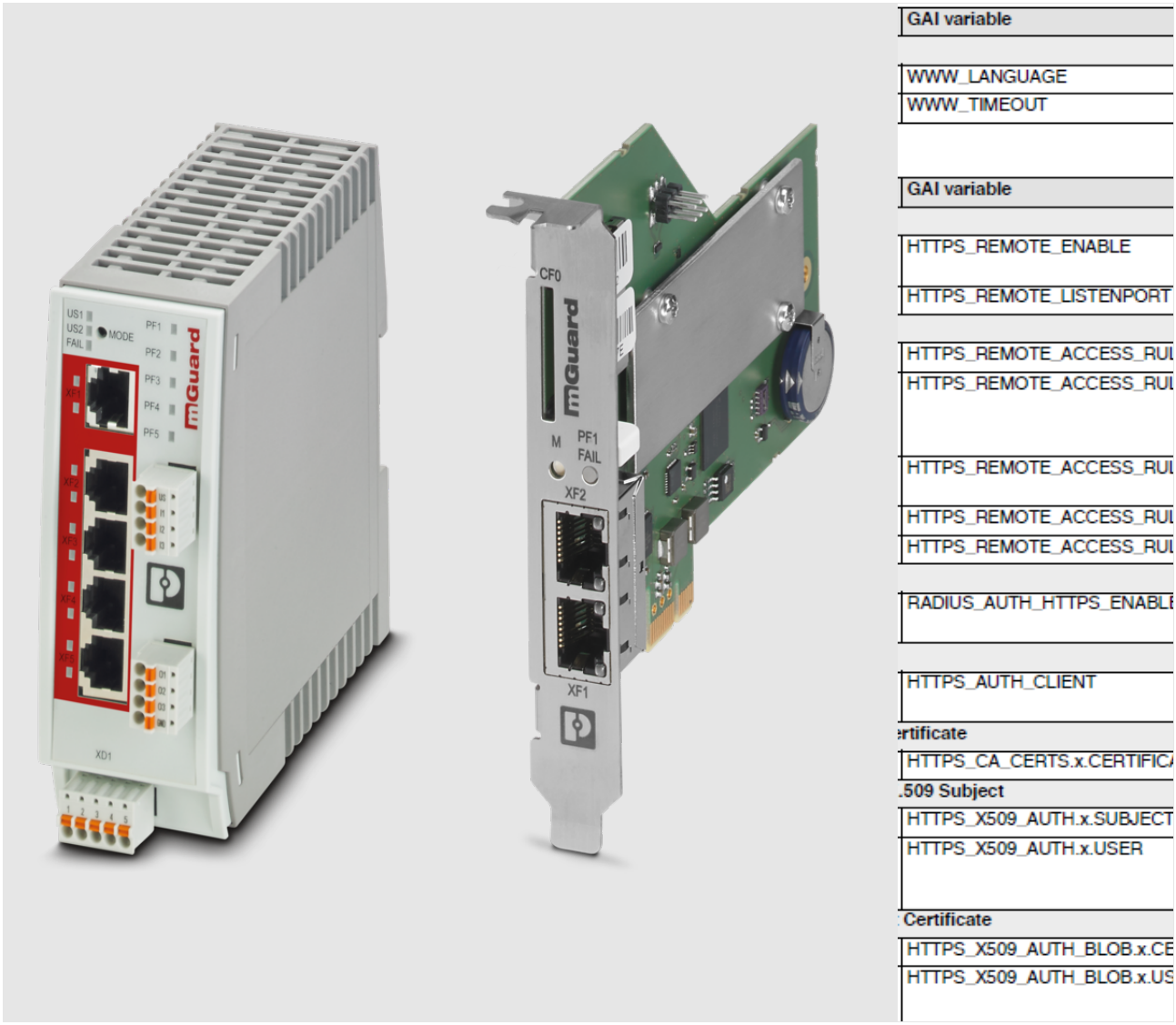

FL MGUARD 2000/4000
Generic Administration Interface
mGuard 10.6.x

User manual

User manual

FL MGUARD 2000/4000 - Generic Administration Interface mGuard 10.6.x

UM EN GAICONFIG MGUARD10, Revision 07 2026-01-27

This user manual is valid for

Designation	Item No.
FL MGUARD 2102	1357828
FL MGUARD 4302	1357840
FL MGUARD 4302/KX	1696708
FL MGUARD 2105	1357850
FL MGUARD 4305	1357875
FL MGUARD 4305/KX	1696779
FL MGUARD 4102 PCI	1441187
FL MGUARD 4102 PCIE	1357842

Firmware version: mGuard 10.6.x

Applicable documentation (available at phoenixcontact.net/product/<item number>):

Release Notes

mGuard 10.6.x Firmware – Release Notes

User Manual „Web-based management“

UM EN FW MGUARD10 – 110191_en_xx

User Manual „Installation and startup“

UM EN HW FL MGUARD 2000/4000 – 110192_en_xx

110193_en_07

Table of contents

1 For your safety

Read this user manual carefully and keep it for future reference.

1.1 Identification of warning notes

This symbol together with the **NOTE** signal word warns the reader of actions that might cause property damage or a malfunction.

Here you will find additional information or detailed sources of information.

1.2 About this user manual

The following elements are used in this user manual:

Bold	Designations of operating elements, variable names or other accentuations
Italic	– Product, module or component designations (e.g., *tftpd64.exe*, *Config API*) – Foreign designations or proper names – Other accentuations
–	Unnumbered list
1.	Numbered list
•	Operating instructions
↳	Result of an operation

1.3 Qualification of users

The use of products described in this user manual is oriented exclusively to:

– Electrically skilled persons or persons instructed by them. The users must be familiar with the relevant safety concepts of automation technology as well as applicable standards and other regulations.

– Qualified application programmers and software engineers. The users must be familiar with the relevant safety concepts of automation technology as well as applicable standards and other regulations.

1.4 Intended use

– The devices of the FL MGUARD series are security routers for industrial use, with integrated stateful packet inspection firewall and VPN. They are suitable for distributed protection of production cells or individual machines against manipulation and for secure remote maintenance.

– The devices are not intended for private use. They may only be used and operated in the commercial or industrial sector.

1.5 Modifications to the product

Modifications to hardware and firmware of the device are not permitted.

Incorrect operation or modifications to the device can endanger your safety or damage the device. Do not repair the device yourself. If the device is defective, please contact Phoenix Contact.

1.6 Safety notes

To ensure correct operation and the safety of the environment and of personnel, the device must be installed, operated, and maintained correctly.

NOTE: Installation only by qualified personnel
Installation, startup and maintenance of the product may only be performed by qualified specialist staff who have been authorized for this by the system operator. An electrically skilled person is someone who, because of their professional training, skills, experience, and their knowledge of relevant standards, can assess any required operations and recognize any possible dangers. Specialist staff must read and understand this documentation and comply with instructions. Observe the national regulations in force for the operation, functional testing, repairs and maintenance of electronic devices.

NOTE: Risk of material damage due to incorrect wiring
Connect the network connections of the device to Ethernet installations only. Some telecommunications connections also use RJ45 jacks; these must not be connected to the RJ45 jacks of the device.

NOTE: Electrostatic discharge
The devices contain components that can be damaged or destroyed by electrostatic discharge. When handling the devices, observe the necessary safety precautions against electrostatic discharge (ESD) in accordance with EN 61340-5-1 and EN 61340-5-2.

NOTE: Requirements for the power supply
The module is designed exclusively for operation with safety extra-low voltage (SELV/PELV). In redundant operation, both power supplies must satisfy the requirements of the safety extra-low voltage.

NOTE: Requirement for control cabinet/control box
DIN rail devices snap onto a DIN rail inside a control cabinet or control box. This control cabinet/box must meet the requirements of IEC/EN 62368-1 with respect to fire protection enclosure.

NOTE: Requirement for functional grounding
Mount the DIN rail devices on a grounded DIN rail. The module is grounded when it is snapped onto the DIN rail.

NOTE: Requirement for mounting location
The prescribed mounting position of DIN rail devices is vertical on a horizontally mounted DIN rail. To allow air to circulate freely, the vents must not be covered. A gap of 3 cm between the vents of the housing is recommended.

Do not open or modify the device. Do not repair the device yourself, but replace it with an equivalent device. Repairs may only be carried out by the manufacturer. The manufacturer is not liable for damage resulting from non-compliance.

The IP20 degree of protection (IEC 60529-0/EN 60529-0) of the device is intended for use in a clean and dry environment. Do not subject the device to mechanical and/or thermal loads that exceed the specified limits.

NOTE: Observe the following safety notes when using the device.

- If the equipment is used in a not specified manner, the protection provided by the equipment may be impaired.
- The external circuits intended to be connected to this device shall be galv. separated from mains supply or hazardous live voltage by reinforced or double insulation and meet the requirements of SELV/PELV (Class III) circuit of UL/CSA/IEC 61010-1, 2-201.
- Use Copper Conductors Only, AWG 24-16, 90 °C
- The modules have to be build-in the final safety enclosure, which has adequate rigidity according to UL 61010-1, 61010-2-201 and meets the requirements with respect to spread of fire.
- When installing and operating the device, the applicable regulations and safety directives (including national safety directives), as well as general technical regulations, must be observed.
- The technical data is provided in the packing slip and on the certificates (conformity assessment, additional approvals where applicable).
- To avoid overheating, do not expose the device to direct sunlight or other heat sources.
- Clean the device housing with a soft cloth. Do not use aggressive solvents.

1.6.1 Safety notes for installation in zone 2 (only devices with Ex approval)

– The category 3 device is designed for installation in Zone 2 potentially explosive areas. It meets the requirements of EN 60079-0 and EN 60079-7.
– The device is not designed for use in atmospheres with a danger of dust explosions.
– The configuration of the device using DIP switches, buttons, or other accessible switches on the device is only permitted outside of potentially explosive areas.
– Observe the specified conditions for use in potentially explosive areas. Install the device in a suitable, approved housing with at least IP54 degree of protection that meets the requirements of IEC/EN 60079-7 and GB/T 3836.1-2021. Also observe the requirements of IEC/EN 60079-14.
– Only devices which are designed for operation in Ex zone 2 and are suitable for the conditions at the installation location may be connected to the circuits in the Ex zone. In potentially explosive areas, only disconnect and connect cables, SFP modules and the SD card when the power is disconnected.
– Only use fault-free Ethernet cables with functioning latches.

- Plug-in connections (e.g., connector, SD card) must have a functional interlock (e.g., locking clip, screw connection). Insert the interlock and repair any damaged interlocks immediately. Make sure that all plug-in connections are inserted completely.
- The device must be stopped and immediately removed from the Ex area if it is damaged, was subject to an impermissible load, stored incorrectly or if it malfunctions.
- The ambient temperature inside the end user housing must be measured within 25 mm of the device and maintained.
- Only connect one cable per terminal point.
- The air pressure during operation is limited to 108 kPa.
- Electrical isolation, 500 V AC in accordance with EN/IEC 60079-7. Observe the limitations in the specific conditions of use.
- Surge protective devices discharge interference of <500 V_{rms} between the voltage supply connections and FE. Therefore disconnect the power supply connector prior to measuring insulation. Otherwise, inaccurate insulation measurements may occur. Reinsert the plug into the socket provided once insulation measurement has been completed.

1.7 IT security

You have to protect components, networks, and systems against unauthorized access and ensure the integrity of data. As a part of this, you must take organizational and technical measures to protect network-capable devices, solutions, and PC-based software.

The use of mGuard devices in a secure environment certified according to IEC 62443-4-2 requires a corresponding configuration of the mGuard device within a defined security context. Both are described in the user manual "IEC 62443-4-2-compliant configuration of the FL MGUARD product family" (UM EN MGUARD 62443-4-2 - 109049_en_xx).

Phoenix Contact strongly recommends using an Information Security Management System (ISMS) to manage all of the infrastructure-based, organizational, and personnel measures that are needed to ensure compliance with information security directives.

In addition, Phoenix Contact recommends taking at least the following measures into account (taking into account your respective applicable security context/security concept).

Furthermore, Phoenix Contact recommends that at minimum the following measures are taken into consideration.

More detailed information on the measures described is available on the following websites (last accessed on 2025-09-15; partly only available in German):

- bsi.bund.de/it-sik.html
- ics-cert.us-cert.gov/content/recommended-practices

Use the latest firmware version

Phoenix Contact regularly provides firmware updates. Any firmware updates available can be found on the product page for the respective device.

- Ensure that the firmware on all devices used is always up to date.
- Observe the Change Notes for the respective firmware version.
-
- Pay attention to the security advisories published on Phoenix Contact‘s Product Security Incident Response Team (PSIRT) website regarding any published vulnerabilities.

Use the latest documentation

Phoenix Contact regularly provides updates of the documentation which can be found on the product page for the respective device.

- Ensure that you always use the latest device related documentation.

Assure the integrity of downloaded files

Phoenix Contact provides checksums of files that can be downloaded on the product page for the respective device.

- To ensure that the downloaded firmware or update files as well as downloaded documentation have not been modified by third parties during the download, compare the SHA256 checksums of the files with the checksums specified on the corresponding product page (phoenixcontact.com/product/<item number>).

Use up-to-date security software

- Install security software on all PCs to detect and eliminate security risks such as viruses, trojans, and other malware.
- Ensure that the security software is always up to date and uses the latest databases.
- Use whitelist tools for monitoring the device context.
- Use an Intrusion-Detection system for checking the communication within your system.

Take Defense-in-Depth strategies into consideration when planning systems

It is not sufficient to take measures that have only been considered in isolation when protecting your components, networks, and systems. Defense-in-Depth strategies encompass several coordinated measures that include operators, integrators, and manufacturers.

- Take Defense-in-Depth strategies into consideration when planning systems.

Perform regular threat analyses

- To determine whether the measures you have taken still provide adequate protection for your components, networks, and systems, threat analyses should be performed regularly.
- Perform a threat analysis on a regular basis.

