Zusatzhandbuch

INSYS icom

Industrielle Datenkommunikation

INSYS Router

Referenzhandbuch für die ASCII-Konfigurationsdatei

Copyright © July 2016 INSYS MICROELECTRONICS GmbH

Jede Vervielfältigung dieses Handbuchs ist nicht erlaubt. Alle Rechte an dieser Dokumentation und an den Geräten liegen bei INSYS MICROELECTRONICS GmbH Regensburg.

Warenzeichen und Firmenzeichen
Die Verwendung eines hier nicht aufgeführten Waren- oder Firmenzeichens ist kein Hinweis auf die freie Verwendbarkeit desselben.

MNP ist ein eingetragenes Warenzeichen von Microcom, Inc.

IBM PC, AT, XT sind Warenzeichen von International Business Machine Corporation.

INSYS®, VCom®, e-Mobility LSG® und e-Mobility PLC® sind eingetragene Warenzeichen der INSYS MICROELECTRONICS GmbH.

Windows™ ist ein Warenzeichen von Microsoft Corporation.

Linux ist ein eingetragenes Warenzeichen von Linus Torvalds.

Herausgeber:
INSYS MICROELECTRONICS GmbH
Hermann-Köhl-Str. 22
93049 Regensburg
Telefon: +49 941 58692 0
Telefax: +49 941 58692 45
E-Mail: info@insys-icom.de
Internet: http://www.insys-icom.de

Datum: Jul-16
Artikelnummer: 31-22-03.165
Version: 1.11
Sprache: DE

1 Allgemeines 5

2 ASCII-Konfigurationsdatei 6

2.1 Aufbau der Konfigurationsdatei 6

2.1.1 Kommentare 6
2.1.2 Formatierung 7
2.1.3 Zeichenfolgen 7
2.1.4 Endloslisten 7
2.1.5 Fehlende oder doppelte Sektionen bzw. Objekte 8
2.1.6 Löschen von Objektwerten 8
2.1.7 Sich ausschließende Einstellungen 9
2.1.8 Neustart am Ende der Konfiguration 9
2.1.9 Laden der alten Konfiguration bei Abbruch der Konfiguration 9
2.1.10 Laden der Konfiguration in die Sandbbox 10
2.1.11 Einbinden von Dateien 10

2.2 Hochladen bestehender Konfigurationsdateien 11

3 Log-Datei 12

4 Konfiguration über ASCII-Konfigurationsdatei 13

5 Referenz für die ASCII-Konfigurationsdatei 14

1 Allgemeines

Dieses Zusatzhandbuch dient als Referenz für die Konfigurationsdatei der INSYS-Router im ASCII-Format und ist nur zusammen mit dem Benutzerhandbuch des jeweiligen Routers zu verwenden. Sicherheitshinweise, Technische Daten und Funktionsbeschreibungen sind dem Benutzerhandbuch zu entnehmen.

Dieses Zusatzhandbuch gilt für alle Router von INSYS icom mit einer Firmware-Version ab 2.4.x.

Diese Referenz beschreibt alle Einstellmöglichkeiten der verschiedenen Varianten des Routers. Die einzelnen Varianten enthalten nicht alle beschriebenen Einstellungen. Der tatsächliche Umfang ist abhängig von der Firmware und Variante.

2 ASCII-Konfigurationsdatei

Der Router ermöglicht eine Ausgabe der Konfigurationsdatei als ASCII-Textdatei. Diese Textdatei kann entsprechend angepasst und wieder auf den Router geladen werden, um diesen auf einfache Art und Weise zu konfigurieren (siehe Hochladen bestehender Konfigurationsdateien auf Seite 11). Weiterhin kann auch eine „leere“ Konfigurationsdatei (ASCII-Vorlage) vom Router heruntergeladen werden, d.h. eine Konfigurationsdatei, die keinerlei Einstellungen enthält, aber alle auf dem jeweiligen Gerät verfügbaren Einstellmöglichkeiten enthält.

Eine genaue Beschreibung der Funktionen zum Herunterladen und Hochladen von Konfigurationsdateien finden Sie im Benutzerhandbuch des Routers.

2.1 Aufbau der Konfigurationsdatei

Die ASCII-Konfigurationsdatei ist in mehrere Sektionen gegliedert. Die Sortierung der Sektionen und Objekte ist der Weboberfläche nachempfunden. Jede Sektion beginnt mit dem Namen der Sektion in eckigen Klammern „`[ Sektion ]`“ gefolgt von weiteren Zeilen mit den einzelnen Objekten dieser Sektion. In den Objekten werden Objektname und Objektwert durch ein Gleichheitszeichen getrennt „`Objektname = Objektwert`“. Jede Zeile wird durch eine Zeilenschaltung abgeschlossen. Das Ende einer Sektion wird durch den Beginn einer neuen Sektion oder das Dateiende bestimmt.

Die Konfigurationsdatei ist „case sensitive“, d.h. Groß- und Kleinschreibung wird berücksichtigt.

Folgender Ausschnitt einer ASCII-Konfigurationsdatei zeigt die Sektion „`textconfig`“ mit den beiden Objekten „`reboot`“ und „`abort_on_error`“ sowie die Sektion „`webinterface`“ mit weiteren Objekten:

```
[ textconfig ]
    reboot = 0
    abort_on_error = 0

[ webinterface ]
    local_http = 1
    remote_http = 1
    remote_https = 1
    http_port = 80
    https_port = 8888
    location = 'Standort'    #This value has to be enclosed in single quotes
```

2.1.1 Kommentare

Kommentare können durch eine Raute „ `#` “ sowohl am Anfang einer Zeile als auch innerhalb einer Zeile eingeleitet werden. Ein Semikolon „ `;` “ kann nur am Anfang einer Zeile (auch nach führenden Leerezeichen oder Tabulatoren) einen Kommentar einleiten. Alle weiteren Zeichen in der Zeile werden ignoriert.

2.1.2 Formatierung

Leerzeilen können beliebig zwischen den Zeilen eingefügt werden.
Leerzeichen und Tabulatoren können eingefügt werden

- am Zeilenanfang
- am Zeilenende
- zwischen eckigen Klammern und Sektionsnamen
- zwischen Objektname und „ = “
- zwischen „ = “ und Objektwert
- zwischen Objektname und „ ; “ bei Endloslisteneinträgen
- zwischen „ ; “ und Objektwerten bei Endloslisteneinträgen

2.1.3 Zeichenfolgen

Zeichenfolgen (Strings), wie sie beispielsweise zur Eingabe von Passwörtern oder Benutzernamen verwendet werden, sind in Hochkommas „ ’ “ zu setzen (in jedem solchen Eintrag weist ein Kommentar auf die Verwendung von Hochkommas hin). Da nur nach dem ersten und letzten Hochkomma gesucht wird, können die Zeichenfolgen auch Hochkommas enthalten. Grundsätzlich sind die Zeichen 0x20 bis 0x7E erlaubt, also 0 bis 9, a bis z, A bis Z, die Sonderzeichen ! " # $ % & ' ( ) * + , - . / ; < = > ? @ [ ] \ ^ _ { } | ~, sowie das Leerzeichen. Der Doppelpunkt ist nicht erlaubt. Folgendes Beispiel zeigt die Eingabe von Zeichenfolgen:

```
    dialnumber = '*99***1#'   #This value has to be enclosed in single quotes
```

2.1.4 Endloslisten

Manche Objekte können Endloslisten bilden (z.B. Routen). Werden mit einem Objekt weitere Objekte übergeben (z.B. bei einer Firewall die Absenderadresse, Netzmaske, Datenrichtung, etc.), werden diese in die gleiche Zeile geschrieben, aber mit einem Semikolon „ ; “ voneinander getrennt. Das Objekt „`list`“ gibt an, ob die in dieser Sektion enthaltene Endlosliste, die sich bereits auf dem Router befindet, gelöscht werden soll „`list = d`“ (d für delete) bevor die neuen Objekte eingetragen werden oder die neuen Objekte an die Liste angehängt werden sollen „`list = a`“ (a für append). Fehlt das Objekt „`list`“, werden die Objekte an die Liste angehängt. Grundsätzlich gibt es nicht mehr als eine Endlosliste pro Sektion. Folgendes Beispiel zeigt eine solche Endlosliste:

```
....list = d
    new_entry = common_name = cname1 ; vpn_ip = 10.1.0.9
    new_entry = common_name = cname2 ; vpn_ip = 10.1.0.13
```

2.1.5 Fehlende oder doppelte Sektionen bzw. Objekte

Fehlen in einer ASCII-Konfigurationsdatei Sektionen bzw. Objekte, werden die fehlenden Sektionen bzw. Objekte nicht auf den Router hochgeladen, d.h. die Konfiguration dieser Objekte wird nicht verändert. Eine einzige Sektion stellt bereits eine gültige Konfigurationsdatei dar. Dabei muss sie nicht einmal ein Objekt enthalten, was man zum Beispiel dazu nützen kann, einen Dial-Out neu zu starten. Das Abarbeiten einer Sektion in einer Konfigurationsdatei entspricht dem Drücken der Schaltfläche „OK“ auf der entsprechenden Seite der Weboberfläche.

Enthält eine ASCII-Konfigurationsdatei ein Objekt mehr als einmal, überschreibt das spätere Objekt das jeweils vorhergehende, da die Konfigurationsdatei sequentiell abgearbeitet wird. Im folgenden Beispiel überschreibt das zweite Objekt das erste, d.h. das Objekt „`dns`“ wird auf „2.2.2.2“ gesetzt:

```
[ dns ]
    dns = 1.1.1.1
    dns = 2.2.2.2
```

Sektionen können ebenfalls mehrmals vorkommen und werden auch mehrmals konfiguriert. Dies kann beispielsweise dazu verwendet werden, um innerhalb einer Konfiguration eine Wählverbindung zu beenden, das Kommunikationsgerät zu konfigurieren, und die Wählverbindung anschließend wieder aufzubauen, wie im folgenden Beispiel gezeigt:

```
[ dialout ]
    start_dialout = 0
[ isdn ]
    msn = 25
[ dialout ]
    start_dialout = 1
```

2.1.6 Löschen von Objektwerten

Dieser Parameter ist erst ab der Firmware-Version 2.10.x verfügbar!

Wenn ein Parameter konfiguriert ist, d.h. einem Objekt wurde ein bestimmter Wert zugewiesen, wird dieser Wert nur bei einer erneuten Konfiguration aktualisiert. Fehlt das Objekt in einer Konfigurationsdatei oder wird ihm kein Objektwert zugewiesen, bleibt der ursprüngliche Objektwert unverändert. Soll der Objektwert explizit gelöscht werden, muss dem Objekt der Objektwert „`C_L_E_A_R`“ zugewiesen werden:

```
[ dns ]
    dns = C_L_E_A_R
```

2.1.7 Sich ausschließende Einstellungen

Wenn in einer ASCII-Konfigurationsdatei Einstellungen durchgeführt werden, die sich gegenseitig ausschließen, beispielsweise das gleichzeitige Aktivieren eines OpenVPN-Clients und -Servers, gilt die zuerst konfigurierte Sektion (d.h. diejenige, die in der Konfigurationsdatei weiter vorne steht). Die zugehörigen Einstellungen werden jedoch übernommen. Ein vergleichbares Verhalten findet sich auch auf der Weboberfläche: hier kann nach dem Konfigurieren einer bestimmten Funktion eine widersprüchliche Konfiguration ebenfalls nicht durchgeführt werden, da diese ausgeblendet wird.

2.1.8 Neustart am Ende der Konfiguration

In der Sektion „`textconfig`“ der ASCII-Konfigurationsdatei befindet sich das Objekt „`reboot`“ mit dem festgelegt werden kann, ob ein Neustart des Routers am Ende der Konfiguration erfolgen soll (0 = kein Neustart; 1 = Neustart). Durch einen Neustart lässt sich sicherstellen, dass alle Dienste mit den neuen Einstellungen gestartet werden (VPN-Einstellungen werden beispielsweise erst bei einem erneuten Dial-Out verwendet). In folgendem Beispiel erfolgt ein Neustart am Ende der Konfiguration:

```
[ textconfig ]
    reboot = 1
    abort_on_error = 0
```

2.1.9 Laden der alten Konfiguration bei Abbruch der Konfiguration

In der Sektion „`textconfig`“ der ASCII-Konfigurationsdatei befindet sich das Objekt „`abort_on_error`“ mit dem festgelegt werden kann, ob bei Abbruch der Konfiguration durch einen Fehler die alte Konfiguration wieder auf den Router geladen werden soll (0 = kein Laden der alten Konfiguration; 1 = Laden der alten Konfiguration). Ein Abbruch der Konfiguration erfolgt bei fehlerhaften Konfigurationen, die auf der Weboberfläche eine rote Warnmeldung hervorrufen würden. Diese Funktion kann beispielsweise zum Absichern „kritischer“ Konfigurationen (z.B. die Wählverbindung, über die gerade die Fernkonfiguration erfolgt) verwendet werden, indem die Funktion vor der „kritischen“ Sektion aktiviert und dahinter wieder deaktiviert wird, d.h. die alte Konfiguration wird nur dann wieder geladen, wenn der Abbruch in der „kritischen“ Sektion erfolgt. In folgendem Beispiel wird die alte Konfiguration nach einem Abbruch wieder geladen:

```
[ textconfig ]
    reboot = 0
    abort_on_error = 1
```

2.1.10 Laden der Konfiguration in die Sandbbox

In der Sektion „`textconfig`“ der ASCII-Konfigurationsdatei befindet sich das Objekt „`ascii_config_to_sandbox`“ mit dem festgelegt werden kann, ob die aktuelle Konfiguration in die Sandbox geladen werden soll (0 = kein Laden der Konfiguration; 1 = Laden der Konfiguration). Wenn eine ASCII-Konfiguration ohne Authentifizierung aus der Sandbox zugelassen ist, wird die Konfigurationsdatei von der Firmware abgeholt und ausgewertet. Ist dieses Objekt auf 1 gesetzt, wird nach dem Ausführen der Konfigurationsdatei eine neue Konfigurationsdatei erstellt und unter dem Namen "ascii_config_download.txt" im Verzeichnis /var/spool/ der Sandbox gespeichert. In folgendem Beispiel wird die Konfiguration in die Sandbox geladen:

```
[ textconfig ]
    ascii_config_to_sandbox = 1
```

2.1.11 Einbinden von Dateien

Es besteht auch die Möglichkeit, den Inhalt anderer Dateien innerhalb der ASCII-Konfigurationsdatei auf den Router zu laden. Dies ist beispielsweise erforderlich, um Zertifikate, Schlüssel, Listen oder Texte für E-Mails und SMS hochzuladen. Diese Dateien werden in Textform als Objektwert mit dem jeweiligen Objekt übergeben. Dabei können auch Zeilenschaltungen innerhalb des Objekts vorhanden sein. Es dürfen jedoch keine Kommentare, wie in Abschnitt 2.1.1 beschrieben, innerhalb dieser Objektwerte enthalten sein.

