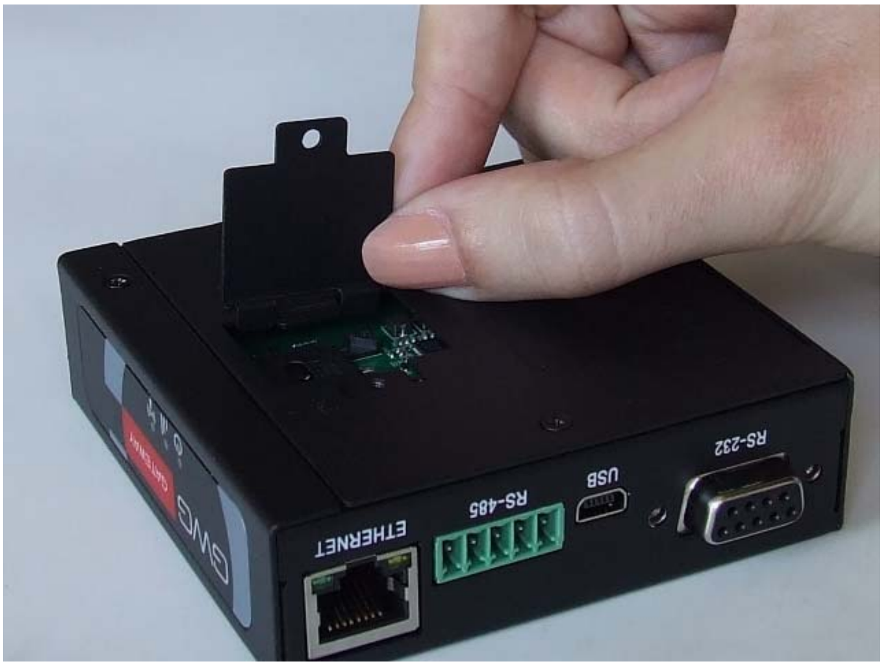


Figure 6 – Insert SIM card

Connecting Gateway

-Connect antenna to gateway. Make sure to tighten antenna so it is not loose.
- Plug AC/DC adapter (9-36VDC) cable into POWER CONNECTOR on the gateway.
-Red wire-power
-Black wire-ground
-Green wire-GPIO output
-White wire-ignition
-All wires must be isolated

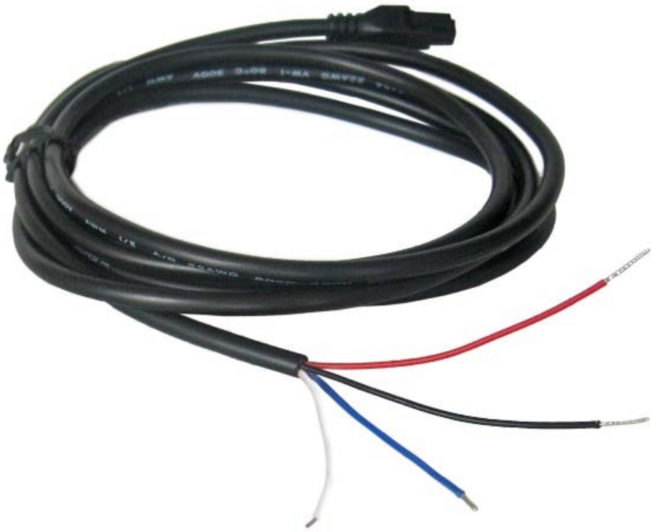


Figure 7 – Wires for power, ground, GPIO output, ignition

-Green POWER indicator will turn on.
- Wait approximately 52 seconds for gateway to become fully operational.
- Plug one side of ETHERNET CABLE to ETHERNET CONNECTOR on a gateway.
-Plug other side of ETHERNET CABLE to Ethernet port on the computer.

Administration Web Page

Add network 192.168.1.0/24 to the interface on your PC
-Optional: Ping 192.168.1.1 to check if the gateway is accessible
-Open your Web browser (e.g. Firefox, Chrome, Safari, Opera, or Internet Explorer) and enter the following address: http://192.168.1.1
-When prompted for your login credentials, use "admin" (without quotes) for both username and password.
-After logging in you should be able to see administration web page, which allows you to easily setup the gateway.

Quick Setup

-Once logged in to administration web page, click on SETTINGS » MOBILE SETTINGS link from the menu on the left side of the screen.
- If SIM card is present, ENABLED check box will be checked. Otherwise, you need to insert SIM card as explained in "Inserting SIM cards" chapter.

-Your GSM operator should provide you with PROVIDER, USERNAME (optional), PASSWORD (optional), APN and PIN (optional) information. Make sure you enter this into corresponding fields, and then click on SAVE button.
- Flashing red NETWORK indicator will turn on.
-After a few minutes when your gateway is connected, connection status will be accomplished.
-Green NETWORK indicator will turn on.
-Click on SETTINGS » ETHERNET SETTINGS »LAN PORTS link from the menu on the left side of the screen

Turn Logging On

When troubleshooting gateway make sure logs are turned on.
You should send logs to Geneko when submitting support request.

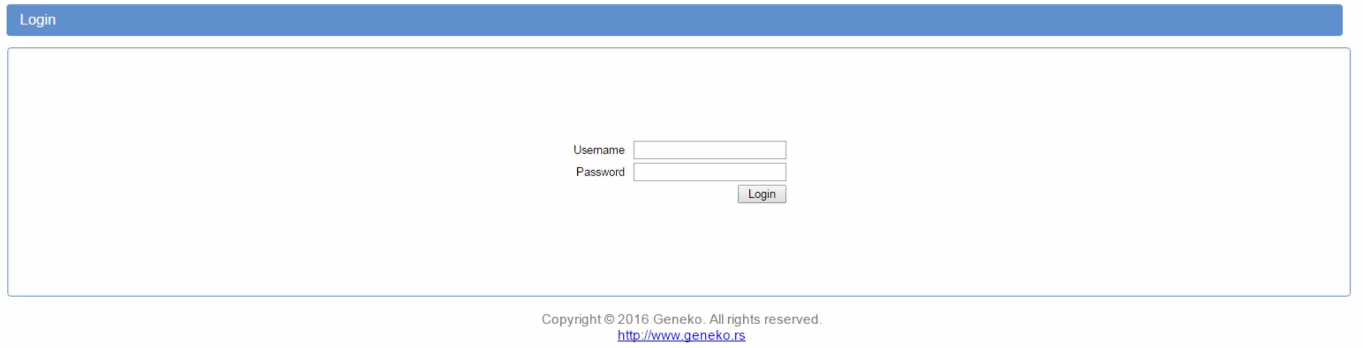
- Click on MANAGEMENT » LOGS link from the menu on the left side of the screen.
- Click on LOCAL SYSLOG radio button, and then click on SAVE button.
- Set appropriate log size and click on SAVE button.
- Log is now available for download from gateway to your computer when you click on EXPORT LOG button.

Device configuration using web application

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

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

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



Copyright © 2016 Geneko. All rights reserved.
http://www.geneko.rs

Figure 8 – User authentication

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

You can set all parameters of the GWG Gateway 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

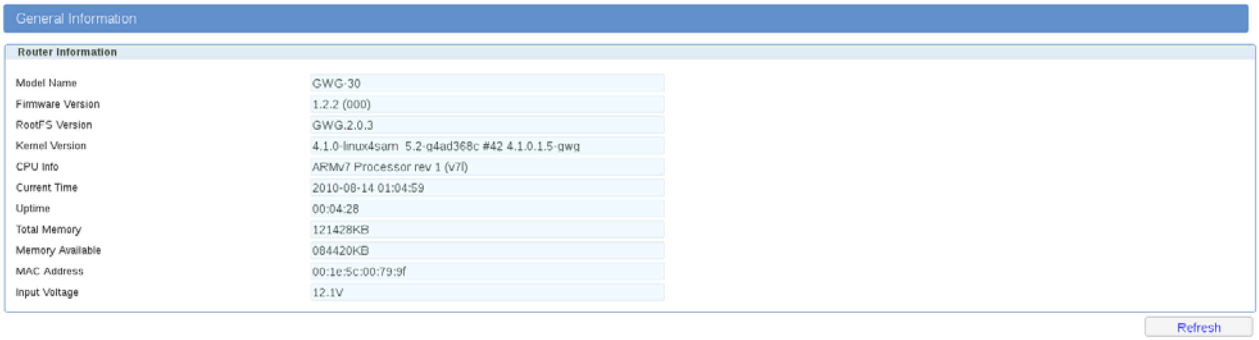
The GWG Gateway’s Status menu provides general information about gateway as well as real–time network information. Status information is divided into following categories:

- General Information
- Lan Information
- DHCP
- Mobile
- Firewall
- Routes
- Router Monitoring

Status – General

General Information Tab provides general information about device type, device firmware version, RootFS version, Kernel version, CPU info, Current Time, UpTime, Total Memory, Used Memory, Free Memory, MAC Address. Screenshot of General Gateway information is shown at **Error! Reference source not found.**. 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.



General Information

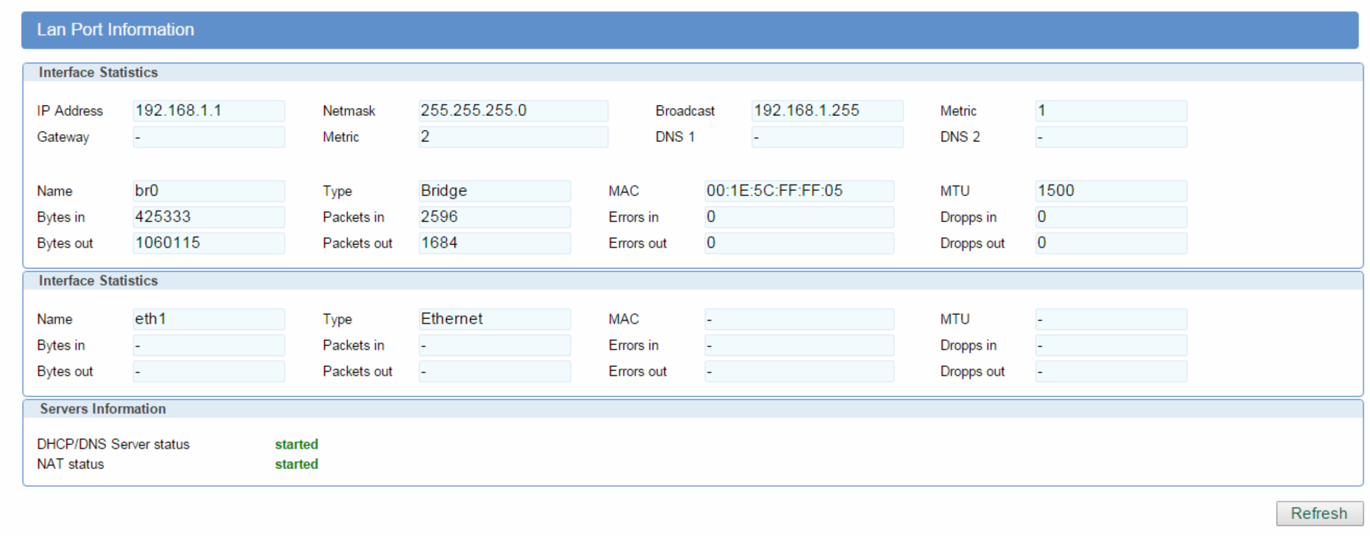
Router Information

Model Name	GWG-30
Firmware Version	1.2.2 (000)
RootFS Version	GWG.2.0.3
Kernel Version	4.1.0-linux4sam_5.2-g4ad368c #42 4.1.0.1.5-gwg
CPU Info	ARMv7 Processor rev 1 (v7l)
Current Time	2010-08-14 01:04:59
Uptime	00:04:28
Total Memory	121428KB
Memory Available	084420KB
MAC Address	00:1e:5c:00:79:9f
Input Voltage	12.1V

Figure 9– General gateway information

Status – LAN Port Information

Lan Port Information Tab provides information about Ethernet port and Ethernet traffic statistics. Screenshot of Lan Port Information is shown in Figure 10.



Lan Port Information

Interface Statistics

IP Address	192.168.1.1	Netmask	255.255.255.0	Broadcast	192.168.1.255	Metric	1
Gateway	-	Metric	2	DNS 1	-	DNS 2	-

Name	br0	Type	Bridge	MAC	00:1E:5C:FF:FF:05	MTU	1500
Bytes in	425333	Packets in	2596	Errors in	0	Dropps in	0
Bytes out	1060115	Packets out	1684	Errors out	0	Dropps out	0

Interface Statistics

Name	eth1	Type	Ethernet	MAC	-	MTU	-
Bytes in	-	Packets in	-	Errors in	-	Dropps in	-
Bytes out	-	Packets out	-	Errors out	-	Dropps out	-

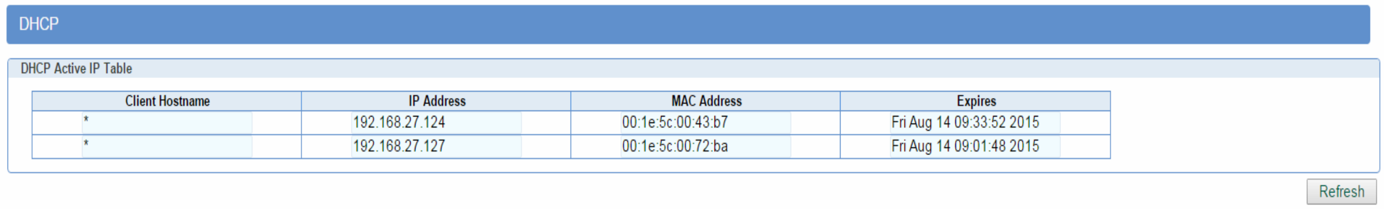
Servers Information

DHCP/DNS Server status	started
NAT status	started

Figure 10– LAN Port 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.



DHCP

DHCP Active IP Table

Client Hostname	IP Address	MAC Address	Expires
*	192.168.27.124	00:1e:5c:00:43:b7	Fri Aug 14 09:33:52 2015
*	192.168.27.127	00:1e:5c:00:72:ba	Fri Aug 14 09:01:48 2015

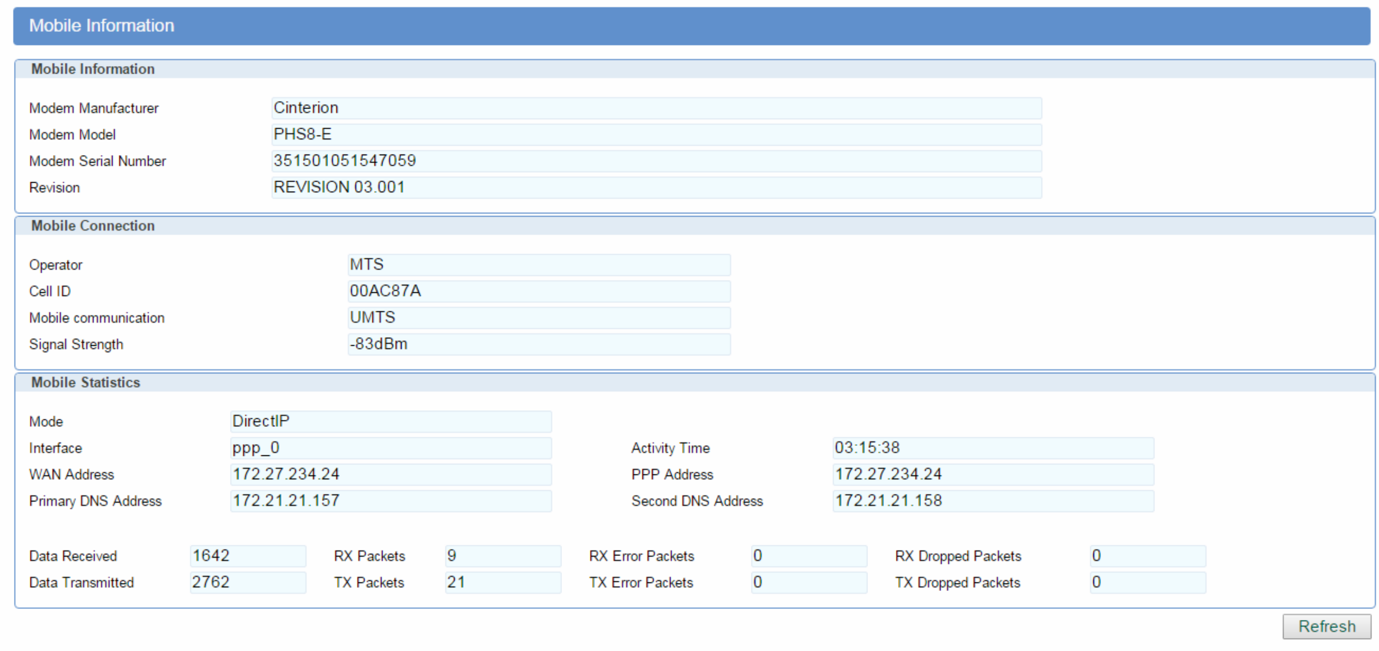
Figure 11 – DHCP Information

Status – Mobile Information

Mobile Information Tab provides information about GPRS/EDGE/HSPA/HSPA+/LTE connection and traffic statistics. *Mobile 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 (in bytes)

Screenshot of Mobile information from the router is shown in Figure 12:



Mobile Information

Mobile Information

Modem Manufacturer	Cinterion
Modem Model	PHS8-E
Modem Serial Number	351501051547059
Revision	REVISION 03.001

Mobile Connection

Operator	MTS
Cell ID	00AC87A
Mobile communication	UMTS
Signal Strength	-83dBm

Mobile Statistics

Mode	DirectIP		
Interface	ppp_0	Activity Time	03:15:38
WAN Address	172.27.234.24	PPP Address	172.27.234.24
Primary DNS Address	172.21.21.157	Second DNS Address	172.21.21.158

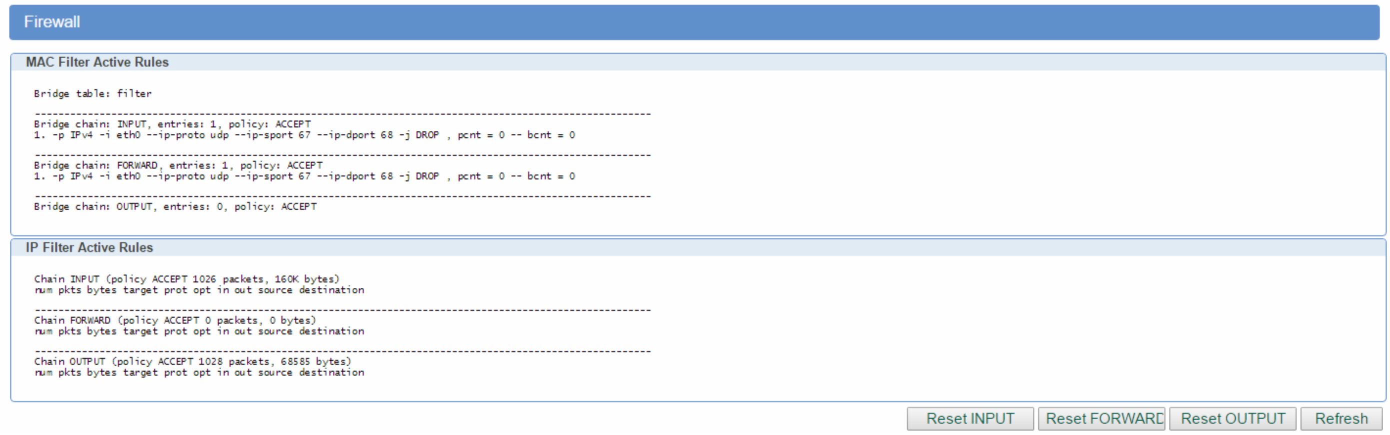
Data Received	1642	RX Packets	9	RX Error Packets	0	RX Dropped Packets	0
Data Transmitted	2762	TX Packets	21	TX Error Packets	0	TX Dropped Packets	0

Figure 12– Mobile Information

As a primary and secondary DNS are always displayed DNS servers assigned by provider. They are not necessarily used by the gateway. If Local DNS is configured it has priority to those DNS servers.

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.



Firewall

MAC Filter Active Rules

```
Bridge table: filter

------------------------------------------------------------------------------------------
Bridge chain: INPUT, entries: 1, policy: ACCEPT
1. -p IPv4 -i eth0 --ip-proto udp --ip-sport 67 --ip-dport 68 -j DROP , pcnt = 0 -- bcnt = 0

------------------------------------------------------------------------------------------
Bridge chain: FORWARD, entries: 1, policy: ACCEPT
1. -p IPv4 -i eth0 --ip-proto udp --ip-sport 67 --ip-dport 68 -j DROP , pcnt = 0 -- bcnt = 0

------------------------------------------------------------------------------------------
Bridge chain: OUTPUT, entries: 0, policy: ACCEPT
```

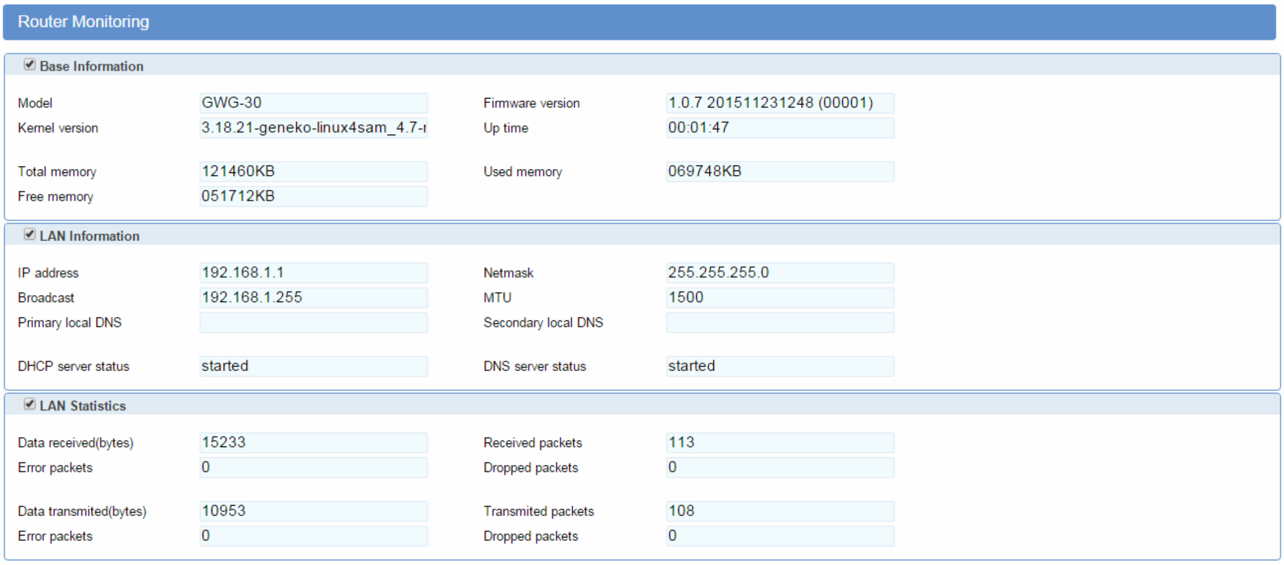
IP Filter Active Rules

```
Chain INPUT (policy ACCEPT 1026 packets, 160K bytes)
num pkts bytes target prot opt in out source destination

------------------------------------------------------------------------------------------
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num pkts bytes target prot opt in out source destination

------------------------------------------------------------------------------------------
Chain OUTPUT (policy ACCEPT 1028 packets, 68585 bytes)
num pkts bytes target prot opt in out source destination
```

Figure 13– Firewall Information

Status – Router Monitoring

Router Monitoring tab provides Base information, LAN and Mobile real-time information about Mobile Connection. You can activate Automatic refresh after 5, 10, 15, 30 or 60 seconds.



Router Monitoring

☑ Base Information

Model	GWG-30	Firmware version	1.0.7 201511231248 (00001)
Kernel version	3.18.21-geneko-linux4sam_4.7-r	Up time	00:01:47
Total memory	121460KB	Used memory	069748KB
Free memory	051712KB		

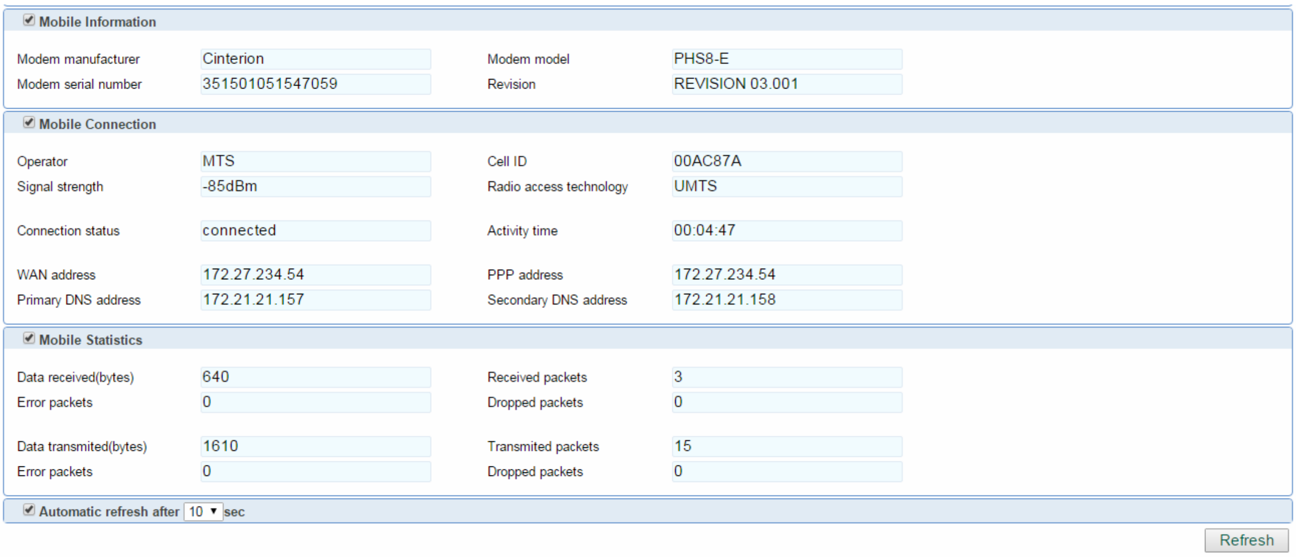
☑ LAN Information

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	started

☑ LAN Statistics

Data received(bytes)	15233	Received packets	113
Error packets	0	Dropped packets	0
Data transmited(bytes)	10953	Transmited packets	108
Error packets	0	Dropped packets	0

Figure 14– Router monitoring #1



☑ Mobile Information

Modem manufacturer	Cinterion	Modem model	PHS8-E
Modem serial number	351501051547059	Revision	REVISION 03.001

☑ Mobile Connection

Operator	MTS	Cell ID	00AC87A
Signal strength	-85dBm	Radio access technology	UMTS
Connection status	connected	Activity time	00:04:47
WAN address	172.27.234.54	PPP address	172.27.234.54
Primary DNS address	172.21.21.157	Secondary DNS address	172.21.21.158

☑ Mobile Statistics

Data received(bytes)	640	Received packets	3
Error packets	0	Dropped packets	0
Data transmited(bytes)	1610	Transmited packets	15
Error packets	0	Dropped packets	0

☑ Automatic refresh after 10 ▾ sec

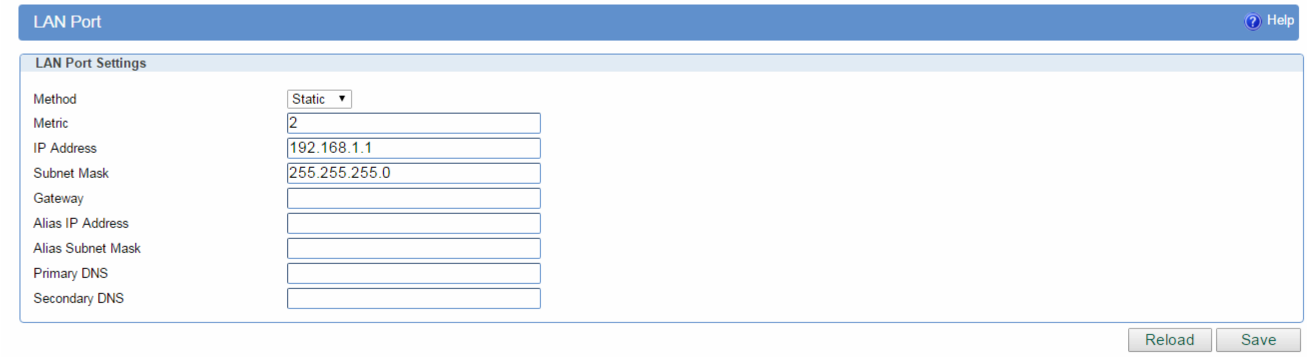
Figure 15– Router monitoring #2

Settings – LAN Ports

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

LAN Ports Parameters	
Label	**Description**
Method	Select static or DHCP. With DHCP option, the router will obtain an IP address from DHCP server on the LAN.
Metric	This field specifies value which define routing priority
IP Address	Type the IP address of your GWG Gateway in dotted decimal notation. 192.168.1.1 is the factory default IP address.
Subnet Mask	The subnet mask specifies the network number portion of an IP address. The GWG Gateway support sub–netting. You must specified subnet mask for your LAN TCP/IP settings.
Gateway	Type the IP address of your local gateway. Use Local Gateway option carefully. Gateway becomes unreachable from local subnet when this option is entered.
Alias IP Address	IP address of internal virtual LAN interfaces (secondary).
Alias Subnet Mask	Corresponding subnet mask for this alias.
Primary DNS	Type the IP address of your primary local DNS server.
Secondary DNS	Type the IP address of your secondary local DNS server.
Reload	Click ***Reload*** to discard any changes and reload previous settings.
Save	Click ***Save*** button to save your changes back to the GWG Gateway. Whether you make changes or not, gateway will reboot every time you click ***Save***.

Table 3 – LAN parameters



Method	Static ▾
Metric	2
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	
Alias IP Address	
Alias Subnet Mask	
Primary DNS	
Secondary DNS	

Figure 16– LAN Port configuration page

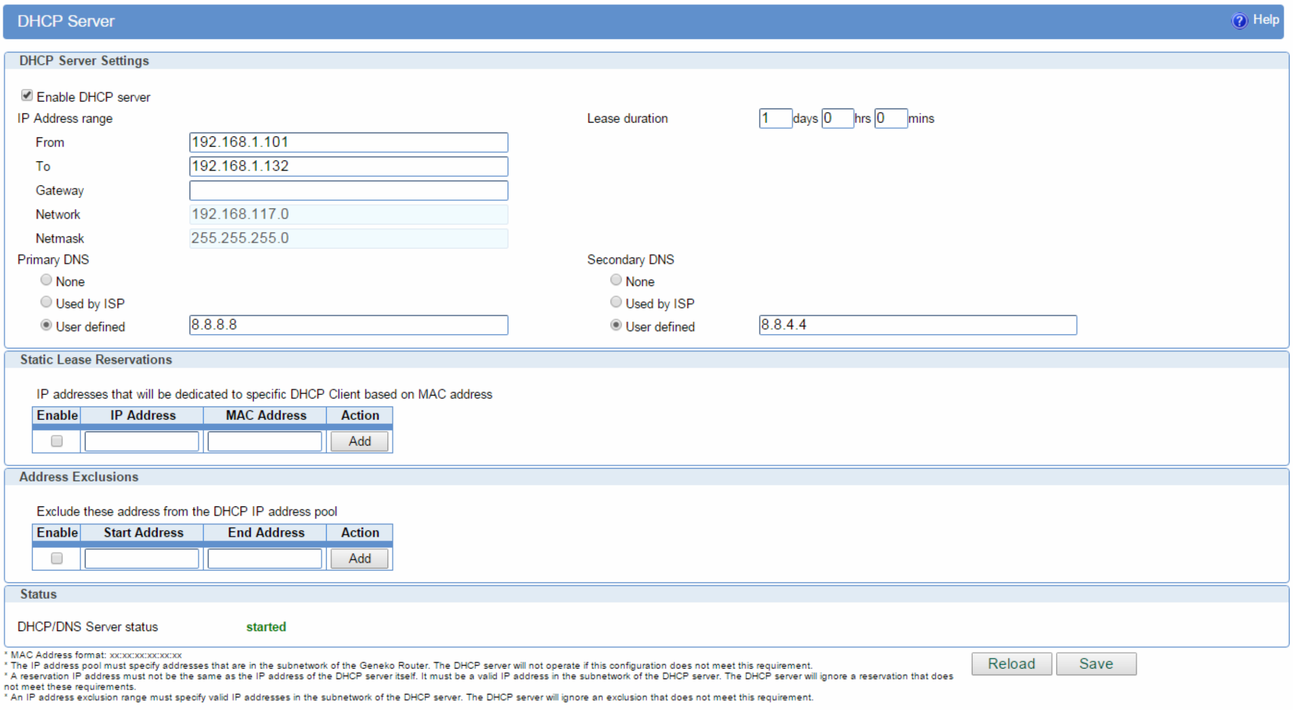
Settings – DHCP Server

The GWG Gateway 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, computers on your LAN which will use DHCP server 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 GWG Gateway as your network's DHCP server, click ***DHCP Server*** Tab for DHCP Server setup. The GWG Gateway 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**
Enable DHCP Server	To activate DHCP server, click checkbox **Enable DHCP Server**. To setup DHCP server fill in the IP Starting Address (**from**) and IP Ending Address (**to**) fields. When checkbox is unchecked, you must have another DHCP server on your LAN, or the computers must be manually configured.
IP address range	This field specifies the IP address pool for assigning IP addresses. **Address range must be in the same network (subnet) as the router's LAN port.**
IP Address range (From)	This field specifies the first of the contiguous addresses in the IP address pool.
IP Address range (To)	This field specifies last of the contiguous addresses in the IP address pool.
Lease Duration	This field specifies DHCP session duration time.
Gateway	This field specifies default gateway for DHCP clients. If left blank, router will become the gateway.
Network/netmask	This field shows current network and netmask of the gateway (DHCP server).
Primary DNS, Secondary DNS	This field specifies IP addresses of DNS server that will be assigned 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 GWG Gateway assign 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 **User defined** to have the GWG Gateway assigns DNS IP address to DHCP clients. DNS address is manually configured by user.
Static Lease Reservation	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.
Address Exclusions	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.
Add	Click ***Add*** to insert (add) new item in table to the GWG Gateway.
Remove	Click ***Remove*** to delete selected item from table.
Save	Click ***Save*** to save your changes back to the GWG Gateway.
Reload	Click ***Reload*** to discard any changes and reload previous settings.

Table 4 – DHCP Server parameters



DHCP Server

DHCP Server Settings

☑ Enable DHCP server

IP Address range

From 192.168.1.101

To 192.168.1.132

Gateway

Network 192.168.117.0

Netmask 255.255.255.0

Lease duration 1 days 0 hrs 0 mins

Primary DNS

○ None

○ Used by ISP

● User defined 8.8.8.8

Secondary DNS

○ None

○ Used by ISP

● User defined 8.8.4.4

Static Lease Reservations

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

Enable	IP Address	MAC Address	Action
□			Add

Address Exclusions

Exclude these address from the DHCP IP address pool

Enable	Start Address	End Address	Action
□			Add

Status

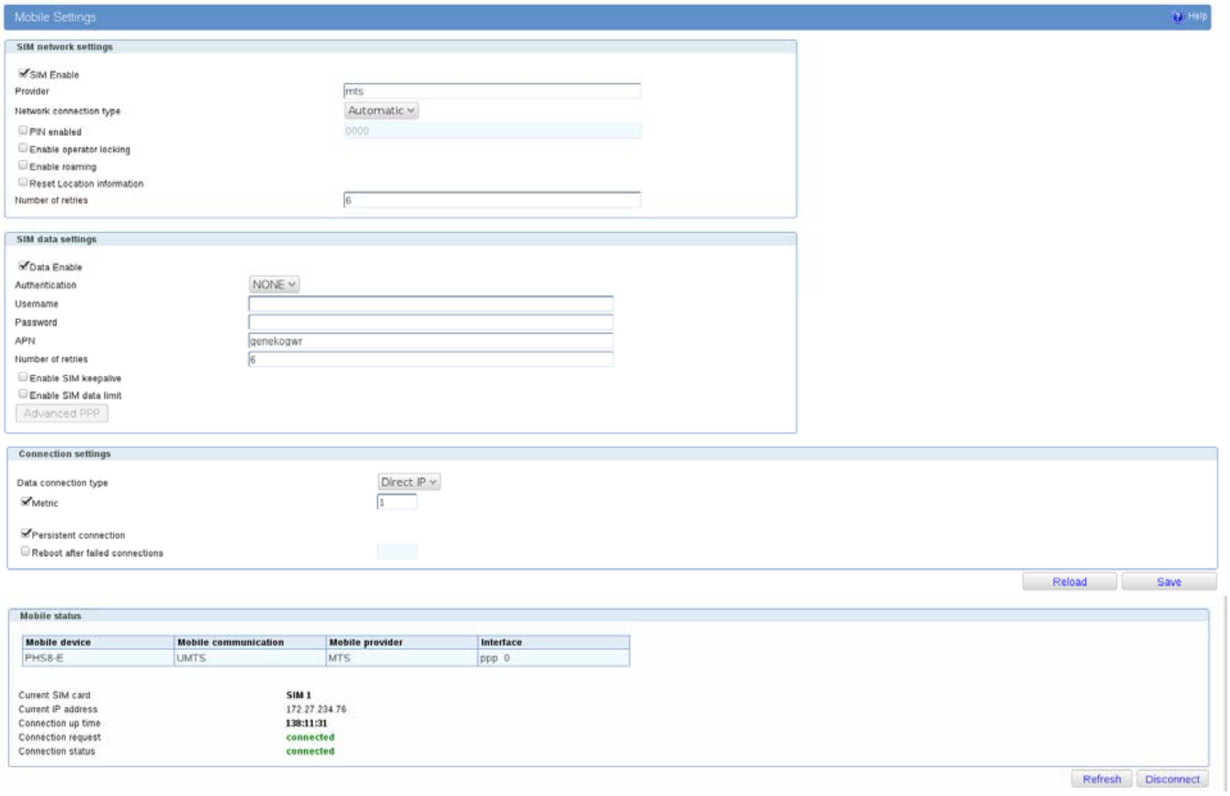
DHCP/DNS Server status started

* MAC Address format: xx:xx:xx:xx:xx:xx
* The IP address pool must specify addresses that are in the subnetwork of the Geneko 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.

Figure 17 – DHCP Server configuration page

Settings – Mobile Settings

Click ***Mobile Settings*** Tab, to open the Mobile Settings screen. Use this screen to configure the GWG Gateway GPRS/EDGE/HSPA/HSPA+/LTE parameters on Figure 18.



Mobile Settings

SIM network settings

☑ SIM Enable

Provider mts

Network connection type Automatic

□ PIN enabled 0000

□ Enable operator locking

□ Enable roaming

□ Reset Location information

Number of retries 6

SIM data settings

☑ Data Enable

Authentication NONE

Username

Password

APN genekogwr

Number of retries 6

□ Enable SIM keepalive

□ Enable SIM data limit

Connection settings

Data connection type Direct IP

☑ Metric 1

☑ Persistent connection

□ Reboot after failed connections

Mobile status

Mobile device	Mobile communication	Mobile provider	Interface
PHS8-E	UMTS	MTS	ppp 0

Current SIM card **SIM 1**
Current IP address 172.27.234.76
Connection up time **138:11:31**
Connection request **connected**
Connection status **connected**

Figure 18– Mobile Settings configuration page

Mobile Settings	
Label	**Description**
Provider	This field specifies name of GSM/UMTS ISP. You can setup any name for provider.
Authentication	This field specifies password authentication protocol. From the pop up window choose appropriate protocol (PAP, CHAP, PAP - CHAP)
Username	This field specifies Username for client authentication at GSM/UMTS network. Mobile provider will assign you specific username for SIM card.
Password	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 for client authentication at GSM/UMTS network. Mobile provider will assign you specific APN for SIM card.
Connection Type	This field enables you to choose between GSM, UMTS and LTE network.
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.
SIM PIN locking ***(PIN enabled)***	Enable locking of SIM card with PIN code.
Enable operator locking	This option forces your SIM card to register to predefined PLMN only.
Enable roaming	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.
Number of retries	This field specifies number of attempts to establish connection.
Default Gateway Metric	Set the metric for mobile network interface as the default gateway.
Persistent connection	Keep connection alive, try to reopen the connection if it is broken.
Reboot after failed connections	Reboot gateway after 'n' consecutive failed connection attempts
Enable SIM keepalive	Make some traffic periodically in order to maintain connection active. You can set keepalive interval value in minutes.
Protocol	Choose which protocol to use for keepalive packets.
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 of 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	If Restart PPP option is selected, gateway will restart the PPP connection.
Enable SIM 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 can no longer be 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).
SIM data limit action	In case of reaching defined data traffic limit, action will be performed, disconnect network connection over the SIM card.
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 Refresh button.
Reset current traffic value	Click on Reset button 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.
Mobile status	Displays data related to mobile connection (current WAN address, uptime, connection status…).
Reload	Click ***Reload*** to discard any changes and reload previous settings.
Save	Click ***Save*** to save your changes back to the GWG Gateway.
Refresh	Click ***Refresh*** to see updated mobile network status.
Connect/ Disconnect	Click ***Connect/Disconnect*** to connect or disconnect from mobile network.

Table 5 – Mobile settings

Figure 18 shows screenshot of GSM/UMTS/LTE tab configuration menu. GSM/UMTS/LTE menu is divided into two parts.

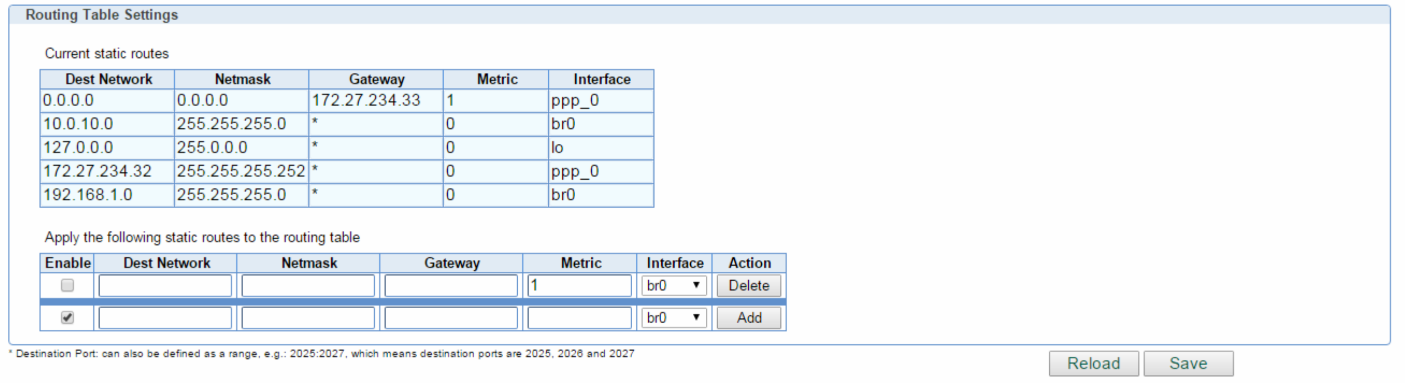
- Upper part provides all parameters for configuration GSM/UMTS/LTE connection. These parameters can be obtained from Mobile Operator. Please use exact parameters given from Mobile Operator.
- Bottom part is used for monitoring status of GSM/UMTS/LTE connection (create/maintain/destroy GSM/UMTS/LTE connection).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

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

Settings – Routing

The static routing function determines the path that data follows over your network before and after it passes through the GWG Gateway. You can use static routing to allow different IP domain users to access the Internet through the GWG Gateway. 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 GWG Gateway to automatically adjust to physical changes in the network's layout.

The GWG Gateway is a fully functional gateway with static routing capability. Figure 19 shows screenshot of Routing page.



Routing Table Settings

Current static routes

Dest Network	Netmask	Gateway	Metric	Interface
0.0.0.0	0.0.0.0	172.27.234.33	1	ppp_0
10.0.10.0	255.255.255.0	*	0	br0
127.0.0.0	255.0.0.0	*	0	lo
172.27.234.32	255.255.255.252	*	0	ppp_0
192.168.1.0	255.255.255.0	*	0	br0

Apply the following static routes to the routing table

Enable	Dest Network	Netmask	Gateway	Metric	Interface	Action
□				1	br0 ▾	Delete
☑					br0 ▾	Add

* Destination Port: can also be defined as a range, e.g.: 2025:2027, which means destination ports are 2025, 2026 and 2027

Figure 19– 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**
Routing Table	
Enable	This check box allows you to activate/deactivate this static route.
Dest Network	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.
Netmask	This parameter specifies the IP netmask address of the final destination.
Gateway	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 does not need to 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 br0 represent LAN interface an ppp0 represent GSM/UMTS/LTE interface of the GWG Gateway.
Add	Click **Add** to insert (add) new item in table to the GWG Gateway.

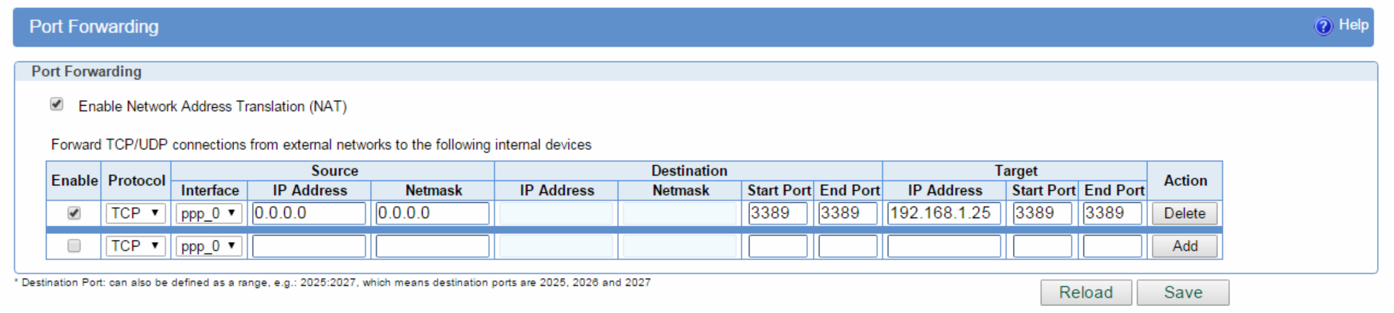
Remove	Click **Remove** to delete selected item from table.
Reload	Click **Reload** to discard any changes and reload previous settings.
Save	Click Sa**ve** to save your changes back to the GWG Gateway. After pressing Save button it make take more than 10 seconds for gateway to save parameters and become operational again.

Table 6 – Routing parameters

Port forwarding

Port forwarding is an application of NAT (*Network Address Translation*) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway.

For incoming data, the GWG Gateway 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 GWG Gateway.



Port Forwarding

Port Forwarding

☑ Enable Network Address Translation (NAT)

Forward TCP/UDP connections from external networks to the following internal devices

Enable	Protocol	Source			Destination				Target			Action
		Interface	IP Address	Netmask	IP Address	Netmask	Start Port	End Port	IP Address	Start Port	End Port	
☑	TCP	ppp_0	0.0.0.0	0.0.0.0			3389	3389	192.168.1.25	3389	3389	Delete
☐	TCP	ppp_0										Add

* Destination Port: can also be defined as a range, e.g.: 2025:2027, which means destination ports are 2025, 2026 and 2027

Figure 20– Port forwarding

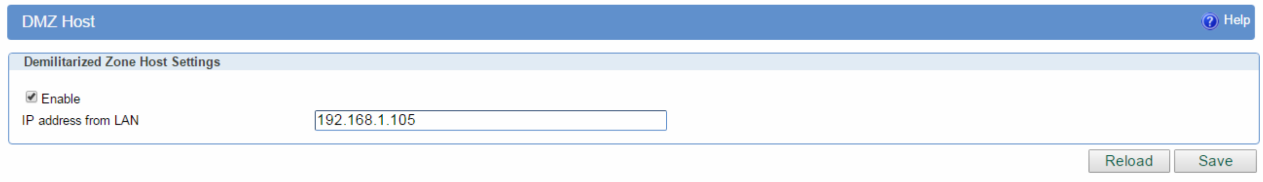
TCP/UDP Traffic forwarding	
Enable Network Address Translation (NAT)	This field specifies if NAT is used on the router.
Protocol	This field specifies the IP protocol type. Choose between TCP and UDP protocol.
Source IP	This field specifies incoming IP address for which port forwarding is configured.
Source Netmask	This field specifies incoming IP address netmask for allowed IP subnet.
Source Interface	Select interface where port forwarding is done. Port forwarding from outside (WAN) interface to inside (LAN) interface is done on PPP, and in reverse direction on Ethernet interface.
Destination IP	This field specifies destination IP address for which port forwarding is configured.
Destination Netmask	This field specifies destination IP address netmask.
Destination Start Port	This is the TCP/UDP start port of incoming traffic.
Destination End Port	This is the TCP/UDP end port of incoming traffic.

Target IP	This field specifies to which address will traffic be forwarded.
Target Start Port	This field specifies starting port for which the traffic will be forwarded.
Target End Port	This field specifies ending port for which the traffic will be forwarded.
Add	Click ***Add*** to insert (add) new item in table to the GWG Gateway.
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 GWG Gateway. After pressing ***Save*** *button* it make take more than 10 seconds for router to save parameters and become operational again.

Table 7 – Port forwarding

Settings – Demilitarized Zone (DMZ)

DMZ (*Demilitarized Zone*) allows one IP Address to be exposed to the Internet. Because 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. In other words, this setting allows one local user to be exposed to the Internet to use a special–purpose services such as Internet gaming, Video–conferencing and etc. Host which will be exposed to the Internet must always have the same IP address, added manually or through DHCP server static lease.



DMZ Host

Demilitarized Zone Host Settings

☑ Enable

IP address from LAN: 192.168.1.105

Figure 21– DMZ configuration page

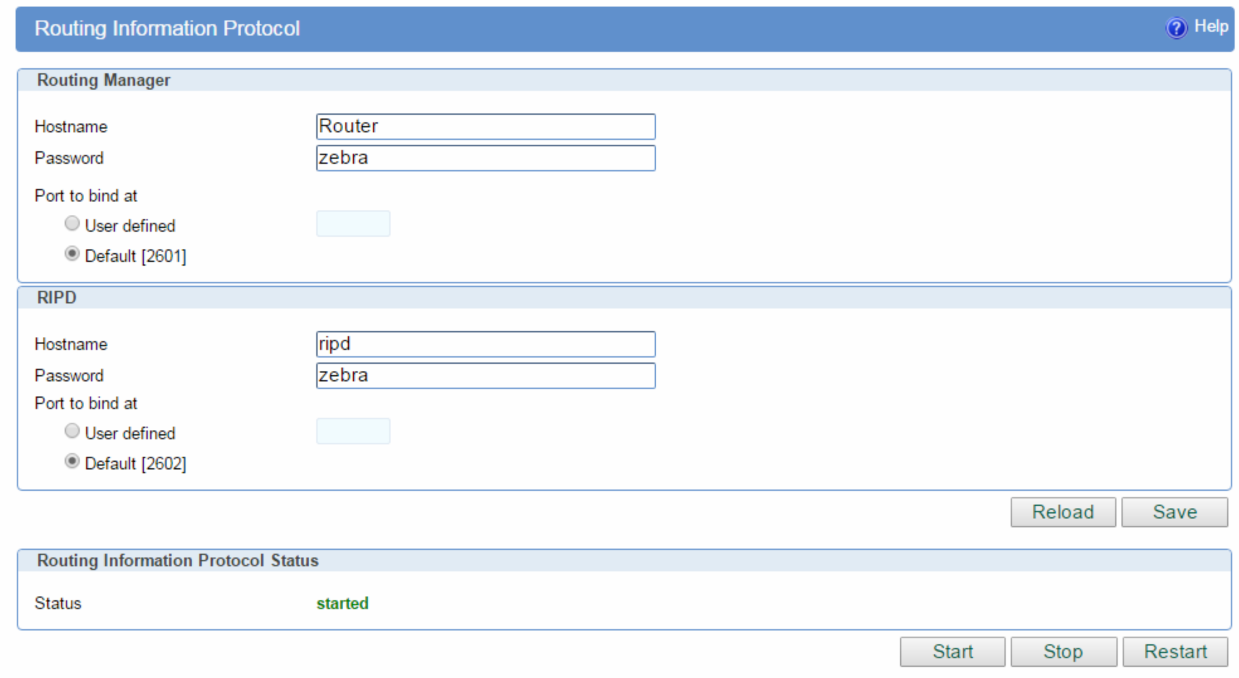
DMZ Settings	
Label	**Description**
	DMZ Settings
Enable	This field specifies if DMZ settings is enabled at the GWG Gateway.
IP address from LAN	IP address which will be exposed to the Internet. This will secure rest of the internal network from external access.
Reload	Click Reload to discard any changes and reload previous settings.
Save	Click Save to save your changes back to the Geneko Gateway.

Table 8- DMZ parameters

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 GWG Gateway RIP parameters.



Routing Manager

Hostname: Router
Password: zebra
Port to bind at
○ User defined
● Default [2601]

RIPD

Hostname: ripd
Password: zebra
Port to bind at
○ User defined
● Default [2602]

Routing Information Protocol Status

Status: started

Figure 22– RIP configuration page

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

Table 9 – RIP parameters

Important: settings must be saved from console in order to be returned after router reboot or export of configuration. It is done with command 'ripd# write' or 'ripd# copy running-config startup-config'.

RIP routing engine for the GWG Gateway

Use telnet to enter in global configuration mode.

telnet 192.168.1.1 2602 // telnet to br0 at TCP port 2602///

After telnet, type **enable** followed by **conf t** and **router rip** to enter RIP configuration mode.

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

- ripd(config-router)# **network** [A.B.C.D/Mask]

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

ripd(config-router)# **version [1|2]** // Same as other router //

Disable route redistribution:

- ripd(config-router)# **no redistribute kernel**
- ripd(config-router)# **no redistribute static**
- ripd(config-router)# **no redistribute connected**

Disable RIP update (optional):

- ripd(config-router)# **passive-interface br0**
- ripd(config-router)# **no passive-interface br0**

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:

- ripd(config-router)# **timers basic** [UPDATE-INTERVAL] [INVALID] [TIMEOUT] [GARBAGE-COLLECT]
- ripd(config-router)# **no timers basic**

Configure interface for RIP protocol (first type exit if you are at ripd(config-router) to get up from config-router to config mode).

- ripd(config)# **interface** greX
- ripd(config-if)# **ip rip send version** [VERSION]
- ripd(config-if)# **ip rip receive version** [VERSION]

Disable rip authentication at an interface.

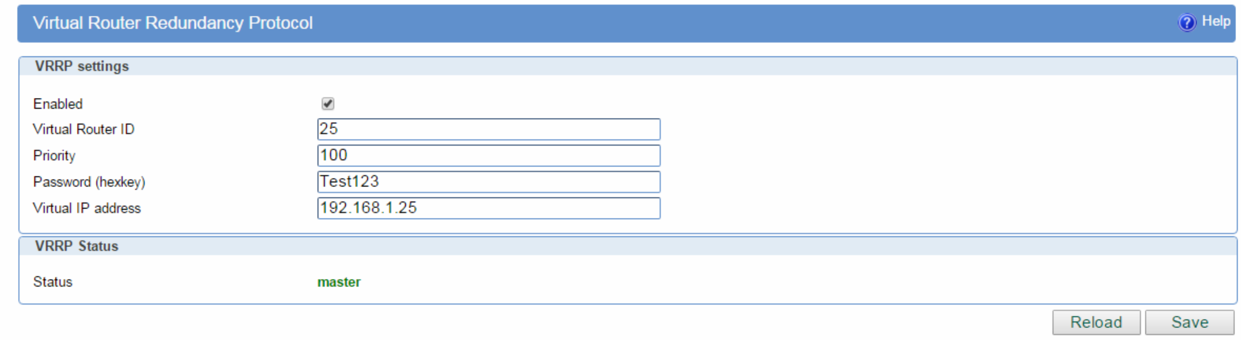
- ripd(config-if)# **no ip rip authentication mode** [md5 | text]

Debug commands:

- ripd(config)# **debug rip**
- ripd(config)# **debug rip events**
- ripd(config)# **debug rip packet**
- ripd(config)# **terminal monitor**

Routing – VRRP

Virtual Router Redundancy Protocol is a protocol which elects a master server on a LAN and the master answers to a 'virtual IP address'. If it fails, a backup server takes over the IP address.
VRRP specifies an election protocol to provide the virtual router function described earlier. All protocol messaging is performed using IP multicast datagrams, thus the protocol can operate over a variety of multi-access LAN technologies supporting IP multicast. Each VRRP virtual router has a single well-known MAC address allocated to it.



Virtual Router Redundancy Protocol

VRRP settings

Enabled ☑
Virtual Router ID 25
Priority 100
Password (hexkey) Test123
Virtual IP address 192.168.1.25

VRRP Status

Status master

Figure 23– VRRP

VRRP	
Label	**Description**
Enabled	Select this option to enable VRRPD service
Virtual Router ID	Enter Virtual Router Identifier (VRID) [1-255], which is the same for all physical routers for virtual router with this ID in the network.
Priority	Routers have a priority of between 1-255 and the router with the highest priority will become the master.
Password	Enter authentication password as hexkey[0-9a-fA-F]+.
Virtual IP address	Enter the IP address of the virtual server.
Reload	Click Reload to discard any changes and reload previous settings.
Save	Click Save to save changes.