Deactivate unneeded communication channels

- Deactivate unnecessary communication channels (e.g., SNMP, FTP, BootP, DCP, etc.) on the components that you are using.

Do not integrate components and systems into public networks

- Avoid integrating your components and systems into public networks.
- If you have to access your components and systems via a public network, use a VPN (Virtual Private Network).

Restrict access rights

- Avoid unauthorized persons gaining physical access to the device. Accessing the hardware of the device could allow an attacker to manipulate the security functions.
- Restrict access rights for components, networks, and systems to those individuals for whom authorization is strictly necessary.
- Deactivate unused user accounts.

Secure access

- Change the default login information after initial startup.
- Use secure passwords reflecting the complexity and service life recommended in the latest guidelines.
- Change passwords in accordance with the rules applicable for their application.
- Use a password manager with randomly generated passwords.
- Wherever possible, use a central user administration system to simplify user management and login information management.

Use secure access paths for remote access

- Use secure access paths such as VPN (Virtual Private Network) or HTTPS for remote access.

Set up a firewall

- Set up a firewall to protect your networks and the components and systems integrated into them against external influences.
- Use a firewall to segment a network or to isolate a controller.

Activate security-relevant event logging

- Activate security-relevant event logging in accordance with the security directive and the legal requirements on data protection.
- Use the "Remote logging" function via an encrypted VPN tunnel to a syslog server.

Secure access to SD cards

Devices with SD cards require protection against unauthorized physical access. An SD card can be read with a conventional SD card reader at any time. If you do not protect the SD card against unauthorized physical access (such as by using a secure control cabinet), sensitive data is accessible to all.

- Ensure that unauthorized persons do not have access to the SD card.
- When destroying the SD card, ensure that the data cannot be retrieved.

1.8 Latest security instructions for your product

Product Security Incident Response Team (PSIRT)

The Phoenix Contact PSIRT is the central team for Phoenix Contact as well as for its subsidiaries, authorized to respond to potential security vulnerabilities, incidents and other security issues related to Phoenix Contact products, solutions as well as services.

Phoenix Contact PSIRT manages the disclosure, investigation internal coordination and publishes security advisories for confirmed vulnerabilities where mitigations/fixes are available.

The PSIRT website (phoenixcontact.com/psirt) is updated regularly. In addition, Phoenix Contact recommends subscribing to the PSIRT newsletter.

Anyone can submit information on potential security vulnerabilities to the Phoenix Contact PSIRT by e-mail.

1.9 Support

For additional information on the device as well as release notes, user assistance and software updates, visit: phoenixcontact.net/product/<item number>.

In the event of problems with your device or with operating your device, please contact your supplier.

To get help quickly in the event of an error, make a snapshot of the device configuration immediately when a device error occurs, if possible. You can then provide the snapshot to the support team.

The usage of snapshots is described in this user manual.

2 Introduction

The *Generic Administration Interface's* (GAI) purpose is to provide user and system interfaces to configure the mGuard. Beside its Web and SNMP interface, GAI also provides the command line interface **gaiconfig** which is explained in this document.

gaiconfig is the command line tool to retrieve and set variables in all configuration files managed by GAI. Depending services are restarted as defined in the registry before the program exits. This command can be used by the user *admin* and *root*.

2.1 Options

Tab. 2-1 shows the most commonly used options. To get a complete list of supported options, execute *gaiconfig --help* from the command line.

Table 2-1 Most commonly used options

Option	Description
--add-row	Add a row to the current variable
--append-row	Append a row to the current variable, same as --add-row
--delete-row	Delete the current row
--delete-all-rows	Delete all rows
--get <variable>	Retrieve and print the value of a variable
--get-access <variable>	Returns the permission of the variable
--get-all	Dump configuration data as ATV to stdout
--get-all-but-private	Dump all configuration data but variables marked as private in registry to stdout
--get-all-but-default	Dump all configuration data but no variables with the default value to stdout
--get-current-path	Prints the current path (useful after goto or add-row)
--get-local <row>	Returns the "local" flag
--get-quoted <variable>	Returns the value with ATV quoting applied
--get-ref --get-reference	Returns the variable or row, the current reference is pointing to
--get-reference-list	Returns a list of references and it targets
--get-rowcount <variable>	Returns the number of rows if this is a table and an error otherwise
--get-rowid	Returns the rowid of the current row, or of the row the current variable lives in
--get-uuid <variable>	Returns the UUID of <variable> or an error if it has no UUID
--goto <variable>|<row>	Go to the specified variable/row
--help	Print help text
--insert-row	Insert a row

Table 2-1 Most commonly used options

--keep-local	Recover locally modified values after configuration
--pragma <name> <value>	Set pragma into atv. Not allowed/useful with --direct
--print	Print the currently changed variables as ATV instead of writing them to maid
--psm-install <package set name>	Install <package set name> using PSM utilities
--reboot	Reboot the device
--reset	Reset all values to their default
--rollback	Finish the current session (branch) without applying the changes
--session	Starts a new session (branch) and returns the session ID
--set <variable> <value>	Set the value of a single variable
--set-access <variable>	must-not-overwrite | may-overwrite | must-overwrite | may-append
--set-admin	Like --set-all but only sets data which cannot be modified by members of the group 'netadmin'
--set-admin-file <filename>	Like --set-admin: read all configuration data from the specified file
--set-all	Read all configuration data from stdin (when called by user 'netadmin', it will only set data which can be accessed by this user)
--set-all-file <filename>	Like --set-all: read all configuration data from the specified file
--set-file <variable> <filename>	Set the value of a single variable from the specified file
--set-reference <variable> <ROWID>	Make <variable> point to row with rowid <ROWID>
--set-refname <variable> <ROW>	Make <variable> point to row named <ROW>
--set-rowid <value>	Sets the rowid (rid) of the current row to <value>
--silent	Don't reconfigure services, just write the new configuration
--strict	Abort on error during --set-all/--set-admin
--synchronous	Stay connected after reconfiguration, even if the network is changed
--validate	Validates the changes of the current session
--vardiff	Print list of changed vars between this and the last commit

2.2 Variables

gaiconfig stores the configuration settings in two types of variables: single variables and tables.

Single variables are simply defined by their name.

For example, the internal IP address of the mGuard in router mode is stored in the single variable MY_LOCAL_IP.

MY_LOCAL_IP = 192.168.27.1

The value of this variable can be retrieved with the following command:

```
$ gaiconfig --get MY_LOCAL_IP
192.168.27.1
```

Tables have the format:

TableName.x.field, where **x** specifies the row in the table.

TableName1.x.TableName2.y.field, for a table containing another table, where **x** specifies the row in table 1 and *y* the row in table 2.

For example, additional internal IP addresses of the mGuard are stored in the table LOCAL_ALIASES.

```
LOCAL_ALIASES = {
 {
  LOCAL_NET = "255.255.255.0"
  LOCAL_IP = "192.168.2.1"
 }
 {
  LOCAL_NET = "255.255.255.0"
  LOCAL_IP = "192.168.1.1"
 }
}
```

The first entry (192.168.2.1/255.255.255.0) has the row number “0” in the table, the second entry (192.168.1.1/255.255.255.0) the row number “1”.

The IP address of the **first** entry can be changed with the following command:

```
$ gaiconfig --set LOCAL_ALIASES.0.LOCAL_IP 192.168.2.100
```

The IP address of the **second** entry can be changed with the following command:

```
$ gaiconfig --set LOCAL_ALIASES.1.LOCAL_IP 192.168.1.100
```

2.3 Examples

We have remote SSH access to an mGuard and also want to enable remote HTTPS access for the IP 62.214.150.190. Any remote access through HTTPS should be logged. For activating HTTPS remote access we need to:

– Enable HTTPS remote access.
– Specify the listening port.
– Add the firewall rules.

Enable HTTPS remote access

Check the current value:

```
$ gaiconfig --get HTTPS_REMOTE_ENABLE
no
```

Enable HTTPS remote access:

```
$ gaiconfig --set HTTPS_REMOTE_ENABLE yes
```

Verify the changes:

```
$ gaiconfig --get HTTPS_REMOTE_ENABLE
yes
```

Verify the port

Check the current value (443 is the default value):

```
$ gaiconfig --get HTTPS_REMOTE_LISTENPORT
443
```

Add firewall rules for the HTTPS remote access

The firewall rules are stored in the table HTTPS_REMOTE_ACCESS_RULES. Each row contains the following fields: *FROM_IP, INTERFACE_DEV, TARGET* and *LOG*. Default setting are *TARGET*=ACCEPT and *INTERFACE_DEV*=extern. Thus we only need to specify the IP address and set *LOG* to yes when adding a new firewall rule. This can be done step by step as well as by one single command.

Check the current value:

```
$ gaiconfig --get HTTPS_REMOTE_ACCESS_RULES
HTTPS_REMOTE_ACCESS_RULES = {
}
```

The table is empty. There do not exist any rules.

Add a row to the table:

```
$ gaiconfig --goto HTTPS_REMOTE_ACCESS_RULES --add-row
```

Verify the changes:

```
$ gaiconfig --get HTTPS_REMOTE_ACCESS_RULES
 HTTPS_REMOTE_ACCESS_RULES = {
   {
     COMMENT = ""
     FROM_IP = "0.0.0.0/0"
     FROM_MAC = "00:00:00:00:00:00"
     INTERFACE_DEV = "extern"
     LOG = "no"
     TARGET = "ACCEPT"
   }
}
```

Set the IP address:

```
$ gaiconfig --set HTTPS_REMOTE_ACCESS_RULES.0.FROM_IP
62.214.150.190/32
```

Verify the changes:

```
$ gaiconfig --get HTTPS_REMOTE_ACCESS_RULES
 HTTPS_REMOTE_ACCESS_RULES = {
   {
     COMMENT = ""
     FROM_IP = "62.214.150.190/32"
     FROM_MAC = "00:00:00:00:00:00"
     INTERFACE_DEV = "extern"
     LOG = "no"
     TARGET = "ACCEPT"
   }
}
```

Enable logging:

```
$ gaiconfig --set HTTPS_REMOTE_ACCESS_RULES.0.LOG yes
```

Verify the changes:

```
$ gaiconfig --get HTTPS_REMOTE_ACCESS_RULES
 HTTPS_REMOTE_ACCESS_RULES = {
   {
     COMMENT = ""
     FROM_IP = "62.214.150.190/32"
     FROM_MAC = "00:00:00:00:00:00"
     INTERFACE_DEV = "extern"
     LOG = "yes"
     TARGET = "ACCEPT"
   }
}
```

Instead of using the following three commands:

```
$ gaiconfig --goto HTTPS_REMOTE_ACCESS_RULES --add-row
$ gaiconfig --set HTTPS_REMOTE_ACCESS_RULES.0.FROM_IP
62.214.150.190/32
$ gaiconfig --set HTTPS_REMOTE_ACCESS_RULES.0.LOG yes
```

You can also configure the firewall with one single command:

```
$ gaiconfig --goto HTTPS_REMOTE_ACCESS_RULES --add-row \
--set .FROM_IP 62.214.150.190/32 --set .LOG yes
```

3 Nomenclature

In Section 4, the following nomenclature is used for the data format assigned to GAI variables:

Table 3-1 Nomenclature

Format	Description
<cidr>	Network/IP address in CIDR notation (192.168.1.0/24, 10.1.0.23/32)
<hex>	Hexadecimal value
<ip>	IP address (192.168.1.102)
<mac>	MAC address (00:0c:be:12:fe:01)
<netmask>	Subnet mask (255.255.255.0)
<num>	Numerical value
<txt>	Textual value
<rowref>	Reference ID of a defined row (e.g. MAI0983174920)

4 Correlation between mGuard menu options and gaiconfig variables

4.1 Management

4.1.1 System Settings

Tab: Host

Menu option	GAI variable	Format
System		
System temperature	HM_TEMP_MIN	<num>
System temperature	HM_TEMP_MAX	<num>
CPU temperature	CPU_TEMP_MIN	<num>
CPU temperature	CPU_TEMP_MAX	<num>
System use notification	SYSTEM_USE_NOTIFICATION	<txt>
Control login via on/off switch (HTTPS/SSH)	LOGIN_CONTROL	none | cmd1 | cmd2 | cmd3
System DNS Hostname		
Hostname mode	NETWORK_HOSTNAME_MODE	user | provider
Hostname	NETWORK_HOSTNAME	<txt>
Domain search path	DNSCACHE_SEARCHPATH	<txt>
SNMP Information		
System name	SYS_NAME	<txt>
Location	SYS_LOCATION	<txt>
Contact	SYS_CONTACT	<txt>

Tab: Time and Date

Menu option	GAI variable	Format
Time and Date		
Timezone in POSIX.1 notation	TIMEZONE	<txt>
Time-stamp in filesystem (2h granularity)	NTP_ENABLE_FILESTAMP	yes | no
NTP Servers		
Enable NTP time synchronization	NTP_ENABLE	yes | no
‘discard minimum1‘	NTP_RATE_LIMIT_DISABLED	yes | no
NTP server	NTP_SERVERS.x.NTP_SERVER	<ip> | <txt>
Via VPN	NTP_SERVERS.x.PREFER_VPN	yes | no
Allowed Networks for NTP Access		
From IP	NTP_ACCESS_RULES.x.FROM_IP	<cidr>

Interface	NTP_ACCESS_RULES.x.INTERFACE_DEV	intern | extern | vi-aipsec | dmz0
Action	NTP_ACCESS_RULES.x.TARGET	ACCEPT | REJECT | DROP
Comment	NTP_ACCESS_RULES.x.COMMENT	<txt>
Log	NTP_ACCESS_RULES.x.LOG	yes | no

