Generic Administration Interface gaiconfig User Guide mGuard 8.8

User Manual

UM EN GAICONFIG USER GUIDE

PHOENIX CONTACT
INSPIRING INNOVATIONS

User Manual

Generic Administration Interface – gaiconfig User Guide

mGuard 8.8

UM EN GAICONFIG USER GUIDE, Revision 06 2019-09-27

The Application Note is valid for mGuard firmware release 8.8.x, installed on the following devices:

FL MGUARD RS4000	FL MGUARD GT/GT
FL MGUARD RS2000	FL MGUARD CENTERPORT
FL MGUARD RS4004	FL MGUARD DELTA
FL MGUARD RS2005	FL MGUARD SMART2
TC MGUARD RS4000 3G	FL MGUARD CORE TX
TC MGUARD RS2000 3G	FL MGUARD PCI(E)4000
TC MGUARD RS4000 4G (incl. VZW and ATT)	FL MGUARD RS
TC MGUARD RS2000 4G (incl. VZW and ATT)	FL MGUARD PCI 533/266
FL MGUARD RS4000-P	FL MGUARD SMART 533/266
FL MGUARD RS4000 VPN-M	
FL MGUARD RS2000-B	

107326_en_06

Table of contents

1 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*.

1.1 Options

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

Table 1-1 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
--keep-local	Recover locally modified values after configuration

Table 1-1 Most commonly used options

--licence-reload	Let maid reload the currently installed licenses
--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

1.2 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
```

1.3 Examples

We currently 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
```

2 Nomenclature

In Section 3, the following nomenclature is used for the data format assigned to GAI variables:

Table 2-1 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)

3 Correlation between mGuard menu options and gaiconfig variables

3.1 Management

3.1.1 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>
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
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 | ext2 | dialin | viaipsec | dmz0 | viagre

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>
Audit	SSH_AUDIT_LOGIN_ALLOWED_MAX	<num>
Mobile	SSH_MOBILE_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 | ext2 | dialin | viaipsec | dmz0 | viagre
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 | mobile
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 | mobile

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 A 2
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>

3.1.2 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>
Allowed Networks		
From IP	HTTPS_REMOTE_ACCESS_RULES.x.FROM_IP	<cidr>
Interface	HTTPS_REMOTE_ACCESS_RULES.x.INTERFACE_DEV	intern | extern | ext2 | dialin | viaipsec | dmz0 | viagre
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	root | admin | netadmin | audit | user | mobile
Authentication by Client Certificate		
Client certificate	HTTPS_X509_AUTH_BLOB.x.CERTIFICATE_REF	<rowref>
Authorized for access as	HTTPS_X509_AUTH_BLOB.x.USER	root | admin | netadmin | audit | user | mobile

3.1.3 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>

3.1.4 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

3.1.5 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 | ext2 | dialin | viaipsec | dmz0 | viagre
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
Blade controller traps		
Blade status change (replug, failure) and power supply	SNMP_TRAP_BLADESTATE	yes | no
Blade reconfiguration (backup/restore)	SNMP_TRAP_BLADECONFIG	yes | no
CIFS Integrity Traps		
Successful integrity check of a CIFS share	SNMP_TRAP_AVINFO	yes | no
Failed integrity check of a CIFS share	SNMP_TRAP_AVFAIL	yes | no
Found a (suspicious) difference on a CIFS share	SNMP_TRAP_AVDETECTION	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
Mobile Network Traps		
Incoming text message and network supervision	SNMP_TRAP_GSM	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

3.1.6 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>

3.1.7 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
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
Connection state of the modem	HM_RS2_SIG_MODEM_ALARM	on | off

3.1.8 Restart

Tab: Restart

Menu option	GAI variable	Format
Reboot via Text Message		
Enable reboot via text message	REBOOT_SMS_ENABLE	yes | no
Token for reboot via text message	REBOOT_SMS_TOKEN	<txt>

3.2 Network

3.2.1 Interfaces

Tab: General

Menu option	GAI variable	Format
Network Mode		
Network mode	NETWORKMODE	stealth | router
Router mode	ROUTER_MODE	static | dhcp | pppoe | pptp | modem | modem_int | gsm
Stealth configuration	STEALTH_MODE	autodetect | static | multi
Autodetect: ignore NetBIOS 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: PPPoE

Menu option	GAI variable	Format
PPPoE		
PPPoE login	PPPOE_LOGIN	<txt>
PPPoE password	PPPOE_PASSWORD	<txt>
Request PPPoE service name	PPPOE_USE_SERVICE_NAME	yes | no
PPPoE service name	PPPOE_SERVICE_NAME	<txt>
Automatic reconnect	PPPOE_RECONNECT	yes | no
Reconnect daily at (hour)	PPPOE_RECONNECT_HOUR	<num>
Reconnect daily at (minute)	PPPOE_RECONNECT_MIN	<num>

Tab: PPTP

Menu option	GAI variable	Format
PPTP		
PPTP login	NETWORK_PPTP_LOGIN	<txt>
PPTP password	NETWORK_PPTP_PASSWORD	<txt>
Local IP mode	NETWORK_PPTP_MODEM_MODE	static | dhcp
Local IP	NETWORK_PPTP_LOCALIP	<ip>
Modem IP	NETWORK_PPTP_MODEMIP	<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>