Table 10- VRRP Parameters

Settings – VPN Settings

VPN (*Virtual private network*) 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:

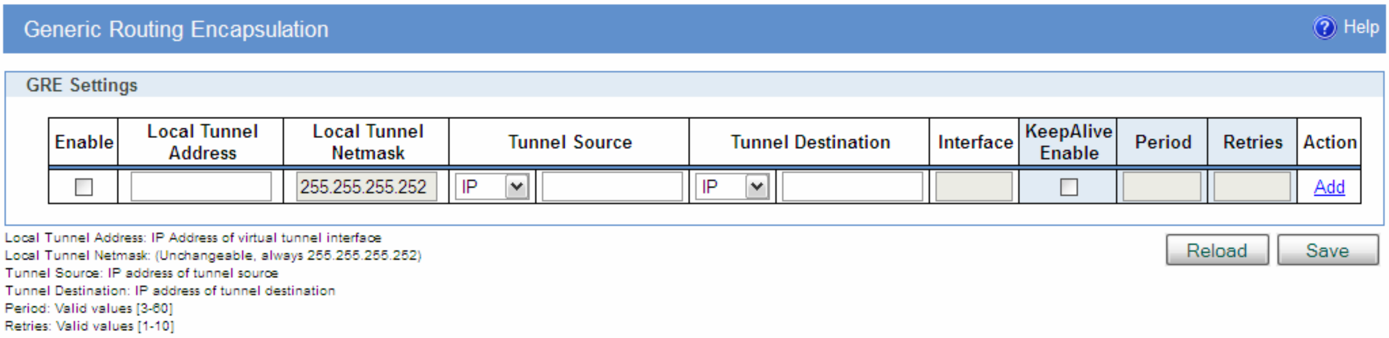
- You need to encrypt multicast traffic. GRE tunnels can carry multicast packets — just like real network interfaces — as opposed to using IPSec by itself, which can't encrypt multicast traffic. Some examples of multicast traffic are OSPF, EIGRP. Also, a number of video, VoIP, and streaming music applications 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 24 you can see screenshot of ***GRE*** Tab configuration menu.

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

Retries	Defines the number of retry times of 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 GWG Gateway.
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 GWG Gateway.

Table 11 – GRE parameters



Enable	Local Tunnel Address	Local Tunnel Netmask	Tunnel Source		Tunnel Destination		Interface	KeepAlive Enable	Period	Retries	Action
□		255.255.255.252	IP		IP			□			Add

Local Tunnel Address: IP Address of virtual tunnel interface
Local Tunnel Netmask: (Unchangeable, always 255.255.255.252)
Tunnel Source: IP address of tunnel source
Tunnel Destination: IP address of tunnel destination
Period: Valid values [3-60]
Retries: Valid values [1-10]

Figure 24– GRE tunnel parameters configuration page

GRE Keep alive

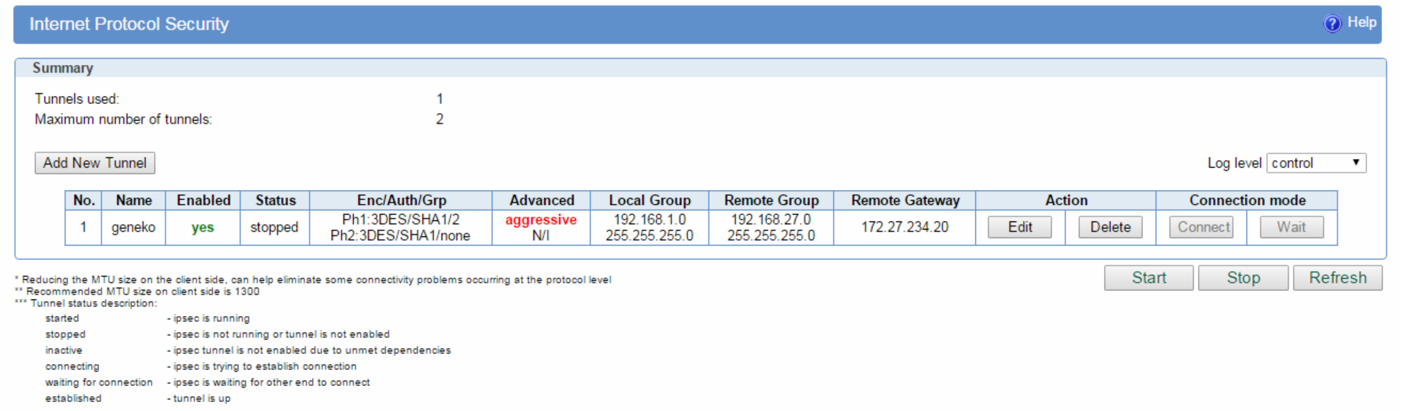
GRE tunnels can use periodic status messages, known as keepalives, to verify the integrity of the tunnel from end to end. By default, GRE tunnel keepalives are disabled. Use the keepalive checkbox to enable this feature. Keepalives do not have to be configured on both ends of the tunnel in order to work; 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)

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

Click ***VPN Settings - IPSec***, to open the VPN configuration screen. At the *Figure 25– IPSec Summary screen* you can see IPSec Summary. This screen gathers information about settings of all defined IPSec tunnels. Up to 3 IPSec tunnels can be defined on GWG Gateway.

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



Internet Protocol Security

Summary

Tunnels used: 1

Maximum number of tunnels: 2

Log level: control

No.	Name	Enabled	Status	Enc/Auth/Grp	Advanced	Local Group	Remote Group	Remote Gateway	Action		Connection mode	
1	geneko	yes	stopped	Ph1:3DES/SHA1/2 Ph2:3DES/SHA1/none	aggressive N/I	192.168.1.0 255.255.255.0	192.168.27.0 255.255.255.0	172.27.234.20	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:

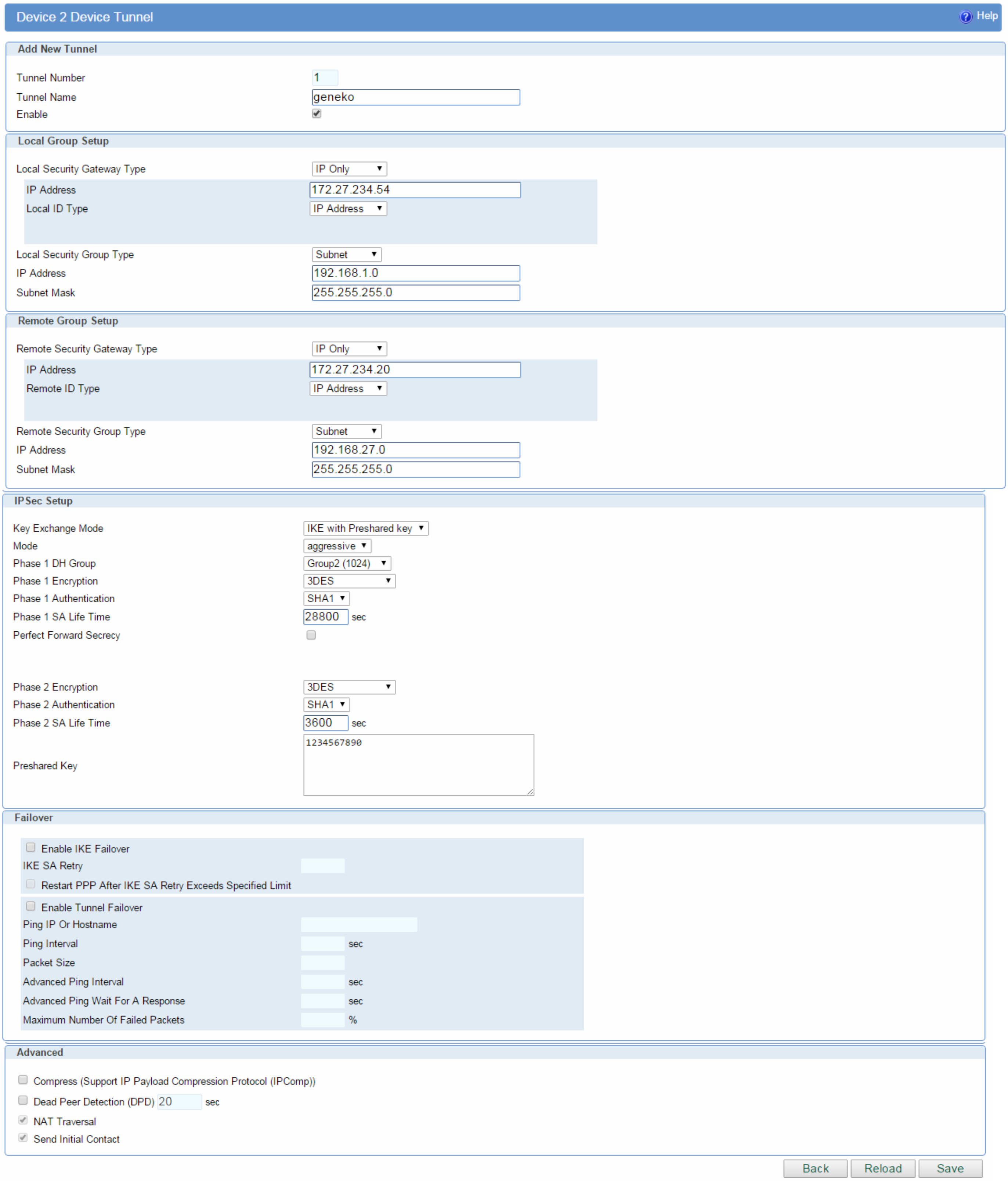
started	- ipsec is running
stopped	- ipsec is not running or tunnel is not enabled
inactive	- ipsec tunnel is not enabled due to unmet dependencies
connecting	- ipsec is trying to establish connection
waiting for connection	- ipsec is waiting for other end to connect
established	- tunnel is up

Figure 25– IPSec Summary screen

VPN Settings / IPSec Summary	
Label	**Description**
Tunnels Used	This is the number of currently configured IPSec tunnels.
Number of available tunnels	This is the number of available, not yet defined, IPSec tunnels.
No	This filed indicates the number of the IPSec tunnel.
Name	This field shows the Tunnel Name that you gave to the IPSec tunnel.
Enabled	This field shows if tunnel is enabled or disabled. After clicking on ***Start*** button, only enabled tunnels will be started.
Status	Field indicates status of the IPSec tunnel. Click on ***Refresh*** button to see current status of defined IPSec tunnels.
Enc/Auth/Grp	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.
Advanced	Field shows the chosen mode of IPSec and options from IPSec Advanced section by displaying the first letters of enabled options.
Local Group	Field shows the IP address and subnet mask of the Local Group.
Remote Group	Field displays the IP address and subnet mask of the Remote Group.
Remote Gateway	Field displays the gateway address of the Remote Group with which the tunnel is formed.
Action	Edit or Delete the tunnel.
Connection mode	Field displays connection mode of the current tunnel.
Log level	Set IPSec log level.
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 12 – IPSec Summary

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

Add New Tunnel

Tunnel Number	1
Tunnel Name	geneko
Enable	☑

Local Group Setup

Local Security Gateway Type	IP Only
IP Address	172.27.234.54
Local ID Type	IP Address
Local Security Group Type	Subnet
IP Address	192.168.1.0
Subnet Mask	255.255.255.0

Remote Group Setup

Remote Security Gateway Type	IP Only
IP Address	172.27.234.20
Remote ID Type	IP Address
Remote Security Group Type	Subnet
IP Address	192.168.27.0
Subnet Mask	255.255.255.0

IPSec Setup

Key Exchange Mode	IKE with Preshared key
Mode	aggressive
Phase 1 DH Group	Group2 (1024)
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

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

Figure 26– 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 GWG Gateway automatically appears. If the GWG Gateway is not yet connected to the GSM/UMTS/LTE network this field will be blank.
Local ID type	Authentication identity for one of the participant. It can be an IP address or a fully-qualified domain name preceded by @. When using certificates, this field must be filled with information from the certificate CN= field (for example FQDN is @vpn.something.com and user FQDN is someone@something.com if that's what's written in the certificate files).
Local Security Group Type	Define if only the computer with a specific IP address or whole subnet will be able to access the tunnel.
IP Address	Select the local LAN user(s) behind the Geneko 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.
Subnet Mask	Enter the subnet mask.
Remote 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 Remote Security Gateway Type you select should match the Local Security Gateway Type selected on the IPSec device at the other end of the tunnel.
IP Address	IP address of the remote end with which the tunnel will be formed.
Remote ID Type	Authentication identity for one of the participant. Can be an IP address or fully–qualified domain name preceded by @.
Remote Security Group Type	Define if only the computer with a specific IP address or whole subnet will be able to access the tunnel.
IP Address	Select the remote LAN user(s) behind the Geneko 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.
Subnet Mask	Enter the subnet mask.
IPSec Setup	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 for the encryption code. For key management, the Geneko Router uses only IKE with Preshared Key mode.
Key Exchange mode	**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 and the same key. **IKE with Preshared Key File** One or more files which contain preshared secret must be uploaded in the IPSec key file management menu. IMPORTANT: context of the file should be plain text and without space characters, so if a tool for generating secrets such as OpenSSL, OpenVPN or IPSec PKI commands were used, make sure there are no spaces for example like in term "----BEGIN CERTIFICATE----", where there is a space between words BEGIN and CERTIFICATE.. **IKE with X509 certificates and PSK** This option is used when X509 certificates are used for authentication. Certificate files must first be uploaded through pages which are in the main menu under file management. Pre shared key (PSK) is entered manually and must match on both peers. **IKE with X509 certificates and PSK file** This option is used when X509 certificates are used for authentication. Certificate files must first be uploaded through pages which are in the main menu under file management. Pre shared key file (PSK) is chosen from uploaded PSK files in the IPSec key file management and must match on both peers.
Mode	Mode of IPSec can be main or aggressive.
Phase 1 DH Group	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.
Phase 1 Encryption	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). 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.
Phase 1 Authentication	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.
Phase 1 SA Life Time	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.
Perfect Forward Secrecy	If the Perfect Forward Secrecy (PFS) feature is enabled, IKE Phase 2 negotiation 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.
Phase 2 DH Group	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.
Phase 2 Encryption	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). 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
Phase 2 Authentication	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.
Phase 2 SA Life Time	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.
Preshared Key	This specifies the pre-shared key used to authenticate the remote IKE peer. Enter a key 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.
Key File	Select which key file to use.
CA Certificate	Select which CA certificate file to use.
Local Client Certificate	Select which Local Client Certificate file to use.
Local Client Key	Select which Local Client Key file to use.
Enable IKE failover	Enable IKE failover option which will try to periodically re-establish security association.
IKE SA retry	Number of IKE retries before failover occurs.
Enable Tunnel Failover	Enables tunnel failover. If there is more than one tunnel defined, this option will failover to other tunnel in case that selected one fails to establish connection.
Ping IP or Hostname	IP address on other side of tunnel which will be pinged in order to determine current state.
Ping interval	Specify time period in seconds between two pings.
Packet size	Specify size of data field in IP packet for ping message.
Maximum number of failed packets	Set percentage of failed packets until failover action is performed.
Compress (Support IP Payload Compression Protocol (IP Comp))	IP Payload Compression is a protocol that reduces the size of IP datagram. Select this option if you want the Geneko Router to propose compression when it initiates a connection.
Dead Peer Detection (DPD)	When DPD is enabled, the Geneko 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 Geneko 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.
NAT Traversal	Both the IPSec initiator and responder must support the mechanism for detecting the NAT gateway in the path and changing to a new port, as defined in RFC 3947. 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.
Send initial contact	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.
Back	Click ***Back*** to return on IPSec Summary screen.
Reload	Click ***Reload*** to discard any changes and reload previous settings.
Save	Click ***Save*** to save your changes back to the GWG Gateway. After that router goes back and begin negotiations of the tunnels by clicking on the ***Start***.

Table 13 – IPSec Parameters

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 multi-client–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.

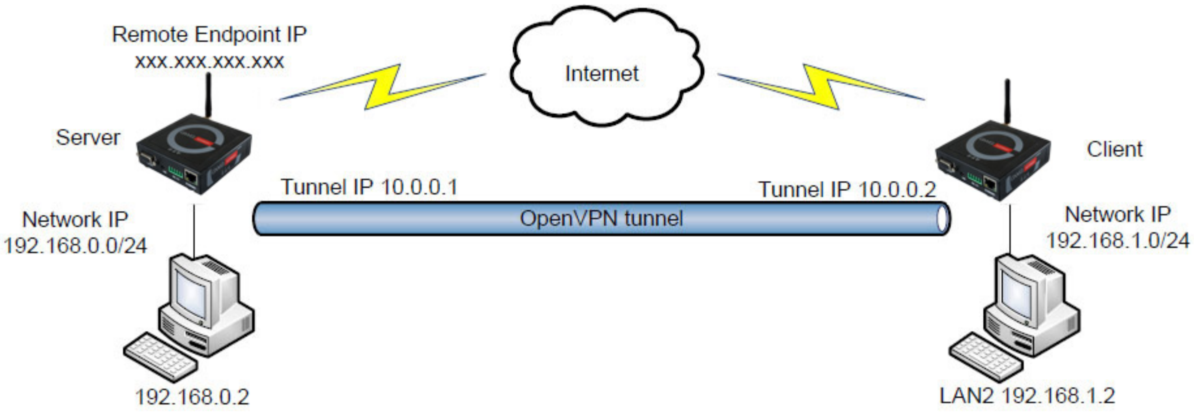
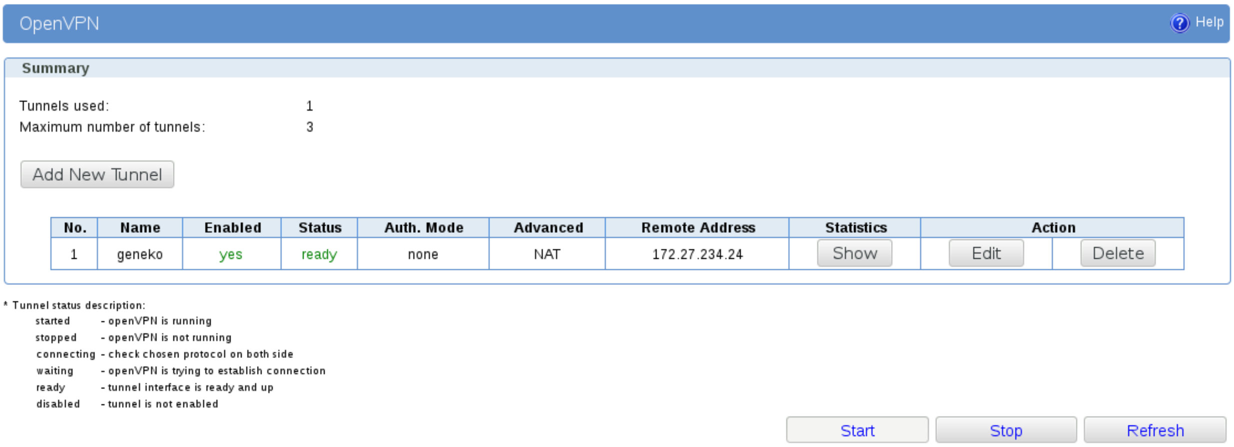


Figure 27– OpenVPN example

Click ***VPN Settings -OpenVPN***, to open the VPN configuration screen. At the Figure 28 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.



Summary

Tunnels used: 1

Maximum number of tunnels: 3

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

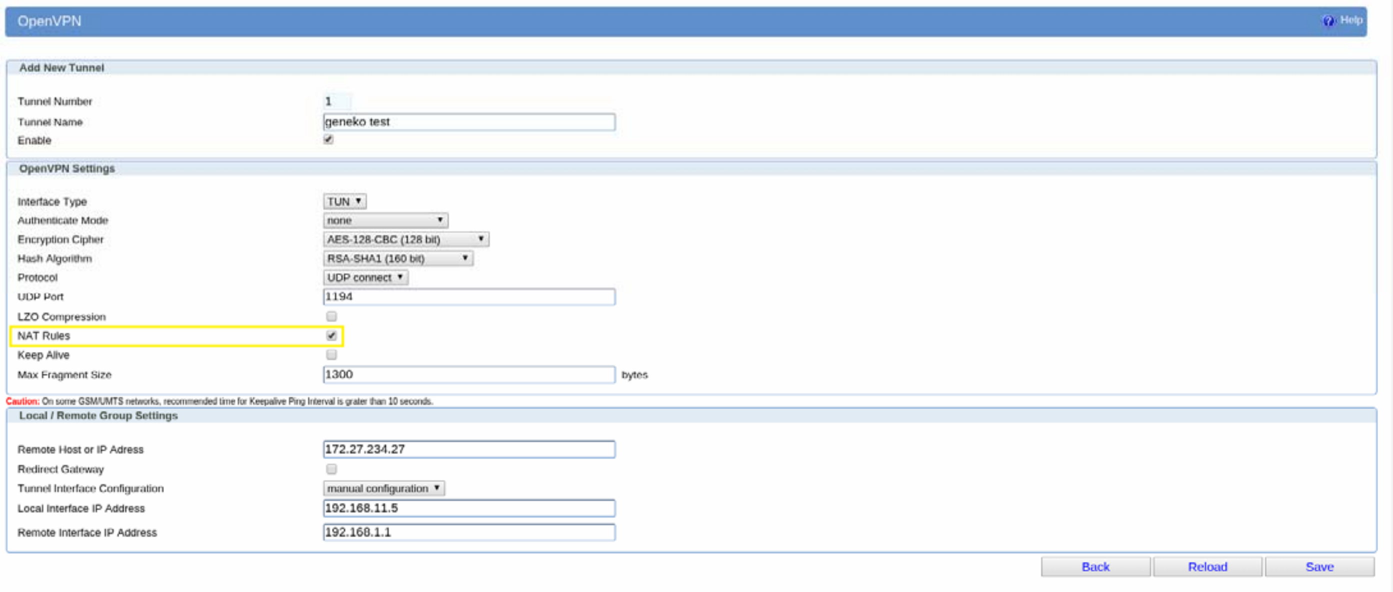
Figure 28-Open VPN Summary screen

OpenVPN	
Label	**Description**
Tunnel Used	This number will be generated automatically and it represents a number of configured tunnels.
Maximum number of tunnels	This is the maximum number of allowed OpenVPN tunnels
No.	This filed indicates the number of the OpenVPN tunnel
Name	This field shows the Tunnel Name that you gave to the OpenVPN tunnel.
Enabled	This field shows if tunnel is enabled or disabled. After clicking on Start button, only enabled tunnels will be started.
Status	This field indicates status of the OpenVPN tunnel. Click on Refresh button to see current status of defined OpenVPN tunnels.
Auth Mode	This field shows authentication mode being used.
Advanced	This field shows the additional chosen options for OpenVPN tunnel.
Remote Address	This field displays the IP address of remote peer. If tunnel is in wait or client state, X letter will appear.
Show	This button opens a detailed statistics window for the tunnel.
Delete	Click on this link to delete the tunnel and all settings for that particular tunnel.
Edit	This link opens screen where you can change the tunnel's settings.
Add New Tunnel	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.
Start	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.
Stop	This button will stop all OpenVPN started negotiations.

Refresh	Click on this button to refresh the Status field in the Summary table.
OpenVPN Settings	
Tunnel Number	This number will be generated automatically and it represents a number of the tunnel.
Tunnel Name	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.
Enable	Check this box to enable this particular OpenVPN tunnel.
Interface Type	Select TUN or TAP mode.
Authenticate Mode	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.
Encryption Cipher	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.
Hash Algorithm	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.
Protocol	Select a protocol you want to use for tunnel connection. UDP connect and TCP client will need the "Remote Host or IP Adress" field in order to successfully establish a tunnel.
UDP Port/TCP Port	Enter a port number for a tunnel connection.
LZO Compression	Use fast LZO compression. This may add up to 1 byte per packet for incompressible data.
NAT Rules	**NAT Rules is enabled by default.**
Keep Alive	Use this mechanism to keep tunnel alive.
Ping Interval	Ping interval for sending pings over the TCP/UDP control channels. Number of seconds is specified in this field.
Ping Timeout	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.

Max Fragment Size	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.
Pre-shared Secret	Use Static Key encryption mode (non-TLS).
Generate PSK	Check this option and use "Generate" button to produce a pre-shared secret.
Paste	Use this option to manualy paste a pre-shared secret from remote host's PSK file.
CA Certificate	Certificate authority (CA) file, also referred to as the root certificate.
DH Group	Choose a Diffie Hellman parameter group. This parameters may be considered public. Available only in X.509 server mode.
Username	Enter a username for authentication to the remote host server.
Password	Enter a password for authentication to the remote host server.
Local Certificate	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 Adress	Enter a remote peer IP address or host name. This filed 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 tunel interface always points to the local endpoint of the server's tunel 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 tunel 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 14 – OpenVPN parameters



OpenVPN

Add New Tunnel

Tunnel Number	1
Tunnel Name	geneko test
Enable	☑

OpenVPN Settings

Interface Type	TUN ▾
Authenticate Mode	none ▾
Encryption Cipher	AES-128-CBC (128 bit) ▾
Hash Algorithm	RSA-SHA1 (160 bit) ▾
Protocol	UDP connect ▾
UDP Port	1194
LZO Compression	□
NAT Rules	☑
Keep Alive	□
Max Fragment Size	1300 bytes

Caution: On some GSM/UMTS networks, recommended time for Keepalive Ping Interval is grater than 10 seconds.

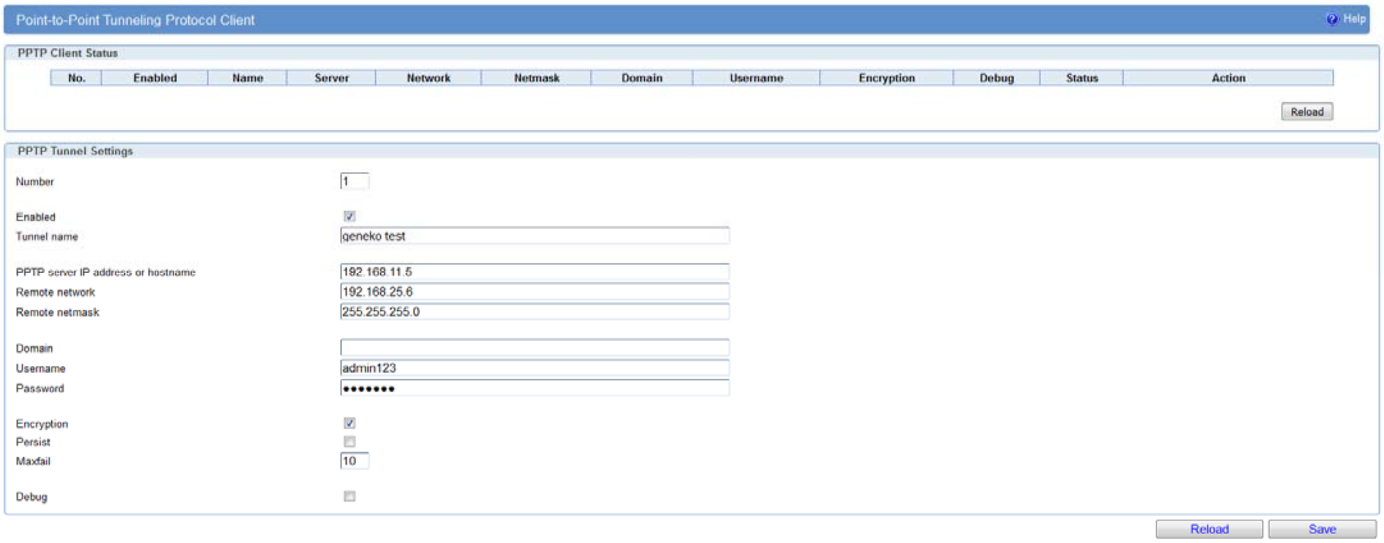
Local / Remote Group Settings

Remote Host or IP Adress	172.27.234.27
Redirect Gateway	□
Tunnel Interface Configuration	manual configuration ▾
Local Interface IP Address	192.168.11.5
Remote Interface IP Address	192.168.1.1

Figure 29– OpenVPN configuration page

Settings – PPTP

The Geneko Router can be used as a PPTP (Point-to-Point Tunneling Protocol) client. PPTP enables the secure transfer of data from a remote computer to a private server by creating a VPN connection across IP-based data networks. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets.



Point-to-Point Tunneling Protocol Client

PPTP Client Status

No.	Enabled	Name	Server	Network	Netmask	Domain	Username	Encryption	Debug	Status	Action

PPTP Tunnel Settings

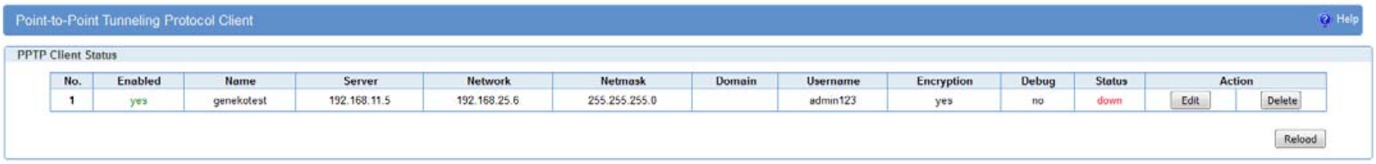
Number	1
Enabled	☑
Tunnel name	geneko test
PPTP server IP address or hostname	192.168.11.5
Remote network	192.168.25.6
Remote netmask	255.255.255.0
Domain	
Username	admin123
Password	•••••••
Encryption	☑
Persist	□
Maxfail	10
Debug	□

Figure 30–PPTP configuration page

PPTP	
Label	**Description**
Number	Selected tunnel number. Number of PPTP tunnels is limited to 5.
Enabled	Select this option to enable tunnel.

Tunnel name	Unique tunnel identifier.
PPTP server IP address or hostname	IPv4 address of remote PPTP server.
Remote Netmask	Netmask of remote subnet to route.
Domain	Some PPTP servers require domain name of authentication.
Username	Username to authenticate to the remote server.
Password	Password to authenticate to the remote server.
Encryption	Leave this option enabled to use default MPPE (Microsoft encryption) and MPPC (Microsoft compression) protocols.
Persist	If this option enabled to use default MPPE (Microsoft encryption) and MPPC (Microsoft compression) protocols.
Maxfail	Max number of retries to reconnect. 0 for infinite retries.
Debug	Enable extra information in system log.
Edit	Click **Edit** to edit selected tunnel from the table.
Delete	Click **Delete** to delete selected tunnel from table.
Reload	Click **Reload** to discard any changes and reload previous settings.
Save	Click **Save** to create new, or save changes to existing tunnel.

Table 15- PPTP Parameters

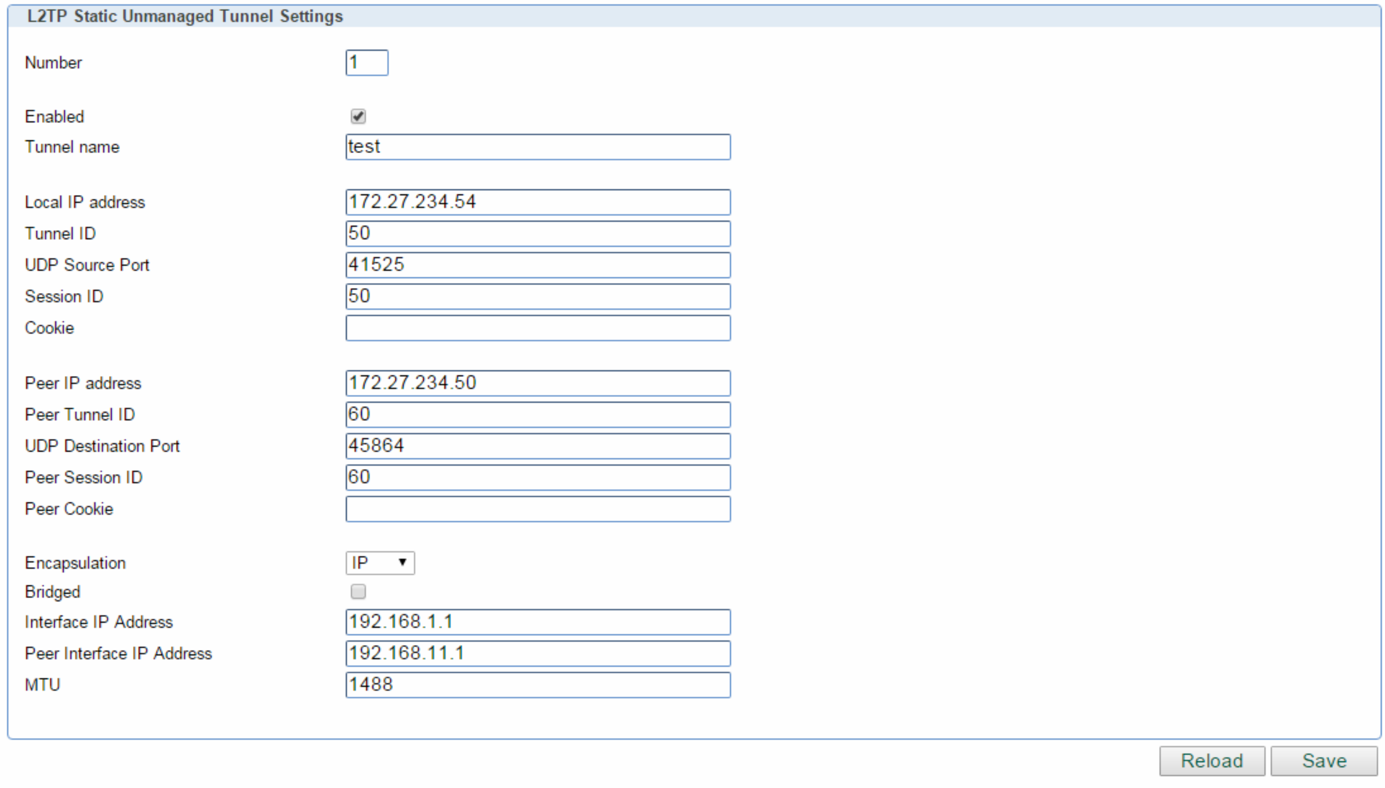


No.	Enabled	Name	Server	Network	Netmask	Domain	Username	Encryption	Debug	Status	Action	
1	yes	genekotest	192.168.11.5	192.168.25.6	255.255.255.0		admin123	yes	no	down	Edit	Delete

Figure 31–PPTP Summary screen

Settings – L2TP

L2TP is suitable for Layer-2 tunneling. Static tunnels are useful to establish network links across IP networks when the tunnels are fixed. L2TP tunnels can carry data of more than one session. Each session is identified by a session id and its parent tunnel's tunnel id. A tunnel must be created before a session can be placed in the tunnel.



L2TP Static Unmanaged Tunnel Settings

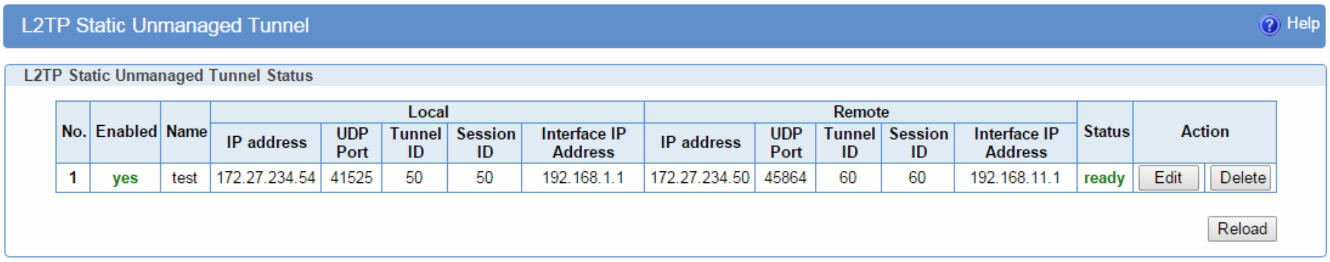
Number	1
Enabled	☑
Tunnel name	test
Local IP address	172.27.234.54
Tunnel ID	50
UDP Source Port	41525
Session ID	50
Cookie	
Peer IP address	172.27.234.50
Peer Tunnel ID	60
UDP Destination Port	45864
Peer Session ID	60
Peer Cookie	
Encapsulation	IP
Bridged	□
Interface IP Address	192.168.1.1
Peer Interface IP Address	192.168.11.1
MTU	1488

Figure 32– L2TP configuration page

L2TP	
Label	**Description**
Number	Selected tunnel number. Number of L2TP tunnels is limited to 5.
Enabled	Select this option to enable L2TP tunnel.
Tunnel name	Unique tunnel identifier.
Local IP address	Set the IP address of the local interface to be used for the tunnel. This address must be the address of a local interface.
Tunnel ID	Set the tunnel id, which is a 32-bit integer value. Uniquely identifies the tunnel. The value used must match the peer tunnel id value being used at the peer.
UDP Source Port	Set the UDP source port to be used for the tunnel. Must be present when udp encapsulation is selected. Ignored when ip encapsulation is selected.
Session ID	Set the session id, which is a 32-bit integer value. Uniquely identifies the session being created. The value used must match the peer_session id value being used at the peer.
Cookie	Sets an optional cookie value to be assigned to the session. This is a 4 or 8 byte value, specified as 8 or 16 hex digits, e.g. 014d3636deadbeef. The value must match the peer cookie value set at the peer. The cookie value is carried in L2TP data packets and is checked for expected value at the peer. Default is to use no cookie.
Peer IP address	Set the IP address of the remote peer.
Peer Tunnel ID	Set the peer tunnel id, which is a 32-bit integer value assigned to the tunnel by the peer. The value used must match the tunnel id value being used at the peer.
UDP Destination Port	Set the UDP destination port to be used for the tunnel. Must be present when UDP encapsulation is selected. Ignored when IP encapsulation is selected.

Peer Session ID	Set the peer session id, which is a 32-bit integer value assigned to the session by the peer. The value used must match the session ID value being used at the peer.
Peer Cookie	Sets an optional peer cookie value to be assigned to the session. This is a 4 or 8 byte value, specified as 8 or 16 hex digits, e.g. 014d3636deadbeef. The value must match the cookie value set at the peer. It tells the local system what cookie value to expect to find in received L2TP packets. Default is to use no cookie
Encapsulation	Set the encapsulation type of the tunnel. Valid values for encapsulation are: UDP, IP.
Bridged	The two interfaces can be configured with IP addresses if only IP data is to be carried. To carry non-IP data, the L2TP network interface is added to a bridge instead of being assigned its own IP address. Since raw ethernet frames are then carried inside the tunnel, the MTU of the L2TP interfaces must be set to allow space for those headers.
Interface IP Address	Local private P-t-P IP address.
Peer Interface IP Address	Remote private P-t-P IP address.
MTU	MTU of the L2TP interface. Default 1446 for bridged or 1488 for Layer 3 tunnel.
Edit	Click Edit to edit selected tunnel from the table.
Delete	Click Delete to delete selected tunnel from table.
Reload	Click Reload to discard any changes and reload previous settings.
Save	Click Save to create new, or save changes to existing tunnel.

Table 16- L2TP Parameters



L2TP Static Unmanaged Tunnel Status

No.	Enabled	Name	Local					Remote					Status	Action
			IP address	UDP Port	Tunnel ID	Session ID	Interface IP Address	IP address	UDP Port	Tunnel ID	Session ID	Interface IP Address		
1	yes	test	172.27.234.54	41525	50	50	192.168.1.1	172.27.234.50	45864	60	60	192.168.11.1	ready	Edit Delete

Figure 33– L2TP Summary screen

File management – CA Certificate

CA Certificate page is used to manage CA certificate files so they can be used for peer authentication.

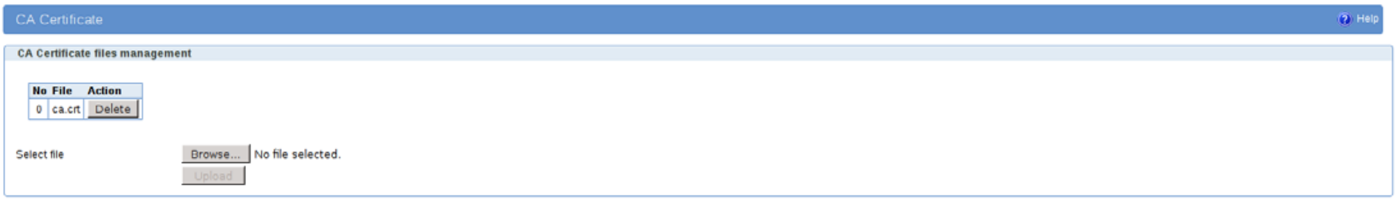
Certification authority (CA) certificates are certificates that are issued by a CA to itself or to a second CA for the purpose of creating a defined relationship between the two CAs. A certificate that is issued by a CA to itself is referred to as a trusted root certificate, because it is intended to establish a point of ultimate trust for a CA hierarchy. Once the trusted root has been established, it can be used to authorize subordinate CAs to issue certificates on its behalf. Although the relationship between CAs is most commonly hierarchical, CA certificates can also be used to establish trust relationships between CAs in two different public key infrastructure (PKI) hierarchies. In all of these cases, the CA certificate is critical to defining the certificate path and usage restrictions for all end entity certificates issued for use in the PKI.

Usually this file is called ca.crt and it can be generated with various tools, for example with OpenSSL, OpenVPN e.t.c. (For details visit OpenVPN HOWTO website. There is instruction of generating certificates and keys).

There are options to first browse for the file, then to upload the file. After one or more files are uploaded, a table with uploaded files is shown with the option to delete each of them if they are no longer needed.

CA Certificate	
Label	**Description**
No	Ordinal number of the file.
File	Filename of the file.
Action	Action field shows the delete button for deleting the file.
Select file	This field shows the browse button for finding the file on local computer which will be uploaded.
Upload	This is the upload button, it is used to start the upload of the file.

Table 17– CA Certificate parameters



CA Certificate

CA Certificate files management

No	File	Action
0	ca.crt	Delete

Select file No file selected.

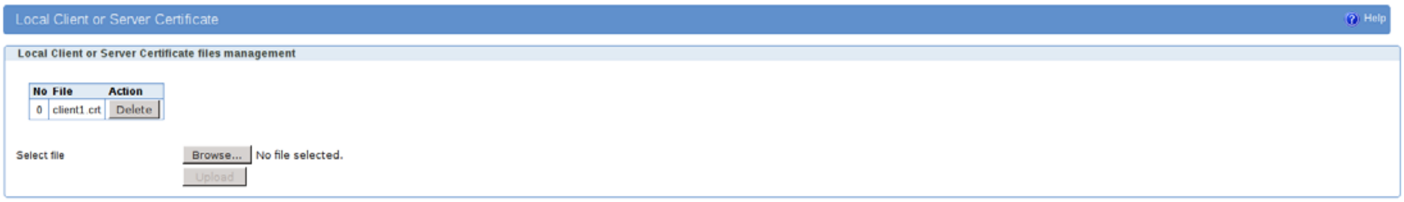
Figure 34– CA Certificate screen

File management – Private Certificate

Local Certificate page is used to manage local client certificate files so they can be used for peer authentication.

In cryptography, a client certificate is a type of digital certificate that is used by client systems to make authenticated requests to a remote server. Client certificates play a key role in many mutual authentication designs, providing strong assurances of a requester's identity. Usually this file is called client1.crt and it can be generated with various tools, for example with OpenSSL e.t.c. (For details visit OpenVPN HOWTO website. There is instruction of generating certificates and keys).

On the web interface is option to browse for the file first, then to upload the file. After one or more files are uploaded, a table with uploaded files is shown with the option to delete each of them if they are no longer needed.



Local Client or Server Certificate

Local Client or Server Certificate files management

No	File	Action
0	client1.crt	Delete

Select file No file selected.

Figure 35– Local Certificate screen

Local Client Certificate files management	
Label	**Description**
Filename	Filename of the file.
Delete	Delete button for deleting the file.

Details	Details button for displaying details about the certificate (issuer, valid from, valid until)
Select file for upload	This field shows the browse button for finding the file on local computer which will be uploaded.
Upload	This is the upload button, it is used to start the upload of the file.

Table 18-Local Certificate parameters

File management – Private Key

This page is used to manage local client or server key files so they can be used for peer authentication.

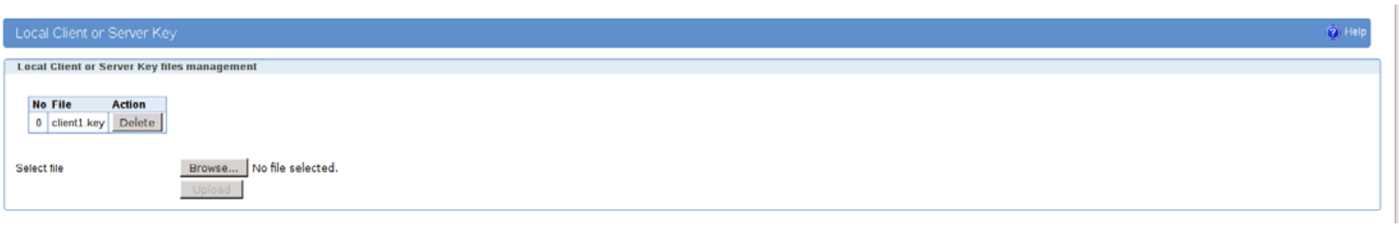
In public key infrastructure (PKI) systems, a certificate signing request (also CSR or certification request) is a message sent from an applicant to a certificate authority in order to apply for a digital identity certificate.

Before creating a CSR, the applicant first generates a key pair, keeping the private key secret. The CSR contains information identifying the applicant (such as a distinguished name in the case of an X.509 certificate) which must be signed using the applicant's private key. The CSR also contains the public key chosen by the applicant. The CSR may be accompanied by other credentials or proofs of identity required by the certificate authority, and the certificate authority may contact the applicant for further information.

The three main parts that a certification request consists of are the certification request information, a signature algorithm identifier, and a digital signature on the certification request information. The first part contains the significant information, including the public key. The signature by the requester prevents an entity from requesting a bogus certificate of someone else's public key. Thus the private key is needed to produce, but it is not part of, the CSR.

Private Key File Management	
Label	**Description**
Filename	Filename of the file.
Delete	Delete button for deleting the file.
Details	Details button for displaying details about the certificate (issuer, valid from, valid until)
Select file for upload	This field shows the browse button for finding the file on local computer which will be uploaded.
Upload	This is the upload button ,it is used to start the upload of the file.

Table 19–Private Key parameters



Local Client or Server Key

Local Client or Server Key files management

No	File	Action
0	client1.key	Delete

Select file: Browse... No file selected.

Figure 36– Private Key screen

File management – CRL Certificates

This page is used to manage Certificate Revocation List certificate files so they can be used for validating certificates. In the operation of some cryptosystems, usually public key infrastructures (PKIs), a certificate revocation list (CRL) is a list of certificates (or more specifically, a list of serial numbers for certificates) that have been revoked, and therefore, entities presenting those (revoked) certificates should no longer be trusted. There are two different states of revocation defined in RFC 3280: revoked and hold. Usually this file is called crl.crl or crl.pem and it can be generated with various tools, for example with OpenSSL. (For details visit OpenVPN HOWTO website. There is instruction of generating certificates and keys).

CRL Certificate	
Label	**Description**
Filename	Filename of the file.
Delete	Delete button for deleting the file.
Details	Details button for displaying details about the certificate (issuer, valid from, valid until).
Select file for upload	This field shows the browse button for finding the file on local computer which will be uploaded.
Upload	This is the upload button, it is used to start the upload of the file.

Table 20–CRL Certificates

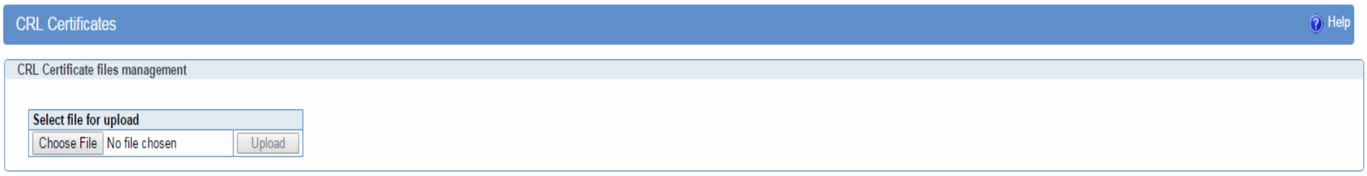


Figure 37– CRL Certificates

File management – Preshared Key Files

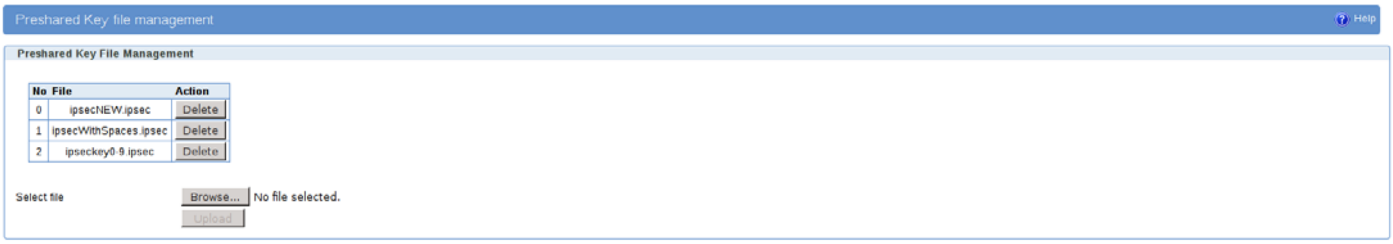
This page is used to manage textual key files with shared secret written into them so the same file can be used on more peers for their authentication.

IMPORTANT: context of the file should be plain text and without space characters, so if a tool for generating secrets such as OpenSSL, OpenVPN or IPSec PKI commands were used, make sure there are no spaces for example like in term "----BEGIN CERTIFICATE----", where there is a space between words BEGIN and CERTIFICATE. There are options to first browse for the file, then to upload the file. After one or more files are uploaded, a table with uploaded files is shown with the option to delete each of them if they are no longer needed.

Preshared Key Files	
Label	**Description**
Filename	Filename of the file.
Delete	Delete button for deleting the file.

Details	Details button for displaying contents of the file.
Select file for upload	This field shows the browse button for finding the file on local computer which will be uploaded.
Upload	This is the upload button ,it is used to start the upload of the file.

Table 21–Preshared Key Files



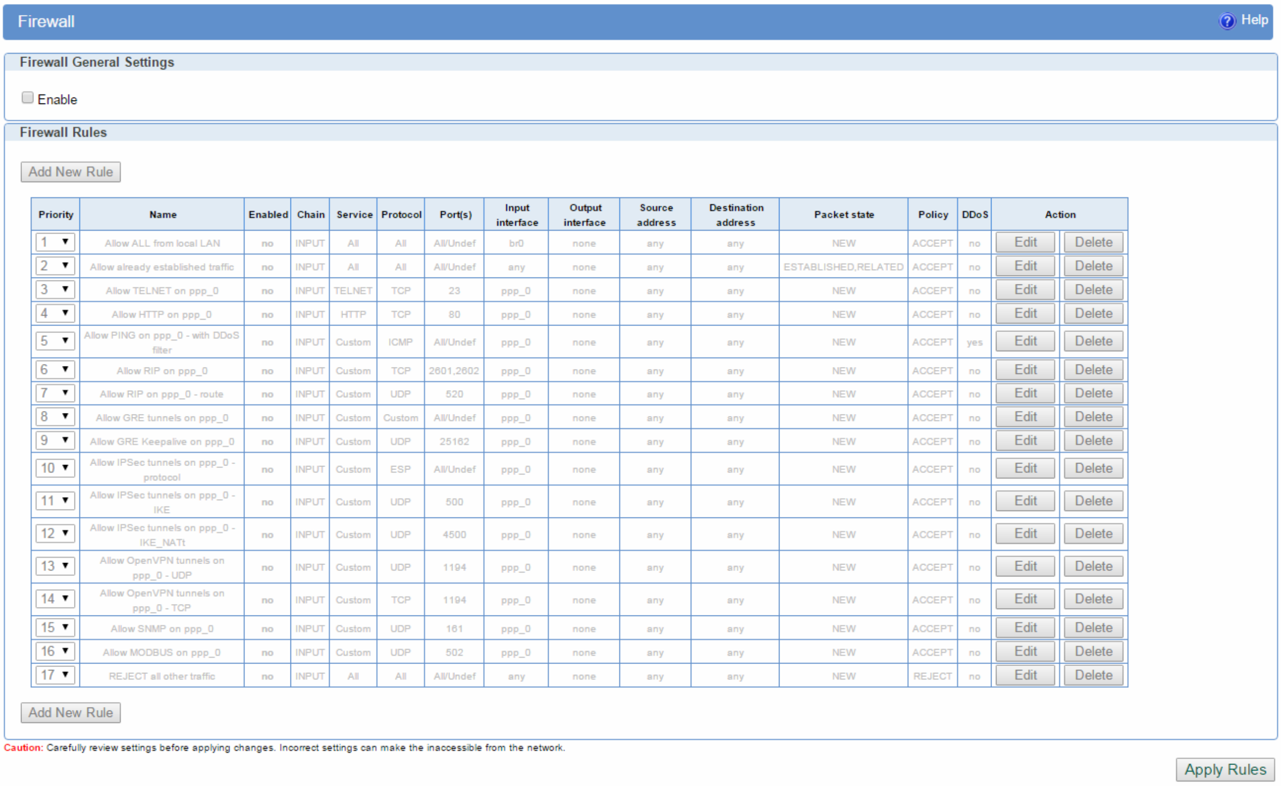
No	File	Action
0	ipsecNEW.ipsec	Delete
1	ipsecWithSpaces.ipsec	Delete
2	ipseckey0-9.ipsec	Delete

Select file Browse... No file selected.

Figure 38-Preshared Key screen

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 of 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.



□ Enable

Priority	Name	Enabled	Chain	Service	Protocol	Port(s)	Input interface	Output interface	Source address	Destination address	Packet state	Policy	DDoS	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 DDoS 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_NATt	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 MODBUS 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

Caution: Carefully review settings before applying changes. Incorrect settings can make the inaccessible from the network.

Figure 39– Firewall configuration page

Firewall	
Label	**Description**
	Firewall Rule Basic
Enable Firewall	This field specifies if Firewall is enabled at the router.
	Firewall Rule Settings
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 specifies 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.
Port(s)	This field specifies a service port with predefined or custom defined values.
Input Interface	Select the name of an interface via which a packet was received (only for packets entering the INPUT and FORWARD chains).
Output Interface	Select the name of an interface via which a packet is going to be sent (for packets entering the FORWARD and OUTPUT chains).
Source address	Field shows source IP address of the packet. It can be single IP address, range of IP addresses or "any".
Destination address	Destination IP address for the packet. It can be single IP address, range of IP addresses or "any".
Packet state	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.
Policy	Field shows selected firewall policy: ACCEPT, REJECT or DROP. If selected policy is REJECT field displays chosen reject type of the firewall rule.
DDos	This field shows if Distributed Denial of Service is disabled or enabled.
Edit	This link opens screen where you can change the rule’s settings.
Delete	Click on this link to delete the rule and all settings for that particular rule.
Add New Rule	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.
Apply rules	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.

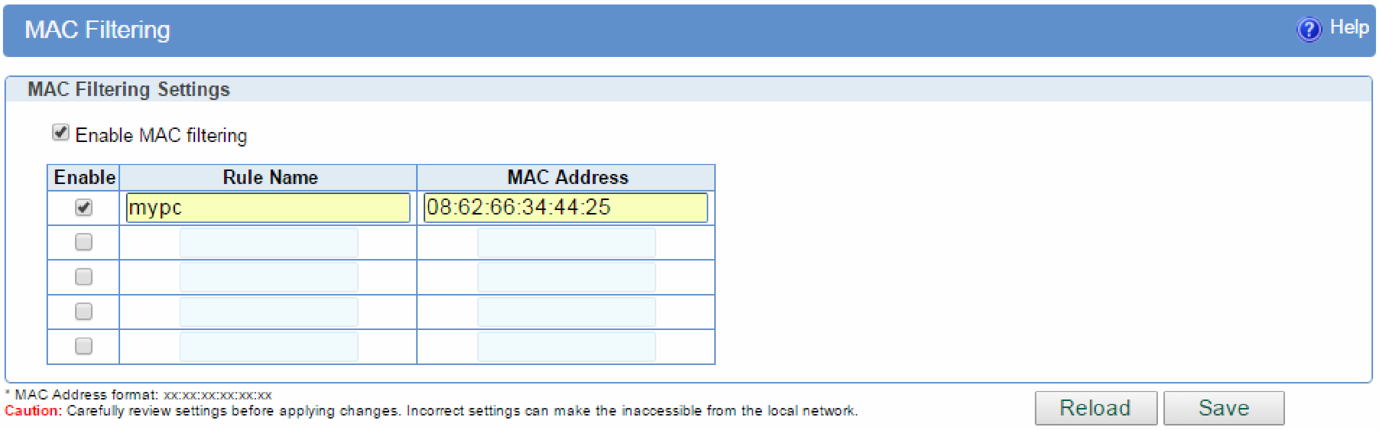
Table 22 – Firewall parameters

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 dropped.