Um beispielsweise Zertifikate oder Schlüssel zu speichern, werden diese nach dem Objektnamen als Objektwert übergeben. Dazu wird das Zertifikat oder der Schlüssel in einem Texteditor geöffnet, dort kopiert und vollständig hinter dem „ = “ im Objekt eingefügt. Das folgende (abgekürzte) Beispiel zeigt das CA-Zertifikat in der ASCII-Konfigurationsdatei:

```
[ openvpn server dialin ]
...
    ca_certificate = -----BEGIN CERTIFICATE-----
MIIC+jCCAmOgAwIBAgIBATANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMCREUx
...
cNAMClSZ3yDocBkiJuL7sMqAk8uN8XI4uKSBhZ0bZUG1O5dubek/Gkl2Bkymjw==
-----END CERTIFICATE-----
```

Die Übergabe von Listen, wie der AT-Antwortliste, erfolgt in ähnlicher Weise und ist in folgendem Beispiel gezeigt:

```
[ serial ethernet modem ]
...
    at_answer_list = -----BEGIN AT ANSWER LIST-----
i="Serial Ethernet Gateway Version 1.0"
-----END AT ANSWER LIST-----
```

Die Konfiguration von E-Mail-Meldungen erfolgt in Form von Endloslisten (siehe Endloslisten). Dabei wird hinter dem Objektnamen „`new_entry`“ der Objektwert in Form weiterer Objekte übergeben, die mit einem Semikolon „ ; “ voneinander getrennt sind. Im Unterobjekt „`text`“ wird dann der Meldungstext übergeben. Bei E-Mails darf dieser auch Zeilenschaltungen enthalten und wird durch die Textfolgen „`-----BEGIN MESSAGE-----`“ und „`-----END MESSAGE-----`“ eingegrenzt. Bei SMS-Meldungen darf dieser keine Zeilenschaltungen enthalten und wird ohne weitere Formatierungen übergeben. Im Folgenden ist dies am Beispiel von E-Mail-Meldungen dargestellt:

```
[ email ]
    start_email = 1
    list = d
    new_entry = recipient = support@insys-tec.de ; cause = 0001 ; attach =
0001 ; status = 1 ; text = -----BEGIN MESSAGE-----
E-Mail-Text
Wird beim Systemstart gesendet-----END MESSAGE-----
    new_entry = recipient = support@insys-tec.de ; cause = 0002 ; attach =
0004 ; text = -----BEGIN MESSAGE-----
E-Mail-Text
Wird beim Aufbau eines OpenVPN-Tunnels gesendet -----END MESSAGE-----
```

2.2 Hochladen bestehender Konfigurationsdateien

Der Router ermöglicht das Hochladen einer ASCII-Konfigurationsdatei. Dabei sind folgende Punkte zu beachten:

- Beim Herunterladen einer ASCII-Konfigurationsdatei werden aus Sicherheitsgründen keine Zertifikatesschlüssel heruntergeladen. Diese fehlen dann beim Wiederhochladen der ASCII-Konfigurationsdatei. Eine manuelle Einbindung ist im Abschnitt Einbinden von Dateien auf Seite 10 beschrieben.
- Beim Herunterladen einer ASCII-Konfigurationsdatei wird die aktuelle Uhrzeit mit heruntergeladen. Diese überschreibt dann beim Wiederhochladen der ASCII-Konfigurationsdatei die aktuelle Uhrzeit mit der Uhrzeit zum Zeitpunkt des Herunterladens.
- Beim Herunterladen einer ASCII-Konfigurationsdatei werden bei bestehenden Listen für Regeln (z.B. für Firewall, Wählfilter oder Portforwarding) mögliche Deaktivierungen einzelner Regeln nicht mit heruntergeladen. Daher sind beim Wiederhochladen der ASCII-Konfigurationsdatei vorher deaktivierte Regeln wieder aktiv.

3 Log-Datei

Während die Konfigurationsdatei abgearbeitet wird, wird eine Log-Datei geschrieben. Neben Beginn und Ende der Konfiguration werden auch folgende Fehler in der Log-Datei festgehalten:

- Unbekannte Sektion
- Sektion auf diesem Router nicht verfügbar (z.B. [dialout] auf MoRoS LAN)
- Fehlender Wert zu einem Objekt
- Unbekanntes Objekt

Die Log-Datei kann auf der Weboberfläche des Routers im Menü „System“ auf der Seite „Systemdaten“ über den Link „Anzeigen des Text-Konfigurations-Logs“ sowie im Menü „System“ auf der Seite „Download“ über den Link „Text-Config-Log“ angezeigt werden.

Eine genaue Beschreibung der Funktionen zum Anzeigen der Log-Datei finden Sie im Benutzerhandbuch des Routers.

4 Konfiguration über ASCII-Konfigurationsdatei

Dieses Kapitel erklärt, wie eine ASCII-Konfigurationsdatei vom Router herunterladen, entsprechend bearbeitet und wieder auf den Router hochgeladen wird.

Um die folgenden Schritte durchzuführen, müssen Sie Ihren Router in Betrieb genommen haben und Zugriff auf die Weboberfläche haben. Dafür setzen wir voraus, dass Sie im Umgang mit dem Router geübt sind und das zugehörige Benutzerhandbuch, insbesondere die Kapitel „Inbetriebnahme“ und „Bedienprinzip“, durchgearbeitet haben.

Konfiguration mit Weboberfläche

Um die **aktuelle Konfiguration des Routers herunterzuladen**, wählen Sie im Menü „System“ auf der Seite „Download“ im Abschnitt „Konfiguration“ mit der rechten Maustaste den Link „ASCII“. Wählen Sie „Ziel speichern unter…“ und speichern Sie die Konfigurationsdatei an einem geeigneten Ort unter einem geeigneten Namen ab.

Um eine **leere Konfigurationsdatei des Routers herunterzuladen**, wählen Sie im Menü „System“ auf der Seite „Download“ im Abschnitt „Konfiguration“ mit der rechten Maustaste den Link „ASCII-Vorlage“. Wählen Sie „Ziel speichern unter…“ und speichern Sie die Konfigurationsdatei an einem geeigneten Ort unter einem geeigneten Namen ab.

Öffnen Sie die Konfigurationsdatei mit einem Texteditor und nehmen Sie die entsprechenden Änderungen daran vor. Speichern Sie die bearbeitete Konfigurationsdatei wieder ab.

ⓘ Löschen Sie nicht benötigte Sektionen und Objekte, um das folgende Hochladen zu beschleunigen.

Um die **bearbeitete Konfiguration auf den Router wieder hochzuladen**, wählen Sie im Menü „System“ auf der Seite „Update“ im Abschnitt „Manuelles Update“ die Schaltfläche „Durchsuchen…“ und öffnen Sie die Konfigurationsdatei, die hochgeladen werden soll.

Übernehmen Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

Bestätigen Sie das Hochladen, indem Sie auf „Ja“ klicken.

Hinweis!

Veränderung der Uhrzeit!

Durch Hochladen einer zuvor heruntergeladenen Konfiguration kann die Uhrzeit verstellt werden.

Wenn Sie eine Konfiguration vom Router laden, wird auch die aktuelle Uhrzeit in der Konfigurationsdatei abgespeichert. Wenn diese Konfigurationsdatei später ohne Löschung bzw. Bearbeitung der Sektion [settime] wieder hochgeladen wird, wird die Uhrzeit im Router mit der (inzwischen falschen) Uhrzeit in der Konfigurationsdatei überschrieben.

5 Referenz für die ASCII-Konfigurationsdatei

In diesem Kapitel finden Sie eine Referenz aller Sektionen mit den zugehörigen Objekten, die in der ASCII-Konfigurationsdatei erscheinen können. Beachten Sie, dass die verfügbaren Sektionen, Objekte und Optionen von der Firmware und Variante des Routers abhängen. Wenn Sie eine aktuelle ASCII-Konfigurationsdatei von einem Router laden, enthält diese nur die aktuell konfigurierten Objekte in ihren jeweiligen Sektionen, d.h. Objekte, die zwar im Router vorhanden, aber nicht konfiguriert sind, sind nicht enthalten. Wenn Sie eine leere ASCII-Konfigurationsdatei als Vorlage von einem Router laden, enthält diese alle verfügbaren Objekte dieses Routers.

Sektionen und Objekte können aus einer ASCII-Konfigurationsdatei gelöscht oder ihr hinzugefügt werden. Auch ist es möglich, eine ASCII-Konfigurationsdatei aus einer leeren TXT-Datei zu erstellen. Dabei müssen die Anforderungen an die ASCII-Konfigurationsdatei, die im Kapitel „ASCII-Konfigurationsdatei“ dieses Handbuchs beschrieben sind, berücksichtigt werden.

[textconfig]

`reboot`	0 = Kein Neustart nach Konfiguration (default)
	1 = Neustart nach Konfiguration
`abort_on_error`	0 = Kein Laden der alten Konfiguration nach Abbruch (default)
	1 = Laden der alten Konfiguration nach Abbruch
`ascii_config_to_sandbox`	0 = Kein Ablegen der Konfiguration in die Sandbox (default)
	1 = Ablegen der Konfiguration in die Sandbox
	(ab FW 2.11.0)

[webinterface]

`username`	Benutzername für Zugriff auf Weboberfläche (default: insys)
	Objektwert muss in Hochkommas übergeben werden!
`password`	Kennwort für Zugriff (default: siehe Handbuch)
	Objektwert muss in Hochkommas übergeben werden!
`local_http`	0 = Lokale Konfiguration per HTTP deaktiviert
	1 = Lokale Konfiguration per HTTP aktiviert (default)
`remote_http`	0 = Fernkonfiguration per HTTP deaktiviert
	1 = Fernkonfiguration per HTTP aktiviert (default)
`local_https`	0 = Lokale Konfiguration per HTTPS deaktiviert
	1 = Lokale Konfiguration per HTTPS aktiviert (default)
	(ab FW 2.11.0)

`remote_https`	0 = Fernkonfiguration per HTTPS deaktiviert 1 = Fernkonfiguration per HTTPS aktiviert (default)
`http_port`	HTTP-Port der Weboberfläche (default: 80)
`https_port`	HTTPS-Port der Weboberfläche (default: 443)
`location`	Standort des Routers Objektwert muss in Hochkommas übergeben werden!
`auth_type`	password = Authentifizierung über Benutzername und Kennwort (default) radius = Authentifizierung über RADIUS-Server *(ab FW 2.12.0)*
`auth_fallback`	0 = Keine Authentifizierung mit Kennwort nach Radius-Timeout (default) 1 = Authentifizierung mit Kennwort nach Radius-Timeout *(ab FW 2.12.0)*

[address]

`ip`	IP-Adresse des Routers (default: 192.168.1.1)
`netmask`	Netzmaske des Routers (default: 255.255.255.0)
`start_netmapping`	0 = Netmapping deaktiviert (default) 1 = Netmapping aktiviert *(ab FW 2.6.0)*
`virtual_net`	Virtuelle Netzwerkadresse des lokalen Netzwerks *(ab FW 2.6.0)*
`slaac_active`	0 = SLAAC deaktiviert 1 = SLAAC aktiviert (default) *(ab FW 2.10.0)*
`ipv6`	IPv6-Adresse des Routers (default: random) *(ab FW 2.10.0)*
`prefix_length`	Länge des IPv6-Adress-Prefix (7-64, default: 64) *(ab FW 2.10.0)*

[wlan_ap]	*bei WLAN-Routern ab FW 2.12.7*
start_ap	0 = WLAN Access Point deaktiviert (default)
	1 = WLAN Access Point aktiviert
channel	WLAN-Frequenzkanal (1-11, default: 1)
hide_ssid	0 = SSID-Broadcast aktiviert (default)
	1 = SSID-Broadcast deaktiviert
ssid	SSID des Access Points (max. 32 ASCII-Zeichen)
security	none = Keine Verschlüsselung
	psk = Verschlüsselung mit PSK (default)
encryption	wpa1 = Verschlüsselungsprotokoll WPA 1
	wpa2 = Verschlüsselungsprotokoll WPA 2 (default)
	wpa12 = Verschlüsselungsprotokoll WPA 1/2
psk_key	WLAN-Schlüssel (8-63 ASCII-Zeichen/64 Hex-Zeichen)
	Objektwert muss in Hochkommas übergeben werden!
[routing local]	
list	a = Neue Einträge werden an bestehende Liste angehängt
	d = Bestehende Liste wird gelöscht (default)
new_entry	Neuer Routeneintrag, der folgende Unterobjekte übergibt:
net	Netzwerkadresse der statischen Route für IPv4
netmask	Netzmaske der statischen Route für IPv4
gateway	Gateway der statischen Route für IPv4
ipv6	Netzwerkadresse der statischen Route für IPv6
	(ab FW 2.10.0)
prefix_length	Netzmaske der statischen Route für IPv6
	(ab FW 2.10.0)
gateway6	Gateway der statischen Route für IPv6
	(ab FW 2.10.0)
[hostnames]	*ab FW 2.10.0*
hostname	Hostname des Routers (default: <Router-Name>)
domainname	Domainname des Routers (default: local)
list	a = Neue Einträge werden an bestehende Liste angehängt
	d = Bestehende Liste wird gelöscht (default)
new_entry	Neuer Routeneintrag, der folgende Unterobjekte übergibt:
ip	IP-Adresse des Host-Eintrags
host	Host-Name des Host-Eintrags
[macfilter]	*ab FW 2.11.0*

`start macfilter`	0 = MAC-Filter deaktiviert (default)
	1 = MAC-Filter aktiviert
`list`	a = Neue Einträge werden an bestehende Liste angehängt
	d = Bestehende Liste wird gelöscht (default)
`new_entry`	Neuer Filtereintrag, der folgende Unterobjekte übergibt:
`mac`	Erlaubte MAC-Adresse
[radius]	*ab FW 2.12.0*
`server`	Adresse des RADIUS-Servers
`port`	Port des RADIUS-Servers
`secret`	„Shared Secret“ des RADIUS-Servers
[command line]	*ab FW 2.12.0*
`username`	Benutzername für Zugriff auf CLI
	Objektwert muss in Hochkommas übergeben werden!
`password`	Kennwort für Zugriff
	Objektwert muss in Hochkommas übergeben werden!
`local_telnet`	0 = Lokale CLI-Konfiguration per Telnet deaktiviert
	1 = Lokale CLI-Konfiguration per Telnet aktiviert (default)
`local_ssh`	0 = Lokale CLI-Konfiguration per SSH deaktiviert
	1 = Lokale CLI-Konfiguration per SSH aktiviert (default)
`remote_telnet`	0 = CLI-Fernkonfiguration per Telnet deaktiviert
	1 = CLI-Fernkonfiguration per Telnet aktiviert (default)
`remote_ssh`	0 = CLI-Fernkonfiguration per SSH deaktiviert
	1 = CLI-Fernkonfiguration per SSH aktiviert (default)
`telnet_port`	Telnet-Port für CLI (default: 23)
`ssh_port`	SSH-Port für CLI (default: 22)
`auth_type`	password = Authentifizierung über Benutzername und Kennwort (default)
	radius = Authentifizierung über RADIUS-Server
`auth_fallback`	0 = Keine Authentifizierung mit Kennwort nach Radius-Timeout (default)
	1 = Authentifizierung mit Kennwort nach Radius-Timeout
`md5_checksum`	MD5-Prüfsumme für SSH-Verbindung (nur Anzeige)
`prompt`	String für Eingabeaufforderung im CLI (default: >)
	Objektwert muss in Hochkommas übergeben werden!
	(ab FW 2.12.4)

