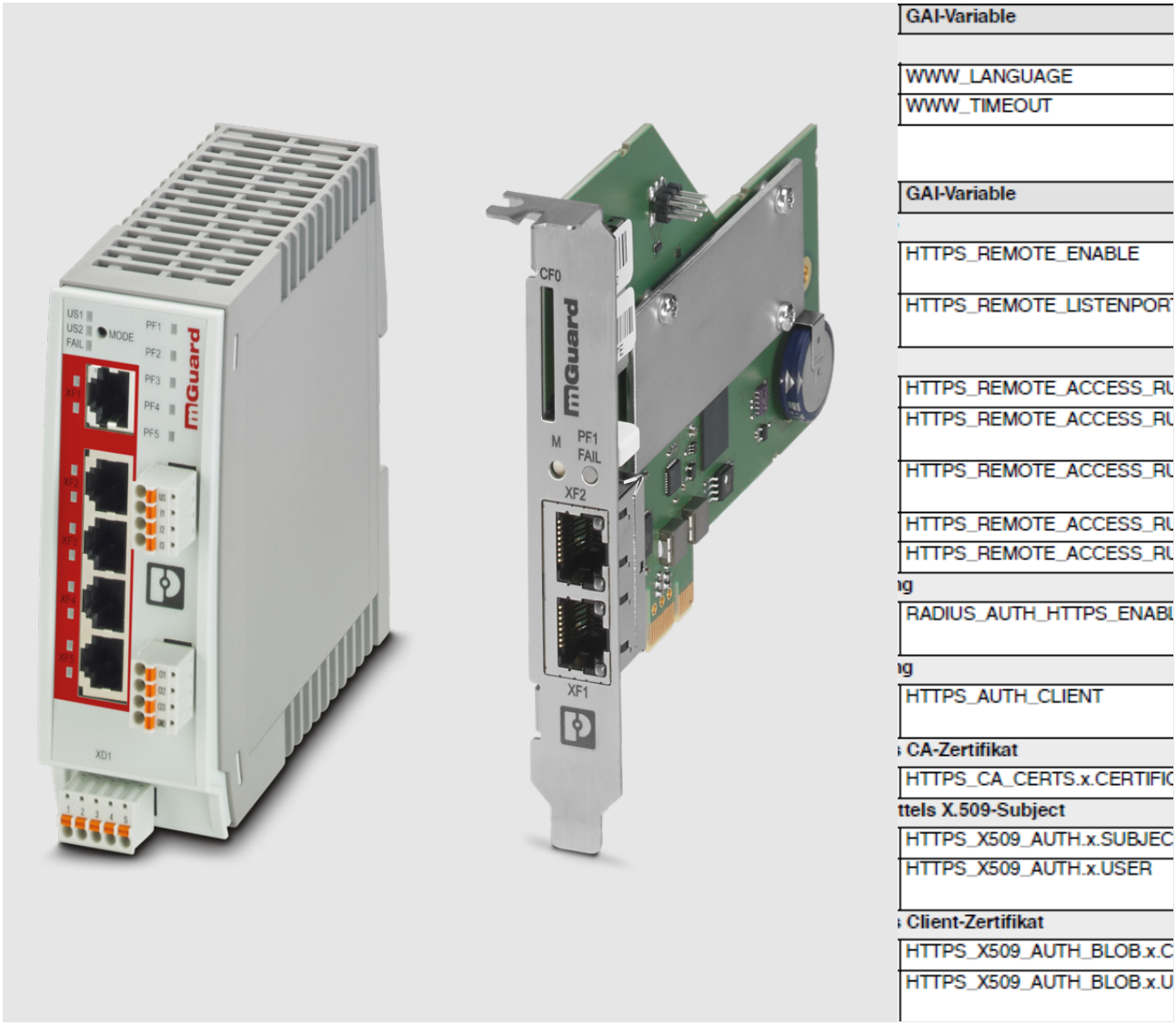

FL MGUARD 2000/4000
Generic Administration Interface
mGuard 10.5.x

Anwenderhandbuch

Anwenderhandbuch

FL MGUARD 2000/4000 - Generic Administration Interface mGuard 10.5.x

UM DE GAICONFIG MGUARD10, Revision 06 2025-01-22

Dieses Handbuch ist gültig für:

Bezeichnung	Artikel-Nr.
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 10.5.x

Mitgeltende Dokumentation (verfügbar unter phoenixcontact.net/product/<artikel-nummer>):

Release Notes

mGuard 10.5.x Firmware – Release Notes

Anwenderhandbuch „Web-based Management“

UM DE FW MGUARD10 – 110191_de_xx

Anwenderhandbuch „Installation und Inbetriebnahme“

UM DE HW FL MGUARD 2000/4000 – 110192_de_xx

110193_de_06

Inhaltsverzeichnis

1 Zu Ihrer Sicherheit

Lesen Sie dieses Handbuch sorgfältig und bewahren Sie es für späteres Nachschlagen auf.

1.1 Kennzeichnung der Warnhinweise

Dieses Symbol mit dem Signalwort **ACHTUNG** warnt vor Handlungen, die zu einem Sachschaden oder einer Fehlfunktion führen können.

Hier finden Sie zusätzliche Informationen oder weiterführende Informationsquellen.

1.2 Über dieses Handbuch

Folgende Elemente werden in diesem Handbuch verwendet:

Fett	Bezeichnung von Bedienelementen, Variablennamen oder sonstige Hervorhebungen
Kursiv	– Produkt-, Modul- oder Komponentenbezeichnungen (z. B. *tftpd64.exe*, *Config API*) – Fremdsprachliche Bezeichnungen oder Eigennamen – Sonstige Hervorhebungen
–	Unnummerierte Aufzählung
1.	Nummerierte Aufzählung
•	Handlungsanweisung
↪	Ergebnis einer Handlung

1.3 Qualifikation der Benutzer

Der in diesem Handbuch beschriebene Produktgebrauch richtet sich ausschließlich an

– Elektrofachkräfte oder von Elektrofachkräften unterwiesene Personen. Die Anwender müssen vertraut sein mit den einschlägigen Sicherheitskonzepten zur Automatisierungstechnik sowie den geltenden Normen und sonstigen Vorschriften.
– Qualifizierte Anwendungsprogrammierer und Software-Ingenieure. Die Anwender müssen vertraut sein mit den einschlägigen Sicherheitskonzepten zur Automatisierungstechnik sowie den geltenden Normen und sonstigen Vorschriften.

1.4 Bestimmungsgemäße Verwendung

– Die Geräte der Serie FL MGUARD sind industrietaugliche Security-Router mit integrierter Stateful-Packet-Inspection-Firewall und VPN. Sie eignen sich für die dezentrale Absicherung von Produktionszellen oder einzelner Maschinen gegen Manipulationen sowie für sichere Fernwartungsszenarien.
– Die Geräte sind nicht für den privaten Gebrauch bestimmt. Sie dürfen ausschließlich im gewerblichen bzw. industriellen Bereich eingesetzt und betrieben werden.

1.5 Veränderung des Produkts

Modifikationen an der Hard- und Firmware des Geräts sind nicht zulässig.

Unsachgemäße Arbeiten oder Veränderungen am Gerät können Ihre Sicherheit gefährden oder das Gerät beschädigen. Sie dürfen das Gerät nicht reparieren. Wenn das Gerät einen Defekt hat, wenden Sie sich an Phoenix Contact.

1.6 Sicherheitshinweise

ACHTUNG: Installation nur durch qualifiziertes Personal
Die Installation, Inbetriebnahme und Wartung des Produkts darf nur durch ausgebildetes Fachpersonal erfolgen, das vom Anlagenbetreiber dazu autorisiert wurde. Elektrofachkraft ist, wer aufgrund seiner fachlichen Ausbildung, Kenntnisse und Erfahrungen sowie Kenntnis der einschlägigen Normen die ihm übertragenen Arbeiten beurteilen und mögliche Gefahren erkennen kann. Das Fachpersonal muss diese Dokumentation gelesen und verstanden haben und die Anweisungen befolgen. Beachten Sie die geltenden nationalen Vorschriften für Betrieb, Funktionsprüfung, Reparatur und Wartung von elektronischen Geräten.

ACHTUNG: Sachschaden durch falsche Beschaltung
Schließen Sie die Netzwerkanschlüsse des Geräts nur an Ethernet-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des Geräts verbunden werden.

ACHTUNG: Elektrostatische Entladung
Die Geräte enthalten Bauelemente, die durch elektrostatische Entladung beschädigt oder zerstört werden können. Beachten Sie beim Umgang mit den Geräten die notwendigen Sicherheitsmaßnahmen gegen elektrostatische Entladung (ESD) gemäß EN 61340-5-1 und EN 61340-5-2.

ACHTUNG: Anforderung an die Spannungsversorgung
Das Modul ist ausschließlich für den Betrieb mit Sicherheitskleinspannung (SELV/PELV) ausgelegt. Im redundanten Betrieb müssen beide Spannungsversorgungen den Anforderungen der Sicherheitskleinspannung genügen.

ACHTUNG: Anforderung an den Schaltschrank/Schaltkasten
Tragschienengeräte werden innerhalb eines Schaltschranks oder -kastens auf eine Norm-Tragschiene aufgerastet. Dieser Schaltschrank/-kasten muss den Anforderungen der EN 60950-1: 2006 bez. der Brandschutzumhüllung genügen.

ACHTUNG: Anforderung an die Funktionserdung
Montieren Sie Tragschienengeräte auf einer geerdeten Tragschiene. Die Erdung des Moduls erfolgt mit dem Aufrasten auf die Tragschiene.

ACHTUNG: Anforderung an den Montageort
Die vorgeschriebene Einbaulage von Tragschienengeräten ist senkrecht auf einer horizontal montierten Tragschiene. Die Lüftungsschlitze dürfen nicht bedeckt werden, so dass die Luft frei zirkulieren kann. Als Abstand zu den Lüftungsschlitzen des Gehäuses werden mindestens 3 cm empfohlen.

Öffnen oder Verändern des Gerätes ist nicht zulässig. Reparieren Sie das Gerät nicht selbst, sondern ersetzen Sie es durch ein gleichwertiges Gerät. Reparaturen dürfen nur vom Hersteller vorgenommen werden. Der Hersteller haftet nicht für Schäden aus Zuwiderhandlung.

Die Schutzart IP20 (IEC 60529-0/EN 60529-0) des Gerätes ist für eine saubere und trockene Umgebung vorgesehen. Setzen Sie das Gerät keiner mechanischen und/oder thermischen Beanspruchung aus, die die beschriebenen Grenzen überschreitet.

ACHTUNG: Beachten Sie beim Einsatz des Geräts folgende Sicherheitshinweise.

- Halten Sie die für das Errichten und Betreiben geltenden Bestimmungen und Sicherheitsvorschriften (auch nationale Sicherheitsvorschriften) sowie die allgemeinen Regeln der Technik ein.
- Die technischen Daten sind der Packungsbeilage und den Zertifikaten (Konformitätsbewertung, ggf. weitere Approbationen) zu entnehmen.
- Setzen Sie das Gerät keinem direktem Sonnenlicht oder dem direkten Einfluss einer Wärmequelle aus, um eine Überhitzung zu vermeiden.
- Verwenden Sie zum Reinigen des Gerätegehäuses ein weiches Tuch. Verwenden Sie keine aggressiven Lösungsmittel.

1.7 IT-Sicherheit

Sie müssen Komponenten, Netzwerke und Systeme vor unberechtigten Zugriffen schützen und die Datenintegrität gewährleisten. Hierzu müssen Sie bei netzwerkfähigen Geräten, Lösungen und PC-basierter Software organisatorische und technische Maßnahmen ergreifen.

Phoenix Contact empfiehlt dringend den Einsatz eines Managementsystems für Informationssicherheit (ISMS) zur Verwaltung aller infrastrukturellen, organisatorischen und personellen Maßnahmen, die zur Erhaltung der Informationssicherheit notwendig sind.

Darüber hinaus empfiehlt Phoenix Contact, mindestens die folgenden Maßnahmen zu berücksichtigen.

Weiterführende Informationen zu den im Folgenden genannten Maßnahmen erhalten Sie auf den folgenden Webseiten (letzter Zugriff am 15.09.2024):

– bsi.bund.de/it-sik.html

– https://www.cisa.gov/resources-tools/resources/ics-recommended-practices

Verwenden Sie die jeweils aktuelle Firmware-Version

Phoenix Contact stellt regelmäßig Firmware-Updates zur Verfügung. Verfügbare Firmware-Updates finden Sie auf der Produktseite des jeweiligen Geräts.

- Stellen Sie sicher, dass die Firmware aller verwendeten Geräte immer auf dem aktuellen Stand ist.
- Beachten Sie die Change Notes / Release Notes zur jeweiligen Firmware-Version.
- Beachten Sie die Webseite des Product Security Incident Response Teams (PSIRT) von Phoenix Contact für Sicherheitshinweise zu veröffentlichten Sicherheitslücken.

Verwenden Sie die jeweils aktuelle Firmware-Version

Phoenix Contact stellt regelmäßig Firmware-Updates zur Verfügung. Verfügbare Firmware-Updates finden Sie auf der Produktseite des jeweiligen Geräts.

- Stellen Sie sicher, dass die Firmware aller verwendeten Geräte immer auf dem aktuellen Stand ist.
- Beachten Sie die Change Notes / Release Notes zur jeweiligen Firmware-Version.
- Beachten Sie die Webseite des Product Security Incident Response Teams (PSIRT) von Phoenix Contact für Sicherheitshinweise zu veröffentlichten Sicherheitslücken.

Verwenden Sie die jeweils aktuelle Dokumentation

Phoenix Contact stellt regelmäßig Updates der Dokumentation zur Verfügung. Diese finden Sie auf der Produktseite des jeweiligen Geräts.

- Stellen Sie sicher, dass Sie immer die aktuelle gerätespezifische Dokumentation verwenden.

Stellen Sie die Integrität von heruntergeladenen Dateien sicher

Phoenix Contact stellt Prüfsummen der Dateien bereit, die über die Produktseite des jeweiligen Geräts heruntergeladen werden können.

- Um sicherzugehen, dass die heruntergeladenen Firmware- oder Update-Dateien als auch heruntergeladene Dokumentation während des Downloads nicht von Dritten verändert wurden, vergleichen Sie die SHA256-Prüfsummen der Dateien mit den auf der entsprechenden Produktseite (phoenixcontact.com/product/<Bestellnummer>) angegebenen Prüfsummen.

Führen Sie regelmäßige Bedrohungsanalysen durch

- Um festzustellen, ob die von Ihnen getroffenen Maßnahmen Ihre Komponenten, Netzwerke und Systeme noch ausreichend schützen, ist eine regelmäßige Bedrohungsanalyse erforderlich.
- Führen Sie regelmäßige Bedrohungsanalysen durch.