MAC Filtering Settings	
Label	**Description**
Enable MAC Filtering	This field specifies if MAC Filtering is enabled at the router
Enable	Enable MAC filtering for a specific MAC address
Name	Field shows the Rule Name that is given to the MAC filtering rule.
MAC address	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 23 - MAC filtering parameters



MAC Filtering Settings

☑ Enable MAC filtering

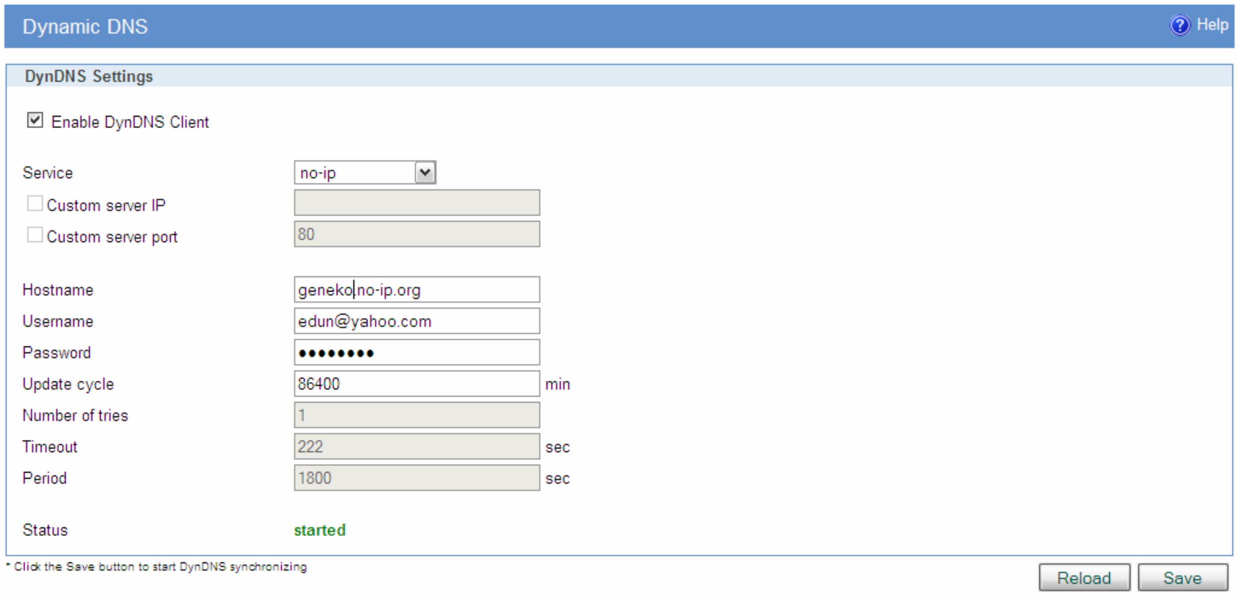
Enable	Rule Name	MAC Address
☑	mypc	08:62:66:34:44:25
☐		
☐		
☐		
☐		

* MAC Address format: xx:xx:xx:xx:xx:xx
Caution: Carefully review settings before applying changes. Incorrect settings can make the inaccessible from the local network.

Figure 40– MAC filtering configuration page

Settings – Dynamic DNS

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 41.



Dynamic DNS

DynDNS Settings

☑ Enable DynDNS Client

Service: no-ip

□ Custom server IP:

□ Custom server port: 80

Hostname: geneko.no-ip.org

Username: edun@yahoo.com

Password: ••••••••

Update cycle: 86400 min

Number of tries: 1

Timeout: 222 sec

Period: 1800 sec

Status: started

* Click the Save button to start DynDNS synchronizing

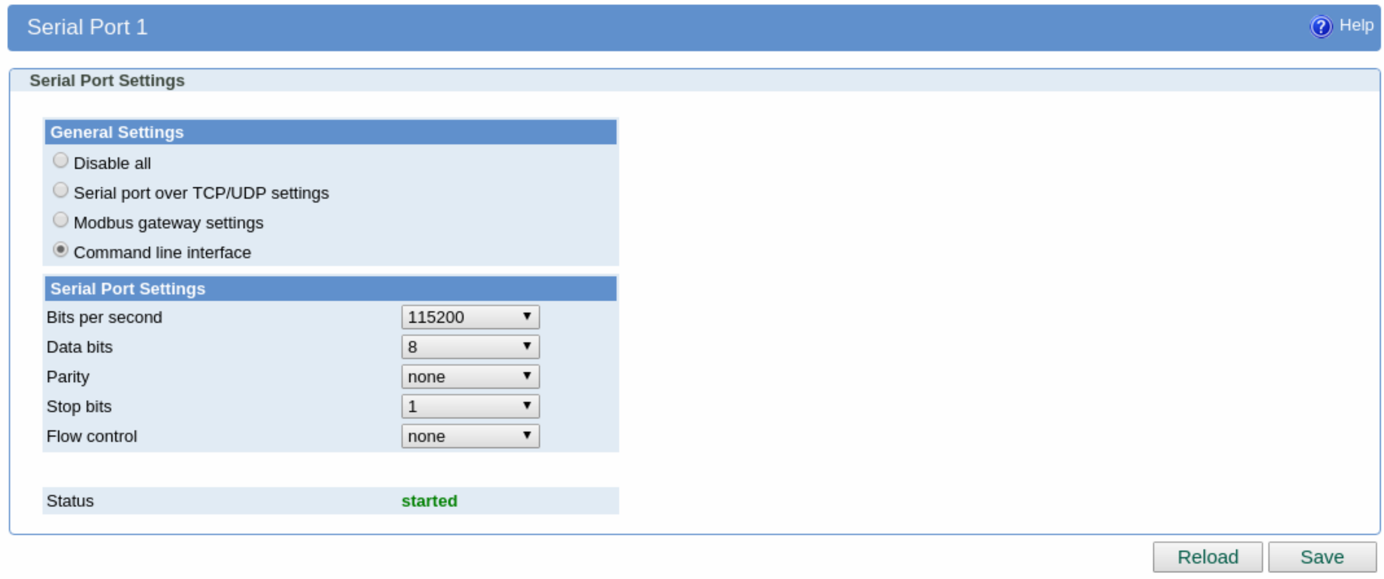
Figure 41– DynDNS settings

DynDNS	
Label	**Description**
Enable DynDNS Cilent	Enable DynDNS Client.
Service	The type of service that you are using (dhs, pgpow, dyndns, dyndns-static, dyndns-custom, ods, easydns, dyns, justlinux, zoneedit and no-ip).
Custom Server IP or Hostname	The server IP or Hostname to connect to.
Custom Server port	The server port to connect to.
Hostname	String to send as host parameter.
Username	User ID
Password	User password.
Update cycle	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.
Number of tries	Number of tries (default: 1) if network problem.
Timeout	The amount of time to wait between retries.
Period	Time between update retry attempts, default value is 1800.
Reload	Click ***Reload*** to discard any changes and reload previous settings.
Save	Click ***Save*** to save your changes back to the GWR Router.

Table 24 – DynDNS parameters

Settings – Serial Port 1

The Geneko GWG Gateway provides a way for a user to connect from a network connection to a serial port. **USB port** works as a serial port, too. 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 Geneko Gateway supports RFC 2217 (remote control of serial port parameters). Modbus 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 converter.



Serial Port Settings

General Settings

○ Disable all
○ Serial port over TCP/UDP settings
○ Modbus gateway settings
● Command line interface

Serial Port Settings

Bits per second	115200
Data bits	8
Parity	none
Stop bits	1
Flow control	none

Status started

Figure 42– Serial Port Settings initial menu

Settings – Serial Port 2

Serial port over TCP/UDP settings

The GWG Gateway 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 GWG Gateway supports RFC 2217 (remote control of serial port parameters).

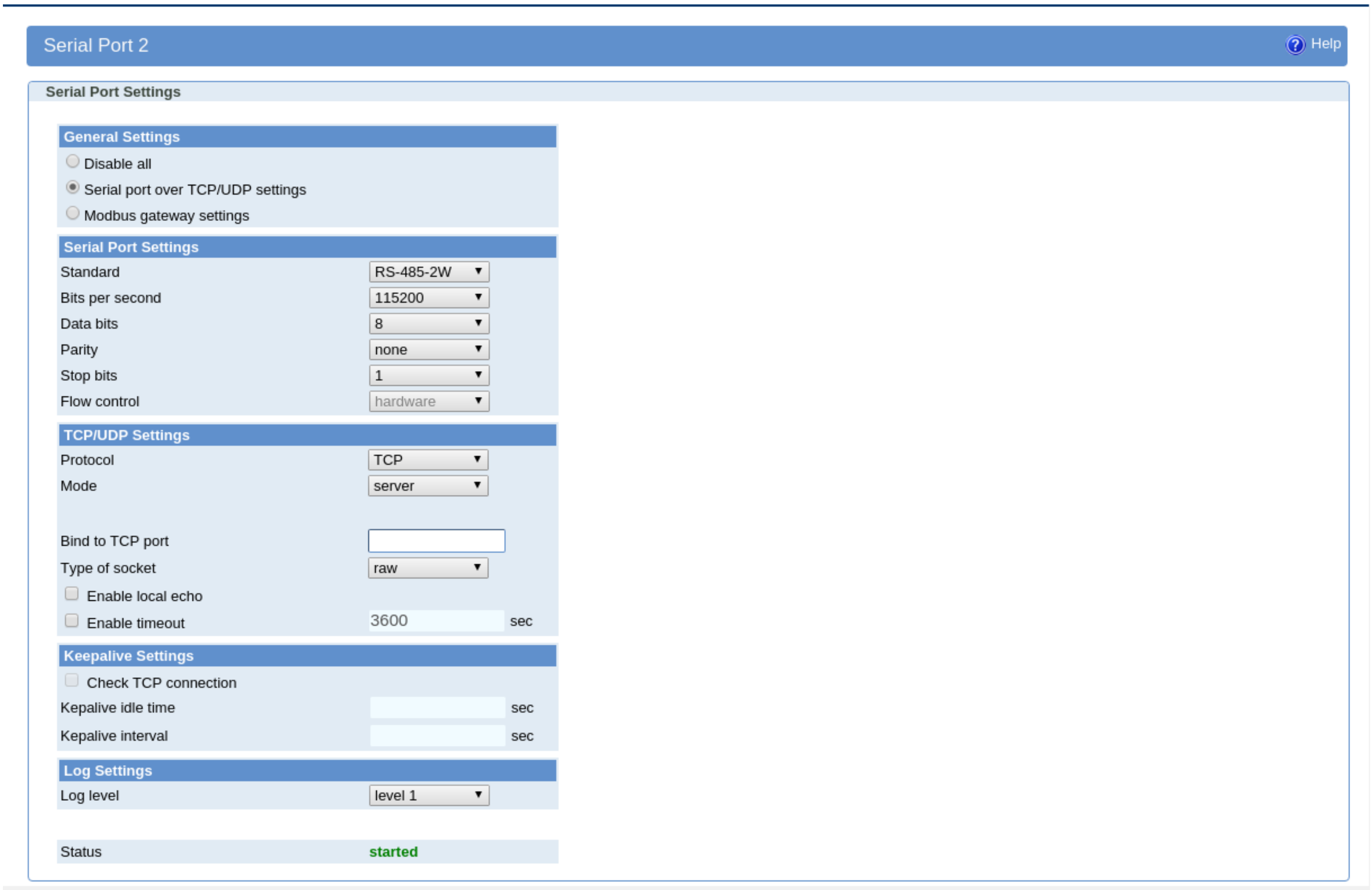
Serial Port over TCP/UDP Settings	
Label	**Description**
Disable all	Disable serial to Ethernet converter and Modbus gateway.
Serial port over TCP/UDP settings	Enable serial to Ethernet converter. This provides a way for a user to connect from a network connection to a serial port.
Modbus gateway settings	Enable translation between Modbus/TCP and Modbus/RTU.
Bits per second	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.

Data bits	Indicates the number of bits in a transmitted data package.
Parity	Checks for the parity bit. None is the default.
Stop bits	The stop bit follows the data and parity bits in serial communication. It indicates the end of transmission. The default is 1.
Flow control	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.
Protocol	Choose which protocol to use [TCP/UDP].
Mode	Select server mode in order to listen for incoming connection, or client mode to establish one.
Type	Select whatever to use server IP address or server hostname.
Server IP address	Enter server's IP address.
Server hostname	Enter server's hostname.
Bind to TCP port	Number of the TCP/IP port on which to accept connections from for this device.
Type of socket	Either *raw or telnet*. Raw enables the port and transfers all data as-is. Telnet enables the port and runs the telnet protocol on the port to set up telnet parameters. This is most useful for using telnet.
Enable local echo	Enables or disables local echo.
Enable inactivity timeout	Close connection after some period of inactivity.
Enable retry timeout	Timeout for retrying connection to unreachable server or port
Check TCP connection	Enable connection checking.
Kepalive idle time	Set keepalive idle time in seconds.
Kepalive interval	Set time period between checking.
TCP accept port	This field determines the TCP port number on which the server will listen for connections. The value entered should be a valid TCP port number. The default Modbus/TCP port number is 502.
Connection timeout	When this field is set to a value greater than 0, the server will close connections that have had no network receive activity for longer than the specified period.
Transmission mode	Select RTU, based on the Modbus slave equipment attached to the port.
Response timeout	This is the timeout (in miliseconds) to wait for a response from a serial slave device before retrying the request or returning an error to the Modbus master.
Pause between request	Set pause between requests in milliseconds. Valid values are between 1 and 10000. Default value is 100.
Maximum number of retries	If no valid response is received from a Modbus slave, the value in this field determines the number of times the serial server will retransmit request before giving up.

Log Level	Set importance level of log messages.
Reload	Click ***Reload*** to discard any changes and reload previous settings.
Save	Click ***Save*** button to save your changes back to the GWR Router. Whether you make changes or not, gateway will reboot every time you click Save.

Table 25 – Serial Port over TCP/UDP parameters

Click *Serial Port* Tab to open the Serial Port Configuration screen. Use this screen to configure the GWG Gateway serial port parameters.



General Settings
○ Disable all
● Serial port over TCP/UDP settings
○ Modbus gateway settings

Serial Port Settings
Standard: RS-485-2W
Bits per second: 115200
Data bits: 8
Parity: none
Stop bits: 1
Flow control: hardware

TCP/UDP Settings
Protocol: TCP
Mode: server
Bind to TCP port:
Type of socket: raw
□ Enable local echo
□ Enable timeout 3600 sec

Keepalive Settings
□ Check TCP connection
Kepalive idle time: sec
Kepalive interval: sec

Log Settings
Log level: level 1

Status: started

Figure 43– Serial Port configuration page

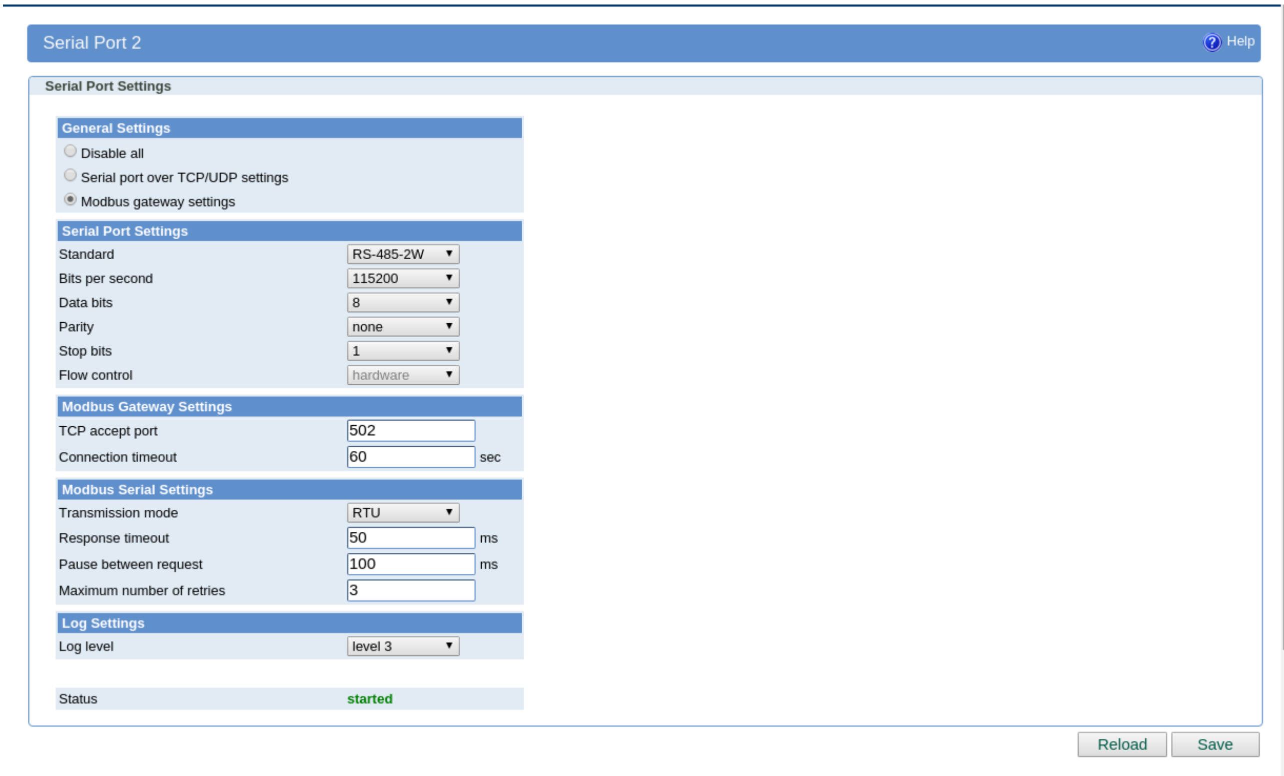
Modbus Gateway settings

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 settings to configure Modbus. At the Figure 44– Modbus gateway configuration page you can see screenshot of Modbus Gateway configuration menu.

Modbus Gateway Settings	
Label	**Description**
TCP accept port	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.
Connection timeout	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.
Transmission mode	Select RTU, based on the Modbus slave equipment attached to the port.
Response timeout	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.
Pause between request	Set pause between requests in milliseconds. Valid values are between 1 and 10000. Default value is 100.
Maximum number of retries	If no valid response is received from a Modbus slave, the value in this field determines the number of times the serial server will retransmit request before giving up.
Log level	Set importance level of log messages.
Reload	Click ***Reload*** to discard any changes and reload previous settings.
Save	Click ***Save*** button to save your changes back to the GWR Router and activate/deactivate serial to Ethernet converter.

Table 26 – Modbus gateway parameters



General Settings

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

Serial Port Settings	
Standard	RS-485-2W
Bits per second	115200
Data bits	8
Parity	none
Stop bits	1
Flow control	hardware

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

Figure 44– Modbus gateway configuration page

GWG RS-422/RS-485 Port Wiring

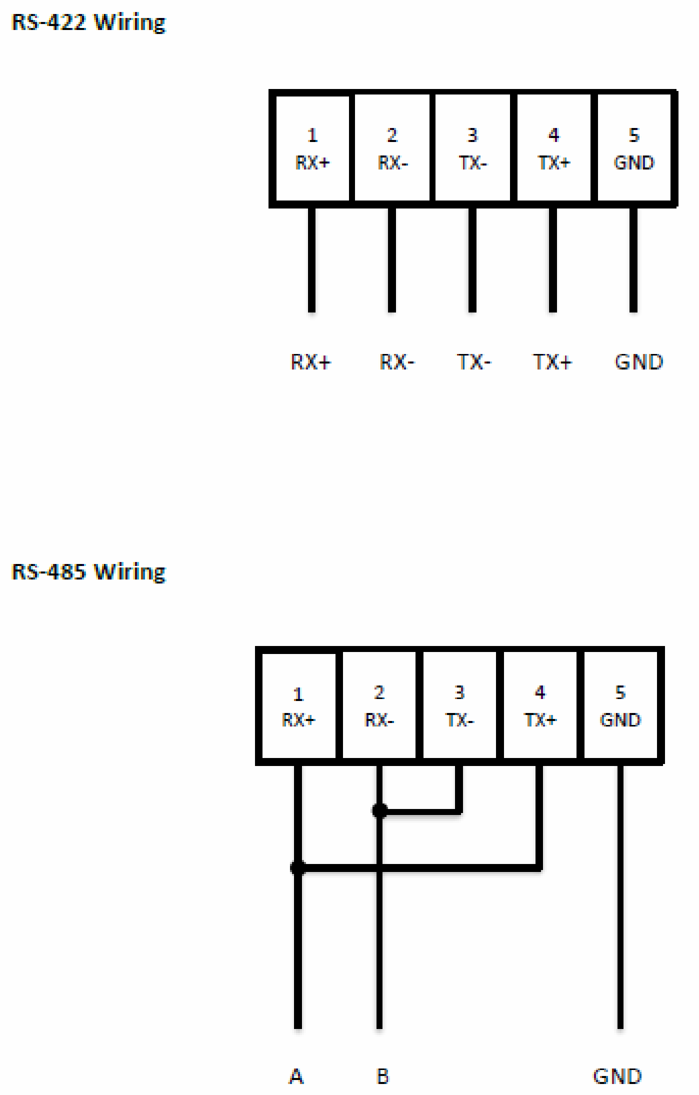


Figure 45- GWR RS-422/RS-485 Port Wiring

SMS – SMS Remote Control

SMS remote control feature allows users to execute a short list of predefined commands by sending SMS messages to the router. GWG-40 v3 with Cinterion PLS8-E rel1.09 can not receive SMS messages.

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.

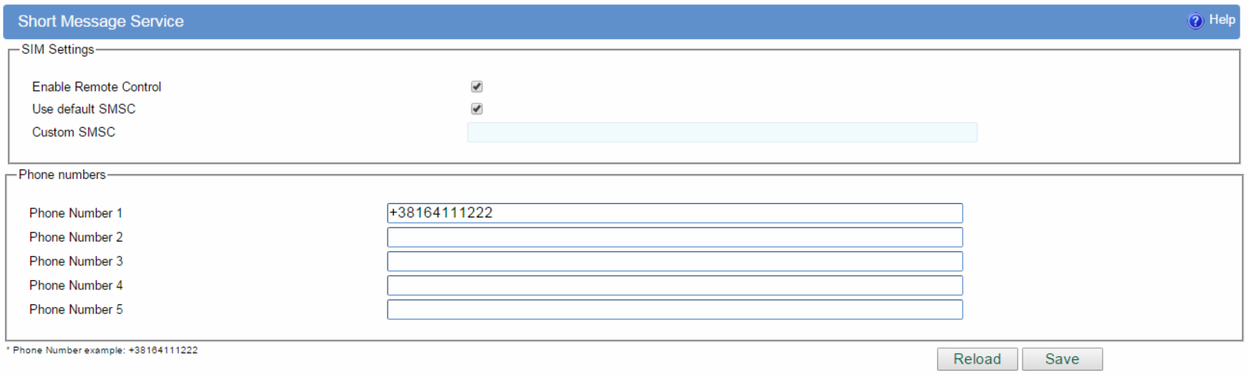
4. In order to obtain the current router status, user should send SMS containing following string:
:PPP–STATUS
After the command is executed, router sends one of the following status reports to the user:
– **CONNECTING**
– **CONNECTED, WAN_IP: {**WAN IP address or the router**}**
– **DISCONNECTING**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

5. In order to establish PPP connection over the other SIM card, user should send SMS containing following string:
:SWITCH-SIM
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.

6. In order to restart whole router user should send SMS containing following string:
:REBOOT
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.

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**). SMS service centre number can be obtained automatically (option "Use default SMSC is enabled") or manually by entering number under field "Custom SMSC".

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



Short Message Service

SIM Settings

Enable Remote Control ☑
Use default SMSC ☑
Custom SMSC

Phone numbers

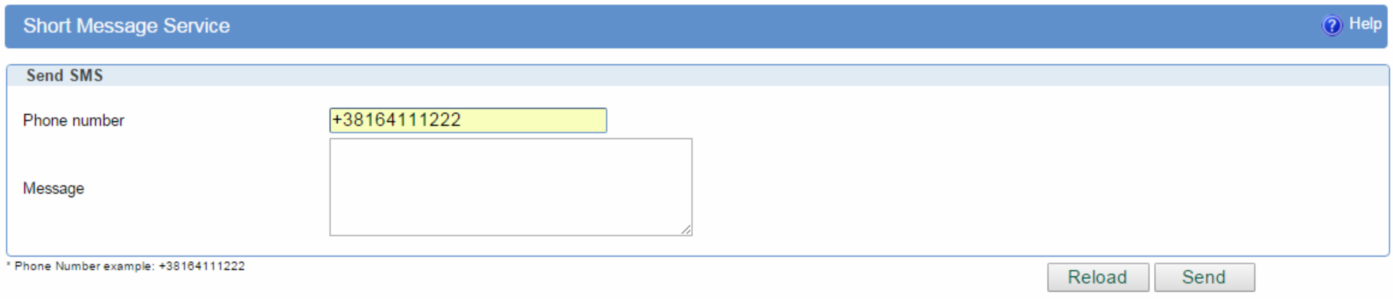
Phone Number 1: +38164111222
Phone Number 2:
Phone Number 3:
Phone Number 4:
Phone Number 5:

* Phone Number example: +38164111222

Figure 46– 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.



Short Message Service

Send SMS

Phone number: +38164111222
Message:

* Phone Number example: +38164111222

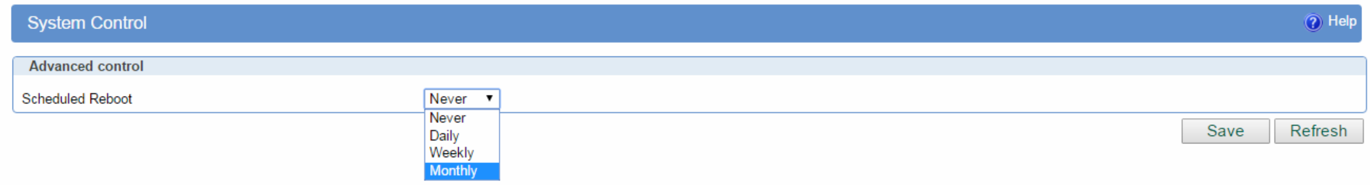
Figure 47– Send SMS

Maintenance

The GWG Gateway 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.



System Control

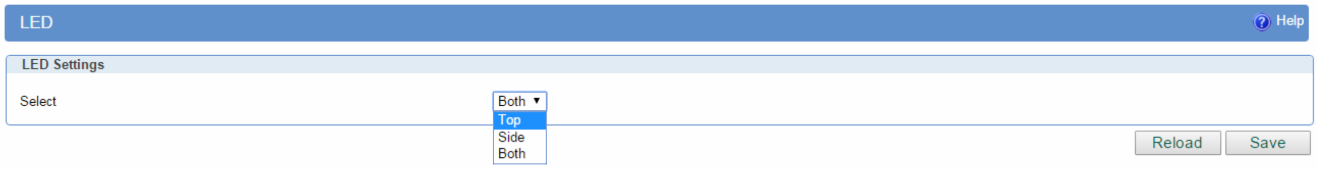
Advanced control

Scheduled Reboot: Never

Figure 48– System Control

Maintenance – LED

Select the side of the router on which will the LEDs be active. LEDs are located on the top and on the side of the router housing.



LED

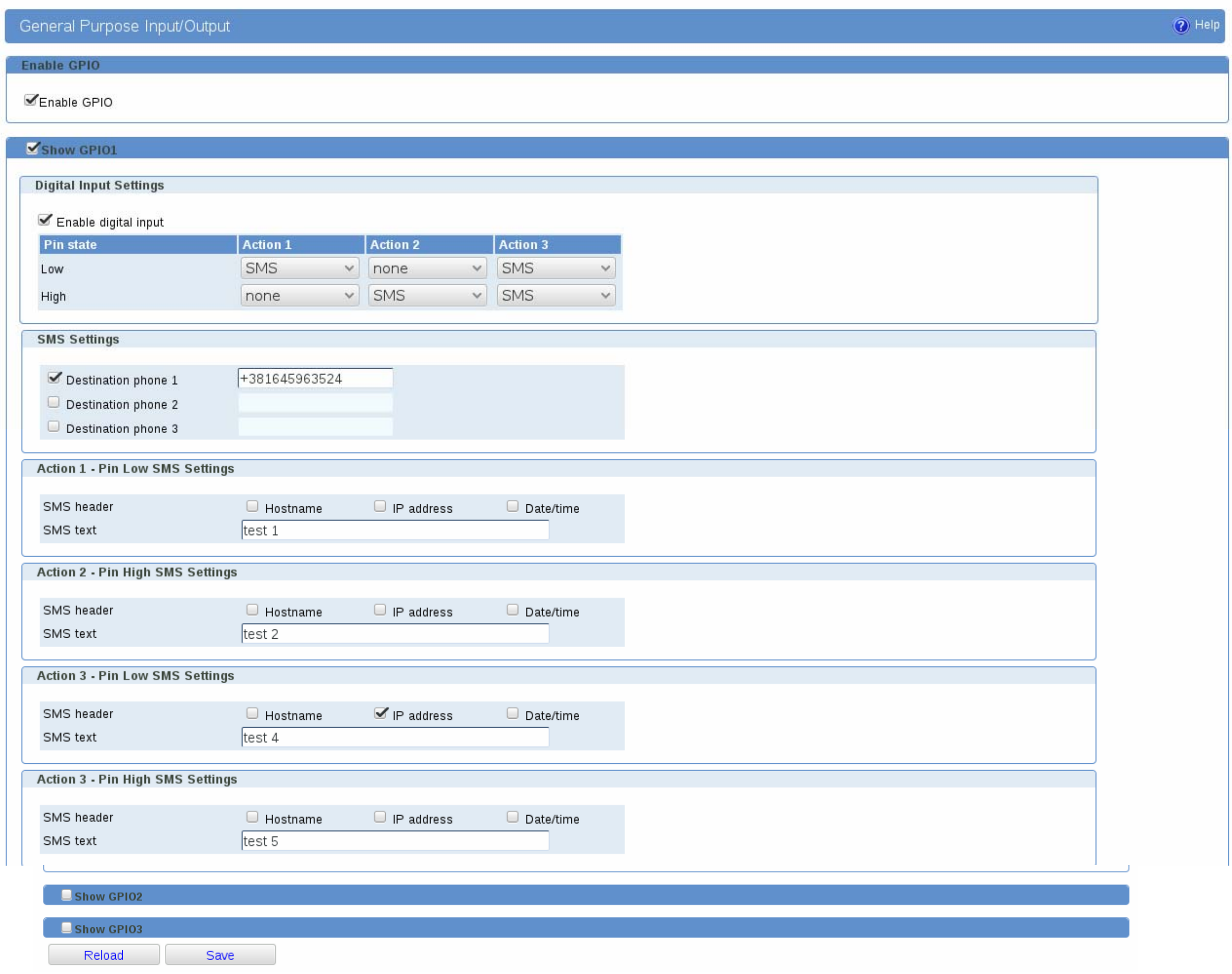
LED Settings

Select: Both ▾ (Top / Side / Both)

Figure 49 – LED

Maintenance – GPIO

GPIO (*General-purpose input/output*) sends SMS when some certain event occur. There is possibility to set GPIO state and 3 separated action for up to three numbers (Destination phone).



General Purpose Input/Output

Enable GPIO

☑ Enable GPIO

☑ Show GPIO1

Digital Input Settings

☑ Enable digital input

Pin state	Action 1	Action 2	Action 3
Low	SMS	none	SMS
High	none	SMS	SMS

SMS Settings

☑ Destination phone 1: +381645963524
□ Destination phone 2
□ Destination phone 3

Action 1 - Pin Low SMS Settings

SMS header: □ Hostname □ IP address □ Date/time
SMS text: test 1

Action 2 - Pin High SMS Settings

SMS header: □ Hostname □ IP address □ Date/time
SMS text: test 2

Action 3 - Pin Low SMS Settings

SMS header: □ Hostname ☑ IP address □ Date/time
SMS text: test 4

Action 3 - Pin High SMS Settings

SMS header: □ Hostname □ IP address □ Date/time
SMS text: test 5

□ Show GPIO2

□ Show GPIO3

Figure 50– GPIO

Enable GPIO	
Label	**Description**
Enable GPIO	Enable or disable GPIO.
Show GPIO1, Show GPIO2, Show GPIO3	Show or hide GPIO settings
Enable digital input	Enable or disable digital input
Pin state	Action executed when GPIO pin change its state to Low or High. Selecting an action will open a new SMS settings section for setting the parameters.
Destination phone	Recipient phone numbers.
SMS header	Text of the message which will be sent.
SMS text	Click Reload to discard any changes and reload previous settings.
Save	Click ***Save*** button to save your changes back to the GWG Gateway.
Reload	Click ***Reload*** to discard any changes and reload previous settings.

Table 27- GPIO Parameters

On router's board are 5 GPIO generic pins which represent:

1. +5VDC with 500mA resettable PTC fuse
2. IO1
3. IO2
4. IO3
5. GND

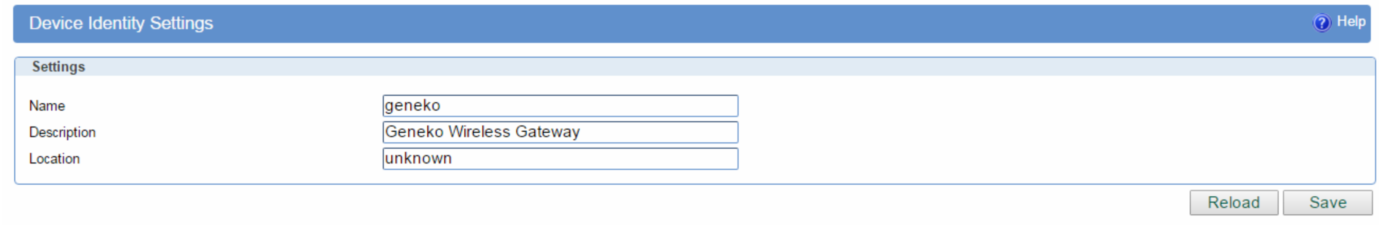
IO1, IO2, IO3 are 3 user selectable input or output.
Input value is readable (high=1, low=0).
Output value is writable (high=1, low=0).

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 48.*

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

Table 28– Device Identity Parameters



Device Identity Settings

Settings

Name: geneko

Description: Geneko Wireless Gateway

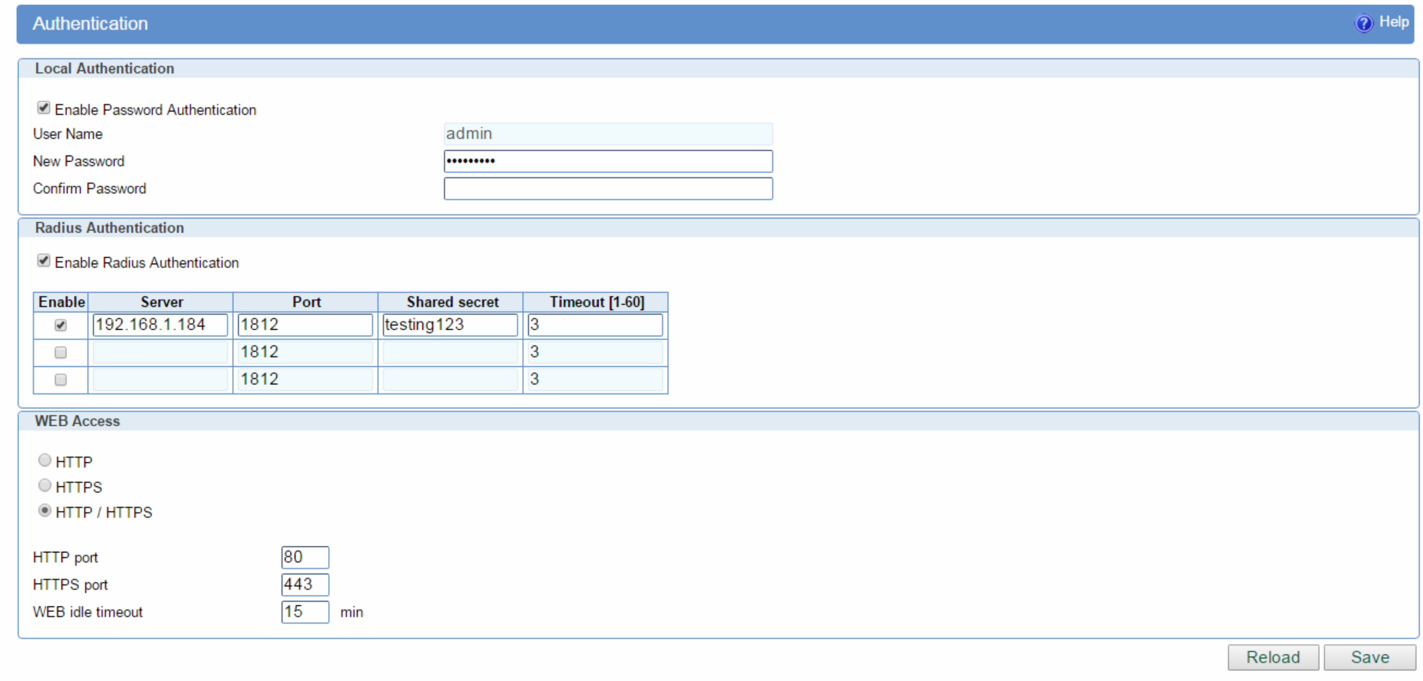
Location: unknown

Figure 51– Device Identity Settings configuration page

Maintenance – Authentication

By ***Administrator Password*** Tab it is possible to activate and deactivate device access system through ***Username*** and ***Password*** mechanism. Within this menu change of authorization data Username/Password is also done. ***Administrator Password*** Tab window is shown on Figure 49.

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



Authentication

Local Authentication

☑ Enable Password Authentication

User Name: admin

New Password: •••••••••

Confirm Password:

Radius Authentication

☑ Enable Radius Authentication

Enable	Server	Port	Shared secret	Timeout [1-60]
☑	192.168.1.184	1812	testing123	3
☐		1812		3
☐		1812		3

WEB Access

○ HTTP
○ HTTPS
● HTTP / HTTPS

HTTP port: 80

HTTPS port: 443

WEB idle timeout: 15 min

Figure 52– Gateway Management configuration page

Administrator Password	
Label	**Description**
Enable Password Authentication	With this checkbox you can activate or deactivate function for local (password) authentication when you access the web/console application.
New Password	Enter a new password for GWG Gateway.
Confirm Password	Re-enter the new password to confirm it.
Enable Radius	With this checkbox you can activate or deactivate function for authentication via

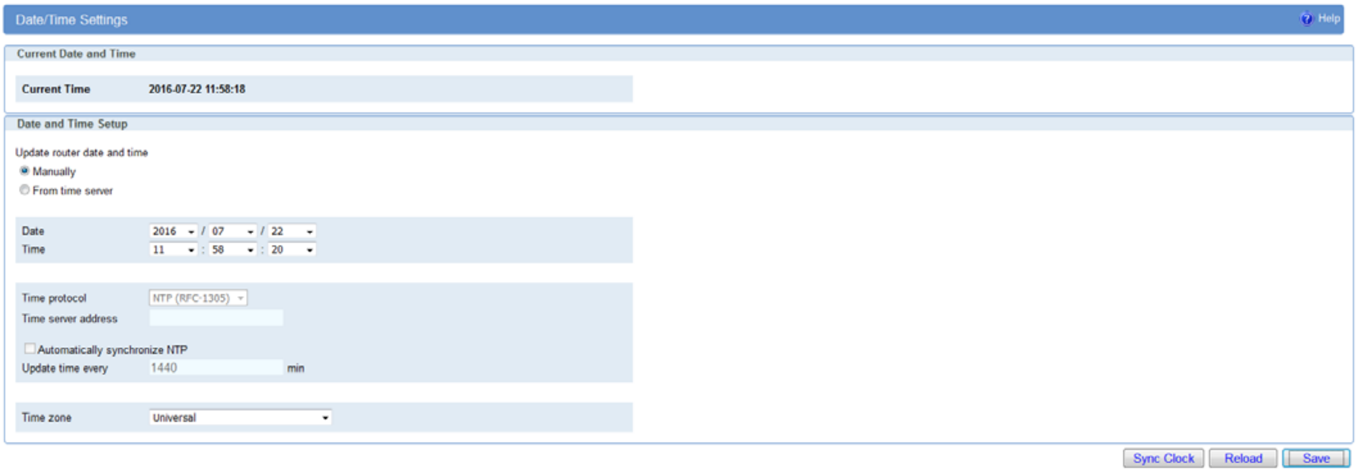
Authentication	remote radius server.
Enable	Enable or disable usage of this radius server.
Server	Enter remote radius server IP address or hostname.
Port	Enter remote radius server port
Shared secret	Enter remote radius server shared secret.
Timeout	Enter remote radius server timeout in seconds [1-60].
Save	Click ***Save*** button to save your changes back to the GWG Gateway. Whether you make changes or not, gateway will reboot every time you click Save.
Reload	Click ***Reload*** to discard any changes and reload previous settings.

Table 29 – Authentication parameters

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

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 settings on the GWG Gateway are done through window Date/Time Settings.



Date/Time Settings

Current Date and Time

Current Time 2016-07-22 11:58:18

Date and Time Setup

Update router date and time

● Manually

○ From time server

Date 2016 / 07 / 22

Time 11 : 58 : 20

Time protocol NTP (RFC-1305)

Time server address

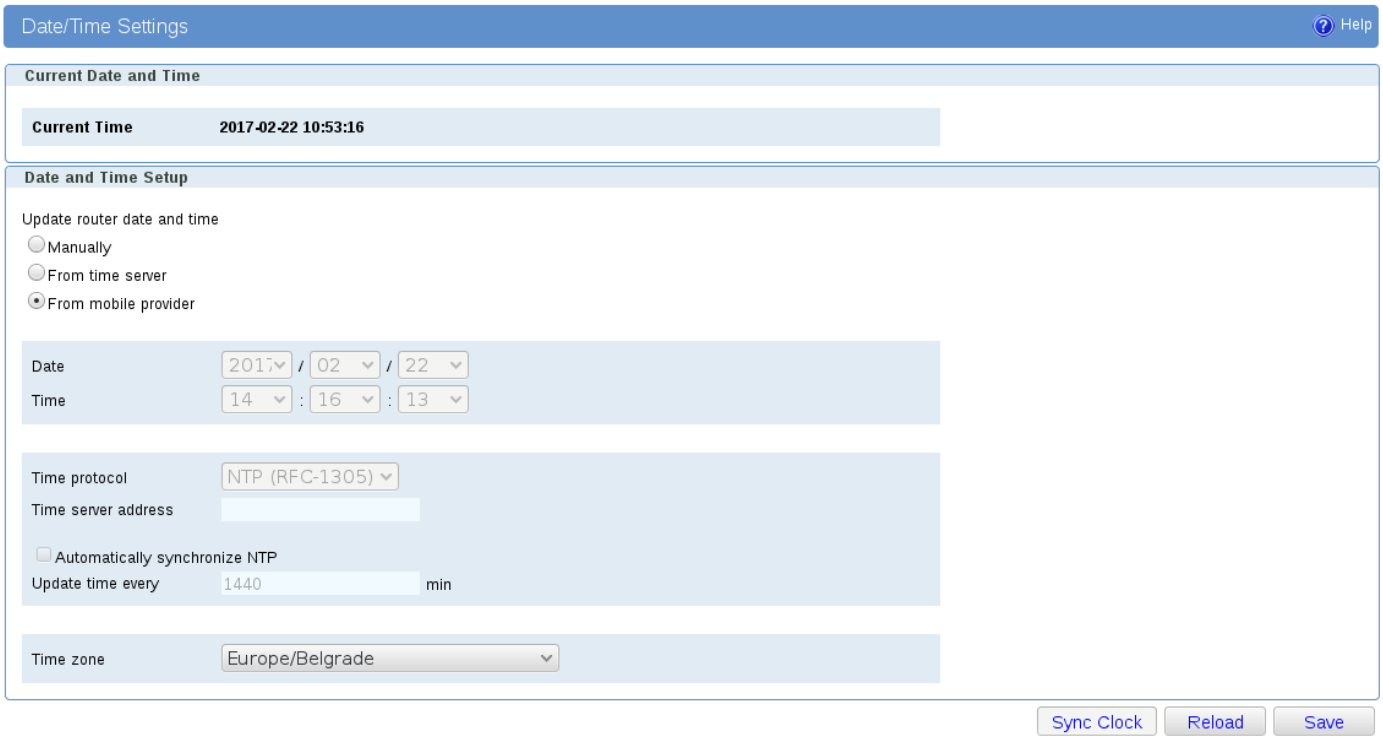
□ Automatically synchronize NTP

Update time every 1440 min

Time zone Universal

Figure 53– Date/Time Settings configuration page

There is possibility to update router date and time from mobile provider.



Current Date and Time

Current Time	2017-02-22 10:53:16

Date and Time Setup

Update router date and time
○ Manually
○ From time server
● From mobile provider

Date	2017 / 02 / 22
Time	14 : 16 : 13
Time protocol	NTP (RFC-1305)
Time server address	
□ Automatically synchronize NTP	
Update time every	1440 min
Time zone	Europe/Belgrade

Figure 54– Date/Time Settings from mobile provider

Date/Time Settings	
Label	**Description**
Manually	Sets date and time manually as you specify it.
From time server	Sets the local time using the Network Time Protocol (NTP) automatically.
From mobile provider	Sets the local time using the NITZ information from provider. Note that this information can be obtained only by re-registering to the network, it can not be used at any moment. After this option is set, time will NOT be updated until mobile connection is restarted, either manually by clicking save button on mobile settings page, or after connection is lost and then reestablished.
Time/Date	This field species Date and Time information. You can change date and time by changing parameters.
Time Protocol	Specify time protocol. Currently only NTP is supported.
Time Server Address	Enter the Hostname or IP address of the NTP server.
Automatically synchronize NTP	Setup automatic synchronization with time server.
Update time every	Time interval for automatic synchronization.
Time Zone	Enables daylight saving time and GMT offset based on TZ database.
Sync Clock	Synchronize Date and time setting with PC calendar.
Save	Click ***Save*** button to save your changes back to the GWG Gateway.
Reload	Click ***Reload*** to discard any changes and reload previous settings.

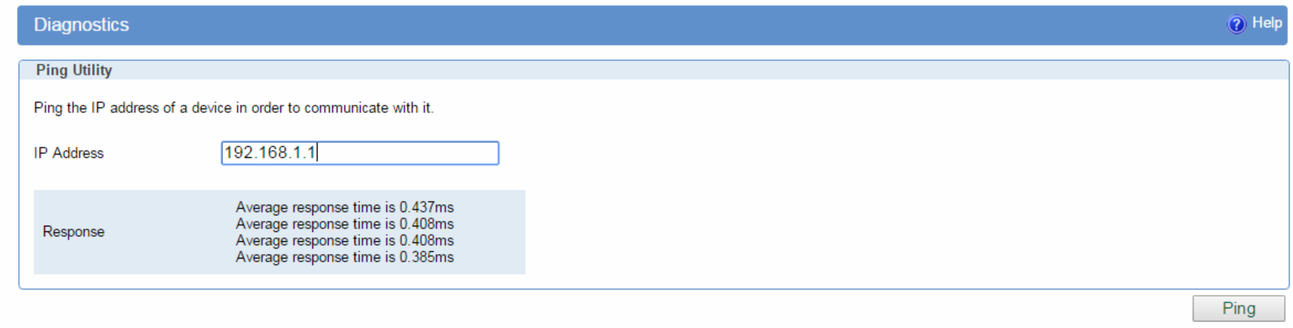
Table 30 – Date/time parameters

Maintenance – Diagnostics

The GWG Gateway provides built–in 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 GWG Gateway 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.



Ping the IP address of a device in order to communicate with it.

IP Address: 192.168.1.1

Response:
Average response time is 0.437ms
Average response time is 0.408ms
Average response time is 0.408ms
Average response time is 0.385ms

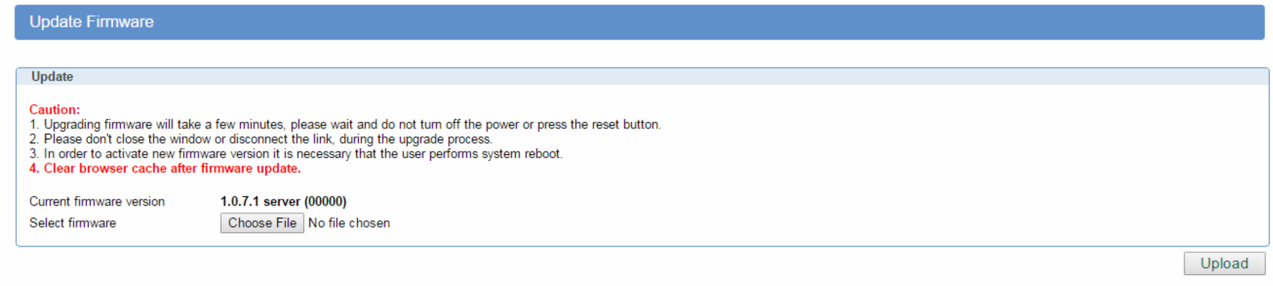
Figure 55– Diagnostic page

Maintenance – Update Firmware

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

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 GWG device takes a few minutes and when it is finished the user is informed about transfer process success.

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



Caution:
1. Upgrading firmware will take a few minutes, please wait and do not turn off the power or press the reset button.
2. Please don't close the window or disconnect the link, during the upgrade process.
3. In order to activate new firmware version it is necessary that the user performs system reboot.
4. Clear browser cache after firmware update.

Current firmware version: 1.0.7.1 server (00000)

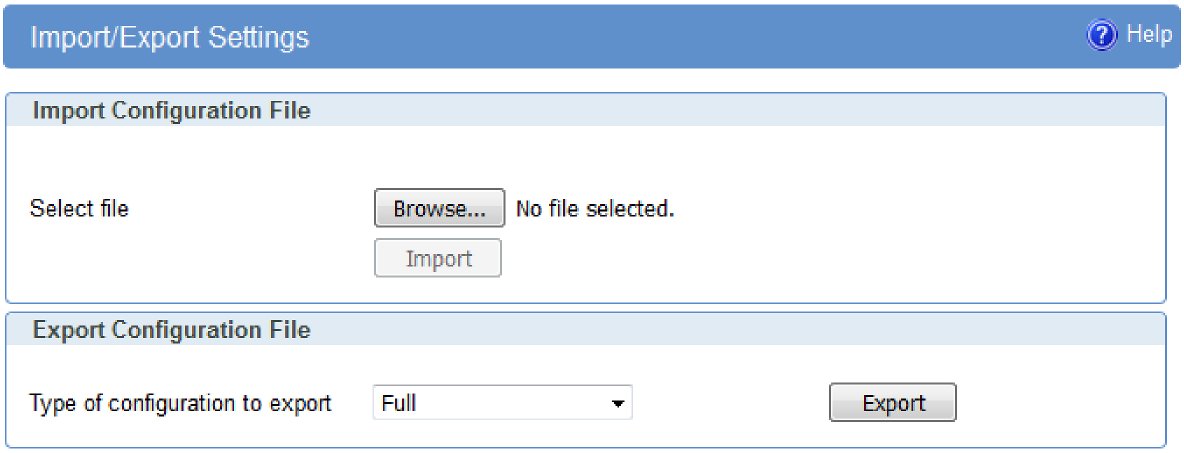
Select firmware: Choose File No file chosen

Figure 56– 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 not changed and after that the system continues to operate with previous values.

Maintenance – Import/Export Settings

To import a configuration file, first specify where your backup configuration file is located. Click Browse, and then select the appropriate configuration file. To export the Router's current configuration file select the part of the configuration you would like to backup and click Export. By default, this file will be called Configuration.tar.gz. This file contains confFile.bkg , cacert and crlcert , Iccert files.



Import/Export Settings

Import Configuration File

Select file: No file selected.

Export Configuration File

Type of configuration to export: Full

Figure 57– Export/Import the configuration on the gateway

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

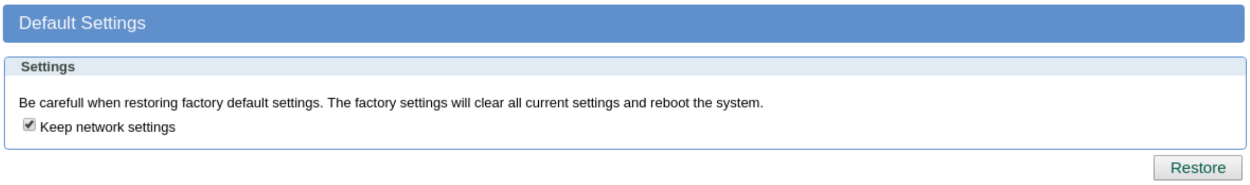
To export the Router's current configuration file select the part of the configuration you would like to backup and click Export.

By default, this file will be called Configuration.tar.gz. This file contains confFile.bkg , cacert and crlcert , Iccert files.

Maintenance – Default Settings

Use this feature to clear all of your configuration information and restore the GWG Gateway 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 GWG Gateway with default parameters. ***Keep network settings*** checkbox allows user to keep all network settings after factory default reset. System will be reset after pressing ***Restore*** button.



Default Settings

Settings

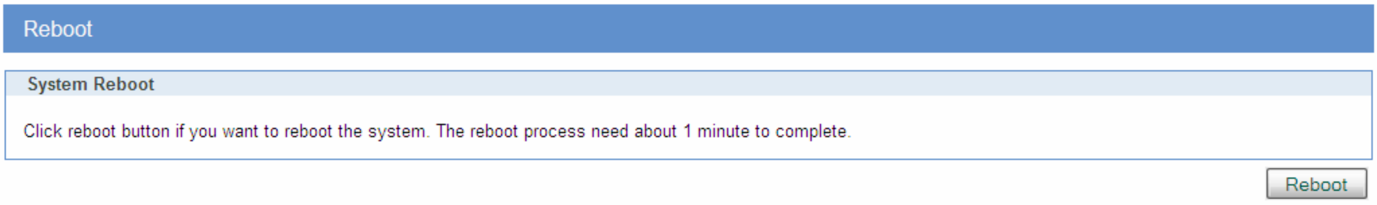
Be carefull when restoring factory default settings. The factory settings will clear all current settings and reboot the system.

☑ Keep network settings

Figure 58– Default Settings page

Maintenance – System Reboot

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



Reboot

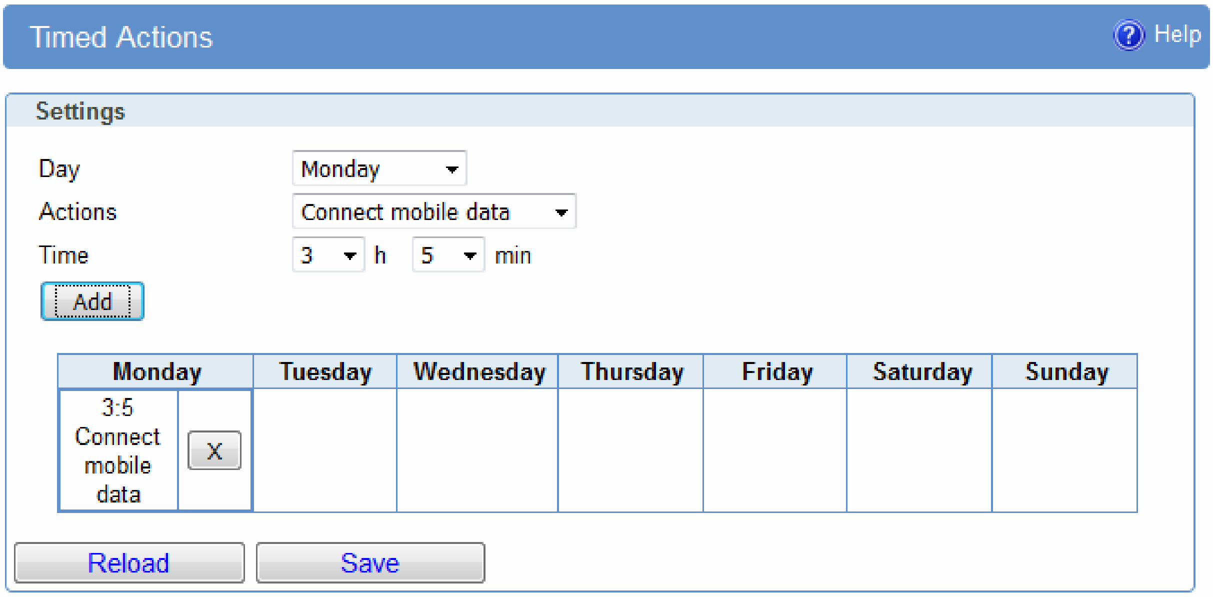
System Reboot

Click reboot button if you want to reboot the system. The reboot process need about 1 minute to complete.

Figure 59– System Reboot page

Management – Timed Actions

Create a schedule of actions to be performed in a certain time of the day. There is a possibility to add more actions for each day of the week.



Timed Actions

Settings

Day: Monday

Actions: Connect mobile data

Time: 3 h 5 min

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
3:5 Connect mobile data X						

Figure 60– Timed Actions

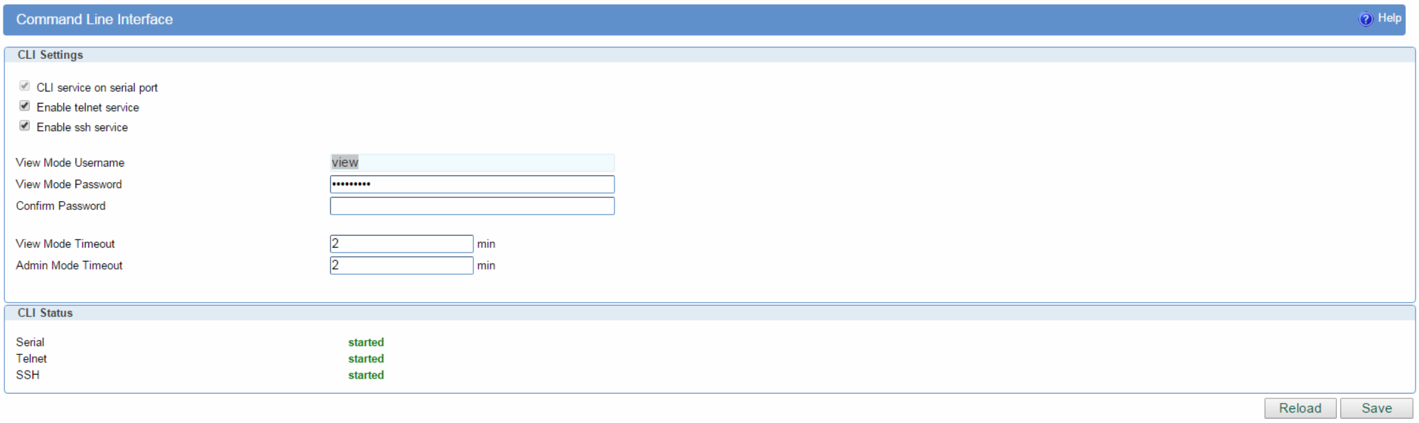
Management – Command Line Interface

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 61 – Command Line Interface*.