Tab: Shell Access

Menu option	GAI variable	Format
Shell Access		
Enable SSH remote access	SSH_REMOTE_ENABLE	yes | no
Port for incoming SSH connections (remote administration only)	SSH_REMOTE_LISTENPORT	<num>
Allow SSH login as user root	SSH_ROOT_LOGIN_ENABLE	yes | no
Session timeout	SHELL_TIMEOUT	<num>
Delay between requests for a sign of life (the value 0 indicates that these messages will not be sent)	SSH_CLIENT_ALIVE_INTERVAL_SECS	<num>
Maximum number of missing signs of life	SSH_CLIENT_ALIVE_COUNT_MAX	<num>
Maximum Number of Concurrent Sessions per Role		
Admin	SSH_ADMIN_LOGIN_ALLOWED_MAX	<num>
Netadmin	SSH_NETADMIN_LOGIN_ALLOWED_MAX	<num>
Update	SSH_UPDATE_LOGIN_ALLOWED_MAX	<num>
Audit	SSH_AUDIT_LOGIN_ALLOWED_MAX	<num>
Allowed Networks		
From IP	SSH_REMOTE_ACCESS_RULES.x.FROM_IP	<cidr>
Interface	SSH_REMOTE_ACCESS_RULES.x.INTERFACE_DEV	intern | extern | vi-aipsec | dmz0
Action	SSH_REMOTE_ACCESS_RULES.x.TARGET	ACCEPT | REJECT | DROP
Comment	SSH_REMOTE_ACCESS_RULES.x.COMMENT	<txt>
Log	SSH_REMOTE_ACCESS_RULES.x.LOG	yes | no
RADIUS Authentication		
Use RADIUS authentication for shell access	RADIUS_AUTH_SHELL_ENABLE	yes | no | exclusive
X.509 Authentication		
Enable X.509 certificates for SSH access	SSH_X509_ENABLE	yes | no
SSH server certificate	SSH_SERVER_CERT_REF	Empty for "None" | <rowref>
Authentication by CA Certificate		
CA certificate	SSH_CA_CERTS.x.CERTIFICATE_REF	<rowref>
Access Permission by X.509 Subject		
X.509 subject	SSH_X509_AUTH.x.SUBJECT	<txt>

Authorized for access as	SSH_X509_AUTH.x.USER	all | root | admin | netadmin | audit | update
Authentication by Client Certificate		
Client certificate	SSH_X509_AUTH_BLOB.x.CERTIFICATE_REF	<rowref>
Authorized for access as	SSH_X509_AUTH_BLOB.x.USER	all | root | admin | netadmin | audit | update

Tab: E-Mail

Menu option	GAI variable	Format
E-Mail		
Sender address of e-mail notifications	EMAIL_FROM	<txt>
Address of the e-mail server	EMAIL_RELAY_HOST	<ip> | <txt>
Port number of the e-mail server	EMAIL_RELAY_PORT	<num>
Encryption mode for the e-mail server	EMAIL_RELAY_TLS	none | tls | starttls
SMTP user name	EMAIL_RELAY_LOGIN	<txt>
SMTP password	EMAIL_RELAY_PASSWORD	<txt>
E-Mail Notifications		
E-Mail recipient	EMAIL_NOTIFICATION.x.TO	<txt>
Event	EMAIL_NOTIFICATION.x.EVENT	Refer to Appendix Chapter 1 1
IPsec selector	EMAIL_NOTIFICATION.x.SELECTOR	Empty for "None" | <rowref>
OpenVPN selector	EMAIL_NOTIFICATION.x.SELECTOR_OPENVPN	Empty for "None" | <rowref>
Rule record selector	EMAIL_NOTIFICATION.x.SELECTOR_FW_RULESET	Empty for "None" | <rowref>
E-Mail subject	EMAIL_NOTIFICATION.x.SUBJECT	<txt>
E-Mail message	EMAIL_NOTIFICATION.x.MESSAGE	<txt>

4.1.2 Web Settings

Tab: General

Menu option	GAI variable	Format
General		
Language	WWW_LANGUAGE	auto | en | de | ja
Session timeout	WWW_TIMEOUT	<num>

Tab: Access

Menu option	GAI variable	Format
HTTPS Web Access		
Enable HTTPS remote access	HTTPS_REMOTE_ENABLE	yes | no
Remote HTTPS TCP port	HTTPS_REMOTE_LISTENPORT	<num>
HTTPS server certificate	HTTPS_SERVER_CERT_REF	Empty for "Builtin" | <rowref> |
Allowed Networks		
From IP	HTTPS_REMOTE_ACCESS_RULES.x.FROM_IP	<cidr>
Interface	HTTPS_REMOTE_ACCESS_RULES.x.INTERFACE_DEV	intern | extern | vi-aipsec | dmz0
Action	HTTPS_REMOTE_ACCESS_RULES.x.TARGET	ACCEPT | REJECT | DROP
Comment	HTTPS_REMOTE_ACCESS_RULES.x.COMMENT	<txt>
Log	HTTPS_REMOTE_ACCESS_RULES.x.LOG	yes | no
RADIUS Authentication		
Enable RADIUS authentication	RADIUS_AUTH_HTTPS_ENABLE	yes | no | exclusive
User Authentication		
User authentication method	HTTPS_AUTH_CLIENT	no | may | must
Authentication by CA Certificate		
CA certificate	HTTPS_CA_CERTS.x.CERTIFICATE_REF	<rowref>
Access Permission by X.509 Subject		
X.509 subject	HTTPS_X509_AUTH.x.SUBJECT	<txt>
Authorized for access as	HTTPS_X509_AUTH.x.USER	all | root | admin | netadmin | audit | update
Authentication by Client Certificate		
Client certificate	HTTPS_X509_AUTH_BLOB.x.CERTIFICATE_REF	<rowref>
Authorized for access as	HTTPS_X509_AUTH_BLOB.x.USER	all | root | admin | netadmin | audit | update

4.1.3 Update

Tab: Update

Menu option	GAI variable	Format
Update Servers		
Protocol	PSM_REPOSITORIES.x.PROTO	https | http | ftp | tftp
Server	PSM_REPOSITORIES.x.SERVER	<ip> | <txt>
Via VPN	PSM_REPOSITORIES.x.PREFER_VPN	yes | no
Login	PSM_REPOSITORIES.x.LOGIN	<txt>
Password	PSM_REPOSITORIES.x.PASSWORD	<txt>
Server certificate	PSM_REPOSITORIES.x.REMOTE_CERT_REF	<rowref> | ignore

4.1.4 Configuration Profiles

Tab: Configuration Profiles

Menu option	GAI variable	Format
External Configuration Storage (ECS)		
Automatically save configuration changes to the ECS	ECS_AUTOSAVE_ENABLE	yes | no
Encrypt the data on the ECS	ECS_ENCRYPTION	yes | no
Load configuration from the ECS during boot	ECS_LOAD_ON_BOOT	yes | no
Configuration Profile Signing		
Enable signed configuration profiles	PROFILE_SECURE_ONLY	yes | no
Export certificate (machine certificate used to sign configuration profiles)	PROFILE_EXPORT_CERT	Empty for "None" | <rowref>
Import certificate (certificate used to validate signature of configuration profiles)	PROFILE_IMPORT_CERT	Empty for "None" | <rowref>

4.1.5 SNMP

Tab: Query

Menu option	GAI variable	Format
Settings		
Enable SNMPv3 access	SNMP_ENABLE_V3	yes | no
Enable SNMPv1/v2 access	SNMP_ENABLE_V1	yes | no
Port for incoming SNMP connections (remote access only)	SNMP_LISTENPORT	<num>
Run SNMP agent under the permissions of the following user	SNMP_GAI_SECURITY_CONTEXT	admin | netadmin
SNMPv3 Credentials		
User name	SNMP_V3_USERNAME	<txt>
Password	SNMP_V3_PASSWORD	<txt>
SNMPv1/v2 Community		
Read-Write community	SNMP_COMMUNITY	<txt>
Read-Only community	SNMP_COMMUNITY_RO	<txt>
Allowed Networks		
From IP	SNMP_ACCESS_RULES.x.FROM_IP	<cidr>
Interface	SNMP_ACCESS_RULES.x.INTERFACE_DEV	intern | extern | viaipsec | dmz0
Action	SNMP_ACCESS_RULES.x.TARGET	ACCEPT | REJECT | DROP
Comment	SNMP_ACCESS_RULES.x.COMMENT	<txt>
Log	SNMP_ACCESS_RULES.x.LOG	yes | no

Tab: Trap

Menu option	GAI variable	Format
Basic Traps		
SNMP authentication	SNMP_AUTHENTICATION_TRAP	yes | no
Link up/down	SNMP_LINKUPDOWN_TRAP	yes | no
Coldstart	SNMP_COLDSTART_TRAP	yes | no
Admin connection attempt (SSH, HTTPS)	SNMP_TRAP_ADMIN_CONNECT	yes | no
Admin access (SSH, HTTPS)	SNMP_TRAP_ADMIN_ACCESS	yes | no
New DHCP client	SNMP_TRAP_NEW_DHCP_CLIENT	yes | no
Hardware-related Traps		
Chassis (power, signal relay)	SNMP_CHASSIS_TRAP	yes | no

Service input/CMD	SNMP_TRAP_CMD	yes | no
Agent (external config storage, temperature)	SNMP_AGENT_TRAP	yes | no
Redundancy Traps		
Status change	SNMP_TRAP_REDUNDANCY_STATE	yes | no
User Firewall Traps		
User firewall traps	SNMP_TRAP_USER_FIREWALL	yes | no
VPN Traps		
IPsec connection status changes	SNMP_TRAP_VPN_IPSEC	yes | no
L2TP connection status changes	SNMP_TRAP_VPN_L2TP	yes | no
Trap Destinations		
Destination IP	SNMP_TRAP_RECEIVERS.x.TARGET_IP	<ip>
Destination port	SNMP_TRAP_RECEIVERS.x.TARGET_PORT	<num>
Destination name	SNMP_TRAP_RECEIVERS.x.TARGET_NAME	<txt>
Destination community	SNMP_TRAP_RECEIVERS.x.TARGET_COMMUNITY	<txt>

Tab: LLDP

Menu option	GAI variable	Format
LLDP		
Enable LLDP	LLDPD_ENABLE	yes | no
LLDP on external networks	LLDPD_EXT_ADMIN_STATUS	enabledRxTx | enabledRxOnly | enabledTxOnly | disabled
LLDP on internal networks	LLDPD_INT_ADMIN_STATUS	enabledRxTx | enabledRxOnly | enabledTxOnly | disabled

4.1.6 Central Management

Tab: Configuration Pull

Menu option	GAI variable	Format
Configuration Pull		
Pull schedule	GAI_PULL_INTERVAL	-1 | 0 | -2 | 15 | 30 | 60 | 120 | 360 | 720 | 1440
Time schedule	GAI_PULL_SCHEDULE	1 | 2 | 3 | 4 | 5 | 6 | 7 | *
Hours	GAI_PULL_SCHEDULE_HOUR	<num>
Minutes	GAI_PULL_SCHEDULE_MIN	<num>
Server	GAI_PULL_HTTPS_HOST	<ip> | <txt>
Port	GAI_PULL_HTTPS_PORT	<num>
Directory	GAI_PULL_HTTPS_DIR	<txt>
Filename (if empty, the device serial number will be used)	GAI_PULL_HTTPS_FILE	<txt>
Number of times a configuration profile is ignored after it was rolled back	GAI_PULL_ROLLBACK_BLOCK	<num>
Download timeout	GAI_PULL_DLTIME	<num>
Login	GAI_PULL_HTTPS_LOGIN	<txt>
Password	GAI_PULL_HTTPS_PASSWORD	<txt>
Server certificate	GAI_PULL_HTTPS_CERT_REF	Empty for "None" | <rowref> |all

4.1.7 Service I/O

Tab: Service Contacts

Menu option	GAI variable	Format
Input/CMD 1		
Switch type connected to the input	SERVICE_SWITCH1_TYPE	button | switch
Output/ACK 1		
Monitor VPN connection or firewall rule record	SERVICE_ACK1_REF	Empty for "Off" | <rowref>
Input/CMD 2		
Switch type connected to the input	SERVICE_SWITCH2_TYPE	button | switch
Output/ACK 2		
Monitor VPN connection or firewall rule record	SERVICE_ACK2_REF	Empty for "Off" | <rowref>
Input/CMD 3		
Switch type connected to the input	SERVICE_SWITCH3_TYPE	button | switch

Tab: Alarm Output

Menu option	GAI variable	Format
General		
Operation mode	HM_RS2_SIG_RELAY_MODE	standard | manual
Manual setting	HM_RS2_SIG_RELAY_MANUAL_STATE	active | inactive
Operation Supervision		
Redundant power supply	HM_RS2_SIG_PS2_ALARM	on | off
Passwords not configured	PASSWORD_ALARM	on | off
Link supervision	SIG_ALARM_LINK	on | off
Temperature condition	HM_RS2_SIG_TEMP_ALARM	on | off
Connectivity state of redundancy	HM_RS2_SIG_CONNECTIVITY_ALARM	on | off

4.2 Network

4.2.1 Interfaces

Tab: General

Menu option	GAI variable	Format
Network Mode		
Network mode	NETWORKMODE	stealth | router
Router mode	ROUTER_MODE	static | dhcp
Cellulink mode	ROUTER_MODE_LINK	yes | no
Stealth configuration	STEALTH_MODE	autodetect | static | multi
Autodetect: ignore Net-BIOS over TCP traffic on TCP port 139	STEALTH_AUTO_IGNORE_TCP139	yes | no