Tab: Secondary External

Menu option	GAI variable	Format
Secondary External Interface		
Network mode	EXT2_ROUTERMODE	modem | modem_int | gsm | none
Secondary External Routes		
Operation mode	EXT2_OPERATIONMODE	permanent | fallback
Network	EXT2_ROUTE.x.NETWORK	<cidr>
Gateway	EXT2_ROUTE.x.GATEWAY	<ip> | %gateway
Secondary External Interface Probes		
Type	EXT2_PROBE.x.TYPE	icmpping | dnsping | ikeping
Destination	EXT2_PROBE.x.DESTINATION	<ip> | <txt>
Comment	EXT2_PROBE.x.COMMENT	<txt>
Probe interval	EXT2_PROBE_INTERVAL_SECONDS	<num>
Number of times all probes need to fail during subsequent runs before the secondary external interface is activated	EXT2_PROBE_FAILCOUNT	<num>
Secondary External Interface DNS		
DNS mode	EXT2_DNS_MODE	root | provider | user | none
DNS Server	EXT2_DNS_USER_DEFINED.x.IP	<ip>

3.2.2 Mobile Network

Tab: General

Menu option	GAI variable	Format
Radio Settings		
Mobile technology standard	GSM_NETWORK_TYPE	none | gsm | cdma
2G (GPRS / EDGE / 1xRTT)	GSM_NETWORK_2G	yes | no
3G (UMTS / EVDO)	GSM_NETWORK_3G	yes | no
4G (LTE)	GSM_NETWORK_4G	yes | no

Tab: SIM Settings

Menu option	GAI variable	Format
Primary SIM (SIM 1)		
Activation	GSM_SIM_ENABLE	yes | no
PIN of the SIM card	GSM_PIN	<txt>
Provider selection	GSM_SIM_PROVIDER	<num>
Manual APN selection	GSM_APN_OVERRIDE	yes | no
Access Point Name (APN) of the Provider	GSM_APN	<txt>
PPP authentication	GSM_AUTH	yes | no
PPP login	GSM_USER	<txt>
PPP password	GSM_PASS	<txt>
Secondary SIM (SIM 2)		
Activation	GSM_SIM_ENABLE2	yes | no
PIN of the SIM card	GSM_PIN2	<txt>
Provider selection	GSM_SIM_PROVIDER2	<num>
Manual APN selection	GSM_APN_OVERRIDE	yes | no
Access Point Name (APN) of the Provider	GSM_APN2	<txt>
PPP authentication	GSM_AUTH2	yes | no
PPP login	GSM_USER2	<txt>
PPP password	GSM_PASS2	<txt>
SIM Fallback		
Switch back to the primary SIM after	GSM_FALLBACK_RETURN_HOURS	<num>
SIM initialization timeout	GSM_SIM_INIT_TOUT	<num>
Mobile network registration timeout	GSM_NETWORK_REGISTER_TOUT	<num>

Tab: Connection Supervision

Menu option	GAI variable	Format
Relogin		
Daily relogin	GSM_RELOGIN	yes | no
Daily relogin at (hour)	GSM_RELOGIN_HOUR	<num>
Daily relogin at (minute)	GSM_RELOGIN_MINUTE	<num>
Mobile Network Supervision		
Probe interval	GSM_PROBE_INTERVAL_MINUTES	<num>
Number of times all probes need to fail before the mobile network connection is considered stalled	GSM_PROBE_FAILCOUNT	<num>
Type	GSM_PROBE.x.TYPE	icmpping | dnsping | ikeping
Destination	GSM_PROBE.x.DESTINATION	<ip> | <txt>
Comment	GSM_PROBE.x.COMMENT	<txt>

Tab: Mobile Network Notifications

Menu option	GAI variable	Format
Text Message Notifications		
Text message recipient number	SMS_NOTIFICATION.x.TO	<num>
Event	SMS_NOTIFICATION.x.EVENT	Refer to Appendix Chapter A 2
Selector	SMS_NOTIFICATION.x.SELECTOR	Empty for "None" | <rowref>
Selector	SMS_NOTIFICATION.x.SELECTOR_OPENVPN	Empty for "None" | <rowref>
Selector	SMS_NOTIFICATION.x.SELECTOR_FW_RULESET	Empty for "None" | <rowref>
Text message content	SMS_NOTIFICATION.x.MESSAGE	<txt>
Text Message Character Set		
Restrict outgoing text messages to basic character set	GSM_SHORT_MESSAGE_ALPHABET_RESTRICTED	yes | no

Tab: Positioning System

Menu option	GAI variable	Format
Settings		
Enable positioning engine	GPS_ENABLE	yes | no
Update system time	GPS_UPDATE_CLOCK	yes | no