Command Line Interface	
Label	**Description**
	CLI Settings
Enable telnet service	Enable or disable CLI via telnet service.
Enable ssh service	Enable or disable CLI via ssh service.
View Mode Username	Username for View mode.
View Mode Password	Password for View mode
Confirm Password	Confirm password for View mode
View Mode Timeout	Inactivity timeout for CLI View mode in minutes. After timeout, session will auto logout.
Admin Mode Timeout	Inactivity timeout for CLI Edit mode in seconds. Note that Username and Password for Edit mode are the same as Web interface login parameters. After timeout, session will auto logout.
Save	Click ***Save*** to save your changes back to the GWG Gateway.
Reload	Click ***Reload*** to discard any changes and reload previous settings.

Table 31 – Command Line Interface parameters



CLI Settings

☑ CLI service on serial port
☑ Enable telnet service
☑ Enable ssh service

View Mode Username: view
View Mode Password: •••••••••
Confirm Password:

View Mode Timeout: 2 min
Admin Mode Timeout: 2 min

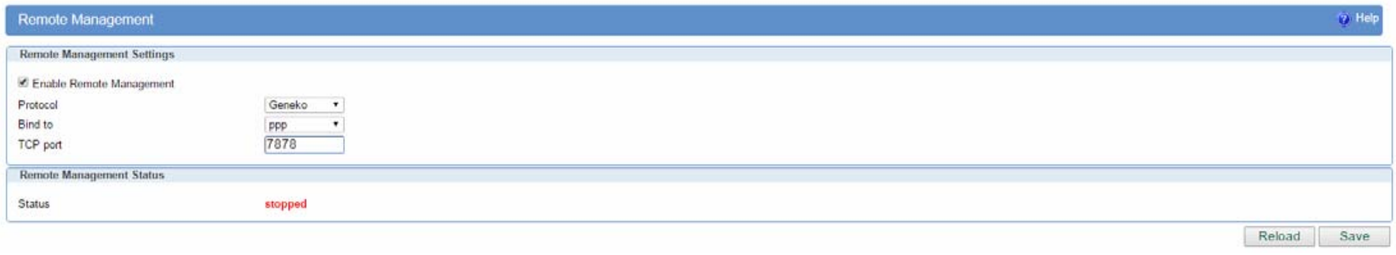
CLI Status

Serial: started
Telnet: started
SSH: started

Figure 61 – Command Line Interface

Management – Remote Management

Remote Management Utility is a standalone Windows application with many useful options for configuration and monitoring of GWG Gateways. In order to use this utility user has to enable Remote Management on the router, Figure 62.


Remote Management

Remote Management Settings
☑ Enable Remote Management
Protocol Geneko
Bind to ppp
TCP port 7878
Remote Management Status
Status stopped

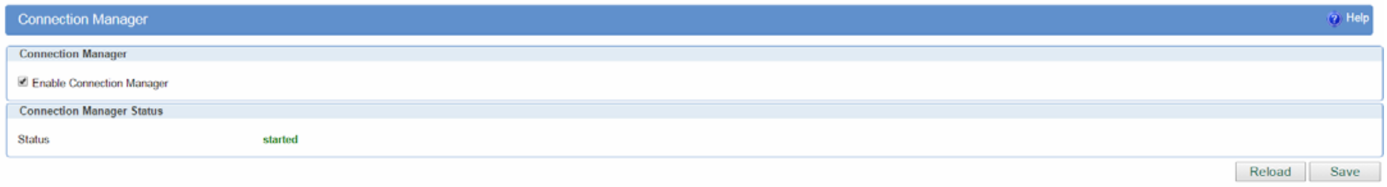
Figure 62– Remote Management

Remote Management	
Label	**Description**
Enable Remote Management	Enable or disable Remote Management.
Protocol	Choose between Geneko and Sarian protocol.
Bind to	Specify the interface.
TCP port	Specify the TCP port.
Save	Click ***Save*** button to save your changes back to the Geneko Router. Whether you make changes or not, gateway will reboot every time you click Save.
Reload	Click ***Reload*** to discard any changes and reload previous settings.

Table 32 – Remote Management parameters

Management – Connection Manager

Enabling Connection Manager will allow Connection Wizard (located on setup CD that goes with the gateway) 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 gateway to the local network without previous setup of the gateway. Connection Wizard will detect the device and allow you to configure some basic functions of the gateway. Connection Manager is enabled by default on the gateway and if you do not want to use it you can simply disable it .


Connection Manager

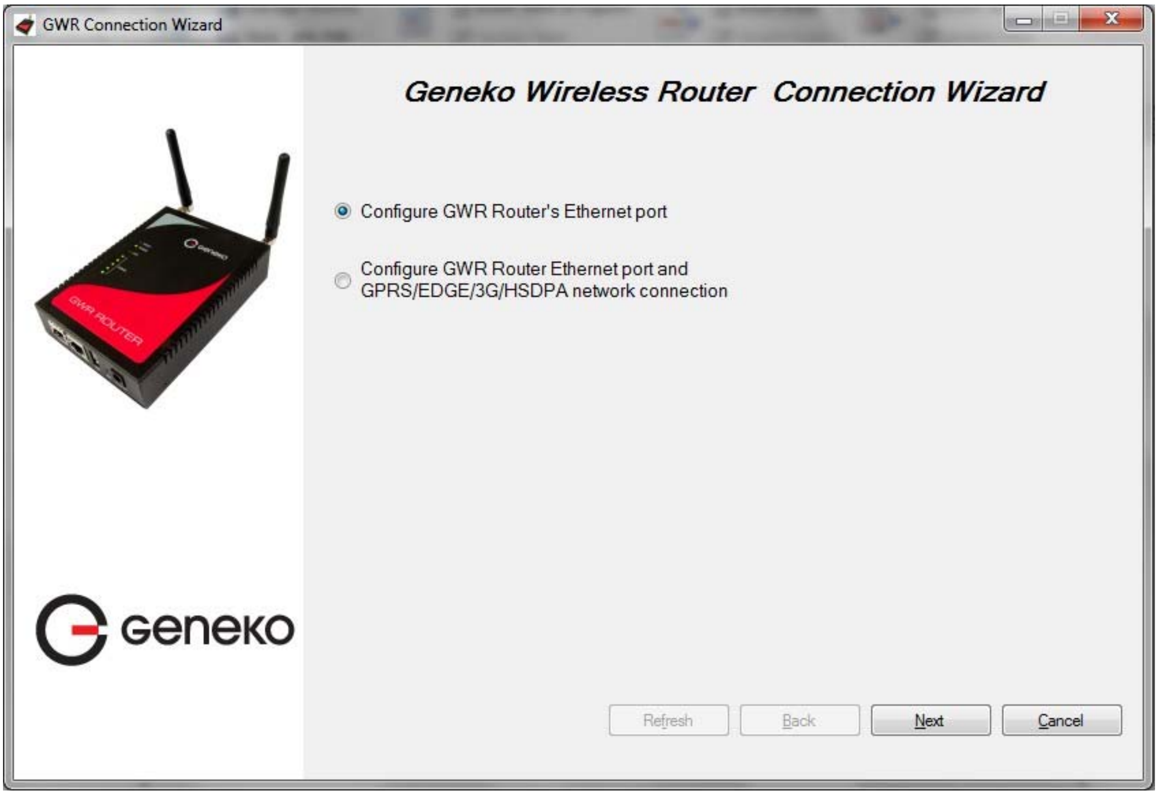
Connection Manager
☑ Enable Connection Manager
Connection Manager Status
Status started

Figure 63– 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. It is only for Windows OS. 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



GWR Connection Wizard

Geneko Wireless Router Connection Wizard

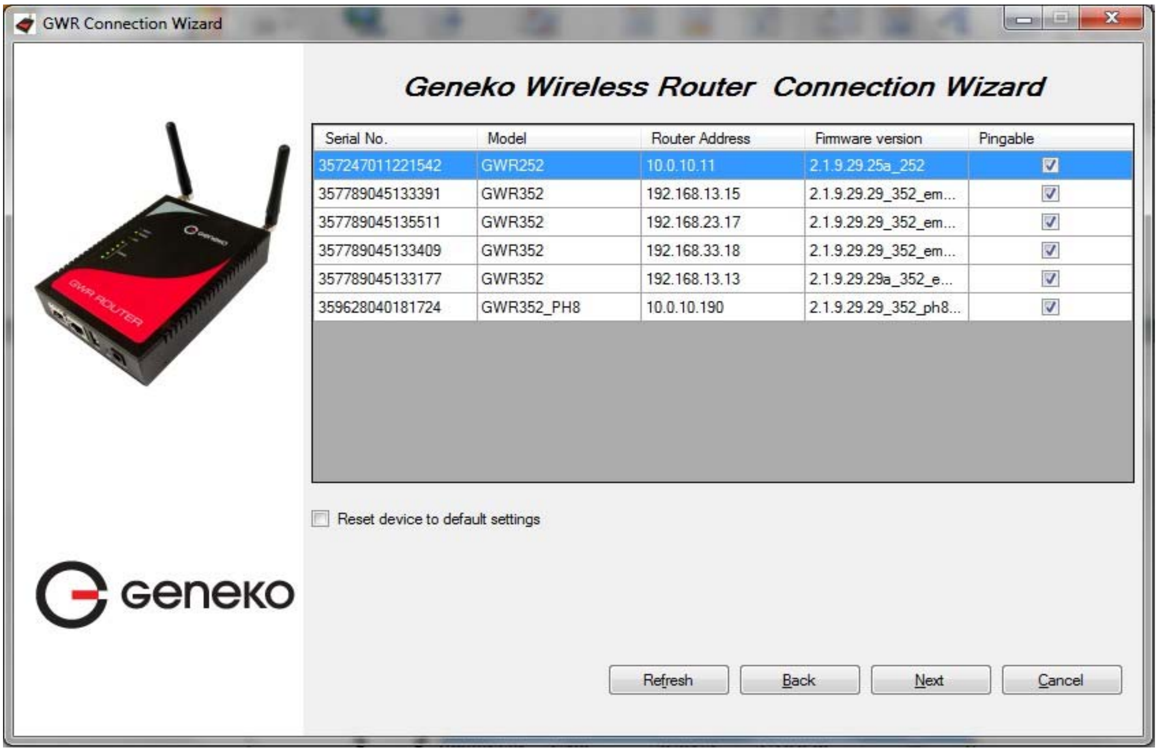
● Configure GWR Router's Ethernet port

○ Configure GWR Router Ethernet port and GPRS/EDGE/3G/HSDPA network connection

Figure 64– 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 and gateways present in the network, with following information:

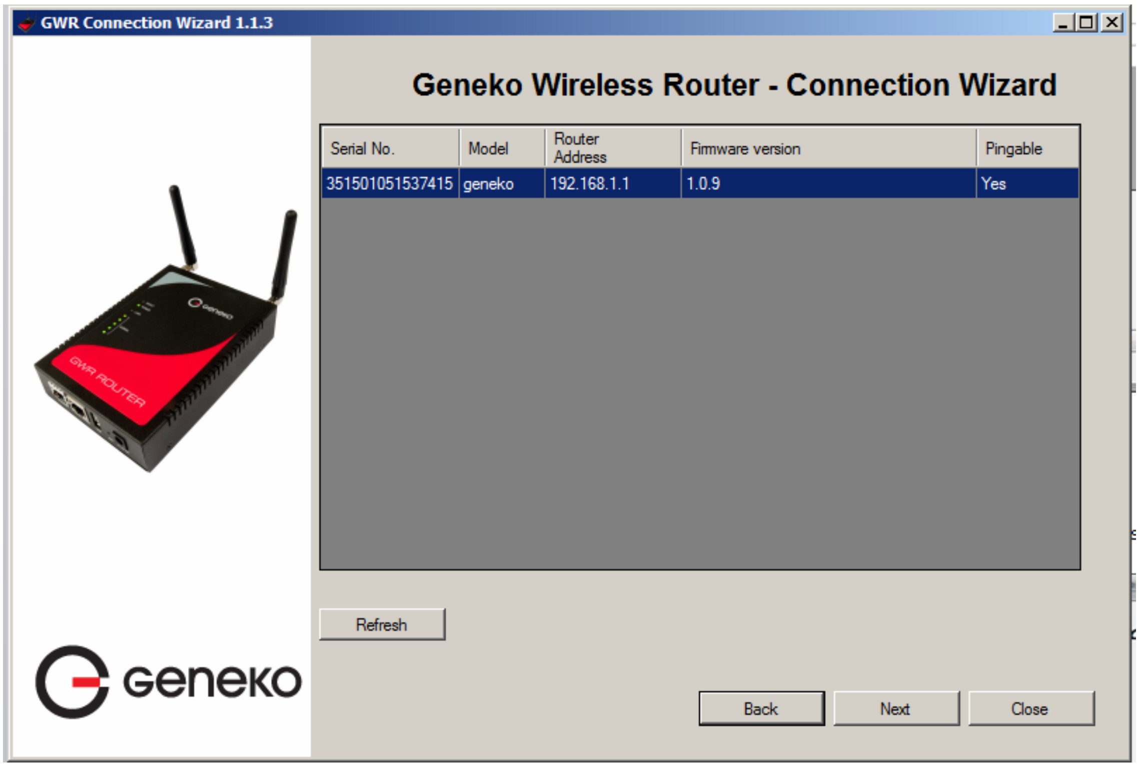
- Serial number
- Model
- Ethernet IP
- Firmware version
- Pingable (if Ethernet IP address of the router is in the same IP subnet as PC interface then this field will be marked, i.e. you can access router over web interface).



Serial No.	Model	Router Address	Firmware version	Pingable
357247011221542	GWR252	10.0.10.11	2.1.9.29.25a_252	☑
357789045133391	GWR352	192.168.13.15	2.1.9.29.29_352_em...	☑
357789045135511	GWR352	192.168.23.17	2.1.9.29.29_352_em...	☑
357789045133409	GWR352	192.168.33.18	2.1.9.29.29_352_em...	☑
357789045133177	GWR352	192.168.13.13	2.1.9.29.29a_352_e...	☑
359628040181724	GWR352_PH8	10.0.10.190	2.1.9.29.29_352_ph8...	☑

☐ Reset device to default settings

Figure 65– Connection Wizard – Router Detection #1

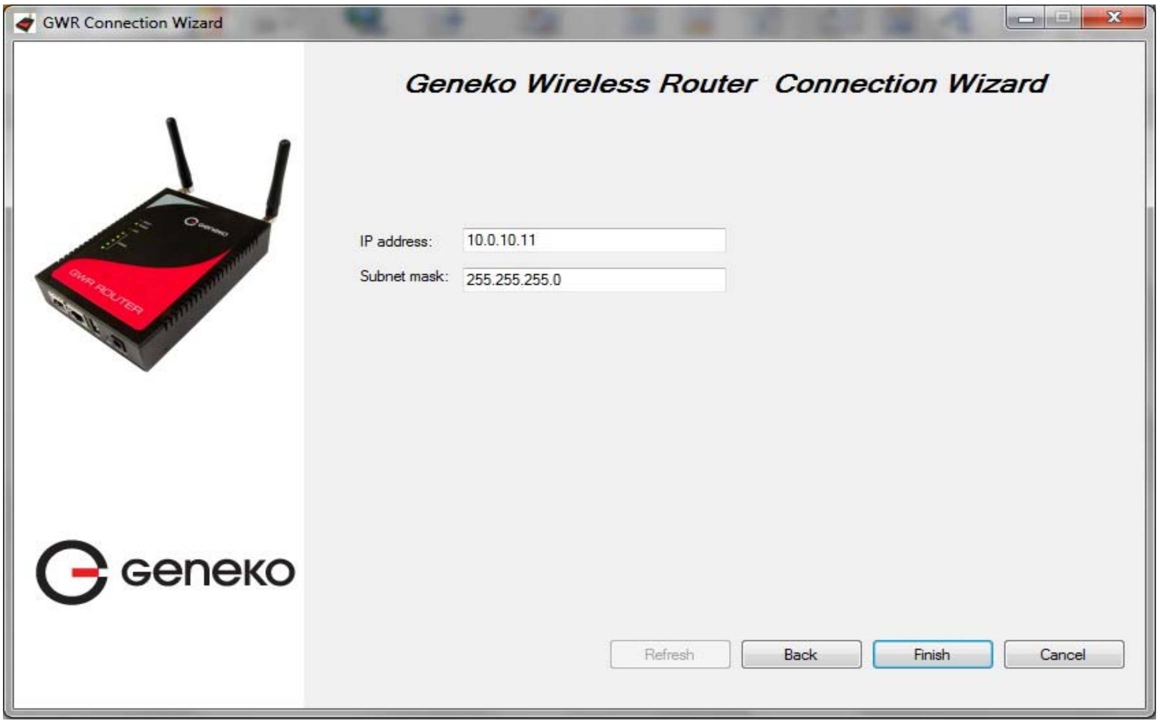


GWR Connection Wizard 1.1.3
Geneko Wireless Router - Connection Wizard
geneko

Serial No.	Model	Router Address	Firmware version	Pingable
351501051537415	geneko	192.168.1.1	1.0.9	Yes

Figure 66– Connection Wizard – Router Detection #2

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



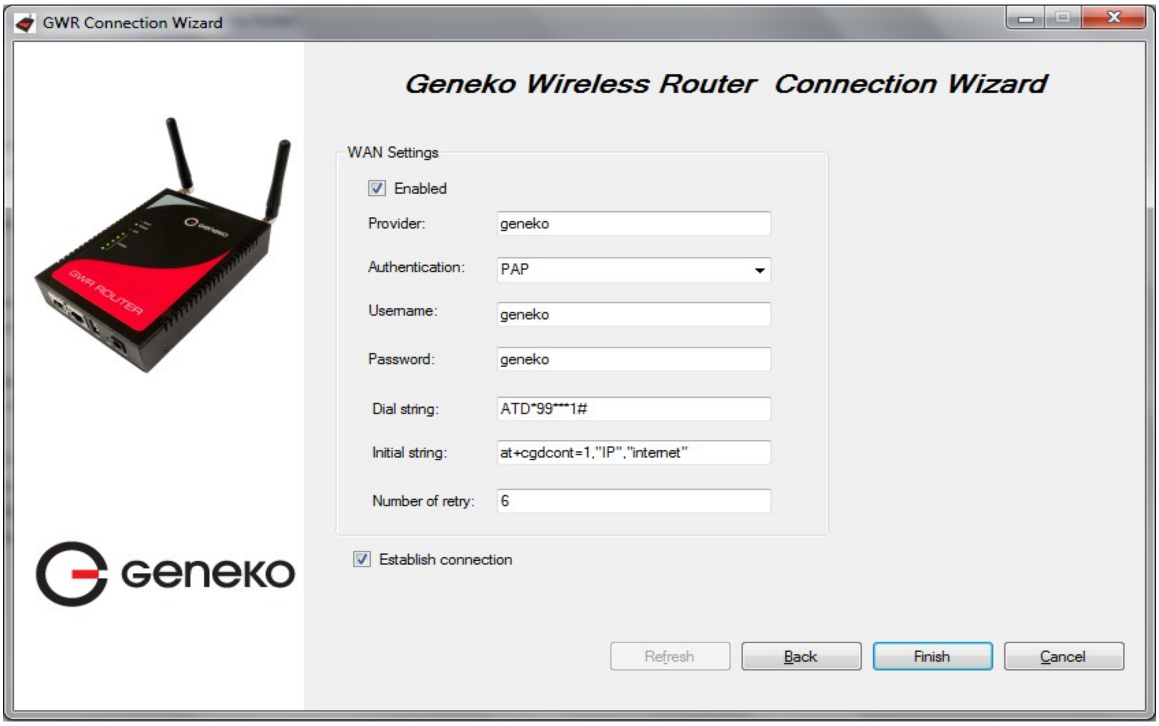
Geneko Wireless Router Connection Wizard

IP address: 10.0.10.11

Subnet mask: 255.255.255.0

Figure 67– 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.



Geneko Wireless Router Connection Wizard

WAN Settings

☑ Enabled

Provider: geneko

Authentication: PAP

Username: geneko

Password: geneko

Dial string: ATD*99***1#

Initial string: at+cgdcont=1,"IP","internet"

Number of retry: 6

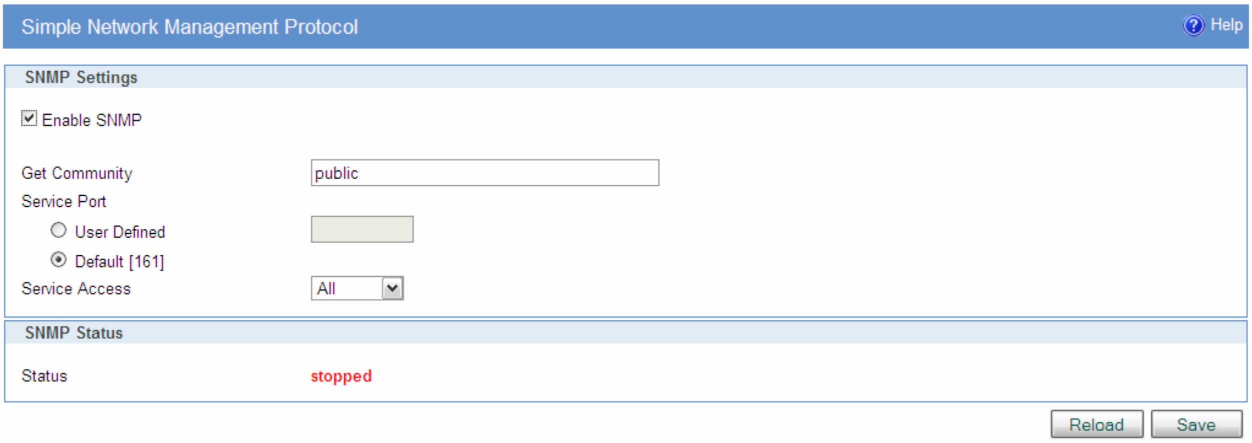
☑ Establish connection

Figure 68– 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 Gateway and receive notification of any critical events as they occur on the network. The Gateway 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 and supports a custom MIB for generating trap messages.



Simple Network Management Protocol

SNMP Settings

☑ Enable SNMP

Get Community: public

Service Port

○ User Defined

● Default [161]

Service Access: All

SNMP Status

Status: stopped

Figure 69 – SNMP configuration page

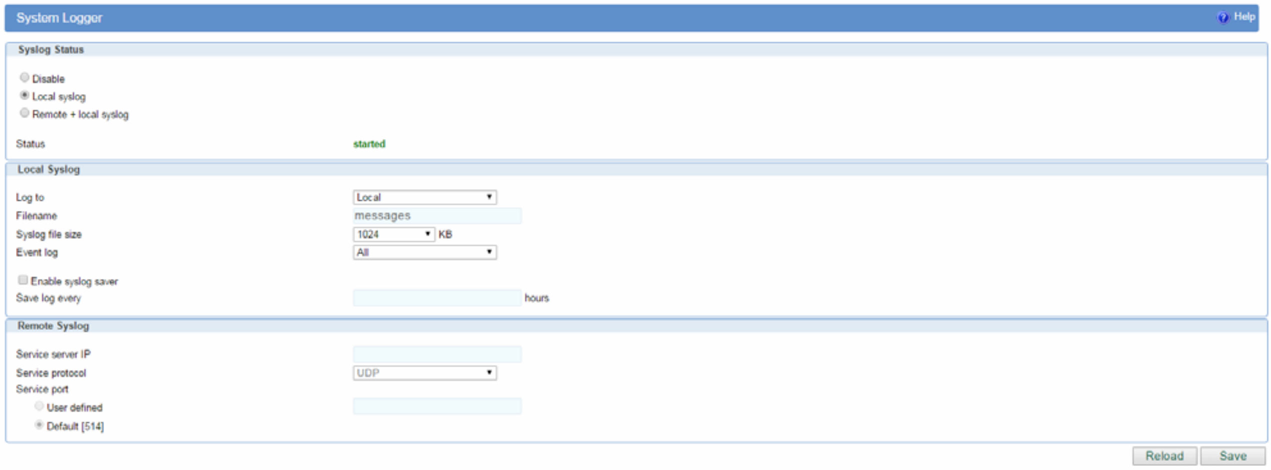
SNMP Settings	
Label	**Description**
Enable SNMP	Enable or disable SNMP.
Get Community	Create the name for a group or community of administrators who can view SNMP data. The default is ***public***. It supports up to 64 alphanumeric characters.
Set Community	Create the name for a group or community of administrators who can view SNMP data and send SET commands via SNPM. The default is private. It supports up to 64 alphanumeric characters.
Service Port	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.
Service Access	Sets the interface enabled for SNMP traps. The default is Both.
Reload	Click ***Reload*** to discard any changes and reload previous settings.
Save	Click ***Save*** button to save your changes back to the GWG Gateway and enable/disable SNMP.

Table 33 – 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.



System Logger

Syslog Status

○ Disable
● Local syslog
○ Remote + local syslog

Status: started

Local Syslog

Log to: Local
Filename: messages
Syslog file size: 1024 KB
Event log: All

□ Enable syslog saver
Save log every: hours

Remote Syslog

Service server IP:
Service protocol: UDP
Service port
○ User defined
● Default [514]

Figure 70 – Syslog configuration page

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

Syslog Settings	
Label	**Description**
Disable	Mark this option in order to disable Syslog feature.
Local syslog	Mark this option in order to enable Local syslog feature. Logs will remain on the router.
Remote + local syslog	Mark this option in order to enable remote and local syslog feature.
Log to	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
Syslog file size	Set log size on one of the six predefined values. [10 / 20 / 50 / 128 / 256 / 512 / 1024]KB
Event log	Choose which events to be stored. You can store System, IPsec events or both of them.
Enable syslog saver	Save logs periodically on filesystem.
Save log every	Set time duration between two saves.

Service server IP	The Geneko Router can send a detailed log to an external syslog server. The Gateway’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.
Service protocol	Sets the protocol type.
Service port	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.
Reload	Click Reload to discard any changes and reload previous settings.
Save	Click *Save* button to save your changes back to the GWG Gateway and enable/disable Syslog.

Table 34 – 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 Username and Password to log in and then manage the Gateway.)

CHROOT

A chroot environment is an operating system call that will change the root location temporarily to a new folder. Chroot runs a command or an interactive shell from another directory, and treats that directory as root. Only a privileged process and root user can use chroot command.

Use Putty, Secure CRT and etc. on Windows, or Putty, GTK on Linux for connection over serial RS-232 port or SSH over LAN port.

For example: Use SSH to enter in global configuration mode.
SSH 192.168.1.1 // SSH to br0 at TCP port 22 //

Login as: **admin**
admin@192.168.1.1's password: **admin**
admin@geneko> gwr_chroot

Press TAB twice quickly to see all commands which are available.

The list of possibilities is:

```
!            dirs         interfaces-up   ping6      tee
./           disown       ip              popd       telnet
:            dmesg        ipcalc          pppstats   test
JSON.sh      do           ipsec           printf     tftp
[            done         ipsec-mode      ps         tftpd
[[           du           ipsec-routes    pushd      then
```

]]
alias
ar
arping
awk
basename
bash
bg
bind
break
builtin
bunzip2
busybox
bzcat
cal
caller
case
cat
cd
chattr
chmod
clear
cmp
command
compgen
complete
compopt
configuration_export
configuration_import
configuration_show
continue
coproc
cp
cpu
cut
date
dc
dd
declare
df
diff
dirname
ebtables
echo
egrep
elif
else
enable
env
esac
eval
exec
exit
export
expr
factory_default
false
fc
fg
fgrep
fi
find
flock
for
free
ftpd
function
fuser
getopts
grep
gunzip
gzip
hash
head
help
hexdump
history
hostname
hwclock
id
if
ifconfig
in
interfaces-all
ipsec-sa-status
ipsec-status
iptables-view
jobs
json2lua
kill
killall
ldd
less
let
ln
local
local_dns
logger
logname
logout
ls
lsof
lua
luac
mapfile
md5sum
microcosm
mkdir
mkfifo
mobile-activity
modem_info
modem_state
more
mv
nc
ncftp
netstat
nohup
nslookup
ntpdate
od
openvt
passwd
perl
pidof
ping
pwd
read
readarray
readlink
readonly
realpath
reboot
return
rip-ripd-conf
rip-zebra-conf
rm
route
run-parts
scp
sed
select
send_at_command
seq
service
set
sh
shift
shopt
show
sleep
sms_send
snmp-view
sort
source
ssh
strace
strings
stty
su
suspend
syslog_export
syslog_start
syslog_start+view
syslog_stop
tail
tar
tcpsvd
time
times
top
touch
tr
traceroute
trap
true
tty
type
typeset
udpsvd
ulimit
umask
unalias
uname
uniq
unset
until
unzip
upfirmware
uptime
users
usleep
vi
wait
wc
wget
which
while
who
whoami
xargs
xtables-multi
yes
zcat
{
}

Configuration Examples

GWG Gateway as Internet Gateway

The GWG Gateways 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 GWG Gateway. The GWG Gateway uses Network Address Translation (NAT) where only the mobile IP address is visible to the outside world. All outgoing traffic uses the GWG Gateway mobile IP address.

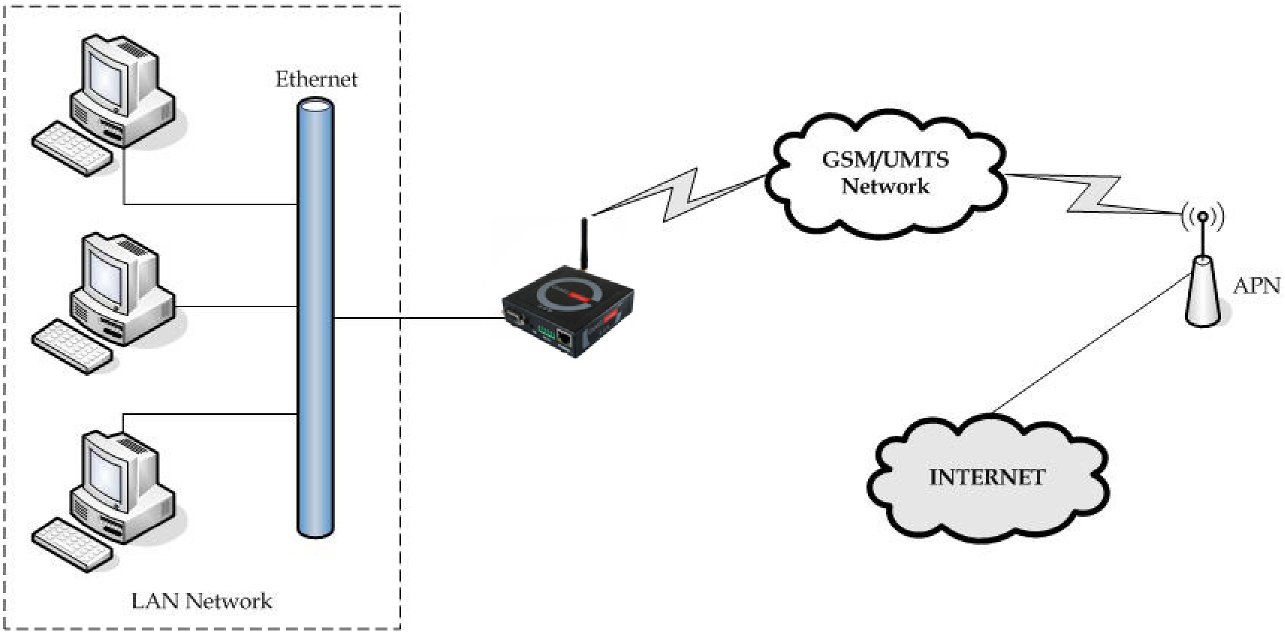


Figure 71 – GWG Gateway as Internet gateway

- Click LAN Ports Tab, to open the LAN Port Settings 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.

- Click ***LAN Ports*** Tab, to open the **LAN Port Settings** 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 ***Mobile Settings*** Tab to configure parameters necessary for GSM/UMTS/LTE connection. All parameters necessary for connection configuration should be provided by your mobile operator.
- Check the status of GSM/UMTS/LTE connection (***Mobile 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 to block any unwanted incoming traffic.
- Configure the GWG Gateway 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 GWG Gateways

GRE tunnel is a type of a VPN tunnel, but it is not a secure tunneling method. Simple network with two GWG Gateways is illustrated on the diagram below (*Figure* 7272). Idea is to create GRE tunnel for LAN to LAN (site to site) connectivity.

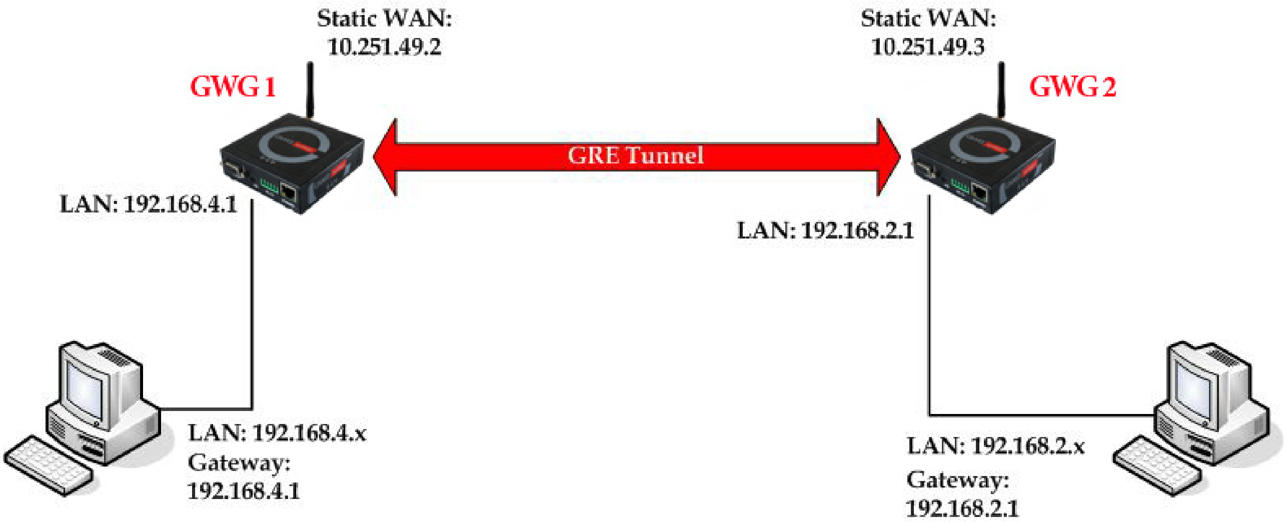


Figure 72 – GRE tunnel between two GWG Gateways

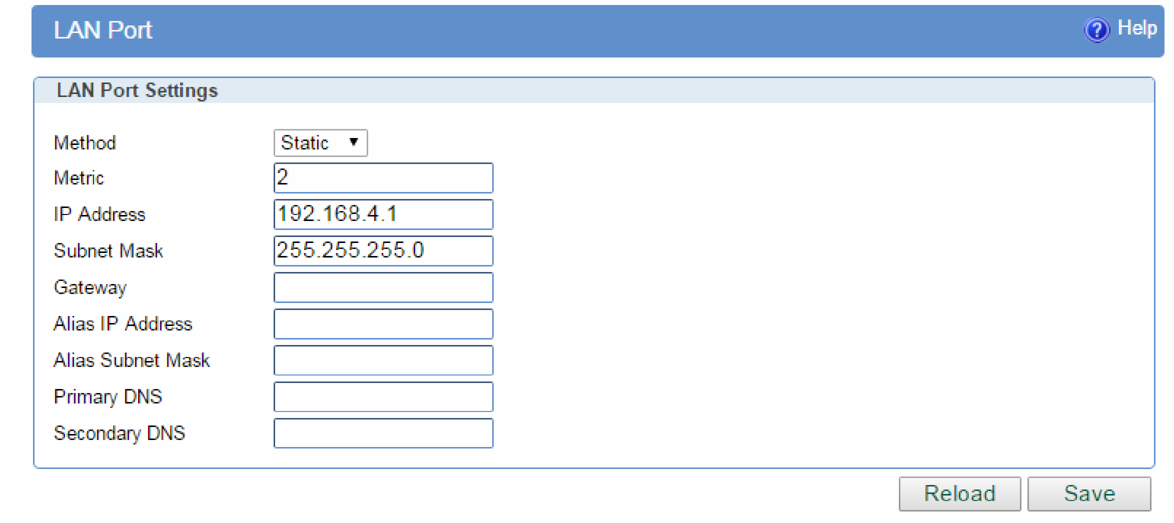
The GWG Gateways requirements:

- 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/LTE networks GWG Gateway 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 GWG Gateway 1 configuration:

- Click ***LAN Ports***, to open the **LAN Port Settings** 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.

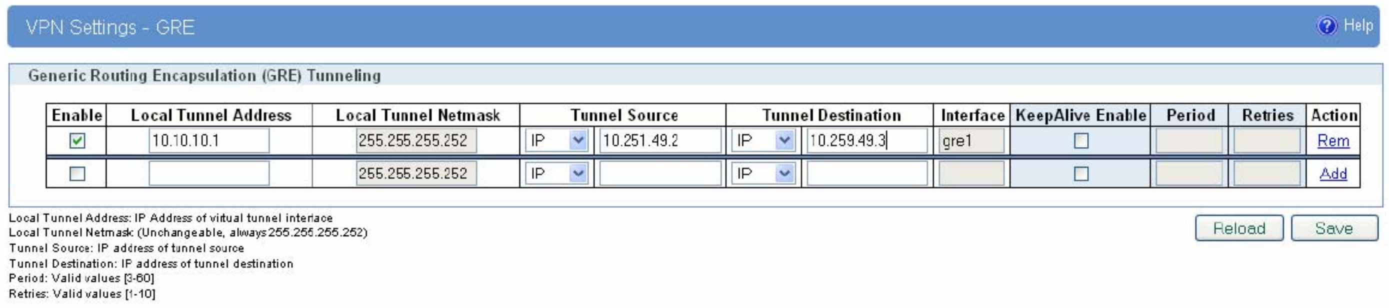


LAN Port Settings

Method	Static ▼
Metric	2
IP Address	192.168.4.1
Subnet Mask	255.255.255.0
Gateway	
Alias IP Address	
Alias Subnet Mask	
Primary DNS	
Secondary DNS	

Figure 73 – 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/LTE provider's network default gateway).
- Click ***Mobile 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/LTE connection (***Mobile 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: 1. 10.251.49.2 (obtained by the network provider)
    2. Select HOST from drop down menu if you want to use host name as peer identifier
  - Tunnel Destination: 1. 10.251.49.3 (obtained by the network provider)
    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.



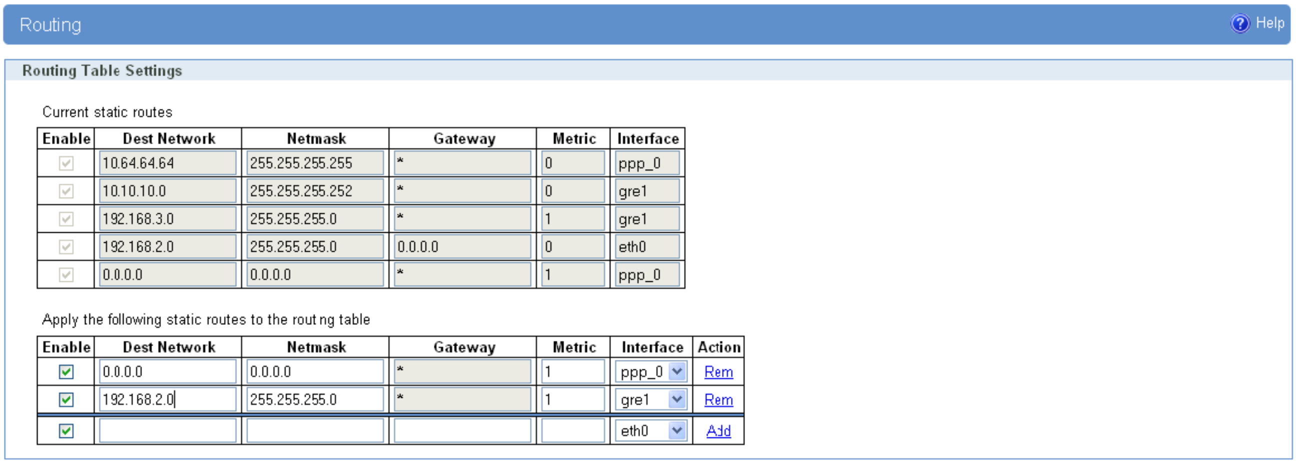
Generic Routing Encapsulation (GRE) Tunneling

Enable	Local Tunnel Address	Local Tunnel Netmask	Tunnel Source		Tunnel Destination		Interface	KeepAlive Enable	Period	Retries	Action
☑	10.10.10.1	255.255.255.252	IP	10.251.49.2	IP	10.259.49.3	gre1	□			Rem
□		255.255.255.252	IP		IP			□			Add

Local Tunnel Address: IP Address of vitual tunnel interface
Local Tunnel Netmask (Unchangeable, always 255.255.255.252)
Tunnel Source: IP address of tunnel source
Tunnel Destination: IP address of tunnel destination
Period: Valid values [3-60]
Retries: Valid values [1-10]

Figure 74 – GRE configuration page for GWR Router 1

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



Routing Table Settings

Current static routes

Enable	Dest Network	Netmask	Gateway	Metric	Interface
☑	10.64.64.64	255.255.255.255	*	0	ppp_0
☑	10.10.10.0	255.255.255.252	*	0	gre1
☑	192.168.3.0	255.255.255.0	*	1	gre1
☑	192.168.2.0	255.255.255.0	0.0.0.0	0	eth0
☑	0.0.0.0	0.0.0.0	*	1	ppp_0

Apply the following static routes to the rout ng table

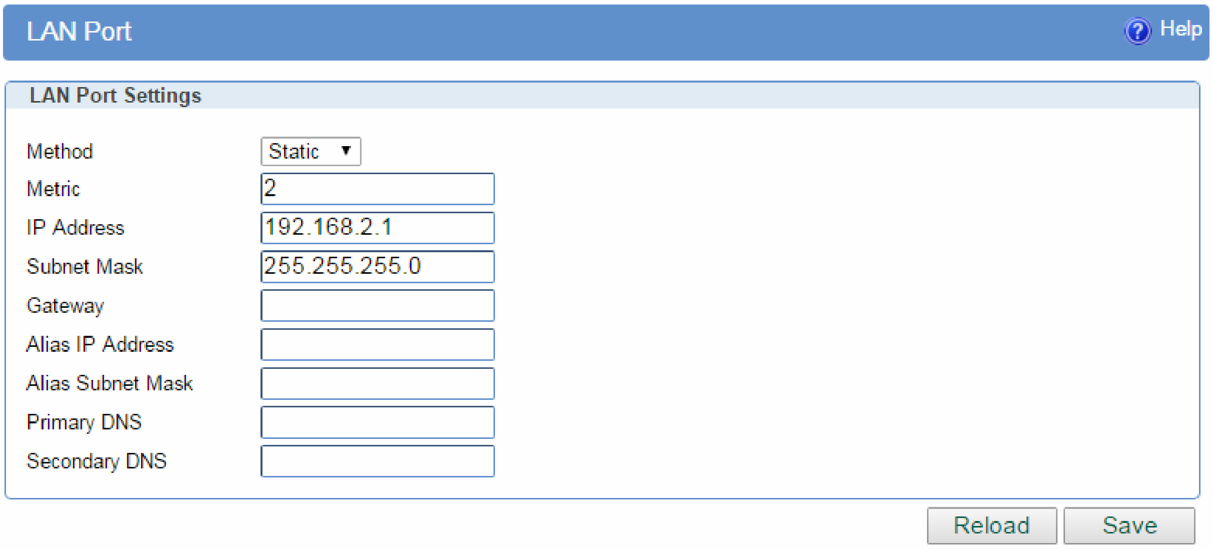
Enable	Dest Network	Netmask	Gateway	Metric	Interface	Action
☑	0.0.0.0	0.0.0.0	*	1	ppp_0	Rem
☑	192.168.2.0	255.255.255.0	*	1	gre1	Rem
☑					eth0	Add

Figure 75 – Routing configuration page for GWG Gateway 1

- Optionally configure IP Filtering to block any unwanted incoming traffic.
- On the device connected on GWG Gateway 1 setup default gateway 192.168.4.1

The GWG Gateway 2 configuration:

- Click ***LAN Ports*** Tab, to open the **LAN Ports Settings** 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.



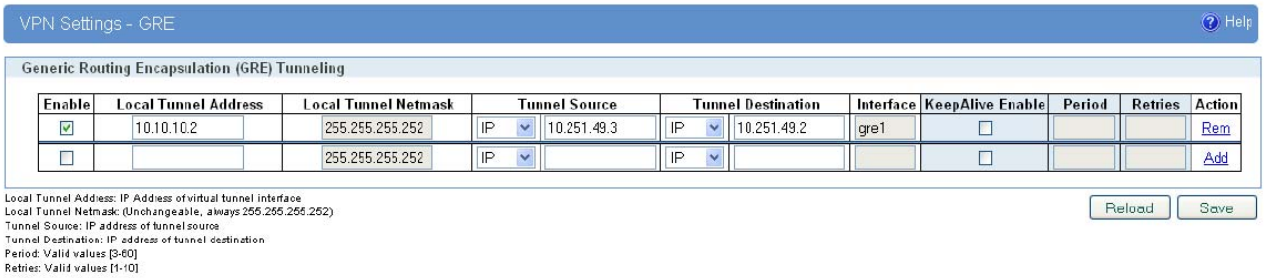
LAN Port Settings

Method	Static
Metric	2
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Gateway	
Alias IP Address	
Alias Subnet Mask	
Primary DNS	
Secondary DNS	

Figure 76 – 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/LTE provider's network default gateway).

- Click ***Mobile Settings*** Tab to configure parameters necessary for GSM/UMTS/LTE connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS/LTE connection (***Mobile 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: 1. 10.251.49.3 (obtained by the network provider)
    2. Select HOST from drop down menu if you want to use host name as peer identifier
  - Tunnel Destination: 1. 10.251.49.2 (obtained by the network provider)
  - 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.

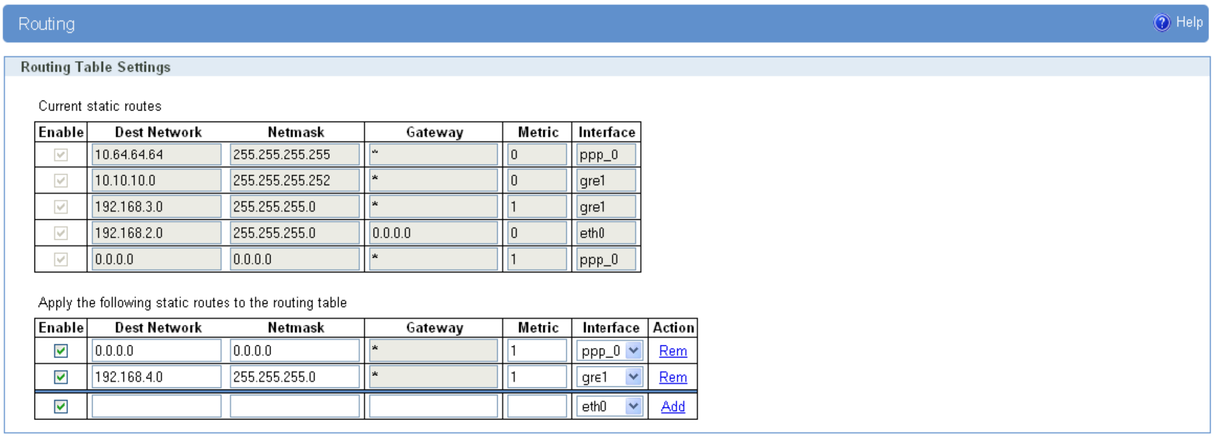


Enable	Local Tunnel Address	Local Tunnel Netmask	Tunnel Source		Tunnel Destination		Interface	KeepAlive Enable	Period	Retries	Action
☑	10.10.10.2	255.255.255.252	IP	10.251.49.3	IP	10.251.49.2	gre1	☐			Rem
☐		255.255.255.252	IP		IP			☐			Add

Local Tunnel Address: IP Address of virtual tunnel interface
Local Tunnel Netmask: (Unchangeable, always 255.255.255.252)
Tunnel Source: IP address of tunnel source
Tunnel Destination: IP address of tunnel destination
Period: Valid values [3-60]
Retries: Valid values [1-10]

Figure 77 – GRE configuration page for GWG Gateway 2

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



Current static routes

Enable	Dest Network	Netmask	Gateway	Metric	Interface
☑	10.64.64.64	255.255.255.255	*	0	ppp_0
☑	10.10.10.0	255.255.255.252	*	0	gre1
☑	192.168.3.0	255.255.255.0	*	1	gre1
☑	192.168.2.0	255.255.255.0	0.0.0.0	0	eth0
☑	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
☑	0.0.0.0	0.0.0.0	*	1	ppp_0	Rem
☑	192.168.4.0	255.255.255.0	*	1	gre1	Rem
☑					eth0	Add

Figure 78 – Routing configuration page for GWG Gateway 2

- Optionally configure IP Filtering to block any unwanted incoming traffic.
- On the device connected on GWG Gateway 2 setup default gateway 192.168.2.1.

GRE Tunnel configuration between GWG Gateway 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 (*Figure* 799) is illustrated simple network with two sites. Idea is to create GRE tunnel for LAN to LAN (site to site) connectivity.

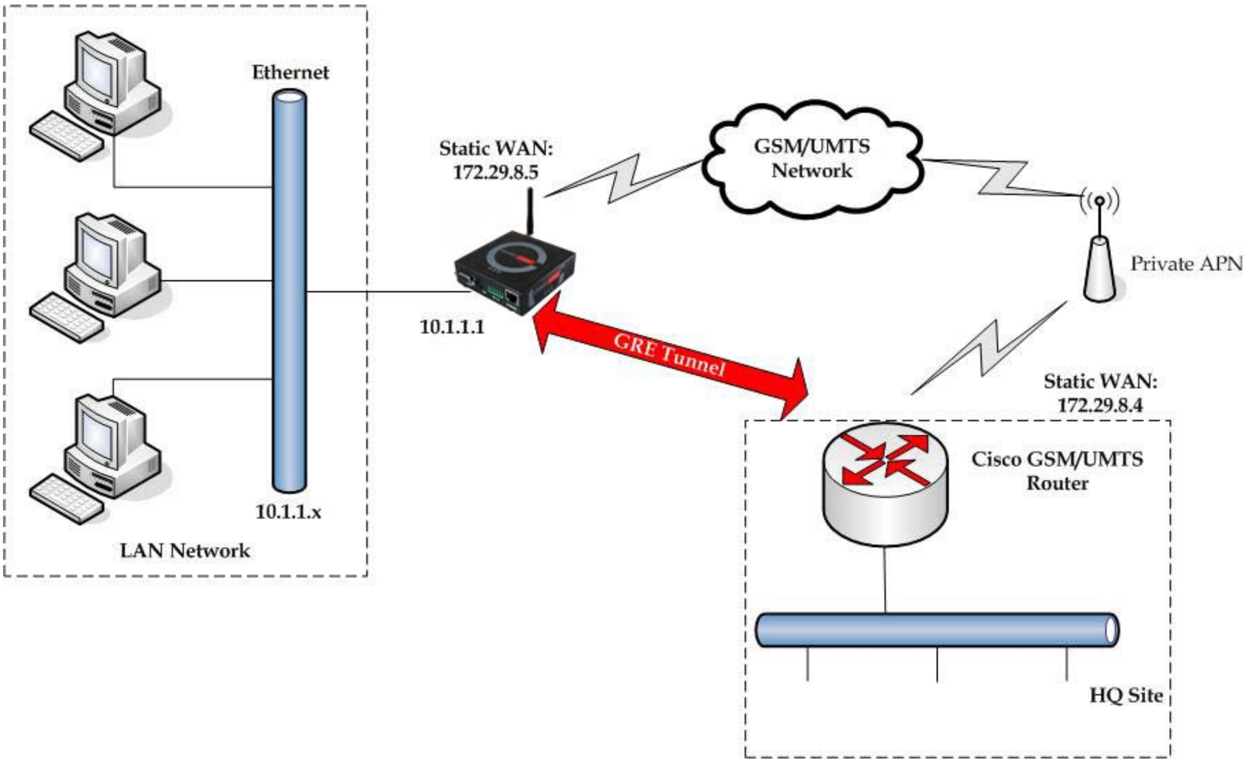


Figure 79 – GRE tunnel between Cisco router and GWG Gateway

GRE tunnel is created between Cisco router with GRE functionality on the HQ Site and the GWG Gateway on the Remote Network. In this example, it is necessary for both, gateway and route, to create tunnel interface (virtual interface). This new tunnel interface is its own network. To each of the gateway and router, 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 GWG Gateway uses Network Address Translation (NAT) where only the mobile IP address is visible to the outside. All outgoing traffic uses the GWG Gateway 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 GWG Gateway 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 has to support GRE protocol,
   - Tunnel peer address will be the GWG Gateway WAN's mobile IP address. For this reason, a static mobile IP address is preferred on the GWG Gateway WAN (GPRS) side,
   - Remote Subnet is remote LAN network address and Remote Subnet Mask is subnet of remote LAN.

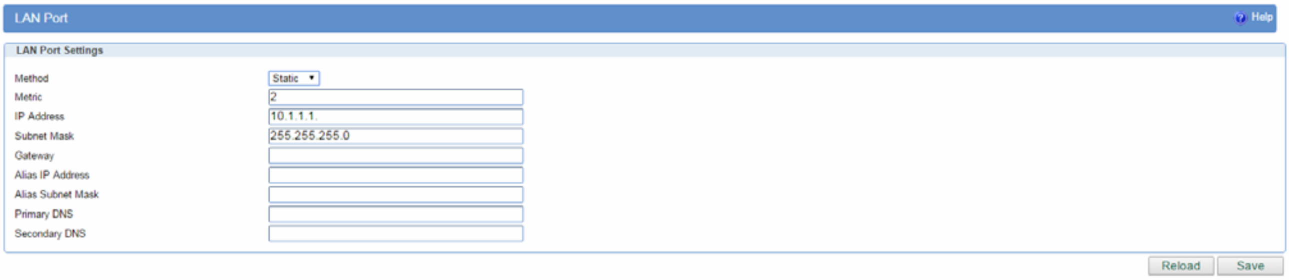
2. The GWG Gateway requirements:
- Static IP WAN address,
- Peer Tunnel Address will be the HQ router WAN IP address (static IP address),
- Remote Subnet is HQ LAN IP address and Remote Subnet Mask is subnet mask of HQ LAN.