Tab: Stealth

Menu option	GAI variable	Format
Stealth Management		
IP	STEALTH_MANAGE_IP	<ip>
Netmask	STEALTH_MANAGE_NET	<netmask>
Use VLAN	STEALTH_MANAGE_USE_VLAN	yes | no
VLAN ID	STEALTH_MANAGE_VLAN_ID	<num>
IP address	STEALTH_MANAGE_ALIASES.x.MANAGE_IP	<ip>
Netmask	STEALTH_MANAGE_ALIASES.x.MANAGE_NET	<netmask>
Use VLAN	STEALTH_MANAGE_ALIASES.x.USE_VLAN	yes | no
VLAN ID	STEALTH_MANAGE_ALIASES.x.VLAN_ID	<num>
Default gateway	STEALTH_MANAGE_GW	<ip>
Networks to be Routed over Alternative Gateways		
Network	STEALTH_ALT_ROUTES.x.NETWORK	<cidr>
Gateway	STEALTH_ALT_ROUTES.x.GATEWAY	<ip>
Static Stealth Settings		
Client's IP address	STEALTH_IP	<ip>
Client's MAC address	STEALTH_MAC	<mac>

Tab: External

Menu option	GAI variable	Format
External Networks		
IP address	MY_ROUTER_IP	<ip>
Netmask	MY_ROUTER_NET	<netmask>
Use VLAN	MY_ROUTER_USE_VLAN	yes | no
VLAN ID	MY_ROUTER_VLAN_ID	<num>

OSPF area	MY_ROUTER_OSPF_AREA_REF	Empty for "None" | <rowref>
IP address	EXTERN_ALIASES.x.EXTERN_IP	<ip>
Netmask	EXTERN_ALIASES.x.EXTERN_NET	<netmask>
Use VLAN	EXTERN_ALIASES.x.USE_VLAN	yes | no
VLAN ID	EXTERN_ALIASES.x.VLAN_ID	<num>
OSPF area	EXTERN_ALIASES.x.OSPF_AREA_REF	Empty for "None" | <rowref>
Additional External Routes		
Network	EXTERN_ROUTES.x.NETWORK	<cidr>
Gateway	EXTERN_ROUTES.x.GATEWAY	<ip>
Default Gateway		
IP of default gateway	DEFAULT_GW	<ip>

Tab: Internal

Menu option	GAI variable	Format
Internal Networks		
IP address	MY_LOCAL_IP	<ip>
Netmask	MY_LOCAL_NET	<netmask>
Use VLAN	MY_LOCAL_USE_VLAN	yes | no
VLAN ID	MY_LOCAL_VLAN_ID	<num>
OSPF area	MY_LOCAL_OSPF_AREA_REF	Empty for "None" | <rowref>
IP address	LOCAL_ALIASES.x.LOCAL_IP	<ip>
Netmask	LOCAL_ALIASES.x.LOCAL_NET	<netmask>
Use VLAN	LOCAL_ALIASES.x.USE_VLAN	yes | no
VLAN ID	LOCAL_ALIASES.x.VLAN_ID	<num>
OSPF area	LOCAL_ALIASES.x.OSPF_AREA_REF	Empty for "None" | <rowref>
Additional Internal Routes		
Network	LOCAL_ROUTES.x.NETWORK	<cidr>
Gateway	LOCAL_ROUTES.x.GATEWAY	<ip>

Tab: DMZ

Menu option	GAI variable	Format
DMZ Networks		
IP address	DMZ_ALIASES.x.DMZ_IP	<ip>
Netmask	DMZ_ALIASES.x.DMZ_NET	<netmask>
OSPF area	DMZ_ALIASES.x.OSPF_AREA_REF	Empty for "None" | <rowref>
Additional DMZ Routes		
Network	DMZ_ROUTES.x.NETWORK	<cidr>
Gateway	DMZ_ROUTES.x.GATEWAY	<ip>

4.2.2 Ethernet

The designation of some GAI variables has changed with version mGuard 10.3. In this manual the old designation is additionally given in brackets.

Tab: MAU Settings

Menu option	GAI variable	Format
Port Mirroring		
Port mirroring receiver	MIRROR_RECEIVER (Old designation: PORT_MIRROR_RECEIVER)	off | swp0 | swp1 | swp2
MAU Configuration		
Automatic configuration	ENABLE_ETH0_AUTONEG	yes | no
Manual configuration	ETH0_FIXEDSETTING	100fd | 100hd | 10fd | 10hd
Port on	ENABLE_ETH0_MAU	yes| no
Link supervision	ETH0_SUPERVISE	yes | no
Automatic configuration	ENABLE_ETH1_AUTONEG	yes | no
Manual configuration	ETH1_FIXEDSETTING	100fd | 100hd | 10fd | 10hd
Port on	ENABLE_ETH1_MAU	yes| no
Link supervision	ETH1_SUPERVISE	yes | no
Automatic configuration	SWITCHPORT.x.AUTONEG (Old designation: PHY_SETTING.x.AUTONEG)	autoneg | noautoneg
Manual configuration	SWITCHPORT.x.FIXEDSETTING (Old designation: PHY_SETTING.x.FIXEDSETTING)	100fd | 100hd | 10fd | 10hd
Port on	SWITCHPORT.x.POWER_UP (Old designation: PHY_SETTING.x.POWER_UP)	up | down
Port mirroring	SWITCHPORT.x.MIRROR (Old designation: PHY_SETTING.x.MIRROR)	none | ingress | egress | both
Link supervision	SWITCHPORT.x.SUPERVISE (Old designation: PHY_SETTING.x.SUPERVISE)	yes | no
Port designation: x = 0 = XF2 x = 1 = XF3 x = 2 = XF4 x = 3 = DMZ (XF5)		

Tab: Multicast

Menu option	GAI variable	Format
Static Multicast Groups		
Multicast group address	MULTICAST_GROUP.x.MAC (Old designation: STATIC_MULTICAST_GROUP.x.MAC)	<mac>
XF2	MULTICAST_GROUP.x.PORT0 (Old designation: STATIC_MULTICAST_GROUP.x.PORT0)	yes | no
XF3	MULTICAST_GROUP.x.PORT1 (Old designation: STATIC_MULTICAST_GROUP.x.PORT1)	yes | no
XF4	MULTICAST_GROUP.x.PORT2 (Old designation: STATIC_MULTICAST_GROUP.x.PORT2)	yes | no
WAN	MULTICAST_GROUP.x.INTERNAL (Old designation: STATIC_MULTICAST_GROUP.x.INTERNAL)	yes | no
General Multicast Configuration		
IGMP snooping	IGMP_SNOOP	yes | no
IGMP snoop aging	IGMP_SNOOP_AGING	<num>
IGMP query	IGMP_QUERY	off | v2
IGMP query interval	IGMP_QUERY_INTERVAL	<num>

Tab: Ethernet

Menu option	GAI variable	Format
ARP Timeout		
ARP timeout	ARP_TIMEOUT	<num>
MTU Settings		
MTU of the internal interface	MY_LOCAL_DEV_MTU	<num>
MTU of the internal interface for VLAN	MY_LOCAL_DEV_VLAN_MTU	<num>
MTU of the external interface	MY_ROUTER_DEV_MTU	<num>
MTU of the external interface for VLAN	MY_ROUTER_DEV_VLAN_MTU	<num>
MTU of the DMZ interface	MY_DMZ_DEV_MTU	<num>
MTU of the management interface	STEALTH_MTU	<num>
MTU of the management interface for VLAN	STEALTH_VLAN_MTU	<num>

4.2.3 NAT

Tab: Masquerading

Menu option	GAI variable	Format
Network Address Translation/IP Masquerading		
Outgoing on interface	FW_NAT.x.EXT_IF	ext1| dmz0 | all | int
From IP	FW_NAT.x.IN_IP	<rowref> | <ip> | <cidr>
Comment	FW_NAT.x.COMMENT	<txt>
1:1 NAT		
Real network	FW_1TO1_NAT.x.LOCAL_NET	<ip>
Virtual network	FW_1TO1_NAT.x.REMOTE_NET	<ip>
Netmask	FW_1TO1_NAT.x.MASK	<num>
Enable ARP	FW_1TO1_NAT.x.ENABLE_ARP	yes | no
Comment	FW_1TO1_NAT.x.COMMENT	<txt>

Tab: IP and Port Forwarding

Menu option	GAI variable	Format
IP and Port Forwarding		
Protocol	FW_PORTFORWARDING.x.PROTO	tcp | udp | gre
From IP	FW_PORTFORWARDING.x.SRC_IP	<rowref> | <ip> | <cidr>
From port	FW_PORTFORWARDING.x.SRC_PORT	<num> | <num>:<num> | <rowref>
Incoming on IP	FW_PORTFORWARDING.x.IN_IP	<ip> | %extern
Incoming on port	FW_PORTFORWARDING.x.IN_PORT	<num>
Redirect to IP	FW_PORTFORWARDING.x.OUT_IP	<ip>
Redirect to port	FW_PORTFORWARDING.x.OUT_PORT	<num>
Comment	FW_PORTFORWARDING.x.COMMENT	<txt>
Log	FW_PORTFORWARDING.x.LOG	yes | no

4.2.4 DNS

Tab: DNS server

Menu option	GAI variable	Format
DNS		
Servers to query	DNSCACHE_MODE	root | provider | user
User Defined DNS Servers		
IP	DNSCACHE_USER_DEFINED.x.IP	<ip>
Local Resolving of Hostnames		
Enabled	DNS_ZONE.x.ZONE_ENABLED	yes | no
Domain name	DNS_ZONE.x.DOMAIN_NAME	<txt>

Tab: DNS Records

Menu option	GAI variable	Format
Local Resolving of Hostnames		
Domain name	DNS_ZONE.x.DOMAIN_NAME	<txt>
Enabled	DNS_ZONE.x.ZONE_ENABLED	yes | no
Resolve IP addresses also	DNS_ZONE.x.AUTO_RR_PTR_ENABLED	yes | no
Hostnames		
Host	DNS_ZONE.x.RR_A.y.LABEL	<txt>
TTL (hh:mm:ss)	DNS_ZONE.x.RR_A.y.TTL	<num>
IP	DNS_ZONE.x.RR_A.y.IP	<ip>

Tab: DynDNS

Menu option	GAI variable	Format
DynDNS		
Register the mGuard at a DynDNS service	VPN_DYNIP_REGISTER	yes | no
Refresh interval	VPN_DYNIP_REGISTER_INTERVAL	<num>
DynDNS provider	VPN_DYNIP_PROVIDER	dyndns-compatible | dyndns | no-ip | freedns | easydns | dnsexit | dynu
DynDNS server	VPN_DYNIP_SERVER	<txt>
DynDNS port	VPN_DYNIP_PORT	<num>
DynDNS login	VPN_DYNIP_LOGIN	<txt>
DynDNS password	VPN_DYNIP_PASSWD	<txt>
DynDNS hostname	VPN_DYNIP_HOSTNAME	<txt>

4.2.5 DHCP

Tab: Internal DHCP

Menu option	GAI variable	Format
Mode		
DHCP mode	DHCP_INT_ENABLE	no | yes | yes-relay
DHCP Server Options		
Enable dynamic IP address pool	DHCP_INT_POOL	yes | no
DHCP lease time	DHCP_INT_LEASE_TIME	<num>
DHCP range start	DHCP_INT_START	<ip>
DHCP range end	DHCP_INT_END	<ip>
Local netmask	DHCP_INT_MASK	<netmask>
Broadcast address	DHCP_INT_BROADCAST	<ip>
Default gateway	DHCP_INT_GW	<ip>
DNS server	DHCP_INT_DNS	<ip>
WINS server	DHCP_INT_WINS	<ip>
Static Mapping		
Client MAC address	DHCP_STATIC_INT.x.MAC	<mac>
Client IP address	DHCP_STATIC_INT.x.IP	<ip>
Comment	DHCP_STATIC_INT.x.COMMENT	<txt>
Relay To		
IP	DHCP_RELAY_INT_SERVER.x.IP	<ip>
DHCP Relay Options		
Append relay agent information (option 82)	DHCP_RELAY_INT_APPEND_AGENT_INFORMATION	yes | no

Tab: External DHCP

Menu option	GAI variable	Format
Mode		
DHCP mode	DHCP_EXT_ENABLE	no | yes | yes-relay
DHCP Server Options		
Enable dynamic IP address pool	DHCP_EXT_POOL	yes | no
DHCP lease time	DHCP_EXT_LEASE_TIME	<num>
DHCP range start	DHCP_EXT_START	<ip>
DHCP range end	DHCP_EXT_END	<ip>
Local netmask	DHCP_EXT_MASK	<netmask>
Broadcast address	DHCP_EXT_BROADCAST	<ip>
Default gateway	DHCP_EXT_GW	<ip>
DNS server	DHCP_EXT_DNS	<ip>
WINS server	DHCP_EXT_WINS	<ip>

Static Mapping		
Client MAC address	DHCP_STATIC_EXT.x.MAC	<mac>
Client IP address	DHCP_STATIC_EXT.x.IP	<ip>
Comment	DHCP_STATIC_EXT.x.COMMENT	<txt>
Relay To		
IP	DHCP_RELAY_EXT_SERVER.x.IP	<ip>
DHCP Relay Options		
Append relay agent information (option 82)	DHCP_RELAY_EXT_APPEND_AGENT_INFORMATION	yes | no

Tab: DMZ DHCP

Menu option	GAI variable	Format
Mode		
Enable DHCP server on the DMZ port	DHCP_DMZ_ENABLE	yes | no
DHCP Server Options		
Enable dynamic IP address pool	DHCP_DMZ_POOL	yes | no
DHCP lease time	DHCP_DMZ_LEASE_TIME	<num>
DHCP range start	DHCP_DMZ_START	<ip>
DHCP range end	DHCP_DMZ_END	<ip>
Local netmask	DHCP_DMZ_MASK	<netmask>
Broadcast address	DHCP_DMZ_BROADCAST	<ip>
Default gateway	DHCP_DMZ_GW	<ip>
DNS server	DHCP_DMZ_DNS	<ip>
WINS server	DHCP_DMZ_WINS	<ip>
Static Mapping		
Client MAC address	DHCP_STATIC_DMZ.x.MAC	<mac>
Client IP address	DHCP_STATIC_DMZ.x.IP	<ip>
Comment	DHCP_STATIC_DMZ.x.COMMENT	<txt>