3.2.3 Serial Line

Tab: Dial-out

Menu option	GAI variable	Format
PPP Dial-out Options		
Phone number to call	MODEM_PHONE	<txt>
Authentication	MODEM_AUTH	none | pap | chap
User name	MODEM_PAP_USER	<txt>
Password	MODEM_PAP_PASS	<txt>
PAP server authentication	MODEM_PAP_REQUIRE_SERVER_AUTH	yes | no
Server user name	MODEM_PAP_SERVER_USER	<txt>
Server password	MODEM_PAP_SERVER_PASS	<txt>
Local name	MODEM_CHAP_LOCAL_NAME	<txt>
Remote name	MODEM_CHAP_REMOTE_NAME	<txt>
Password for client authentication	MODEM_CHAP_SECRET	<txt>
CHAP server authentication	MODEM_CHAP_REQUIRE_SERVER_AUTH	yes | no
Password for server authentication	MODEM_CHAP_SERVER_SECRET	<txt>
Dial on demand	MODEM_DOD	yes | no
Idle timeout	MODEM_IDLE_TIMEOUT	yes | no
Idle time	MODEM_IDLE_TIMEOUT_SECONDS	<num>
Local IP	MODEM_LOCAL_IP	<ip>
Remote IP	MODEM_REMOTE_IP	<ip>
Netmask	MODEM_NETMASK	<netmask>

Tab: Dial-in

Menu option	GAI variable	Format
PPP Dial-in Options		
Modem (PPP)	SERIAL_PPP_MODEM	off | internal | external
Local IP	SERIAL_PPP_IP_LOCAL	<ip>
Remote IP	SERIAL_PPP_IP_REMOTE	<ip>
PPP login	SERIAL_PPP_LOGIN	<txt>
PPP password	SERIAL_PPP_PASSWORD	<txt>
Incoming Rules (PPP)		
Protocol	SERIAL_FW_INCOMING.x.PROTO	tcp | udp | icmp | gre | all
From IP	SERIAL_FW_INCOMING.x.FROM_IP	<cidr>
From port	SERIAL_FW_INCOMING.x.FROM_PORT	<num> | <num>:<num>
To IP	SERIAL_FW_INCOMING.x.IN_IP	<cidr>

To port	SERIAL_FW_INCOMING.x.IN_PORT	<num> | <num>:<num>
Action	SERIAL_FW_INCOMING.x.TARGET_REF	<rowref> | ACCEPT | DROP | REJECT
Comment	SERIAL_FW_INCOMING.x.COMMENT	<txt>
Log	SERIAL_FW_INCOMING.x.LOG	yes | no
Log entries for unknown connection attempts	SERIAL_FW_LOG_DEFAULT_INCOMING	yes | no
Outgoing Rules (PPP)		
Protocol	SERIAL_FW_OUTGOING.x.PROTO	tcp | udp | icmp | gre | all
From IP	SERIAL_FW_OUTGOING.x.FROM_IP	<cidr>
From port	SERIAL_FW_OUTGOING.x.FROM_PORT	<num> | <num>:<num>
To IP	SERIAL_FW_OUTGOING.x.IN_IP	<cidr>
To port	SERIAL_FW_OUTGOING.x.IN_PORT	<num> | <num>:<num>
Action	SERIAL_FW_OUTGOING.x.TARGET_REF	<rowref> | ACCEPT | DROP | REJECT
Comment	SERIAL_FW_OUTGOING.x.COMMENT	<txt>
Log	SERIAL_FW_OUTGOING.x.LOG	yes | no
Log entries for unknown connection attempts	SERIAL_FW_LOG_DEFAULT_OUTGOING	yes | no

Tab: Modem

Menu option	GAI variable	Format
External Modem		
Hardware handshake RTS/CTS	MODEM_CRTSCTS	crtscts | Empty for "Off"
Baud rate	MODEM_BAUDRATE	9600 | 19200 | 38400 | 57600
Handle modem transparently (for dial-in only)	SERIAL_TRANSPARENT	yes | no
Modem init string	MODEM_RESET_STRING	<txt>
Built-in Modem (ISDN)		
1st MSN	MODEM_ISDN_MSN1	<txt>
2nd MSN	MODEM_ISDN_MSN2	<txt>
ISDN protocol	MODEM_ISDN_PROTOCOL	0 | 1 | 2 | 4 | 5 | 6
Layer-2 protocol	MODEM_ISDN_L2PROTO	9
Built-in Modem (analog)		
Country	MODEM_ANALOG_COUNTRY	AR | AT | AU | BE | BG | BR | CA | CH | CL | CN | CY | CZ | DE | DK | EE | ES | FI | FR | GB | GR | HK | HU | ID | IE | IL | IN | IS | IT | JP | KR | LI | LT | LU | LV | MT | MX | MY | NL | NO | NZ | PH | PL | PT | RO | RU | SE | SG | SI | SK | TH | TR | TW | US | ZA
Extension line (regarding dial tone)	MODEM_ANALOG_EXTLINE	yes | no
Speaker volume (built-in speaker)	MODEM_ANALOG_VOLUME	0 | 1 | 2 | 3
Speaker control (built-in speaker)	MODEM_ANALOG_SPKRCTRL	0 | 1 | 2 | 3

Tab: Console

Menu option	GAI variable	Format
Serial Console		
Baud rate	SERIAL_BAUDRATE	9600 | 19200 | 38400 | 57600 | 115200
Hardware handshake RTS/CTS	SERIAL_CRTSCTS	crtscts | Empty for "Off"
Serial console via USB	SERIAL_CONSOLE_VIA_USB_ENABLE	yes | no