[com1]	*bei Mobilfunk-Routern*
pin	PIN der SIM-Karte 1
pin2	PIN der SIM-Karte 2
provider_mode	auto = Automatisches Einbuchen beim Standardprovider der SIM-Karte 1
	preferred = Einbuchen beim bevorzugten Provider für SIM-Karte 1, ansonsten beim Standardprovider
	exclusive = Ausschließliches Einbuchen beim exklusiven Provider für SIM-Karte 1
pref_provider	Provider-ID des bevorzugten Providers für SIM-Karte 1
excl_provider	Provider-ID des exklusiven Providers für SIM-Karte 1
provider_mode2	auto = Automatisches Einbuchen beim Standardprovider der SIM-Karte 2
	preferred = Einbuchen beim bevorzugten Provider für SIM-Karte 2, ansonsten beim Standardprovider
	exclusive = Ausschließliches Einbuchen beim exklusiven Provider für SIM-Karte 2
pref_provider2	Provider-ID des bevorzugten Providers für SIM-Karte 2
excl_provider2	Provider-ID des exklusiven Providers für SIM-Karte 2
auto_login	0 = Tägliches Aus- und Einbuchen deaktiviert
	1 = Tägliches Aus- und Einbuchen aktiviert (default)
hour_out	Tägliches Ausbuchen um (Stunde; 00-23)
min_out	Tägliches Ausbuchen um (Minute; 00-59)
hour_in	Tägliches Einbuchen um (Stunde; 00-23)
min_in	Tägliches Einbuchen um (Minute; 00-59)

[com1]	*bei ISDN-Routern*
msn	MSN des Anschlusses an den der Router angeschlossen ist
caller1	Zugelassene Anrufernummer 1
caller2	Zugelassene Anrufernummer 2
caller3	Zugelassene Anrufernummer 3
caller4	Zugelassene Anrufernummer 4
caller5	Zugelassene Anrufernummer 5

[com1]	*bei Modem-Routern*
country	Länderspezifische Einstellung des Modems (default: FD)
wait_for_dialtone	0 = Vor dem Wählen nicht auf Wählton warten (default)
	1 = Vor dem Wählen auf Wählton warten

[com2]	*bei redundantem Mobilfunk-Kommunikationsgerät*
pin	PIN der SIM-Karte des redundanten Kommunikationsgeräts
provider_mode	auto = Automatisches Einbuchen beim Standardprovider der SIM-Karte 1 preferred = Einbuchen beim bevorzugten Provider für SIM-Karte 1, ansonsten beim Standardprovider exclusive = Ausschließliches Einbuchen beim exklusiven Provider für SIM-Karte 1
pref_provider	Provider-ID des bevorzugten Providers für SIM-Karte 1
excl_provider	Provider-ID des exklusiven Providers für SIM-Karte 1
auto_login	0 = Tägliches Aus- und Einbuchen deaktiviert 1 = Tägliches Aus- und Einbuchen aktiviert (default)
hour_out	Tägliches Ausbuchen um (Stunde; 00-23)
min_out	Tägliches Ausbuchen um (Minute; 00-59)
hour_in	Tägliches Einbuchen um (Stunde; 00-23)
min_in	Tägliches Einbuchen um (Minute; 00-59)
[com2]	*bei redundantem ISDN-Kommunikationsgerät*
msn	MSN des Anschlusses an den das redundante Kommunikationsgerät angeschlossen ist
caller1	Zugelassene Anrufernummer 1
caller2	Zugelassene Anrufernummer 2
caller3	Zugelassene Anrufernummer 3
caller4	Zugelassene Anrufernummer 4
caller5	Zugelassene Anrufernummer 5
[com2]	*bei redundantem Modem-Kommunikationsgerät*
country	Länderspezifische Einstellung des Modems (default: FD)
wait_for_dialtone	0 = Vor dem Wählen nicht auf Wählton warten (default) 1 = Vor dem Wählen auf Wählton warten
[terminal1]	*nicht bei LAN-Routern*
command	AT-Befehl, der an das Kommunikationsgerät übergeben wird
[terminal2]	*bei redundantem Kommunikationsgerät*
command	AT-Befehl, der an das redundante Kommunikationsgerät übergeben wird

[wwan]	*bei LTE-Routern*
pin	PIN der SIM-Karte
auth	pap = Authentifizierung über PAP (default)
	chap = Authentifizierung über CHAP
allow_2G	0 = 2G-Verbindungen sind nicht erlaubt
	1 = 2G-Verbindungen sind erlaubt (default)
allow_3G	0 = 3G-Verbindungen sind nicht erlaubt
	1 = 3G-Verbindungen sind erlaubt (default)
allow_4G	0 = 4G-Verbindungen sind nicht erlaubt
	1 = 4G-Verbindungen sind erlaubt (default)
username	Benutzername
	Objektwert muss in Hochkommas übergeben werden!
password	Passwort
	Objektwert muss in Hochkommas übergeben werden!
apn	Access Point Name
check_type	dns = Verbindungsprüfung über DNS-Abfrage (default)
	ping = Verbindungsprüfung über Ping
check_interval	Zeitintervall der Verbindungsüberprüfung (in Min., default: 10)
dns_target	Ziel der Verbindungsprüfung über DNS-Abfrage (default: ptbtime1.ptb.de)
ping_target	Ziel der Verbindungsprüfung über Ping
provider_mode	auto = Automatisches Einbuchen beim Standardprovider
	preferred = Einbuchen beim bevorzugten Provider, ansonsten beim Standardprovider
	exclusive = Ausschließliches Einbuchen beim exklusiven Provider
pref_provider	Provider-ID des bevorzugten Providers
excl_provider	Provider-ID des exklusiven Providers
daily_auto_log	0 = Tägliches Aus- und Einbuchen deaktiviert
	1 = Tägliches Aus- und Einbuchen aktiviert (default)
hour_out	Tägliches Ausbuchen um (Stunde; 00-23, default: 00)
min_out	Tägliches Ausbuchen um (Minute; 00-59, default: 01)
hour_in	Tägliches Einbuchen um (Stunde; 00-23, default: 00)
min_in	Tägliches Einbuchen um (Minute; 00-59, default: 02)
[routing wwan]	*bei LTE-Routern*
default_route	0 = Keine Default-Route setzen
	1 = Default-Route setzen (default)

`nat_incoming`	0 = NAT für eingehende Pakete deaktiviert
	1 = NAT für eingehende Pakete aktiviert (default)
`nat_outgoing`	0 = NAT für ausgehende Pakete deaktiviert
	1 = NAT für ausgehende Pakete aktiviert (default)
`list`	a = Neue Einträge werden an bestehende Liste angehängt
	d = Bestehende Liste wird gelöscht (default)
`default6_route`	0 = Keine IPv6-Default-Route setzen
	1 = IPv6-Default-Route setzen (default)
`new_entry`	Neuer Routeneintrag, der folgende Unterobjekte übergibt:
`net`	Netzwerkadresse der Route für IPv4
`netmask`	Netzmaske der Route für IPv4
`ipv6`	Netzwerkadresse der Route für IPv6
`prefix_length`	Netzmaske der Route für IPv6

[firewall wwan]	*bei LTE-Routern*
start_firewall	0 = Firewall für WWAN-Verbindungen deaktiviert (default)
	1 = Firewall für WWAN-Verbindungen aktiviert
start_firewall6	0 = Firewall für IPv6-WWAN-Verbindungen deaktiviert
	1 = Firewall für IPv6-WWAN-Verbindungen aktiviert (default)
list	a = Neue Einträge werden an bestehende Liste angehängt
	d = Bestehende Liste wird gelöscht (default)
new_entry	Neue zugelassene Verbindung, die folgende Unterobjekte übergibt:
protocol	tcp = TCP-Protokoll wird verwendet
	udp = UDP-Protokoll wird verwendet
	icmp = ICMP-Protokoll wird verwendet
	icmpv6 = ICMPv6-Protokoll wird verwendet
	esp = ESP-Protokoll wird verwendet
	ah = AH-Protokoll wird verwendet
	gre = GRE-Protokoll wird verwendet
	all = Alle Protokolle sind zugelassen
direction	in = Nur eingehende Verbindungen sind zugelassen
	out = Nur ausgehende Verbindungen sind zugelassen
	both = Ein- und ausgehende Verbindungen sind zugelassen
source_ip	IP-Adresse des Absenders
source_netmask	Netzmaske des Absenders
dest_port	Port des Empfängers (oder Anfang des Portbereichs)
dest_port_end	Ende des Portbereichs des Empfängers
dest_ip	IP-Adresse des Empfängers
dest_netmask	Netzmaske des Empfängers
ip_version	ipv4 = Regel kann nur für IPv4-Verbindungen angelegt werden
	ipv6 = Regel kann nur für IPv6-Verbindungen angelegt werden
	all = Regel kann für IPv4-und IPv6-Verbindungen angelegt werden

[portforward wwan]	*bei LTE-Routern*
start_portforwarding	0 = Port-Forwarding für WWAN -Verbindungen deaktiviert
	1 = Port-Forwarding für WWAN -Verbindungen aktiviert (default)
exposed_host	IP-Adresse des „Exposed Host“
list	a = Neue Einträge werden an bestehende Liste angehängt
	d = Bestehende Liste wird gelöscht (default)
new_entry	Neue zugelassene Verbindung, die folgende Unterobjekte übergibt:
protocol	tcp = TCP-Protokoll wird verwendet
	udp = UDP-Protokoll wird verwendet
	icmp = ICMP-Protokoll wird verwendet
	esp = ESP-Protokoll wird verwendet
	ah = AH-Protokoll wird verwendet
	gre = GRE-Protokoll wird verwendet
source_port_start	Beginn des Port-Bereichs für die Weiterleitung
source_port_end	Ende des Port-Bereichs für die Weiterleitung
dest_ip	IP-Adresse des Weiteleitungsziels
dest_port	Port des Weiteleitungsziels
apply	always = Regel gilt immer
	wan = Regel gilt für WWAN-Verbindungen
	openvpn = Regel gilt für OpenVPN-Verbindungen
	(ab FW 2.12.6)

[openvpn server wwan]	*bei LTE-Routern*	
`start_openvpn_server`	0 =	OpenVPN-Server für WWAN-Verbindungen deaktiviert (default)
	1 =	OpenVPN-Server für WWAN-Verbindungen aktiviert
`lport`	Lokaler Port des Tunnels (default: 1194)	
`rport`	Gegenstellen-Port des Tunnels (default: 1194)	
`protocol`	udp =	UDP-Protokoll wird verwendet
	tcp =	TCP-Protokoll wird verwendet
`push_server_route`	0 =	Server-Netz den Clients mitteilen deaktiviert
	1 =	Server-Netz den Clients mitteilen aktiviert (default)
`float`	0 =	Float (Gegenstelle darf IP-Adresse ändern) deaktiviert
	1 =	Float (Gegenstelle darf IP-Adresse ändern) aktiviert (default)
`comp_lzo`	0 =	LZO-Komprimierung deaktiviert
	1 =	LZO-Komprimierung aktiviert (default)
`masquerade`	0 =	Pakete vor Tunneln nicht maskieren
	1 =	Pakete vor Tunneln maskieren (default)
`cipher`	BF-CBC =	Verschlüsselungsalgorithmus Blowfish 128 Bit (default)
	DES-CBC =	Verschlüsselungsalg. DES 64 Bit
	DES-EDE-CBC =	Verschlüsselungsalg. DES EDE 128 Bit
	DES-EDE3-CBC =	Verschlüsselungsalg. DES EDE3 192 Bit
	DESX-CBC =	Verschlüsselungsalg. DESX 192 Bit
	CAST5-CBC =	Verschlüsselungsalg. CAST5 128 Bit
	IDEA-CBC =	Verschlüsselungsalg. IDEA 128 Bit
	RC2-CBC =	Verschlüsselungsalg. RC2 128 Bit
	RC2-40-CBC =	Verschlüsselungsalg. RC2 40 Bit
	RC2-64-CBC =	Verschlüsselungsalg. RC2 64 Bit
	AES-128-CBC =	Verschlüsselungsalg. AES 128 Bit
	AES-192-CBC =	Verschlüsselungsalg. AES 192 Bit
	AES-256-CBC =	Verschlüsselungsalg. AES 256 Bit
	none =	Keine Verschlüsselung
`verb`	Ausführlichkeit der Meldungen im Verb.-Log (default: 3, 0-9)	
`fragment`	Maximale Größe der Tunnelpakete (in Bytes)	
`reneg`	Intervall für Schlüsselerneuerung (in Sekunden, default: 3600)	
`ping`	Intervall für Ping-Versand an Gegenstelle (in Sekunden, default: 30)	
`restart`	Intervall für Ping-Restart (in Sekunden, default: 60)	