GSM/UMTS APN Type: For GSM/UMTS networks GWG Gateway 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 10.10.10.2 255.255.255.252
tunnel source FastEthernet0/0
tunnel destination 172.29.8.5

ip route 10.1.1.0 255.255.255.0 tunnel0

Command for tunnel status: show ip interface brief
```

The GWG Gateway Sample Configuration:
- Click ***LAN Ports*** Tab, to open the **LAN Port Settings** 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.



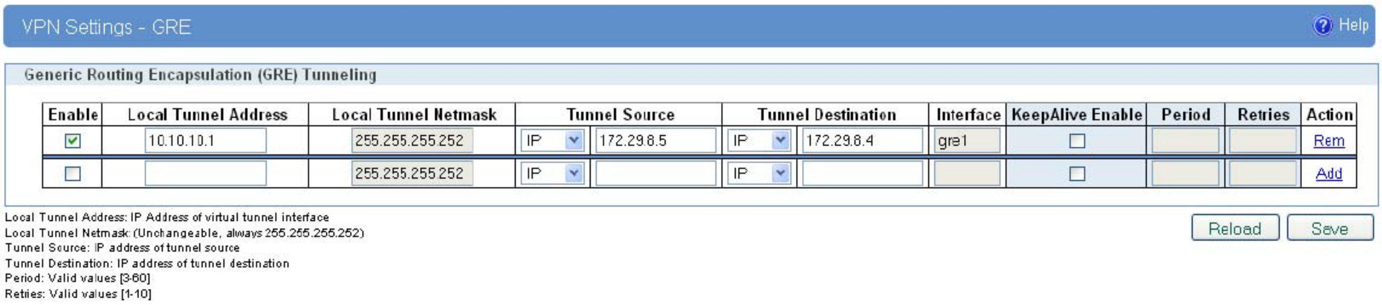
LAN Port Settings

Method	Static ▾
Metric	2
IP Address	10.1.1.1.
Subnet Mask	255.255.255.0
Gateway	
Alias IP Address	
Alias Subnet Mask	
Primary DNS	
Secondary DNS	

Figure 80 – LAN Port 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/LTE provider's network default gateway).
- Click ***Mobile Settings Tab*** to configure parameters necessary for GSM/UMTS/LTE connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS/LTE connection (***Mobile Settings*** Tab). If disconnected please click ***Connect*** button.
- Click ***VPN Settings > GRE Tunneling*** to configure new VPN tunnel parameters:

  - Enable: yes,
  - Local Tunnel Address: 10.10.10.1,
  - 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.



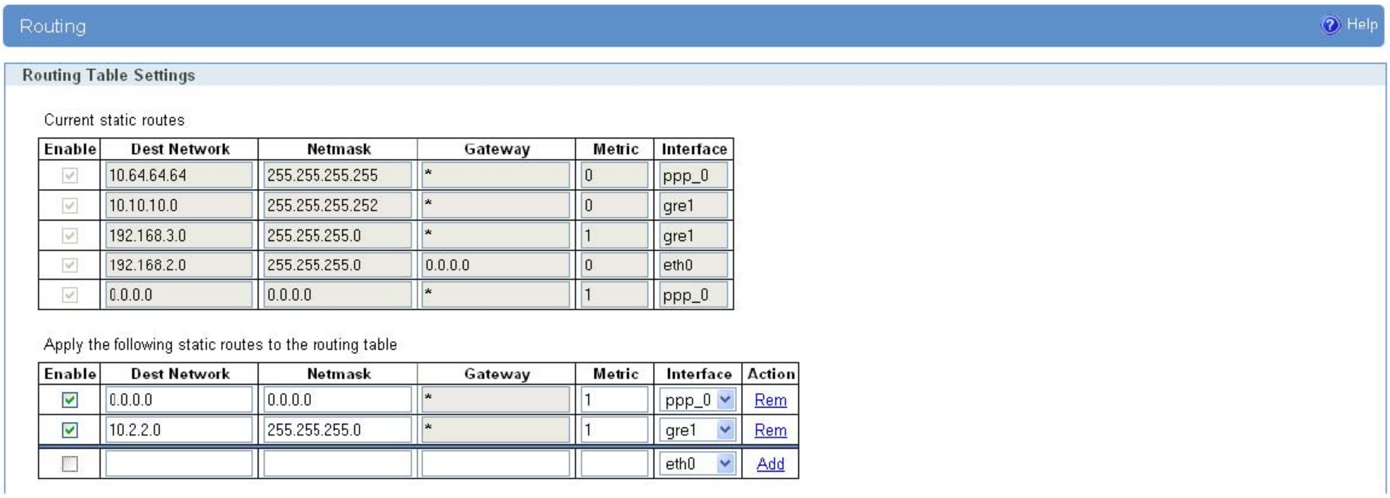
Generic Routing Encapsulation (GRE) Tunneling

Enable	Local Tunnel Address	Local Tunnel Netmask	Tunnel Source		Tunnel Destination		Interface	KeepAlive Enable	Period	Retries	Action
☑	10.10.10.1	255.255.255.252	IP	172.29.8.5	IP	172.29.8.4	gre1	□			Rem
□		255.255.255.252	IP		IP			□			Add

Local Tunnel Address: IP Address of virtual tunnel interface
Local Tunnel Netmask: (Unchangeable, always 255.255.255.252)
Tunnel Source: IP address of tunnel source
Tunnel Destination: IP address of tunnel destination
Period: Valid values [3-60]
Retries: Valid values [1-10]

Figure 81 – GRE configuration page

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



Routing Table Settings

Current static routes

Enable	Dest Network	Netmask	Gateway	Metric	Interface
☑	10.64.64.64	255.255.255.255	*	0	ppp_0
☑	10.10.10.0	255.255.255.252	*	0	gre1
☑	192.168.3.0	255.255.255.0	*	1	gre1
☑	192.168.2.0	255.255.255.0	0.0.0.0	0	eth0
☑	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
☑	0.0.0.0	0.0.0.0	*	1	ppp_0	Rem
☑	10.2.2.0	255.255.255.0	*	1	gre1	Rem
□					eth0	Add

Figure 82 – 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 GWG Gateways

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

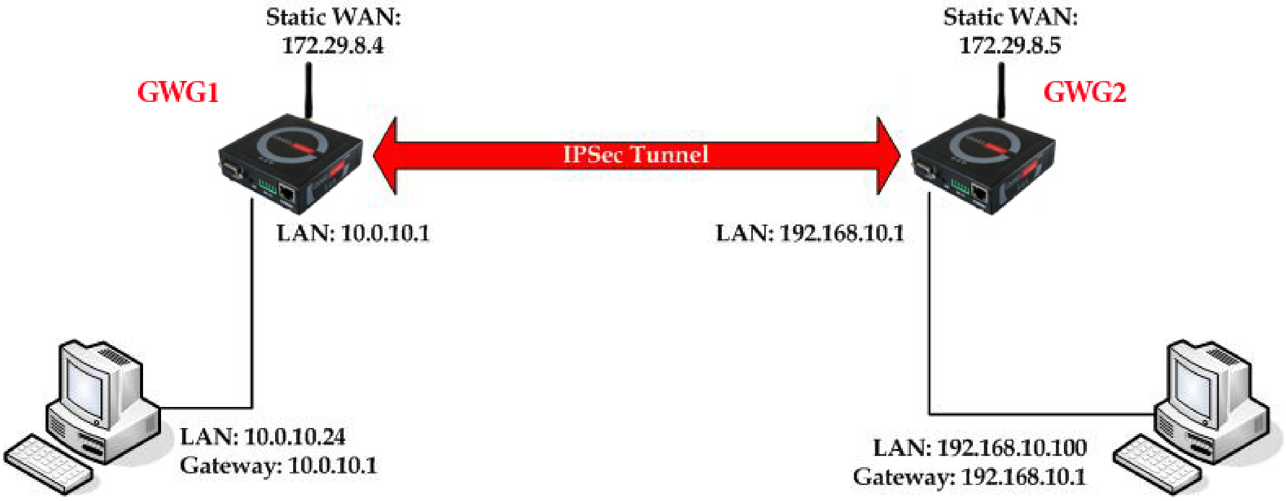


Figure 83 – IPSec tunnel between two GWG Gateways

The GWG Gateways 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 GWG Gateway 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* 83 will be used for both scenarios.

Scenario #1

Gateway 1 and Gateway 2 , presented in the *Figure 84*, have firmware version that provides two modes of negotiation in IPSec tunnel configuration process:

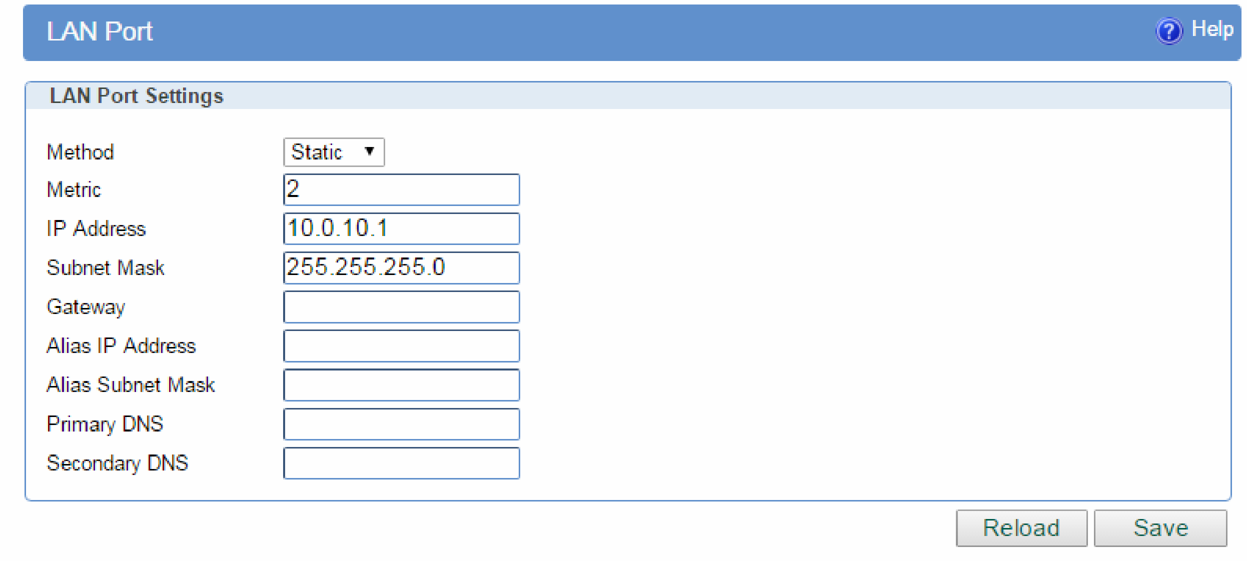
- Aggressive
- Main

In this scenario, aggressive mode will be used. Configurations for Gateway 1 and Gateway 2 are listed below.

The GWG Gateway 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.



LAN Port

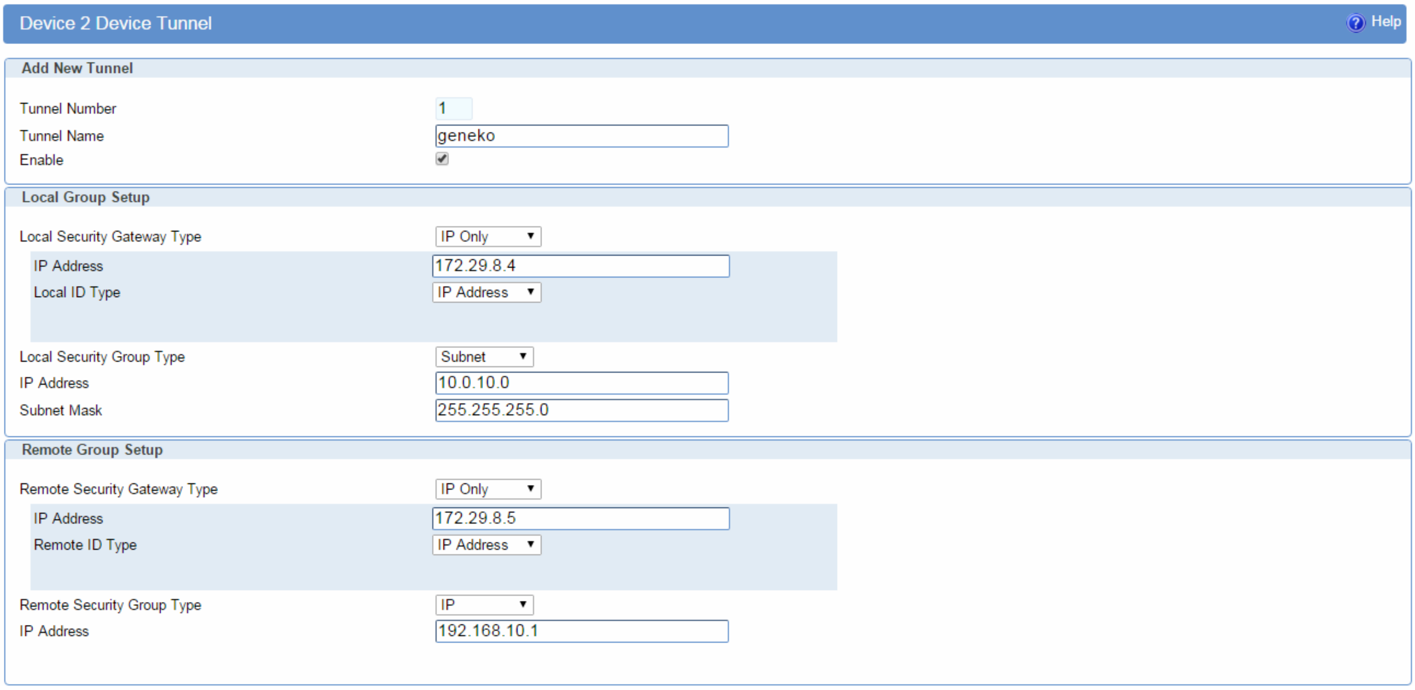
LAN Port Settings

Method	Static
Metric	2
IP Address	10.0.10.1
Subnet Mask	255.255.255.0
Gateway	
Alias IP Address	
Alias Subnet Mask	
Primary DNS	
Secondary DNS	

Figure 84 – LAN Port configuration page for GWG Gateway 1

- Use SIM card with a static IP address, obtained from Mobile Operator.
- Click ***Mobile Settings*** Tab to configure parameters necessary for GSM/UMTS/LTE connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS/LTE connection (***Mobile 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: geneko,
    - Enable: true,
  - ***Local Group Setup***
    - Local Security Gateway Type: IP only
    - IP Address: 172.29.8.4
    - 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.
  - ***IPSec Setup***
    - Key Exchange Mode: IKE with Preshared key,
    - Mode: aggressive,
    - Phase 1 DH group: Group 2,
    - Phase 1 Encryption: AES-128,
    - Phase 1 Authentication: SHA1,
    - Phase 1 SA Life Time: 28800,
    - Perfect Forward Secrecy: true,
    - Phase 2 DH group: Group 2,
    - Phase 2 Encryption: AES-128,
    - Phase 2 Authentication: SHA1,
    - Phase 2 SA Life Time: 3600,

- Preshared Key: 1234567890.
- *Failover*
  - 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.



Device 2 Device Tunnel

Add New Tunnel

Tunnel Number	1
Tunnel Name	geneko
Enable	☑

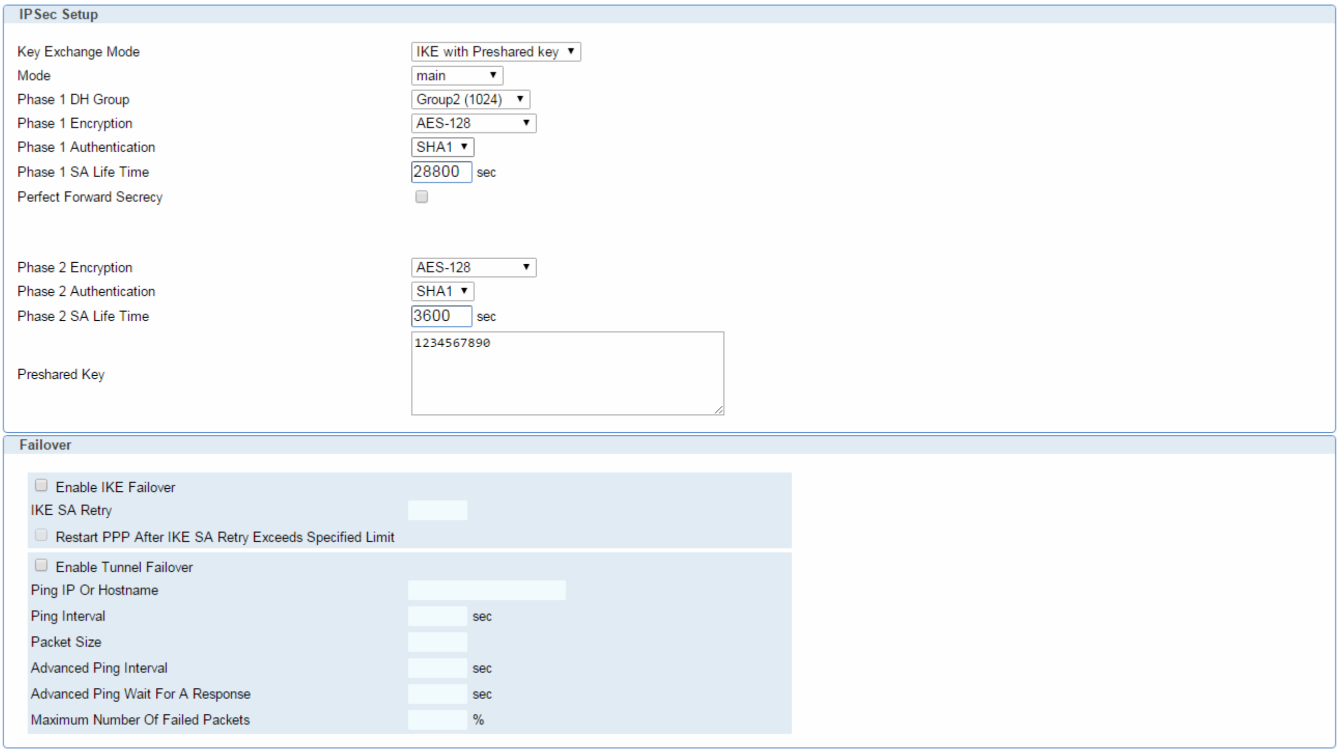
Local Group Setup

Local Security Gateway Type	IP Only
IP Address	172.29.8.4
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

Figure 85 – IPSEC configuration page I for GWG Gateway 1

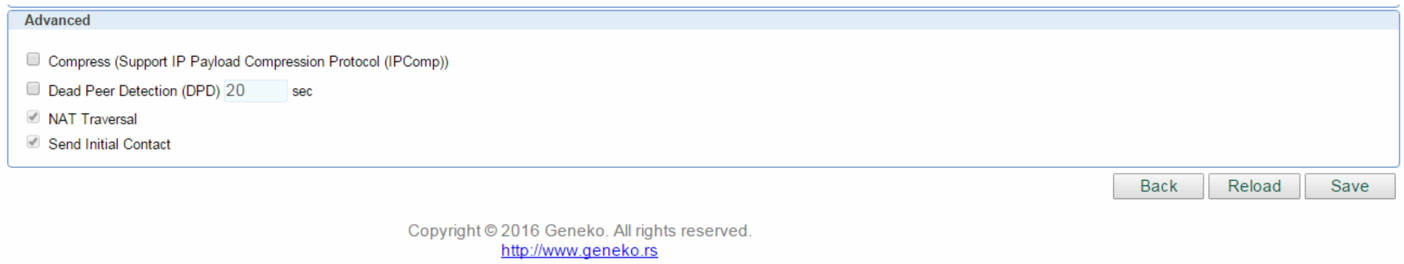


IPSec Setup

Key Exchange Mode	IKE with Preshared key
Mode	main
Phase 1 DH Group	Group2 (1024)
Phase 1 Encryption	AES-128
Phase 1 Authentication	SHA1
Phase 1 SA Life Time	28800 sec
Perfect Forward Secrecy	□
Phase 2 Encryption	AES-128
Phase 2 Authentication	SHA1
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 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

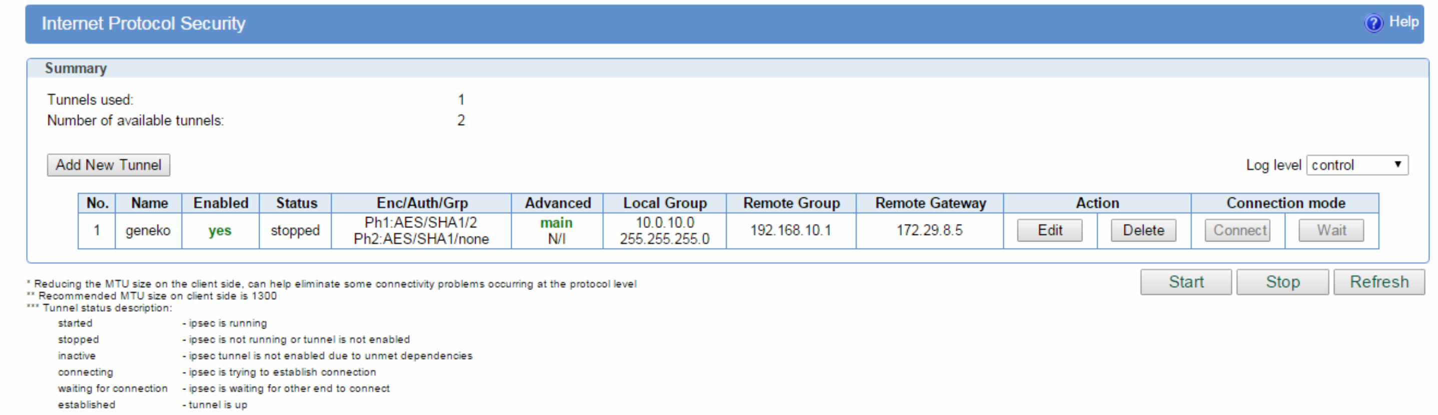
☑ Send Initial Contact

Copyright © 2016 Geneko. All rights reserved.
http://www.geneko.rs

Figure 86 – IPSec configuration page II for GWG Gateway 1

NOTE : Options NAT Traversal and Send Initial Contact are predefined
Click ***Start*** button on ***Internet Protocol Security*** page to initiate IPSEC tunnel.

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.



Summary

Tunnels used: 1
Number of available tunnels: 2

Log level control

No.	Name	Enabled	Status	Enc/Auth/Grp	Advanced	Local Group	Remote Group	Remote Gateway	Action		Connection mode	
1	geneko	yes	stopped	Ph1:AES/SHA1/2 Ph2:AES/SHA1/none	main 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 occuring 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

Figure 87 – IPSec start/stop page for GWG Gateway 1

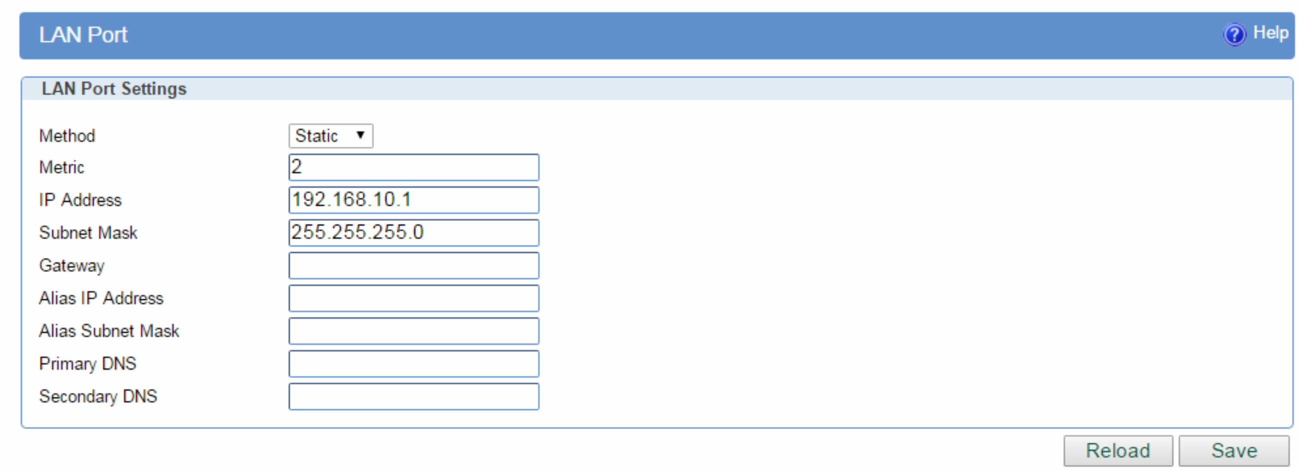
Click **Start** button and after that **Connect** button on **Internet Protocol Security** page to initiate IPSEC tunnel

- On the device connected on GWG gateway 1 setup default gateway 10.0.10.1

The GWG Gateway 2 configuration:

- Click ***LAN Ports*** Tab, to open the **LAN Ports Settings** 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.



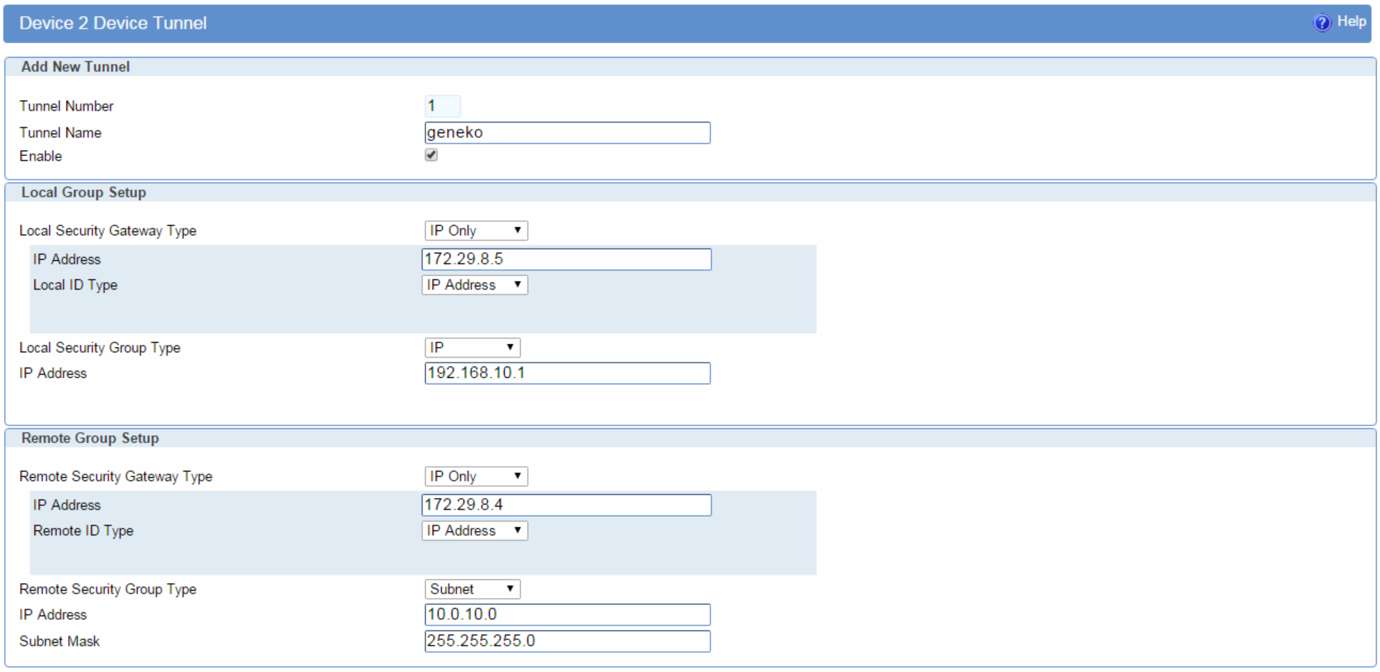
Method	Static ▾
Metric	2
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
Gateway	
Alias IP Address	
Alias Subnet Mask	
Primary DNS	
Secondary DNS	

Figure 88 – Network configuration page for GWR Router 2

- Use SIM card with a static IP address, obtained from Mobile Operator.
- Click ***Mobile Settings*** Tab to configure parameters necessary for GSM/UMTS/LTE connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS/LTE connection (***Mobile 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: IPsec tunnel
    - Enable: true.
  - ***Local Group Setup***
    - Local Security Gateway Type: IP only
    - IP Address: 172.29.8.5
    - 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
  - ***IPSec Setup***
    - Keying Mode: IKE with Preshared key
    - Mode: aggressive
    - Phase 1 DH group: Group 2
    - Phase 1 Encryption: AES-128
    - Phase 1 Authentication: SHA1
    - Phase 1 SA Life Time: 28800
    - Perfect Forward Secrecy: true
    - Phase 2 DH group: Group 2
    - Phase 2 Encryption: AES128
    - Phase 2 Authentication: SHA1
    - Phase 2 SA Life Time: 3600
    - Preshared Key: 1234567890

- *Failover*
  - 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

Add New Tunnel

Tunnel Number	1
Tunnel Name	geneko
Enable	☑

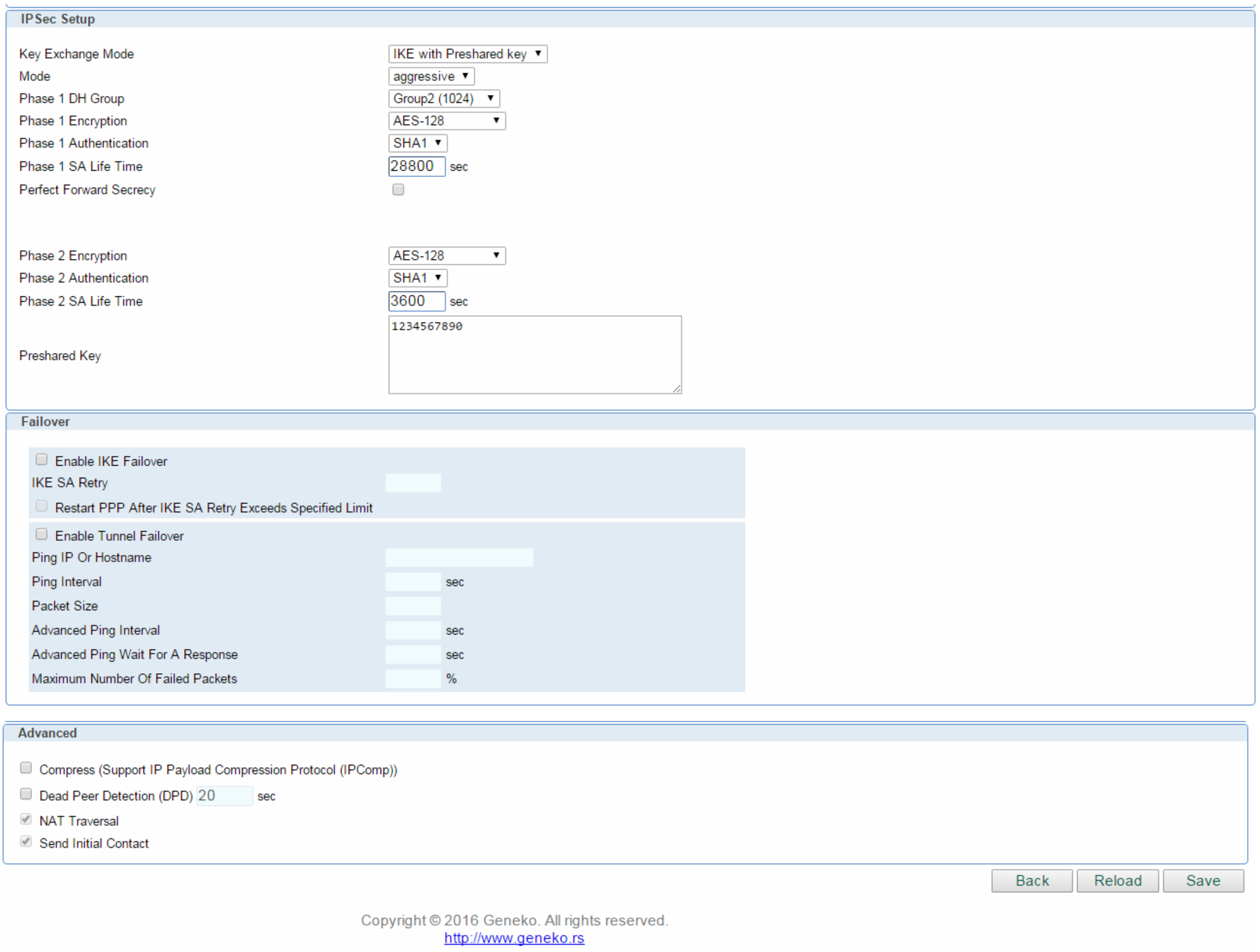
Local Group Setup

Local Security Gateway Type	IP Only
IP Address	172.29.8.5
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 Mask	255.255.255.0

Figure 89 – IPSEC configuration page I for GWG Gateway 2



IPSec Setup

Key Exchange Mode	IKE with Preshared key
Mode	aggressive
Phase 1 DH Group	Group2 (1024)
Phase 1 Encryption	AES-128
Phase 1 Authentication	SHA1
Phase 1 SA Life Time	28800 sec
Perfect Forward Secrecy	□
Phase 2 Encryption	AES-128
Phase 2 Authentication	SHA1
Phase 2 SA Life Time	3600 sec
Preshared Key	1234567890

Failover

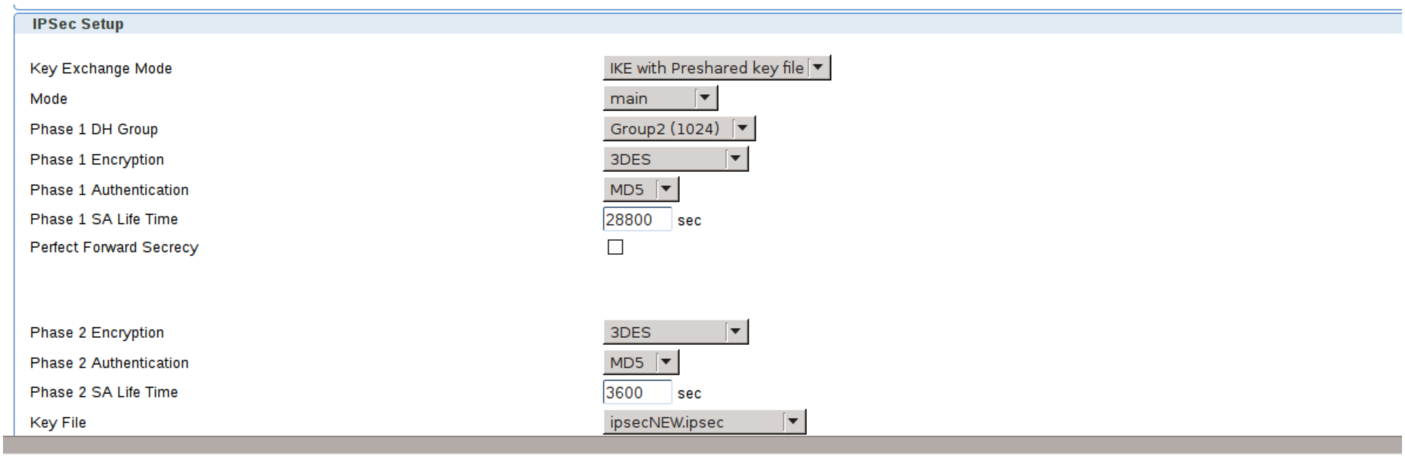
□ Enable IKE Failover	
IKE SA Retry	
□ Restart PPP After IKE SA Retry Exceeds Specified Limit	
□ Enable Tunnel Failover	
Ping IP Or Hostname	
Ping Interval	sec
Packet Size	
Advanced Ping Interval	sec
Advanced Ping Wait For A Response	sec
Maximum Number Of Failed Packets	%

Advanced

□ Compress (Support IP Payload Compression Protocol (IPComp))
□ Dead Peer Detection (DPD) 20 sec
☑ NAT Traversal
☑ Send Initial Contact

Copyright © 2016 Geneko. All rights reserved.
http://www.geneko.rs

Figure 90 – IPSec configuration page II for GWG Gateway 2



IPSec Setup

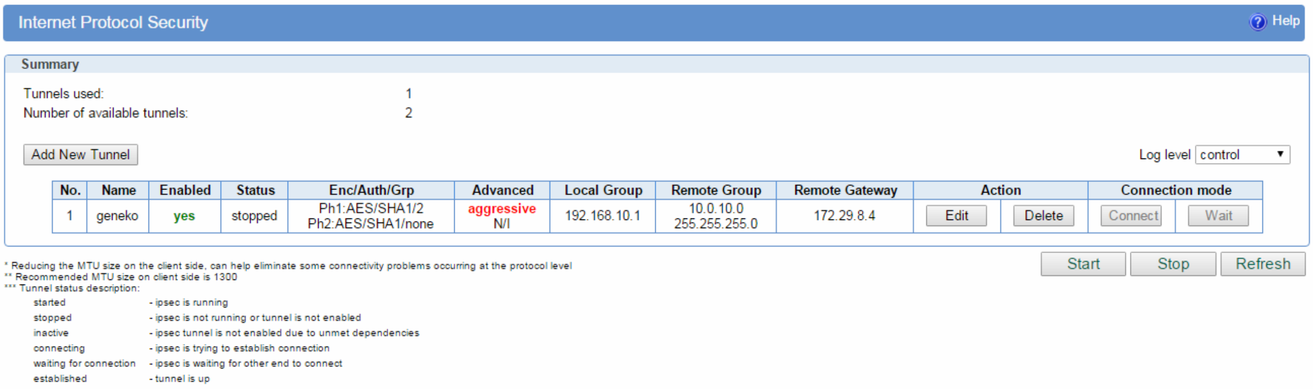
Key Exchange Mode	IKE with Preshared key file
Mode	main
Phase 1 DH Group	Group2 (1024)
Phase 1 Encryption	3DES
Phase 1 Authentication	MD5
Phase 1 SA Life Time	28800 sec
Perfect Forward Secrecy	□
Phase 2 Encryption	3DES
Phase 2 Authentication	MD5
Phase 2 SA Life Time	3600 sec
Key File	ipsecNEW.ipsec

Figure 91- IPSec configuration using certificates

NOTE : Options NAT Traversal and Send Initial Contact are predefined.
Click ***Start*** button on ***Internet Protocol Security*** page to initiate IPSEC tunnel.

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.



Summary

Tunnels used: 1
Number of available tunnels: 2

Log level: control

No.	Name	Enabled	Status	Enc/Auth/Grp	Advanced	Local Group	Remote Group	Remote Gateway	Action		Connection mode	
1	geneko	yes	stopped	Ph1:AES/SHA1/2 Ph2:AES/SHA1/none	aggressive N/I	192.168.10.1	10.0.10.0 255.255.255.0	172.29.8.4	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

Figure 92 – IPSec start/stop page for GWG Gateway 2

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

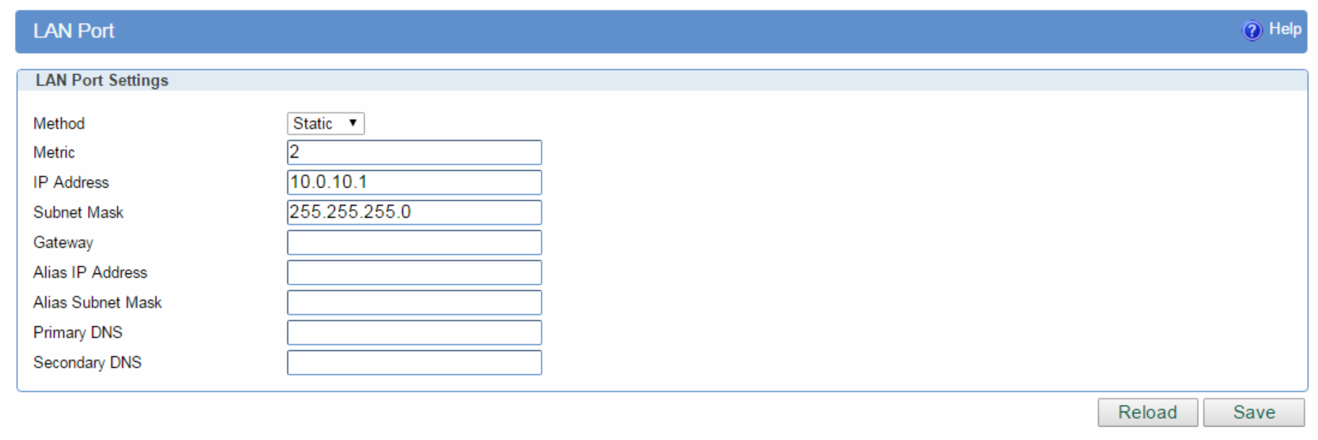
- On the device connected on GWG gateway 2 setup default gateway 192.168.10.1.

Scenario #2

Gateway 1 and Gateway 2, presented in the *Figure 93*, are configured with IPSec tunnel in Main mode.
Configurations for Router 1 and Router 2 are listed below.

The GWG Gateway 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.



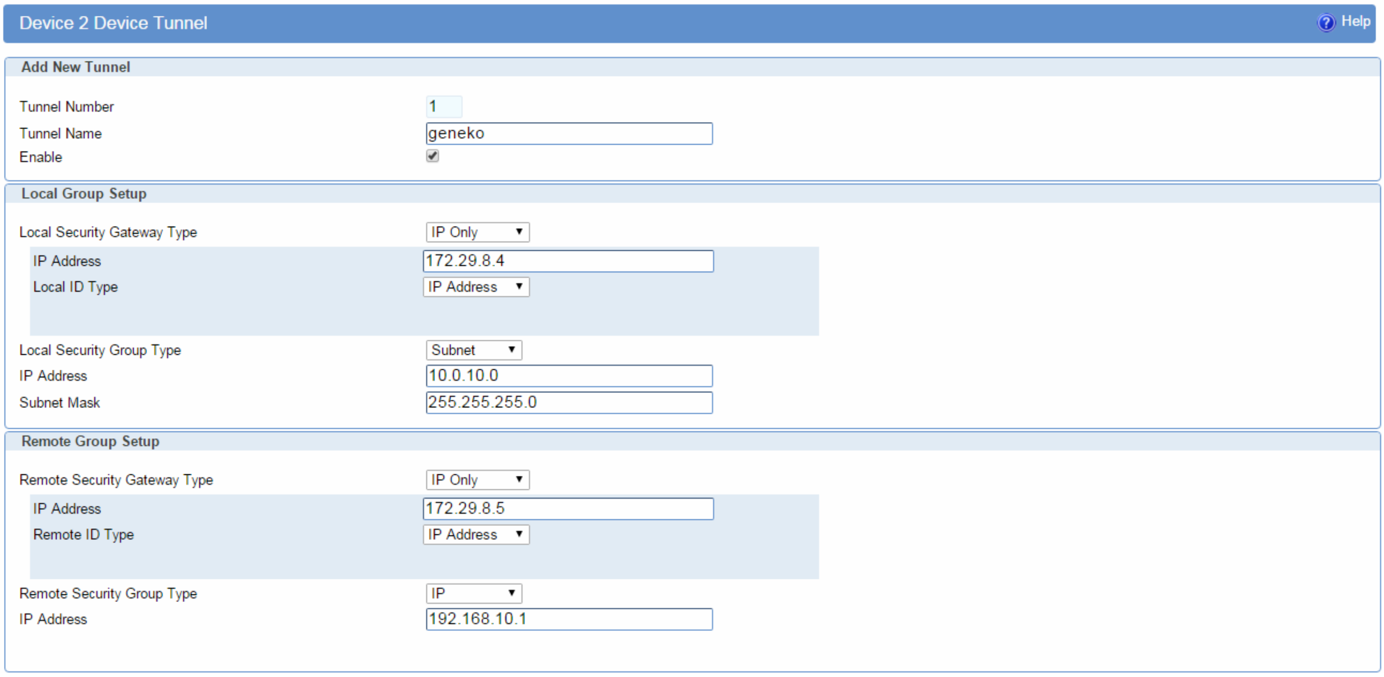
LAN Port Settings

Method	Static
Metric	2
IP Address	10.0.10.1
Subnet Mask	255.255.255.0
Gateway	
Alias IP Address	
Alias Subnet Mask	
Primary DNS	
Secondary DNS	

Figure 93 – Network configuration page for GWG Gateway 1

- Use SIM card with a static IP address, obtained from Mobile Operator.

- Click ***Mobile settings*** Tab to configure parameters necessary for GSM/UMTS/LTE connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS/LTE connection (***Mobile 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: geneko,
    - 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: SHA1,
    - Phase 1 SA Life Time: 28800,
    - Perfect Forward Secrecy: true,
    - Phase 2 DH group: Group 2,
    - Phase 2 Encryption: AES-128,
    - Phase 2 Authentication: SHA1,
    - Phase 2 SA Life Time: 3600,
    - Preshared Key: 1234567890.
  - ***Local Group Setup***
    - Local Security Gateway Type: IP Only,
    - IP Address: 172.29.8.4
    - 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***
    - Eanble 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.



Device 2 Device Tunnel

Help

Add New Tunnel

Tunnel Number	1
Tunnel Name	geneko
Enable	☑

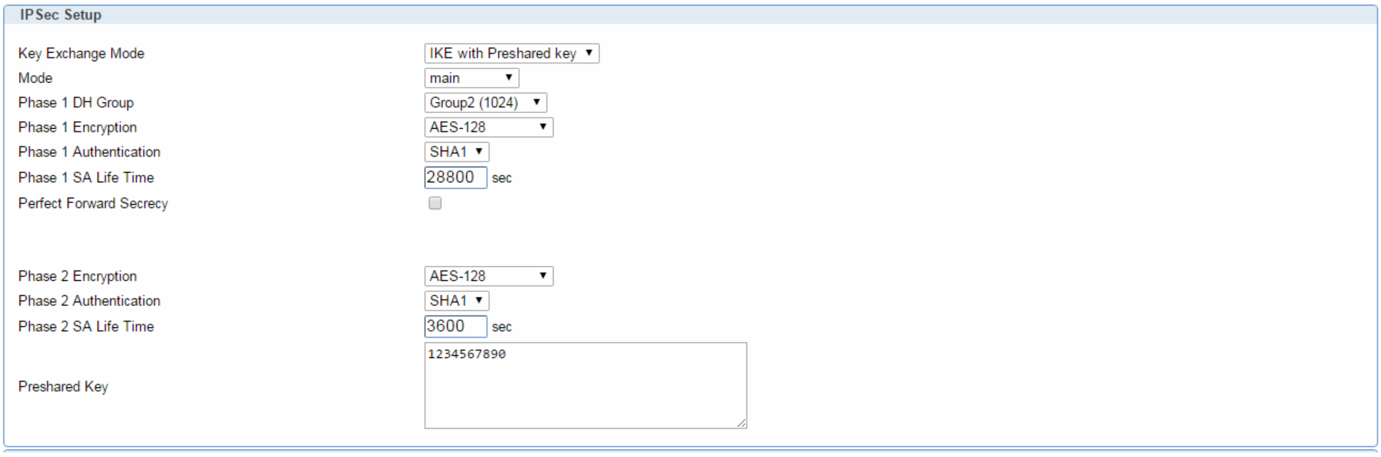
Local Group Setup

Local Security Gateway Type	IP Only ▾
IP Address	172.29.8.4
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

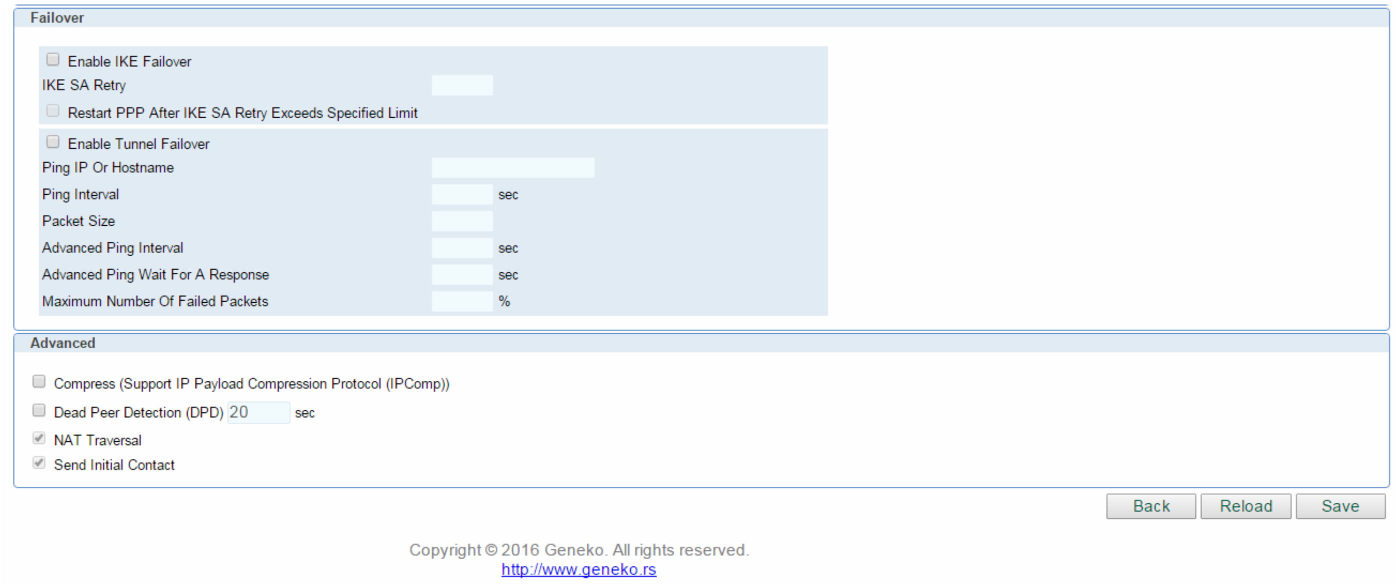
Figure 94 – IPSEC configuration page I for GWG Gateway 1



IPSec Setup

Key Exchange Mode	IKE with Preshared key ▾
Mode	main ▾
Phase 1 DH Group	Group2 (1024) ▾
Phase 1 Encryption	AES-128 ▾
Phase 1 Authentication	SHA1 ▾
Phase 1 SA Life Time	28800 sec
Perfect Forward Secrecy	□
Phase 2 Encryption	AES-128 ▾
Phase 2 Authentication	SHA1 ▾
Phase 2 SA Life Time	3600 sec
Preshared Key	1234567890

Figure 95 – IPSEC configuration page II for GWG Gateway 1



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 %

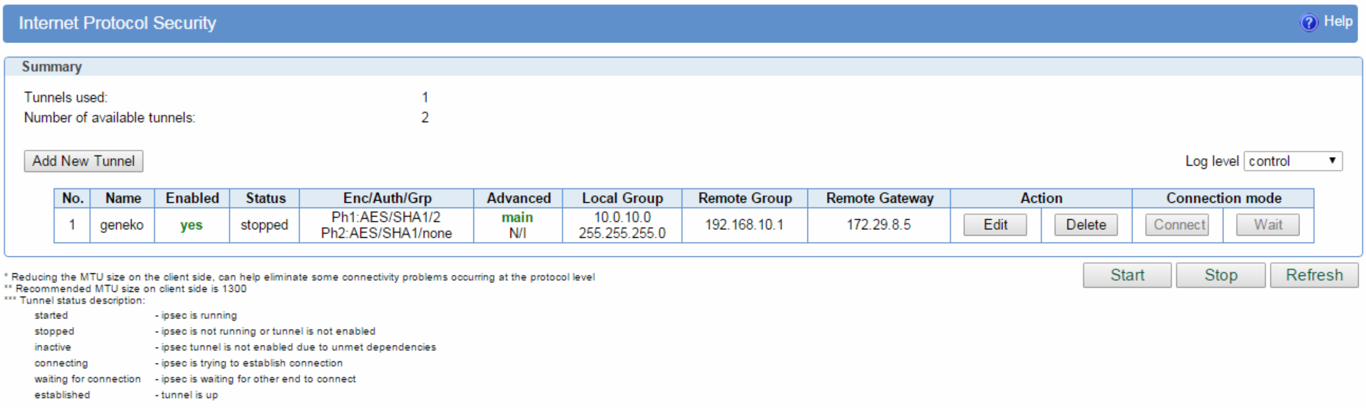
Advanced

☐ Compress (Support IP Payload Compression Protocol (IPComp))
☐ Dead Peer Detection (DPD) 20 sec
☑ NAT Traversal
☑ Send Initial Contact

Copyright © 2016 Geneko. All rights reserved.
http://www.geneko.rs

Figure 96 – IPSEC configuration page III for GWG Gateway 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.



Summary

Tunnels used: 1
Number of available tunnels: 2

Log level control

No.	Name	Enabled	Status	Enc/Auth/Grp	Advanced	Local Group	Remote Group	Remote Gateway	Action		Connection mode	
1	geneko	yes	stopped	Ph1:AES/SHA1/2 Ph2:AES/SHA1/none	main 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
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

Figure 97 – IPSec start/stop page for GWG Gateway 1

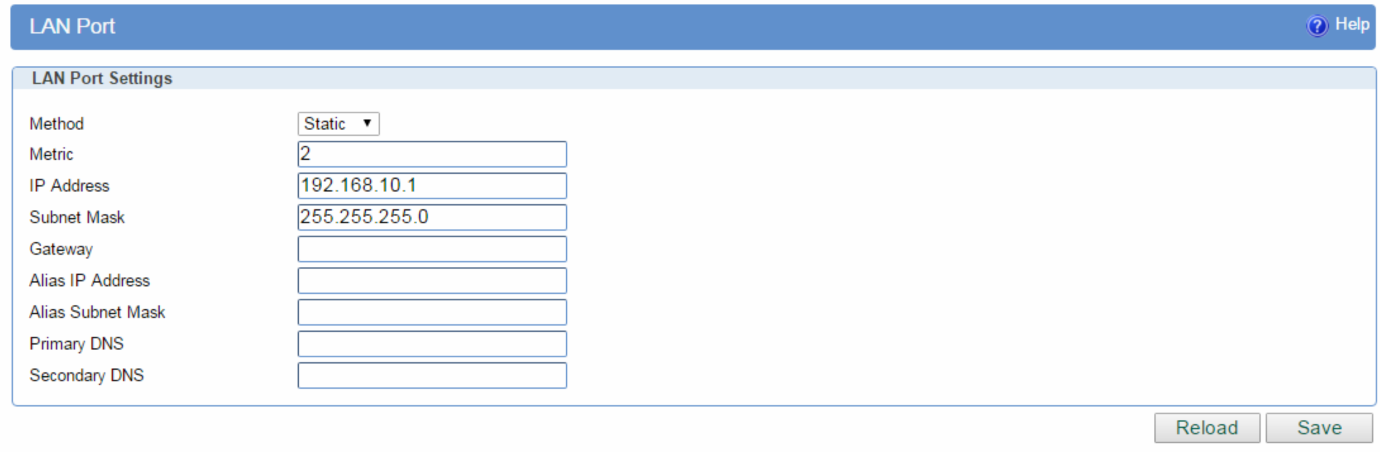
Click *Start* button and after that *Connect* button on *Internet Protocol Security* page to initiate IPSEC tunnel

- On the device connected on GWG Gateway 1 setup default gateway 10.0.10.1.

The GWG Gateway 2 configuration:

- Click ***LAN Port*** 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.



LAN Port

LAN Port Settings

Method	Static
Metric	2
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
Gateway	
Alias IP Address	
Alias Subnet Mask	
Primary DNS	
Secondary DNS	

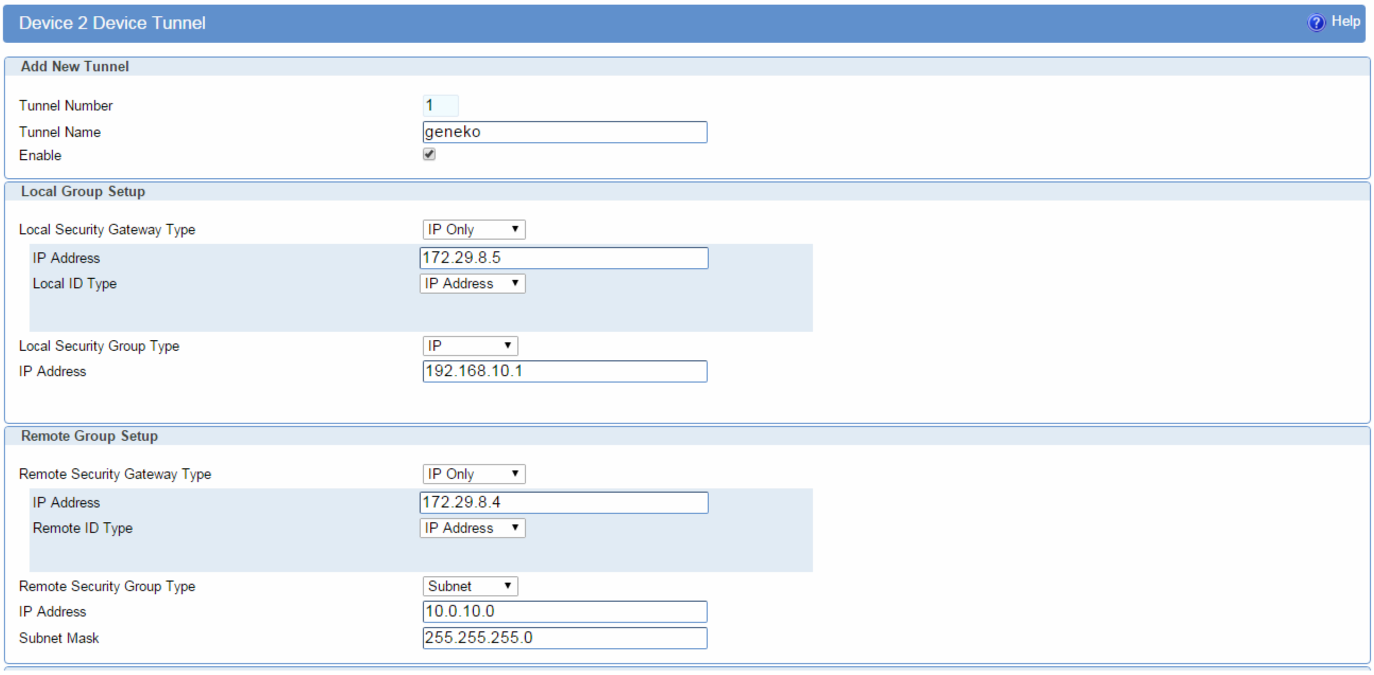
Figure 98 – Network configuration page for GWG Gateway 2

- Use SIM card with a static IP address, obtained from Mobile Operator.
- Click ***Mobile Settings*** Tab to configure parameters necessary for GSM/UMTS/LTE connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS/LTE connection (***Mobile 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: geneko
    - Enable: true
  - ***IPSec Setup***
    - Keying Mode: IKE with Preshared key
    - Mode: main
    - 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: 3DES
    - Phase 2 Authentication: MD5
    - Phase 2 SA Life Time: 3600
    - Preshared Key: 1234567890
  - ***Local Group Setup***
    - Local Security Gateway Type: IP Only
    - IP Address: 172.29.8.5
    - 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 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

Add New Tunnel

Tunnel Number	1
Tunnel Name	geneko
Enable	☑

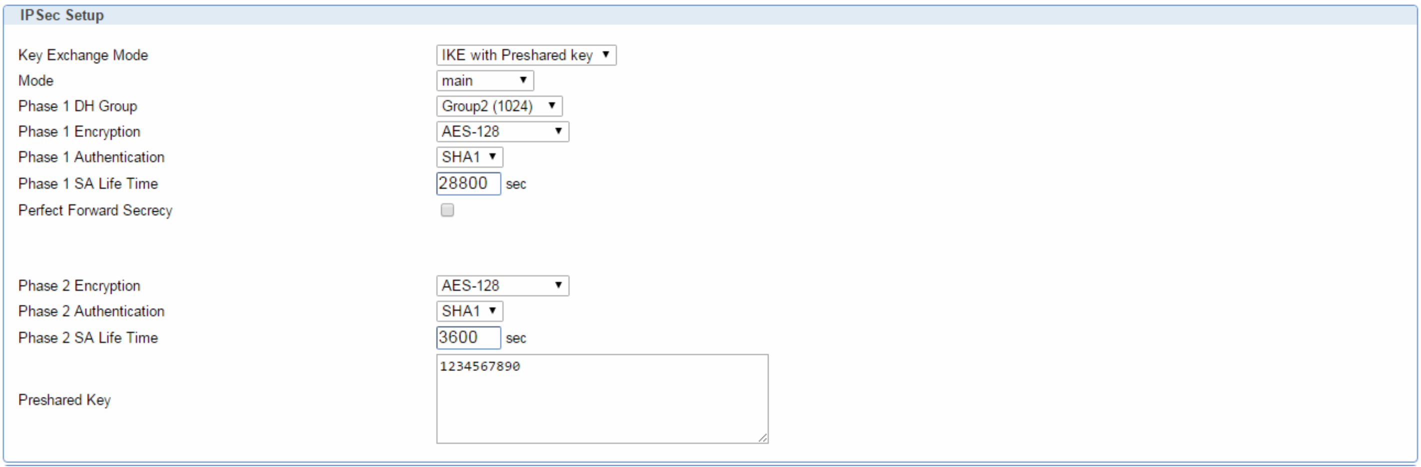
Local Group Setup

Local Security Gateway Type	IP Only
IP Address	172.29.8.5
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 Mask	255.255.255.0

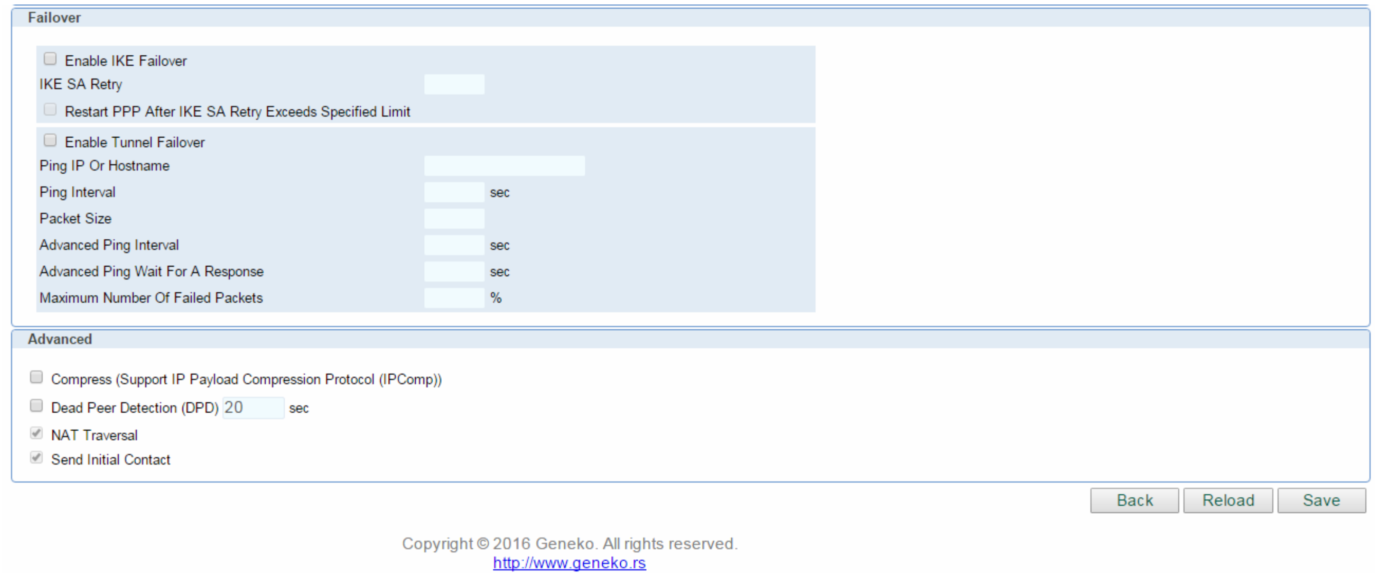
Figure 99 – IPSEC configuration page I for GWG Gateway 2



IPSec Setup

Key Exchange Mode	IKE with Preshared key
Mode	main
Phase 1 DH Group	Group2 (1024)
Phase 1 Encryption	AES-128
Phase 1 Authentication	SHA1
Phase 1 SA Life Time	28800 sec
Perfect Forward Secrecy	☐
Phase 2 Encryption	AES-128
Phase 2 Authentication	SHA1
Phase 2 SA Life Time	3600 sec
Preshared Key	1234567890

Figure 100 – IPSEC configuration page II for GWG Gateway 2



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

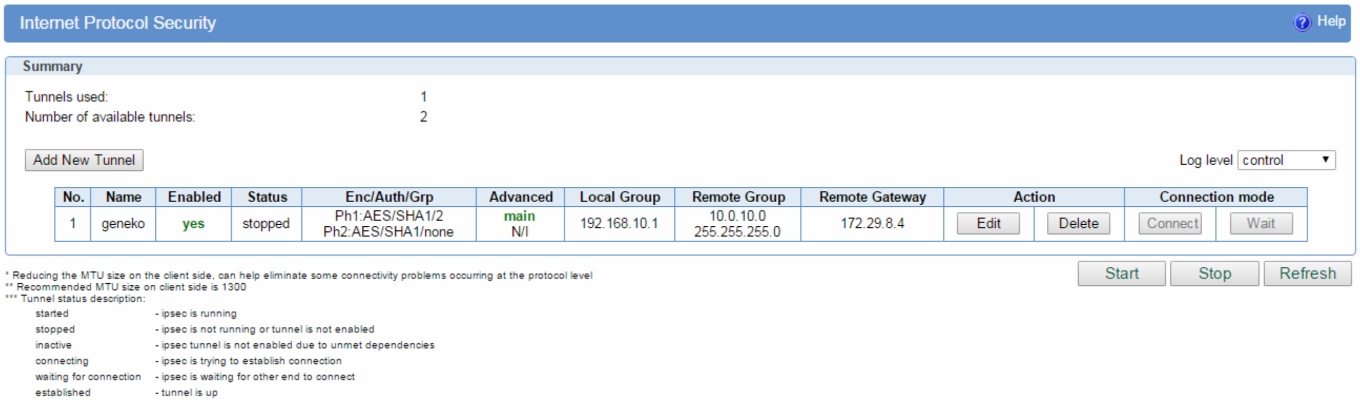
☑ NAT Traversal

☑ Send Initial Contact

Copyright © 2016 Geneko. All rights reserved.
http://www.geneko.rs

Figure 101 – IPSEC configuration page III for GWG Gateway 2

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.



Summary

Tunnels used:	1
Number of available tunnels:	2

Log level control

No.	Name	Enabled	Status	Enc/Auth/Grp	Advanced	Local Group	Remote Group	Remote Gateway	Action		Connection mode	
1	geneko	yes	stopped	Ph1:AES/SHA1/2 Ph2:AES/SHA1/none	main N/I	192.168.10.1	10.0.10.0 255.255.255.0	172.29.8.4	Edit	Delete	Connect	Wait

* Reducing the MTU size on the client side, can help eliminate some connectivity problems occuring 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

Figure 102 – IPSec start/stop page for GWG Gateway 1

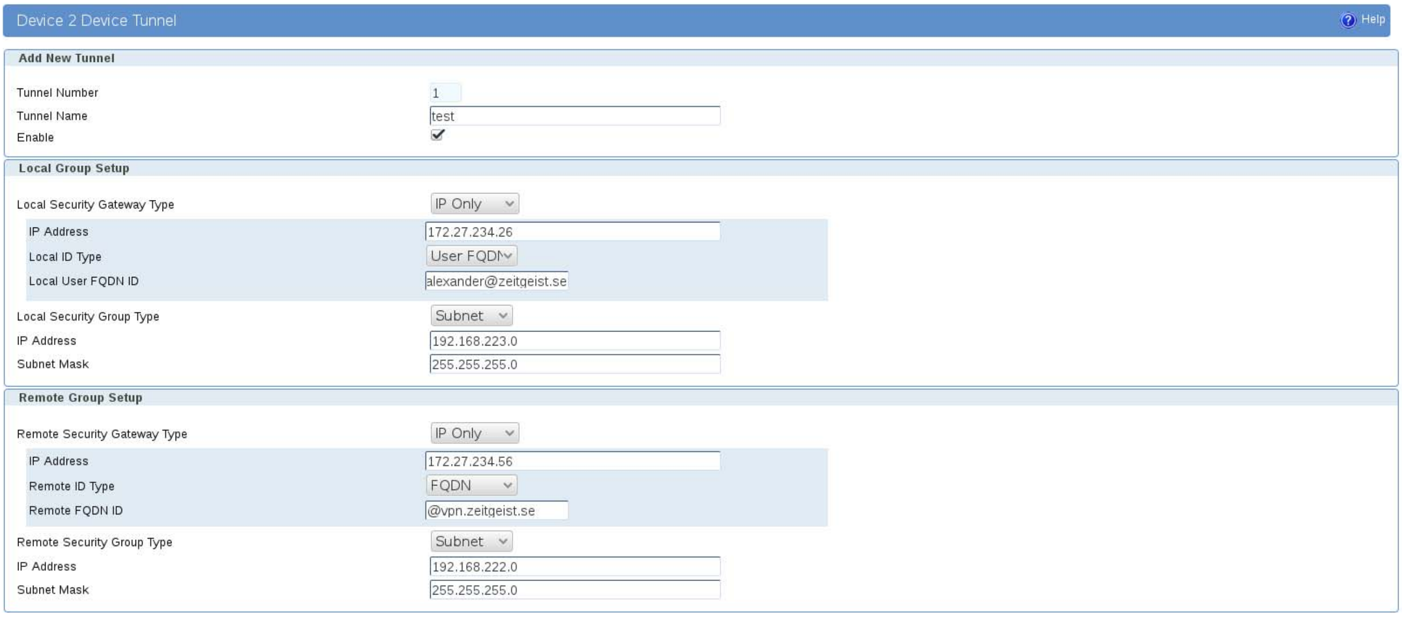
Click ***Start*** button and after that ***Wait*** button on ***Internet Protocol Security*** page to initiate IPSEC tunnel.

- On the device connected on GWG Gateway 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,
        - Key File: ipsecNEW.ipsec,
        - CA Certificate: strongswanCert.pem,
        - Local Client Certificate: AlexanderCert.pem,
        - Local Client Key: AlexanderKey.pem
    - ***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

Add New Tunnel

Tunnel Number	1
Tunnel Name	test
Enable	☑

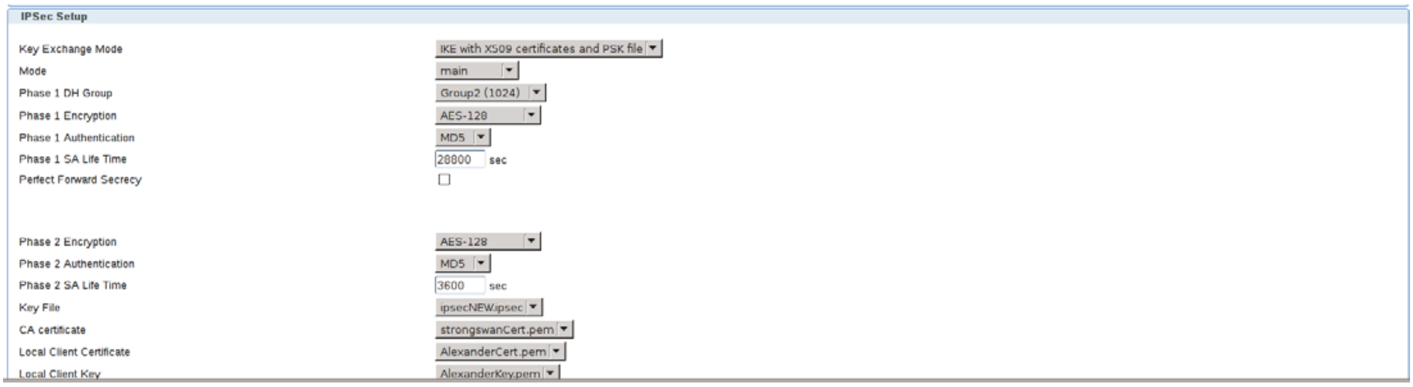
Local Group Setup

Local Security Gateway Type	IP Only
IP Address	172.27.234.26
Local ID Type	User FQDN
Local User FQDN ID	alexander@zeitgeist.se
Local Security Group Type	Subnet
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
Remote Security Group Type	Subnet
IP Address	192.168.222.0
Subnet Mask	255.255.255.0

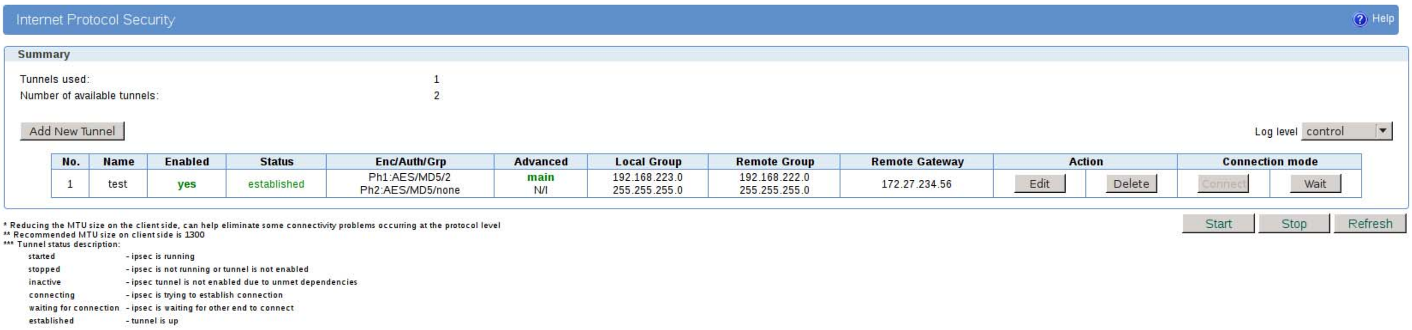
Figure 103 – IPSEC configuration page I for GWG Gateway 1



IPSec Setup

Key Exchange Mode	IKE with X509 certificates and PSK file
Mode	main
Phase 1 DH Group	Group2 (1024)
Phase 1 Encryption	AES-128
Phase 1 Authentication	MD5
Phase 1 SA Life Time	28800 sec
Perfect Forward Secrecy	□
Phase 2 Encryption	AES-128
Phase 2 Authentication	MD5
Phase 2 SA Life Time	3600 sec
Key File	ipsecNEW.ipsec
CA certificate	strongswanCert.pem
Local Client Certificate	AlexanderCert.pem
Local Client Key	AlexanderKey.pem

Figure 104 – IPSEC configuration page II for GWG Gateway 1



Internet Protocol Security

Summary

Tunnels used:	1
Number of available tunnels:	2

Log level control

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 N/I	192.168.223.0 255.255.255.0	192.168.222.0 255.255.255.0	172.27.234.56	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

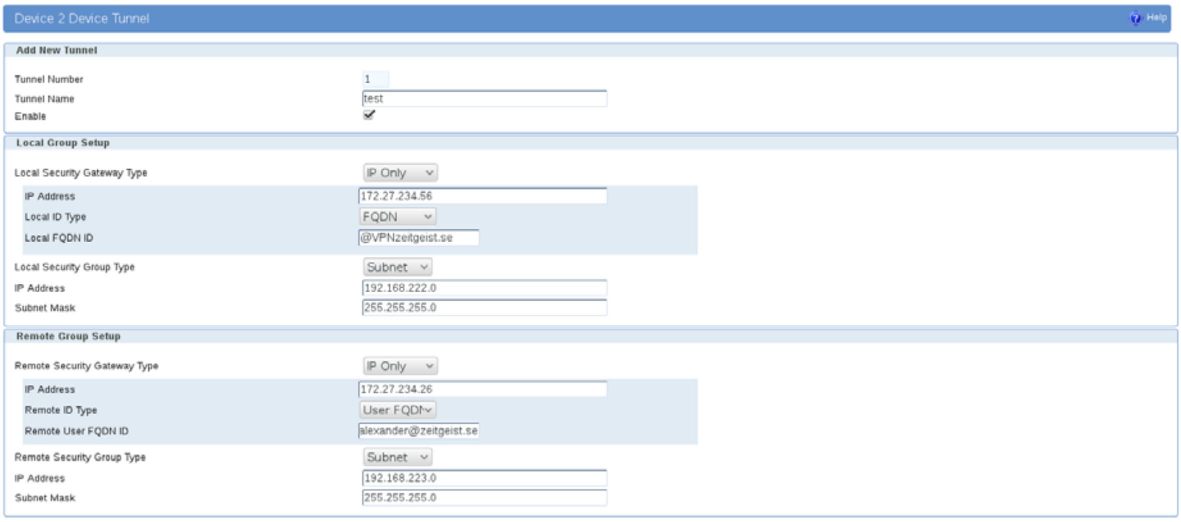
Figure 105 – IPSec start/stop page for GWG Gateway 1

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
        - Key File: ipsecNEW.ipsec
        - CA Certificate: strongswanCert.pem
        - Local Client Certificate: vpnHostCert.pem
        - Local Client Key: vpnHostKey.pem
    - ***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



Add New Tunnel

Tunnel Number	1
Tunnel Name	test
Enable	✓

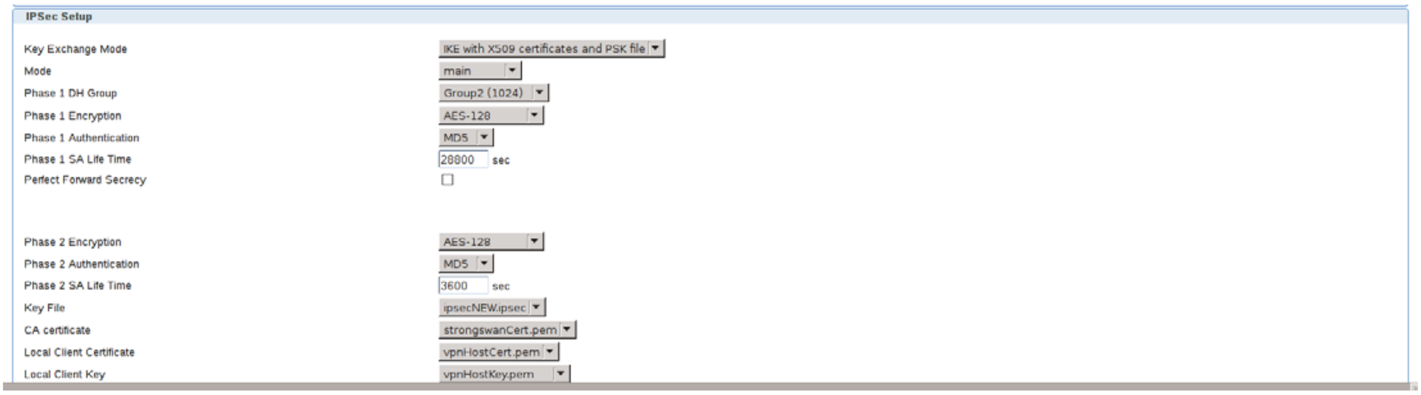
Local Group Setup

Local Security Gateway Type	IP Only
IP Address	172.27.234.56
Local ID Type	FQDN
Local FQDN ID	@VPNzeitgeist.se
Local Security Group Type	Subnet
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
Remote Security Group Type	Subnet
IP Address	192.168.223.0
Subnet Mask	255.255.255.0

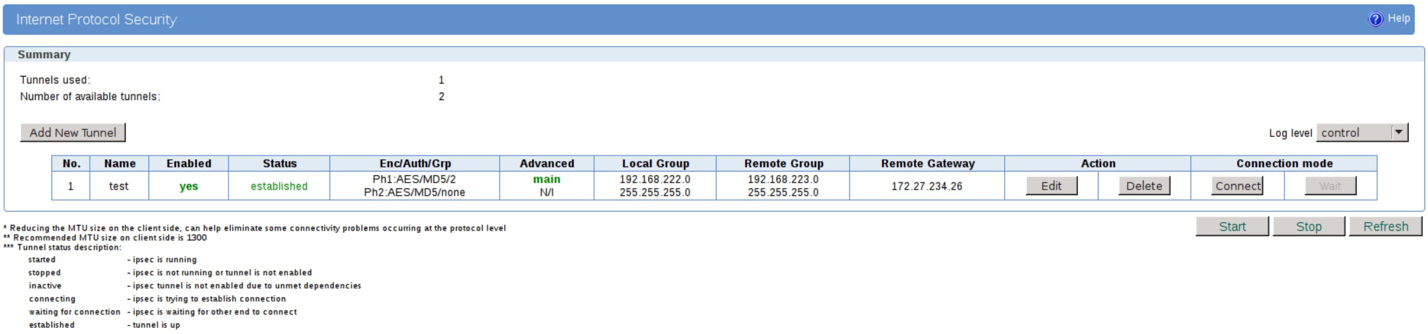
Figure 106 – IPSEC configuration page I for GWG Gateway 2



IPSec Setup

Key Exchange Mode	IKE with X509 certificates and PSK file
Mode	main
Phase 1 DH Group	Group2 (1024)
Phase 1 Encryption	AES-128
Phase 1 Authentication	MD5
Phase 1 SA Life Time	28800 sec
Perfect Forward Secrecy	□
Phase 2 Encryption	AES-128
Phase 2 Authentication	MD5
Phase 2 SA Life Time	3600 sec
Key File	ipsecNEW.ipsec
CA certificate	strongswanCert.pem
Local Client Certificate	vpnHostCert.pem
Local Client Key	vpnHostKey.pem

Figure 107 – IPSEC configuration page II for GWG Gateway 2



Internet Protocol Security

Summary

Tunnels used: 1

Number of available tunnels: 2

Log level control

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 N/I	192.168.222.0 255.255.255.0	192.168.223.0 255.255.255.0	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
```