COM Server		
Type	COM_SERVER_TYPE	off | rawclient | rawserver | rfc2217
Local port	COM_SERVER_PORT	<num>
Remote IP	COM_SERVER_REMOTE_IP	<ip>
Remote port	COM_SERVER_REMOTE_PORT	<num>
Via VPN	COM_SERVER_PREFER_VPN	yes | no
Serial parameters	SERIAL_PARAMS	8n1 | 8e1 | 8o1 | 8n2 | 8e2 | 8o2 | 7n1 | 7e1 | 7o1 | 7n2 | 7e2 | 7o2
COM Server Allowed Networks		
From IP	COM_SERVER_ACCESS_RULES.x.FROM_IP	<cidr>
Interface	COM_SERVER_ACCESS_RULES.x.INTERFACE_DEV	intern | extern | ext2 | dialin | viaipsec | dmz0 | viagre
Action	COM_SERVER_ACCESS_RULES.x.TARGET	ACCEPT | REJECT | DROP
Comment	COM_SERVER_ACCESS_RULES.x.COMMENT	<txt>
Log	COM_SERVER_ACCESS_RULES.x.LOG	yes | no

3.2.4 Ethernet

Tab: MAU Settings

Menu option	GAI variable	Format
Port Mirroring		
Port mirroring receiver	PORT_MIRROR_RECEIVER	off | swp2 | swp0 | swp1 | swp3 | swp4
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	PHY_SETTING.x.AUTONEG	autoneg | noautoneg
Manual configuration	PHY_SETTING.x.FIXEDSETTING	100fd | 100hd | 10fd | 10hd
Port on	PHY_SETTING.x.POWER_UP	up | down
Port mirroring	PHY_SETTING.x.MIRROR	none | ingress | egress | both
Link supervision	PHY_SETTING.x.SUPERVISE	yes | no
LAN1: x=2 LAN2: x=0 LAN3: x=1 LAN4: x=3 DMZ: x=4		

Tab: Multicast

Menu option	GAI variable	Format
Static Multicast Groups		
Multicast group address	STATIC_MULTICAST_GROUP.x.MAC	<mac>
LAN1	STATIC_MULTICAST_GROUP.x.PORT2	yes | no
LAN2	STATIC_MULTICAST_GROUP.x.PORT0	yes | no
LAN3	STATIC_MULTICAST_GROUP.x.PORT1	yes | no
LAN4	STATIC_MULTICAST_GROUP.x.PORT3	yes | no
LAN5	STATIC_MULTICAST_GROUP.x.PORT4	yes | no
WAN	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 | v1 | 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>

3.2.5 NAT

Tab: Masquerading

Menu option	GAI variable	Format
Network Address Translation/IP Masquerading		
Outgoing on interface	FW_NAT.x.EXT_IF	ext1 | ext2 | 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

3.2.6 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>

3.2.7 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>

3.2.8 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
Secondary external interface uses proxy	EXT2_USE_PROXY	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>

3.2.9 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>

3.2.10 GRE Tunnel

Tab: GRE Tunnel

Menu option	GAI variable	Format
Local endpoint	GRE_TUNNEL.x.TUNNEL_SRC	<ip>
Remote endpoint	GRE_TUNNEL.x.TUNNEL_DST	<ip>
Use IPsec VPN connection for securing the tunnel	GRE_TUNNEL.x.VPN_CONNECTION_REF	Empty for "Ignore" | <rowref>

Tab: General

Menu option	GAI variable	Format
Options		
Local endpoint	GRE_TUNNEL.x.TUNNEL_SRC	<ip>
Remote endpoint	GRE_TUNNEL.x.TUNNEL_DST	<ip>
Use IPsec VPN connection for securing the tunnel	GRE_TUNNEL.x.VPN_CONNECTION_REF	Empty for "Ignore" | <rowref>
Routes to Tunnel		
Network	GRE_TUNNEL.x.ROUTES.y.NETWORK	<cidr>
Dynamic Routing		
OSPF area	GRE_TUNNEL.x.OSPF_AREA_REF	Empty for "None" | <rowref>
OSPF metric	GRE_TUNNEL.x.OSPF_METRIC	<num>
Local interface IP (needed for OSPF routing)	GRE_TUNNEL.x.INTERFACE_IP	<ip>
Local interface mask (needed for OSPF routing)	GRE_TUNNEL.x.INTERFACE_MASK	<netmask>

Tab: Firewall

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

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

3.3 Authentication

3.3.1 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 HTTP	USER_LOGIN_REQUIRED	yes | no
Account: mobile		
Mobile password	MOBILE_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

3.3.2 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
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 | ext2 | dmz0 | ipsec | dial-in

3.3.3 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>

3.3.4 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

3.4 Network Security

3.4.1 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 | ext2 | 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
Token for text message trigger	FW_RULESETS.x.SMS_TOKEN	<txt>
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/PPTP/PPPoE)		
ICMP via primary external interface for the mGuard	FW_ICMP	drop | ping | all
ICMP via secondary external interface for the mGuard	FW_ICMP_EXT2	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

3.4.2 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>

3.4.3 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>

3.4.4 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> | %authorized_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