`auth_type`	static = Keine Authentifizierung oder mit statischem Schlüssel
	cert = Authentifizierung mit Zertifikaten
`client_to_client`	0 = Kommunikation zwischen Clients nicht erlauben (default)
	1 = Kommunikation zwischen Clients erlauben
`pool_ip`	IP-Adressen-Pool für die Clients
`pool_netmask`	Netzmaske des IP-Adressen-Pools
`list`	a = Neue Einträge werden an bestehende Liste angehängt
	d = Bestehende Liste wird gelöscht (default)
`remote_peer`	IP-Adresse oder Domainname der Gegenstelle
`remote_peer2`	IP-Adresse oder Domainname der alternativen Gegenstelle
`local_vpn_ip`	IP-Adresse des VPN-Tunnels lokal
`remote_vpn_ip`	IP-Adresse des VPN-Tunnels der Gegenstelle
`remote_net`	Netzadresse des Netzwerks hinter dem VPN-Tunnel
`remote_netmask`	Netzmaske des Netzwerks hinter dem VPN-Tunnel
`pool_ip6`	IPv6-Adressen-Pool für die Clients
`pool_netmask6`	Netzmaske des IPv6-Adressen-Pools
`local_vpn_ip6`	IPv6-Adresse des VPN-Tunnels lokal
`remote_vpn_ip6`	IPv6-Adresse des VPN-Tunnels der Gegenstelle
`remote_net6`	IPv6-Netzadresse des Netzwerks hinter dem VPN-Tunnel
`remote_netmask6`	IPv6-Netzmaske des Netzwerks hinter dem VPN-Tunnel
`tls_auth`	0 = Statischer Schlüssel wird nicht zusätzlich zur Authentifizierung mit Zertifikaten verwendet (default)
	1 = Statischer Schlüssel wird zusätzlich zur Authentifizierung mit Zertifikaten verwendet
	(ab FW 2.12.3)
`key_direction`	none = Keine Benutzungsrichtung des Schlüssels vorgegeben (default)
	0 = Benutzungsrichtung des Schlüssels ist „0“
	1 = Benutzungsrichtung des Schlüssels ist „1“
	(ab FW 2.12.3)
`hash`	sha1 = Hash-Algorithmus SHA-1 (default)
	sha224 = Hash-Algorithmus SHA-224
	sha256 = Hash-Algorithmus SHA-256
	sha384 = Hash-Algorithmus SHA-384
	sha512 = Hash-Algorithmus SHA-512
	none = Kein Hash-Algorithmus verwendet
	(ab FW 2.12.7)
`new_entry`	Neuer Routeneintrag zu Client-Netzwerk, der folgende Unterobjekte übergibt:

common_name	„Common Name“ im Zertifikat des Clients
net	Netzwerkadresse des Clients
netmask	Netzmaske des Clients
vpn_ip	VPN-IP-Adresse des Clients
dh_parameters	Diffie-Hellman-Parametersatz
crl	Certificate Revocation List
ca_certificate	CA-Zertifikat
public_certificate	Öffentliches Zertifikat des Servers
private_key	Privater Schlüssel des Servers
static_key	Statischer Schlüssel
[openvpn client wwan]	*bei LTE-Routern*
start_openvpn_client	0 = OpenVPN-Client für WWAN-Verbindungen deaktiviert (default)
	1 = OpenVPN-Client für WWAN-Verbindungen aktiviert
remote_peer	IP-Adresse oder Domainname der Gegenstelle
remote_peer2	IP-Adresse oder Domainname der alternativen Gegenstelle
lport	Lokaler Port des Tunnels (default: 1194)
rport	Gegenstellen-Port des Tunnels (default: 1194)
protocol	udp = UDP-Protokoll wird verwendet
	tcp = TCP-Protokoll wird verwendet
defaultroute	0 = Default-Route deaktiviert (default)
	1 = Default-Route aktiviert
bind	0 = Nobind (lokale Adresse und Port fixieren) deaktiviert
	1 = Nobind (lokale Adresse und Port fixieren) aktiviert (default)
float	0 = Float (Gegenstelle darf IP-Adresse ändern) deaktiviert
	1 = Float (Gegenstelle darf IP-Adresse ändern) aktiviert (default)
comp_lzo	0 = LZO-Komprimierung deaktiviert
	1 = LZO-Komprimierung aktiviert (default)
masquerade	0 = Pakete vor Tunneln nicht maskieren
	1 = Pakete vor Tunneln maskieren (default)

`cipher`	BF-CBC =	Verschlüsselungsalgorithmus Blowfish 128 Bit (default)
	DES-CBC =	Verschlüsselungsalg. DES 64 Bit
	DES-EDE-CBC =	Verschlüsselungsalg. DES EDE 128 Bit
	DES-EDE3-CBC =	Verschlüsselungsalg. DES EDE3 192 Bit
	DESX-CBC =	Verschlüsselungsalg. DESX 192 Bit
	CAST5-CBC =	Verschlüsselungsalg. CAST5 128 Bit
	IDEA-CBC =	Verschlüsselungsalg. IDEA 128 Bit
	RC2-CBC =	Verschlüsselungsalg. RC2 128 Bit
	RC2-40-CBC =	Verschlüsselungsalg. RC2 40 Bit
	RC2-64-CBC =	Verschlüsselungsalg. RC2 64 Bit
	AES-128-CBC =	Verschlüsselungsalg. AES 128 Bit
	AES-192-CBC =	Verschlüsselungsalg. AES 192 Bit
	AES-256-CBC =	Verschlüsselungsalg. AES 256 Bit
	none =	Keine Verschlüsselung
`verb`	Ausführlichkeit der Meldungen im Verb.-Log (default: 3, 0-9)	
`fragment`	Maximale Größe der Tunnelpakete (in Bytes)	
`reneg`	Intervall für Schlüsselerneuerung (in Sekunden, default: 3600)	
`ping`	Intervall für Ping-Versand an Gegenstelle (in Sekunden, default: 30)	
`restart`	Intervall für Ping-Restart (in Sekunden, default: 60)	
`icmp_ping`	IP-Adresse oder Domainname für zusätzlichen ICMP-Ping	

`auth_type`	static = Keine Authentifizierung oder mit statischem Schlüssel cert = Authentifizierung mit Zertifikaten
`username`	Benutzername des Clients für Anmeldung am OpenVPN-Server Objektwert muss in Hochkommas übergeben werden!
`password`	Kennwort des Clients für Anmeldung am OpenVPN-Server Objektwert muss in Hochkommas übergeben werden!
`check_server_cert`	0 = Überprüfung des Zertifikatstyps der Gegenstelle deaktiviert (default) 1 = Überprüfung des Zertifikatstyps der Gegenstelle aktiviert
`local_vpn_ip`	IP-Adresse des VPN-Tunnels lokal
`remote_vpn_ip`	IP-Adresse des VPN-Tunnels der Gegenstelle
`remote_net`	Netzadresse des Netzwerks hinter dem VPN-Tunnel
`remote_netmask`	Netzmaske des Netzwerks hinter dem VPN-Tunnel
`local_vpn_ip6`	IPv6-Adresse des VPN-Tunnels lokal
`remote_vpn_ip6`	IPv6-Adresse des VPN-Tunnels der Gegenstelle
`remote_net6`	IPv6-Netzadresse des Netzwerks hinter dem VPN-Tunnel
`remote_netmask6`	IPv6-Netzmaske des Netzwerks hinter dem VPN-Tunnel
`proxy_name`	IP-Adresse oder Domainname des Proxy-Servers
`proxy_type`	http = HTTP-Proxy wird verwendet socks5 = SOCKS5-Proxy wird verwendet
`proxy_port`	Port des Proxy-Servers
`proxy_user`	Benutzername für den Proxy-Servers Objektwert muss in Hochkommas übergeben werden!
`proxy_password`	Passwort für den Proxy-Servers Objektwert muss in Hochkommas übergeben werden!
`tls_auth`	0 = Statischer Schlüssel wird nicht zusätzlich zur Authentifizierung mit Zertifikaten verwendet (default) 1 = Statischer Schlüssel wird zusätzlich zur Authentifizierung mit Zertifikaten verwendet *(ab FW 2.12.3)*
`key_direction`	none = Keine Benutzungsrichtung des Schlüssels vorgegeben (default) 0 = Benutzungsrichtung des Schlüssels ist „0“ 1 = Benutzungsrichtung des Schlüssels ist „1“ *(ab FW 2.12.3)*

`hash`	sha1 = Hash-Algorithmus SHA-1 (default)
	sha224 = Hash-Algorithmus SHA-224
	sha256 = Hash-Algorithmus SHA-256
	sha384 = Hash-Algorithmus SHA-384
	sha512 = Hash-Algorithmus SHA-512
	none = Kein Hash-Algorithmus verwendet
	(ab FW 2.12.7)
`ca_certificate`	CA-Zertifikat
`public_certificate`	Öffentliches Zertifikat des Clients
`private_key`	Privater Schlüssel des Clients
`static_key`	Statischer Schlüssel
[pptp server wwan]	*bei LTE-Routern*
`start_pptp_server`	0 = PPTP-Server für WWAN-Verbindungen deaktiviert (default)
	1 = PPTP-Server für WWAN-Verbindungen aktiviert
`authentication`	none = Keine Authentifizierung
	pap = Authentifizierung über PAP
	chap = Authentifizierung über CHAP
	mschap = Authentifizierung über MS-CHAP
	mschap-v2 = Authentifizierung über MS-CHAP-v2 (default)
`encryption`	none = Keine Verschlüsselung
	mppe-40 = Verschlüsselung über MPPE-40
	mppe-128 = Verschlüsselung über MPPE-128
`mtu`	MTU (Maximum Transmission Unit)
`mru`	MRU (Maximum Receive Unit)
`local_ip`	IPv4-Adresse des VPN-Tunnels lokal
`remote_vpn_ip_start`	IP-Adressen-Pool für die Clients (Anfang des Adressbereichs)
`remote_vpn_ip_end`	IP-Adressen-Pool für die Clients (Ende des Adressbereichs)
`list`	a = Neue Einträge werden an bestehende Liste angehängt
	d = Bestehende Liste wird gelöscht (default)
`new_entry`	Neuer Benutzereintrag, der folgende Unterobjekte übergibt:
`username`	Benutzername des Benutzers
	Objektwert muss in Hochkommas übergeben werden!
`password`	Kennwort des Benutzers
	Objektwert muss in Hochkommas übergeben werden!

[pptp client wwan]	*bei LTE-Routern*
start_pptp_client	0 = PPTP-Client für WWAN-Verbindungen deaktiviert (default)
	1 = PPTP-Client für WWAN-Verbindungen aktiviert
remote_peer	IP-Adresse oder Domainname der Gegenstelle
username	Benutzername des Clients für Anmeldung am PPTP-Server
	Objektwert muss in Hochkommas übergeben werden!
password	Kennwort des Clients für Anmeldung am PPTP-Server
	Objektwert muss in Hochkommas übergeben werden!
encryption	none = Keine Verschlüsselung
	mppe-40 = Verschlüsselung über MPPE-40
	mppe-128 = Verschlüsselung über MPPE-128
defaultroute	0 = Default-Route deaktiviert (default)
	1 = Default-Route aktiviert
remote_net	Lokales Subnetz der Gegenstelle
remote_netmask	Netzmaske des lokalen Subnetzes der Gegenstelle
mtu	MTU (Maximum Transmission Unit)
mru	MRU (Maximum Receive Unit)
icmp_ping	IP-Adresse oder Domainname für zusätzlichen ICMP-Ping
[ipsec wwan]	*bei LTE-Routern; <x> = 1-10*
start_ipsec	0 = IPsec für WWAN-Verbindungen deaktiviert (default)
	1 = IPsec für WWAN-Verbindungen aktiviert
nat_traversal	on = NAT-Traversal ist aktiviert (default)
	off = NAT-Traversal ist deaktiviert
	forced = NAT-Traversal wird erzwungen
keep_alive	Intervall der Keep-Alive-Pakete (in Sekunden, default: 10)
start_tunnel<x>	0 = IPsec-Tunnel <x> deaktiviert (default)
	1 = IPsec-Tunnel <x> aktiviert
	10<X> = Fallback für Tunnel <X>
tunnel_name<x>	Name für IPsec-Tunnel <x>
remote_peer<x>	IP-Adresse oder Domainname der Gegenstelle
local_net<x>	Eigenes Subnetz
local_netmask<x>	Netzmaske des eigenen Subnetzes
remote_net<x>	Lokales Subnetz der Gegenstelle
remote_netmask<x>	Netzmaske des lokalen Subnetzes der Gegenstelle
remote_id<x>	ID der Gegenstelle
	Objektwert muss in Hochkommas übergeben werden!

`local_id<x>`	Eigene ID Objektwert muss in Hochkommas übergeben werden!
`auth_mode<x>`	main = Authentifizierungsmodus Main wird verwendet (default) aggressive = Authentifizierungsmodus Aggressive wird verwendet
`ike_cipher<x>`	3des = IKE-Verschlüsselungsalg. DES EDE3 (default) aes128 = IKE-Verschlüsselungsalg. AES 128 Bit aes192 = IKE-Verschlüsselungsalg. AES 192 Bit aes256 = IKE-Verschlüsselungsalg. AES 256 Bit
`ike_hash<x>`	sha1 = IKE-Hash-Algorithmus SHA1 (default) md5 = IKE-Hash-Algorithmus MD5
`ike_dh<x>`	modp768 = Diffie-Hellman-Gruppe für IKE ist DH 768 modp1024 = Diffie-Hellman-Gruppe für IKE ist DH 1024 (default) modp1536 = Diffie-Hellman-Gruppe für IKE ist DH 1536
`ipsec_cipher<x>`	3des = IPsec-Verschlüsselungsalg. DES EDE3 (default) aes128 = IPsec-Verschlüsselungsalg. AES 128 Bit aes192 = IPsec-Verschlüsselungsalg. AES 192 Bit aes256 = IPsec-Verschlüsselungsalg. AES 256 Bit
`ipsec_hash<x>`	sha1 = IPsec-Hash-Algorithmus SHA1 (default) md5 = IPsec-Hash-Algorithmus MD5
`key_attempts<x>`	Maximale Verbindungsversuche (0 = unendlich)
`masquerade<x>`	0 = Pakete durch den Tunnel nicht maskieren 1 = Pakete durch den Tunnel maskieren (default)
`dpd_interval<x>`	Intervall für Dead-Peer-Detection (in Sekunden, default: 30)
`dpd_timeout<x>`	Timeout für Dead-Peer-Detection (in Sekunden, default: 120)

`dpd_action<x>`	clear = Abbauen der Verbindung bei Dead-Peer-Detection hold = Halten der Verbindung bei Dead-Peer-Detection restart = Neu starten der Verbindung bei Dead-Peer-Detection (default)
`pfs<x>`	0 = Perfect-Forward-Secrecy ist deaktiviert 1 = Perfect-Forward-Secrecy ist aktiviert (default)
`key_lifetime<x>`	Intervall für Schlüsselerneuerung (in Sekunden, default: 3600) *(bis FW 2.12.3)*
`icmp_ping<x>`	IP-Adresse oder Domainname für zusätzlichen ICMP-Ping
`auth_type<x>`	cert = Authentifizierung mit Zertifikaten psk = Authentifizierung mit Passphrase (PSK)
`psk<x>`	Passphrase (PSK) Objektwert muss in Hochkommas übergeben werden!
`ca_certificate<x>`	CA-Zertifikat
`public_certificate<x>`	Öffentliches Zertifikat
`private_key<x>`	Privater Schlüssel
`ipsec_lifetime<x>`	Intervall für IPsec SA Schlüsselerneuerung (in Sekunden, default: 3600) *(ab FW 2.12.3)*
`ike_lifetime<x>`	Intervall für IKE SA Schlüsselerneuerung (in Sekunden, default: 86400) *(ab FW 2.12.3)*
`local_protocol<x>`	Zugelassenes Protokoll am lokalen Ende des Tunnels (IANA-Nummer) *(ab FW 2.12.3)*
`local_port<x>`	Zugelassener Port am lokalen Ende des Tunnels *(ab FW 2.12.3)*
`remote_protocol<x>`	Zugelassenes Protokoll am Gegenstellen-Ende des Tunnels (IANA-Nummer) *(ab FW 2.12.3)*
`remote_port<x>`	Zugelassener Port am Gegenstellen-Ende des Tunnels *(ab FW 2.12.3)*