Figure 108 – 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 GWG Gateway and Cisco Router

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

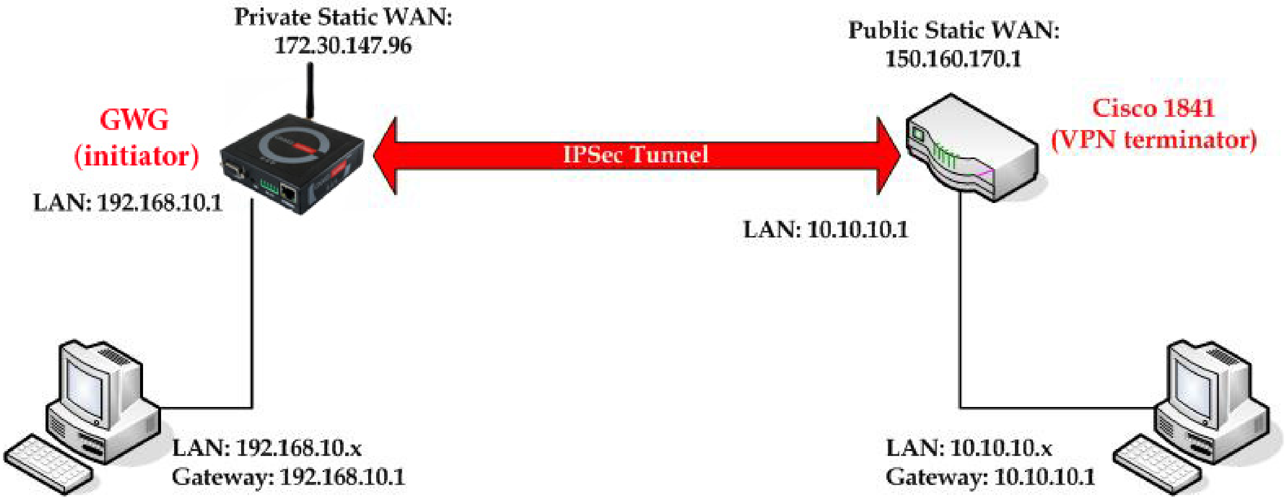


Figure 109 – IPSec tunnel between GWG Gateway and Cisco Router

The GWG Gateways requirements:

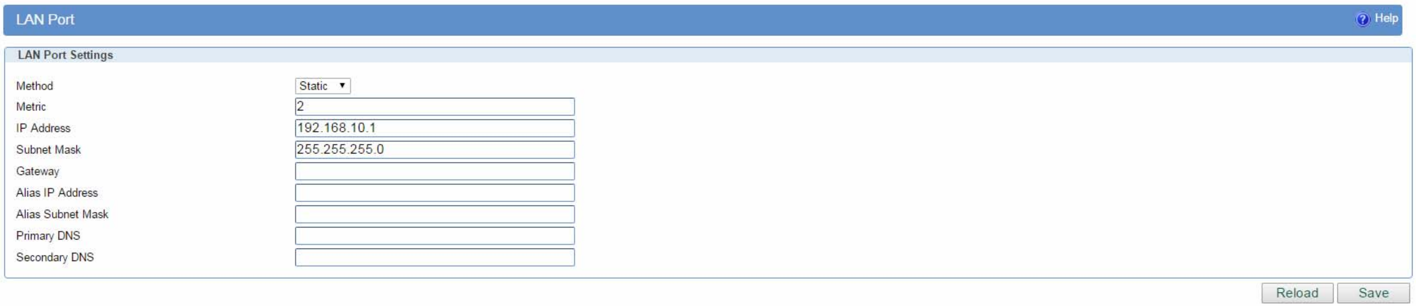
- Static IP WAN address for tunnel source and tunnel destination address
- Dynamic IP WAN address must be mapped to hostname with DynDNS service (for synchronization with DynDNS server SIM card must have internet access).

GSM/UMTS APN Type: For GSM/UMTS networks GWG Gateway 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 GWG Gateway 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.



LAN Port Settings

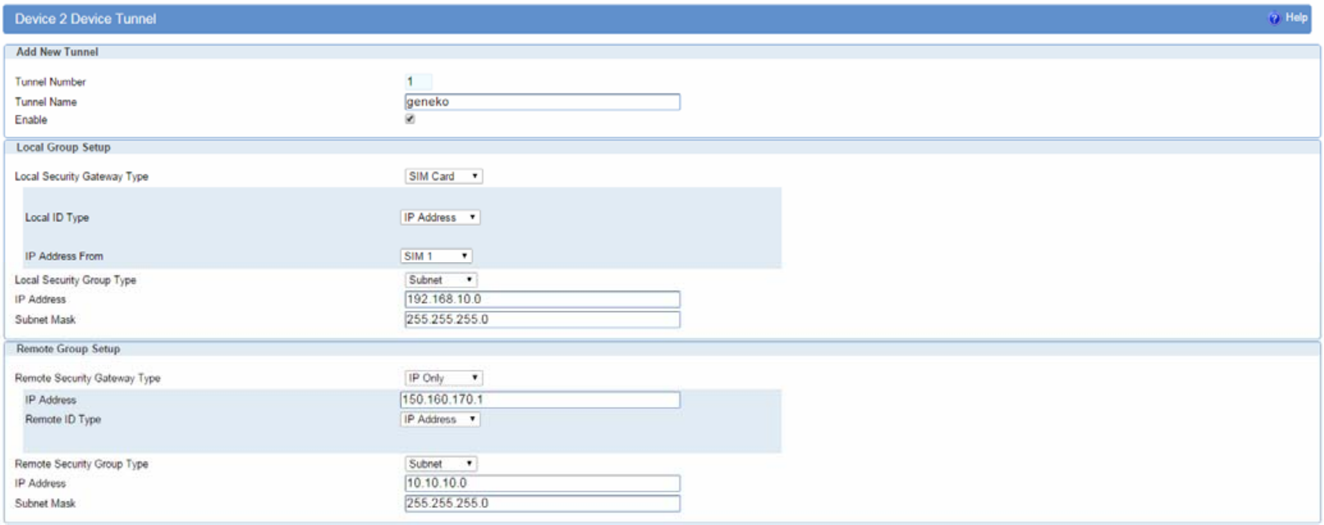
Method	Static ▾
Metric	2
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
Gateway	
Alias IP Address	
Alias Subnet Mask	
Primary DNS	
Secondary DNS	

Figure 110 –LAN Port configuration page for GWG Gateway

- Click *Mobile Settings* Tab to configure parameters necessary for GSM/UMTS/LTE connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS/LTE connection (*Mobile 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: IPsec tunnel,
  - Enable: true.
- *Local Group Setup*
  - Local Security Gateway Type: SIM card,
  - Local ID Type: IP Address,
  - IP Address From: SIM 1 (WAN connection is established over SIM 1),
  - 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.
- *IPSec Setup*

  - Keying Mode: IKE with Preshared key,
  - Mode: aggressive,
  - Phase 1 DH group: Group 2,
  - Phase 1 Encryption: 3DES,
  - Phase 1 Authentication: SHA1,
  - Phase 1 SA Life Time: 28800,
  - Phase 2 Encryption: 3DES,
  - Phase 2 Authentication: SHA1,
  - Phase 2 SA Life Time: 3600,
  - Preshared Key: 1234567890.
- ***Failover***
  - Enable Tunnel Failover: false.
- ***Advanced***
  - 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.



Add New Tunnel

Tunnel Number	1
Tunnel Name	geneko
Enable	☑

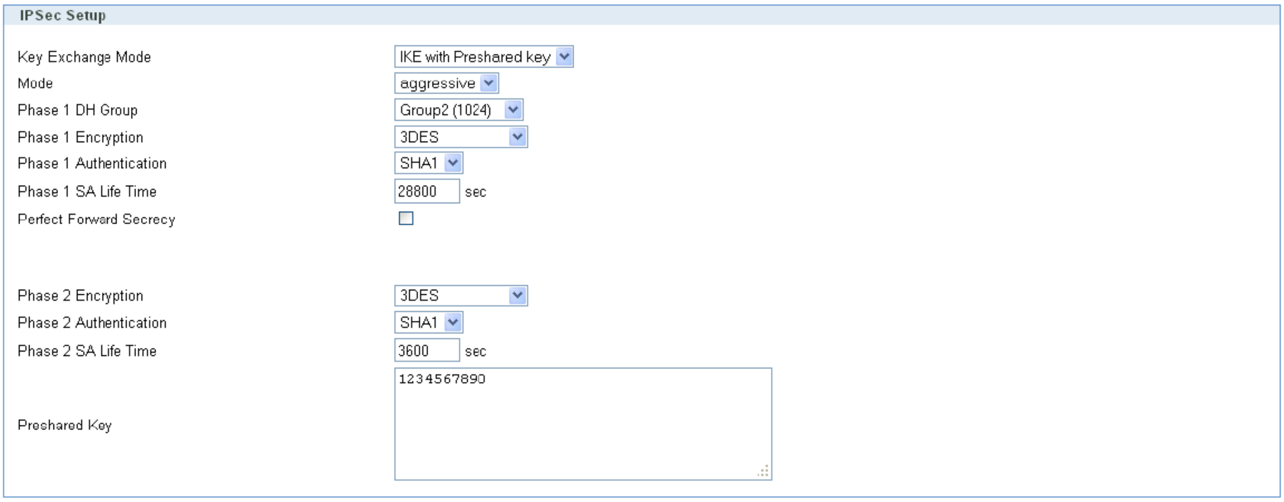
Local Group Setup

Local Security Gateway Type	SIM Card
Local ID Type	IP Address
IP Address From	SIM 1
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

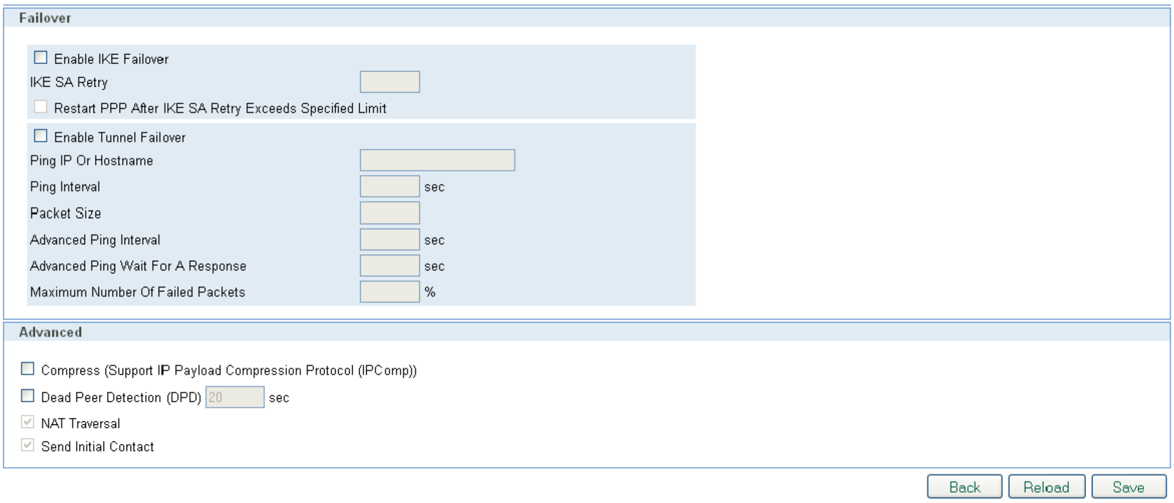
Figure 111 – IPSEC configuration page I for GWG Gateway



IPSec Setup

Key Exchange Mode	IKE with Preshared key
Mode	aggressive
Phase 1 DH Group	Group2 (1024)
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 112 – IPSec configuration page II for GWG Gateway



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

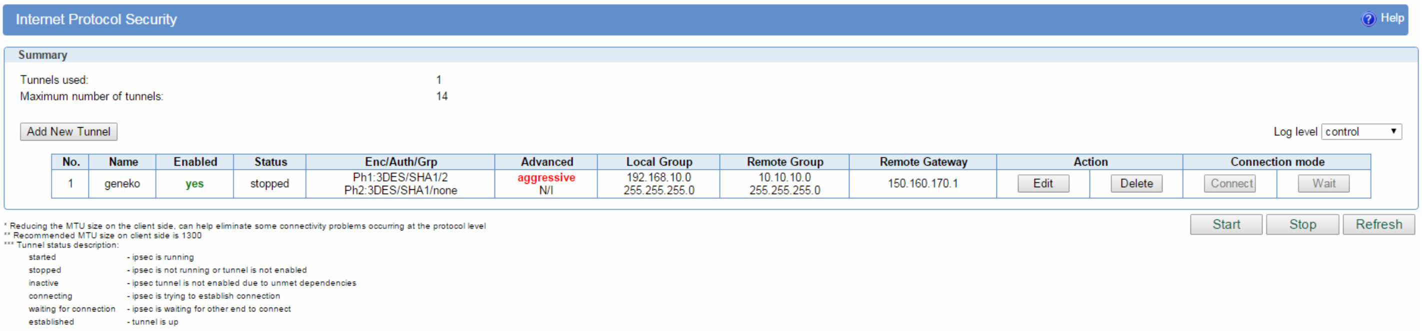
☑ NAT Traversal

☑ Send Initial Contact

Figure 113 – IPSec configuration page III for GWG Gateway

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

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



Internet Protocol Security

Summary

Tunnels used: 1

Maximum number of tunnels: 14

Log level control

No.	Name	Enabled	Status	Enc/Auth/Grp	Advanced	Local Group	Remote Group	Remote Gateway	Action		Connection mode	
1	geneko	yes	stopped	Ph1:3DES/SHA1/2 Ph2:3DES/SHA1/none	aggressive N/I	192.168.10.0 255.255.255.0	10.10.10.0 255.255.255.0	150.160.170.1	Edit	Delete	Connect	Wait

* Reducing the MTU size on the client side, can help eliminate some connectivity problems occuring 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

Figure 114 - IPSec start/stop page for GWG Gateway

- On the device connected on GWG Gateway 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  testGWG  esp-3des esp-sha-hmac
!
!--- Instances of the dynamic crypto map
!--- reference previous IPsec profile.
!
crypto dynamic-map dynGWG 5
 set transform-set testGWG
 set isakmp-profile L2L
 match address 121
!
!--- Crypto-map only references instances of the previous dynamic crypto map.
!
crypto map GWG 10 ipsec-isakmp dynamic dynGWG
!
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 GWG
!
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
access-list 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 GWG Gateway and Juniper SSG firewall

IPSec tunnel is a type of a VPN tunnels with a secure tunneling method. On the diagram below *Figure 87* is illustrated simple network with GWG Gateway and Cisco Router. Idea is to create IPSec tunnel for LAN to LAN (site to site) connectivity.

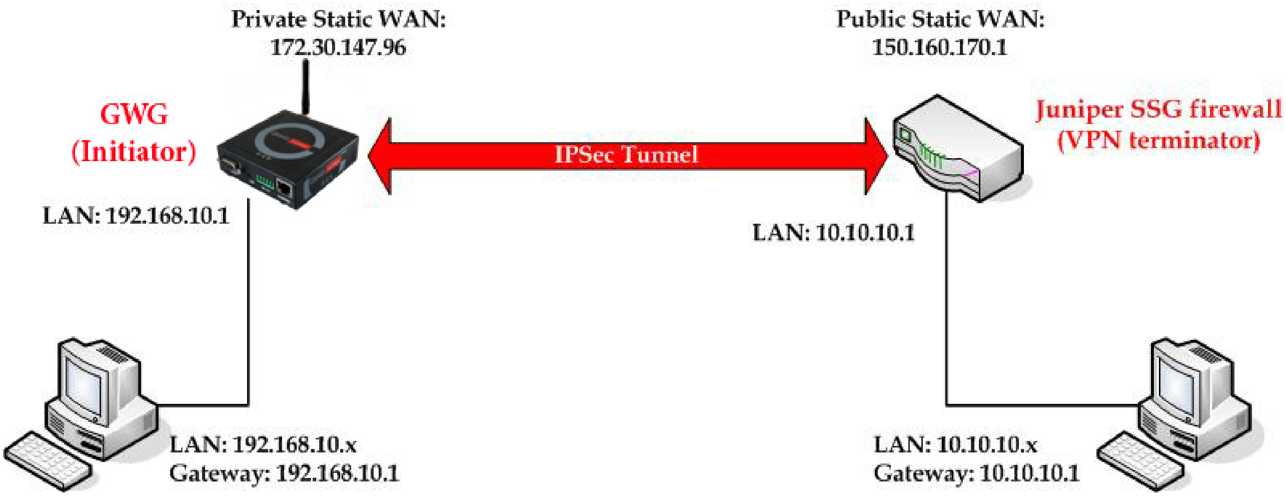


Figure 115 – IPSec tunnel between GWG Gateway and Juniper SSG

The GWG Gateway requirements:

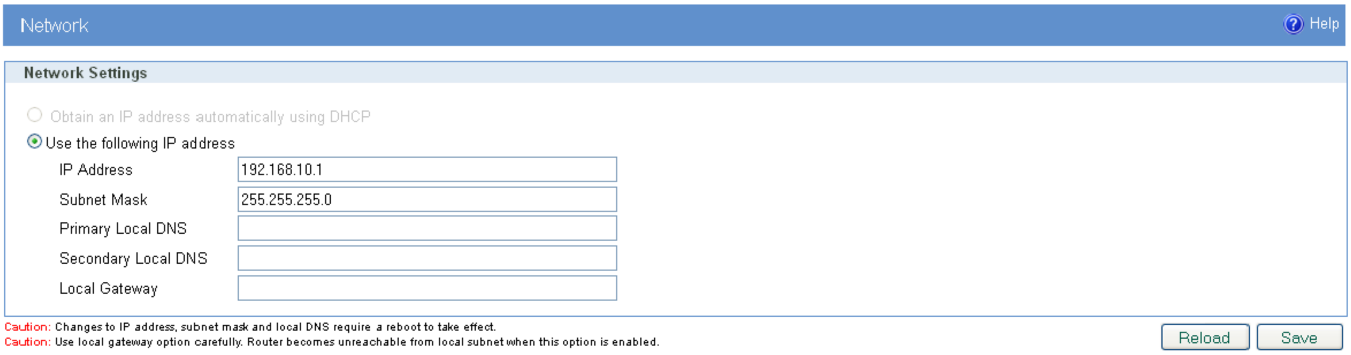
- Static IP WAN address for tunnel source and tunnel destination address,
- Source tunnel address should have static WAN IP address,
- Source tunnel address should have static WAN IP address,
- Destination tunnel address should have static WAN IP address.

GSM/UMTS APN Type: For GSM/UMTS networks GWG Gateway 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 GWG Gateway 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

Network Settings

○ Obtain an IP address automatically using DHCP
● Use the following IP address

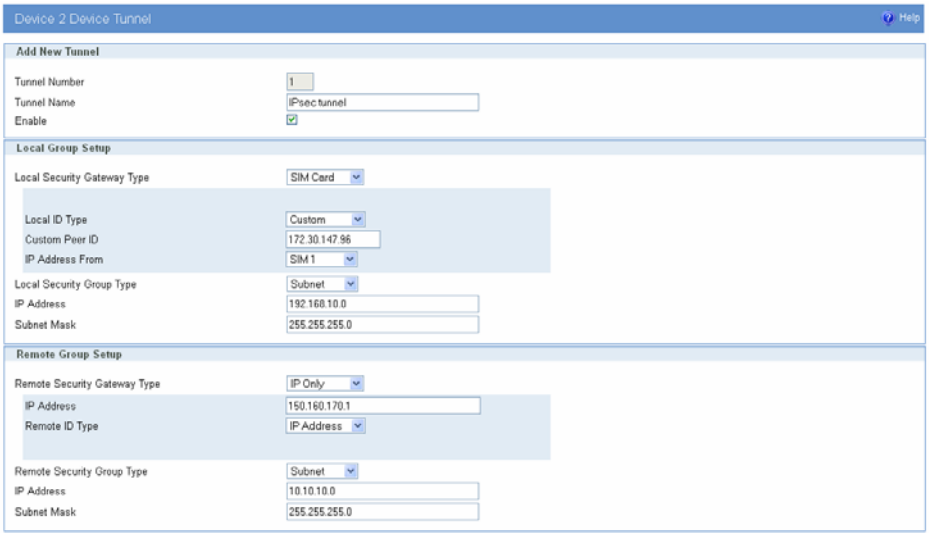
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
Primary Local DNS	
Secondary Local DNS	
Local Gateway	

Caution: Changes to IP address, subnet mask and local DNS require a reboot to take effect.
Caution: Use local gateway option carefully. Router becomes unreachable from local subnet when this option is enabled.

Figure 116 – Network configuration page for GWG Gateway

- Use SIM card with a static IP address, obtained from Mobile Operator.
- Click ***WAN Settings Tab*** to configure parameters necessary for GSM/UMTS/LTE connection. All parameters necessary for connection configuration should be required from mobile operator.
- Check the status of GSM/UMTS/LTE 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: IPsec tunnel,
    - Enable: true.
  - ***IPSec Setup***
    - Keying Mode: IKE with Preshared key,
    - Mode: aggressive,
    - 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.
  - ***Local Group Setup***
    - Local Security Gateway Type: IP Only,
    - Local ID Type: Custom,
    - Custom Peer ID: 172.30.147.96,
    - IP Address: SIM 1,
    - 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.
- *Advanced*
  - Compress(Support IP Payload Compression Protocol(IPComp)): false,
  - Dead Peer Detection(DPD): false,
  - NAT Traversal: true,
  - Press *Save* to accept the changes.



Add New Tunnel

Tunnel Number	1
Tunnel Name	IPsec tunnel
Enable	☑

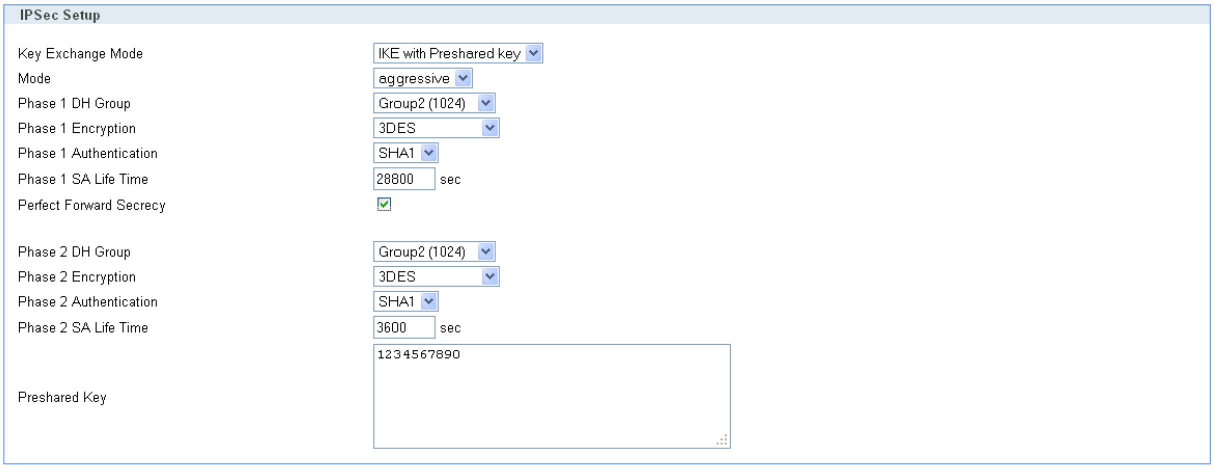
Local Group Setup

Local Security Gateway Type	SIM Card
Local ID Type	Custom
Custom Peer ID	172.30.147.96
IP Address From	SIM 1
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

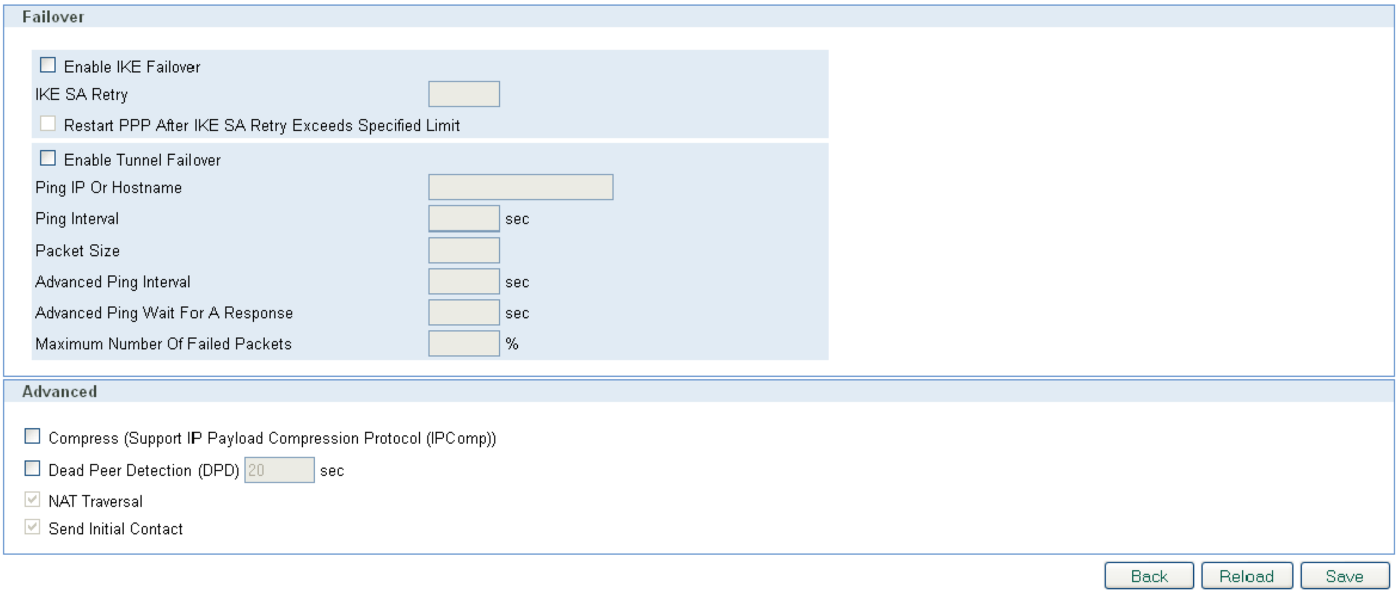
Figure 117 – IPSEC configuration page I for GWG Gateway



IPSec Setup

Key Exchange Mode	IKE with Preshared key
Mode	aggressive
Phase 1 DH Group	Group2 (1024)
Phase 1 Encryption	3DES
Phase 1 Authentication	SHA1
Phase 1 SA Life Time	28800 sec
Perfect Forward Secrecy	☑
Phase 2 DH Group	Group2 (1024)
Phase 2 Encryption	3DES
Phase 2 Authentication	SHA1
Phase 2 SA Life Time	3600 sec
Preshared Key	1234567890

Figure 118 – IPSec configuration page II for GWG Gateway



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

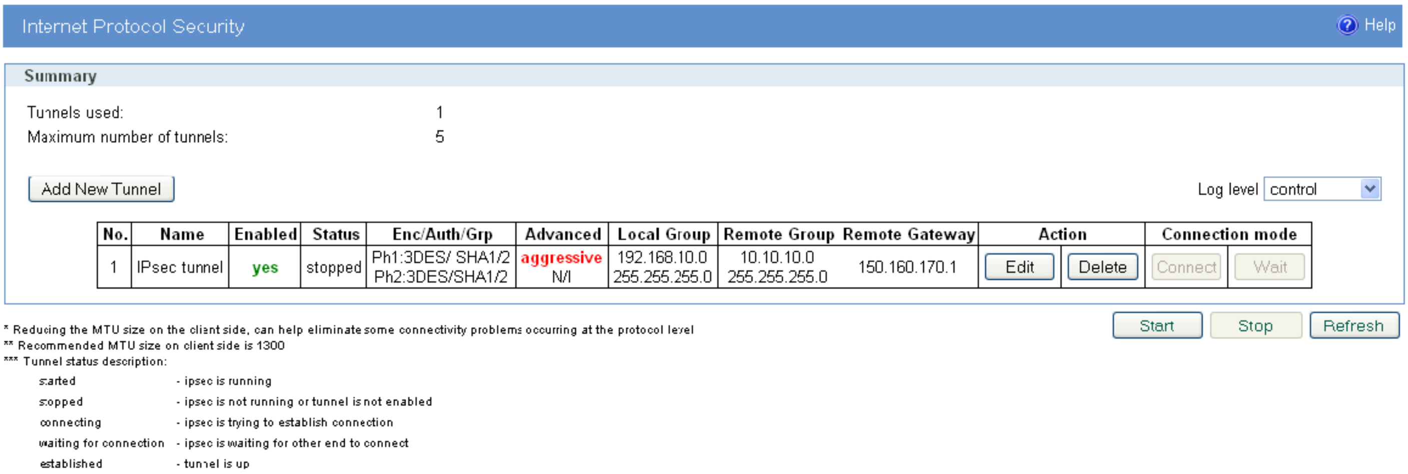
☑ NAT Traversal

☑ Send Initial Contact

Figure 119 – IPSec configuration page III for GWG Gateway

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

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



Internet Protocol Security

Summary

Tunnels used: 1

Maximum number of tunnels: 5

Log level control

No.	Name	Enabled	Status	Enc/Auth/Grp	Advanced	Local Group	Remote Group	Remote Gateway	Action		Connection mode	
1	IPsec tunnel	yes	stopped	Ph1:3DES/ SHA1/2 Ph2:3DES/SHA1/2	aggressive N/I	192.168.10.0 255.255.255.0	10.10.10.0 255.255.255.0	150.160.170.1	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

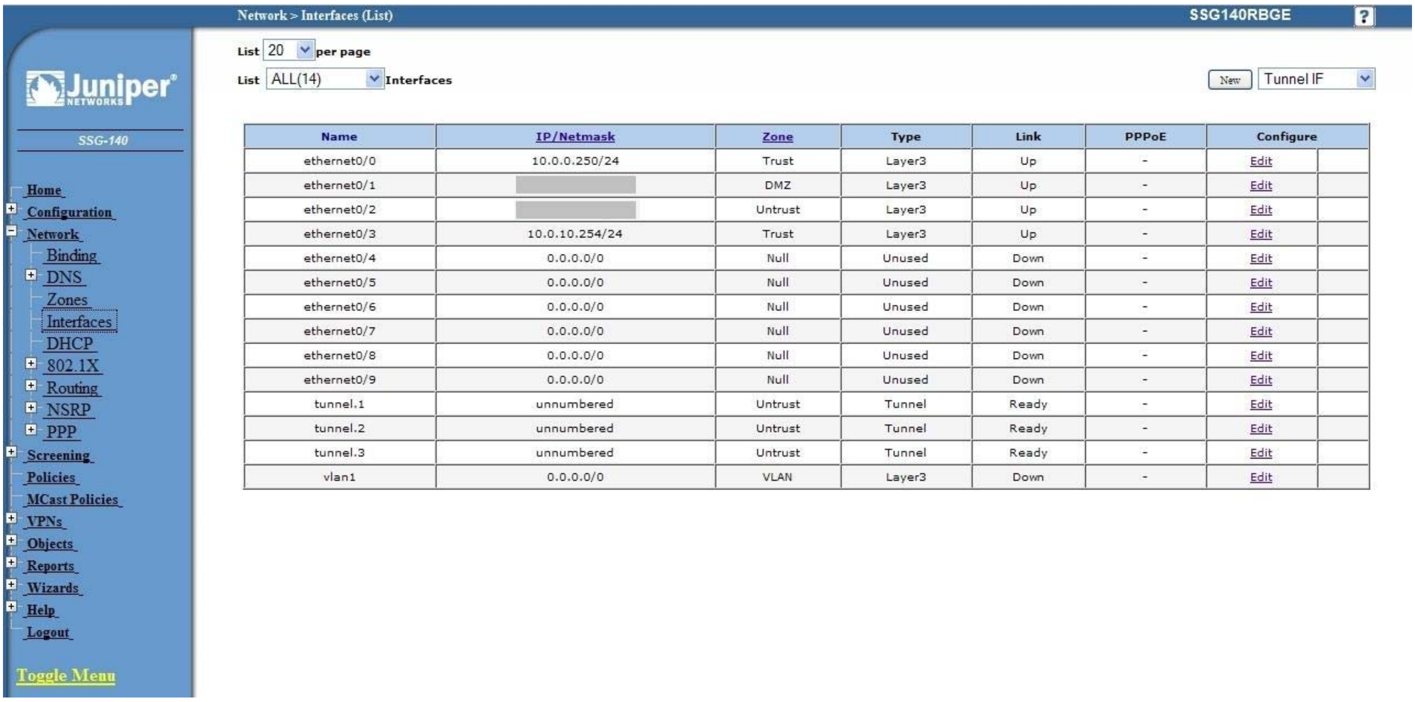
Figure 120 - IPSec start/stop page for GWG Gateway

On the device connected on GWG gateway setup default gateway 192.168.10.1.

The Juniper SSG firewall configuration:

Step1 – Create New Tunnel Interface

- Click Interfaces on Network Tab.