Berücksichtigen Sie bei der Anlagenplanung Defense-in-depth-Mechanismen

Um Ihre Komponenten, Netzwerke und Systeme zu schützen, ist es nicht ausreichend, isoliert betrachtete Maßnahmen zu ergreifen. Defense-in-Depth-Mechanismen umfassen mehrere, aufeinander abgestimmte und koordinierte Maßnahmen, die Betreiber, Integratoren und Hersteller miteinbeziehen.

- Berücksichtigen Sie bei der Anlagenplanung Defense-in-depth-Mechanismen

Deaktivieren Sie nicht benötigte Kommunikationskanäle

- Deaktivieren Sie nicht benötigte Kommunikationskanäle (z. B. SNMP, FTP, BootP, DCP etc.) an den von Ihnen eingesetzten Komponenten.

Binden Sie Komponenten und Systeme nicht in öffentliche Netzwerke ein

- Vermeiden Sie es, Komponenten und Systeme in öffentliche Netzwerke einzubinden.
- Wenn Sie Ihre Komponenten und Systeme über ein öffentliches Netzwerk erreichen müssen, verwenden Sie ein VPN (Virtual Private Network).

Beschränken Sie die Zugangsberechtigung zum Gerät

- Vermeiden Sie, dass unberechtigte Personen physischen Zugriff auf das Gerät erlangen. Ein Zugriff auf die Hardware des Geräts könnte es einem Angreifer ermöglichen, die Sicherheitsfunktionen zu manipulieren.
- Beschränken Sie die Zugangsberechtigung zu Komponenten, Netzwerken und Systemen auf die Personen, für die eine Berechtigung unbedingt notwendig ist.
- Deaktivieren Sie nicht genutzte Benutzerkonten.

Sichern Sie den Zugriff ab

- Ändern Sie voreingestellte Passwörter während der ersten Inbetriebnahme.
- Verwenden Sie sichere Passwörter, deren Komplexität und Lebensdauer dem Stand der Technik entsprechen (z. B. mit einer Länge von mindestens zehn Zeichen und einer Mischung aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen).
- Verwenden Sie Passwort-Manager mit zufällig erzeugten Passwörtern.
- Ändern Sie Passwörter entsprechend der für Ihre Anwendung geltenden Regeln.
- Verwenden Sie, sofern möglich, zentrale Benutzerverwaltungen zur Vereinfachung des User Managements und der Anmeldeinformationen.

Verwenden Sie bei Fernzugriff sichere Zugriffswege

- Verwenden Sie für einen Fernzugriff sichere Zugriffswege wie VPN (Virtual Private Network) oder HTTPS.

Verwenden Sie eine Firewall

- Richten Sie eine Firewall ein, um Ihre Netzwerke und darin eingebundene Komponenten und Systeme vor ungewollten Netzwerkzugriffen zu schützen.
- Verwenden Sie eine Firewall, um ein Netzwerk zu segmentieren oder bestimmte Komponenten (z. B. Steuerungen) zu isolieren.

Aktivieren Sie eine sicherheitsrelevante Ereignisprotokollierung (Logging)

- Aktivieren Sie die sicherheitsrelevante Ereignisprotokollierung (Logging) gemäß der Sicherheitsrichtlinie und der gesetzlichen Bestimmungen zum Datenschutz.

Schützen Sie den Zugriff auf die SD-Karte

Geräte mit SD-Karten benötigen Schutz gegen unerlaubte physische Zugriffe. Eine SD-Karte kann mit einem herkömmlichen SD-Kartenleser jederzeit ausgelesen werden. Wenn Sie die SD-Karte nicht physisch gegen unbefugte Zugriffe schützen (z. B. mithilfe eines gesicherten Schaltschranks), sind somit auch sensible Daten für jeden abrufbar.

- Stellen Sie sicher, dass Unbefugte keinen Zugriff auf die SD-Karte haben.
- Stellen Sie bei der Vernichtung der SD-Karte sicher, dass die Daten nicht wiederhergestellt werden können.

1.8 Aktuelle Sicherheitshinweise zu Ihrem Produkt

Product Security Incident Response Team (PSIRT)

Das Phoenix Contact PSIRT ist das zentrale Team für Phoenix Contact und dessen Tochterunternehmen, dessen Aufgabe es ist, auf potenzielle Sicherheitslücken, Vorfälle und andere Sicherheitsprobleme im Zusammenhang mit Produkten, Lösungen sowie Diensten von Phoenix Contact zu reagieren.

Das Phoenix Contact PSIRT leitet die Offenlegung, Untersuchung und interne Koordination und veröffentlicht Sicherheitshinweise zu bestätigten Sicherheitslücken, bei denen Maßnahmen zur Abschwächung oder Behebung verfügbar sind.

Die PSIRT-Webseite (phoenixcontact.com/psirt) wird regelmäßig aktualisiert. Zusätzlich empfiehlt Phoenix Contact, den PSIRT-Newsletter zu abonnieren.

Jeder kann per E-Mail Informationen zu potenziellen Sicherheitslücken beim Phoenix Contact PSIRT einreichen.

1.9 Support

Zusätzliche Informationen zum Gerät sowie Release Notes, Anwenderhilfen und Software-Updates finden Sie unter folgender Internet-Adresse: phoenixcontact.com/product/<Artikelnummer>.

Bei Problemen mit Ihrem Gerät oder der Bedienung Ihres Geräts wenden Sie sich bitte an Ihre Bezugsquelle.

Um in einem Fehlerfall schnelle Hilfe zu erhalten, erstellen Sie, falls möglich, beim Auftreten des Fehlers umgehend einen Snapshot der Gerätekonfiguration, den Sie dem Support zur Verfügung stellen können.

2 Einleitung

Über das *Generic Administration Interface* (GAI) werden Benutzer- und Systemschnittstellen zur Konfiguration des mGuards bereitgestellt. Zusätzlich zur Web- und SNMP-Schnittstelle stellt GAI die Kommandozeilenschnittstelle **gaiconfig** zur Verfügung, die in diesem Dokument beschrieben wird.

gaiconfig ist das Kommandozeilen-Tool zum Abrufen und Konfigurieren von Variablen in allen von GAI verwalteten Konfigurationsdateien. Abhängige Dienste werden wie in der *Registry* definiert neu gestartet, bevor das Programm beendet wird. Der Befehl *gaiconfig* kann von den mGuard-Benutzern *admin* und *root* verwendet werden.

2.1 Optionen

Tab. 2-1 zeigt die am häufigsten verwendeten Optionen. Um eine vollständige Liste der unterstützten Optionen zu erhalten, führen Sie *gaiconfig --help* auf der Kommandozeile aus.

Tabelle 2-1 Die am häufigsten verwendeten Optionen.

Option	Beschreibung
--add-row	Fügt eine Zeile zur aktuellen Variablen hinzu
--append-row	Hängt eine Zeile an die aktuelle Variable an, genau wie *--add-row*
--delete-row	Löscht die aktuelle Zeile
--delete-all-rows	Löscht alle Zeilen
--get <variable>	Ruft den Wert der Variablen ab und zeigt diesen an
--get-access <variable>	Meldet die Berechtigung der Variablen zurück
--get-all	Gibt alle Konfigurationsdaten als ATV nach *stdout* aus (*dump*)
--get-all-but-private	Gibt alle Konfigurationsdaten, außer Variablen, die in der *Registry* als privat markiert sind, nach *stdout* aus (*dump*)
--get-all-but-default	Gibt alle Konfigurationsdaten, außer Variablen mit dem Standardwert an *stdout* aus (*dump*)
--get-current-path	Zeigt den aktuellen Pfad an (nützlich nach *goto* oder *add-row*)
--get-local <row>	Gibt das "local flag“ zurück
--get-quoted <variable>	Gibt den Wert unter Anwendung von ATV-Quoting zurück
--get-ref --get-reference	Gibt die Variable oder Zeile zurück, auf die die aktuelle Referenz verweist
--get-reference-list	Gibt eine Liste von Referenzen und ihren Verweiszielen zurück
--get-rowcount <variable>	Gibt die Anzahl der Zeilen zurück, wenn es sich um eine Tabelle handelt; in allen anderen Fällen einen Fehler
--get-rowid	Gibt die *rowid* der aktuellen Zeile oder der Zeile, in der die aktuelle Variable befindet, zurück

Tabelle 2-1 Die am häufigsten verwendeten Optionen.

--get-uuid <variable>	Gibt die UUID von <variable> zurück, wenn die Variable eine UUID besitzt; in allen anderen Fällen einen Fehler.
--goto <variable>|<row>	Geht zur angegebenen Variablen | Zeile
--help	Zeigt einen Hilfetext an
--insert-row	Fügt eine Zeile ein
--keep-local	Stellt lokal geänderte Werte nach einer Konfiguration wieder her
--pragma <name> <value>	Setzt pragma in atv. Nicht erlaubt/zu empfehlen mit *--direct*
--print	Gibt die aktuell geänderten Variablen als ATV aus, anstatt sie nach *maid* zu schreiben
--psm-install <package set name>	Installiert <Package Set Name> mit Hilfe der PSM-Utilities
--reboot	Startet das Gerät neu
--reset	Setzt alle Werte auf die werkseitige Voreinstellung zurück
--rollback	Beendet die aktuellen Sitzung (*branch*) ohne die Änderungen zu übernehmen
--session	Startet eine neue Session (*branch*) und gibt die Session-ID zurück
--set <variable> <value>	Setzt den Wertes einer einzelnen Variablen
--set-access <variable>	must-not-overwrite | may-overwrite | must-overwrite | may-append
--set-admin	Wie *--set-all*: Setzt aber nur Daten, die nicht von Mitgliedern der Gruppe ‘netadmin' geändert werden können
--set-admin-file <filename>	Wie *--set-admin*: Liest alle Konfigurationsdaten aus der angegebenen Datei
--set-all	Liest alle Konfigurationsdaten von *stdin* (bei Aufruf durch den Benutzer netadmin' werden nur die Daten gesetzt, auf die dieser Benutzer zugreifen kann)
--set-all-file <filename>	Wie *--set-all*: Liest alle Konfigurationsdaten aus der angegebenen Datei
--set-file <variable> <filename>	Setzt den Wert einer einzelnen Variablen aus der angegebenen Datei
--set-reference <variable> <ROWID>	Verweist die Variable auf die Zeile mit der *rowid* <ROWID>
--set-refname <variable> <ROW>	Verweist die Variable auf die Zeile mit den Namen <ROW>
--set-rowid <value>	Setzt die *rowid* (*rid*) der aktuellen Zeile auf <*value*>
--silent	Dienste werden nicht umkonfiguriert, die neue Konfiguration wird nur geschrieben
--strict	Bricht bei einem Fehler während *--set-all/--set-admin* ab

Tabelle 2-1 Die am häufigsten verwendeten Optionen.

--synchronous	Nach einen Neukonfiguration verbunden bleiben, auch wenn das Netzwerk geändert wurde
--validate	Validiert die Änderungen der aktuellen Sitzung
--vardiff	Zeigt Liste der geänderten Variablen zwischen diesem und dem letzten Commit an

2.2 Variablen

gaiconfig speichert die Konfigurationseinstellungen in zwei Arten von Variablen: Einzelvariablen (*single variables*) und Tabellen.

Einzelvariablen (*single variables*) werden einfach durch ihren Namen definiert.

Beispielsweise wird die interne IP-Adresse des mGuards im Netzwerkmodus „Router“ in der Einzelvariablen MY_LOCAL_IP gespeichert.

MY_LOCAL_IP = 192.168.27.1

Der Wert dieser Variable kann mit folgendem Befehl abgefragt werden:

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

Tabellen haben das Format:

TableName.x.field, wobei **x** die Zeile in der Tabelle angibt.

TableName1.x.TableName2.y.field, für eine Tabelle, die eine andere Tabelle enthält, wobei **x** die Zeile in Tabelle 1 und **y** die Zeile in Tabelle 2 angibt.

So werden z. B. zusätzliche interne IP-Adressen des mGuards in der Tabelle

LOCAL_ALIASES gespeichert.

```
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"
 }
}
```

Der erste Eintrag (192.168.2.1/255.255.255.0) hat in der Tabelle die Zeilennummer „0“, der zweite Eintrag (192.168.1.1/255.255.255.0) die Zeilennummer „1“.

Die IP-Adresse des **ersten** Eintrags kann mit folgendem Befehl geändert werden:

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

Die IP-Adresse des **zweiten** Eintrags kann mit folgendem Befehl geändert werden:

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

2.3 Beispiele

Wir greifen per Remote-SSH-Zugriff auf einen mGuard zu und wollen zusätzlich auch Remote-HTTPS-Zugriff von der IP-Adresse 62.214.150.190 ermöglichen. Jeder Remote-Zugriff über HTTPS soll protokolliert werden. Für die Aktivierung des HTTPS Remote-Zugriffs müssen Sie folgende Schritte durchführen:

1. Aktivieren Sie den HTTPS-Fernzugriff.
2. Geben Sie den Port für den HTTPS-Fernzugriff an.
3. Fügen Sie eine Firewall-Regeln hinzu.

Aktiviere HTTPS-Fernzugang

Prüfen Sie den aktuellen Wert:

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

Aktivieren Sie HTTPS-Fernzugang:

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

Überprüfen Sie die Änderungen:

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

Port für HTTPS-Verbindungen (nur Fernzugang)

Prüfen Sie den aktuellen Wert (443 ist der Standard-Wert):

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

Füge Firewall-Regeln für den HTTPS-Fernzugang hinzu (Erlaubte Netzwerke)

Die Firewall-Regeln sind in der Tabelle HTTPS_REMOTE_ACCESS_RULES abgelegt. Jede Zeile enthält folgende Felder:

– FROM_IP
– INTERFACE_DEV
– TARGET
– LOG

Die werkseitige Voreinstellung ist TARGET=ACCEPT und INTERFACE_DEV=extern. Sie müssen daher nur die IP-Adresse angeben und „LOG“ auf „Ja“ zu setzen, wenn Sie eine neue Firewall-Regel hinzufügen. Dies kann sowohl Schritt-für-Schritt als auch mit einem einzigen Befehl erfolgen.

Überprüfen Sie den aktuellen Wert:

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

Die Tabelle ist leer. Es gibt keine Regeln.

Fügen Sie eine Tabellenzeile hinzu:

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

Überprüfen Sie die Änderungen:

```
$ 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"
   }
}
```

Konfigurieren Sie die IP-Adresse:

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

Überprüfen Sie die Änderungen:

```
$ 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"
   }
}
```

Aktivieren Sie das Loggen:

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

Überprüfen Sie die Änderungen:

```
$ 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"
   }
}
```

Anstatt die folgenden drei Befehle zu verwenden,

```
$ 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
```

können Sie die Firewall auch mit einem einzigen Kommando konfigurieren:

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

3 Nomenklatur

In Kapitel 4 wird für das den GAI-Variablen zugeordnete Datenformat, die in Tabelle 3-1 beschriebene Nomenklatur verwendet.