3.5 CIFS Integrity Monitoring

3.5.1 Importable Shares

Tab: Importable Shares

Menu option	GAI variable	Format
Importable CIFS Shares		
Name	CIFS_SHARE.x.NAME	<txt>
Address of the server	CIFS_SHARE.x.FROM_SERVER	<ip> | <txt>
Imported share's name	CIFS_SHARE.x.SHARE_NAME	<txt>

Tab: Importable Share

Menu option	GAI variable	Format
Identification for Reference		
Name	CIFS_SHARE.x.NAME	<txt>
Location of the Importable Share		
Address of the server	CIFS_SHARE.x.FROM_SERVER	<ip> | <txt>
Imported share's name	CIFS_SHARE.x.SHARE_NAME	<txt>
Authentication for Mounting the Share		
Domain/Workgroup	CIFS_SHARE.x.WORKGROUP	<txt>
NetBIOS name (Windows 95/98 only)	CIFS_SHARE.x.NETBIOSNAME	<txt>
Login	CIFS_SHARE.x.USER	<txt>
Password	CIFS_SHARE.x.PASSWORD	<txt>

3.5.2 CIFS Integrity Checking

Tab: Settings

Menu option	GAI variable	Format
General		
Integrity certificate (Machine certificate used to sign integrity databases)	CIFS_INTEGRITY_CERT	Empty for "None" | <rowref>
Send notifications via e-mail	CIFS_INTEGRITY_EMAIL_NOTIFY	off | just-fails-diffs | always
Target address for e-mail notifications	CIFS_INTEGRITY_EMAIL_TO	<txt>
Subject prefix for e-mail notifications	CIFS_INTEGRITY_EMAIL_SUBJECT	<txt>
Checking of Shares		
Enabled	CIFS_FILE_CHECK.x.ENABLED	yes | no | suspended
Checked CIFS share	CIFS_FILE_CHECK.x.SCANNED_SHARE	<rowref>
To be stored on CIFS share	CIFS_FILE_CHECK.x.CHECKSUM_SHARE	<rowref>

Tab: Checked Share

Menu option	GAI variable	Format
Settings		
Enabled	CIFS_FILE_CHECK.x.ENABLED	yes | no | suspended
Checked CIFS share	CIFS_FILE_CHECK.x.SCANNED_SHARE	<rowref>
Patterns for filenames	CIFS_FILE_CHECK.x.PATTERNS	<rowref>
Time schedule	CIFS_FILE_CHECK.x.SCHEDULE	7 | 1 | 2 | 3 | 4 | 5 | 6 | * | h | c
Every	CIFS_FILE_CHECK.x.SCHEDULE_INTERVAL_HOURS	1 | 2 | 3 | 4 | 6 | 8 | 12
Start at (hour)	CIFS_FILE_CHECK.x.SCHEDULE_HOUR	<num>
Start at (minute)	CIFS_FILE_CHECK.x.SCHEDULE_MIN	<num>
Maximum time a check may take	CIFS_FILE_CHECK.x.MAX_DURATION_MINUTES	<num>
Checksum Memory		
Checksum algorithm	CIFS_FILE_CHECK.x.CHECKSUM_ALGO	md5 | sha | sha256
To be stored on CIFS share	CIFS_FILE_CHECK.x.CHECKSUM_SHARE	<rowref>
Basename of the checksum files (may be prefixed with a directory)	CIFS_FILE_CHECK.x.CHECKSUM_FILE_BASE	<txt>

Tab: Filename Patterns

Menu option	GAI variable	Format
Sets of Filename Patterns		
Name	CHECK_PATTERN_SET.x.NAME	<txt>

Tab: Set of Filename Patterns

Menu option	GAI variable	Format
Settings		
Name	CHECK_PATTERN_SET.x.NAME	<txt>
Rules for Files to Check		
Filename pattern	CHECK_PATTERN_SET.x.SET.y.PATTERN	<txt>
Include in check	CHECK_PATTERN_SET.x.SET.y.CHECK	yes | no

3.6 IPsec VPN

3.6.1 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>

3.6.2 Connections

Tab: Connections

Menu option	GAI variable	Format
Connections		
Initial mode	VPN_CONNECTION.x.VPN_START	disabled | stopped | started
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 | ext2 | dialin | dmz0 | bylp
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>
Token for text message trigger	VPN_CONNECTION.x.SMS_TOKEN	<txt>
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>
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>
Remote	VPN_CONNECTION.x.TUNNEL.y.REMOTE	<cidr>
Remote NAT for IPsec tunnel connections	VPN_CONNECTION.x.TUNNEL.y.REMOTE_NAT	none | 1to1nat | masq
Network address for remote 1:1 NAT	VPN_CONNECTION.x.TUNNEL.y.REMOTE_1TO1NAT	<ip>
Internal IP address used for remote masquerading	VPN_CONNECTION.x.TUNNEL.y.REMOTE_MASQ_IP	<ip>
The virtual IP which will be used by the client in Stealth mode	VPN_CONNECTION.x.TUNNEL.y.VIRTUAL_IP	<ip>

Tab: General

Menu option	GAI variable	Format
Options		
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>
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>

3.6.3 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>

3.7 OpenVPN Client

3.7.1 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>
Token for text message trigger	OPENVPN_CONNECTION.x.SMS_TOKEN	<txt>
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	bf-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc
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