4.2.6 Proxy Settings

Tab: HTTP(S) Proxy Settings

Menu option	GAI variable	Format
HTTP(S) Proxy Settings		
Use proxy for HTTP and HTTPS (also used for VPN in TCP encapsulation)	PROXY_HTTP_ENABLE	yes | no
HTTP(S) proxy server	PROXY_HTTP_URL	<ip> | <txt>
Port	PROXY_HTTP_PORT	<num>
Proxy Authentication		
Login	PROXY_HTTP_LOGIN	<txt>
Password	PROXY_HTTP_PASSWORD	<txt>

4.2.7 Dynamic Routing

Tab: OSPF

Menu option	GAI variable	Format
Enabling		
Enable OSPF	OSPF_ENABLE	yes | no
OSPF hostname (overrides global hostname)	OSPF_HOSTNAME	<txt>
Router ID	OSPF_ROUTER_ID	<ip>
OSPF Areas		
Name	OSPF_AREA.x.NAME	<txt>
ID	OSPF_AREA.x.ID	<num> | <ip>
Stub area	OSPF_AREA.x.STUB	yes | no
Authentication	OSPF_AREA.x.AUTH	none | simple | digest
Additional Interface Settings		
Interface	OSPF_INTERFACE.x.ID	int | ext1 | dmz
Passive interface	OSPF_INTERFACE.x.PASSIVE	yes | no
Authentication (overrides authentication by area)	OSPF_INTERFACE.x.AUTH	none | digest
Simple authentication password	OSPF_INTERFACE.x.SIMPLE_KEY	<txt>
Digest key	OSPF_INTERFACE.x.DIGEST_KEY	<txt>
Digest key ID	OSPF_INTERFACE.x.DIGEST_KEY_ID	<num>
Route Redistribution		
Type	OSPF_REDISTRIBUTION.x.ROUTE_TYPE	connected | kernel
Metric	OSPF_REDISTRIBUTION.x.METRIC	<num>
Access list	OSPF_REDISTRIBUTION.x.ACCESS_LIST_REF	Empty for "None" | <rowref>

Tab: Distribution Settings

Menu option	GAI variable	Format
Access Lists		
Name	DYNROUTING_ACCESSLIST.x.NAME	<txt>

Tab: Access List Settings

Menu option	GAI variable	Format
Settings		
Name	DYNROUTING_ACCESSLIST.x.NAME	<txt>
Rules		
Permit/Deny	DYNROUTING_ACCESSLIST.x.ENTRY.y.PERMIT	permit | deny
Network	DYNROUTING_ACCESSLIST.x.ENTRY.y.NET	<cidr>

4.3 Authentication

4.3.1 Administrative Users

Tab: Passwords

Menu option	GAI variable	Format
Account: root		
Root password	ROOT_PASSWORD	<txt>
Account: admin		
Administrator password	WWW_PASSWORD	<txt>
Account: user		
User password	USER_PASSWORD	<txt>
Disable VPN until the user is authenticated via HTTPS	USER_LOGIN_REQUIRED	yes | no
Account: update		
Update password (The menu item is currently not available in the WBM. It is not possible to change the password in the WBM).	UPDATE_PASSWORD	<txt>

Tab: RADIUS Filters

Menu option	GAI variable	Format
RADIUS Filters for Administrative Access		
Group/Filter ID	RADIUS_FILTER.x.FILTER_ID	<txt>
Authorized for access as	RADIUS_FILTER.x.ROLE	admin | netadmin | audit | update

4.3.2 Firewall Users

Tab: Firewall Users

Menu option	GAI variable	Format
Users		
Enable user firewall	USERFW_ENABLE	yes | no
Enable group authentication	USERFW_GROUP_AUTH_ENABLE	yes | no
Enable/disable user firewall via on/off switch	USERFW_CONTROL	none | cmd1 | cmd2 | cmd3
User name	USERFW_USERS.x.USERNAME	<txt>
Authentication method	USERFW_USERS.x.AUTHMETHOD	radius | local
User password	USERFW_USERS.x.PLAINPASSWORD	<txt>
Access (HTTPS Authentication via)		
Interface	USERFW_INTERFACES.x.INTERFACE	int | ext1 | dmz0 | ipsec

4.3.3 RADIUS

Tab: RADIUS Servers

Menu option	GAI variable	Format
RADIUS Servers		
RADIUS timeout	RADIUS_TIMEOUT	<num>
RADIUS retries	RADIUS_RETRIES	<num>
RADIUS NAS identifier	RADIUS_NAS	<txt>
Server	RADIUS_SERVERS.x.RADSERVER	<ip> | <txt>
Via VPN	RADIUS_SERVERS.x.RAD_PREFER_VPN	yes | no
Port	RADIUS_SERVERS.x.RAD_PORT	<num>
Secret	RADIUS_SERVERS.x.RADSECRET	<txt>

4.3.4 Certificates

Tab: Certificate Settings

Menu option	GAI variable	Format
Certificate Settings		
Check the validity period of certificates and CRLs	IGNORE_CERT_TIMES	never | synced | always
Enable CRL checking	CRL_CHECKING	yes | no
CRL download interval	CRL_PULL_INTERVAL	0 | 900 | 1800 | 3600 | 7200 | 21600 | 43200 | 86400 | 30

Tab: Machine Certificates

Menu option	GAI variable	Format
Machine Certificates		
Short name	PRIVATE_CERTS.x.FRIENDLY_NAME	<txt>

Tab: CA Certificates

Menu option	GAI variable	Format
Trusted CA Certificates		
Short name	CA_CERTS.x.FRIENDLY_NAME	<txt>

Tab: Remote Certificates

Menu option	GAI variable	Format
Trusted Remote Certificates		
Short name	REMOTE_CERTS.x.FRIENDLY_NAME	<txt>

Tab: CRL

Menu option	GAI variable	Format
Certificate Revocation List (CRL)		
URL	CRL_STORE.x.URI	<txt>
Via VPN	CRL_STORE.x.PREFER_VPN	yes | no

Tab: Certificate Enrollment

Menu option	GAI variable	Format
CA Server for Certificate Renewal		
Server	CERT_ENROLL_CA_HOST	<ip> | <txt>
Port	CERT_ENROLL_CA_PORT	<num>
Directory	CERT_ENROLL_CA_DIR	<txt>
Settings		
Enrollment root CA certificate	CERT_ENROLL_CA_REF	Empty for "None" | <rowref>

Generate a new key on certificate renewal	CERT_ENROLL_KEY_UPDATE	yes | no

4.4 Network Security

4.4.1 Packet Filter

Tab: Incoming Rules

Menu option	GAI variable	Format
Incoming		
General firewall setting	FW_INCOMING_GLOBAL	accept | drop | ping | rules
Interface	FW_INCOMING.x.EXT_IF	ext1 | all
Protocol	FW_INCOMING.x.PROTO	tcp | udp | icmp | gre | all
From IP	FW_INCOMING.x.FROM_IP	<rowref> | <ip> | <cidr>
From port	FW_INCOMING.x.FROM_PORT	<num> | <num>:<num> | <rowref>
To IP	FW_INCOMING.x.IN_IP	<rowref> | <ip> | <cidr>
To port	FW_INCOMING.x.IN_PORT	<num> | <num>:<num> | <rowref>
Action	FW_INCOMING.x.TARGET_REF	<rowref> | ACCEPT | DROP | REJECT
Comment	FW_INCOMING.x.COMMENT	<txt>
Log	FW_INCOMING.x.LOG	yes | no
Log entries for unknown connection attempts	LOG_DEFAULT_INCOMING	yes | no

Tab: Outgoing Rules

Menu option	GAI variable	Format
Outgoing		
General firewall setting	FW_OUTGOING_GLOBAL	accept | drop | ping | rules
Protocol	FW_OUTGOING.x.PROTO	tcp | udp | icmp | gre | all
From IP	FW_OUTGOING.x.FROM_IP	<rowref> | <ip> | <cidr>
From port	FW_OUTGOING.x.FROM_PORT	<num> | <num>:<num> | <rowref>
To IP	FW_OUTGOING.x.IN_IP	<rowref> | <ip> | <cidr>

To port	FW_OUTGOING.x.IN_PORT	<num> | <num>:<num> | <rowref>
Action	FW_OUTGOING.x.TARGET_REF	<rowref> | ACCEPT | DROP | REJECT
Comment	FW_OUTGOING.x.COMMENT	<txt>
Log	FW_OUTGOING.x.LOG	yes | no
Log entries for unknown connection attempts	LOG_DEFAULT_OUTGOING	yes | no

Tab: DMZ

Menu option	GAI variable	Format
WAN → DMZ		
Protocol	FW_INCOMING_WAN_DMZ.x.PROTO	tcp | udp | icmp | gre | all
From IP	FW_INCOMING_WAN_DMZ.x.FROM_IP	<rowref> | <ip> | <cidr>
From port	FW_INCOMING_WAN_DMZ.x.FROM_PORT	<num> | <num>:<num> | <rowref>
To IP	FW_INCOMING_WAN_DMZ.x.IN_IP	<rowref> | <ip> | <cidr>
To port	FW_INCOMING_WAN_DMZ.x.IN_PORT	<num> | <num>:<num> | <rowref>
Action	FW_INCOMING_WAN_DMZ.x.TARGET_REF	<rowref> | ACCEPT | DROP | REJECT
Comment	FW_INCOMING_WAN_DMZ.x.COMMENT	<txt>
Log	FW_INCOMING_WAN_DMZ.x.LOG	yes | no
Log entries for unknown connection attempts	LOG_DEFAULT_INCOMING_WAN_DMZ	yes | no
DMZ → LAN		
Protocol	FW_INCOMING_DMZ_LAN.x.PROTO	tcp | udp | icmp | gre | all
From IP	FW_INCOMING_DMZ_LAN.x.FROM_IP	<rowref> | <ip> | <cidr>
From port	FW_INCOMING_DMZ_LAN.x.FROM_PORT	<num> | <num>:<num> | <rowref>
To IP	FW_INCOMING_DMZ_LAN.x.IN_IP	<rowref> | <ip> | <cidr>
To port	FW_INCOMING_DMZ_LAN.x.IN_PORT	<num> | <num>:<num> | <rowref>
Action	FW_INCOMING_DMZ_LAN.x.TARGET_REF	<rowref> | ACCEPT | DROP | REJECT
Comment	FW_INCOMING_DMZ_LAN.x.COMMENT	<txt>
Log	FW_INCOMING_DMZ_LAN.x.LOG	yes | no
Log entries for unknown connection attempts	LOG_DEFAULT_INCOMING_DMZ_LAN	yes | no
DMZ → WAN		
Protocol	FW_OUTGOING_DMZWAN.x.PROTO	tcp | udp | icmp | gre | all
From IP	FW_OUTGOING_DMZWAN.x.FROM_IP	<rowref> | <ip> | <cidr>

From port	FW_OUTGOING_DMZWAN.x.FROM_PORT	<num> | <num>:<num> | <rowref>
To IP	FW_OUTGOING_DMZWAN.x.IN_IP	<rowref> | <ip> | <cidr>
To port	FW_OUTGOING_DMZWAN.x.IN_PORT	<num> | <num>:<num> | <rowref>
Action	FW_OUTGOING_DMZWAN.x.TARGET_REF	<rowref> | ACCEPT | DROP | REJECT
Comment	FW_OUTGOING_DMZWAN.x.COMMENT	<txt>
Log	FW_OUTGOING_DMZWAN.x.LOG	yes | no
Log entries for unknown connection attempts	LOG_DEFAULT_OUTGOING_DMZ_WAN	yes | no
LAN → DMZ		
Protocol	FW_OUTGOING_LANDMZ.x.PROTO	tcp | udp | icmp | gre | all
From IP	FW_OUTGOING_LANDMZ.x.FROM_IP	<rowref> | <ip> | <cidr>
From port	FW_OUTGOING_LANDMZ.x.FROM_PORT	<num> | <num>:<num> | <rowref>
To IP	FW_OUTGOING_LANDMZ.x.IN_IP	<rowref> | <ip> | <cidr>
To port	FW_OUTGOING_LANDMZ.x.IN_PORT	<num> | <num>:<num> | <rowref>
Action	FW_OUTGOING_LANDMZ.x.TARGET_REF	<rowref> | ACCEPT | DROP | REJECT
Comment	FW_OUTGOING_LANDMZ.x.COMMENT	<txt>
Log	FW_OUTGOING_LANDMZ.x.LOG	yes | no
Log entries for unknown connection attempts	LOG_DEFAULT_OUTGOING_LAN_DMZ	yes | no

Tab: Rule Records

Menu option	GAI variable	Format
Rule Records		
Initial mode	FW_RULESETS.x.SET_ACTIVE	disabled | inactive | active
Controlling service input or VPN connection	FW_RULESETS.x.CONTROL	none | cmd1 | cmd2 | cmd3 | <rowref>
A descriptive name	FW_RULESETS.x.FRIENDLY_NAME	<txt>

Tab: Rule Record

Menu option	GAI variable	Format
General		
A descriptive name	FW_RULESETS.x.FRIENDLY_NAME	<txt>
Initial mode	FW_RULESETS.x.SET_ACTIVE	disabled | inactive | active
Controlling service input or VPN connection	FW_RULESETS.x.CONTROL	none | cmd1 | cmd2 | cmd3 | <rowref>
Use inverted control logic	FW_RULESETS.x.CONTROL_INV	yes | no
Deactivation timeout	FW_RULESETS.x.TIMEOUT	<num>
Firewall Rules		
Protocol	FW_RULESETS.x.SET.y.PROTO	tcp | udp | icmp | all
From IP	FW_RULESETS.x.SET.y.FROM_IP	<rowref> | <ip> | <cidr>
From port	FW_RULESETS.x.SET.y.FROM_PORT	<num> | <num>:<num> | <rowref>
To IP	FW_RULESETS.x.SET.y.IN_IP	<rowref> | <ip> | <cidr>
To port	FW_RULESETS.x.SET.y.IN_PORT	<num> | <num>:<num> | <rowref>
Action	FW_RULESETS.x.SET.y.TARGET_REF	<rowref> | ACCEPT | DROP | REJECT
Comment	FW_RULESETS.x.SET.y.COMMENT	<txt>
Log	FW_RULESETS.x.SET.y.LOG	yes | no