Tabelle 3-1 Nomenklatur

Format	Beschreibung
<cidr>	Netzwerk/IP-Adresse in CIDR-Schreibweise (192.168.1.0/24, 10.1.0.23/32)
<hex>	Hexadezimaler Wert
<ip>	IP-Adresse (192.168.1.102)
<mac>	MAC-Adresse (00:0c:be:12:fe:01)
<netmask>	Subnetzmaske (255.255.255.0)
<num>	Numerischer Wert
<txt>	Textueller Wert
<rowref>	Referenz-ID einer definierten Zeile (z. B. MAI0983174920)

4 Korrelation zwischen mGuard-Menüoptionen und gaiconfig-Variablen

4.1 Verwaltung

4.1.1 Systemeinstellungen

Registerkarte: Host

Menü-Option	GAI-Variable	Format
System		
Systemtemperatur	HM_TEMP_MIN	<num>
Systemtemperatur	HM_TEMP_MAX	<num>
CPU-Temperatur	CPU_TEMP_MIN	<num>
CPU-Temperatur	CPU_TEMP_MAX	<num>
Systembenachrichtigung	SYSTEM_USE_NOTIFICATION	<txt>
System DNS-Hostname		
Hostnamen-Modus	NETWORK_HOSTNAME_MODE	user | provider
Hostname	NETWORK_HOSTNAME	<txt>
Domain-Suchpfad	DNSCACHE_SEARCHPATH	<txt>
SNMP-Information		
Systemname	SYS_NAME	<txt>
Standort	SYS_LOCATION	<txt>
Kontakt	SYS_CONTACT	<txt>

Registerkarte: Zeit und Datum

Menü-Option	GAI-Variable	Format
Zeit und Datum		
Zeitzone in POSIX.1-Notation	TIMEZONE	<txt>
Zeitmarke im Dateisystem (2h-Auflösung)	NTP_ENABLE_FILESTAMP	yes | no
NTP-Server		
Aktiviere NTP-Zeitsynchronisation	NTP_ENABLE	yes | no
‘discard minimum1‘	NTP_RATE_LIMIT_DISABLED	yes | no
NTP-Server	NTP_SERVERS.x.NTP_SERVER	<ip> | <txt>
Über VPN	NTP_SERVERS.x.PREFER_VPN	yes | no
Erlaubte Netzwerke für NTP-Zugriff		
Von IP	NTP_ACCESS_RULES.x.FROM_IP	<cidr>
Interface	NTP_ACCESS_RULES.x.INTERFACE_DEV	intern | extern | vi-aipsec | dmz0

Aktion	NTP_ACCESS_RULES.x.TARGET	ACCEPT | REJECT | DROP
Kommentar	NTP_ACCESS_RULES.x.COMMENT	<txt>
Log	NTP_ACCESS_RULES.x.LOG	yes | no

Registerkarte: Shell-Zugang

Menü-Option	GAI-Variable	Format
Shell-Zugang		
Aktiviere SSH-Fernzugang	SSH_REMOTE_ENABLE	yes | no
Port für eingehende SSH-Verbindungen (nur Fernzugang)	SSH_REMOTE_LISTENPORT	<num>
Erlaube SSH-Zugang als Benutzer root	SSH_ROOT_LOGIN_ENABLE	yes | no
Ablauf der Sitzung	SHELL_TIMEOUT	<num>
Verzögerung bis zur nächsten Anfrage nach einem Lebenszeichen (der Wert 0 bedeutet, dass keine Anfragen gesendet werden)	SSH_CLIENT_ALIVE_INTERVAL_SECS	<num>
Maximale Anzahl ausbleibender Lebenszeichen	SSH_CLIENT_ALIVE_COUNT_MAX	<num>
Maximale Anzahl gleichzeitiger Sitzungen pro Rolle		
Admin	SSH_ADMIN_LOGIN_ALLOWED_MAX	<num>
Netadmin	SSH_NETADMIN_LOGIN_ALLOWED_MAX	<num>
Audit	SSH_AUDIT_LOGIN_ALLOWED_MAX	<num>
Erlaubte Netzwerke		
Von IP	SSH_REMOTE_ACCESS_RULES.x.FROM_IP	<cidr>
Interface	SSH_REMOTE_ACCESS_RULES.x.INTERFACE_DEV	intern | extern | viaipsec | dmz0
Aktion	SSH_REMOTE_ACCESS_RULES.x.TARGET	ACCEPT | REJECT | DROP
Kommentar	SSH_REMOTE_ACCESS_RULES.x.COMMENT	<txt>
Log	SSH_REMOTE_ACCESS_RULES.x.LOG	yes | no
RADIUS-Authentifizierung		
Nutze RADIUS-Authentifizierung für den Shell-Zugang	RADIUS_AUTH_SHELL_ENABLE	yes | no | exclusive
X.509-Authentifizierung		
Unterstütze X.509-Zertifikate für den SSH-Zugang	SSH_X509_ENABLE	yes | no
SSH Server-Zertifikat	SSH_SERVER_CERT_REF	Empty for "None" | <rowref>
Authentifizierung mittels CA-Zertifikat		
CA-Zertifikat	SSH_CA_CERTS.x.CERTIFICATE_REF	<rowref>
Zugriffsberechtigung mittels X.509-Subject		
X.509-Subject	SSH_X509_AUTH.x.SUBJECT	<txt>

Für den Zugriff autorisiert als	SSH_X509_AUTH.x.USER	all | root | admin | netadmin | audit
Authentifizierung mittels Client-Zertifikat		
Client-Zertifikat	SSH_X509_AUTH_BLOB.x.CERTIFICATE_REF	<rowref>
Für den Zugriff autorisiert als	SSH_X509_AUTH_BLOB.x.USER	all | root | admin | netadmin | audit

Registerkarte: E-Mail

Menü-Option	GAI-Variable	Format
E-Mail		
Absenderadresse von E-Mail-Benachrichtigungen	EMAIL_FROM	<txt>
Adresse des E-Mail-Servers	EMAIL_RELAY_HOST	<ip> | <txt>
Portnummer des E-Mail-Servers	EMAIL_RELAY_PORT	<num>
Verschlüsselungsmodus für den E-Mail-Server	EMAIL_RELAY_TLS	none | tls | starttls
SMTP-Benutzerkennung	EMAIL_RELAY_LOGIN	<txt>
SMTP-Passwort	EMAIL_RELAY_PASSWORD	<txt>
E-Mail-Benachrichtigungen		
E-Mail-Empfänger	EMAIL_NOTIFICATION.x.TO	<txt>
Ereignis	EMAIL_NOTIFICATION.x.EVENT	Refer to Appendix 4.2
IPsec-Selektor	EMAIL_NOTIFICATION.x.SELECTOR	Empty for "None" | <rowref>
Open-VPN-Selektor	EMAIL_NOTIFICATION.x.SELECTOR_OPENVPN	Empty for "None" | <rowref>
Regelsatz-Selektor	EMAIL_NOTIFICATION.x.SELECTOR_FW_RULESET	Empty for "None" | <rowref>
E-Mail-Betreff	EMAIL_NOTIFICATION.x.SUBJECT	<txt>
E-Mail-Nachricht	EMAIL_NOTIFICATION.x.MESSAGE	<txt>

4.1.2 Web-Einstellungen

Registerkarte: Allgemein

Menü-Option	GAI-Variable	Format
Allgemein		
Sprache	WWW_LANGUAGE	auto | en | de | ja
Ablauf der Sitzung	WWW_TIMEOUT	<num>

Registerkarte: Zugriff

Menü-Option	GAI-Variable	Format
Web-Zugriff über HTTPS		
Aktiviere HTTPS-Fernzugang	HTTPS_REMOTE_ENABLE	yes | no
Port für HTTPS-Verbindungen (nur Fernzugang)	HTTPS_REMOTE_LISTENPORT	<num>
HTTPS Server-Zertifikat	HTTPS_SERVER_CERT_REF	Empty for "Builtin" | <rowref> |
Erlaubte Netzwerke		
Von IP	HTTPS_REMOTE_ACCESS_RULES.x.FROM_IP	<cidr>
Interface	HTTPS_REMOTE_ACCESS_RULES.x.INTERFACE_DEV	intern | extern | vi-aipsec | dmz0
Aktion	HTTPS_REMOTE_ACCESS_RULES.x.TARGET	ACCEPT | REJECT | DROP
Kommentar	HTTPS_REMOTE_ACCESS_RULES.x.COMMENT	<txt>
Log	HTTPS_REMOTE_ACCESS_RULES.x.LOG	yes | no
RADIUS-Authentifizierung		
Ermögliche RADIUS-Authentifizierung	RADIUS_AUTH_HTTPS_ENABLE	yes | no | exclusive
Benutzerauthentifizierung		
Methode zur Benutzerauthentifizierung	HTTPS_AUTH_CLIENT	no | may | must
Authentifizierung mittels CA-Zertifikat		
CA-Zertifikat	HTTPS_CA_CERTS.x.CERTIFICATE_REF	<rowref>
Zugriffsberechtigung mittels X.509-Subject		
X.509-Subject	HTTPS_X509_AUTH.x.SUBJECT	<txt>
Für den Zugriff autorisiert als	HTTPS_X509_AUTH.x.USER	root | admin | netadmin | audit | user
Authentifizierung mittels Client-Zertifikat		
Client-Zertifikat	HTTPS_X509_AUTH_BLOB.x.CERTIFICATE_REF	<rowref>
Für den Zugriff autorisiert als	HTTPS_X509_AUTH_BLOB.x.USER	root | admin | netadmin | audit | user

4.1.3 Update

Registerkarte: Update

Menü-Option	GAI-Variable	Format
Update-Server		
Protokoll	PSM_REPOSITORIES.x.PROTO	https | http | ftp | tftp
Server	PSM_REPOSITORIES.x.SERVER	<ip> | <txt>
Über VPN	PSM_REPOSITORIES.x.PREFER_VPN	yes | no
Login	PSM_REPOSITORIES.x.LOGIN	<txt>
Passwort	PSM_REPOSITORIES.x.PASSWORD	<txt>
Server-Zertifikat	PSM_REPOSITORIES.x.REMOTE_CERT_REF	<rowref> | ignore

4.1.4 Konfigurationsprofile

Registerkarte: Konfigurationsprofile

Menü-Option	GAI-Variable	Format
Externer Konfigurationsspeicher (ECS)		
Konfigurationsänderungen automatisch auf dem ECS speichern	ECS_AUTOSAVE_ENABLE	yes | no
Daten auf dem ECS verschlüsseln	ECS_ENCRYPTION	yes | no
Lade die aktuelle Konfiguration vom ECS beim Start	ECS_LOAD_ON_BOOT	yes | no
Signierte Konfigurationsprofile		
Signierte Konfigurationsprofile aktivieren	PROFILE_SECURE_ONLY	yes | no
Export-Zertifikat (Maschinenzertifikat zum Signieren von Konfigurationsprofilen)	PROFILE_EXPORT_CERT	Empty for "None" | <rowref>
Import-Zertifikat (Zertifikat zur Prüfung signierter Konfigurationsprofile)	PROFILE_IMPORT_CERT	Empty for "None" | all | <rowref>

4.1.5 SNMP

Registerkarte: Abfrage

Menü-Option	GAI-Variable	Format
Einstellungen		
Aktiviere SNMPv3	SNMP_ENABLE_V3	yes | no
Aktiviere SNMPv1/v2	SNMP_ENABLE_V1	yes | no
Port für eingehende SNMP-Verbindungen (nur Fernzugang)	SNMP_LISTENPORT	<num>
Führe den SNMP-Agent mit den Rechten des folgenden Benutzers aus	SNMP_GAI_SECURITY_CONTEXT	admin | netadmin
SNMPv3-Zugangsdaten		
Benutzerkennung	SNMP_V3_USERNAME	<txt>
Passwort	SNMP_V3_PASSWORD	<txt>
SNMPv1/v2-Community		
Read-Write-Community	SNMP_COMMUNITY	<txt>
Read-Only-Community	SNMP_COMMUNITY_RO	<txt>
Erlaubte Netzwerke		
Von IP	SNMP_ACCESS_RULES.x.FROM_IP	<cidr>
Interface	SNMP_ACCESS_RULES.x.INTERFACE_DEV	intern | extern | vi-aipsec | dmz0
Aktion	SNMP_ACCESS_RULES.x.TARGET	ACCEPT | REJECT | DROP
Kommentar	SNMP_ACCESS_RULES.x.COMMENT	<txt>
Log	SNMP_ACCESS_RULES.x.LOG	yes | no

Registerkarte: Trap

Menü-Option	GAI-Variable	Format
Basis-Traps		
SNMP-Authentifikation	SNMP_AUTHENTICATION_TRAP	yes | no
Linkstatus An/Aus	SNMP_LINKUPDOWN_TRAP	yes | no
Kaltstart	SNMP_COLDSTART_TRAP	yes | no
Administrativer Verbindungsversuch (SSH, HTTPS)	SNMP_TRAP_ADMIN_CONNECT	yes | no
Administrativer Zugriff (SSH, HTTPS)	SNMP_TRAP_ADMIN_ACCESS	yes | no
Neuer DHCP-Client	SNMP_TRAP_NEW_DHCP_CLIENT	yes | no
Hardwarebezogene Traps		
Chassis (Stromversorgung, Relais)	SNMP_CHASSIS_TRAP	yes | no
Service-Eingang/CMD	SNMP_TRAP_CMD	yes | no

Agent (externer Konfigurationsspeicher, Temperatur)	SNMP_AGENT_TRAP	yes | no
Redundanz-Traps		
Statusänderung	SNMP_TRAP_REDUNDANCY_STATE	yes | no
Benutzerfirewall-Traps		
Benutzerfirewall-Traps	SNMP_TRAP_USER_FIREWALL	yes | no
VPN-Traps		
Statusänderungen von IPsec-Verbindungen	SNMP_TRAP_VPN_IPSEC	yes | no
Statusänderungen von L2TP-Verbindungen	SNMP_TRAP_VPN_L2TP	yes | no
Trap-Ziele		
Ziel-IP	SNMP_TRAP_RECEIVERS.x.TARGET_IP	<ip>
Ziel-Port	SNMP_TRAP_RECEIVERS.x.TARGET_PORT	<num>
Zielname	SNMP_TRAP_RECEIVERS.x.TARGET_NAME	<txt>
Ziel-Community	SNMP_TRAP_RECEIVERS.x.TARGET_COMMUNITY	<txt>

Registerkarte: LLDP

Menü-Option	GAI-Variable	Format
LLDP		
LLDP aktivieren	LLDPD_ENABLE	yes | no
LLDP auf externen Netzwerken	LLDPD_EXT_ADMIN_STATUS	enabledRxTx | enabledRxOnly | enabledTxOnly | disabled
LLDP auf internen Netzwerken	LLDPD_INT_ADMIN_STATUS	enabledRxTx | enabledRxOnly | enabledTxOnly | disabled