3.8 QoS

3.8.1 Ingress Filters

Tab: Internal

Menu option	GAI variable	Format
Enabling		
Enable Ingress QoS	QOS_INGRESS_LOCAL_ENABLE	yes | no
Measurement unit	QOS_INGRESS_LOCAL_UNIT	kbit_per_sec | packet_per_sec
Filters		
Use VLAN	QOS_INGRESS_LOCAL_FILTERS.x.USE_VLAN	yes | no
VLAN ID	QOS_INGRESS_LOCAL_FILTERS.x.VLAN_ID	<num>
Ethernet protocol	QOS_INGRESS_LOCAL_FILTERS.x.ETHERTYPE_HEX	%any | arp | ipv4 | length | <hex>
IP protocol	QOS_INGRESS_LOCAL_FILTERS.x.PROTO	icmp | tcp | udp | esp | all
From IP	QOS_INGRESS_LOCAL_FILTERS.x.FROM_IP	<cidr>
To IP	QOS_INGRESS_LOCAL_FILTERS.x.IN_IP	<cidr>
Current TOS/DSCP	QOS_INGRESS_LOCAL_FILTERS.x.FIND_TOSDSCP	Refer to Appendix Chapter A 1
Guaranteed	QOS_INGRESS_LOCAL_FILTERS.x.MIN_RATE	<num>
Upper limit	QOS_INGRESS_LOCAL_FILTERS.x.MAX_RATE	<num>
Comment	QOS_INGRESS_LOCAL_FILTERS.x.COMMENT	<txt>

Tab: External

Menu option	GAI variable	Format
Enabling		
Enable Ingress QoS	QOS_INGRESS_EXTERN_ENABLE	yes | no
Measurement unit	QOS_INGRESS_EXTERN_UNIT	kbit_per_sec | packet_per_sec
Filters		
Use VLAN	QOS_INGRESS_EXTERN_FILTERS.x.USE_VLAN	yes | no
VLAN ID	QOS_INGRESS_EXTERN_FILTERS.x.VLAN_ID	<num>
Ethernet protocol	QOS_INGRESS_EXTERN_FILTERS.x.ETHERTYPE_HEX	%any | arp | ipv4 | length | <hex>
IP protocol	QOS_INGRESS_EXTERN_FILTERS.x.PROTO	icmp | tcp | udp | esp | all
From IP	QOS_INGRESS_EXTERN_FILTERS.x.FROM_IP	<cidr>
To IP	QOS_INGRESS_EXTERN_FILTERS.x.IN_IP	<cidr>
Current TOS/DSCP	QOS_INGRESS_EXTERN_FILTERS.x.FIND_TOSDSCP	Refer to Appendix Chapter A 1
Guaranteed	QOS_INGRESS_EXTERN_FILTERS.x.MIN_RATE	<num>

Upper limit	QOS_INGRESS_EXTERN_FILTERS.x.MAX_RATE	<num>
Comment	QOS_INGRESS_EXTERN_FILTERS.x.COMMENT	<txt>

3.8.2 Egress Queues

Tab: Internal

Menu option	GAI variable	Format
Enabling		
Enable Egress QoS	QOS_EGRESS_LOCAL_ENABLE	yes | no
Total Bandwidth/Rate		
Bandwidth	QOS_EGRESS_LOCAL_RATE	<num>
Measurement unit	QOS_EGRESS_LOCAL_UNIT	kbit_per_sec | packet_per_sec
Queues		
Name	QOS_EGRESS_LOCAL_QUEUES.x.NAME	<txt>
Guaranteed	QOS_EGRESS_LOCAL_QUEUES.x.MIN_RATE	<num>
Upper limit	QOS_EGRESS_LOCAL_QUEUES.x.MAX_RATE	<num>
Priority	QOS_EGRESS_LOCAL_QUEUES.x.PREFERENCE	low | medium | high
Comment	QOS_EGRESS_LOCAL_QUEUES.x.COMMENT	<txt>

Tab: External

Menu option	GAI variable	Format
Enabling		
Enable Egress QoS	QOS_EGRESS_EXTERN_ENABLE	yes | no
Total Bandwidth/Rate		
Bandwidth	QOS_EGRESS_EXTERN_RATE	<num>
Measurement unit	QOS_EGRESS_EXTERN_UNIT	kbit_per_sec | packet_per_sec
Queues		
Name	QOS_EGRESS_EXTERN_QUEUES.x.NAME	<txt>
Guaranteed	QOS_EGRESS_EXTERN_QUEUES.x.MIN_RATE	<num>
Upper limit	QOS_EGRESS_EXTERN_QUEUES.x.MAX_RATE	<num>
Priority	QOS_EGRESS_EXTERN_QUEUES.x.PREFERENCE	low | medium | high
Comment	QOS_EGRESS_EXTERN_QUEUES.x.COMMENT	<txt>

Tab: External 2

Menu option	GAI variable	Format
Enabling		
Enable Egress QoS	QOS_EGRESS_EXTERN2_ENABLE	yes | no
Total Bandwidth/Rate		
Bandwidth	QOS_EGRESS_EXTERN2_RATE	<num>
Measurement unit	QOS_EGRESS_EXTERN2_UNIT	kbit_per_sec | packet_per_sec
Queues		
Name	QOS_EGRESS_EXTERN2_QUEUES.x.NAME	<txt>