Tab: MAC Filtering

Menu option	GAI variable	Format
Incoming		
Source MAC	STEALTH_L2_FILTER_EXTERN.x.SOURCE_MAC	<mac>
Destination MAC	STEALTH_L2_FILTER_EXTERN.x.DEST_MAC	<mac>
Ethernet protocol	STEALTH_L2_FILTER_EXTERN.x.ETHERTYPE_HEX	%any | arp | ipv4 | length | <hex>
Action	STEALTH_L2_FILTER_EXTERN.x.TARGET	ACCEPT | DROP

Comment	STEALTH_L2_FILTER_EXTERN.x.COMMENT	<txt>
Outgoing		
Source MAC	STEALTH_L2_FILTER_INTERN.x.SOURCE_MAC	<mac>
Destination MAC	STEALTH_L2_FILTER_INTERN.x.DEST_MAC	<mac>
Ethernet protocol	STEALTH_L2_FILTER_INTERN.x.ETHERTYPE_HEX	%any | arp | ipv4 | length | <hex>
Action	STEALTH_L2_FILTER_INTERN.x.TARGET	ACCEPT | DROP
Comment	STEALTH_L2_FILTER_INTERN.x.COMMENT	<txt>

Tab: IP/Port Groups

Menu option	GAI variable	Format
IP Groups		
Name	FW_GROUP_IP.x.NAME	<txt>
Comment	FW_GROUP_IP.x.COMMENT	<txt>

Tab: IP Group Settings

Menu option	GAI variable	Format
Settings		
Name	FW_GROUP_IP.x.NAME	<txt>
Comment	FW_GROUP_IP.x.COMMENT	<txt>
Host name, IP, IP range or network	FW_GROUP_IP.x.ENTRY.y.IP	<ip>-<ip> | <cidr> | <txt>
Port Groups		
Name	FW_GROUP_PORT.x.NAME	<txt>
Comment	FW_GROUP_PORT.x.COMMENT	<txt>

Tab: Port Group Settings

Menu option	GAI variable	Format
Settings		
Name	FW_GROUP_PORT.x.NAME	<txt>
Comment	FW_GROUP_PORT.x.COMMENT	<txt>
Port or Port Range	FW_GROUP_PORT.x.ENTRY.y.PORT	<num> | <num>-<num>

Tab: Advanced

Menu option	GAI variable	Format
Global Filters		
Block URGENT-flagged TCP traffic	TCP_BLOCK_URG	yes | no
Consistency Checks		
Maximum size of "ping" packets (ICMP echo request)	ICMP_LENGTH_MAX	<num>

Enable TCP/UDP/ICMP consistency checks	IP_UNCLEAN_MATCH	yes | no
Allow TCP keepalive packets without TCP flags	NF_CONNTRACK_TCP_NOFLAGS_EST	yes | no
Network Modes (Router/Stealth)		
ICMP via primary external interface for the mGuard	FW_ICMP	drop | ping | all
ICMP via DMZ interface for the mGuard	FW_ICMP_DMZ0	drop | ping | all
Stealth Mode		
Allow forwarding of GVRP frames	STEALTH_ENABLE_GVRP_FORWARDING	yes | no
Allow forwarding of STP frames	STEALTH_ENABLE_STP_FORWARDING	yes | no
Allow forwarding of DHCP frames	STEALTH_ENABLE_DHCP_FORWARDING	yes | no
Connection Tracking		
Maximum table size	IP_CONNTRACK_MAX	<num>
Allow TCP connections upon SYN only (After reboot connections need to be re-established.)	FW_NEW_CONNECTIONS_UPON_SYN_ONLY	yes | no
Timeout for established TCP connections	IP_CONNTRACK_TCP_TIMEOUT_ESTABLISHED	<num>
Timeout for closed TCP connections	IP_CONNTRACK_TCP_TIMEOUT_CLOSE_WAIT	<num>
Abort existing connections upon firewall reconfiguration	FW_CONNTRACK_FLUSH	yes | no
FTP	IP_CONNTRACK_FTP	yes | no
IRC	IP_CONNTRACK_IRC	yes | no
PPTP	IP_CONNTRACK_PPTP	yes | no
H.323	IP_CONNTRACK_H323	yes | no
SIP	IP_CONNTRACK_SIP	yes | no

4.4.2 Firewall Assistant

Tab: Firewall Assistant

Menu option	GAI variable	Format
Firewall Assistant		
Enable Firewall Assistant	FWASSIST_ENABLE	yes | no

4.4.3 Deep Packet Inspection

Tab: Modbus TCP

Menu option	GAI variable	Format
Rule Records		
Name	MODBUS_RULESETS.x.FRIENDLY_NAME	<txt>

Tab: Modbus TCP Rule Record

Menu option	GAI variable	Format
Options		
Name	MODBUS_RULESETS.x.FRIENDLY_NAME	<txt>
Filter Rules		
Function code	MODBUS_RULESETS.x.SET.y.MODBUS_FUNCTION_CODE	any | <num>
PDU addresses	MODBUS_RULESETS.x.SET.y.ADDRESS_RANGE	any | <num>
Action	MODBUS_RULESETS.x.SET.y.TARGET	ACCEPT | DROP
Comment	MODBUS_RULESETS.x.SET.y.COMMENT	<txt>
Log	MODBUS_RULESETS.x.SET.y.LOG	yes | no
Log entries for unknown packets	MODBUS_RULESETS.x.LOG_DEFAULT	yes | no

Tab: OPC Inspector

Menu option	GAI variable	Format
OPC Inspector		
OPC Classic	IP_CONNTRACK_OPC	yes | no
Sanity check for OPC Classic	IP_CONNTRACK_OPC_SANITY	yes | no
Timeout for OPC Classic connection expectations	IP_CONNTRACK_OPC_TIMEOUT	<num>

4.4.4 DoS Protection

Tab: Flood Protection

Menu option	GAI variable	Format
Maximum Number of New TCP Connections (SYN)		
Outgoing	IP_SYNFLOOD_LIMIT_INT	<num>
Incoming	IP_SYNFLOOD_LIMIT_EXT	<num>
Maximum Number of Ping Frames (ICMP Echo Request)		
Outgoing	ICMP_LIMIT_INT	<num>
Incoming	ICMP_LIMIT_EXT	<num>
Maximum Number of ARP Requests or ARP Replies each		
Outgoing	ARP_LIMIT_INT	<num>
Incoming	ARP_LIMIT_EXT	<num>

4.4.5 User Firewall

Tab: User Firewall Templates

Menu option	GAI variable	Format
Enabled	USERFW_TEMPLATE.x.TEMPLATE_ENABLED	yes | no
A descriptive name	USERFW_TEMPLATE.x.TEMPLATE_NAME	<txt>

Tab: General

Menu option	GAI variable	Format
Options		
A descriptive name	USERFW_TEMPLATE.x.TEMPLATE_NAME	<txt>
Enabled	USERFW_TEMPLATE.x.TEMPLATE_ENABLED	yes | no
Comment	USERFW_TEMPLATE.x.TEMPLATE_COMMENT	<txt>
Timeout	USERFW_TEMPLATE.x.TEMPLATE_TIMEOUT	<num>
Timeout type	USERFW_TEMPLATE.x.TEMPLATE_TOUT_TYPE	static | dynamic
VPN connection	USERFW_TEMPLATE.x.VPN_CONN_REF	Empty for "None" | <rowref>

Tab: Template Users

Menu option	GAI variable	Format
Users		
User	USERFW_TEMPLATE.x.TEMPLATE_USERS.y.USERNAME	<txt>

Tab: Firewall Rules

Menu option	GAI variable	Format
Firewall Rules		
Source IP	USERFW_TEMPLATE.x.TEMPLATE_SRC_IP	<ip> | %autho-rized_ip
Protocol	USERFW_TEMPLATE.x.TEMPLATE_RULE.y.PROTO	tcp | udp | icmp | gre | all
From port	USERFW_TEMPLATE.x.TEMPLATE_RULE.y.SRC_PORT	<num> | <num>:<num> | <rowref>
To IP	USERFW_TEMPLATE.x.TEMPLATE_RULE.y.DST_IP	<rowref> | <ip> | <cidr>
To port	USERFW_TEMPLATE.x.TEMPLATE_RULE.y.DST_PORT	<num> | <num>:<num> | <rowref>
Comment	USERFW_TEMPLATE.x.TEMPLATE_RULE.y.COMMENT	<txt>
Log	USERFW_TEMPLATE.x.TEMPLATE_RULE.y.LOG	yes | no

4.5 IPsec VPN

4.5.1 Global

Tab: Options

Menu option	GAI variable	Format
Options		
Allow packet forwarding between VPN connections	VPN_HUB_AND_SPOKE	yes | no
Archive diagnostic messages for VPN connections	VPN_LOG_PERSIST_ENABLED	yes | no
Archive diagnostic messages only upon failure	VPN_LOG_PERSIST_FAILURES_ONLY	yes | no
TCP Encapsulation		
Listen for incoming VPN connections, which are encapsulated	VPN_IPTUN_ENABLE	yes | no
TCP port to listen on	VPN_IPTUN_LISTEN_PORT	<num>
Server ID (0-63)	VPN_IPTUN_POOL	<num>
Enable Path Finder for mGuard Secure VPN Client	VPN_TCPENCAP_ENABLE	yes | no
TCP port to listen on	VPN_TCPENCAP_LISTEN_PORT	<num>
IP Fragmentation		
IKE fragmentation	VPN_IKE_FRAGMENTATION	yes | no
IPsec MTU (default is 16260)	VPN_IPSEC0_MTU	<num>

Tab: DynDNS Monitoring

Menu option	GAI variable	Format
DynDNS Monitoring		
Watch hostnames of remote VPN gateways	VPN_DYNIP_WATCH	yes | no
Refresh interval	VPN_DYNIP_WATCH_INTERVAL	<num>

4.5.2 Connections

Tab: Connections

Menu option	GAI variable	Format
Connections		
Initial mode	VPN_CONNECTION.x.VPN_START	disabled | stopped | started
Name (A descriptive name for the connection)	VPN_CONNECTION.x.VPN_NAME	<txt>

Tab: General

Menu option	GAI variable	Format
Options		
A descriptive name for the connection	VPN_CONNECTION.x.VPN_NAME	<txt>
Initial mode	VPN_CONNECTION.x.VPN_START	disabled | stopped | started
Address of the remote site's VPN gateway (IP address, hostname, or '%any' for any IP, multiple clients or clients behind a NAT gateway)	VPN_CONNECTION.x.VPN_GW	<ip> | <txt> | %any
Interface to use for gateway setting %any	VPN_CONNECTION.x.INTERFACE	int | ext1 | dmz0 | byIp
IP address to use for gateway setting %any	VPN_CONNECTION.x.HOST_IP	<ip>
Connection startup	VPN_CONNECTION.x.INITIATE	yes | no | on-demand
Controlling service input	VPN_CONNECTION.x.CONTROL	none | cmd1 | cmd2 | cmd3
Use inverted control logic	VPN_CONNECTION.x.CONTROL_INV	yes | no
Deactivation timeout	VPN_CONNECTION.x.TIMEOUT_SECONDS	<num>
Encapsulate the VPN traffic in TCP	VPN_CONNECTION.x.IPTUN_ENABLE	no | yes | ncp

TCP-Port of the server, which accepts the encapsulated connection	VPN_CONNECTION.x.IPTUN_DEST_PORT	<num>
Mode Configuration		
Mode configuration	VPN_CONNECTION.x.MODECFG_XAUTH_MODE	off | server | client
Local Virtual IP	VPN_CONNECTION.x.GUI_VIRTUAL_IP	<ip>
Local	VPN_CONNECTION.x.MODECFG_SERVER_LOCAL	fixed | splitinc-static
Local IP network	VPN_CONNECTION.x.GUI_MODECFG_SERVER_LOCAL	<cidr>
Network	VPN_CONNECTION.x.MODECFG_SERVER_LOCAL_NETWORKS.y.NETWORK	<cidr>
Remote	VPN_CONNECTION.x.MODECFG_SERVER_REMOTE	pool | isplitinc-static
Remote IP network pool	VPN_CONNECTION.x.GUI_MODECFG_SERVER_REMOTE	<cidr>
Tranches of size (network size between 0 and 32)	VPN_CONNECTION.x.MODECFG_POOL_TRANCH_SIZE	<num>
Network	VPN_CONNECTION.x.MODECFG_SERVER_REMOTE_NETWORKS.y.NETWORK	<cidr>
1st DNS Server for the peer	VPN_CONNECTION.x.MODECFG_DNS1	<ip>
2nd DNS Server for the peer	VPN_CONNECTION.x.MODECFG_DNS2	<ip>
1st WINS server for the peer	VPN_CONNECTION.x.MODECFG_WINS1	<ip>
2nd WINS server for the peer	VPN_CONNECTION.x.MODECFG_WINS2	<ip>
Local NAT	VPN_CONNECTION.x.GUI_MODECFG_CLIENT_LOCAL_NAT	none | masq
Local IP network	VPN_CONNECTION.x.GUI_MODECFG_CLIENT_LOCAL_MASQ_NET	<cidr>
Remote	VPN_CONNECTION.x.MODECFG_CLIENT_REMOTE	fixed | splitinc
Remote IP network	VPN_CONNECTION.x.GUI_MODECFG_CLIENT_REMOTE	<cidr>
XAuth login	VPN_CONNECTION.x.XAUTH_LOGIN	<txt>
XAuth password	VPN_CONNECTION.x.XAUTH_PASSWORD	<txt>
Transport and Tunnel Settings		
Enabled	VPN_CONNECTION.x.TUNNEL.y.ENABLED	yes | no
Comment	VPN_CONNECTION.x.TUNNEL.y.COMMENT	<txt>
Type	VPN_CONNECTION.x.TUNNEL.y.TYPE	tunnel | transport | modecfg
Local	VPN_CONNECTION.x.TUNNEL.y.LOCAL	<cidr>
Remote	VPN_CONNECTION.x.TUNNEL.y.REMOTE	<cidr>