4.1.6 Zentrale Verwaltung

Registerkarte: Konfiguration holen

Menü-Option	GAI-Variable	Format
Konfiguration holen		
Zeitplan	GAI_PULL_INTERVAL	-1 | 0 | -2 | 15 | 30 | 60 | 120 | 360 | 720 | 1440
Zeitgesteuert	GAI_PULL_SCHEDULE	1 | 2 | 3 | 4 | 5 | 6 | 7 | *
Stunden	GAI_PULL_SCHEDULE_HOUR	<num>
Minuten	GAI_PULL_SCHEDULE_MIN	<num>
Server	GAI_PULL_HTTPS_HOST	<ip> | <txt>
Port	GAI_PULL_HTTPS_PORT	<num>
Verzeichnis	GAI_PULL_HTTPS_DIR	<txt>
Dateiname (bei fehlender Angabe wird die Seriennummer des Geräts verwendet)	GAI_PULL_HTTPS_FILE	<txt>
Anzahl der Zyklen, die ein Konfigurationsprofil nach einem Rollback ignoriert wird	GAI_PULL_ROLLBACK_BLOCK	<num>
Download-Timeout	GAI_PULL_DLTIME	<num>
Login	GAI_PULL_HTTPS_LOGIN	<txt>
Passwort	GAI_PULL_HTTPS_PASSWORD	<txt>
Server-Zertifikat	GAI_PULL_HTTPS_CERT_REF	Empty for "None" | <rowref>

4.1.7 Service I/O

Registerkarte: Servicekontakte

Menü-Option	GAI-Variable	Format
Eingang/CMD 1		
Am Kontakt angeschlossener Schaltertyp	SERVICE_SWITCH1_TYPE	button | switch
Ausgang/ACK 1		
Zu überwachende VPN-Verbindung bzw. Firewall Regelsatz	SERVICE_ACK1_REF	Empty for "Off" | <rowref>
Eingang/CMD 2		
Am Kontakt angeschlossener Schaltertyp	SERVICE_SWITCH2_TYPE	button | switch
Ausgang/ACK 2		
Zu überwachende VPN-Verbindung bzw. Firewall Regelsatz	SERVICE_ACK2_REF	Empty for "Off" | <rowref>
Eingang/CMD 3		
Am Kontakt angeschlossener Schaltertyp	SERVICE_SWITCH3_TYPE	button | switch

Registerkarte: Alarmausgang

Menü-Option	GAI-Variable	Format
Allgemein		
Betriebs-Modus	HM_RS2_SIG_RELAY_MODE	standard | manual
Manuelle Einstellung	HM_RS2_SIG_RELAY_MANUAL_STATE	active | inactive
Funktions-Überwachung		
Redundante Stromversorgung	HM_RS2_SIG_PS2_ALARM	on | off
Passwörter nicht konfiguriert	PASSWORD_ALARM	on | off
Link-Überwachung	SIG_ALARM_LINK	on | off
Temperaturzustand	HM_RS2_SIG_TEMP_ALARM	on | off
Verbindungsstatus der Redundanz	HM_RS2_SIG_CONNECTIVITY_ALARM	on | off

4.2 Netzwerk

4.2.1 Interfaces

Registerkarte: Allgemein

Menü-Option	GAI-Variable	Format
Netzwerk-Modus		
Netzwerk-Modus	NETWORKMODE	stealth | router
Router-Modus	ROUTER_MODE	static | dhcp
LINK-Modus	ROUTER_MODE_LINK	yes | no
Stealth-Konfiguration	STEALTH_MODE	autodetect | static | multi
Automatische Konfiguration: Ignoriere NetBIOS über TCP auf TCP Port 139	STEALTH_AUTO_IGNORE_TCP139	yes | no

Registerkarte: Stealth

Menü-Option	GAI-Variable	Format
Stealth-Management		
IP	STEALTH_MANAGE_IP	<ip>
Netzmaske	STEALTH_MANAGE_NET	<netmask>
VLAN verwenden	STEALTH_MANAGE_USE_VLAN	yes | no
VLAN-ID	STEALTH_MANAGE_VLAN_ID	<num>
IP-Adresse	STEALTH_MANAGE_ALIASES.x.MANAGE_IP	<ip>
Netzmaske	STEALTH_MANAGE_ALIASES.x.MANAGE_NET	<netmask>
VLAN verwenden	STEALTH_MANAGE_ALIASES.x.USE_VLAN	yes | no
VLAN-ID	STEALTH_MANAGE_ALIASES.x.VLAN_ID	<num>
Standard-Gateway	STEALTH_MANAGE_GW	<ip>
Route folgende Netzwerke über alternative Gateways		
Netzwerk	STEALTH_ALT_ROUTES.x.NETWORK	<cidr>
Gateway	STEALTH_ALT_ROUTES.x.GATEWAY	<ip>
Einstellungen Stealth-Modus (statisch)		
IP-Adresse des Clients	STEALTH_IP	<ip>
MAC-Adresse des Clients	STEALTH_MAC	<mac>

Registerkarte: Extern

Menü-Option	GAI-Variable	Format
Externe Netzwerke		
IP-Adresse	MY_ROUTER_IP	<ip>
Netzmaske	MY_ROUTER_NET	<netmask>
VLAN verwenden	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-Adresse	EXTERN_ALIASES.x.EXTERN_IP	<ip>
Netzmaske	EXTERN_ALIASES.x.EXTERN_NET	<netmask>
VLAN verwenden	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>
Zusätzliche externe Routen		
Netzwerk	EXTERN_ROUTES.x.NETWORK	<cidr>
Gateway	EXTERN_ROUTES.x.GATEWAY	<ip>
Standard-Gateway		
IP-Adresse des Standard-Gateways	DEFAULT_GW	<ip>

Registerkarte: Intern

Menü-Option	GAI-Variable	Format
Interne Netzwerke		
IP-Adresse	MY_LOCAL_IP	<ip>
Netzmaske	MY_LOCAL_NET	<netmask>
VLAN verwenden	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-Adresse	LOCAL_ALIASES.x.LOCAL_IP	<ip>
Netzmaske	LOCAL_ALIASES.x.LOCAL_NET	<netmask>
VLAN verwenden	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>
Zusätzliche interne Routen		
Netzwerk	LOCAL_ROUTES.x.NETWORK	<cidr>
Gateway	LOCAL_ROUTES.x.GATEWAY	<ip>

Registerkarte: DMZ

Menü-Option	GAI-Variable	Format
DMZ-Netzwerke		
IP-Adresse	DMZ_ALIASES.x.DMZ_IP	<ip>
Netzmaske	DMZ_ALIASES.x.DMZ_NET	<netmask>
OSPF-Area	DMZ_ALIASES.x.OSPF_AREA_REF	Empty for "None" | <rowref>
Zusätzliche DMZ-Routen		

Netzwerk	DMZ_ROUTES.x.NETWORK	<cidr>
Gateway	DMZ_ROUTES.x.GATEWAY	<ip>

4.2.2 Ethernet

Die Bezeichnung einiger GAI-Variablen hat sich mit der Version mGuard 10.3 geändert. In diesem Handbuch wird die alte Bezeichnung zusätzlich in Klammern angegeben.

Registerkarte: MAU-Einstellungen

Menü-Option	GAI-Variable	Format
Port-Mirroring		
Port-Mirroring-Empfänger	MIRROR_RECEIVER (Alte Bezeichnung: PORT_MIRROR_RECEIVER)	off | | swp0 | swp1 | swp2
MAU-Konfiguration		
Automatische Konfiguration	ENABLE_ETH0_AUTONEG	yes | no
Manuelle Konfiguration	ETH0_FIXEDSETTING	100fd | 100hd | 10fd | 10hd
Port an	ENABLE_ETH0_MAU	yes | no
Link-Überwachung	ETH0_SUPERVISE	yes | no
Automatische Konfiguration	ENABLE_ETH1_AUTONEG	yes | no
Manuelle Konfiguration	ETH1_FIXEDSETTING	100fd | 100hd | 10fd | 10hd
Port an	ENABLE_ETH1_MAU	yes | no
Link-Überwachung	ETH1_SUPERVISE	yes | no
Automatische Konfiguration	SWITCHPORT.x.AUTONEG (Alte Bezeichnung: PHY_SETTING.x.AUTONEG)	autoneg | noautoneg
Manuelle Konfiguration	SWITCHPORT.x.FIXEDSETTING (Alte Bezeichnung: PHY_SETTING.x.FIXEDSETTING)	100fd | 100hd | 10fd | 10hd
Port an	SWITCHPORT.x.POWER_UP (Alte Bezeichnung: PHY_SETTING.x.POWER_UP)	up | down
Port-Mirroring	SWITCHPORT.x.MIRROR (Alte Bezeichnung: PHY_SETTING.x.MIRROR)	none | ingress | egress | both
Link-Überwachung	SWITCHPORT.x.SUPERVISE (Alte Bezeichnung: PHY_SETTING.x.SUPERVISE)	yes | no
Port-Bezeichnung: x = 0 = XF2 x = 1 = XF3 x = 2 = XF4 x = 3 = DMZ (XF5)		

Registerkarte: Multicast

Menü-Option	GAI-Variable	Format
Statische Multicast-Gruppen		

Multicast-Gruppen-Adresse	MULTICAST_GROUP.x.MAC (Alte Bezeichnung: STATIC_MULTICAST_GROUP.x.MAC)	<mac>
XF2	MULTICAST_GROUP.x.PORT0 (Alte Bezeichnung: STATIC_MULTICAST_GROUP.x.PORT0)	yes | no
XF3	MULTICAST_GROUP.x.PORT1 (Alte Bezeichnung: STATIC_MULTICAST_GROUP.x.PORT1)	yes | no
XF4	MULTICAST_GROUP.x.PORT2 (Alte Bezeichnung: STATIC_MULTICAST_GROUP.x.PORT2)	yes | no
WAN	MULTICAST_GROUP.x.INTERNAL (Alte Bezeichnung: STATIC_MULTICAST_GROUP.x.INTERNAL)	yes | no
Allgemeine Multicast-Konfiguration		
IGMP-Snooping	IGMP_SNOOP	yes | no
IGMP-Snoop-Aging	IGMP_SNOOP_AGING	<num>
IGMP-Anfrage	IGMP_QUERY	off | v2
IGMP-Anfragen-Intervall	IGMP_QUERY_INTERVAL	<num>

Registerkarte: Ethernet

Menü-Option	GAI-Variable	Format
ARP-Timeout		
ARP-Timeout	ARP_TIMEOUT	<num>
MTU-Einstellungen		
MTU des internen Interface	MY_LOCAL_DEV_MTU	<num>
MTU des internen Interface für VLAN	MY_LOCAL_DEV_VLAN_MTU	<num>
MTU des externen Interface	MY_ROUTER_DEV_MTU	<num>
MTU des externen Interface für VLAN	MY_ROUTER_DEV_VLAN_MTU	<num>
MTU des DMZ Interface	MY_DMZ_DEV_MTU	<num>
MTU des Management-Interface	STEALTH_MTU	<num>
MTU des Management-Interface für VLAN	STEALTH_VLAN_MTU	<num>

4.2.3 NAT

Registerkarte: Maskierung

Menü-Option	GAI-Variable	Format
Network Address Translation/IP-Masquerading		
Ausgehend über Interface	FW_NAT.x.EXT_IF	ext1 | dmz0 | all | int
Von IP	FW_NAT.x.IN_IP	<rowref> | <ip> | <cidr>
Kommentar	FW_NAT.x.COMMENT	<txt>
1:1-NAT		
Reales Netzwerk	FW_1TO1_NAT.x.LOCAL_NET	<ip>
Virtuelles Netzwerk	FW_1TO1_NAT.x.REMOTE_NET	<ip>
Netzmaske	FW_1TO1_NAT.x.MASK	<num>
ARP aktivieren	FW_1TO1_NAT.x.ENABLE_ARP	yes | no
Kommentar	FW_1TO1_NAT.x.COMMENT	<txt>

Registerkarte: IP- und Port-Weiterleitung

Menü-Option	GAI-Variable	Format
IP- und Port-Weiterleitung		
Protokoll	FW_PORTFORWARDING.x.PROTO	tcp | udp | gre
Von IP	FW_PORTFORWARDING.x.SRC_IP	<rowref> | <ip> | <cidr>
Von Port	FW_PORTFORWARDING.x.SRC_PORT	<num> | <num>:<num> | <rowref>
Eintreffend auf IP	FW_PORTFORWARDING.x.IN_IP	<ip> | %extern
Eintreffend auf Port	FW_PORTFORWARDING.x.IN_PORT	<num>
Weiterleiten an IP	FW_PORTFORWARDING.x.OUT_IP	<ip>
Weiterleiten an Port	FW_PORTFORWARDING.x.OUT_PORT	<num>
Kommentar	FW_PORTFORWARDING.x.COMMENT	<txt>
Log	FW_PORTFORWARDING.x.LOG	yes | no

4.2.4 DNS

Registerkarte: DNS-Server

Menü-Option	GAI-Variable	Format
DNS		
Zu benutzende Nameserver	DNSCACHE_MODE	root | provider | user
Benutzerdefinierte DNS-Server		
IP	DNSCACHE_USER_DEFINED.x.IP	<ip>
Lokale Auflösung von Hostnamen		
Aktiv	DNS_ZONE.x.ZONE_ENABLED	yes | no
Domain-Name	DNS_ZONE.x.DOMAIN_NAME	<txt>

Registerkarte: DNS-Einträge

Menü-Option	GAI-Variable	Format
Lokale Auflösung von Hostnamen		
Domain-Name	DNS_ZONE.x.DOMAIN_NAME	<txt>
Aktiv	DNS_ZONE.x.ZONE_ENABLED	yes | no
Auch IP-Adressen auflösen	DNS_ZONE.x.AUTO_RR_PTR_ENABLED	yes | no
Hostnamen		
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>

Registerkarte: DynDNS

Menü-Option	GAI-Variable	Format
DynDNS		
Den mGuard bei einem DynDNS-Service anmelden	VPN_DYNIP_REGISTER	yes | no
Abfrageintervall	VPN_DYNIP_REGISTER_INTERVAL	<num>
DynDNS-Anbieter	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-Benutzerkennung	VPN_DYNIP_LOGIN	<txt>
DynDNS-Passwort	VPN_DYNIP_PASSWD	<txt>
DynDNS-Hostname	VPN_DYNIP_HOSTNAME	<txt>

4.2.5 DHCP

Registerkarte: Internes DHCP

Menü-Option	GAI-Variable	Format
Modus		
DHCP-Modus	DHCP_INT_ENABLE	no | yes | yes-relay
DHCP-Server-Optionen		
Dynamischen IP-Adres-spool aktivieren	DHCP_INT_POOL	yes | no
DHCP-Lease-Dauer	DHCP_INT_LEASE_TIME	<num>
DHCP-Bereichsanfang	DHCP_INT_START	<ip>
DHCP-Bereichsende	DHCP_INT_END	<ip>
Lokale Netzmaske	DHCP_INT_MASK	<netmask>
Broadcast-Adresse	DHCP_INT_BROADCAST	<ip>
Standard-Gateway	DHCP_INT_GW	<ip>
DNS-Server	DHCP_INT_DNS	<ip>
WINS-Server	DHCP_INT_WINS	<ip>
Statische Zuordnung		
MAC-Adresse des Clients	DHCP_STATIC_INT.x.MAC	<mac>
IP-Adresse des Clients	DHCP_STATIC_INT.x.IP	<ip>
Kommentar	DHCP_STATIC_INT.x.COMMENT	<txt>
Weiterleitung an (Relay to)		
IP	DHCP_RELAY_INT_SERVER.x.IP	<ip>
DHCP-Relay-Optionen		
Füge Relay-Agent-Infor-mation (Option 82) an	DHCP_RELAY_INT_APPEND_AGENT_INFORMATION	yes | no