[gre wwan]	*bei LTE-Routern*
start_gre_tunnel	0 = GRE-Tunnel für WWAN-Verbindungen deaktiviert (default) 1 = GRE-Tunnel für WWAN-Verbindungen aktiviert
remote_ip	IP-Adresse oder Domainname der Gegenstelle
local_ip	Eigene IP-Adresse
tunnel_ip	Lokale Tunnel-IP-Adresse
tunnel_netmask	Optionale Netzmaske der lokalen Tunnel-IP-Adresse
mtu	MTU (Maximum Transmission Unit)
ttl	TTL (Time to Live, default: 0)
list	a = Neue Einträge werden an bestehende Liste angehängt d = Bestehende Liste wird gelöscht (default)
new_entry	Neuer Routeneintrag, der folgende Unterobjekte übergibt:
net	Netzwerkadresse der Route
netmask	Netzmaske der Route
gateway	Gateway der Route

[dialin]

`start_dialin`	0 = Dial-In deaktiviert (default)
	1 = Dial-In erfolgt über internes Kommunikationsgerät
	2 = Dial-In erfolgt über redundantes Kommunikationsgerät
	3 = Dial-In erfolgt über internes oder redundantes Kommunikationsgerät
`dialin_prio`	0 = Dial-In vor LAN (ext) nicht priorisieren (default)
	1 = Dial-In vor LAN (ext) priorisieren
`idletime`	Leerlaufzeit in Sekunden, nach der eine Einwahlverbindung ohne Datenverkehr getrennt wird (default: 0, keine Trennung)
`rings`	Anzahl der Klingelzeichen bis zur Anrufannahme
`authentication`	0 = Authentifizierung für Dial-In deaktiviert
	1 = Authentifizierung für Dial-In aktiviert (default)
`username<x>`	Benutzername für Authentifizierungskonto <x> (*<x> = 0-9*)
	Objektwert muss in Hochkommas übergeben werden!
`password<x>`	Passwort für Authentifizierungskonto <x> (*<x> = 0-9*)
	Objektwert muss in Hochkommas übergeben werden!
`auth<x>`	pap = Authentifizierung für Authentifizierungskonto <x> über PAP
	chap = Authentifizierung für Authentifizierungskonto <x> über CHAP
`callback<x>`	0 = Rückruf für Authentifizierungskonto <x> deaktiviert (default)
	1 = Rückruf für Authentifizierungskonto <x> aktiviert
`ip_local_intern`	Eigene IP-Adresse
`ip_remote_intern`	IP-Adresse der Gegenstelle
`ip_local_extern`	Eigene IP-Adresse des redundanten Kommunikationsgeräts
`ip_remote_extern`	IP-Adresse der Gegenstelle des red. Kommunikationsgeräts
`callback`	0 = Automatischer Rückruf deaktiviert (default)
	1 = Automatischer Rückruf aktiviert
	bei HSPA, GRPS, ISDN- oder Modem-Routern
`callback_mode`	auth = Rückruf nach PPP-Authentifizierung
	clip = Rückruf nach Anruf einer der angegebenen Nummern:
`clip1`	Rufnummer 1, nach deren Anruf ein Rückruf erfolgt
`clip2`	Rufnummer 2, nach deren Anruf ein Rückruf erfolgt
`clip3`	Rufnummer 3, nach deren Anruf ein Rückruf erfolgt

`clip4`	Rufnummer 4, nach deren Anruf ein Rückruf erfolgt
`clip5`	Rufnummer 5, nach deren Anruf ein Rückruf erfolgt

`[ routing dialin ]`

`default_route`	0 = Keine Default-Route setzen
	1 = Default-Route setzen (default)
`nat_incoming`	0 = NAT für eingehende Pakete deaktiviert
	1 = NAT für eingehende Pakete aktiviert (default)
`nat_outgoing`	0 = NAT für ausgehende Pakete deaktiviert
	1 = NAT für ausgehende Pakete aktiviert (default)
`list`	a = Neue Einträge werden an bestehende Liste angehängt
	d = Bestehende Liste wird gelöscht (default)
`default6_route`	0 = Keine IPv6-Default-Route setzen
	1 = IPv6-Default-Route setzen (default)
	(ab FW 2.10.0)
`new_entry`	Neuer Routeneintrag, der folgende Unterobjekte übergibt:
`net`	Netzwerkadresse der Route für IPv4
`netmask`	Netzmaske der Route für IPv4
`ipv6`	Netzwerkadresse der Route für IPv6
	(ab FW 2.10.0)
`prefix_length`	Netzmaske der Route für IPv6
	(ab FW 2.10.0)

[firewall dialin]

`start_firewall`	0 = Firewall für Dial-In-Verbindungen deaktiviert (default)
	1 = Firewall für Dial-In-Verbindungen aktiviert
`start_firewall6`	0 = Firewall für IPv6-Dial-In-Verbindungen deaktiviert
	1 = Firewall für IPv6-Dial-In-Verbindungen aktiviert (default)
	(ab FW 2.10.0)
`list`	a = Neue Einträge werden an bestehende Liste angehängt
	d = Bestehende Liste wird gelöscht (default)
`new_entry`	Neue zugelassene Verbindung, die folgende Unterobjekte übergibt:
`protocol`	tcp = TCP-Protokoll wird verwendet
	udp = UDP-Protokoll wird verwendet
	icmp = ICMP-Protokoll wird verwendet
	icmpv6 = ICMPv6-Protokoll wird verwendet *(ab FW 2.12.0)*
	esp = ESP-Protokoll wird verwendet *(ab FW 2.12.0)*
	ah = AH-Protokoll wird verwendet *(ab FW 2.12.0)*
	gre = GRE-Protokoll wird verwendet *(ab FW 2.12.0)*
	all = Alle Protokolle sind zugelassen *(ab FW 2.12.0)*
`direction`	in = Nur eingehende Verbindungen sind zugelassen
	out = Nur ausgehende Verbindungen sind zugelassen
	both = Ein- und ausgehende Verbindungen sind zugelassen
`source_ip`	IP-Adresse des Absenders
`source_netmask`	Netzmaske des Absenders
`dest_port`	Port des Empfängers (oder Anfang des Portbereichs *(ab FW 2.6.0)*)
`dest_port_end`	Ende des Portbereichs des Empfängers *(ab FW 2.6.0)*
`dest_ip`	IP-Adresse des Empfängers
`dest_netmask`	Netzmaske des Empfängers
`dialinuser`	Name des zugelassenen Benutzers *(--- für alle)*
	Objektwert muss in Hochkommas übergeben werden!
`ip_version`	ipv4 = Regel kann nur für IPv4-Verbindungen angelegt werden
	ipv6 = Regel kann nur für IPv6-Verbindungen angelegt werden
	all = Regel kann für IPv4-und IPv6-Verbindungen angelegt werden
	(ab FW 2.12.0)

[openvpn server dialin]

`start_openvpn_server`	0 = OpenVPN-Server für Dial-In-Verbindungen deaktiviert (default)
	1 = OpenVPN-Server für Dial-In-Verbindungen aktiviert
`lport`	Lokaler Port des Tunnels (default: 1194)
`rport`	Gegenstellen-Port des Tunnels (default: 1194)
`protocol`	udp = UDP-Protokoll wird verwendet
	tcp = TCP-Protokoll wird verwendet
`push_server_route`	0 = Server-Netz den Clients mitteilen deaktiviert
	1 = Server-Netz den Clients mitteilen aktiviert (default)
	(ab FW 2.6.0)
`float`	0 = Float (Gegenstelle darf IP-Adresse ändern) deaktiviert
	1 = Float (Gegenstelle darf IP-Adresse ändern) aktiviert (default)
`comp_lzo`	0 = LZO-Komprimierung deaktiviert
	1 = LZO-Komprimierung aktiviert (default)
`masquerade`	0 = Pakete vor Tunneln nicht maskieren
	1 = Pakete vor Tunneln maskieren (default)
`cipher`	BF-CBC = Verschlüsselungsalgorithmus Blowfish 128 Bit (default)
	DES-CBC = Verschlüsselungsalg. DES 64 Bit
	DES-EDE-CBC = Verschlüsselungsalg. DES EDE 128 Bit
	DES-EDE3-CBC = Verschlüsselungsalg. DES EDE3 192 Bit
	DESX-CBC = Verschlüsselungsalg. DESX 192 Bit
	CAST5-CBC = Verschlüsselungsalg. CAST5 128 Bit
	IDEA-CBC = Verschlüsselungsalg. IDEA 128 Bit
	RC2-CBC = Verschlüsselungsalg. RC2 128 Bit
	RC2-40-CBC = Verschlüsselungsalg. RC2 40 Bit
	RC2-64-CBC = Verschlüsselungsalg. RC2 64 Bit
	AES-128-CBC = Verschlüsselungsalg. AES 128 Bit
	AES-192-CBC = Verschlüsselungsalg. AES 192 Bit
	AES-256-CBC = Verschlüsselungsalg. AES 256 Bit
	none = Keine Verschlüsselung (*ab FW 2.8.0)*
`verb`	Ausführlichkeit der Meldungen im Verbindungs-Log (default: 3, 0-9)
`fragment`	Maximale Größe der Tunnelpakete (in Bytes)
`reneg`	Intervall für Schlüsselerneuerung (in Sekunden, default: 3600)
`ping`	Intervall für Ping-Versand an Gegenstelle (in Sekunden, default: 30)
`restart`	Intervall für Ping-Restart (in Sekunden, default: 60)

`auth_type`	static = Keine Authentifizierung oder mit statischem Schlüssel
	cert = Authentifizierung mit Zertifikaten
`client_to_client`	0 = Kommunikation zwischen Clients nicht erlauben (default)
	1 = Kommunikation zwischen Clients erlauben
`pool_ip`	IP-Adressen-Pool für die Clients
`pool_netmask`	Netzmaske des IP-Adressen-Pools
`list`	a = Neue Einträge werden an bestehende Liste angehängt
	d = Bestehende Liste wird gelöscht (default)
`remote_peer`	IP-Adresse oder Domainname der Gegenstelle
`remote_peer2`	IP-Adresse oder Domainname der alternativen Gegenstelle
`local_vpn_ip`	IP-Adresse des VPN-Tunnels lokal
`remote_vpn_ip`	IP-Adresse des VPN-Tunnels der Gegenstelle
`remote_net`	Netzadresse des Netzwerks hinter dem VPN-Tunnel
`remote_netmask`	Netzmaske des Netzwerks hinter dem VPN-Tunnel
`pool_ip6`	IPv6-Adressen-Pool für die Clients
	(ab FW 2.10.0)
`pool_netmask6`	Netzmaske des IPv6-Adressen-Pools
	(ab FW 2.10.0)
`local_vpn_ip6`	IPv6-Adresse des VPN-Tunnels lokal
	(ab FW 2.10.0)
`remote_vpn_ip6`	IPv6-Adresse des VPN-Tunnels der Gegenstelle
	(ab FW 2.10.0)
`remote_net6`	IPv6-Netzadresse des Netzwerks hinter dem VPN-Tunnel
	(ab FW 2.10.0)
`remote_netmask6`	IPv6-Netzmaske des Netzwerks hinter dem VPN-Tunnel
	(ab FW 2.10.0)
`tls_auth`	0 = Statischer Schlüssel wird nicht zusätzlich zur Authentifizierung mit Zertifikaten verwendet (default)
	1 = Statischer Schlüssel wird zusätzlich zur Authentifizierung mit Zertifikaten verwendet
	(ab FW 2.12.3)
`key_direction`	none = Keine Benutzungsrichtung des Schlüssels vorgegeben (default)
	0 = Benutzungsrichtung des Schlüssels ist „0“
	1 = Benutzungsrichtung des Schlüssels ist „1“
	(ab FW 2.12.3)

`hash`	sha1 = Hash-Algorithmus SHA-1 (default)
	sha224 = Hash-Algorithmus SHA-224
	sha256 = Hash-Algorithmus SHA-256
	sha384 = Hash-Algorithmus SHA-384
	sha512 = Hash-Algorithmus SHA-512
	none = Kein Hash-Algorithmus verwendet
	(ab FW 2.12.7)
`new_entry`	Neuer Routeneintrag zu Client-Netzwerk, der folgende Unterobjekte übergibt:
`common_name`	„Common Name“ im Zertifikat des Clients
`net`	Netzwerkadresse des Clients
`netmask`	Netzmaske des Clients
`vpn_ip`	VPN-IP-Adresse des Clients
`dh_parameters`	Diffie-Hellman-Parametersatz
`crl`	Certificate Revocation List
`ca_certificate`	CA-Zertifikat
`public_certificate`	Öffentliches Zertifikat des Servers
`private_key`	Privater Schlüssel des Servers
`static_key`	Statischer Schlüssel

[openvpn client dialin]

`start_openvpn_client`	0 = OpenVPN-Client für Dial-In-Verbindungen deaktiviert (default)
	1 = OpenVPN-Client für Dial-In-Verbindungen aktiviert
`remote_peer`	IP-Adresse oder Domainname der Gegenstelle
`remote_peer2`	IP-Adresse oder Domainname der alternativen Gegenstelle
`lport`	Lokaler Port des Tunnels (default: 1194)
`rport`	Gegenstellen-Port des Tunnels (default: 1194)
`protocol`	udp = UDP-Protokoll wird verwendet
	tcp = TCP-Protokoll wird verwendet
`defaultroute`	0 = Default-Route deaktiviert (default)
	1 = Default-Route aktiviert
	(ab FW 2.6.0)
`bind`	0 = Nobind (lokale Adresse und Port fixieren) deaktiviert
	1 = Nobind (lokale Adresse und Port fixieren) aktiviert (default)
`float`	0 = Float (Gegenstelle darf IP-Adresse ändern) deaktiviert
	1 = Float (Gegenstelle darf IP-Adresse ändern) aktiviert (default)