Guaranteed	QOS_EGRESS_EXTERN2_QUEUES.x.MIN_RATE	<num>
Upper limit	QOS_EGRESS_EXTERN2_QUEUES.x.MAX_RATE	<num>
Priority	QOS_EGRESS_EXTERN2_QUEUES.x.PREFERENCE	low | medium | high
Comment	QOS_EGRESS_EXTERN2_QUEUES.x.COMMENT	<txt>

Tab: Dial-in

Menu option	GAI variable	Format
Enabling		
Enable Egress QoS	QOS_EGRESS_DIALIN_ENABLE	yes | no
Total Bandwidth/Rate		
Bandwidth	QOS_EGRESS_DIALIN_RATE	<num>
Measurement unit	QOS_EGRESS_DIALIN_UNIT	kbit_per_sec | packet_per_sec
Queues		
Name	QOS_EGRESS_DIALIN_QUEUES.x.NAME	<txt>
Guaranteed	QOS_EGRESS_DIALIN_QUEUES.x.MIN_RATE	<num>
Upper limit	QOS_EGRESS_DIALIN_QUEUES.x.MAX_RATE	<num>
Priority	QOS_EGRESS_DIALIN_QUEUES.x.PREFERENCE	low | medium | high
Comment	QOS_EGRESS_DIALIN_QUEUES.x.COMMENT	<txt>

3.8.3 Egress Rules

Tab: Internal

Menu option	GAI variable	Format
Default		
Default queue	QOS_EGRESS_LOCAL_DEFAULT	<rowref>
Rules		
Protocol	QOS_EGRESS_LOCAL_RULES.x.PROTO	icmp | tcp | udp | esp | all
From IP	QOS_EGRESS_LOCAL_RULES.x.FROM_IP	<cidr>
From port	QOS_EGRESS_LOCAL_RULES.x.FROM_PORT	<num> | <num>:<num>
To IP	QOS_EGRESS_LOCAL_RULES.x.IN_IP	<cidr>
To port	QOS_EGRESS_LOCAL_RULES.x.IN_PORT	<num> | <num>:<num>
Current TOS/DSCP	QOS_EGRESS_LOCAL_RULES.x.FIND_TOSDSCP	Refer to Appendix Chapter A 1
New TOS/DSCP	QOS_EGRESS_LOCAL_RULES.x.SET_TOSDSCP	Refer to Appendix Chapter A 1
Queue name	QOS_EGRESS_LOCAL_RULES.x.QUEUE	<rowref>
Comment	QOS_EGRESS_LOCAL_RULES.x.COMMENT	<txt>

Tab: External

Menu option	GAI variable	Format
Default		
Default queue	QOS_EGRESS_EXTERN_DEFAULT	<rowref>
Rules		
Protocol	QOS_EGRESS_EXTERN_RULES.x.PROTO	icmp | tcp | udp | esp | all
From IP	QOS_EGRESS_EXTERN_RULES.x.FROM_IP	<cidr>
From port	QOS_EGRESS_EXTERN_RULES.x.FROM_PORT	<num> | <num>:<num>
To IP	QOS_EGRESS_EXTERN_RULES.x.IN_IP	<cidr>
To port	QOS_EGRESS_EXTERN_RULES.x.IN_PORT	<num> | <num>:<num>
Current TOS/DSCP	QOS_EGRESS_EXTERN_RULES.x.FIND_TOSDSCP	Refer to Appendix Chapter A 1
New TOS/DSCP	QOS_EGRESS_EXTERN_RULES.x.SET_TOSDSCP	Refer to Appendix Chapter A 1
Queue name	QOS_EGRESS_EXTERN_RULES.x.QUEUE	<rowref>
Comment	QOS_EGRESS_EXTERN_RULES.x.COMMENT	<txt>

Tab: External 2

Menu option	GAI variable	Format
Default		
Default queue	QOS_EGRESS_EXTERN2_DEFAULT	<rowref>
Rules		
Protocol	QOS_EGRESS_EXTERN2_RULES.x.PROTO	icmp | tcp | udp | esp | all
From IP	QOS_EGRESS_EXTERN2_RULES.x.FROM_IP	<cidr>
From port	QOS_EGRESS_EXTERN2_RULES.x.FROM_PORT	<num> | <num>:<num>
To IP	QOS_EGRESS_EXTERN2_RULES.x.IN_IP	<cidr>
To port	QOS_EGRESS_EXTERN2_RULES.x.IN_PORT	<num> | <num>:<num>
Current TOS/DSCP	QOS_EGRESS_EXTERN2_RULES.x.FIND_TOSDSCP	Refer to Appendix Chapter A 1
New TOS/DSCP	QOS_EGRESS_EXTERN2_RULES.x.SET_TOSDSCP	Refer to Appendix Chapter A 1
Queue name	QOS_EGRESS_EXTERN2_RULES.x.QUEUE	<rowref>
Comment	QOS_EGRESS_EXTERN2_RULES.x.COMMENT	<txt>