Registerkarte: Externes DHCP

Menü-Option	GAI-Variable	Format
Modus		
DHCP-Modus	DHCP_EXT_ENABLE	no | yes | yes-relay
DHCP-Server-Optionen		
Dynamischen IP-Adres-spool aktivieren	DHCP_EXT_POOL	yes | no
DHCP-Lease-Dauer	DHCP_EXT_LEASE_TIME	<num>
DHCP-Bereichsanfang	DHCP_EXT_START	<ip>
DHCP-Bereichsende	DHCP_EXT_END	<ip>
Lokale Netzmaske	DHCP_EXT_MASK	<netmask>
Broadcast-Adresse	DHCP_EXT_BROADCAST	<ip>
Standard-Gateway	DHCP_EXT_GW	<ip>
DNS-Server	DHCP_EXT_DNS	<ip>
WINS-Server	DHCP_EXT_WINS	<ip>

Statische Zuordnung		
MAC-Adresse des Clients	DHCP_STATIC_EXT.x.MAC	<mac>
IP-Adresse des Clients	DHCP_STATIC_EXT.x.IP	<ip>
Kommentar	DHCP_STATIC_EXT.x.COMMENT	<txt>
Weiterleitung an (Relay to)		
IP	DHCP_RELAY_EXT_SERVER.x.IP	<ip>
DHCP-Relay-Optionen		
Füge Relay-Agent-Information (Option 82) an	DHCP_RELAY_EXT_APPEND_AGENT_INFORMATION	yes | no

Registerkarte: DMZ DHCP

Menü-Option	GAI-Variable	Format
Modus		
Aktiviere DHCP-Server auf dem DMZ-Port	DHCP_DMZ_ENABLE	yes | no
DHCP-Server-Optionen		
Dynamischen IP-Adressspool aktivieren	DHCP_DMZ_POOL	yes | no
DHCP-Lease-Dauer	DHCP_DMZ_LEASE_TIME	<num>
DHCP-Bereichsanfang	DHCP_DMZ_START	<ip>
DHCP-Bereichsende	DHCP_DMZ_END	<ip>
Lokale Netzmaske	DHCP_DMZ_MASK	<netmask>
Broadcast-Adresse	DHCP_DMZ_BROADCAST	<ip>
Standard-Gateway	DHCP_DMZ_GW	<ip>
DNS-Server	DHCP_DMZ_DNS	<ip>
WINS-Server	DHCP_DMZ_WINS	<ip>
Statische Zuordnung		
MAC-Adresse des Clients	DHCP_STATIC_DMZ.x.MAC	<mac>
IP-Adresse des Clients	DHCP_STATIC_DMZ.x.IP	<ip>
Kommentar	DHCP_STATIC_DMZ.x.COMMENT	<txt>

4.2.6 Proxy-Einstellungen

Registerkarte: HTTP(S) Proxy-Einstellungen

Menü-Option	GAI-Variable	Format
HTTP(S) Proxy-Einstellungen		
Proxy für HTTP und HTTPS benutzen (wird auch für die VPN-TCP-Kapselung verwendet)	PROXY_HTTP_ENABLE	yes | no
HTTP(S)-Proxy-Server	PROXY_HTTP_URL	<ip> | <txt>
Port	PROXY_HTTP_PORT	<num>
Proxy-Authentifizierung		
Login	PROXY_HTTP_LOGIN	<txt>
Passwort	PROXY_HTTP_PASSWORD	<txt>

4.2.7 Dynamisches Routing

Registerkarte: OSPF

Menü-Option	GAI-Variable	Format
Aktivierung		
OSPF aktivieren	OSPF_ENABLE	yes | no
OSPF-Hostname (überschreibt den globalen Hostnamen)	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
Authentifizierung	OSPF_AREA.x.AUTH	none | simple | digest
Zusätzliche Interface-Einstellungen		
Interface	OSPF_INTERFACE.x.ID	int | ext1 | dmz
Passives Interface	OSPF_INTERFACE.x.PASSIVE	yes | no
Authentifizierung (überschreibt Authentifizierungsmethode der Area)	OSPF_INTERFACE.x.AUTH	none | digest
Passwort Simple-Authentifizierung	OSPF_INTERFACE.x.SIMPLE_KEY	<txt>
Digest-Key	OSPF_INTERFACE.x.DIGEST_KEY	<txt>
Digest-Key-ID	OSPF_INTERFACE.x.DIGEST_KEY_ID	<num>
Routen-Weiterverbreitung		
Typ	OSPF_REDISTRIBUTION.x.ROUTE_TYPE	connected | kernel
Metrik	OSPF_REDISTRIBUTION.x.METRIC	<num>
Access-Liste	OSPF_REDISTRIBUTION.x.ACCESS_LIST_REF	Empty for "None" | <rowref>

Registerkarte: Distributions-Einstellungen

Menü-Option	GAI-Variable	Format
Access-Listen		
Name	DYNROUTING_ACCESSLIST.x.NAME	<txt>

Registerkarte: Access-Listen-Einstellungen

Menü-Option	GAI-Variable	Format
Einstellungen		
Name	DYNROUTING_ACCESSLIST.x.NAME	<txt>
Zuordnungen		

Zulassen/Ablehnen	DYNROUTING_ACCESSLIST.x.ENTRY.y.PERMIT	permit | deny
Netzwerk	DYNROUTING_ACCESSLIST.x.ENTRY.y.NET	<cidr>

4.3 Authentifizierung

4.3.1 Administrative Benutzer

Registerkarte: Passwörter

Menü-Option	GAI-Variable	Format
Account: root		
Root-Passwort	ROOT_PASSWORD	<txt>
Account: admin		
Administrator-Passwort	WWW_PASSWORD	<txt>
Account: user		
Benutzerpasswort	USER_PASSWORD	<txt>
Deaktiviere das VPN, bis sich der Benutzer über HTTPS authentifiziert	USER_LOGIN_REQUIRED	yes | no

Registerkarte: RADIUS-Filter

Menü-Option	GAI-Variable	Format
RADIUS-Filter für administrativen Zugriff		
Gruppen-/Filter-ID	RADIUS_FILTER.x.FILTER_ID	<txt>
Für den Zugriff autorisiert als	RADIUS_FILTER.x.ROLE	admin | netadmin | audit

4.3.2 Firewall-Benutzer

Registerkarte: Firewall-Benutzer

Menü-Option	GAI-Variable	Format
Benutzer		
Aktiviere Benutzerfirewall	USERFW_ENABLE	yes | no
Aktiviere Gruppenauthentifizierung	USERFW_GROUP_AUTH_ENABLE	yes | no
Benutzerkennung	USERFW_USERS.x.USERNAME	<txt>
Authentisierungsverfahren	USERFW_USERS.x.AUTHMETHOD	radius | local
Benutzerpasswort	USERFW_USERS.x.PLAINPASSWORD	<txt>
Zugang (Authentisierung per HTTPS über)		
Interface	USERFW_INTERFACES.x.INTERFACE	int | ext1 | dmz0 | ipsec

4.3.3 RADIUS

Registerkarte: RADIUS-Server

Menü-Option	GAI-Variable	Format
RADIUS-Server		
RADIUS-Timeout	RADIUS_TIMEOUT	<num>
RADIUS-Wiederholungen	RADIUS_RETRIES	<num>
RADIUS-NAS-Identifier	RADIUS_NAS	<txt>
Server	RADIUS_SERVERS.x.RADSERVER	<ip> | <txt>
Über 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 Zertifikate

Registerkarte: Zertifikatseinstellungen

Menü-Option	GAI-Variable	Format
Zertifikatseinstellungen		
Beachte den Gültigkeitszeitraum von Zertifikaten und CRLs	IGNORE_CERT_TIMES	never | synced | always
CRL-Prüfung aktivieren	CRL_CHECKING	yes | no
CRL-Download-Intervall	CRL_PULL_INTERVAL	0 | 900 | 1800 | 3600 | 7200 | 21600 | 43200 | 86400 | 30

Registerkarte: Maschinenzertifikate

Menü-Option	GAI-Variable	Format
Maschinenzertifikate		
Kurzname	PRIVATE_CERTS.x.FRIENDLY_NAME	<txt>

Registerkarte: CA-Zertifikate

Menü-Option	GAI-Variable	Format
Vertrauenswürdige CA-Zertifikate		
Kurzname	CA_CERTS.x.FRIENDLY_NAME	<txt>

Registerkarte: Gegenstellen-Zertifikate

Menü-Option	GAI-Variable	Format
Vertrauenswürdige Gegenstellen-Zertifikate		
Kurzname	REMOTE_CERTS.x.FRIENDLY_NAME	<txt>

Registerkarte: CRL

Menü-Option	GAI-Variable	Format
Certificate Revocation List (CRL)		
URL	CRL_STORE.x.URI	<txt>
Über VPN	CRL_STORE.x.PREFER_VPN	yes | no

Registerkarte: Zertifikatsregistrierung

Menü-Option	GAI-Variable	Format
CA-Server für Zertifikatserneuerung		
Server	CERT_ENROLL_CA_HOST	<ip> | <txt>
Port	CERT_ENROLL_CA_PORT	<num>
Verzeichnis	CERT_ENROLL_CA_DIR	<txt>
Einstellungen		

Root-CA-Zertifikat der Zertifizierungsstelle	CERT_ENROLL_CA_REF	Empty for "None" | <rowref>
Bei Zertifikatserneuerung einen neuen Schlüssel erstellen	CERT_ENROLL_KEY_UPDATE	yes | no

4.4 Netzwerksicherheit

4.4.1 Paketfilter

Registerkarte: Eingangsregeln

Menü-Option	GAI-Variable	Format
Eingehend		
Allgemeine Firewall-Einstellung	FW_INCOMING_GLOBAL	accept | drop | ping | rules
Interface	FW_INCOMING.x.EXT_IF	ext1 | all
Protokoll	FW_INCOMING.x.PROTO	tcp | udp | icmp | gre | all
Von IP	FW_INCOMING.x.FROM_IP	<rowref> | <ip> | <cidr>
Von Port	FW_INCOMING.x.FROM_PORT	<num> | <num>:<num> | <rowref>
Nach IP	FW_INCOMING.x.IN_IP	<rowref> | <ip> | <cidr>
Nach Port	FW_INCOMING.x.IN_PORT	<num> | <num>:<num> | <rowref>
Aktion	FW_INCOMING.x.TARGET_REF	<rowref> | ACCEPT | DROP | REJECT
Kommentar	FW_INCOMING.x.COMMENT	<txt>
Log	FW_INCOMING.x.LOG	yes | no
Erstelle Log-Einträge für unbekannte Verbindungsversuche	LOG_DEFAULT_INCOMING	yes | no

Registerkarte: Ausgangsregeln

Menü-Option	GAI-Variable	Format
Ausgehend		
Allgemeine Firewall-Einstellung	FW_OUTGOING_GLOBAL	accept | drop | ping | rules
Protokoll	FW_OUTGOING.x.PROTO	tcp | udp | icmp | gre | all
Von IP	FW_OUTGOING.x.FROM_IP	<rowref> | <ip> | <cidr>
Von Port	FW_OUTGOING.x.FROM_PORT	<num> | <num>:<num> | <rowref>
Nach IP	FW_OUTGOING.x.IN_IP	<rowref> | <ip> | <cidr>

Nach Port	FW_OUTGOING.x.IN_PORT	<num> | <num>:<num> | <rowref>
Aktion	FW_OUTGOING.x.TARGET_REF	<rowref> | ACCEPT | DROP | REJECT
Kommentar	FW_OUTGOING.x.COMMENT	<txt>
Log	FW_OUTGOING.x.LOG	yes | no
Erstelle Log-Einträge für unbekannte Verbindungsversuche	LOG_DEFAULT_OUTGOING	yes | no

Registerkarte: DMZ

Menü-Option	GAI-Variable	Format
WAN → DMZ		
Protokoll	FW_INCOMING_WAN_DMZ.x.PROTO	tcp | udp | icmp | gre | all
Von IP	FW_INCOMING_WAN_DMZ.x.FROM_IP	<rowref> | <ip> | <cidr>
Von Port	FW_INCOMING_WAN_DMZ.x.FROM_PORT	<num> | <num>:<num> | <rowref>
Nach IP	FW_INCOMING_WAN_DMZ.x.IN_IP	<rowref> | <ip> | <cidr>
Nach Port	FW_INCOMING_WAN_DMZ.x.IN_PORT	<num> | <num>:<num> | <rowref>
Aktion	FW_INCOMING_WAN_DMZ.x.TARGET_REF	<rowref> | ACCEPT | DROP | REJECT
Kommentar	FW_INCOMING_WAN_DMZ.x.COMMENT	<txt>
Log	FW_INCOMING_WAN_DMZ.x.LOG	yes | no
Erstelle Log-Einträge für unbekannte Verbindungsversuche	LOG_DEFAULT_INCOMING_WAN_DMZ	yes | no
DMZ → LAN		
Protokoll	FW_INCOMING_DMZ_LAN.x.PROTO	tcp | udp | icmp | gre | all
Von IP	FW_INCOMING_DMZ_LAN.x.FROM_IP	<rowref> | <ip> | <cidr>
Von Port	FW_INCOMING_DMZ_LAN.x.FROM_PORT	<num> | <num>:<num> | <rowref>
Nach IP	FW_INCOMING_DMZ_LAN.x.IN_IP	<rowref> | <ip> | <cidr>
Nach Port	FW_INCOMING_DMZ_LAN.x.IN_PORT	<num> | <num>:<num> | <rowref>
Aktion	FW_INCOMING_DMZ_LAN.x.TARGET_REF	<rowref> | ACCEPT | DROP | REJECT
Kommentar	FW_INCOMING_DMZ_LAN.x.COMMENT	<txt>
Log	FW_INCOMING_DMZ_LAN.x.LOG	yes | no
Erstelle Log-Einträge für unbekannte Verbindungsversuche	LOG_DEFAULT_INCOMING_DMZ_LAN	yes | no
DMZ → WAN		
Protokoll	FW_OUTGOING_DMZWAN.x.PROTO	tcp | udp | icmp | gre | all