`comp_lzo`	0 =	LZO-Komprimierung deaktiviert
	1 =	LZO-Komprimierung aktiviert (default)
`masquerade`	0 =	Pakete vor Tunneln nicht maskieren
	1 =	Pakete vor Tunneln maskieren (default)
`cipher`	BF-CBC =	Verschlüsselungsalgorithmus Blowfish 128 Bit (default)
	DES-CBC =	Verschlüsselungsalg. DES 64 Bit
	DES-EDE-CBC =	Verschlüsselungsalg. DES EDE 128 Bit
	DES-EDE3-CBC =	Verschlüsselungsalg. DES EDE3 192 Bit
	DESX-CBC =	Verschlüsselungsalg. DESX 192 Bit
	CAST5-CBC =	Verschlüsselungsalg. CAST5 128 Bit
	IDEA-CBC =	Verschlüsselungsalg. IDEA 128 Bit
	RC2-CBC =	Verschlüsselungsalg. RC2 128 Bit
	RC2-40-CBC =	Verschlüsselungsalg. RC2 40 Bit
	RC2-64-CBC =	Verschlüsselungsalg. RC2 64 Bit
	AES-128-CBC =	Verschlüsselungsalg. AES 128 Bit
	AES-192-CBC =	Verschlüsselungsalg. AES 192 Bit
	AES-256-CBC =	Verschlüsselungsalg. AES 256 Bit
	none =	Keine Verschlüsselung (*ab FW 2.8.0)*
`verb`	Ausführlichkeit der Meldungen im Verbindungs-Log (default: 3, 0-9)	
`fragment`	Maximale Größe der Tunnelpakete (in Bytes)	
`reneg`	Intervall für Schlüsselerneuerung (in Sekunden, default: 3600)	
`ping`	Intervall für Ping-Versand an Gegenstelle (in Sekunden, default: 30)	
`restart`	Intervall für Ping-Restart (in Sekunden, default: 60)	
`icmp_ping`	IP-Adresse oder Domainname für zusätzlichen ICMP-Ping	
`auth_type`	static =	Keine Authentifizierung oder mit statischem Schlüssel
	cert =	Authentifizierung mit Zertifikaten
`username`	Benutzername des Clients für Anmeldung am OpenVPN-Server	
	Objektwert muss in Hochkommas übergeben werden!	
`password`	Kennwort des Clients für Anmeldung am OpenVPN-Server	
	Objektwert muss in Hochkommas übergeben werden!	
`check_server_cert`	0 =	Überprüfung des Zertifikatstyps der Gegenstelle deaktiviert (default)
	1 =	Überprüfung des Zertifikatstyps der Gegenstelle aktiviert

`local_vpn_ip`	IP-Adresse des VPN-Tunnels lokal
`remote_vpn_ip`	IP-Adresse des VPN-Tunnels der Gegenstelle
`remote_net`	Netzadresse des Netzwerks hinter dem VPN-Tunnel
`remote_netmask`	Netzmaske des Netzwerks hinter dem VPN-Tunnel
`local_vpn_ip6`	IPv6-Adresse des VPN-Tunnels lokal *(ab FW 2.10.0)*
`remote_vpn_ip6`	IPv6-Adresse des VPN-Tunnels der Gegenstelle *(ab FW 2.10.0)*
`remote_net6`	IPv6-Netzadresse des Netzwerks hinter dem VPN-Tunnel *(ab FW 2.10.0)*
`remote_netmask6`	IPv6-Netzmaske des Netzwerks hinter dem VPN-Tunnel *(ab FW 2.10.0)*
`proxy_name`	IP-Adresse oder Domainname des Proxy-Servers *(ab FW 2.11.0)*
`proxy_type`	http = HTTP-Proxy wird verwendet socks5 = SOCKS5-Proxy wird verwendet *(ab FW 2.11.0)*
`proxy_port`	Port des Proxy-Servers *(ab FW 2.11.0)*
`proxy_user`	Benutzername für den Proxy-Servers *(ab FW 2.11.0)* Objektwert muss in Hochkommas übergeben werden!
`proxy_password`	Passwort für den Proxy-Servers *(ab FW 2.11.0)* Objektwert muss in Hochkommas übergeben werden!
`tls_auth`	0 = Statischer Schlüssel wird nicht zusätzlich zur Authentifizierung mit Zertifikaten verwendet (default) 1 = Statischer Schlüssel wird zusätzlich zur Authentifizierung mit Zertifikaten verwendet *(ab FW 2.12.3)*
`key_direction`	none = Keine Benutzungsrichtung des Schlüssels vorgegeben (default) 0 = Benutzungsrichtung des Schlüssels ist „0“ 1 = Benutzungsrichtung des Schlüssels ist „1“ *(ab FW 2.12.3)*
`hash`	sha1 = Hash-Algorithmus SHA-1 (default) sha224 = Hash-Algorithmus SHA-224 sha256 = Hash-Algorithmus SHA-256 sha384 = Hash-Algorithmus SHA-384 sha512 = Hash-Algorithmus SHA-512 none = Kein Hash-Algorithmus verwendet *(ab FW 2.12.7)*
`ca_certificate`	CA-Zertifikat
`public_certificate`	Öffentliches Zertifikat des Clients
`private_key`	Privater Schlüssel des Clients

`static_key`	Statischer Schlüssel
`[ pptp server dialin ]`	*ab FW 2.6.0*
`start_pptp_server`	0 = PPTP-Server für Dial-In-Verbindungen deaktiviert (default) 1 = PPTP-Server für Dial-In-Verbindungen aktiviert
`authentication`	none = Keine Authentifizierung pap = Authentifizierung über PAP chap = Authentifizierung über CHAP mschap = Authentifizierung über MS-CHAP mschap-v2 = Authentifizierung über MS-CHAP-v2 (default)
`encryption`	none = Keine Verschlüsselung mppe-40 = Verschlüsselung über MPPE-40 mppe-128 = Verschlüsselung über MPPE-128
`mtu`	MTU (Maximum Transmission Unit)
`mru`	MRU (Maximum Receive Unit)
`local_ip`	IPv4-Adresse des VPN-Tunnels lokal
`remote_vpn_ip_start`	IP-Adressen-Pool für die Clients (Anfang des Adressbereichs)
`remote_vpn_ip_end`	IP-Adressen-Pool für die Clients (Ende des Adressbereichs)
`list`	a = Neue Einträge werden an bestehende Liste angehängt d = Bestehende Liste wird gelöscht (default)
`new_entry`	Neuer Benutzereintrag, der folgende Unterobjekte übergibt:
`username`	Benutzername des Benutzers Objektwert muss in Hochkommas übergeben werden!
`password`	Kennwort des Benutzers Objektwert muss in Hochkommas übergeben werden!
`[ pptp client dialin ]`	*ab FW 2.6.0*
`start_pptp_client`	0 = PPTP-Client für Dial-In-Verbindungen deaktiviert (default) 1 = PPTP-Client für Dial-In-Verbindungen aktiviert
`remote_peer`	IP-Adresse oder Domainname der Gegenstelle
`username`	Benutzername des Clients für Anmeldung am PPTP-Server Objektwert muss in Hochkommas übergeben werden!
`password`	Kennwort des Clients für Anmeldung am PPTP-Server Objektwert muss in Hochkommas übergeben werden!

`encryption`	none = Keine Verschlüsselung
	mppe-40 = Verschlüsselung über MPPE-40
	mppe-128 = Verschlüsselung über MPPE-128
`defaultroute`	0 = Default-Route deaktiviert (default)
	1 = Default-Route aktiviert
`remote_net`	Lokales Subnetz der Gegenstelle
`remote_netmask`	Netzmaske des lokalen Subnetzes der Gegenstelle
`mtu`	MTU (Maximum Transmission Unit)
`mru`	MRU (Maximum Receive Unit)
`icmp_ping`	IP-Adresse oder Domainname für zusätzlichen ICMP-Ping
[ipsec dialin]	*FW 2.4.0*
`start_ipsec`	0 = IPsec für Dial-In-Verbindungen deaktiviert (default)
	1 = IPsec für Dial-In-Verbindungen aktiviert
`remote_peer`	IP-Adresse oder Domainname der Gegenstelle
`remote_net`	Lokales Subnetz der Gegenstelle
`remote_netmask`	Netzmaske des lokalen Subnetzes der Gegenstelle
`remote_id`	ID der Gegenstelle
	Objektwert muss in Hochkommas übergeben werden!
`local_id`	Eigene ID
	Objektwert muss in Hochkommas übergeben werden!
`auth_mode`	main = Authentifizierungsmodus Main wird verwendet (default)
	aggressive = Authentifizierungsmodus Aggressive wird verwendet
`ike_cipher`	3des = IKE-Verschlüsselungsalgorithmus DES EDE3 (default)
	aes128 = IKE-Verschlüsselungsalgorithmus AES 128 Bit
	aes192 = IKE-Verschlüsselungsalgorithmus AES 192 Bit
	aes256 = IKE-Verschlüsselungsalgorithmus AES 256 Bit
`ike_hash`	sha1 = IKE-Hash-Algorithmus SHA1 (default)
	md5 = IKE-Hash-Algorithmus MD5
`ike_dh`	modp768 = Diffie-Hellman-Gruppe für IKE ist DH 768
	modp1024 = Diffie-Hellman-Gruppe für IKE ist DH 1024 (default)
	modp1536 = Diffie-Hellman-Gruppe für IKE ist DH 1536
`ipsec_cipher`	3des = IPsec-Verschlüsselungsalg. DES EDE3 (default)
	aes128 = IPsec-Verschlüsselungsalg. AES 128 Bit
	aes192 = IPsec-Verschlüsselungsalg. AES 192 Bit
	aes256 = IPsec-Verschlüsselungsalg. AES 256 Bit

`ipsec_hash`	sha1 = IPsec-Hash-Algorithmus SHA1 (default)
	md5 = IPsec-Hash-Algorithmus MD5
`key_attempts`	Maximale Verbindungsversuche (0 = unendlich)
`nat_traversal`	on = NAT-Traversal ist aktiviert (default)
	off = NAT-Traversal ist deaktiviert
	forced = NAT-Traversal wird erzwungen
`keep_alive`	Intervall der Keep-Alive-Pakete (in Sekunden, default: 10)
`pfs`	0 = Perfect-Forward-Secrecy ist deaktiviert
	1 = Perfect-Forward-Secrecy ist aktiviert (default)
`dpd_interval`	Intervall für Dead-Peer-Detection (in Sekunden, default: 30)
`dpd_timeout`	Timeout für Dead-Peer-Detection (in Sekunden, default: 120)
`dpd_action`	clear = Abbauen der Verbindung bei Dead-Peer-Detection
	hold = Halten der Verbindung bei Dead-Peer-Detection
	restart = Neu starten der Verbindung bei Dead-Peer-Detection (default)
`key_lifetime`	Intervall für Schlüsselerneuerung (in Sekunden, default: 3600)
`icmp_ping`	IP-Adresse oder Domainname für zusätzlichen ICMP-Ping
`auth_type`	cert = Authentifizierung mit Zertifikaten
	psk = Authentifizierung mit Passphrase (PSK)
`psk`	Passphrase (PSK)
	Objektwert muss in Hochkommas übergeben werden!
`masquerade`	0 = Pakete durch den Tunnel nicht maskieren
	1 = Pakete durch den Tunnel maskieren (default)
`ca_certificate`	CA-Zertifikat
`public_certificate`	Öffentliches Zertifikat
`private_key`	Privater Schlüssel
[ipsec dialin]	*ab FW 2.5.0; <x> = 1-10*
`start_ipsec`	0 = IPsec für Dial-In-Verbindungen deaktiviert (default)
	1 = IPsec für Dial-In-Verbindungen aktiviert
`nat_traversal`	on = NAT-Traversal ist aktiviert (default)
	off = NAT-Traversal ist deaktiviert
	forced = NAT-Traversal wird erzwungen
`keep_alive`	Intervall der Keep-Alive-Pakete (in Sekunden, default: 10)
`start_tunnel<x>`	0 = IPsec-Tunnel <x> deaktiviert (default)
	1 = IPsec-Tunnel <x> aktiviert
	10<X> = Fallback für Tunnel <X> (ab FW 2.12.0)

tunnel_name<x>	Name für IPsec-Tunnel <x>
remote_peer<x>	IP-Adresse oder Domainname der Gegenstelle
local_net<x>	Eigenes Subnetz
local_netmask<x>	Netzmaske des eigenen Subnetzes
remote_net<x>	Lokales Subnetz der Gegenstelle
remote_netmask<x>	Netzmaske des lokalen Subnetzes der Gegenstelle
remote_id<x>	ID der Gegenstelle
	Objektwert muss in Hochkommas übergeben werden!
local_id<x>	Eigene ID
	Objektwert muss in Hochkommas übergeben werden!
auth_mode<x>	main = Authentifizierungsmodus Main wird verwendet (default)
	aggressive = Authentifizierungsmodus Aggressive wird verwendet
ike_cipher<x>	3des = IKE-Verschlüsselungsalgorithmus DES EDE3 (default)
	aes128 = IKE-Verschlüsselungsalgorithmus AES 128 Bit
	aes192 = IKE-Verschlüsselungsalgorithmus AES 192 Bit
	aes256 = IKE-Verschlüsselungsalgorithmus AES 256 Bit
ike_hash<x>	sha1 = IKE-Hash-Algorithmus SHA1 (default)
	md5 = IKE-Hash-Algorithmus MD5
ike_dh<x>	modp768 = Diffie-Hellman-Gruppe für IKE ist DH 768
	modp1024 = Diffie-Hellman-Gruppe für IKE ist DH 1024 (default)
	modp1536 = Diffie-Hellman-Gruppe für IKE ist DH 1536
ipsec_cipher<x>	3des = IPsec-Verschlüsselungsalg. DES EDE3 (default)
	aes128 = IPsec-Verschlüsselungsalg. AES 128 Bit
	aes192 = IPsec-Verschlüsselungsalg. AES 192 Bit
	aes256 = IPsec-Verschlüsselungsalg. AES 256 Bit
ipsec_hash<x>	sha1 = IPsec-Hash-Algorithmus SHA1 (default)
	md5 = IPsec-Hash-Algorithmus MD5
key_attempts<x>	Maximale Verbindungsversuche (0 = unendlich)
masquerade<x>	0 = Pakete durch den Tunnel nicht maskieren
	1 = Pakete durch den Tunnel maskieren (default)
dpd_interval<x>	Intervall für Dead-Peer-Detection (in Sekunden, default: 30)
dpd_timeout<x>	Timeout für Dead-Peer-Detection (in Sekunden, default: 120)

dpd_action<x>	clear = Abbauen der Verbindung bei Dead-Peer-Detection
	hold = Halten der Verbindung bei Dead-Peer-Detection
	restart = Neu starten der Verbindung bei Dead-Peer-Detection (default)
pfs<x>	0 = Perfect-Forward-Secrecy ist deaktiviert
	1 = Perfect-Forward-Secrecy ist aktiviert (default)
key_lifetime<x>	Intervall für Schlüsselerneuerung (in Sekunden, default: 3600)
	(bis FW 2.12.3)
icmp_ping<x>	IP-Adresse oder Domainname für zusätzlichen ICMP-Ping
auth_type<x>	cert = Authentifizierung mit Zertifikaten
	psk = Authentifizierung mit Passphrase (PSK)
psk<x>	Passphrase (PSK)
	Objektwert muss in Hochkommas übergeben werden!
ca_certificate<x>	CA-Zertifikat
public_certificate<x>	Öffentliches Zertifikat
private_key<x>	Privater Schlüssel
ipsec_lifetime<x>	Intervall für IPsec SA Schlüsselerneuerung (in Sekunden, default: 3600)
	(ab FW 2.12.3)
ike_lifetime<x>	Intervall für IKE SA Schlüsselerneuerung (in Sekunden, default: 86400)
	(ab FW 2.12.3)
local_protocol<x>	Zugelassenes Protokoll am lokalen Ende des Tunnels (IANA-Nummer)
	(ab FW 2.12.3)
local_port<x>	Zugelassener Port am lokalen Ende des Tunnels
	(ab FW 2.12.3)
remote_protocol<x>	Zugelassenes Protokoll am Gegenstellen-Ende des Tunnels (IANA-Nummer)
	(ab FW 2.12.3)
remote_port<x>	Zugelassener Port am Gegenstellen-Ende des Tunnels
	(ab FW 2.12.3)