Network > Interfaces (List) SSG140RBGE

List 20 per page

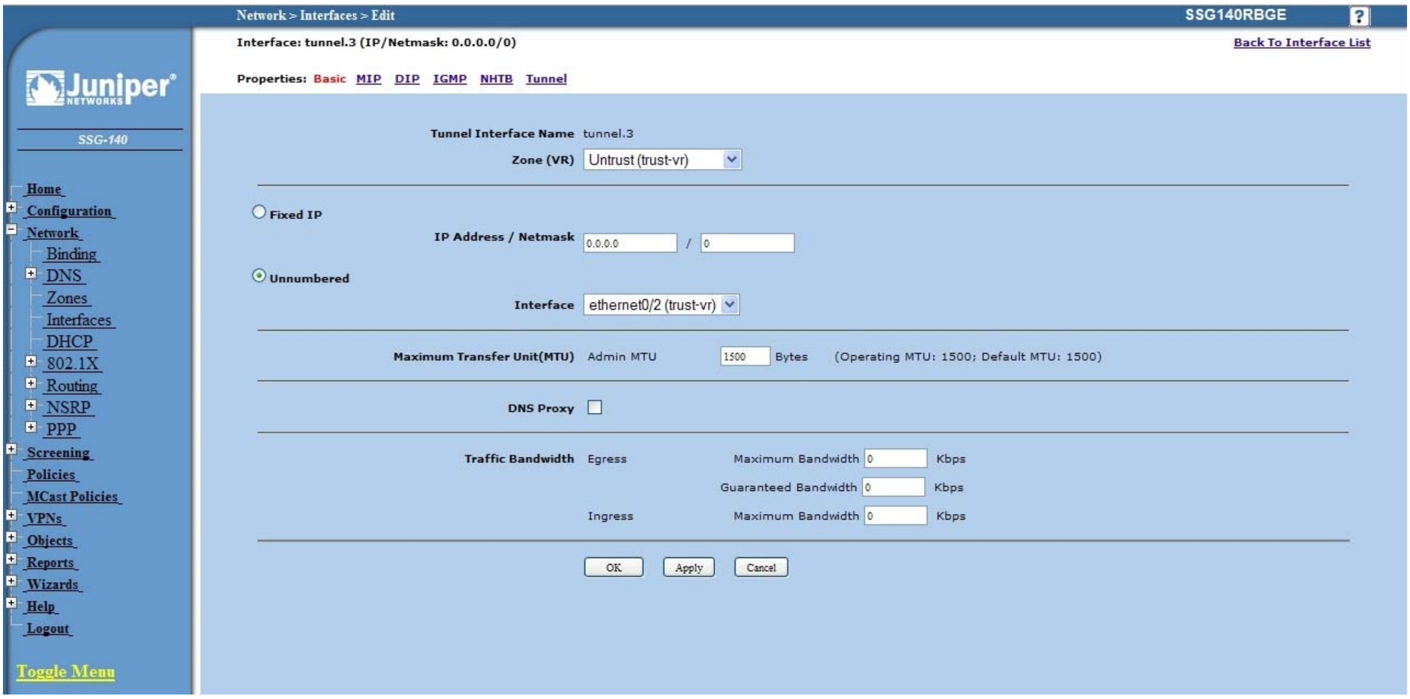
List ALL(14) Interfaces

New Tunnel IF

Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure
ethernet0/0	10.0.0.250/24	Trust	Layer3	Up	-	Edit
ethernet0/1	[redacted]	DMZ	Layer3	Up	-	Edit
ethernet0/2	[redacted]	Untrust	Layer3	Up	-	Edit
ethernet0/3	10.0.10.254/24	Trust	Layer3	Up	-	Edit
ethernet0/4	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet0/5	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet0/6	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet0/7	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet0/8	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet0/9	0.0.0.0/0	Null	Unused	Down	-	Edit
tunnel.1	unnumbered	Untrust	Tunnel	Ready	-	Edit
tunnel.2	unnumbered	Untrust	Tunnel	Ready	-	Edit
tunnel.3	unnumbered	Untrust	Tunnel	Ready	-	Edit
vlan1	0.0.0.0/0	VLAN	Layer3	Down	-	Edit

Figure 121 – Network Interfaces (list)

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



Network > Interfaces > Edit SSG140RBGE

Interface: tunnel.3 (IP/Netmask: 0.0.0.0/0) Back To Interface List

Properties: Basic MIP DIP IGMP NHTB Tunnel

Tunnel Interface Name tunnel.3

Zone (VR) Untrust (trust-vr)

○ Fixed IP

IP Address / Netmask 0.0.0.0 / 0

● Unnumbered

Interface ethernet0/2 (trust-vr)

Maximum Transfer Unit(MTU) Admin MTU 1500 Bytes (Operating MTU: 1500; Default MTU: 1500)

DNS Proxy □

Traffic Bandwidth Egress Maximum Bandwidth 0 Kbps

Guaranteed Bandwidth 0 Kbps

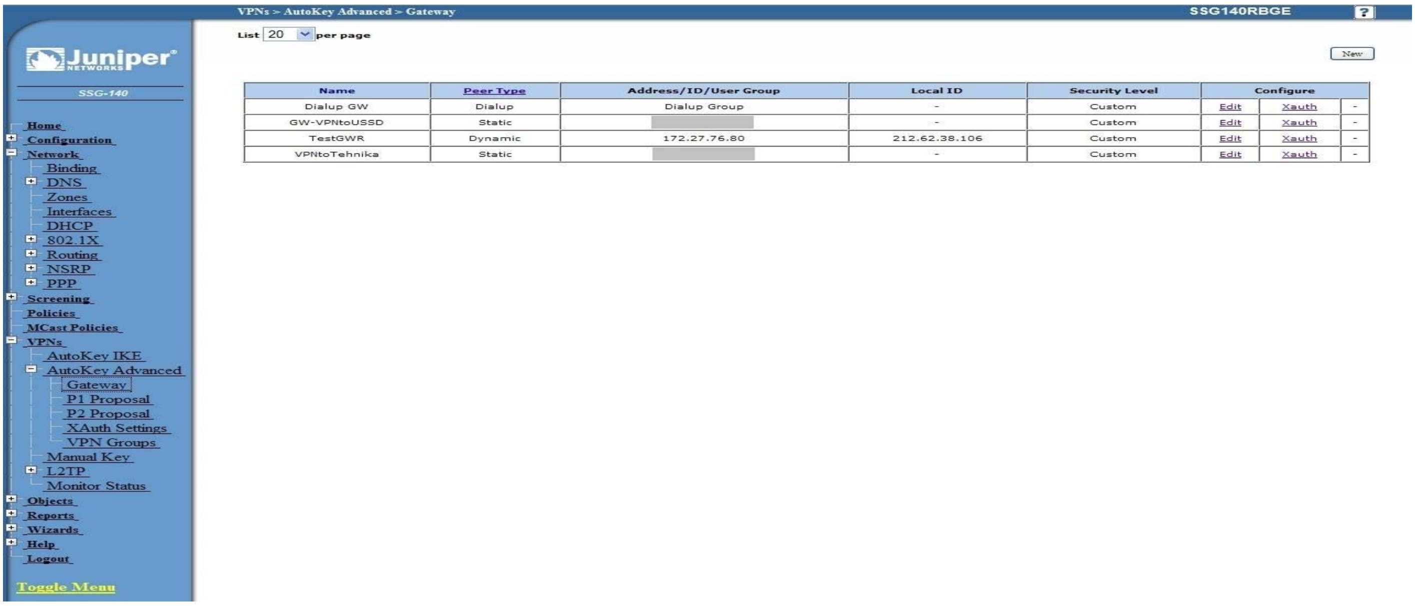
Ingress Maximum Bandwidth 0 Kbps

OK Apply Cancel

Figure 122 – 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.



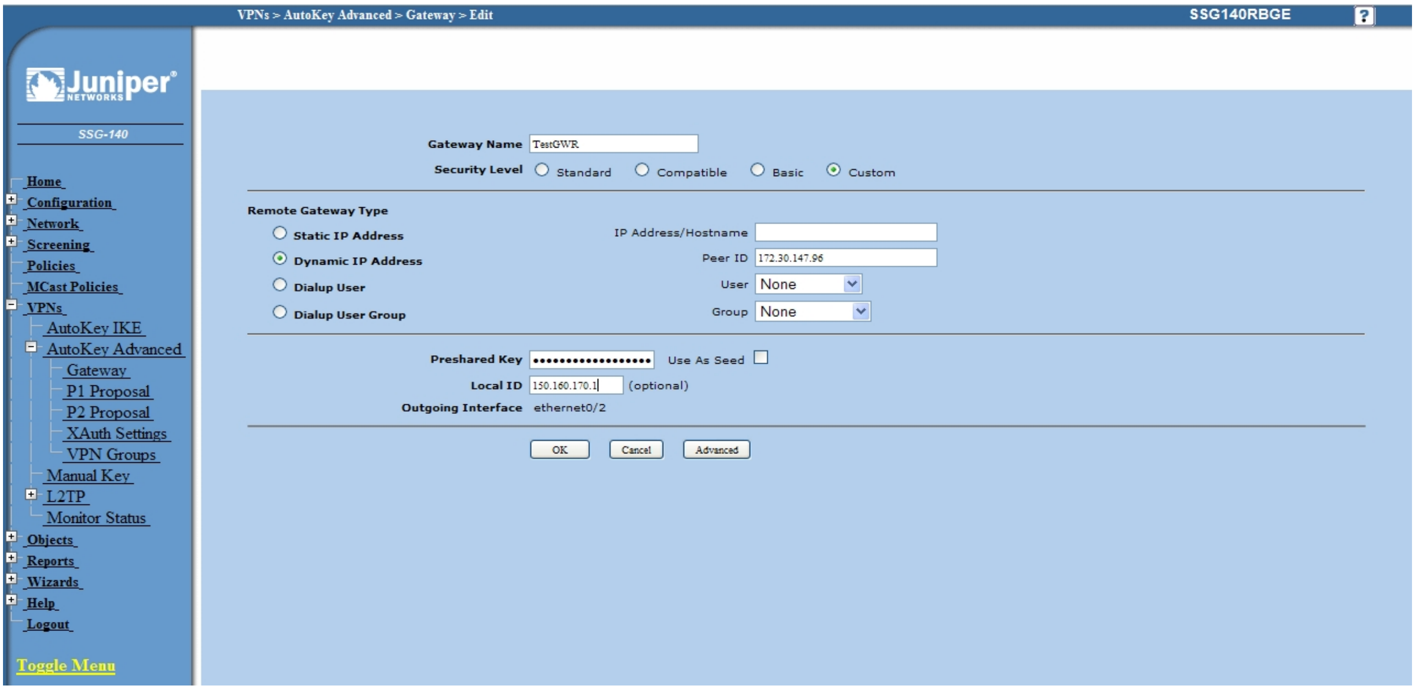
VPNs > AutoKey Advanced > Gateway

List 20 per page

Name	Peer Type	Address/ID/User Group	Local ID	Security Level	Configure		
Dialup GW	Dialup	Dialup Group	-	Custom	Edit	Xauth	-
GW-VPNtoUSSD	Static	[redacted]	-	Custom	Edit	Xauth	-
TestGWR	Dynamic	172.27.76.80	212.62.38.106	Custom	Edit	Xauth	-
VPNtoTehnika	Static	[redacted]	-	Custom	Edit	Xauth	-

Figure 123 – AutoKey Advanced Gateway

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



VPNs > AutoKey Advanced > Gateway > Edit

Gateway Name TestGWR

Security Level ○ Standard ○ Compatible ○ Basic ● Custom

Remote Gateway Type

○ Static IP Address — IP Address/Hostname

● Dynamic IP Address — Peer ID 172.30.147.96

○ Dialup User — User None

○ Dialup User Group — Group None

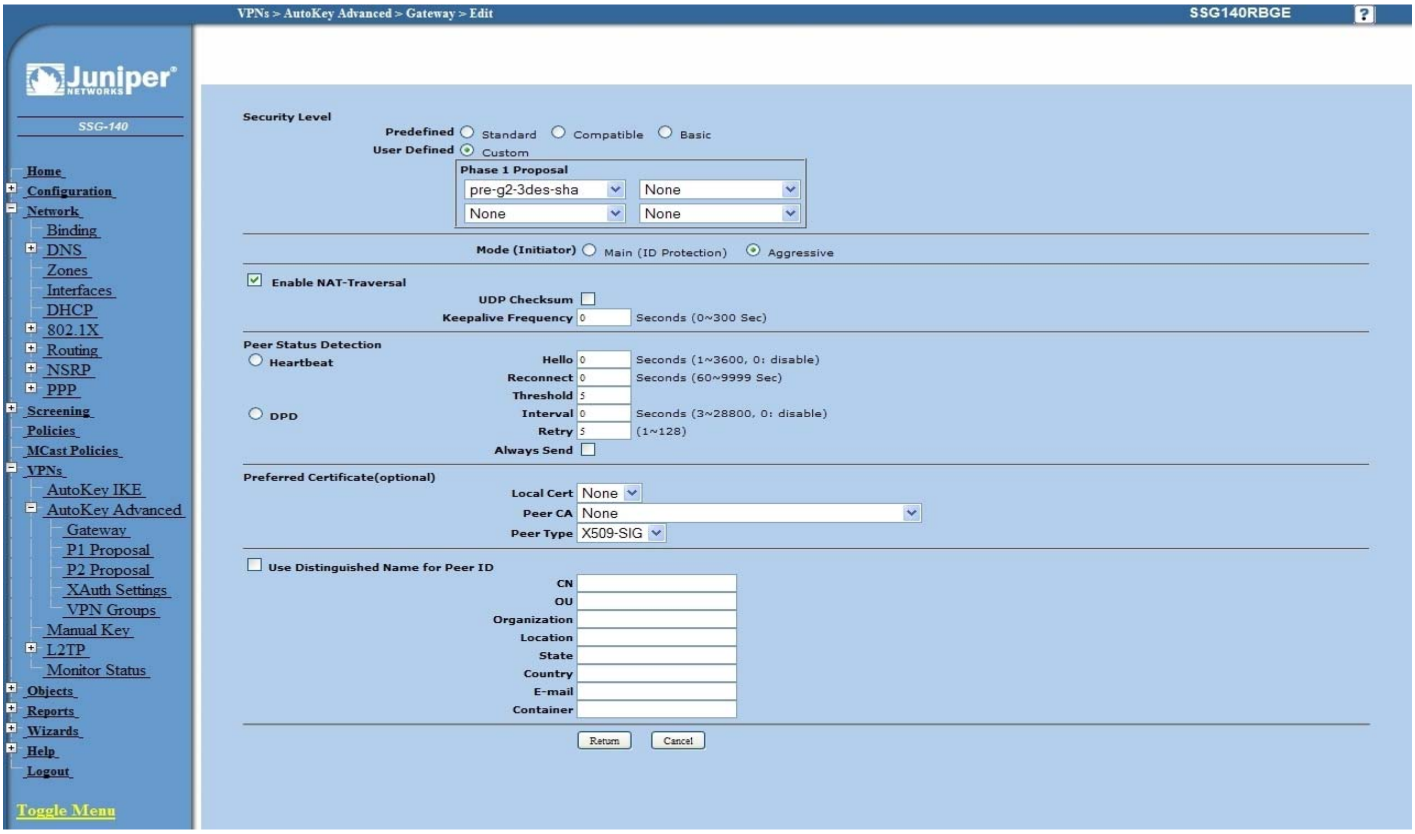
Preshared Key •••••••••••••••••• Use As Seed □

Local ID 150.160.170.1 (optional)

Outgoing Interface ethernet0/2

Figure 124 – Gateway parameters

- Click *Advanced* button.
  - **Security level – User Defined:** custom,
  - **Phase 1 proposal:** pre–g2–3des–sha,
  - **Mode:** Agressive(must be aggressive because of NAT),
  - **Nat–Traversal:** enabled,
  - Click *Return* and *OK*.



Security Level
Predefined ○ Standard ○ Compatible ○ Basic
User Defined ● Custom

Phase 1 Proposal
pre-g2-3des-sha | None
None | None

Mode (Initiator) ○ Main (ID Protection) ● Aggressive

☑ Enable NAT-Traversal
UDP Checksum □
Keepalive Frequency 0 Seconds (0~300 Sec)

Peer Status Detection
○ Heartbeat
Hello 0 Seconds (1~3600, 0: disable)
Reconnect 0 Seconds (60~9999 Sec)
Threshold 5
○ DPD
Interval 0 Seconds (3~28800, 0: disable)
Retry 5 (1~128)
Always Send □

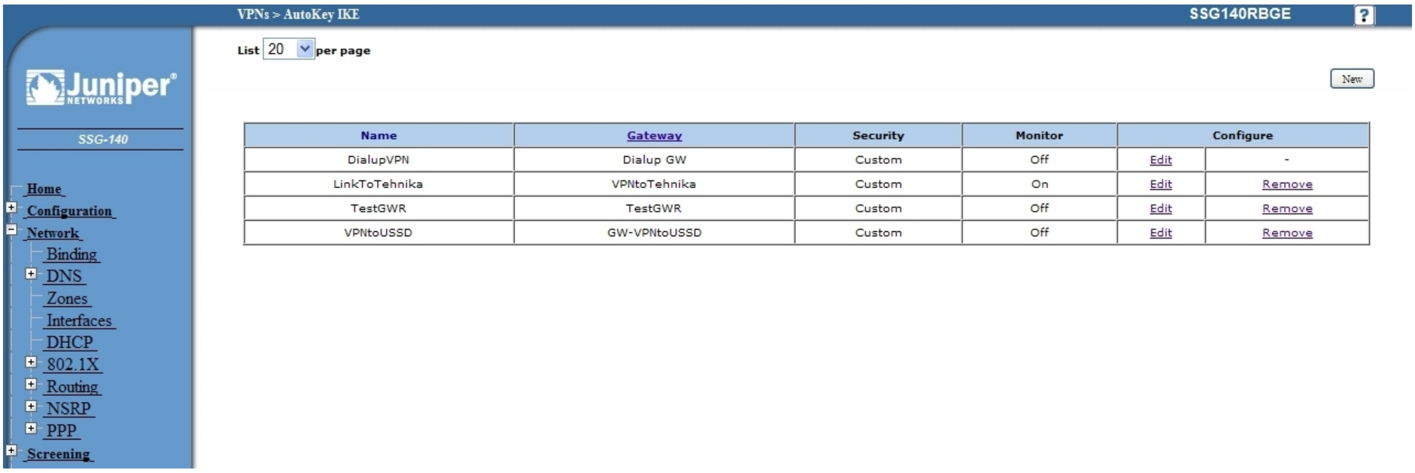
Preferred Certificate(optional)
Local Cert None
Peer CA None
Peer Type X509-SIG

□ Use Distinguished Name for Peer ID
CN
OU
Organization
Location
State
Country
E-mail
Container

Figure 125 – Gateway advanced parameters

Step 3 – Create AutoKey IKE

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



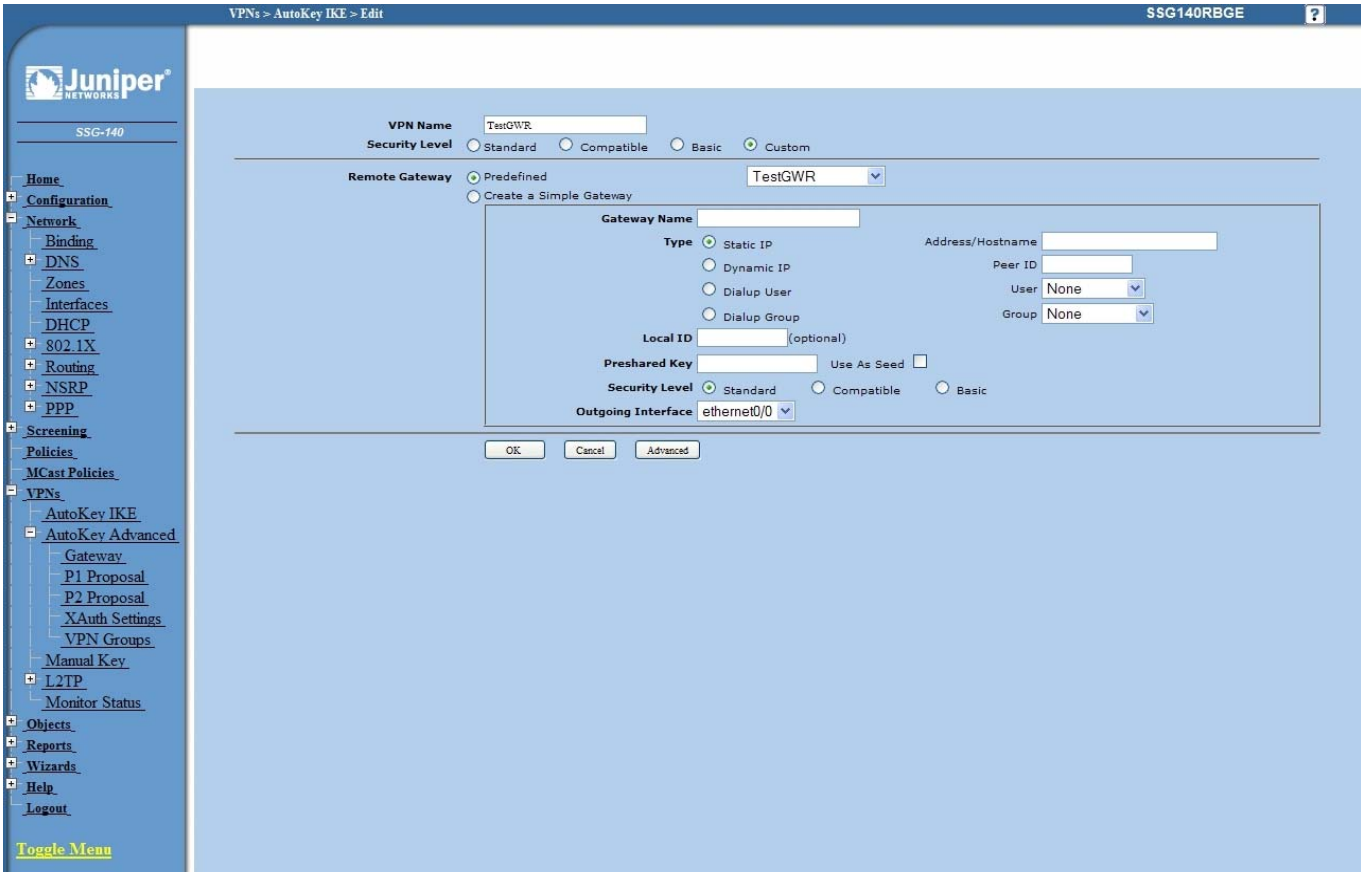
List 20 per page

Name	Gateway	Security	Monitor	Configure	
DialupVPN	Dialup GW	Custom	Off	Edit	-
LinkToTehnika	VPNtoTehnika	Custom	On	Edit	Remove
TestGWR	TestGWR	Custom	Off	Edit	Remove
VPNtoUSSD	GW-VPNtoUSSD	Custom	Off	Edit	Remove

Figure 126 – AutoKey IKE

AutoKey IKE parameters are:

- **VPNname:** TestGWG,
- **Security level:** Custom,
- **Remote Gateway:** Predefined,
- Choose VPN Gateway from step 2.



VPN Name: TestGWR

Security Level: ○ Standard ○ Compatible ○ Basic ● Custom

Remote Gateway: ● Predefined TestGWR

○ Create a Simple Gateway

Gateway Name:

Type: ● Static IP ○ Dynamic IP ○ Dialup User ○ Dialup Group

Address/Hostname:

Peer ID:

User: None

Group: None

Local ID: (optional)

Preshared Key: Use As Seed □

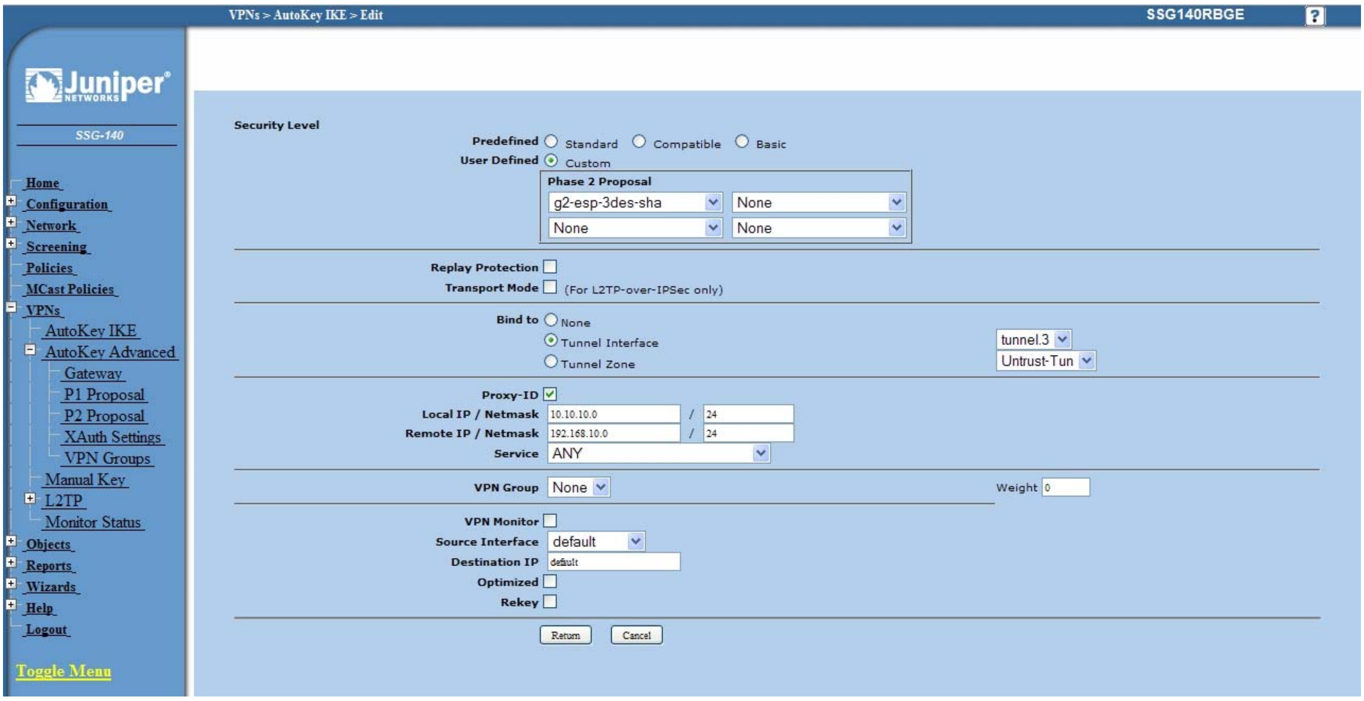
Security Level: ● Standard ○ Compatible ○ Basic

Outgoing Interface: ethernet0/0

OK Cancel Advanced

Figure 127 – 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*.

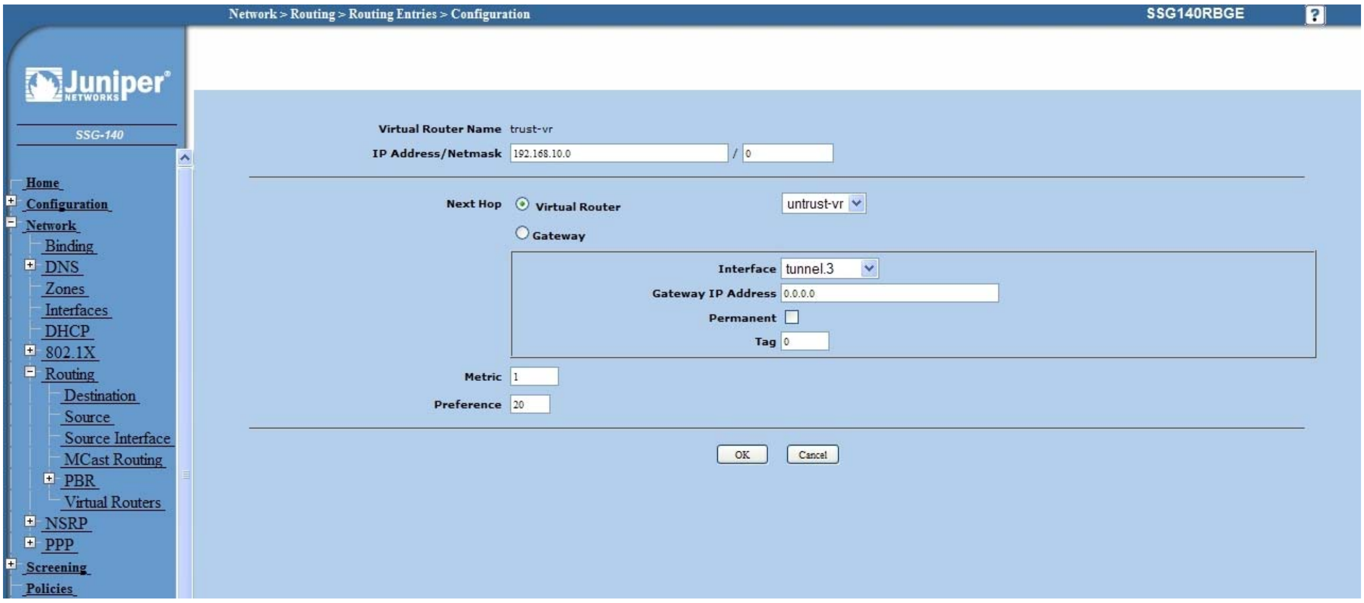


Security Level
Predefined ○ Standard ○ Compatible ○ Basic
User Defined ● Custom
Phase 2 Proposal
g2-esp-3des-sha | None
None | None
Replay Protection □
Transport Mode □ (For L2TP-over-IPSec only)
Bind to ○ None
● Tunnel Interface tunnel.3
○ Tunnel Zone Untrust-Tun
Proxy-ID ☑
Local IP / Netmask 10.10.10.0 / 24
Remote IP / Netmask 192.168.10.0 / 24
Service ANY
VPN Group None Weight 0
VPN Monitor □
Source Interface default
Destination IP default
Optimized □
Rekey □

Figure 128 – 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.***

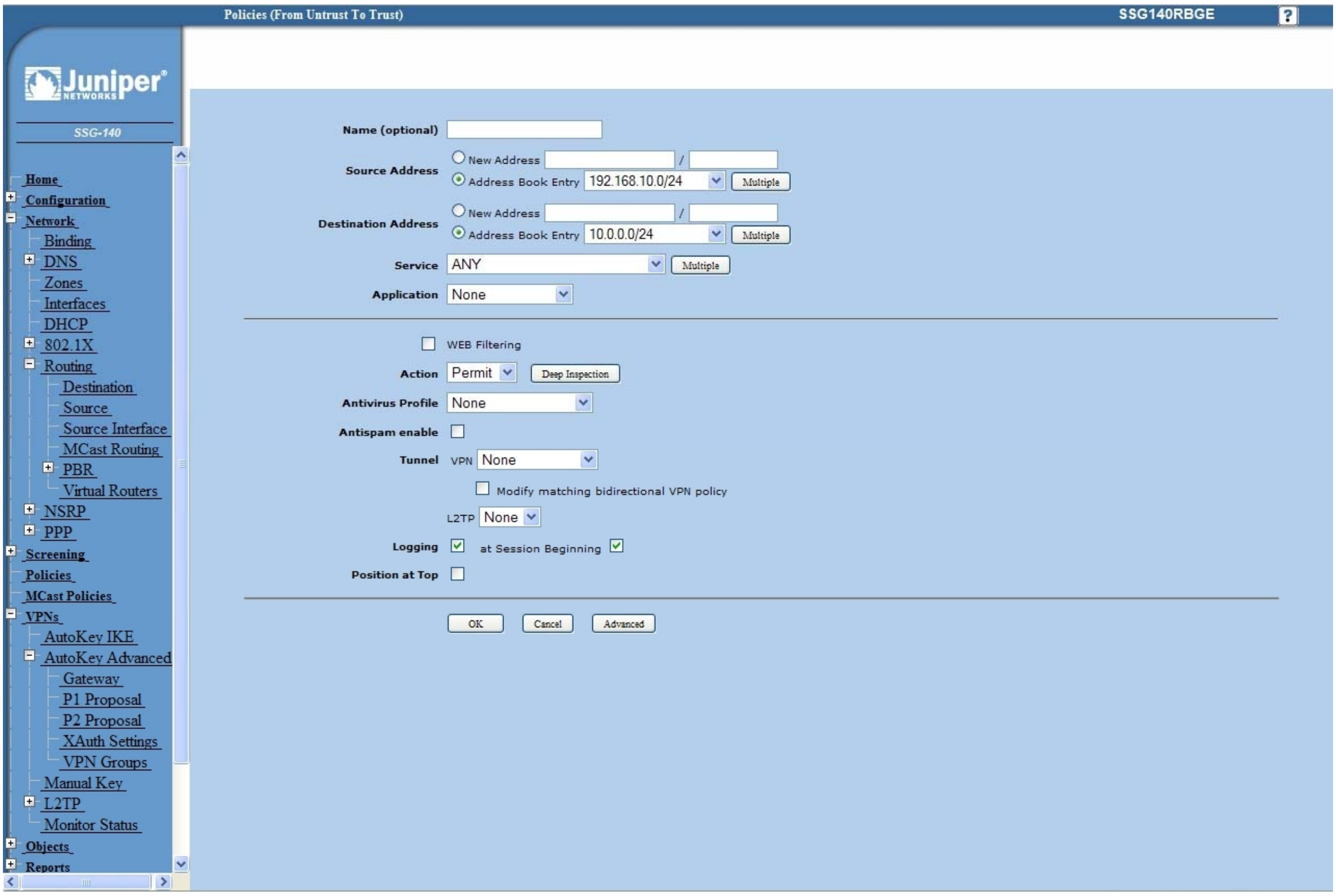


Virtual Router Name trust-vr
IP Address/Netmask 192.168.10.0 / 0
Next Hop ● Virtual Router untrust-vr
○ Gateway
Interface tunnel.3
Gateway IP Address 0.0.0.0
Permanent □
Tag 0
Metric 1
Preference 20

Figure 129 – 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.*



Policies (From Untrust To Trust) SSG140RBGE

Name (optional)

Source Address ○ New Address / ● Address Book Entry 192.168.10.0/24

Destination Address ○ New Address / ● Address Book Entry 10.0.0.0/24

Service ANY

Application None

□ WEB Filtering

Action Permit

Antivirus Profile None

Antispam enable □

Tunnel VPN None

□ Modify matching bidirectional VPN policy

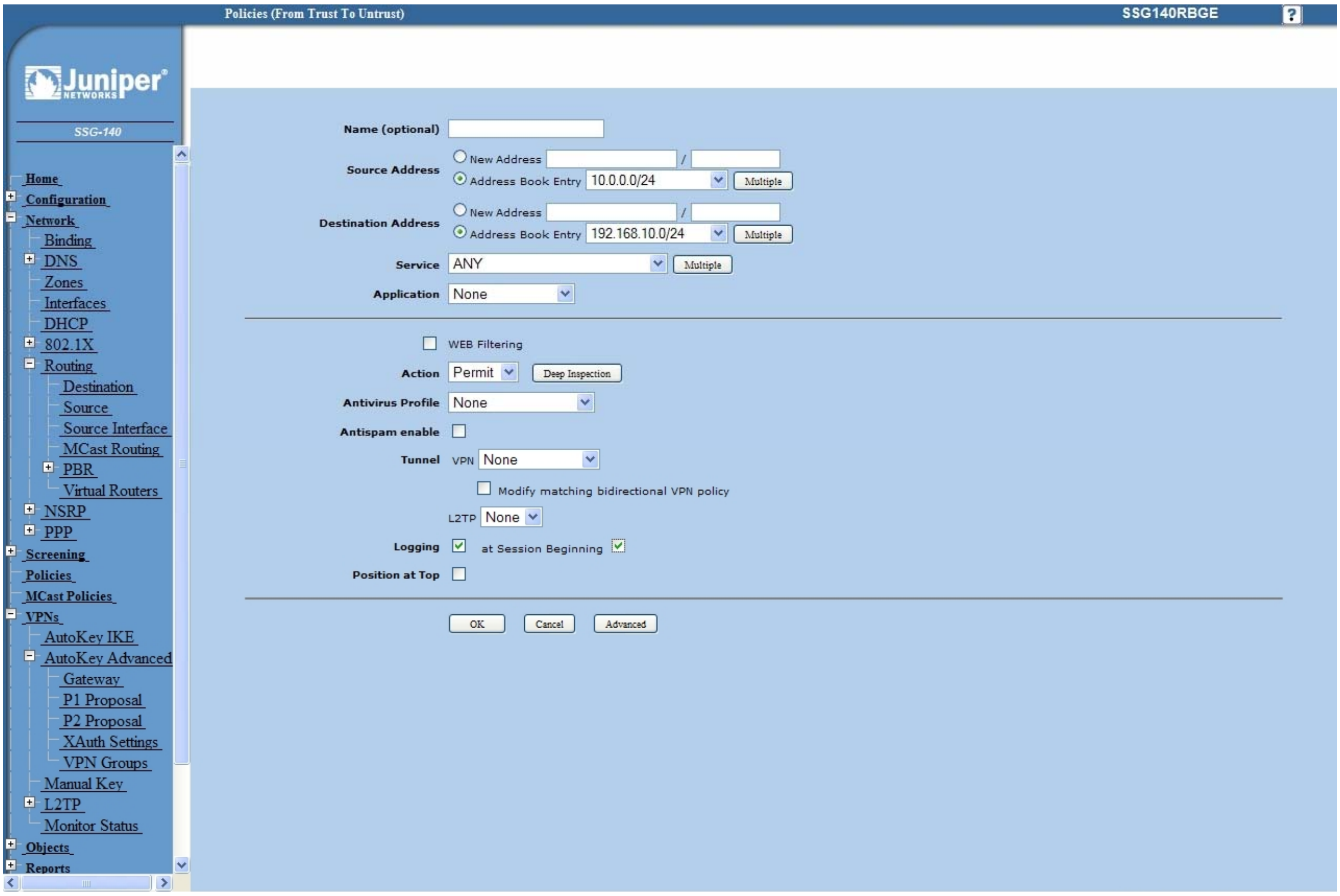
L2TP None

Logging ☑ at Session Beginning ☑

Position at Top □

Figure 130 – 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.*



Name (optional)

Source Address ○ New Address /
● Address Book Entry 10.0.0.0/24 Multiple

Destination Address ○ New Address /
● Address Book Entry 192.168.10.0/24 Multiple

Service ANY Multiple

Application None

□ WEB Filtering

Action Permit Deep Inspection

Antivirus Profile None

Antispam enable □

Tunnel VPN None

□ Modify matching bidirectional VPN policy

L2TP None

Logging ☑ at Session Beginning ☑

Position at Top □

OK Cancel Advanced

Figure 131 – Policies from trust to untrust zone

OpenVPN tunnel between GWG Gateway and OpenVNP server

Overview

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.

OpenVPN configuration example

Open VPN is established between one central locations and three remote locations with GWG Gateway configured in TCP client mode. Authentication used is pre-shared key.

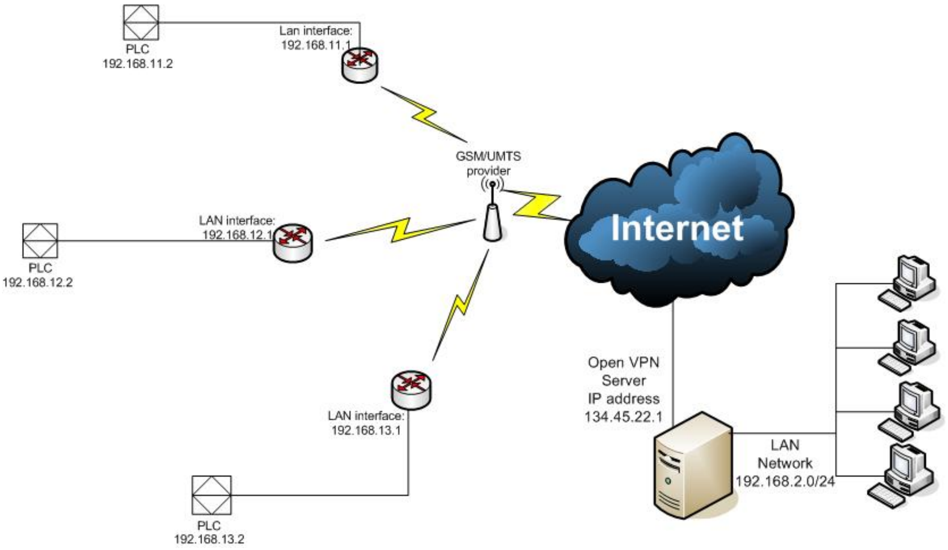


Figure 132 – Multipoint OpenVPN topology

Configuration

1. Open VPN server is in TCP listening mode and it is reachable from the internet over static public IP address 134.45.22.1 and TCP port 1194 (default Open VPN port)
2 Configuration file in Open VPN server is applied in following way:
   a) Open any Text Editor application and make configuration txt file.
   In this example configuration file looks like this

proto tcp-server	TCP server protocol mode
dev tun	dev tun mod of Open VPN server
ifconfig 2.2.2.1 2.2.2.2	Local and remote IP address of the Open VPN tunnel (both addresses must be within 255.255.255.252 subnet)
dev-node adap1	Selection of virtual network adapter named adap1
secret key.txt	Implementing file with pre-shared secret named key.txt
ping 10	Keepalive
comp-lzo	LZO compression enabled
disable-occ	disable option consistency

b) Save configuration file in C:\Program Files\OpenVPN\config as *name.*ovpn file.
It is OpenVPN configuration file directory and you can reach it directly through Start menu>OpenVPN where you get options:

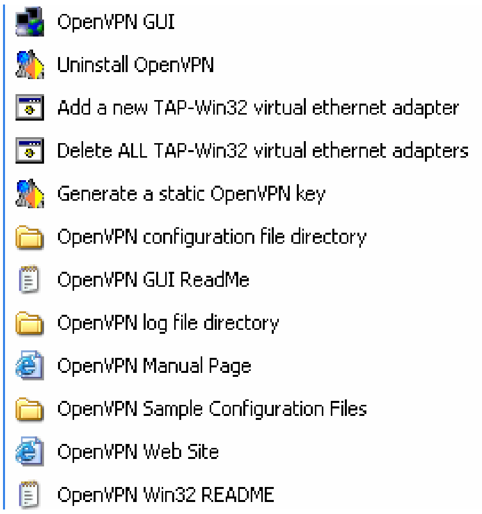

OpenVPN GUI
Uninstall OpenVPN
Add a new TAP-Win32 virtual ethernet adapter
Delete ALL TAP-Win32 virtual ethernet adapters
Generate a static OpenVPN key
OpenVPN configuration file directory
OpenVPN GUI ReadMe
OpenVPN log file directory
OpenVPN Manual Page
OpenVPN Sample Configuration Files
OpenVPN Web Site
OpenVPN Win32 README

Figure 133 – OpenVPN application settings

c) Generate a static OpenVPN key from the menu above. File will be automatically Saved in Open VPN configuration file directory. Configuration file and pre-shared key must be in same directory.

d) If you have more remote locations every location has to have its own configuration file with different remote interface IP address and virtual network adapter. Second virtual network adapter you can create by selecting "Add a new TAP-Win32 virtual ethernet adapter". The same way you can create the third virtual adapter . Name virtual adapters as adap1, adap2 and adap3 .

For example configuration file for second remote location can be:

```
proto tcp-server
dev tun
ifconfig 2.2.2.5 2.2.2.6
dev-node adap2
secret key.txt
ping 10
comp-lzo
disable-occ
```

Only difference to previous configuration is 2.2.2.5, 2.2.2.6
(IP address of local and remote interface) and dev-node adap2.

Configuration file for third remote location is:

```
proto tcp-server
dev tun
ifconfig 2.2.2.9 2.2.2.10
dev-node adap3
secret key.txt
ping 10
comp-lzo
disable-occ
```

All three configuration files (e.g. Server1.ovpn, Server2.ovpn, Server3.ovpn) have to be saved in same directory C:\Program Files\OpenVPN\config. Name of configuration file is name of your OpenVPN tunnel.

e) Workstation where OpenVPN server is installed should have ip route to subnet which is on the other end of the OpenVPN tunnel. This subnet is reachable over remote OpenVPN interface which is in this case 2.2.2.2.

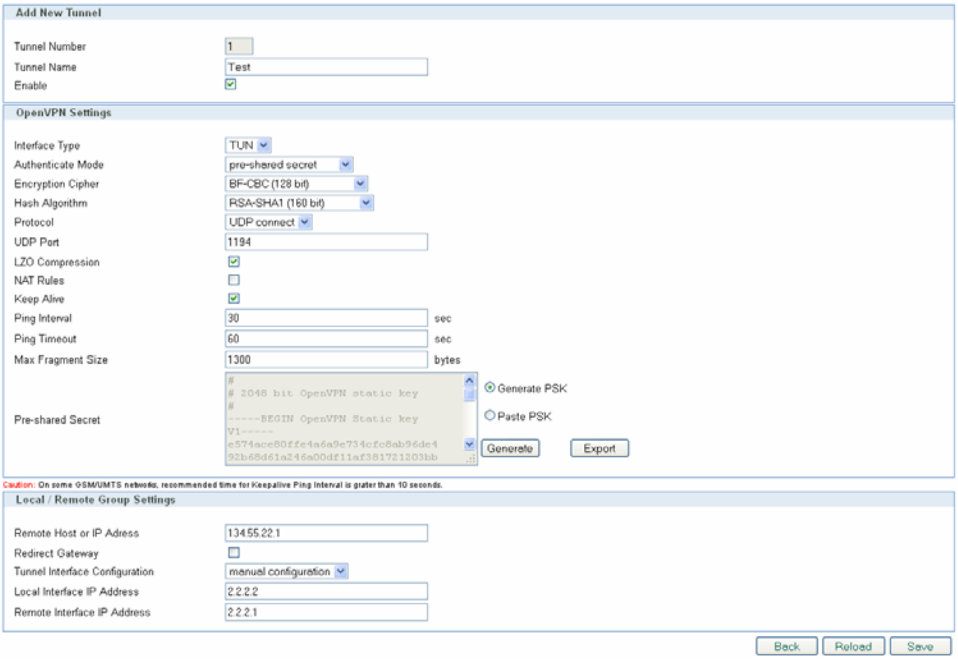
Enter following command in the command prompt:

route –p add 192.168.11.0 mask 255.255.255.0 2.2.2.2
first remote location

route –p add 192.168.12.0 mask 255.255.255.0 2.2.2.6
second remote location

route –p add 192.168.13.0 mask 255.255.255.0 2.2.2.10
third remote location

2. GWG gateway is configured with SIM card which has internet access. Configuration of OpenVPN is following:



Add New Tunnel

Tunnel Number	1
Tunnel Name	Test
Enable	☑

OpenVPN Settings

Interface Type	TUN
Authenticate Mode	pre-shared secret
Encryption Cipher	BF-CBC (128 bit)
Hash Algorithm	RSA-SHA1 (160 bit)
Protocol	UDP connect
UDP Port	1194
LZO Compression	☑
NAT Rules	□
Keep Alive	☑
Ping Interval	30 sec
Ping Timeout	60 sec
Max Fragment Size	1300 bytes
Pre-shared Secret	● Generate PSK ○ Paste PSK

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
e574ace80ffe4a6a9e734cfc8ab96de4
92b68d61a246a00df11af381721203bb
```

Caution: On some GSM/UMTS networks, recommended time for Keepalive Ping Interval is grater than 10 seconds.

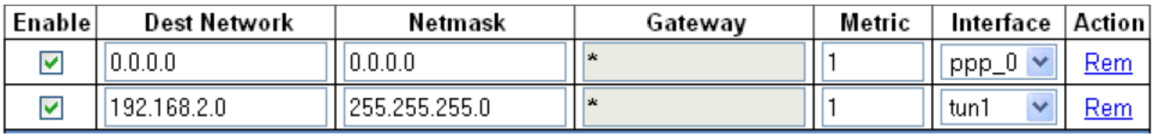
Local / Remote Group Settings

Remote Host or IP Adress	134.55.22.1
Redirect Gateway	□
Tunnel Interface Configuration	manual configuration
Local Interface IP Address	2.2.2.2
Remote Interface IP Address	2.2.2.1

Figure 134 – OpenVPN GWG settings

Where pre-shared secret you paste from the *key.txt* file which you generate on OpenVPN server.

In routing table static ip route to local OpenVPN server network (in this case it is 192.168.2.0/24) should be entered.



Enable	Dest Network	Netmask	Gateway	Metric	Interface	Action
☑	0.0.0.0	0.0.0.0	*	1	ppp_0	Rem
☑	192.168.2.0	255.255.255.0	*	1	tun1	Rem

Figure 135 – Static routes on GWG

TUN1 interface isn't available before you start the OpenVPN tunnel so you must start it first

That accomplishes configuration of the GWG regarding establishing the OpenVPN and routing through it.

Implementation

You start Open VPN tunnel on server side by right click on the icon in notification bar. You choose Open

VPN tunnel (Server1) and click Connect. The same procedure repeat for Server2 and Server3.

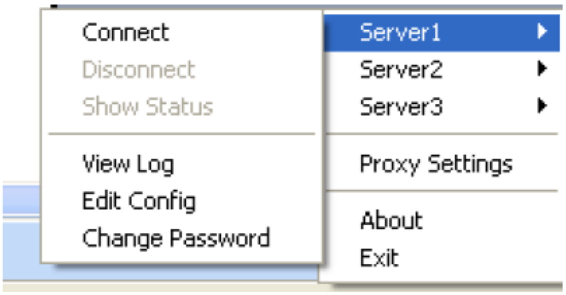
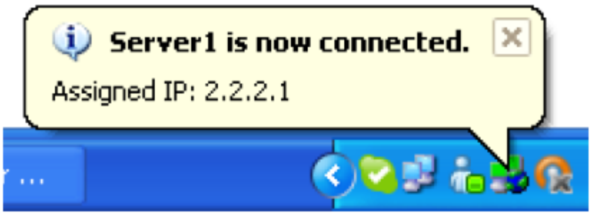


Figure 136 – Starting OpenVPN application

When OpenVPN tunnel is up on the Open VPN server you should get following notification:

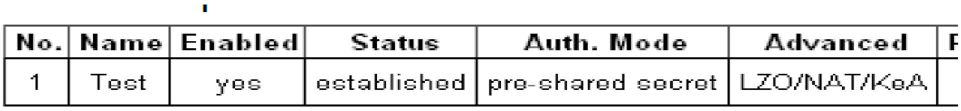


Server1 is now connected.

Assigned IP: 2.2.2.1

Figure 137 – OpenVPN status on PC

On the GWR side status of the OpenVPN tunnel should be established.



No.	Name	Enabled	Status	Auth. Mode	Advanced	F
1	Test	yes	established	pre-shared secret	LZO/NAT/KeA	

Figure 138 – OpenVPN status on GWG

Port forwarding example

Port forwarding feature enables access to workstations behind the gateway and redirecting traffic in both traffic flow directions – inbound and outbound. **Direction is selected by interface – PPP0 for inbound (WAN -> ETH0) and ETH0 for outbound traffic (ETH0 ->WAN).**

In the following example there are three types of access to LAN network enabled, every workstation with different service allowed from the outside. LAN is accessed through the WAN IP of the gateway. Second and forth rule have additional limitation per source IP address of the incoming packets. The forth defined access flow is redirecting all WEB traffic from the local workstation to one outside IP address, web authentication server for example.

Implemented rules are following:

1. Traffic destined to WAN IP by port 5022 is forwarded to workstation 192.168.1.2 and port 22. Result – SSH is accessible from the outside to the first workstation
2. Traffic destined to WAN IP by port 8080 is forwarded to workstation 192.168.1.3 and port 80. Result – WEB is accessible from the outside to the second workstation. This rule is limited only to traffic coming from the 172.16.234.0/24 subnet
3. Traffic destined to WAN IP from port range 300:400 is forwarded to workstation 192.168.1.4 to port 12345

4. WEB traffic from the workstation 192.168.1.5 is forwarded to one outside IP address (212.62.49.109 for example)

If Source IP and Source Netmask fields are empty stated entry is applied to all incoming packets. When PPP0 interface is selected Destination IP and Netmask are predefined to WAN IP and subnet 32 and cannot be changed.

On the following picture are marked traffic flows stated above.

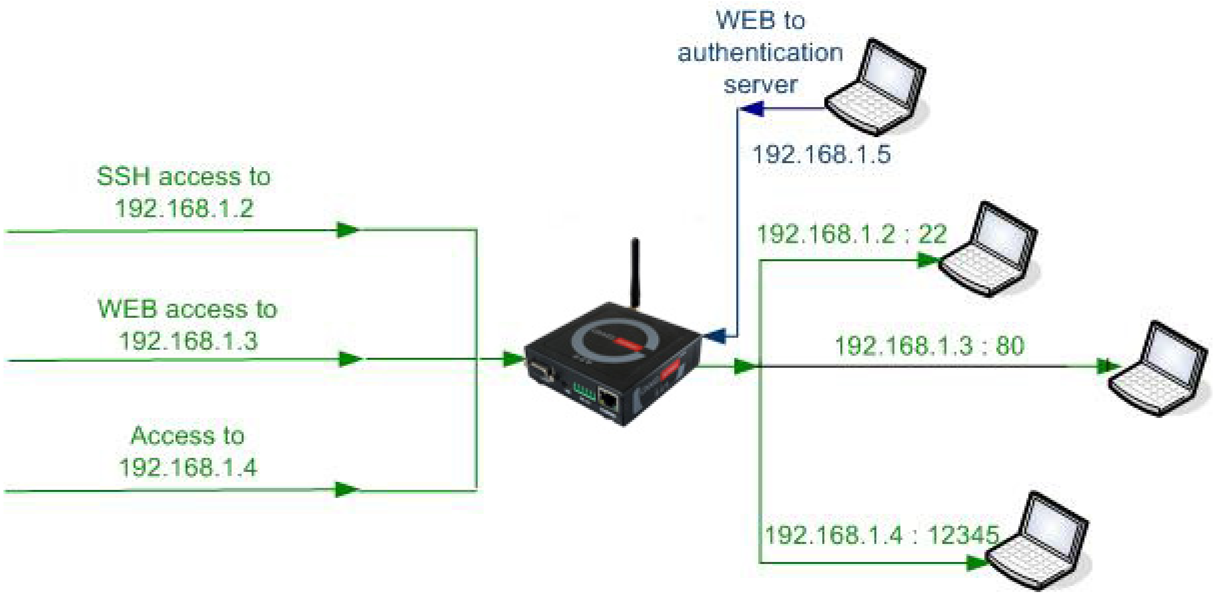
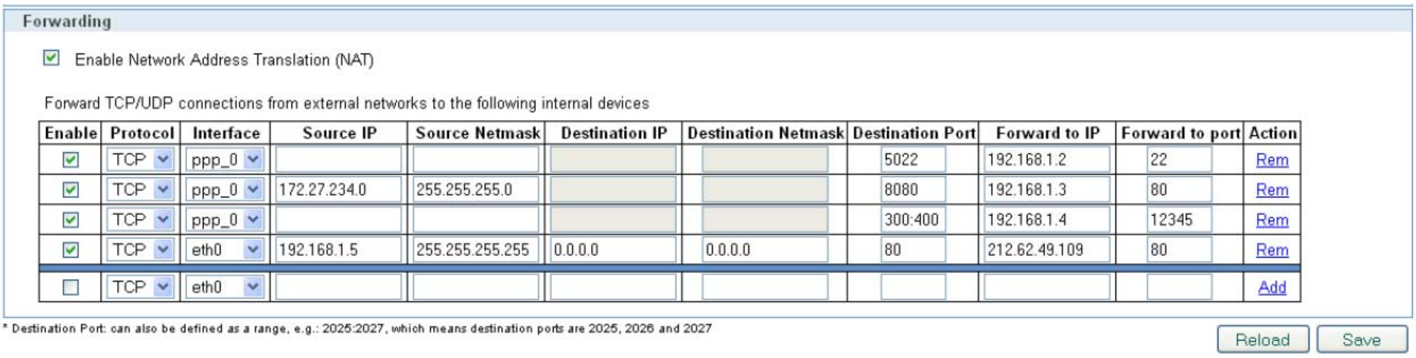


Figure 139– Portforwarding example

Port forwarding is configured on the ROUTING page selected from the main menu. Configuration of the examples described above is presented in the following picture:



Forwarding

☑ Enable Network Address Translation (NAT)

Forward TCP/UDP connections from external networks to the following internal devices

Enable	Protocol	Interface	Source IP	Source Netmask	Destination IP	Destination Netmask	Destination Port	Forward to IP	Forward to port	Action
☑	TCP	ppp_0					5022	192.168.1.2	22	Rem
☑	TCP	ppp_0	172.27.234.0	255.255.255.0			8080	192.168.1.3	80	Rem
☑	TCP	ppp_0					300:400	192.168.1.4	12345	Rem
☑	TCP	eth0	192.168.1.5	255.255.255.255	0.0.0.0	0.0.0.0	80	212.62.49.109	80	Rem
□	TCP	eth0								Add

* Destination Port: can also be defined as a range, e.g.: 2025:2027, which means destination ports are 2025, 2026 and 2027

Figure 140– GWG port forwarding configuration

Serial port – example

For connecting serial devices from remote locations to central location serial transparent conversion can be used. Serial communication is encapsulated in TCP/IP header and on the central location is recognized by the Virtual COM port application. This way serial communication is enabled between two distant locations.

In the picture below serial communication is achieved over GWG Gateway in client mode on remote location and Virtual COM port application on central side. As application is in server mode, IP address of the workstation has to be accessible from the gateway. In this example that is IP address GWG gateways supports both server and client mode, so you can use one GWG gateway on both side of communication link (one in server and one in client mode).

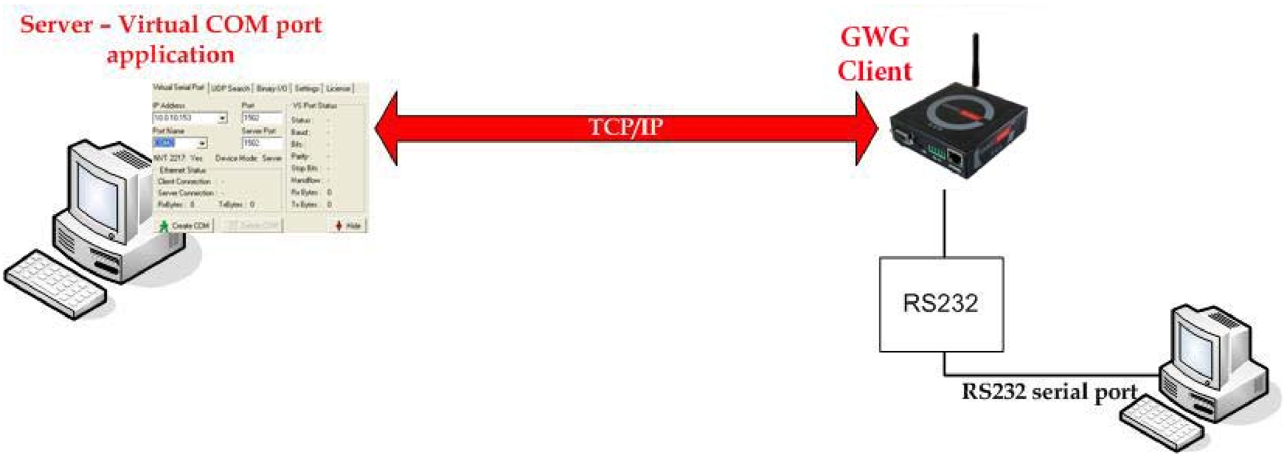
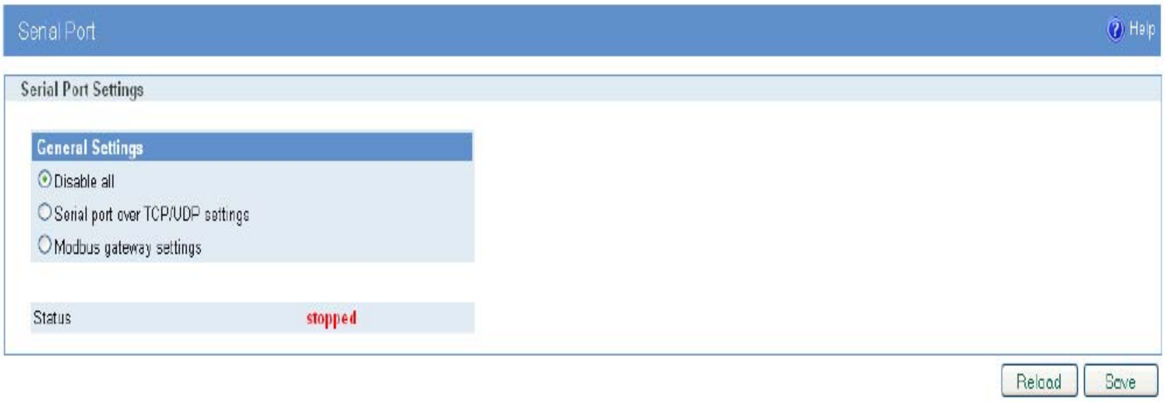


Figure 141– Transparent serial connection

1. Settings on GWG gateway

From the main menu on the left side of web interface option SERIAL PORT should be selected and following page is displayed.



Serial Port

Serial Port Settings

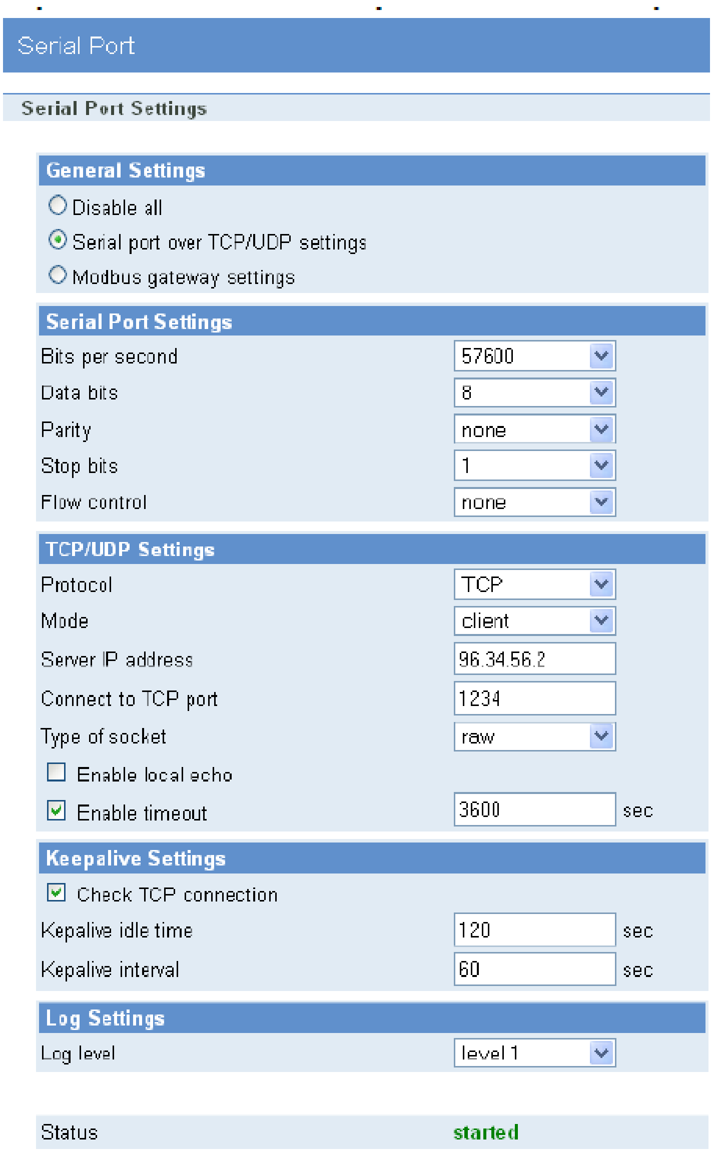
General Settings

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

Status stopped

Figure 142– GWG Serial port settings

Option SERIAL PORT OVER TCP/UDP SETTINGS is used for configuration of transparent serial communication. Configuration parameters are presented in picture below



Serial Port

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	client	
Server IP address	96.34.56.2	
Connect to TCP port	1234	
Type of socket	raw	
□ Enable local echo		
☑ Enable timeout	3600	sec

Keepalive Settings

☑ Check TCP connection		
Kepalive idle time	120	sec
Kepalive interval	60	sec

Log Settings

Log level	level 1

Status started

Figure 143– GWG settings for Serial-to-IP conversion

General Settings

- Serial port over TCP/UDP 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: client
- Server IP address: 96.34.56.2 (IP address of server)
- Connect to TCP port: 1234
- Type of socket: raw
- Enable local echo: Disabled
- Enable timeout: 3600 sec

Keepalive Settings

- Check TCP connection: Enable
- Keepalive idle time: 120 sec
- Keepalive interval: 60 sec

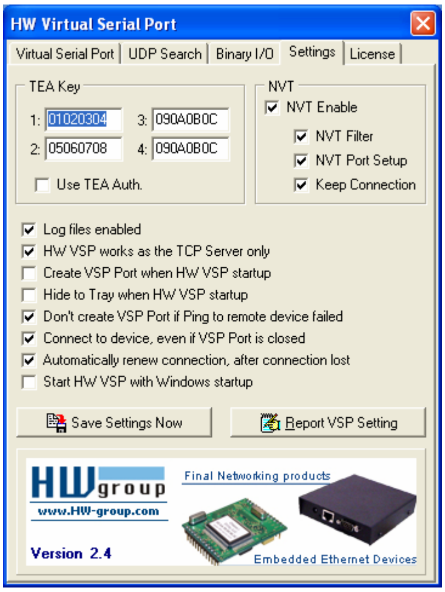
Log Settings

- Log level: level 1

When serial port is configured button SAVE should be selected and STATUS of the service should change to **started** like on the picture above.

2. Application settings

In this example is used application HW Virtual Serial Port which is installed on workstation on central location. When application is started on Settings tab option "HW VSP works as the TCP Server only" should be enabled.



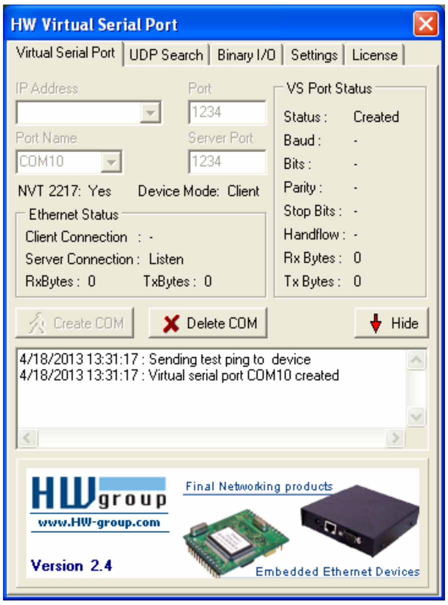
TEA Key
1: 01020304
2: 05060708
3: 090A0B0C
4: 090A0B0C
□ Use TEA Auth.

NVT
☑ NVT Enable
☑ NVT Filter
☑ NVT Port Setup
☑ Keep Connection

☑ Log files enabled
☑ HW VSP works as the TCP Server only
□ Create VSP Port when HW VSP startup
□ Hide to Tray when HW VSP startup
☑ Don't create VSP Port if Ping to remote device failed
☑ Connect to device, even if VSP Port is closed
☑ Automatically renew connection, after connection lost
□ Start HW VSP with Windows startup

Figure 144- Virtual COM port application

In Virtual Serial Port tab settings should be following:



IP Address
Port: 1234
Port Name: COM10
Server Port: 1234
NVT 2217: Yes
Device Mode: Client

Ethernet Status
Client Connection : -
Server Connection : Listen
RxBytes : 0
TxBytes : 0

VS Port Status
Status : Created
Baud : -
Bits : -
Parity : -
Stop Bits : -
Handflow : -
Rx Bytes : 0
Tx Bytes : 0