Von IP	FW_OUTGOING_DMZWAN.x.FROM_IP	<rowref> | <ip> | <cidr>
Von Port	FW_OUTGOING_DMZWAN.x.FROM_PORT	<num> | <num>:<num> | <rowref>
Nach IP	FW_OUTGOING_DMZWAN.x.IN_IP	<rowref> | <ip> | <cidr>
Nach Port	FW_OUTGOING_DMZWAN.x.IN_PORT	<num> | <num>:<num> | <rowref>
Aktion	FW_OUTGOING_DMZWAN.x.TARGET_REF	<rowref> | ACCEPT | DROP | REJECT
Kommentar	FW_OUTGOING_DMZWAN.x.COMMENT	<txt>
Log	FW_OUTGOING_DMZWAN.x.LOG	yes | no
Erstelle Log-Einträge für unbekannte Verbindungsversuche	LOG_DEFAULT_OUTGOING_DMZ_WAN	yes | no
LAN → DMZ		
Protokoll	FW_OUTGOING_LANDMZ.x.PROTO	tcp | udp | icmp | gre | all
Von IP	FW_OUTGOING_LANDMZ.x.FROM_IP	<rowref> | <ip> | <cidr>
Von Port	FW_OUTGOING_LANDMZ.x.FROM_PORT	<num> | <num>:<num> | <rowref>
Nach IP	FW_OUTGOING_LANDMZ.x.IN_IP	<rowref> | <ip> | <cidr>
Nach Port	FW_OUTGOING_LANDMZ.x.IN_PORT	<num> | <num>:<num> | <rowref>
Aktion	FW_OUTGOING_LANDMZ.x.TARGET_REF	<rowref> | ACCEPT | DROP | REJECT
Kommentar	FW_OUTGOING_LANDMZ.x.COMMENT	<txt>
Log	FW_OUTGOING_LANDMZ.x.LOG	yes | no
Erstelle Log-Einträge für unbekannte Verbindungsversuche	LOG_DEFAULT_OUTGOING_LAN_DMZ	yes | no

Registerkarte: Regelsätze

Menü-Option	GAI-Variable	Format
Regelsätze		
Initialer Modus	FW_RULESETS.x.SET_ACTIVE	disabled | inactive | active
Schaltender Service-Eingang oder VPN-Verbindung	FW_RULESETS.x.CONTROL	none | cmd1 | cmd2 | cmd3 | <rowref>
Ein beschreibender Name	FW_RULESETS.x.FRIENDLY_NAME	<txt>

Registerkarte: Regelsatz

Menü-Option	GAI-Variable	Format
Allgemein		
Ein beschreibender Name	FW_RULESETS.x.FRIENDLY_NAME	<txt>
Initialer Modus	FW_RULESETS.x.SET_ACTIVE	disabled | inactive | active
Schaltender Service-Eingang oder VPN-Verbindung	FW_RULESETS.x.CONTROL	none | cmd1 | cmd2 | cmd3 | <rowref>
Invertierte Logik verwenden	FW_RULESETS.x.CONTROL_INV	yes | no
Timeout zur Deaktivierung	FW_RULESETS.x.TIMEOUT	<num>
Firewall-Regeln		
Protokoll	FW_RULESETS.x.SET.y.PROTO	tcp | udp | icmp | all
Von IP	FW_RULESETS.x.SET.y.FROM_IP	<rowref> | <ip> | <cidr>
Von Port	FW_RULESETS.x.SET.y.FROM_PORT	<num> | <num>:<num> | <rowref>
Nach IP	FW_RULESETS.x.SET.y.IN_IP	<rowref> | <ip> | <cidr>
Nach Port	FW_RULESETS.x.SET.y.IN_PORT	<num> | <num>:<num> | <rowref>
Aktion	FW_RULESETS.x.SET.y.TARGET_REF	<rowref> | ACCEPT | DROP | REJECT
Kommentar	FW_RULESETS.x.SET.y.COMMENT	<txt>
Log	FW_RULESETS.x.SET.y.LOG	yes | no

Registerkarte: MAC-Filter

Menü-Option	GAI-Variable	Format
Eingehend		

Quell-MAC	STEALTH_L2_FILTER_EXTERN.x.SOURCE_MAC	<mac>
Ziel-MAC	STEALTH_L2_FILTER_EXTERN.x.DEST_MAC	<mac>
Ethernet-Protokoll	STEALTH_L2_FILTER_EXTERN.x.ETHERTYPE_HEX	%any | arp | ipv4 | length | <hex>
Aktion	STEALTH_L2_FILTER_EXTERN.x.TARGET	ACCEPT | DROP
Kommentar	STEALTH_L2_FILTER_EXTERN.x.COMMENT	<txt>
Ausgehend		
Quell-MAC	STEALTH_L2_FILTER_INTERN.x.SOURCE_MAC	<mac>
Ziel-MAC	STEALTH_L2_FILTER_INTERN.x.DEST_MAC	<mac>
Ethernet-Protokoll	STEALTH_L2_FILTER_INTERN.x.ETHERTYPE_HEX	%any | arp | ipv4 | length | <hex>
Aktion	STEALTH_L2_FILTER_INTERN.x.TARGET	ACCEPT | DROP
Kommentar	STEALTH_L2_FILTER_INTERN.x.COMMENT	<txt>

Registerkarte: IP- und Portgruppen

Menü-Option	GAI-Variable	Format
IP-Gruppen		
Name	FW_GROUP_IP.x.NAME	<txt>
Kommentar	FW_GROUP_IP.x.COMMENT	<txt>

Registerkarte: Einstellung IP-Gruppen

Menü-Option	GAI-Variable	Format
Einstellungen		
Name	FW_GROUP_IP.x.NAME	<txt>
Kommentar	FW_GROUP_IP.x.COMMENT	<txt>
Hostname, IP, IP-Bereich oder Netzwerk	FW_GROUP_IP.x.ENTRY.y.IP	<ip>-<ip> | <cidr> | <txt>
Portgruppen		
Name	FW_GROUP_PORT.x.NAME	<txt>
Kommentar	FW_GROUP_PORT.x.COMMENT	<txt>

Registerkarte: Einstellung Portgruppen

Menü-Option	GAI-Variable	Format
Einstellungen		
Name	FW_GROUP_PORT.x.NAME	<txt>
Kommentar	FW_GROUP_PORT.x.COMMENT	<txt>
Port oder Portbereich	FW_GROUP_PORT.x.ENTRY.y.PORT	<num> | <num>-<num>

Registerkarte: Erweitert

Menü-Option	GAI-Variable	Format
Globale Filter		
TCP-Pakete mit gesetztem URGENT-Flag blockieren	TCP_BLOCK_URG	yes | no
Konsistenzprüfungen		
Maximale Länge für "Ping"-Pakete (ICMP-Echo-Anfrage)	ICMP_LENGTH_MAX	<num>
Aktiviere TCP/UDP/ICMP-Konsistenzprüfungen	IP_UNCLEAN_MATCH	yes | no
Erlaube TCP-Keepalive-Pakete ohne TCP-Flags	NF_CONNTRACK_TCP_NOFLAGS_EST	yes | no
Netzwerkmodi (Router/PPTP/PPPoE)		
ICMP via primärem externen Interface für den mGuard	FW_ICMP	drop | ping | all
ICMP via DMZ-Interface für den mGuard	FW_ICMP_DMZ0	drop | ping | all
Stealth-Modus		
Erlaube Weiterleitung von GVRP-Paketen	STEALTH_ENABLE_GVRP_FORWARDING	yes | no
Erlaube Weiterleitung von STP-Paketen	STEALTH_ENABLE_STP_FORWARDING	yes | no
Erlaube Weiterleitung von DHCP-Paketen	STEALTH_ENABLE_DHCP_FORWARDING	yes | no
Verbindungs-Verfolgung (Connection Tracking)		
Maximale Zahl gleichzeitiger Verbindungen	IP_CONNTRACK_MAX	<num>
Erlaube TCP-Verbindungen nur mit SYN (Nach einem Neustart müssen Verbindungen neu aufgebaut werden.)	FW_NEW_CONNECTIONS_UPON_SYN_ONLY	yes | no
Timeout für aufgebaute TCP-Verbindungen	IP_CONNTRACK_TCP_TIMEOUT_ESTABLISHED	<num>
Timeout für geschlossene TCP-Verbindungen	IP_CONNTRACK_TCP_TIMEOUT_CLOSE_WAIT	<num>
Bestehende Verbindungen nach Ã„nderungen an der Firewall zurücksetzen	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 Deep Packet Inspection

Registerkarte: Modbus TCP

Menü-Option	GAI-Variable	Format
Regelsätze		
Name	MODBUS_RULESETS.x.FRIENDLY_NAME	<txt>

Registerkarte: Modbus-TCP-Regelsatz

Menü-Option	GAI-Variable	Format
Optionen		
Name	MODBUS_RULESETS.x.FRIENDLY_NAME	<txt>
Filterregeln		
Funktionscode	MODBUS_RULESETS.x.SET.y.MODBUS_FUNCTION_CODE	any | <num>
PDU-Adressen	MODBUS_RULESETS.x.SET.y.ADDRESS_RANGE	any | <num>
Aktion	MODBUS_RULESETS.x.SET.y.TARGET	ACCEPT | DROP
Kommentar	MODBUS_RULESETS.x.SET.y.COMMENT	<txt>
Log	MODBUS_RULESETS.x.SET.y.LOG	yes | no
Erstelle Log-Einträge für unbekannte Pakete	MODBUS_RULESETS.x.LOG_DEFAULT	yes | no

Registerkarte: OPC Inspector

Menü-Option	GAI-Variable	Format
OPC Inspector		
OPC Classic	IP_CONNTRACK_OPC	yes | no
Gültigkeitsprüfung für OPC Classic	IP_CONNTRACK_OPC_SANITY	yes | no
Zeitspanne für OPC Classic Verbindungserwartungen	IP_CONNTRACK_OPC_TIMEOUT	<num>

4.4.3 DoS-Schutz

Registerkarte: Flood Protection

Menü-Option	GAI-Variable	Format
Maximale Anzahl neuer TCP-Verbindungen (SYN)		
Ausgehend	IP_SYNFLOOD_LIMIT_INT	<num>
Eingehend	IP_SYNFLOOD_LIMIT_EXT	<num>
Maximale Anzahl von Ping-Paketen (ICMP-Echo-Anfrage)		
Ausgehend	ICMP_LIMIT_INT	<num>
Eingehend	ICMP_LIMIT_EXT	<num>
Jeweils maximale Anzahl von ARP-Anfragen und ARP-Antworten		
Ausgehend	ARP_LIMIT_INT	<num>
Eingehend	ARP_LIMIT_EXT	<num>

4.4.4 Benutzerfirewall

Registerkarte: Benutzerfirewall-Templates

Menü-Option	GAI-Variable	Format
Aktiv	USERFW_TEMPLATE.x.TEMPLATE_ENABLED	yes | no
Ein beschreibender Name	USERFW_TEMPLATE.x.TEMPLATE_NAME	<txt>

Registerkarte: Allgemein

Menü-Option	GAI-Variable	Format
Optionen		
Ein beschreibender Name	USERFW_TEMPLATE.x.TEMPLATE_NAME	<txt>
Aktiv	USERFW_TEMPLATE.x.TEMPLATE_ENABLED	yes | no
Kommentar	USERFW_TEMPLATE.x.TEMPLATE_COMMENT	<txt>
Timeout	USERFW_TEMPLATE.x.TEMPLATE_TIMEOUT	<num>
Timeout-Typ	USERFW_TEMPLATE.x.TEMPLATE_TOUT_TYPE	static | dynamic
VPN-Verbindung	USERFW_TEMPLATE.x.VPN_CONN_REF	Empty for "None" | <rowref>

Registerkarte: Template-Benutzer

Menü-Option	GAI-Variable	Format
Benutzer		
Benutzer	USERFW_TEMPLATE.x.TEMPLATE_USERS.y.USERNAME	<txt>

Registerkarte: Firewall-Regeln

Menü-Option	GAI-Variable	Format
Firewall-Regeln		
Quell-IP	USERFW_TEMPLATE.x.TEMPLATE_SRC_IP	<ip> | %authorized_ip
Protokoll	USERFW_TEMPLATE.x.TEMPLATE_RULE.y.PROTO	tcp | udp | icmp | gre | all
Von Port	USERFW_TEMPLATE.x.TEMPLATE_RULE.y.SRC_PORT	<num> | <num>:<num> | <rowref>
Nach IP	USERFW_TEMPLATE.x.TEMPLATE_RULE.y.DST_IP	<rowref> | <ip> | <cidr>
Nach Port	USERFW_TEMPLATE.x.TEMPLATE_RULE.y.DST_PORT	<num> | <num>:<num> | <rowref>
Kommentar	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

Registerkarte: Optionen

Menü-Option	GAI-Variable	Format
Optionen		
Erlaube Paketweiterleitung zwischen VPN-Verbindungen	VPN_HUB_AND_SPOKE	yes | no
Archiviere Diagnosemeldungen zu VPN-Verbindungen	VPN_LOG_PERSIST_ENABLED	yes | no
Archiviere Diagnosemeldungen nur bei Fehlverhalten	VPN_LOG_PERSIST_FAILURES_ONLY	yes | no
TCP-Kapselung		
Horche auf eingehende VPN-Verbindungen, die eingekapselt sind	VPN_IPTUN_ENABLE	yes | no
TCP-Port, auf dem zu horchen ist	VPN_IPTUN_LISTEN_PORT	<num>
Server-ID (0-63)	VPN_IPTUN_POOL	<num>
Aktiviere Path Finder für mGuard Secure VPN Client	VPN_TCPENCAP_ENABLE	yes | no
TCP-Port, auf dem zu horchen ist	VPN_TCPENCAP_LISTEN_PORT	<num>
IP-Fragmentierung		
IKE-Fragmentierung	VPN_IKE_FRAGMENTATION	yes | no
MTU für IPsec (Voreinstellung ist 16260)	VPN_IPSEC0_MTU	<num>

Registerkarte: DynDNS-Überwachung

Menü-Option	GAI-Variable	Format
DynDNS-Überwachung		
Hostnamen von VPN-Gegenstellen überwachen	VPN_DYNIP_WATCH	yes | no
Abfrageintervall	VPN_DYNIP_WATCH_INTERVAL	<num>

4.5.2 Verbindungen

Registerkarte: Verbindungen

Menü-Option	GAI-Variable	Format
Verbindungen		
Initialer Modus	VPN_CONNECTION.x.VPN_START	disabled | stopped | started
Ein beschreibender Name für die Verbindung	VPN_CONNECTION.x.VPN_NAME	<txt>