[gre dialin]	*ab FW 2.11.0*
`start_gre_tunnel`	0 = GRE-Tunnel für Dial-In-Verbindungen deaktiviert (default) 1 = GRE-Tunnel für Dial-In-Verbindungen aktiviert
`remote_ip`	IP-Adresse oder Domainname der Gegenstelle
`local_ip`	Eigene IP-Adresse
`tunnel_ip`	Lokale Tunnel-IP-Adresse
`tunnel_netmask`	Optionale Netzmaske der lokalen Tunnel-IP-Adresse
`mtu`	MTU (Maximum Transmission Unit)
`ttl`	TTL (Time to Live, default: 0)
`list`	a = Neue Einträge werden an bestehende Liste angehängt d = Bestehende Liste wird gelöscht (default)
`new_entry`	Neuer Routeneintrag, der folgende Unterobjekte übergibt:
`net`	Netzwerkadresse der Route
`netmask`	Netzmaske der Route
`gateway`	Gateway der Route

[dialout]

`start_dialout`	0 = Dial-Out deaktiviert (default)
	1 = Dial-Out erfolgt über internes Kommunikationsgerät
	2 = Dial-Out erfolgt primär über internes und sekundär über redundantes Kommunikationsgerät
	3 = Dial-Out erfolgt primär über redundantes und sekundär über internes Kommunikationsgerät
	4 = Dial-Out erfolgt primär über zuletzt verwendetes, funktionierendes Kommunikationsgerät
`dialnumber`	Rufnummer für Ziel A
	Objektwert muss in Hochkommas übergeben werden!
`dialnumber_b`	Rufnummer für Ziel B
	Objektwert muss in Hochkommas übergeben werden!
`username`	Benutzername für Ziel A
	Objektwert muss in Hochkommas übergeben werden!
`username_b`	Benutzername für Ziel B
	Objektwert muss in Hochkommas übergeben werden!
`password`	Kennwort für Ziel A
	Objektwert muss in Hochkommas übergeben werden!
`password_b`	Kennwort für Ziel B
	Objektwert muss in Hochkommas übergeben werden!
`auth`	both = Authentifizierung für Ziel A über PAP oder CHAP
	pap = Authentifizierung für Ziel A über PAP
	chap = Authentifizierung für Ziel A über CHAP
`auth_b`	both = Authentifizierung für Ziel B über PAP oder CHAP
	pap = Authentifizierung für Ziel B über PAP
	chap = Authentifizierung für Ziel B über CHAP
`apn`	Access Point Name für Ziel A *(nur bei Mobilfunk-Routern)*
`apn_b`	Access Point Name für Ziel B *(nur bei Mobilfunk-Routern)*
`sim`	1 = SIM-Karte 1 wird für Ziel B verwendet (default)
	2 = SIM-Karte 2 wird für Ziel B verwendet
	(nur bei Mobilfunk-Routern)
`idletime`	Maximale Leerlaufzeit (in Sekunden, default: 20, 0 = unbegrenzt)
`maxtime`	Maximale Verbindungszeit (in Sekunden, default: 0, 0 = unbegrenzt)
`prio`	target_a = Immer Ziel A zuerst versuchen
	last = Zuletzt erfolgreiches Ziel zuerst versuchen
	toggle = Anderes als zuletzt erfolgreiches Ziel zuerst versuchen *(ab FW 2.11.0)*

`fetch_dns`	0 = Keine DNS-Server-Adresse anfordern 1 = DNS-Server-Adresse anfordern (default)
`dialnumber_extern`	Rufnummer für Ziel A des red. Kommunikationsgeräts Objektwert muss in Hochkommas übergeben werden!
`dialnumber_extern_b`	Rufnummer für Ziel B des red. Kommunikationsgeräts Objektwert muss in Hochkommas übergeben werden!
`username_extern`	Benutzername für Ziel A des red. Kommunikationsgeräts Objektwert muss in Hochkommas übergeben werden!
`username_extern_b`	Benutzername für Ziel B des red. Kommunikationsgeräts Objektwert muss in Hochkommas übergeben werden!
`password_extern`	Kennwort für Ziel A des red. Kommunikationsgeräts Objektwert muss in Hochkommas übergeben werden!
`password_extern_b`	Kennwort für Ziel B des red. Kommunikationsgeräts Objektwert muss in Hochkommas übergeben werden!
`auth_extern`	both = Authentifizierung für Ziel A des redundanten Kommunikationsgeräts über PAP oder CHAP pap = Authentifizierung für Ziel A des redundanten Kommunikationsgeräts über PAP chap = Authentifizierung für Ziel A des redundanten Kommunikationsgeräts über CHAP
`auth_extern_b`	both = Authentifizierung für Ziel B des redundanten Kommunikationsgeräts über PAP oder CHAP pap = Authentifizierung für Ziel B des redundanten Kommunikationsgeräts über PAP chap = Authentifizierung für Ziel B des redundanten Kommunikationsgeräts über CHAP
`apn_extern`	Access Point Name für Ziel A des red. Kommunikationsgeräts *(nur bei Mobilfunk-Routern)*
`apn_extern_b`	Access Point Name für Ziel B des red. Kommunikationsgeräts *(nur bei Mobilfunk-Routern)*
`sim_extern`	1 = SIM-Karte 1 wird für Ziel B des redundanten Kommunikationsgeräts verwendet (default) 2 = SIM-Karte 2 wird für Ziel B des redundanten Kommunikationsgeräts verwendet *(nur bei Mobilfunk-Routern)*
`idletime_extern`	Maximale Leerlaufzeit (in Sekunden, default: 20, 0 = unbegrenzt) des redundanten Kommunikationsgeräts
`maxtime_extern`	Maximale Verbindungszeit (in Sekunden, default: 0, 0 = unbegrenzt) des redundanten Kommunikationsgeräts
`prio_extern`	target_a = Immer Ziel A des redundanten Kommunikationsgeräts zuerst versuchen last = Zuletzt erfolgreiches Ziel des redundanten Kommunikationsgeräts zuerst versuchen

`fetch_dns_extern`	0 = Keine DNS-Server-Adresse des redundanten Kommunikationsgeräts anfordern
	1 = DNS-Server-Adresse des redundanten Kommunikationsgeräts anfordern (default)
`flat`	0 = Standleitungsbetrieb deaktiviert (default)
	1 = Standleitungsbetrieb aktiviert
`check_interval`	Zeitintervall der Verbindungsüberprüfung (in Min., default: 60)
`check_type`	dns = Verbindungsprüfung über DNS-Abfrage (default)
	ping = Verbindungsprüfung über Ping
`dns_target`	Ziel der Verbindungsprüfung über DNS-Abfrage
`ping_target`	Ziel der Verbindungsprüfung über Ping
`auto_daily_start`	0 = Täglicher automatischer Verbindungsaufbau deaktiviert (default)
	1 = Täglicher automatischer Verbindungsaufbau
`auto_hour_start`	Täglicher autom. Verbindungsaufbau um (Stunde, 00-23)
`auto_minutes_start`	Täglicher autom. Verbindungsaufbau um (Minute, 00-59)
`auto_daily_stop`	0 = Täglicher automatischer Verbindungsabbau deaktiviert (default)
	1 = Täglicher automatischer Verbindungsabbau
`auto_hour_stop`	Täglicher autom. Verbindungsabbau um (Stunde, 00-23)
`auto_minutes_stop`	Täglicher autom. Verbindungsabbau um (Minute, 00-59)
`mtu`	MTU (Maximum Transmission Unit) *(ab FW 2.11.0)*
`mru`	MRU (Maximum Receive Unit) *(ab FW 2.11.0)*
`renegotiate`	0 = Eine bestehende WAN-Verbindung wird im Fehlerfall nicht abgebaut
	1 = Eine bestehende WAN-Verbindung wird im Fehlerfall abgebaut bevor eine neue Verbindung aufgebaut wird (default)
	(ab FW 2.11.0)

`[ routing dialout ]`

`default_route`	0 = Keine Default-Route setzen
	1 = Default-Route setzen (default)
`nat_incoming`	0 = NAT für eingehende Pakete deaktiviert
	1 = NAT für eingehende Pakete aktiviert (default)
`nat_outgoing`	0 = NAT für ausgehende Pakete deaktiviert
	1 = NAT für ausgehende Pakete aktiviert (default)
`list`	a = Neue Einträge werden an bestehende Liste angehängt
	d = Bestehende Liste wird gelöscht (default)

`default6_route`	0 = Keine IPv6-Default-Route setzen
	1 = IPv6-Default-Route setzen (default)
	(ab FW 2.10.0)
`new_entry`	Neuer Routeneintrag, der folgende Unterobjekte übergibt:
`net`	Netzwerkadresse der Route
`netmask`	Netzmaske der Route
`ipv6`	Netzwerkadresse der Route für IPv6
	(ab FW 2.10.0)
`prefix_length`	Netzmaske der Route für IPv6
	(ab FW 2.10.0)

[dialfilters dialout]

`start_dialfilter`	0 = Wählfilter für Dial-Out-Verbindungen deaktiviert (default)
	1 = Wählfilter für Dial-Out-Verbindungen aktiviert
`list`	a = Neue Einträge werden an bestehende Liste angehängt
	d = Bestehende Liste wird gelöscht (default)
`new_entry`	Neue Wählfilterregel, die folgende Unterobjekte übergibt:
`protocol`	icmp = ICMP-Protokoll wird verwendet
	udp = UDP-Protokoll wird verwendet
	tcp = TCP-Protokoll wird verwendet
`source_ip`	IP-Adresse des Absenders
`source_netmask`	Netzmaske des Absenders
`dest_port`	Port des Empfängers
`dest_ip`	IP-Adresse des Empfängers
`dest_netmask`	Netzmaske des Empfängers
`dns`	0 = DNS-Anfragen der Absender-IP-Adresse dürfen keine Verbindung initiieren (default)
	1 = DNS-Anfragen der Absender-IP-Adresse dürfen eine Verbindung initiieren

[firewall dialout]

`start_firewall`	0 = Firewall für Dial-Out-Verbindungen deaktiviert (default) 1 = Firewall für Dial-Out-Verbindungen aktiviert
`start_firewall6`	0 = Firewall für IPv6-Dial-Out-Verbindungen deaktiviert 1 = Firewall für IPv6-Dial-Out-Verbindungen aktiviert (default) *(ab FW 2.10.0)*
`list`	a = Neue Einträge werden an bestehende Liste angehängt d = Bestehende Liste wird gelöscht (default)
`new_entry`	Neue zugelassene Verbindung, die folgende Unterobjekte übergibt:
`protocol`	tcp = TCP-Protokoll wird verwendet udp = UDP-Protokoll wird verwendet icmp = ICMP-Protokoll wird verwendet icmpv6 = ICMPv6-Protokoll wird verwendet *(ab FW 2.12.0)* esp = ESP-Protokoll wird verwendet *(ab FW 2.12.0)* ah = AH-Protokoll wird verwendet *(ab FW 2.12.0)* gre = GRE-Protokoll wird verwendet *(ab FW 2.12.0)* all = Alle Protokolle sind zugelassen *(ab FW 2.12.0)*
`direction`	in = Nur eingehende Verbindungen sind zugelassen out = Nur ausgehende Verbindungen sind zugelassen both = Ein- und ausgehende Verbindungen sind zugelassen
`source_ip`	IP-Adresse des Absenders
`source_netmask`	Netzmaske des Absenders
`dest_port`	Port des Empfängers (oder Anfang des Portbereichs *(ab FW 2.6.0)*)
`dest_port_end`	Ende des Portbereichs des Empfängers *(ab FW 2.6.0)*
`dest_ip`	IP-Adresse des Empfängers
`dest_netmask`	Netzmaske des Empfängers
`ip_version`	ipv4 = Regel kann nur für IPv4-Verbindungen angelegt werden ipv6 = Regel kann nur für IPv6-Verbindungen angelegt werden all = Regel kann für IPv4-und IPv6-Verbindungen angelegt werden *(ab FW 2.12.0)*

[portforward dialout]

`start_portforwarding`	0 = Port-Forwarding für Dial-Out-Verbindungen deaktiviert 1 = Port-Forwarding für Dial-Out-Verbindungen aktiviert (default)
`exposed_host`	IP-Adresse des „Exposed Host“
`list`	a = Neue Einträge werden an bestehende Liste angehängt d = Bestehende Liste wird gelöscht (default)
`new_entry`	Neue zugelassene Verbindung, die folgende Unterobjekte übergibt:
`protocol`	tcp = TCP-Protokoll wird verwendet udp = UDP-Protokoll wird verwendet icmp = ICMP-Protokoll wird verwendet esp = ESP-Protokoll wird verwendet ah = AH-Protokoll wird verwendet *(ab FW 2.12.0)* gre = GRE-Protokoll wird verwendet *(ab FW 2.12.0)*
`source_port_start`	Beginn des Port-Bereichs für die Weiterleitung
`source_port_end`	Ende des Port-Bereichs für die Weiterleitung
`dest_ip`	IP-Adresse des Weiteleitungsziels
`dest_port`	Port des Weiteleitungsziels
`apply`	always = Regel gilt immer wan = Regel gilt für WAN-Verbindungen openvpn = Regel gilt für OpenVPN-Verbindungen *(ab FW 2.12.6)*