Virtual IP (The virtual IP which will be used by the client in Stealth mode)	VPN_CONNECTION.x.TUNNEL.y.VIRTUAL_IP	<ip>
Local NAT		
Local NAT for IPsec tunnel connections	VPN_CONNECTION.x.TUNNEL.y.LOCAL_NAT	none | 1to1nat | masq
Internal network address for local masquerading	VPN_CONNECTION.x.TUNNEL.y.LOCAL_MASQ_NET	<cidr>
Real network	VPN_CONNECTION.x.TUNNEL.y.LOCAL_N_TO_N_NAT.z.FROM_NET	<ip>
Virtual network	VPN_CONNECTION.x.TUNNEL.y.LOCAL_N_TO_N_NAT.z.TO_NET	<ip>
Netmask	VPN_CONNECTION.x.TUNNEL.y.LOCAL_N_TO_N_NAT.z.MASK	<num>
Comment	VPN_CONNECTION.x.TUNNEL.y.LOCAL_N_TO_N_NAT.z.COMMENT	<txt>
Remote NAT		
Remote NAT for IPsec tunnel connections	VPN_CONNECTION.x.TUNNEL.y.REMOTE_NAT	none | 1to1nat | masq
Internal IP address used for remote masquerading	VPN_CONNECTION.x.TUNNEL.y.REMOTE_MASQ_IP	<ip>
Network address for remote 1:1 NAT	VPN_CONNECTION.x.TUNNEL.y.REMOTE_1TO1NAT	<ip>
Protocol		
Protocol	VPN_CONNECTION.x.TUNNEL.y.PROTOCOL	icmp | tcp | udp | all
Local Port ('%all' for all ports, a number between 1 and 65535 or '%any' to accept any proposal.)	VPN_CONNECTION.x.TUNNEL.y.LOCAL_PORT	<num> | %all | %any
Remote Port ('%all' for all ports, a number between 1 and 65535 or '%any' to accept any proposal.)	VPN_CONNECTION.x.TUNNEL.y.REMOTE_PORT	<num> | %all | %any
Dynamic Routing		
Add kernel route to remote net to allow OSPF route redistribution	VPN_CONNECTION.x.TUNNEL.y.DUMMY_ROUTE	yes | no

Tab: Authentication

Menu option	GAI variable	Format
Authentication		
Authentication method	VPN_CONNECTION.x.VPN_AUTH	psk | x509
Pre-shared key (PSK)	VPN_CONNECTION.x.VPN_PSK	<txt>
ISAKMP mode (Please note that 'Aggressive Mode' is vulnerable to attacks.)	VPN_CONNECTION.x.AGGRESSIVE	no | yes
Local X.509 certificate	VPN_CONNECTION.x.LOCAL_CERT_REF	Empty for "None" | enrolled | <rowref>
Remote CA certificate	VPN_CONNECTION.x.REMOTE_CERT_REF	selfsigned | anyca | <rowref>
VPN Identifier		
Local	VPN_CONNECTION.x.LOCAL_ID	<txt>
Remote	VPN_CONNECTION.x.REMOTE_ID	<txt>

Tab: Firewall

Menu option	GAI variable	Format
Incoming		
General firewall setting	VPN_CONNECTION.x.FW_INCOMING_GLOBAL	accept | drop | ping | rules
Protocol	VPN_CONNECTION.x.FW_INCOMING.y.PROTO	tcp | udp | icmp | gre | all
From IP	VPN_CONNECTION.x.FW_INCOMING.y.FROM_IP	<rowref> | <ip> | <cidr>
From port	VPN_CONNECTION.x.FW_INCOMING.y.FROM_PORT	<num> | <num>:<num> | <rowref>
To IP	VPN_CONNECTION.x.FW_INCOMING.y.IN_IP	<rowref> | <ip> | <cidr>
To port	VPN_CONNECTION.x.FW_INCOMING.y.IN_PORT	<num> | <num>:<num> | <rowref>
Action	VPN_CONNECTION.x.FW_INCOMING.y.TARGET_REF	<rowref> | ACCEPT | DROP | REJECT
Comment	VPN_CONNECTION.x.FW_INCOMING.y.COMMENT	<txt>
Log	VPN_CONNECTION.x.FW_INCOMING.y.LOG	yes | no
Log entries for unknown connection attempts	VPN_CONNECTION.x.LOG_DEFAULT_INCOMING	yes | no
Outgoing		
General firewall setting	VPN_CONNECTION.x.FW_OUTGOING_GLOBAL	accept | drop | ping | rules
Protocol	VPN_CONNECTION.x.FW_OUTGOING.y.PROTO	tcp | udp | icmp | gre | all

From IP	VPN_CONNECTION.x.FW_OUTGOING.y.FROM_IP	<rowref> | <ip> | <cidr>
From port	VPN_CONNECTION.x.FW_OUTGOING.y.FROM_PORT	<num> | <num>:<num> | <rowref>
To IP	VPN_CONNECTION.x.FW_OUTGOING.y.IN_IP	<rowref> | <ip> | <cidr>
To port	VPN_CONNECTION.x.FW_OUTGOING.y.IN_PORT	<num> | <num>:<num> | <rowref>
Action	VPN_CONNECTION.x.FW_OUTGOING.y.TARGET_REF	<rowref> | ACCEPT | DROP | REJECT
Comment	VPN_CONNECTION.x.FW_OUTGOING.y.COMMENT	<txt>
Log	VPN_CONNECTION.x.FW_OUTGOING.y.LOG	yes | no
Log entries for unknown connection attempts	VPN_CONNECTION.x.LOG_DEFAULT_OUTGOING	yes | no

Tab: IKE Options

Menu option	GAI variable	Format
ISAKMP SA (Key Exchange)		
Encryption	VPN_CONNECTION.x.VPN_IKE_PREF.y.ALG	des | 3des | aes128 | aes192 | aes256
Hash	VPN_CONNECTION.x.VPN_IKE_PREF.y.HASH	all | md5 | sha | sha2_256 | sha2_384 | sha2_512
Diffie-Hellman	VPN_CONNECTION.x.VPN_IKE_PREF.y.DH	all | modp1024 | modp1536 | modp2048 | modp3072 | modp4096 | modp6144 | modp8192
IPsec SA (Data Exchange)		
Encryption	VPN_CONNECTION.x.VPN_IPSEC_PREF.y.ALG	des | 3des | aes128 | aes192 | aes256 | null
Hash	VPN_CONNECTION.x.VPN_IPSEC_PREF.y.HASH	all | md5 | sha1 | sha2_256 | sha2_384 | sha2_512
Perfect Forward Secrecy (PFS) (Activation recommended. The remote site must have the same entry.)	VPN_CONNECTION.x.VPN_PFS	no | yes | modp1024 | modp1536 | modp2048 | modp3072 | modp4096 | modp6144 | modp8192
Lifetimes and Limits		
ISAKMP SA lifetime	VPN_CONNECTION.x.IKELIFETIME	<num>
IPsec SA lifetime	VPN_CONNECTION.x.IPSECLIFETIME	<num>
IPsec SA traffic limit	VPN_CONNECTION.x.IPSEC_HARD_LIMIT_BYTES	<num>
Re-key margin for lifetimes (applies to ISAKMP SAs and IPsec SAs)	VPN_CONNECTION.x.REKEYMARGIN	<num>
Re-key margin for the traffic limit (applies to IPsec SAs only)	VPN_CONNECTION.x.IPSEC_REKEYMARGIN_BYTES	<num>
Re-key fuzz (applies to all re-key margins)	VPN_CONNECTION.x.REKEYFUZZ	<num>
Keying tries (0 means unlimited tries)	VPN_CONNECTION.x.KEYINGTRIES	<num>
Dead Peer Detection		
Delay between requests for a sign of life	VPN_CONNECTION.x.DPD_DELAY	<num>

Timeout for absent sign of life after which peer is assumed dead	VPN_CONNECTION.x.DPD_TIMEOUT	<num>

4.5.3 Connections IKEv2 (beta)

Tab: Connections

Menu option	GAI variable	Format
Connections		
Initial mode	IPSEC_CON.x.VPN_START	disabled | stopped | started
Name (A descriptive name for the connection)	IPSEC_CON.x.VPN_NAME	<txt>

Tab: General

Menu option	GAI variable	Format
Options		
A descriptive name for the connection	IPSEC_CON.x.VPN_NAME	<txt>
Initial mode	IPSEC_CON.x.VPN_START	disabled | stopped | started
Address of the remote site's VPN gateway (IP address, hostname, or '%any' for any IP, multiple clients or clients behind a NAT gateway)	IPSEC_CON.x.VPN_GW	<ip> | <txt> | %any
Interface to use for gateway setting %any	IPSEC_CON.x.INTERFACE	int | ext1 | dmz0 | byIp
IP address to use for gateway setting %any	IPSEC_CON.x.HOST_IP	<ip>
Connection startup	IPSEC_CON.x.INITIATE	yes | no | on-demand
Controlling service input	IPSEC_CON.x.CONTROL	none | cmd1 | cmd2 | cmd3
Use inverted control logic	IPSEC_CON.x.CONTROL_INV	yes | no
Tunnel Settings		
Enabled	IPSEC_CON.x.TUNNEL.y.ENABLED	yes | no
Comment	IPSEC_CON.x.TUNNEL.y.COMMENT	<txt>
Type	IPSEC_CON.x.TUNNEL.y.TYPE	tunnel
Local	IPSEC_CON.x.TUNNEL.y.LOCAL	<cidr>
Remote	IPSEC_CON.x.TUNNEL.y.REMOTE	<cidr>

Virtual IP (The virtual IP which will be used by the client in Stealth mode)	IPSEC_CON.x.TUNNEL.y.VIRTUAL_IP	<ip>

Tab: Authentication

Menu option	GAI variable	Format
Authentication		
Authentication method	IPSEC_CON.x.VPN_AUTH	psk | x509
Pre-shared key (PSK)	IPSEC_CON.x.VPN_PSK	<txt>
Local X.509 certificate	IPSEC_CON.x.LOCAL_CERT_REF	Empty for "None" | enrolled | <rowref>
Remote CA certificate	IPSEC_CON.x.REMOTE_CERT_REF	selfsigned | anyca | <rowref>
VPN Identifier		
Local	IPSEC_CON.x.LOCAL_ID	<txt>
Remote	IPSEC_CON.x.REMOTE_ID	<txt>

Tab: Firewall

Menu option	GAI variable	Format
Incoming		
General firewall setting	IPSEC_CON.x.FW_INCOMING_GLOBAL	accept | drop | ping | rules
Protocol	IPSEC_CON.x.FW_INCOMING.y.PROTO	tcp | udp | icmp | gre | all
From IP	IPSEC_CON.x.FW_INCOMING.y.FROM_IP	<rowref> | <ip> | <cidr>
From port	IPSEC_CON.x.FW_INCOMING.y.FROM_PORT	<num> | <num>:<num> | <rowref>
To IP	IPSEC_CON.x.FW_INCOMING.y.IN_IP	<rowref> | <ip> | <cidr>
To port	IPSEC_CON.x.FW_INCOMING.y.IN_PORT	<num> | <num>:<num> | <rowref>
Action	IPSEC_CON.x.FW_INCOMING.y.TARGET_REF	<rowref> | ACCEPT | DROP | REJECT
Comment	IPSEC_CON.x.FW_INCOMING.y.COMMENT	<txt>
Log	IPSEC_CON.x.FW_INCOMING.y.LOG	yes | no
Log entries for unknown connection attempts	IPSEC_CON.x.LOG_DEFAULT_INCOMING	yes | no
Outgoing		
General firewall setting	IPSEC_CON.x.FW_OUTGOING_GLOBAL	accept | drop | ping | rules
Protocol	IPSEC_CON.x.FW_OUTGOING.y.PROTO	tcp | udp | icmp | gre | all
From IP	IPSEC_CON.x.FW_OUTGOING.y.FROM_IP	<rowref> | <ip> | <cidr>

From port	IPSEC_CON.x.FW_OUTGOING.y.FROM_PORT	<num> | <num>:<num> | <rowref>
To IP	IPSEC_CON.x.FW_OUTGOING.y.IN_IP	<rowref> | <ip> | <cidr>
To port	IPSEC_CON.x.FW_OUTGOING.y.IN_PORT	<num> | <num>:<num> | <rowref>
Action	IPSEC_CON.x.FW_OUTGOING.y.TARGET_REF	<rowref> | ACCEPT | DROP | REJECT
Comment	IPSEC_CON.x.FW_OUTGOING.y.COMMENT	<txt>
Log	IPSEC_CON.x.FW_OUTGOING.y.LOG	yes | no
Log entries for unknown connection attempts	IPSEC_CON.x.LOG_DEFAULT_OUTGOING	yes | no

Tab: IKE Options (Tunnel settings)

Menu option	GAI variable	Format
Dead Peer Detection		
Delay between requests for a sign of life	IPSEC_CON.x.DPD_DELAY	<num>