Registerkarte: Allgemein

Menü-Option	GAI-Variable	Format
Optionen		
Ein beschreibender Name für die Verbindung	VPN_CONNECTION.x.VPN_NAME	<txt>
Initialer Modus	VPN_CONNECTION.x.VPN_START	disabled | stopped | started
Adresse des VPN-Gateways der Gegenstelle: (IP-Adresse, Hostname oder '%any' für beliebige IP-Adressen, mehrere Gegenstellen oder Gegenstellen hinter einem NAT-Router)	VPN_CONNECTION.x.VPN_GW	<ip> | <txt> | %any
Interface, das bei der Einstellung %any für das Gateway benutzt wird	VPN_CONNECTION.x.INTERFACE	int | ext1 | dmz0 | byIp
IP-Adresse, die bei der Einstellung %any für das Gateway benutzt wird	VPN_CONNECTION.x.HOST_IP	<ip>
Verbindungsinitiierung	VPN_CONNECTION.x.INITIATE	yes | no | on-demand
Schaltender Service-Eingang/CMD	VPN_CONNECTION.x.CONTROL	none | cmd1 | cmd2 | cmd3
Invertierte Logik verwenden	VPN_CONNECTION.x.CONTROL_INV	yes | no
Timeout zur Deaktivierung	VPN_CONNECTION.x.TIMEOUT_SECONDS	<num>
Kapsele den VPN Datenverkehr in TCP ein	VPN_CONNECTION.x.IPTUN_ENABLE	no | yes | ncp

TCP-Port des Servers, welcher die gekapselte Verbindung annimmt	VPN_CONNECTION.x.IPTUN_DEST_PORT	<num>
Mode Configuration		
Mode Configuration	VPN_CONNECTION.x.MODECFG_XAUTH_MODE	off | server | client
Lokale virtuelle IP	VPN_CONNECTION.x.GUI_VIRTUAL_IP	<ip>
Lokal	VPN_CONNECTION.x.MODECFG_SERVER_LOCAL	fixed | splitinc-static
Lokales IP-Netzwerk	VPN_CONNECTION.x.GUI_MODECFG_SERVER_LOCAL	<cidr>
Netzwerk	VPN_CONNECTION.x.MODECFG_SERVER_LOCAL_NETWORKS.y.NETWORK	<cidr>
Gegenstelle	VPN_CONNECTION.x.MODECFG_SERVER_REMOTE	pool | isplitinc-static
IP-Netzwerk-Pool der Gegenstelle	VPN_CONNECTION.x.GUI_MODECFG_SERVER_REMOTE	<cidr>
Abschnittsgröße (Netzwerkgröße zwischen 0 und 32)	VPN_CONNECTION.x.MODECFG_POOL_TRANCH_SIZE	<num>
Netzwerk	VPN_CONNECTION.x.MODECFG_SERVER_REMOTE_NETWORKS.y.NETWORK	<cidr>
1. DNS-Server für die Gegenstelle	VPN_CONNECTION.x.MODECFG_DNS1	<ip>
2. DNS-Server für die Gegenstelle	VPN_CONNECTION.x.MODECFG_DNS2	<ip>
1. WINS-Server für die Gegenstelle	VPN_CONNECTION.x.MODECFG_WINS1	<ip>
2. WINS-Server für die Gegenstelle	VPN_CONNECTION.x.MODECFG_WINS2	<ip>
Lokales NAT	VPN_CONNECTION.x.GUI_MODECFG_CLIENT_LOCAL_NAT	none | masq
Lokales IP-Netzwerk	VPN_CONNECTION.x.GUI_MODECFG_CLIENT_LOCAL_MASQ_NET	<cidr>
Gegenstelle	VPN_CONNECTION.x.MODECFG_CLIENT_REMOTE	fixed | splitinc
IP-Netzwerk der Gegenstelle	VPN_CONNECTION.x.GUI_MODECFG_CLIENT_REMOTE	<cidr>
XAuth-Login	VPN_CONNECTION.x.XAUTH_LOGIN	<txt>
XAuth-Passwort	VPN_CONNECTION.x.XAUTH_PASSWORD	<txt>
Transport- und Tunneleinstellungen		
Aktiv	VPN_CONNECTION.x.TUNNEL.y.ENABLED	yes | no
Kommentar	VPN_CONNECTION.x.TUNNEL.y.COMMENT	<txt>
Typ	VPN_CONNECTION.x.TUNNEL.y.TYPE	tunnel | transport | modecfg
Lokal	VPN_CONNECTION.x.TUNNEL.y.LOCAL	<cidr>
Lokales NAT für IPsec-Tunnelverbindungen	VPN_CONNECTION.x.TUNNEL.y.LOCAL_NAT	none | 1to1nat | masq

Interne Netzwerkadresse für lokales Maskieren	VPN_CONNECTION.x.TUNNEL.y.LOCAL_MASQ_NET	<cidr>
Gegenstelle	VPN_CONNECTION.x.TUNNEL.y.REMOTE	<cidr>
Remote-NAT für IPsec-Tunnelverbindungen	VPN_CONNECTION.x.TUNNEL.y.REMOTE_NAT	none | 1to1nat | masq
Netzwerkadresse für 1:1-NAT im Remote-Netz	VPN_CONNECTION.x.TUNNEL.y.REMOTE_1TO1NAT	<ip>
Interne IP-Adresse zur Maskierung des Remote-Netzwerks	VPN_CONNECTION.x.TUNNEL.y.REMOTE_MASQ_IP	<ip>
Die virtuelle IP-Adresse für den Client im Stealth-Modus	VPN_CONNECTION.x.TUNNEL.y.VIRTUAL_IP	<ip>

Registerkarte: Allgemein

Menü-Option	GAI-Variable	Format
Optionen		
Aktiv	VPN_CONNECTION.x.TUNNEL.y.ENABLED	yes | no
Kommentar	VPN_CONNECTION.x.TUNNEL.y.COMMENT	<txt>
Typ	VPN_CONNECTION.x.TUNNEL.y.TYPE	tunnel | transport | modecfg
Lokal	VPN_CONNECTION.x.TUNNEL.y.LOCAL	<cidr>
Gegenstelle	VPN_CONNECTION.x.TUNNEL.y.REMOTE	<cidr>
Die virtuelle IP-Adresse für den Client im Stealth-Modus	VPN_CONNECTION.x.TUNNEL.y.VIRTUAL_IP	<ip>
Lokales NAT		
Lokales NAT für IPsec-Tunnelverbindungen	VPN_CONNECTION.x.TUNNEL.y.LOCAL_NAT	none | 1to1nat | masq
Interne Netzwerkadresse für lokales Maskieren	VPN_CONNECTION.x.TUNNEL.y.LOCAL_MASQ_NET	<cidr>
Reales Netzwerk	VPN_CONNECTION.x.TUNNEL.y.LOCAL_N_TO_N_NAT.z.FROM_NET	<ip>
Virtuelles Netzwerk	VPN_CONNECTION.x.TUNNEL.y.LOCAL_N_TO_N_NAT.z.TO_NET	<ip>
Netzmaske	VPN_CONNECTION.x.TUNNEL.y.LOCAL_N_TO_N_NAT.z.MASK	<num>
Kommentar	VPN_CONNECTION.x.TUNNEL.y.LOCAL_N_TO_N_NAT.z.COMMENT	<txt>
Remote-NAT		
Remote-NAT für IPsec-Tunnelverbindungen	VPN_CONNECTION.x.TUNNEL.y.REMOTE_NAT	none | 1to1nat | masq
Interne IP-Adresse zur Maskierung des Remote-Netzwerks	VPN_CONNECTION.x.TUNNEL.y.REMOTE_MASQ_IP	<ip>
Netzwerkadresse für 1:1-NAT im Remote-Netz	VPN_CONNECTION.x.TUNNEL.y.REMOTE_1TO1NAT	<ip>
Protokoll		
Protokoll	VPN_CONNECTION.x.TUNNEL.y.PROTOCOL	icmp | tcp | udp | all
Lokaler Port ('%all' für alle Ports, eine Nummer zwischen 1 und 65535 oder '%any' um den Vorschlag dem Client zu überlassen.)	VPN_CONNECTION.x.TUNNEL.y.LOCAL_PORT	<num> | %all | %any
Remote-Port ('%all' für alle Ports, eine Nummer zwischen 1 und 65535 oder '%any' um den Vorschlag dem Client zu überlassen.)	VPN_CONNECTION.x.TUNNEL.y.REMOTE_PORT	<num> | %all | %any

Dynamisches Routing		
Füge Kernel-Route zum Remote-Netz hinzu, um die Weiterverbreitung durch OSPF zu ermöglichen	VPN_CONNECTION.x.TUNNEL.y.DUMMY_ROUTE	yes | no

Registerkarte: Authentifizierung

Menü-Option	GAI-Variable	Format
Authentifizierung		
Authentisierungsverfahren	VPN_CONNECTION.x.VPN_AUTH	psk | x509
Pre-Shared Key (PSK)	VPN_CONNECTION.x.VPN_PSK	<txt>
ISAKMP-Modus (Bitte beachten Sie, dass der 'Aggressive Mode' angreifbar ist.)	VPN_CONNECTION.x.AGGRESSIVE	no | yes
Lokales X.509-Zertifikat	VPN_CONNECTION.x.LOCAL_CERT_REF	Empty for "None" | enrolled | <rowref>
Remote CA-Zertifikat	VPN_CONNECTION.x.REMOTE_CERT_REF	selfsigned | anyca | <rowref>
VPN-Identifier		
Lokal	VPN_CONNECTION.x.LOCAL_ID	<txt>
Gegenstelle	VPN_CONNECTION.x.REMOTE_ID	<txt>

Registerkarte: Firewall

Menü-Option	GAI-Variable	Format
Eingehend		
Allgemeine Firewall-Einstellung	VPN_CONNECTION.x.FW_INCOMING_GLOBAL	accept | drop | ping | rules
Protokoll	VPN_CONNECTION.x.FW_INCOMING.y.PROTO	tcp | udp | icmp | gre | all
Von IP	VPN_CONNECTION.x.FW_INCOMING.y.FROM_IP	<rowref> | <ip> | <cidr>
Von Port	VPN_CONNECTION.x.FW_INCOMING.y.FROM_PORT	<num> | <num>:<num> | <rowref>
Nach IP	VPN_CONNECTION.x.FW_INCOMING.y.IN_IP	<rowref> | <ip> | <cidr>
Nach Port	VPN_CONNECTION.x.FW_INCOMING.y.IN_PORT	<num> | <num>:<num> | <rowref>
Aktion	VPN_CONNECTION.x.FW_INCOMING.y.TARGET_REF	<rowref> | ACCEPT | DROP | REJECT
Kommentar	VPN_CONNECTION.x.FW_INCOMING.y.COMMENT	<txt>
Log	VPN_CONNECTION.x.FW_INCOMING.y.LOG	yes | no
Erstelle Log-Einträge für unbekannte Verbindungsversuche	VPN_CONNECTION.x.LOG_DEFAULT_INCOMING	yes | no
Ausgehend		
Allgemeine Firewall-Einstellung	VPN_CONNECTION.x.FW_OUTGOING_GLOBAL	accept | drop | ping | rules

Protokoll	VPN_CONNECTION.x.FW_OUTGOING.y.PROTO	tcp | udp | icmp | gre | all
Von IP	VPN_CONNECTION.x.FW_OUTGOING.y.FROM_IP	<rowref> | <ip> | <cidr>
Von Port	VPN_CONNECTION.x.FW_OUTGOING.y.FROM_PORT	<num> | <num>:<num> | <rowref>
Nach IP	VPN_CONNECTION.x.FW_OUTGOING.y.IN_IP	<rowref> | <ip> | <cidr>
Nach Port	VPN_CONNECTION.x.FW_OUTGOING.y.IN_PORT	<num> | <num>:<num> | <rowref>
Aktion	VPN_CONNECTION.x.FW_OUTGOING.y.TARGET_REF	<rowref> | ACCEPT | DROP | REJECT
Kommentar	VPN_CONNECTION.x.FW_OUTGOING.y.COMMENT	<txt>
Log	VPN_CONNECTION.x.FW_OUTGOING.y.LOG	yes | no
Erstelle Log-Einträge für unbekannte Verbindungsversuche	VPN_CONNECTION.x.LOG_DEFAULT_OUTGOING	yes | no

Registerkarte: IKE-Optionen

Menü-Option	GAI-Variable	Format
ISAKMP-SA (Schlüsselaustausch)		
Verschlüsselung	VPN_CONNECTION.x.VPN_IKE_PREF.y.ALG	des | 3des | aes128 | aes192 | aes256
Prüfsumme	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 (Datenaustausch)		
Verschlüsselung	VPN_CONNECTION.x.VPN_IPSEC_PREF.y.ALG	des | 3des | aes128 | aes192 | aes256 | null
Prüfsumme	VPN_CONNECTION.x.VPN_IPSEC_PREF.y.HASH	all | md5 | sha1 | sha2_256 | sha2_384 | sha2_512

Perfect Forward Secrecy (PFS) (Aktivierung empfohlen. Die Gegenstelle muss den gleichen Eintrag haben.)	VPN_CONNECTION.x.VPN_PFS	no | yes | modp1024 | modp1536 | modp2048 | modp3072 | modp4096 | modp6144 | modp8192
Lebensdauer und Grenzen		
ISAKMP-SA-Lebensdauer	VPN_CONNECTION.x.IKELIFETIME	<num>
IPsec-SA-Lebensdauer	VPN_CONNECTION.x.IPSECLIFETIME	<num>
IPsec-SA-Volumengrenze	VPN_CONNECTION.x.IPSEC_HARD_LIMIT_BYTES	<num>
Re-Key-Margin bzgl. der Lebensdauer (gilt für ISAKMP-SAs and IPsec-SAs)	VPN_CONNECTION.x.REKEYMARGIN	<num>
Re-Key-Margin bzgl. der Volumengrenze (gilt nur für IPsec SAs)	VPN_CONNECTION.x.IPSEC_REKEYMARGIN_BYTES	<num>
Re-Key-Fuzz (gilt für alle Re-Key-Margins)	VPN_CONNECTION.x.REKEYFUZZ	<num>
Keying-Versuche (0 bedeutet 'unbegrenzt')	VPN_CONNECTION.x.KEYINGTRIES	<num>
Dead Peer Detection		
Verzögerung bis zur nächsten Anfrage nach einem Lebenszeichen	VPN_CONNECTION.x.DPD_DELAY	<num>
Zeitüberschreitung bei Ausbleiben des Lebenszeichens, nach welcher die Gegenstelle für tot befunden wird	VPN_CONNECTION.x.DPD_TIMEOUT	<num>

4.5.3 L2TP über IPsec

Registerkarte: L2TP-Server

Menü-Option	GAI-Variable	Format
Einstellungen		
Starte L2TP-Server für IPsec/L2TP	L2TP_ENABLED	yes | no
Lokale IP-Adresse für L2TP-Verbindungen	L2TP_LOCAL	<ip>
Beginn des Remote-IP-Adressbereichs	L2TP_FROM	<ip>
Ende des Remote-IP-Adressbereichs	L2TP_TO	<ip>

4.6 OpenVPN-Client

4.6.1 Verbindungen

Registerkarte: Verbindungen

Menü-Option	GAI-Variable	Format
Verbindungen		
Initialer Modus	OPENVPN_CONNECTION.x.VPN_START	disabled | stopped | started
Ein beschreibender Name für die Verbindung	OPENVPN_CONNECTION.x.VPN_NAME	<txt>