Tab: Dial-in

Menu option	GAI variable	Format
Default		
Default queue	QOS_EGRESS_DIALIN_DEFAULT	<rowref>
Rules		
Protocol	QOS_EGRESS_DIALIN_RULES.x.PROTO	icmp | tcp | udp | esp | all
From IP	QOS_EGRESS_DIALIN_RULES.x.FROM_IP	<cidr>
From port	QOS_EGRESS_DIALIN_RULES.x.FROM_PORT	<num> | <num>:<num>
To IP	QOS_EGRESS_DIALIN_RULES.x.IN_IP	<cidr>
To port	QOS_EGRESS_DIALIN_RULES.x.IN_PORT	<num> | <num>:<num>
Current TOS/DSCP	QOS_EGRESS_DIALIN_RULES.x.FIND_TOSDSCP	Refer to Appendix Chapter A 1
New TOS/DSCP	QOS_EGRESS_DIALIN_RULES.x.SET_TOSDSCP	Refer to Appendix Chapter A 1
Queue name	QOS_EGRESS_DIALIN_RULES.x.QUEUE	<rowref>
Comment	QOS_EGRESS_DIALIN_RULES.x.COMMENT	<txt>

3.9 Redundancy

3.9.1 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>

3.9.2 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

3.10 Logging

3.10.1 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
Verbose mobile network logging	GSM_DEBUG	yes | no

A Appendix

A 1 Supported QoS values for TOS/DSCP

The following values are supported when setting TOS/DSCP:

- TOS-Not-Normal-Service
- TOS-Normal-Service
- TOS-Minimize-Delay
- TOS-Maximize-Throughput
- TOS-Maximize-Reliability
- TOS-Minimize-Cost
- DSCP-Class-Not-BE
- DSCP-Class-BE
- DSCP-Class-AF11
- DSCP-Class-AF12
- DSCP-Class-AF13
- DSCP-Class-AF21
- DSCP-Class-AF22
- DSCP-Class-AF23
- DSCP-Class-AF31
- DSCP-Class-AF32
- DSCP-Class-AF33
- DSCP-Class-AF41
- DSCP-Class-AF42
- DSCP-Class-AF43
- DSCP-Class-EF
- DSCP-Class-Not-CS0
- DSCP-Class-CS0
- DSCP-Class-CS1
- DSCP-Class-CS2
- DSCP-Class-CS3
- DSCP-Class-CS4
- DSCP-Class-CS5
- DSCP-Class-CS6
- DSCP-Class-CS7
- DSCP-Value-Not-0x00
- DSCP-Value-0x00
- DSCP-Value-0x01
- DSCP-Value-0x02
- DSCP-Value-0x03
- DSCP-Value-0x04
- DSCP-Value-0x05
- DSCP-Value-0x06
- DSCP-Value-0x07
- DSCP-Value-0x08

- DSCP-Value-0x09
- DSCP-Value-0x0a
- DSCP-Value-0x0b
- DSCP-Value-0x0c
- DSCP-Value-0x0d
- DSCP-Value-0x0e
- DSCP-Value-0x0f
- DSCP-Value-0x10
- DSCP-Value-0x11
- DSCP-Value-0x12
- DSCP-Value-0x13
- DSCP-Value-0x14
- DSCP-Value-0x15
- DSCP-Value-0x16
- DSCP-Value-0x17
- DSCP-Value-0x18
- DSCP-Value-0x19
- DSCP-Value-0x1a
- DSCP-Value-0x1b
- DSCP-Value-0x1c
- DSCP-Value-0x1d
- DSCP-Value-0x1e
- DSCP-Value-0x1f
- DSCP-Value-0x20
- DSCP-Value-0x21
- DSCP-Value-0x22
- DSCP-Value-0x23
- DSCP-Value-0x24
- DSCP-Value-0x25
- DSCP-Value-0x26
- DSCP-Value-0x27
- DSCP-Value-0x28
- DSCP-Value-0x29
- DSCP-Value-0x2a
- DSCP-Value-0x2b
- DSCP-Value-0x2c
- DSCP-Value-0x2d
- DSCP-Value-0x2e
- DSCP-Value-0x2f
- DSCP-Value-0x30
- DSCP-Value-0x31
- DSCP-Value-0x32
- DSCP-Value-0x33
- DSCP-Value-0x34
- DSCP-Value-0x35
- DSCP-Value-0x36

- DSCP-Value-0x37
- DSCP-Value-0x38
- DSCP-Value-0x39
- DSCP-Value-0x3a
- DSCP-Value-0x3b
- DSCP-Value-0x3c
- DSCP-Value-0x3d
- DSCP-Value-0x3e
- DSCP-Value-0x3f

A 2 E-Mail/SMS Notification Events

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

- /vpn/con/*/armed
- /ihal/temperature/temp_board_alarm
- /gsm/selected_sim
- /gsm/sim_fallback
- /gsm/network_probe
- /gsm/incoming_sms
- /ihal/power/psu2
- /network/modem/state
- /openvpn/con/*/armed
- /gps/valid
- /fwrules/*/state
- /gsm/service
- /ihal/power/psu1
- /redundancy/status
- /vpn/con/*/ipsec
- /ihal/contactreason
- /gsm/roaming
- /ecs/status
- /ihal/contact
- /ihal/service/cmd1
- /ihal/service/cmd2
- /ihal/service/cmd3
- /network/ext2up
- /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