4.5.4 L2TP over IPsec

Tab: L2TP Server

Menu option	GAI variable	Format
Settings		
Start L2TP server for IPsec/L2TP	L2TP_ENABLED	yes | no
Local IP for L2TP connections	L2TP_LOCAL	<ip>
Remote IP range start	L2TP_FROM	<ip>
Remote IP range end	L2TP_TO	<ip>

4.6 OpenVPN Client

4.6.1 Connections

Tab: Connections

Menu option	GAI variable	Format
Connections		
Initial mode	OPENVPN_CONNECTION.x.VPN_START	disabled | stopped | started
A descriptive name for the connection	OPENVPN_CONNECTION.x.VPN_NAME	<txt>

Tab: General

Menu option	GAI variable	Format
Options		
A descriptive name for the connection	OPENVPN_CONNECTION.x.VPN_NAME	<txt>
Initial mode	OPENVPN_CONNECTION.x.VPN_START	disabled | stopped | started
Controlling service input	OPENVPN_CONNECTION.x.CONTROL	none | cmd1 | cmd2 | cmd3
Use inverted control logic	OPENVPN_CONNECTION.x.CONTROL_INV	yes | no
Deactivation timeout	OPENVPN_CONNECTION.x.TIMEOUT_SECONDS	<num>
Connection		
Address of the remote site's VPN gateway (IP address or hostname)	OPENVPN_CONNECTION.x.VPN_GW	<ip> | <txt>
Protocol	OPENVPN_CONNECTION.x.PROTOCOL	tcp | udp
Local port	OPENVPN_CONNECTION.x.LOCAL_PORT	<num> | %any
Remote port	OPENVPN_CONNECTION.x.REMOTE_PORT	<num>

Tab: Tunnel Settings

Menu option	GAI variable	Format
Remote Networks		
Network	OPENVPN_CONNECTION.x.REMOTE.y.NET	<cidr>
Comment	OPENVPN_CONNECTION.x.REMOTE.y.COMMENT	<txt>
Tunnel Settings		
Learn remote routes from server	OPENVPN_CONNECTION.x.REMOTE_LEARN	yes | no
Use compression	OPENVPN_CONNECTION.x.PROTO_COMP	yes | no | adaptive | disabled
Data Encryption		

Encryption algorithm	OPENVPN_CONNECTION.x.VPN_ENCRYPTION	aes-128-cbc | aes-192-cbc | aes-256-cbc | aes-128-gcm | aes-192-gcm | aes-256-gcm
Hash algorithm (HMAC authentication)	OPENVPN_CONNECTION.x.VPN_AUTH_HMAC	sha1 | sha256 | sha512
Key renegotiation	OPENVPN_CONNECTION.x.RENEG	yes | no
Key renegotiation interval	OPENVPN_CONNECTION.x.RENEGTIME	<num>
Dead Peer Detection		
Delay between requests for a sign of life	OPENVPN_CONNECTION.x.DPD_DELAY	<num>
Timeout for absent sign of life after which peer is assumed dead	OPENVPN_CONNECTION.x.DPD_TIMEOUT	<num>

Tab: Authentication

Menu option	GAI variable	Format
Authentication		
Authentication method	OPENVPN_CONNECTION.x.VPN_AUTH	simple | x509 | x509plus
User name	OPENVPN_CONNECTION.x.LOGIN	<txt>
Password	OPENVPN_CONNECTION.x.PASSWORD	<txt>
Local X.509 certificate	OPENVPN_CONNECTION.x.LOCAL_CERT_REF	Empty for "None" | <rowref>
CA certificate (for verification of server certificate)	OPENVPN_CONNECTION.x.CA_CERT_REF	Empty for "None" | <rowref>
Pre-shared key for TLS auth	OPENVPN_CONNECTION.x.TLS_AUTH	<txt>
Key direction for TLS auth	OPENVPN_CONNECTION.x.TLS_AUTH_KEY_DIRECTION	none | dir0 | dir1

Tab: Firewall

Menu option	GAI variable	Format
Incoming		
General firewall setting	OPENVPN_CONNECTION.x.FW_INCOMING_GLOBAL	accept | drop | ping | rules
Protocol	OPENVPN_CONNECTION.x.FW_INCOMING.y.PROTO	tcp | udp | icmp | gre | all
From IP	OPENVPN_CONNECTION.x.FW_INCOMING.y.FROM_IP	<rowref> | <ip> | <cidr>
From port	OPENVPN_CONNECTION.x.FW_INCOMING.y.FROM_PORT	<num> | <num>:<num> | <rowref>
To IP	OPENVPN_CONNECTION.x.FW_INCOMING.y.IN_IP	<rowref> | <ip> | <cidr>
To port	OPENVPN_CONNECTION.x.FW_INCOMING.y.IN_PORT	<num> | <num>:<num> | <rowref>
Action	OPENVPN_CONNECTION.x.FW_INCOMING.y.TARGET_REF	<rowref> | ACCEPT | DROP | REJECT
Comment	OPENVPN_CONNECTION.x.FW_INCOMING.y.COMMENT	<txt>
Log	OPENVPN_CONNECTION.x.FW_INCOMING.y.LOG	yes | no
Log entries for unknown connection attempts	OPENVPN_CONNECTION.x.LOG_DEFAULT_INCOMING	yes | no
Outgoing		
General firewall setting	OPENVPN_CONNECTION.x.FW_OUTGOING_GLOBAL	accept | drop | ping | rules
Protocol	OPENVPN_CONNECTION.x.FW_OUTGOING.y.PROTO	tcp | udp | icmp | gre | all
From IP	OPENVPN_CONNECTION.x.FW_OUTGOING.y.FROM_IP	<rowref> | <ip> | <cidr>
From port	OPENVPN_CONNECTION.x.FW_OUTGOING.y.FROM_PORT	<num> | <num>:<num> | <rowref>
To IP	OPENVPN_CONNECTION.x.FW_OUTGOING.y.IN_IP	<rowref> | <ip> | <cidr>
To port	OPENVPN_CONNECTION.x.FW_OUTGOING.y.IN_PORT	<num> | <num>:<num> | <rowref>
Action	OPENVPN_CONNECTION.x.FW_OUTGOING.y.TARGET_REF	<rowref> | ACCEPT | DROP | REJECT
Comment	OPENVPN_CONNECTION.x.FW_OUTGOING.y.COMMENT	<txt>
Log	OPENVPN_CONNECTION.x.FW_OUTGOING.y.LOG	yes | no
Log entries for unknown connection attempts	OPENVPN_CONNECTION.x.LOG_DEFAULT_OUTGOING	yes | no

Tab: NAT

Menu option	GAI variable	Format
Local NAT		
Local NAT for OpenVPN connections	OPENVPN_CONNECTION.x.LOCAL_NAT	none | 1to1nat | masq
Virtual local network for 1:1 NAT	OPENVPN_CONNECTION.x.LOCAL	<cidr>
Local address for 1:1 NAT	OPENVPN_CONNECTION.x.LOCAL_1TO1NAT	<ip>
Network	OPENVPN_CONNECTION.x.MASQUERADE.y.NET	<cidr>
Comment	OPENVPN_CONNECTION.x.MASQUERADE.y.COMMENT	<txt>
IP and Port Forwarding		
Protocol	OPENVPN_CONNECTION.x.PORTFORWARDING.y.PROTO	tcp | udp | gre
From IP	OPENVPN_CONNECTION.x.PORTFORWARDING.y.SRC_IP	<rowref> | <ip> | <cidr>
From port	OPENVPN_CONNECTION.x.PORTFORWARDING.y.SRC_PORT	<num> | <num>:<num> | <rowref>
Incoming on port	OPENVPN_CONNECTION.x.PORTFORWARDING.y.IN_PORT	<num>
Redirect to IP	OPENVPN_CONNECTION.x.PORTFORWARDING.y.OUT_IP	<ip>
Redirect to port	OPENVPN_CONNECTION.x.PORTFORWARDING.y.OUT_PORT	<num>
Comment	OPENVPN_CONNECTION.x.PORTFORWARDING.y.COMMENT	<txt>
Log	OPENVPN_CONNECTION.x.PORTFORWARDING.y.LOG	yes | no

4.7 Redundancy

4.7.1 Firewall Redundancy

Tab: Redundancy

Menu option	GAI variable	Format
General		
Enable redundancy	REDUNDANCY_ENABLE	yes | no
Fail-over switching time	REDUNDANCY_FAILOVER_MS	1000 | 3000 | 10000
Latency before fail-over	REDUNDANCY_LATENCY_MS	<num>
Priority of this device	REDUNDANCY_PRIORITY	low | high
Passphrase for availability checks	REDUNDANCY_AVAIL_PASSWORD	<txt>
External Virtual Interfaces		
External virtual router ID	REDUNDANCY_ID_EXT	<num>
IP	REDUNDANCY_VIRT_EXT.x.IP	<ip>
Internal Virtual Interfaces		
Internal virtual router ID	REDUNDANCY_ID_INT	<num>
IP	REDUNDANCY_VIRT_INT.x.IP	<ip>
Virtual Interface		
Virtual router ID	REDUNDANCY_ID_BRIDGE	<num>
Enable virtual IP	REDUNDANCY_VIRT_BRIDGE_ENABLE	yes | no
IP	REDUNDANCY_VIRT_BRIDGE.x.IP	<ip>
Management IP Addresses of the Second Device		
IP	REDUNDANCY_BRIDGE_PEER_MANAGE.x.IP	<ip>
Interface for State Synchronization		
Interface which is used for state synchronization	REDUNDANCY_SYNCIF_ENABLE	yes | no
IP	REDUNDANCY_SYNCIF_IP	<ip>
Netmask	REDUNDANCY_SYNCIF_NET	<netmask>
Use VLAN	REDUNDANCY_SYNCIF_USE_VLAN	yes | no
VLAN ID	REDUNDANCY_SYNCIF_VLAN_ID	<num>
Disable the availability check at the external interface.	REDUNDANCY_AVAIL_EXT_DISABLE	yes | no

Tab: Connectivity Checks

Menu option	GAI variable	Format
External Interface		
Kind of check	REDUNDANCY_CHECK_MODE_EXT	none | any | all
Primary External Targets		

IP	REDUNDANCY_CHECK_HOSTS_PRIM_EXT.x.IP	<ip>
Secondary External Targets		
IP	REDUNDANCY_CHECK_HOSTS_SEC_EXT.x.IP	<ip>
Internal Interface		
Kind of check	REDUNDANCY_CHECK_MODE_INT	none | any | all
Primary Internal Targets		
IP	REDUNDANCY_CHECK_HOSTS_PRIM_INT.x.IP	<ip>
Secondary Internal Targets		
IP	REDUNDANCY_CHECK_HOSTS_SEC_INT.x.IP	<ip>

4.7.2 Ring/Network Coupling

Tab: Ring/Network Coupling

Menu option	GAI variable	Format
Settings		
Enable ring/network coupling/dual homing	L2REDUNDANCY	yes | no
Redundancy port	L2REDUNDANCY_PORT	intern | extern

4.8 Logging

4.8.1 Settings

Tab: Settings

Menu option	GAI variable	Format
Remote Logging		
Activate remote UDP logging	LOGGING_UDP_ENABLE	yes | no
Log server IP address	LOGGING_UDP_SERVER_IP	<ip>
Log server port (normally 514)	LOGGING_UDP_SERVER_PORT	<num>
Verbose Logging		
Verbose modem logging	MODEM_DEBUG	yes | no
Data Protection		
Maximum retention period for log entries (0 = unlimited)	LOGGING_MAX_DAYS	<num>

1 Appendix

1 1 E-Mail Notification Events

The following values are supported when specifying an E-Mail notification event:

- /fwrules/*/state
- /redundancy/status
- /ecs/status
- /ihal/temperature/temp_board_alarm
- /ihal/power/psu1
- /ihal/power/psu2
- /ihal/contactreason
- /ihal/contact
- /ihal/service/cmd1
- /ihal/service/cmd2
- /ihal/service/cmd3
- /vpn/con/*/armed
- /vpn/con/*/ipsec
- /openvpn/con/*/armed
- /openvpn/con/*/state

Please observe the following notes

General terms and conditions of use for technical documentation

Phoenix Contact reserves the right to alter, correct, and/or improve the technical documentation and the products described in the technical documentation at its own discretion and without giving prior notice, insofar as this is reasonable for the user. The same applies to any technical changes that serve the purpose of technical progress.

The receipt of technical documentation (in particular user documentation) does not constitute any further duty on the part of Phoenix Contact to furnish information on modifications to products and/or technical documentation. You are responsible to verify the suitability and intended use of the products in your specific application, in particular with regard to observing the applicable standards and regulations. All information made available in the technical data is supplied without any accompanying guarantee, whether expressly mentioned, implied or tacitly assumed.

In general, the provisions of the current standard Terms and Conditions of Phoenix Contact apply exclusively, in particular as concerns any warranty liability.

Phoenix Contact reserves the right to register its own intellectual property rights for the product identifications of Phoenix Contact products that are used here. Registration of such intellectual property rights by third parties is prohibited.

Other product identifications may be afforded legal protection, even where they may not be indicated as such.

How to contact us

Internet

Up-to-date information on Phoenix Contact products and our Terms and Conditions can be found on the Internet at:
phoenixcontact.com

Make sure you always use the latest documentation.
It can be downloaded at:
phoenixcontact.net/products

Subsidiaries

If there are any problems that cannot be solved using the documentation, please contact your Phoenix Contact subsidiary.
Subsidiary contact information is available at phoenixcontact.com.

Published by

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
GERMANY

PHOENIX CONTACT Development and Manufacturing, Inc.
586 Fulling Mill Road
Middletown, PA 17057
USA

Should you have any suggestions or recommendations for improvement of the contents and layout of our manuals, please send your comments to:
tecdoc@phoenixcontact.com

Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Phone: +49 5235 3-00
Fax: +49 5235 3-41200
Email: info@phoenixcontact.com
phoenixcontact.com

110193_en_07
Item No. –07