Registerkarte: Allgemein

Menü-Option	GAI-Variable	Format
Optionen		
Ein beschreibender Name für die Verbindung	OPENVPN_CONNECTION.x.VPN_NAME	<txt>
Initialer Modus	OPENVPN_CONNECTION.x.VPN_START	disabled | stopped | started
Schaltender Service-Eingang/CMD	OPENVPN_CONNECTION.x.CONTROL	none | cmd1 | cmd2 | cmd3
Invertierte Logik verwenden	OPENVPN_CONNECTION.x.CONTROL_INV	yes | no
Timeout zur Deaktivierung	OPENVPN_CONNECTION.x.TIMEOUT_SECONDS	<num>
Verbindung		
Adresse des VPN-Gateways der Gegenstelle (IP-Adresse oder Hostname)	OPENVPN_CONNECTION.x.VPN_GW	<ip> | <txt>
Protokoll	OPENVPN_CONNECTION.x.PROTOCOL	tcp | udp
Lokaler Port	OPENVPN_CONNECTION.x.LOCAL_PORT	<num> | %any
Remote-Port	OPENVPN_CONNECTION.x.REMOTE_PORT	<num>

Registerkarte: Tunneleinstellungen

Menü-Option	GAI-Variable	Format
Remote-Netze		
Netzwerk	OPENVPN_CONNECTION.x.REMOTE.y.NET	<cidr>
Kommentar	OPENVPN_CONNECTION.x.REMOTE.y.COMMENT	<txt>
Tunneleinstellungen		
Lerne Remote-Netze vom Server	OPENVPN_CONNECTION.x.REMOTE_LEARN	yes | no
Verwende Komprimierung	OPENVPN_CONNECTION.x.PROTO_COMP	yes | no | adaptive | disabled

Datenverschlüsselung		
Verschlüsselungsalgorithmus	OPENVPN_CONNECTION.x.VPN_ENCRYPTION	aes-128-cbc | aes-192-cbc | aes-256-cbc | aes-128-gcm | aes-192-gcm | aes-256-gcm
Hash-Algorithmus (HMAC-Authentifizierung)	OPENVPN_CONNECTION.x.VPN_AUTH_HMAC	sha1 | sha256 | sha512
Key-Renegotiation	OPENVPN_CONNECTION.x.RENEG	yes | no
Key-Renegotiation-Intervall	OPENVPN_CONNECTION.x.RENEGTIME	<num>
Dead Peer Detection		
Verzögerung bis zur nächsten Anfrage nach einem Lebenszeichen	OPENVPN_CONNECTION.x.DPD_DELAY	<num>
Zeitüberschreitung bei Ausbleiben des Lebenszeichens, nach welcher die Gegenstelle für tot befunden wird	OPENVPN_CONNECTION.x.DPD_TIMEOUT	<num>

Registerkarte: Authentifizierung

Menü-Option	GAI-Variable	Format
Authentifizierung		
Authentisierungsverfahren	OPENVPN_CONNECTION.x.VPN_AUTH	simple | x509 | x509plus
Benutzerkennung	OPENVPN_CONNECTION.x.LOGIN	<txt>
Passwort	OPENVPN_CONNECTION.x.PASSWORD	<txt>
Lokales X.509-Zertifikat	OPENVPN_CONNECTION.x.LOCAL_CERT_REF	Empty for "None" | <rowref>
CA-Zertifikat (zur Verifizierung des Server-Zertifikats)	OPENVPN_CONNECTION.x.CA_CERT_REF	Empty for "None" | <rowref>
Pre-Shared Key für die TLS-Authentifizierung	OPENVPN_CONNECTION.x.TLS_AUTH	<txt>
Schlüsselrichtung für TLS-Authentifizierung	OPENVPN_CONNECTION.x.TLS_AUTH_KEY_DIRECTION	none | dir0 | dir1

Registerkarte: Firewall

Menü-Option	GAI-Variable	Format
Eingehend		
Allgemeine Firewall-Einstellung	OPENVPN_CONNECTION.x.FW_INCOMING_GLOBAL	accept | drop | ping | rules
Protokoll	OPENVPN_CONNECTION.x.FW_INCOMING.y.PROTO	tcp | udp | icmp | gre | all
Von IP	OPENVPN_CONNECTION.x.FW_INCOMING.y.FROM_IP	<rowref> | <ip> | <cidr>
Von Port	OPENVPN_CONNECTION.x.FW_INCOMING.y.FROM_PORT	<num> | <num>:<num> | <rowref>
Nach IP	OPENVPN_CONNECTION.x.FW_INCOMING.y.IN_IP	<rowref> | <ip> | <cidr>
Nach Port	OPENVPN_CONNECTION.x.FW_INCOMING.y.IN_PORT	<num> | <num>:<num> | <rowref>
Aktion	OPENVPN_CONNECTION.x.FW_INCOMING.y.TARGET_REF	<rowref> | ACCEPT | DROP | REJECT
Kommentar	OPENVPN_CONNECTION.x.FW_INCOMING.y.COMMENT	<txt>
Log	OPENVPN_CONNECTION.x.FW_INCOMING.y.LOG	yes | no
Erstelle Log-Einträge für unbekannte Verbindungsversuche	OPENVPN_CONNECTION.x.LOG_DEFAULT_INCOMING	yes | no
Ausgehend		
Allgemeine Firewall-Einstellung	OPENVPN_CONNECTION.x.FW_OUTGOING_GLOBAL	accept | drop | ping | rules
Protokoll	OPENVPN_CONNECTION.x.FW_OUTGOING.y.PROTO	tcp | udp | icmp | gre | all

Von IP	OPENVPN_CONNECTION.x.FW_OUTGOING.y.FROM_IP	<rowref> | <ip> | <cidr>
Von Port	OPENVPN_CONNECTION.x.FW_OUTGOING.y.FROM_PORT	<num> | <num>:<num> | <rowref>
Nach IP	OPENVPN_CONNECTION.x.FW_OUTGOING.y.IN_IP	<rowref> | <ip> | <cidr>
Nach Port	OPENVPN_CONNECTION.x.FW_OUTGOING.y.IN_PORT	<num> | <num>:<num> | <rowref>
Aktion	OPENVPN_CONNECTION.x.FW_OUTGOING.y.TARGET_REF	<rowref> | ACCEPT | DROP | REJECT
Kommentar	OPENVPN_CONNECTION.x.FW_OUTGOING.y.COMMENT	<txt>
Log	OPENVPN_CONNECTION.x.FW_OUTGOING.y.LOG	yes | no
Erstelle Log-Einträge für unbekannte Verbindungsversuche	OPENVPN_CONNECTION.x.LOG_DEFAULT_OUTGOING	yes | no

Registerkarte: NAT

Menü-Option	GAI-Variable	Format
Lokales NAT		
Lokales NAT für OpenVPN-Verbindungen	OPENVPN_CONNECTION.x.LOCAL_NAT	none | 1to1nat | masq
Virtuelles lokales Netzwerk für 1:1-NAT	OPENVPN_CONNECTION.x.LOCAL	<cidr>
Lokale Adresse für 1:1-NAT	OPENVPN_CONNECTION.x.LOCAL_1TO1NAT	<ip>
Netzwerk	OPENVPN_CONNECTION.x.MASQUERADE.y.NET	<cidr>
Kommentar	OPENVPN_CONNECTION.x.MASQUERADE.y.COMMENT	<txt>
IP- und Port-Weiterleitung		
Protokoll	OPENVPN_CONNECTION.x.PORTFORWARDING.y.PROTO	tcp | udp | gre
Von IP	OPENVPN_CONNECTION.x.PORTFORWARDING.y.SRC_IP	<rowref> | <ip> | <cidr>
Von Port	OPENVPN_CONNECTION.x.PORTFORWARDING.y.SRC_PORT	<num> | <num>:<num> | <rowref>
Eintreffend auf Port	OPENVPN_CONNECTION.x.PORTFORWARDING.y.IN_PORT	<num>
Weiterleiten an IP	OPENVPN_CONNECTION.x.PORTFORWARDING.y.OUT_IP	<ip>
Weiterleiten an Port	OPENVPN_CONNECTION.x.PORTFORWARDING.y.OUT_PORT	<num>
Kommentar	OPENVPN_CONNECTION.x.PORTFORWARDING.y.COMMENT	<txt>
Log	OPENVPN_CONNECTION.x.PORTFORWARDING.y.LOG	yes | no

4.7 Redundanz

4.7.1 Firewall-Redundanz

Registerkarte: Redundanz

Menü-Option	GAI-Variable	Format
Allgemein		
Aktiviere Redundanz	REDUNDANCY_ENABLE	yes | no
Umschaltzeit im Fehlerfall	REDUNDANCY_FAILOVER_MS	1000 | 3000 | 10000
Wartezeit vor Umschaltung	REDUNDANCY_LATENCY_MS	<num>
Priorität dieses Gerätes	REDUNDANCY_PRIORITY	low | high
Passphrase für Verfügbarkeitsprüfungen	REDUNDANCY_AVAIL_PASSWORD	<txt>
Externe virtuelle Interfaces		
Externe virtuelle Router-ID	REDUNDANCY_ID_EXT	<num>
IP	REDUNDANCY_VIRT_EXT.x.IP	<ip>
Interne virtuelle Interfaces		
Interne virtuelle Router-ID	REDUNDANCY_ID_INT	<num>
IP	REDUNDANCY_VIRT_INT.x.IP	<ip>
Virtuelles Interface		
Virtuelle Router-ID	REDUNDANCY_ID_BRIDGE	<num>
Aktiviere virtuelle IP	REDUNDANCY_VIRT_BRIDGE_ENABLE	yes | no
IP	REDUNDANCY_VIRT_BRIDGE.x.IP	<ip>
Management-IP-Adressen des zweiten Geräts		
IP	REDUNDANCY_BRIDGE_PEER_MANAGE.x.IP	<ip>
Interface für den Zustandsabgleich		
Interface, das zum Zustandsabgleich verwendet wird	REDUNDANCY_SYNCIF_ENABLE	yes | no
IP	REDUNDANCY_SYNCIF_IP	<ip>
Netzmaske	REDUNDANCY_SYNCIF_NET	<netmask>
VLAN verwenden	REDUNDANCY_SYNCIF_USE_VLAN	yes | no
VLAN-ID	REDUNDANCY_SYNCIF_VLAN_ID	<num>
Unterlasse die Verfügbarkeitsprüfung an der externen Schnittstelle.	REDUNDANCY_AVAIL_EXT_DISABLE	yes | no

Registerkarte: Konnektivitätsprüfungen

Menü-Option	GAI-Variable	Format
Externes Interface		
Art der Prüfung	REDUNDANCY_CHECK_MODE_EXT	none | any | all
Primäre externe Ziele		
IP	REDUNDANCY_CHECK_HOSTS_PRIM_EXT.x.IP	<ip>
Sekundäre externe Ziele		
IP	REDUNDANCY_CHECK_HOSTS_SEC_EXT.x.IP	<ip>
Internes Interface		
Art der Prüfung	REDUNDANCY_CHECK_MODE_INT	none | any | all
Primäre interne Ziele		
IP	REDUNDANCY_CHECK_HOSTS_PRIM_INT.x.IP	<ip>
Sekundäre interne Ziele		
IP	REDUNDANCY_CHECK_HOSTS_SEC_INT.x.IP	<ip>

4.7.2 Ring-/Netzkopplung

Registerkarte: Ring-/Netzkopplung

Menü-Option	GAI-Variable	Format
Einstellungen		
Aktiviere Ring-/Netz-werkkopplung/Dual Ho-ming	L2REDUNDANCY	yes | no
Redundanz-Port	L2REDUNDANCY_PORT	intern | extern

4.8 Logging

4.8.1 Einstellungen

Registerkarte: Einstellungen

Menü-Option	GAI-Variable	Format
Remote Logging		
Aktiviere Remote UDP-Logging	LOGGING_UDP_ENABLE	yes | no
Log-Server IP-Adresse	LOGGING_UDP_SERVER_IP	<ip>
Log-Server Port (normalerweise 514)	LOGGING_UDP_SERVER_PORT	<num>
Ausführliches Logging		
Ausführliches Modem-Logging	MODEM_DEBUG	yes | no
Datenschutz		
Maximale Aufbewahrungsfrist für Log-Einträge (0 = unlimitiert)	LOGGING_MAX_DAYS	<num>

A Technischer Anhang

A 1 E-Mail-Benachrichtigungen

Die folgenden Werte werden für Benachrichtigungsereignisse (E-Mail-Benachrichtigungen) unterstützt:

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

Bitte beachten Sie folgende Hinweise

Allgemeine Nutzungsbedingungen für Technische Dokumentation

Phoenix Contact behält sich das Recht vor, die technische Dokumentation und die in den technischen Dokumentationen beschriebenen Produkte jederzeit ohne Vorankündigung zu ändern, zu korrigieren und/oder zu verbessern, soweit dies dem Anwender zumutbar ist. Dies gilt ebenfalls für Änderungen, die dem technischen Fortschritt dienen.

Der Erhalt von technischer Dokumentation (insbesondere von Benutzerdokumentation) begründet keine weitergehende Informationspflicht von Phoenix Contact über etwaige Änderungen der Produkte und/oder technischer Dokumentation. Sie sind dafür eigenverantwortlich, die Eignung und den Einsatzzweck der Produkte in der konkreten Anwendung, insbesondere im Hinblick auf die Befolgung der geltenden Normen und Gesetze, zu überprüfen. Sämtliche der technischen Dokumentation zu entnehmenden Informationen werden ohne jegliche ausdrückliche, konkludente oder stillschweigende Garantie erteilt.

Im Übrigen gelten ausschließlich die Regelungen der jeweils aktuellen Allgemeinen Geschäftsbedingungen von Phoenix Contact, insbesondere für eine etwaige Gewährleistungshaftung.

Phoenix Contact behält sich das Recht vor, für die hier verwendeten Produktkennzeichnungen von Phoenix Contact-Produkten eigene Schutzrechte anzumelden. Die Anmeldung von Schutzrechten hierauf durch Dritte ist verboten.

Andere Produktkennzeichnungen können gesetzlich geschützt sein, auch wenn sie nicht als solche markiert sind.

So erreichen Sie uns

Internet

Aktuelle Informationen zu Produkten von Phoenix Contact und zu unseren Allgemeinen Geschäftsbedingungen finden Sie im Internet unter:
phoenixcontact.com.

Stellen Sie sicher, dass Sie immer mit der aktuellen Dokumentation arbeiten.
Diese steht unter der folgenden Adresse zum Download bereit:
phoenixcontact.net/products.

Ländervertretungen

Bei Problemen, die Sie mit Hilfe dieser Dokumentation nicht lösen können, wenden Sie sich bitte an Ihre jeweilige Ländervertretung.
Die Adresse erfahren Sie unter phoenixcontact.com.

Herausgeber

Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
DEUTSCHLAND

Wenn Sie Anregungen und Verbesserungsvorschläge zu Inhalt und Gestaltung unseres Handbuchs haben, würden wir uns freuen, wenn Sie uns Ihre Vorschläge zusenden an:
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_de_06
Item No. –06