```
4/18/2013 13:31:17 : Sending test ping to  device
4/18/2013 13:31:17 : Virtual serial port COM10 created
```

Figure 145– Settings for virtual COM port

- IP address: - (not used in server mode)
- Port: 1234
- Server Port: 1234
- Port Name: COM10 (random selected)

After "Create COM" is activated if everything is alright in log will be shown message that port COM10 is created, like in picture above. In communication with remote serial device COM10 should be selected on workstation.

Firewall – example

Firewall implemented in GWG gateways has numerous options for matching interesting traffic. Traffic flow is controlled through the gateway with three actions triggered by firewall:

1. ACCEPT – traffic is passed through the gateway without any changes implemented
2. REJECT – traffic is blocked with ICMP error messages
3. DROP – traffic is blocked without any error messages, connection is retried until the threshold for retransmission is exceeded

By default all traffic is PERMITTED. To block all the traffic not defined under stated rules last entry in firewall table should be DROP ALL.

Rule priority defines order by which gateway matches inspected packets. After first match between rule and packet, no other rule is compared against matched traffic.

Firewall has 17 predefined rules for the most common usage. These 17 rules are following:

1. Allow ALL from local LAN

All traffic originating from local subnet is allowed to access gateway Ethernet interface. It is important to keep this rule enabled to prevent losing local management interface.

2. Allow already established traffic

For inbound TCP only. Allows TCP traffic to pass if the packet is a response to an outbound-initiated session.

3. Allow TELNET on ppp_0

Accepts telnet connection from the outside to router's WAN interface, for management over CLI interface

4. Allow HTTP on ppp_0

Accepts WEB traffic from the outside to gateway's WAN interface, for management over WEB interface

5. Allow PING on ppp_0-with DDoS filter

ICMP traffic to WAN interface of the gateway is allowed with prevention of Distributed Denial-of-service attack

Allow RIP protocol

6. Allow RIP on ppp_0
7. Allo RIP on ppp_0 – route

Allow GRE protocol

8. Allow GRE tunnels on ppp_0
9. Allow GRE Keepalive on ppp_0

Allow IPSec protocol

10. Allow IPSec tunnels on ppp_0 – protocol

11. Allow IPSec tunnels on ppp_0 – IKE
12. Allow IPSec tunnel on ppp_0 – IKE_NATt

Allow OpenVPN protocol
13. Allow OpenVPN tunnels on ppp_0 – UDP
14. Allow OpenVPN tunnels on ppp_0 – TCP

15. Allow SNMP on ppp_0
SNMP requests are allowed to be sent to the router over WAN interface

16. Allow MODBUS on ppp_0
MODBUS conversion over default UDP 502 is permitted

17. REJECT all other traffic
All packets which are not stated as ACCEPT in previous rules are denied. If this rule is not enabled all packets which are not stated as DROP/REJECT are permitted.

In following example 8 traffic flows are defined under firewall rules. In the picture presented with green are marked permitted packets and with red blocked.

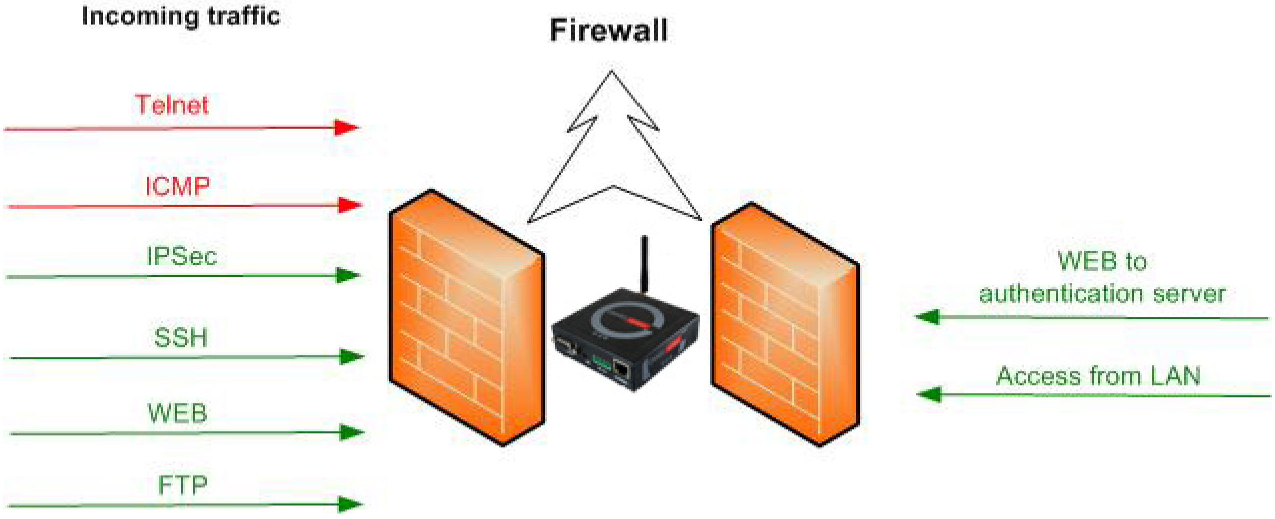
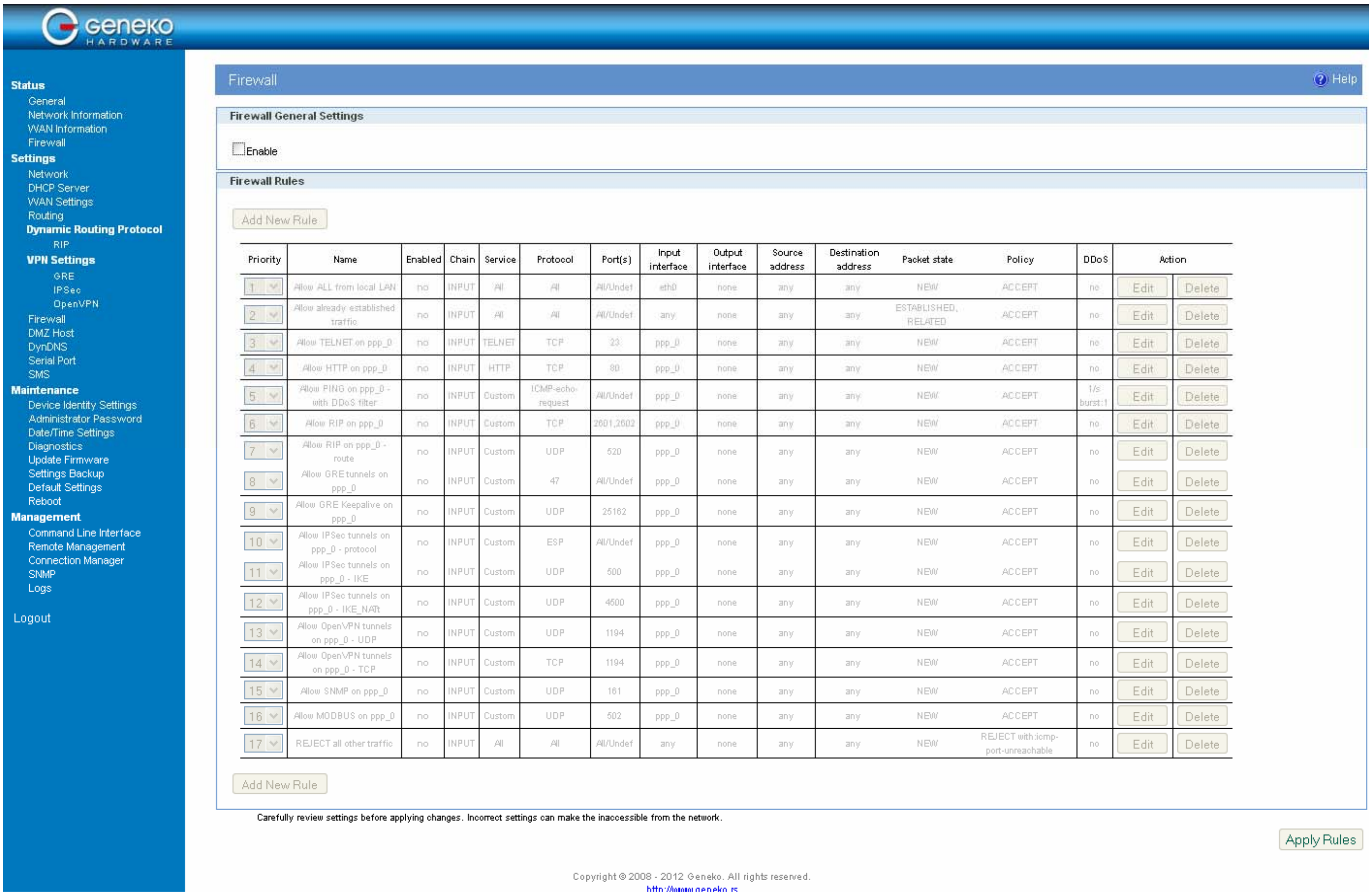


Figure 146 – Firewall example

Firewall is enabled in SETTINGS>FIREWALL page. Page for firewall configuration is presented in the following picture:



Firewall

Firewall General Settings

☐ Enable

Firewall Rules

Add New Rule

Priority	Name	Enabled	Chain	Service	Protocol	Port(s)	Input interface	Output interface	Source address	Destination address	Packet state	Policy	DDoS	Action	
1	Allow ALL from local LAN	no	INPUT	All	All	All/Undef	eth0	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 DDoS filter	no	INPUT	Custom	ICMP-echo-request	All/Undef	ppp_0	none	any	any	NEW	ACCEPT	1/s burst:1	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	47	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_NAT	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 MODBUS 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 with:icmp-port-unreachable	no	Edit	Delete

Add New Rule

Carefully review settings before applying changes. Incorrect settings can make the inaccessible from the network.

Apply Rules

Copyright © 2008 - 2012 Geneko. All rights reserved.
http://www.geneko.rs

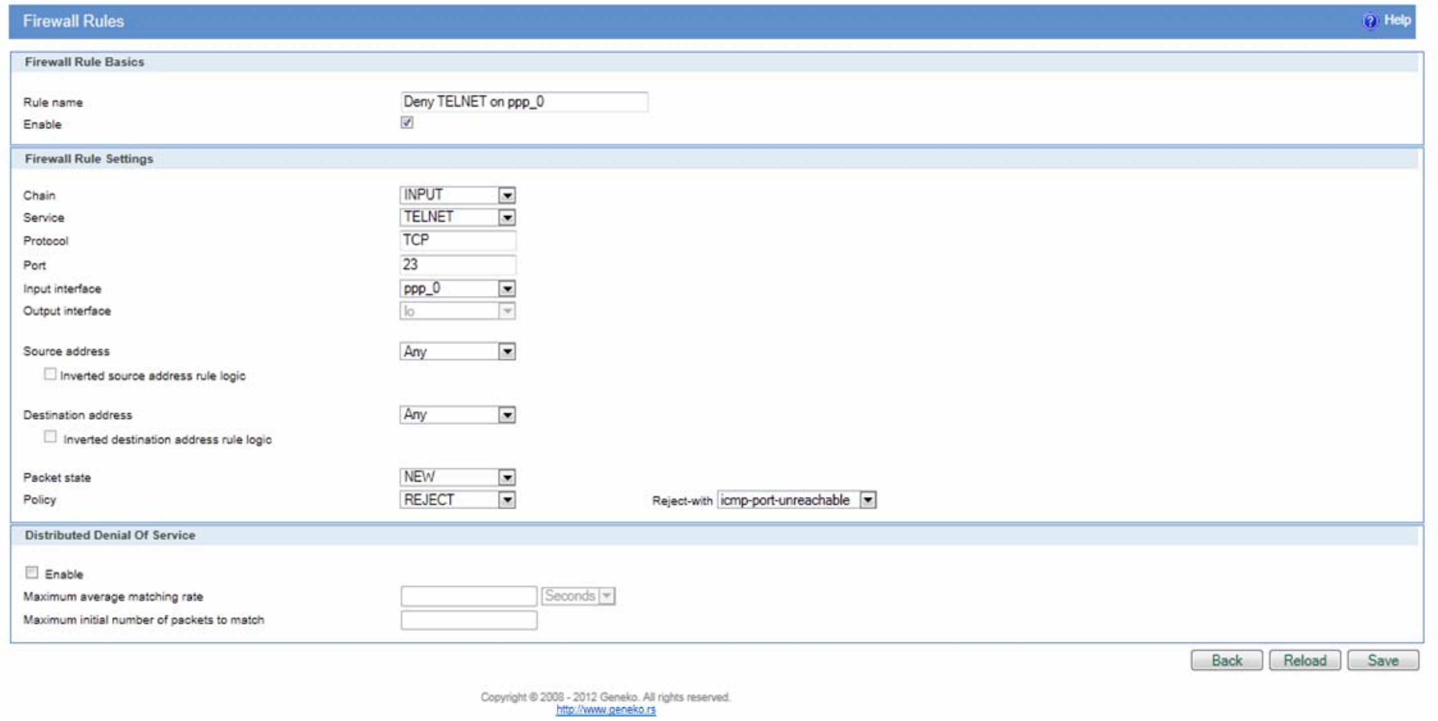
Figure 147 – Initial firewall configuration on GWG

Firstly firewall should be enabled, that is done by selecting:
Firewall General Settings>Enable

Firewall can be configured by enabling or editing existing, predefined rules or by adding new one. Firewall is configured in following way:

1. Telnet traffic is denied

Select predefined rule number 3. Configuration page like on picture below is shown.



Firewall Rules

Firewall Rule Basics

Rule name: Deny TELNET on ppp_0
Enable: ☑

Firewall Rule Settings

Chain: INPUT
Service: TELNET
Protocol: TCP
Port: 23
Input interface: ppp_0
Output interface: lo
Source address: Any
☐ Inverted source address rule logic
Destination address: Any
☐ Inverted destination address rule logic
Packet state: NEW
Policy: REJECT   Reject-with: icmp-port-unreachable

Distributed Denial Of Service

☐ Enable
Maximum average matching rate: Seconds
Maximum initial number of packets to match

Figure 148 – Filtering of Telnet traffic

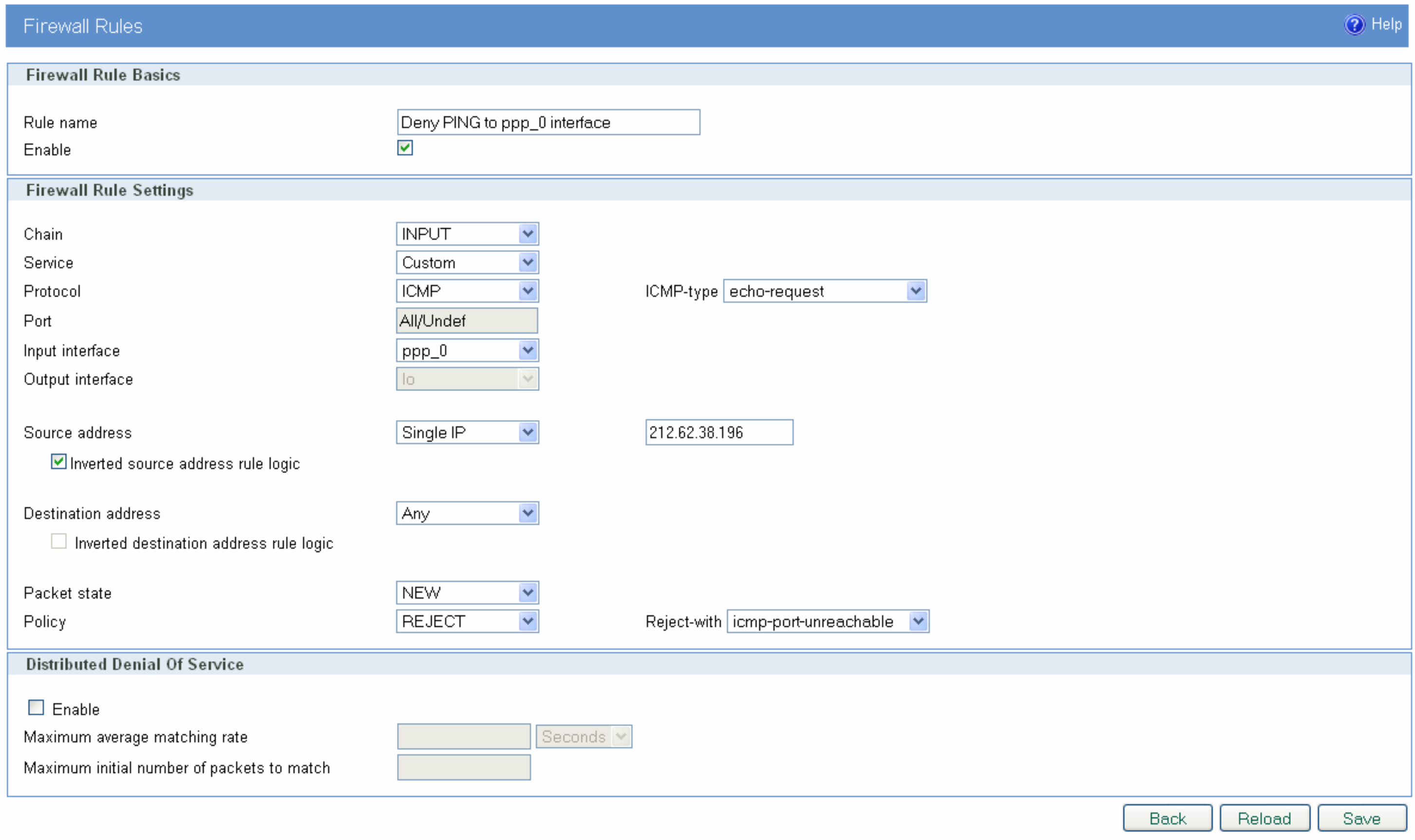
ENABLE option should be selected to have this rule active. To deny Telnet traffic POLICY should be changed from ACCEPT to REJECT (ICMP error message type can be selected when policy reject is selected). After that SAVE button should be pressed and user is returned to main configuration page.

2. ICMP traffic is denied from all IP addresses except 212.62.38.196

New rule should be added by selecting ADD NEW RULE button. Policy should be configured in following way:

- Rule name: Deny PING to ppp_0 interface
- Enable: selected
- Chain: INPUT
- Service: Custom
- Protocol: ICMP
- ICMP-Type: echo-request
- Input interface: ppp_0
- Source address: Single IP ; 212.62.38.196
- Inverted source address rule logic: selected
- Destination address: Any
- Packet state: NEW
- Policy: REJECT
- Reject-with: icmp-port-unreachable

Configuration should be like on the picture below.



Firewall Rule Basics

Rule name	Deny PING to ppp_0 interface
Enable	☑

Firewall Rule Settings

Chain	INPUT		
Service	Custom		
Protocol	ICMP	ICMP-type	echo-request
Port	All/Undef		
Input interface	ppp_0		
Output interface	lo		
Source address	Single IP		212.62.38.196
☑ Inverted source address rule logic			
Destination address	Any		
□ Inverted destination address rule logic			
Packet state	NEW		
Policy	REJECT	Reject-with	icmp-port-unreachable

Distributed Denial Of Service

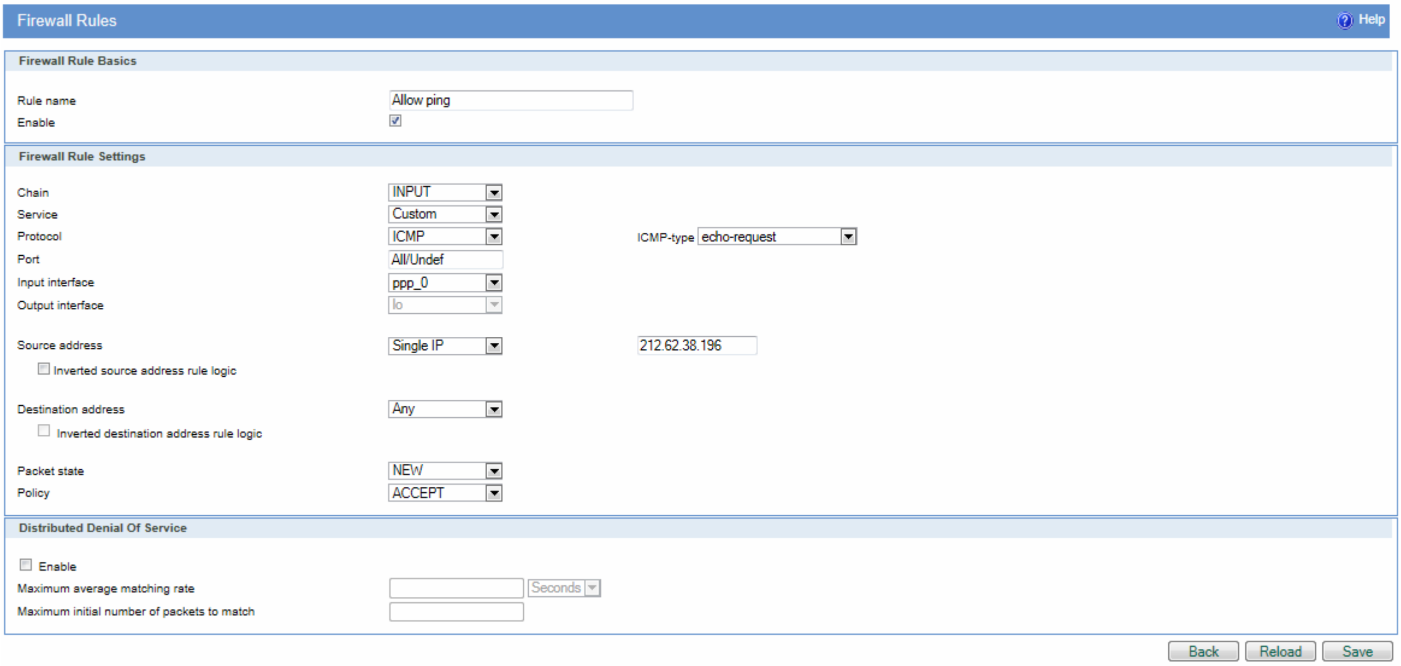
□ Enable	
Maximum average matching rate	Seconds
Maximum initial number of packets to match	

Figure 149 – Filtering of ICMP traffic

After configuration is finished SAVE button should be selected and user is returned to main configuration page. **Priority of rule** is changed by selecting number in drop-down menu. In this example number 4 is selected.

3. ICMP traffic is allowed from single IP addresses

With firewall rule configuration shown above, IP address stated in Source address field is excluded from REJECT policy but in order to allow ping from that IP address it has to be matched with another rule. Configuration of appropriate rule for allowing ping traffic originating from precise IP address is shown below



Firewall Rules

Firewall Rule Basics

Rule name	Allow ping
Enable	☑

Firewall Rule Settings

Chain	INPUT	
Service	Custom	
Protocol	ICMP	ICMP-type echo-request
Port	All/Undef	
Input interface	ppp_0	
Output interface	lo	
Source address	Single IP	212.62.38.196
□ Inverted source address rule logic		
Destination address	Any	
□ Inverted destination address rule logic		
Packet state	NEW	
Policy	ACCEPT	

Distributed Denial Of Service

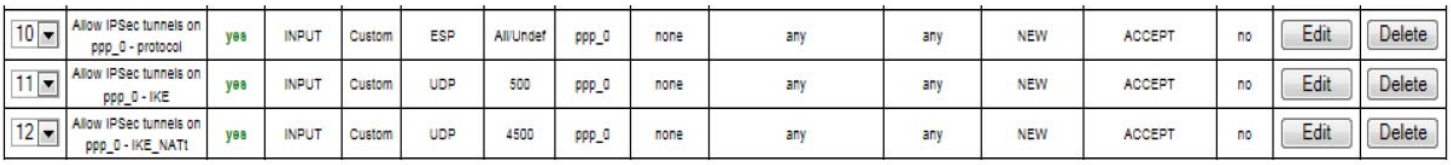
□ Enable	
Maximum average matching rate	Seconds
Maximum initial number of packets to match	

Figure 150 – Allowing ICMP traffic

After configuration is finished SAVE button should be selected and user is returned to main configuration page. **Priority of rule** is changed by selecting number in drop-down menu. In this example number 5 is selected.

4. Establishing of IPSec tunnel is allowed

Firewall has to allow IKE and ESP protocol for IPSec tunnel establishment. If NAT traversal is used one additional port has to be allowed. All these rules are predefined and they have priorities 10, 11 and 12 in default firewall configuration (they are named as *Allow IPSec tunnels on ppp_0 –protocol, IKE and NATt*). As these rules are already configured it is enough just to enable them to have IPSec passed through firewall.



10	Allow IPSec tunnels on ppp_0 - protocol	yes	INPUT	Custom	ESP	All/Undef	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
11	Allow IPSec tunnels on ppp_0 - IKE	yes	INPUT	Custom	UDP	500	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
12	Allow IPSec tunnels on ppp_0 - IKE_NATt	yes	INPUT	Custom	UDP	4500	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete

Figure 151 – IPSec firewall rules

These three rules are enabled in following way:

- Select EDIT of the rule
- Enable: selected
- SAVE and exit

5. SSH access is allowed from IP range 212.62.38.210-220

New rule should be added by selecting ADD NEW RULE button. Policy should be configured in following way:

- Rule name: Allow SSH
- Enable: selected

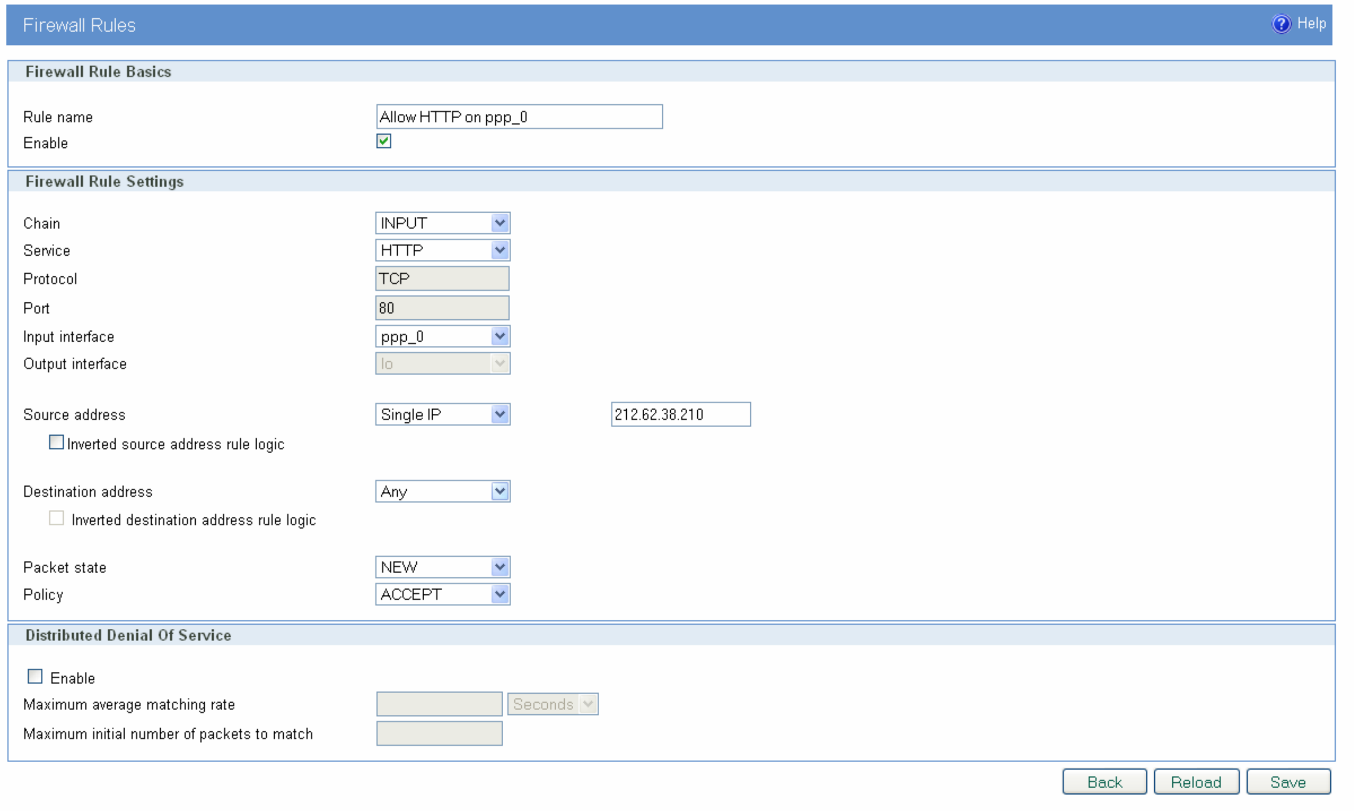
- Chain: INPUT
- Service: Custom
- Protocol: TCP
- Port: Custom; 22
- Input interface: ppp_0
- Source address: Range ; 212.62.38.210 : 212.62.38.220
- Destination address: Any
- Packet state: NEW
- Policy: ACCEPT

After configuration is finished SAVE button should be selected and user is returned to main configuration page. **Priority of rule** is changed by selecting number in drop-down menu. In this example number 6 is selected.

6. WEB access is allowed from 212.62.38.210 IP address

In default firewall configuration rule for allowing WEB traffic is predefined (rule with priority 4, named *Allow HTTP on ppp_0*) This rule can be used in example with additional restriction in source IP address to 212.62.38.210. Policy should be configured in following way:

- Enable: selected
- Source address: Single IP; 212.62.38.210
- All other settings should remain the same like in the picture below



Firewall Rule Basics

Rule name: Allow HTTP on ppp_0
Enable: ☑

Firewall Rule Settings

Chain: INPUT
Service: HTTP
Protocol: TCP
Port: 80
Input interface: ppp_0
Output interface: lo
Source address: Single IP 212.62.38.210
☐ Inverted source address rule logic
Destination address: Any
☐ Inverted destination address rule logic
Packet state: NEW
Policy: ACCEPT

Distributed Denial Of Service

☐ Enable
Maximum average matching rate: Seconds
Maximum initial number of packets to match

Figure 152 – Allowing WEB access

After configuration is finished SAVE button should be selected and user is returned to main configuration page.

7. FTP traffic is allowed

New rule should be added by selecting ADD NEW RULE button. Policy should be configured in following way:

- Rule name: Allow FTP
- Enable: selected
- Chain: INPUT
- Service: FTP
- Protocol: TCP
- Port: 21
- Input interface: ppp_0
- Source address: Any
- Destination address: Any
- Packet state: NEW
- Policy: ACCEPT

After configuration is finished SAVE button should be selected and user is returned to main configuration page. **Priority of rule** is changed by selecting number in drop-down menu. In this example number 8 is selected.

8. Access from LAN to gateway is allowed

This is first rule in predefined firewall settings (*Allow ALL from local LAN*). It is recommended to have this rule enabled to allow access to management interfaces of the router. As this rules is already configured it is enough just to enable it to have access to router from LAN:

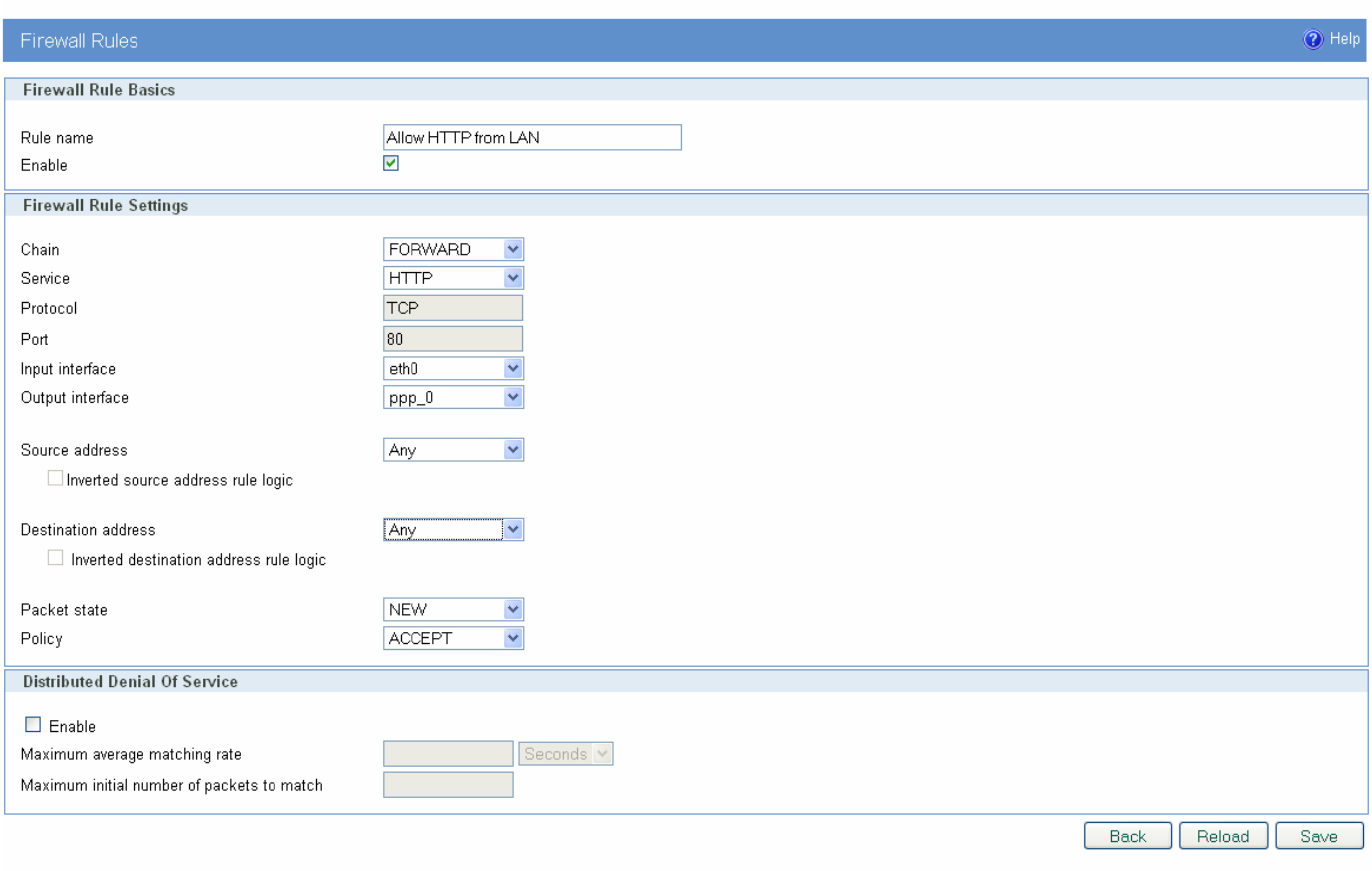
- Select EDIT of the rule
- Enable: selected
- SAVE and exit

9. WEB traffic is permitted only to 212.62.38.210 from LAN

This rule is example of traffic filtering in direction from inside to outside. New rule should be added by selecting ADD NEW RULE button. Policy should be configured in following way:

- Rule name: Allow HTTP from LAN
- Enable: selected
- Chain: FORWARD
- Service: HTTP
- Protocol: TCP
- Port: 80
- Input interface: eth0
- Output interface: ppp_0
- Source address: Any
- Destination address: Any
- Packet state: NEW
- Policy: ACCEPT

Configuration is shown in following picture:



Firewall Rules

Firewall Rule Basics

Rule name	Allow HTTP from LAN
Enable	☑

Firewall Rule Settings

Chain	FORWARD
Service	HTTP
Protocol	TCP
Port	80
Input interface	eth0
Output interface	ppp_0
Source address	Any
□ Inverted source address rule logic	
Destination address	Any
□ Inverted destination address rule logic	
Packet state	NEW
Policy	ACCEPT

Distributed Denial Of Service

□ Enable	
Maximum average matching rate	Seconds
Maximum initial number of packets to match	

Figure 153 – Outbound rule for WEB access

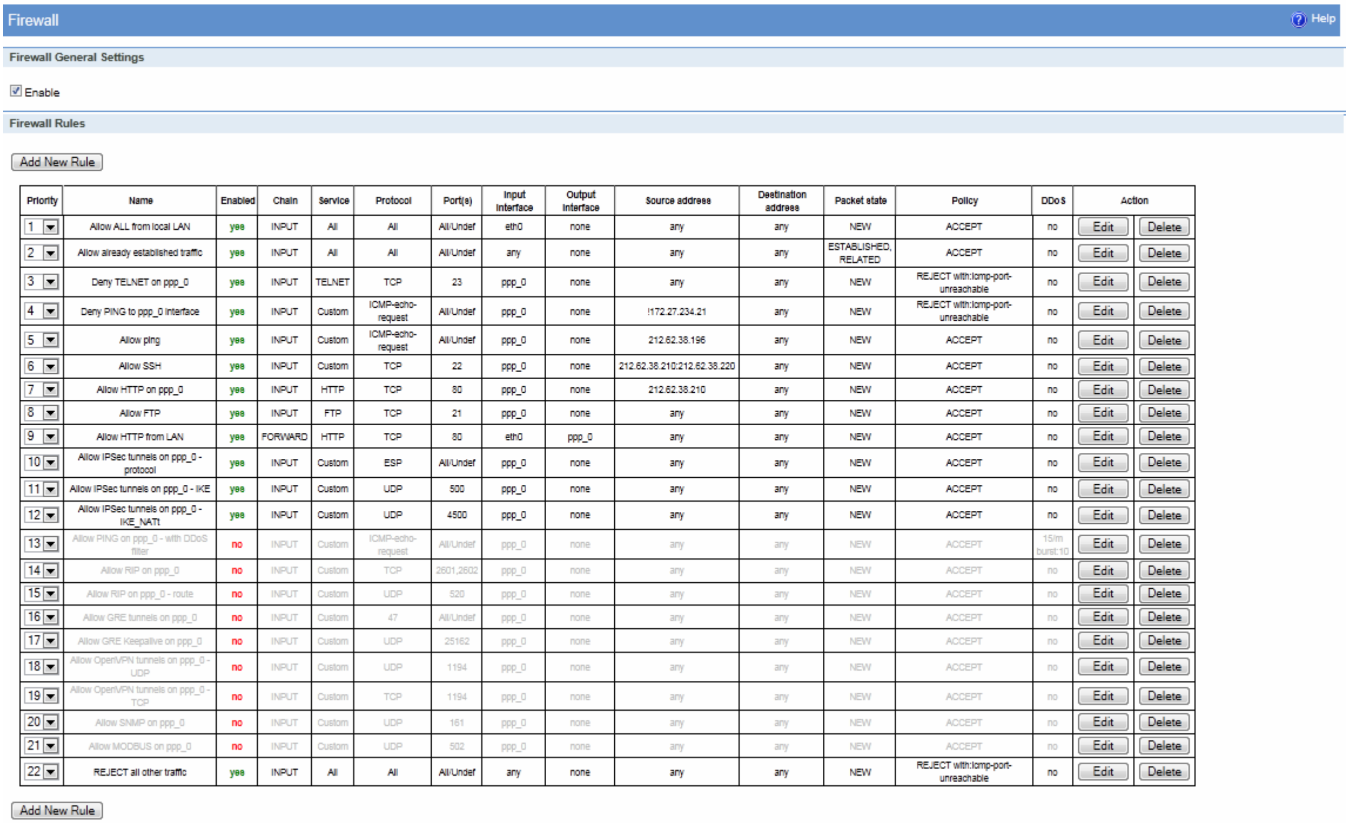
After configuration is finished SAVE button should be selected and user is returned to main configuration page. **Priority of rule** is changed by selecting number in drop-down menu. In this example number 9 is selected.

Additionally to these 11 rules two more rules are enabled:

- Allow already established traffic (priority number 2)
- Reject all other traffic (priority number 22)

After all rules are configured and saved button APPLY RULES in bottom right corner should be selected to activate traffic filtering.

When all 13 rules from this example is configured firewall should look like this:



Firewall General Settings

☑ Enable

Firewall Rules

Add New Rule

Priority	Name	Enabled	Chain	Service	Protocol	Port(s)	Input Interface	Output Interface	Source address	Destination address	Packet state	Policy	DDoS	Action	
1	Allow ALL from local LAN	yes	INPUT	All	All	All/Undef	eth0	none	any	any	NEW	ACCEPT	no	Edit	Delete
2	Allow already established traffic	yes	INPUT	All	All	All/Undef	any	none	any	any	ESTABLISHED, RELATED	ACCEPT	no	Edit	Delete
3	Deny TELNET on ppp_0	yes	INPUT	TELNET	TCP	23	ppp_0	none	any	any	NEW	REJECT with:icmp-port-unreachable	no	Edit	Delete
4	Deny PING to ppp_0 interface	yes	INPUT	Custom	ICMP-echo-request	All/Undef	ppp_0	none	!172.27.234.21	any	NEW	REJECT with:icmp-port-unreachable	no	Edit	Delete
5	Allow ping	yes	INPUT	Custom	ICMP-echo-request	All/Undef	ppp_0	none	212.62.38.196	any	NEW	ACCEPT	no	Edit	Delete
6	Allow SSH	yes	INPUT	Custom	TCP	22	ppp_0	none	212.62.38.210:212.62.38.220	any	NEW	ACCEPT	no	Edit	Delete
7	Allow HTTP on ppp_0	yes	INPUT	HTTP	TCP	80	ppp_0	none	212.62.38.210	any	NEW	ACCEPT	no	Edit	Delete
8	Allow FTP	yes	INPUT	FTP	TCP	21	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
9	Allow HTTP from LAN	yes	FORWARD	HTTP	TCP	80	eth0	ppp_0	any	any	NEW	ACCEPT	no	Edit	Delete
10	Allow IPSec tunnels on ppp_0 - protocol	yes	INPUT	Custom	ESP	All/Undef	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
11	Allow IPSec tunnels on ppp_0 - IKE	yes	INPUT	Custom	UDP	500	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
12	Allow IPSec tunnels on ppp_0 - IKE_NATt	yes	INPUT	Custom	UDP	4500	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
13	Allow PING on ppp_0 - with DDoS filter	no	INPUT	Custom	ICMP-echo-request	All/Undef	ppp_0	none	any	any	NEW	ACCEPT	15/m burst:10	Edit	Delete
14	Allow RIP on ppp_0	no	INPUT	Custom	TCP	2601,2602	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
15	Allow RIP on ppp_0 - route	no	INPUT	Custom	UDP	520	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
16	Allow GRE tunnels on ppp_0	no	INPUT	Custom	47	All/Undef	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
17	Allow GRE Keepalive on ppp_0	no	INPUT	Custom	UDP	25162	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
18	Allow OpenVPN tunnels on ppp_0 - UDP	no	INPUT	Custom	UDP	1194	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
19	Allow OpenVPN tunnels on ppp_0 - TCP	no	INPUT	Custom	TCP	1194	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
20	Allow SNMP on ppp_0	no	INPUT	Custom	UDP	161	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
21	Allow MODBUS on ppp_0	no	INPUT	Custom	UDP	502	ppp_0	none	any	any	NEW	ACCEPT	no	Edit	Delete
22	REJECT all other traffic	yes	INPUT	All	All	All/Undef	any	none	any	any	NEW	REJECT with:icmp-port-unreachable	no	Edit	Delete

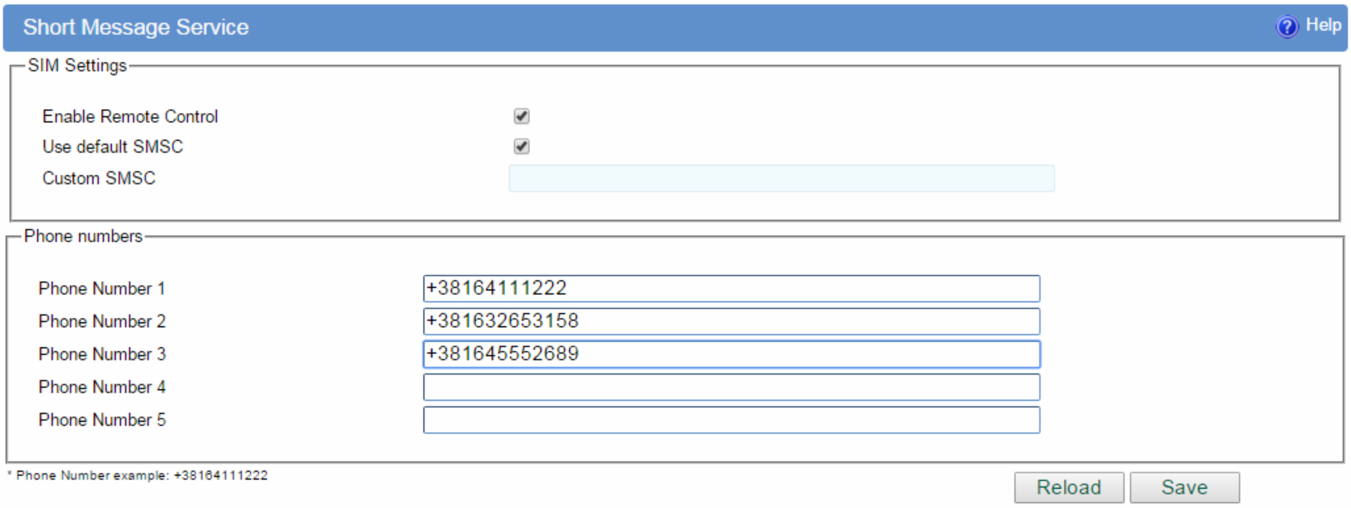
Add New Rule

Figure 154 – Complete firewall configuration

SMS management – example

GWG gateways can be managed over the SMS messages. Commands from the SMS are executed on the router with status report sent back to the sender.

On the picture below are settings for SMS management where three mobile phone numbers are allowed to send commands to the gateway over SIM card. In this example management over SIM is not enabled. Please have in mind that gateway can receive messages only on SIM card if it is enabled. This information is displayed in Mobile settings page. SMS service center number is automatically obtained.



SIM Settings

Enable Remote Control ☑
Use default SMSC ☑
Custom SMSC

Phone numbers

Phone Number 1	+38164111222
Phone Number 2	+381632653158
Phone Number 3	+381645552689
Phone Number 4	
Phone Number 5	

* Phone Number example: +38164111222

Figure 155– Configuration page for SMS management

Settings are following:

- Enable Remote Control: Enabled
- Use default SMSC: Enabled
- Phone Number 1,2…5: Allowed phone number

From the mobile phone user can send 6 different commands for gateway management. Commands are following:

1. *:PPP-CONNECT*
2. *:PPP-DISCONNECT*
3. *:PPP-RECONNECT*
4. *:PPP-STATUS*

Reply to this command is one of four possible states:

- CONNECTING
- CONNECTED, WAN_IP:{WAN IP address}
- DISCONNECTING
- DISCONNECTED

5. *:SWITCH-SIM*, for changing SIM slot

6 *:REBOOT*, for router reboot

After every SMS sent to the gateway, reply is sent back with status information about SMS received by the gateway.

Defining keepalive functionality

Keep-alive mechanism works through two simple steps.

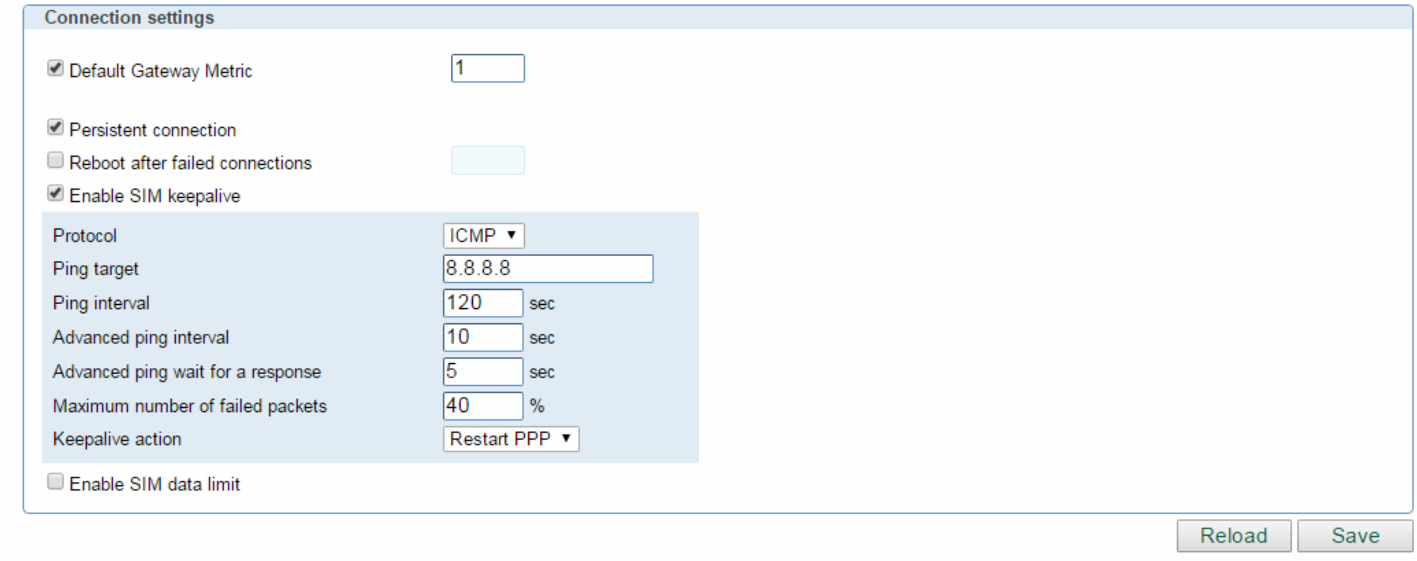
First step is STANDARD ping proofing. This ping periodically checks if link is alive. Standard ping has 4 packets which are sent over the link and if all 4 are returned keep-alive remains in standard ping proofing mode. If two or more of 4 packets are dropped keep-alive activates ADVANCED ping proofing.

ADVANCED ping proofing is second step in link quality detection. Advanced ping proofing sends 5 ping packets in short period of time and gives statistic how much packets are dropped (for example if 4 packets are dropped, ping lost is 80%). If this value is defined as 100% for example, that means only if all packets are dropped action will be performed (PPP restart). Value which is entered here depends on that how many packets can be tolerated to lose on the link. For example if value 60% is entered 2 packets of 5 (40%) are lost, keep-alive is returned to step one (standard ping proofing) with no action performed. If PPP should be restarted only when all packets are dropped defined value should be 100%.

In following example keepalive is enabled on SIM card. Settings are following:

SIM

Ping target: 8.8.8.8
Ping interval: 120
Advanced ping interval: 10
Advanced ping wait for response: 5
Maximum number of failed packets: 80
Keepalive action: Restart PPP



Connection settings

☑ Default Gateway Metric 1

☑ Persistent connection

☐ Reboot after failed connections

☑ Enable SIM keepalive

Protocol	ICMP ▾
Ping target	8.8.8.8
Ping interval	120 sec
Advanced ping interval	10 sec
Advanced ping wait for a response	5 sec
Maximum number of failed packets	40 %
Keepalive action	Restart PPP ▾

☐ Enable SIM data limit

Figure 156– Configuration page for SIM keepalive

Appendix

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 GWG Gateway 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