[openvpn server dialout]

`start_openvpn_server`	0 =	OpenVPN-Server für Dial-Out-Verbindungen deaktiviert (default)
	1 =	OpenVPN-Server für Dial-Out-Verbindungen aktiviert
`lport`	Lokaler Port des Tunnels (default: 1194)	
`rport`	Gegenstellen-Port des Tunnels (default: 1194)	
`protocol`	udp =	UDP-Protokoll wird verwendet
	tcp =	TCP-Protokoll wird verwendet
`push_server_route`	0 =	Server-Netz den Clients mitteilen deaktiviert
	1 =	Server-Netz den Clients mitteilen aktiviert (default)
	(ab FW 2.6.0)	
`float`	0 =	Float (Gegenstelle darf IP-Adresse ändern) deaktiviert
	1 =	Float (Gegenstelle darf IP-Adresse ändern) aktiviert (default)
`comp_lzo`	0 =	LZO-Komprimierung deaktiviert
	1 =	LZO-Komprimierung aktiviert (default)
`masquerade`	0 =	Pakete vor Tunneln nicht maskieren
	1 =	Pakete vor Tunneln maskieren (default)
`cipher`	BF-CBC =	Verschlüsselungsalgorithmus Blowfish 128 Bit (default)
	DES-CBC =	Verschlüsselungsalg. DES 64 Bit
	DES-EDE-CBC =	Verschlüsselungsalg. DES EDE 128 Bit
	DES-EDE3-CBC =	Verschlüsselungsalg. DES EDE3 192 Bit
	DESX-CBC =	Verschlüsselungsalg. DESX 192 Bit
	CAST5-CBC =	Verschlüsselungsalg. CAST5 128 Bit
	IDEA-CBC =	Verschlüsselungsalg. IDEA 128 Bit
	RC2-CBC =	Verschlüsselungsalg. RC2 128 Bit
	RC2-40-CBC =	Verschlüsselungsalg. RC2 40 Bit
	RC2-64-CBC =	Verschlüsselungsalg. RC2 64 Bit
	AES-128-CBC =	Verschlüsselungsalg. AES 128 Bit
	AES-192-CBC =	Verschlüsselungsalg. AES 192 Bit
	AES-256-CBC =	Verschlüsselungsalg. AES 256 Bit
	none =	Keine Verschlüsselung (*ab FW 2.8.0)*
`verb`	Ausführlichkeit der Meldungen im Verb.-Log (default: 3, 0-9)	
`fragment`	Maximale Größe der Tunnelpakete (in Bytes)	
`reneg`	Intervall für Schlüsselerneuerung (in Sekunden, default: 3600)	
`ping`	Intervall für Ping-Versand an Gegenstelle (in Sekunden, default: 30)	

`restart`	Intervall für Ping-Restart (in Sekunden, default: 60)
`auth_type`	static = Keine Authentifizierung oder mit statischem Schlüssel
	cert = Authentifizierung mit Zertifikaten
`client_to_client`	0 = Kommunikation zwischen Clients nicht erlauben (default)
	1 = Kommunikation zwischen Clients erlauben
`pool_ip`	IP-Adressen-Pool für die Clients
`pool_netmask`	Netzmaske des IP-Adressen-Pools
`list`	a = Neue Einträge werden an bestehende Liste angehängt
	d = Bestehende Liste wird gelöscht (default)
`remote_peer`	IP-Adresse oder Domainname der Gegenstelle
`remote_peer2`	IP-Adresse oder Domainname der alternativen Gegenstelle
`local_vpn_ip`	IP-Adresse des VPN-Tunnels lokal
`remote_vpn_ip`	IP-Adresse des VPN-Tunnels der Gegenstelle
`remote_net`	Netzadresse des Netzwerks hinter dem VPN-Tunnel
`remote_netmask`	Netzmaske des Netzwerks hinter dem VPN-Tunnel
`pool_ip6`	IPv6-Adressen-Pool für die Clients
	(ab FW 2.10.0)
`pool_netmask6`	Netzmaske des IPv6-Adressen-Pools
	(ab FW 2.10.0)
`local_vpn_ip6`	IPv6-Adresse des VPN-Tunnels lokal
	(ab FW 2.10.0)
`remote_vpn_ip6`	IPv6-Adresse des VPN-Tunnels der Gegenstelle
	(ab FW 2.10.0)
`remote_net6`	IPv6-Netzadresse des Netzwerks hinter dem VPN-Tunnel
	(ab FW 2.10.0)
`remote_netmask6`	IPv6-Netzmaske des Netzwerks hinter dem VPN-Tunnel
	(ab FW 2.10.0)
`tls_auth`	0 = Statischer Schlüssel wird nicht zusätzlich zur Authentifizierung mit Zertifikaten verwendet (default)
	1 = Statischer Schlüssel wird zusätzlich zur Authentifizierung mit Zertifikaten verwendet
	(ab FW 2.12.3)
`key_direction`	none = Keine Benutzungsrichtung des Schlüssels vorgegeben (default)
	0 = Benutzungsrichtung des Schlüssels ist „0“
	1 = Benutzungsrichtung des Schlüssels ist „1“
	(ab FW 2.12.3)

`hash`	sha1 = Hash-Algorithmus SHA-1 (default)
	sha224 = Hash-Algorithmus SHA-224
	sha256 = Hash-Algorithmus SHA-256
	sha384 = Hash-Algorithmus SHA-384
	sha512 = Hash-Algorithmus SHA-512
	none = Kein Hash-Algorithmus verwendet
	(ab FW 2.12.7)
`new_entry`	Neuer Routeneintrag zu Client-Netzwerk, der folgende Unterobjekte übergibt:
`common_name`	„Common Name“ im Zertifikat des Clients
`net`	Netzwerkadresse des Clients
`netmask`	Netzmaske des Clients
`vpn_ip`	VPN-IP-Adresse des Clients
`dh_parameters`	Diffie-Hellman-Parametersatz
`crl`	Certificate Revocation List
`ca_certificate`	CA-Zertifikat
`public_certificate`	Öffentliches Zertifikat des Servers
`private_key`	Privater Schlüssel des Servers
`static_key`	Statischer Schlüssel

[openvpn client dialout]

`start_openvpn_client`	0 = OpenVPN-Client für Dial-Out-Verbindungen deaktiviert (default)
	1 = OpenVPN-Client für Dial-Out-Verbindungen aktiviert
`remote_peer`	IP-Adresse oder Domainname der Gegenstelle
`remote_peer2`	IP-Adresse oder Domainname der alternativen Gegenstelle
`lport`	Lokaler Port des Tunnels (default: 1194)
`rport`	Gegenstellen-Port des Tunnels (default: 1194)
`protocol`	udp = UDP-Protokoll wird verwendet
	tcp = TCP-Protokoll wird verwendet
`defaultroute`	0 = Default-Route deaktiviert (default)
	1 = Default-Route aktiviert
	(ab FW 2.6.0)
`bind`	0 = Nobind (lokale Adresse und Port fixieren) deaktiviert
	1 = Nobind (lokale Adresse und Port fixieren) aktiviert (default)
`float`	0 = Float (Gegenstelle darf IP-Adresse ändern) deaktiviert
	1 = Float (Gegenstelle darf IP-Adresse ändern) aktiviert (default)

`comp_lzo`	0 = LZO-Komprimierung deaktiviert	
	1 = LZO-Komprimierung aktiviert (default)	
`masquerade`	0 = Pakete vor Tunneln nicht maskieren	
	1 = Pakete vor Tunneln maskieren (default)	
`cipher`	BF-CBC =	Verschlüsselungsalgorithmus Blowfish 128 Bit (default)
	DES-CBC =	Verschlüsselungsalg. DES 64 Bit
	DES-EDE-CBC =	Verschlüsselungsalg. DES EDE 128 Bit
	DES-EDE3-CBC =	Verschlüsselungsalg. DES EDE3 192 Bit
	DESX-CBC =	Verschlüsselungsalg. DESX 192 Bit
	CAST5-CBC =	Verschlüsselungsalg. CAST5 128 Bit
	IDEA-CBC =	Verschlüsselungsalg. IDEA 128 Bit
	RC2-CBC =	Verschlüsselungsalg. RC2 128 Bit
	RC2-40-CBC =	Verschlüsselungsalg. RC2 40 Bit
	RC2-64-CBC =	Verschlüsselungsalg. RC2 64 Bit
	AES-128-CBC =	Verschlüsselungsalg. AES 128 Bit
	AES-192-CBC =	Verschlüsselungsalg. AES 192 Bit
	AES-256-CBC =	Verschlüsselungsalg. AES 256 Bit
	none =	Keine Verschlüsselung (*ab FW 2.8.0)*
`verb`	Ausführlichkeit der Meldungen im Verb.-Log (default: 3, 0-9)	
`fragment`	Maximale Größe der Tunnelpakete (in Bytes)	
`reneg`	Intervall für Schlüsselerneuerung (in Sekunden, default: 3600)	
`ping`	Intervall für Ping-Versand an Gegenstelle (in Sekunden, default: 30)	
`restart`	Intervall für Ping-Restart (in Sekunden, default: 60)	
`icmp_ping`	IP-Adresse oder Domainname für zusätzlichen ICMP-Ping	

`auth_type`	static = Keine Authentifizierung oder mit statischem Schlüssel cert = Authentifizierung mit Zertifikaten
`username`	Benutzername des Clients für Anmeldung am OpenVPN-Server Objektwert muss in Hochkommas übergeben werden!
`password`	Kennwort des Clients für Anmeldung am OpenVPN-Server Objektwert muss in Hochkommas übergeben werden!
`check_server_cert`	0 = Überprüfung des Zertifikatstyps der Gegenstelle deaktiviert (default) 1 = Überprüfung des Zertifikatstyps der Gegenstelle aktiviert
`local_vpn_ip`	IP-Adresse des VPN-Tunnels lokal
`remote_vpn_ip`	IP-Adresse des VPN-Tunnels der Gegenstelle
`remote_net`	Netzadresse des Netzwerks hinter dem VPN-Tunnel
`remote_netmask`	Netzmaske des Netzwerks hinter dem VPN-Tunnel
`local_vpn_ip6`	IPv6-Adresse des VPN-Tunnels lokal *(ab FW 2.10.0)*
`remote_vpn_ip6`	IPv6-Adresse des VPN-Tunnels der Gegenstelle *(ab FW 2.10.0)*
`remote_net6`	IPv6-Netzadresse des Netzwerks hinter dem VPN-Tunnel *(ab FW 2.10.0)*
`remote_netmask6`	IPv6-Netzmaske des Netzwerks hinter dem VPN-Tunnel *(ab FW 2.10.0)*
`proxy_name`	IP-Adresse oder Domainname des Proxy-Servers *(ab FW 2.11.0)*
`proxy_type`	http = HTTP-Proxy wird verwendet socks5 = SOCKS5-Proxy wird verwendet *(ab FW 2.11.0)*
`proxy_port`	Port des Proxy-Servers *(ab FW 2.11.0)*
`proxy_user`	Benutzername für den Proxy-Servers *(ab FW 2.11.0)* Objektwert muss in Hochkommas übergeben werden!
`proxy_password`	Passwort für den Proxy-Servers *(ab FW 2.11.0)* Objektwert muss in Hochkommas übergeben werden!
`tls_auth`	0 = Statischer Schlüssel wird nicht zusätzlich zur Authentifizierung mit Zertifikaten verwendet (default) 1 = Statischer Schlüssel wird zusätzlich zur Authentifizierung mit Zertifikaten verwendet *(ab FW 2.12.3)*

`key_direction`	none = Keine Benutzungsrichtung des Schlüssels vorgegeben (default) 0 = Benutzungsrichtung des Schlüssels ist „0“ 1 = Benutzungsrichtung des Schlüssels ist „1“ *(ab FW 2.12.3)*
`hash`	sha1 = Hash-Algorithmus SHA-1 (default) sha224 = Hash-Algorithmus SHA-224 sha256 = Hash-Algorithmus SHA-256 sha384 = Hash-Algorithmus SHA-384 sha512 = Hash-Algorithmus SHA-512 none = Kein Hash-Algorithmus verwendet *(ab FW 2.12.7)*
`ca_certificate`	CA-Zertifikat
`public_certificate`	Öffentliches Zertifikat des Clients
`private_key`	Privater Schlüssel des Clients
`static_key`	Statischer Schlüssel

[pptp server dialout]	*ab FW 2.6.0*
start_pptp_server	0 = PPTP-Server für Dial-Out-Verbindungen deaktiviert (default)
	1 = PPTP-Server für Dial-Out-Verbindungen aktiviert
authentication	none = Keine Authentifizierung
	pap = Authentifizierung über PAP
	chap = Authentifizierung über CHAP
	mschap = Authentifizierung über MS-CHAP
	mschap-v2 = Authentifizierung über MS-CHAP-v2 (default)
encryption	none = Keine Verschlüsselung
	mppe-40 = Verschlüsselung über MPPE-40
	mppe-128 = Verschlüsselung über MPPE-128
mtu	MTU (Maximum Transmission Unit)
mru	MRU (Maximum Receive Unit)
local_ip	IPv4-Adresse des VPN-Tunnels lokal
remote_vpn_ip_start	IP-Adressen-Pool für die Clients (Anfang des Adressbereichs)
remote_vpn_ip_end	IP-Adressen-Pool für die Clients (Ende des Adressbereichs)
list	a = Neue Einträge werden an bestehende Liste angehängt
	d = Bestehende Liste wird gelöscht (default)
new_entry	Neuer Benutzereintrag, der folgende Unterobjekte übergibt:
username	Benutzername des Benutzers
	Objektwert muss in Hochkommas übergeben werden!
password	Kennwort des Benutzers
	Objektwert muss in Hochkommas übergeben werden!

[pptp client dialout]	*ab FW 2.6.0*
start_pptp_client	0 = PPTP-Client für Dial-Out-Verbindungen deaktiviert (default)
	1 = PPTP-Client für Dial-Out-Verbindungen aktiviert
remote_peer	IP-Adresse oder Domainname der Gegenstelle
username	Benutzername des Clients für Anmeldung am PPTP-Server
	Objektwert muss in Hochkommas übergeben werden!
password	Kennwort des Clients für Anmeldung am PPTP-Server
	Objektwert muss in Hochkommas übergeben werden!

`encryption`	none = Keine Verschlüsselung mppe-40 = Verschlüsselung über MPPE-40 mppe-128 = Verschlüsselung über MPPE-128
`defaultroute`	0 = Default-Route deaktiviert (default) 1 = Default-Route aktiviert
`remote_net`	Lokales Subnetz der Gegenstelle
`remote_netmask`	Netzmaske des lokalen Subnetzes der Gegenstelle
`mtu`	MTU (Maximum Transmission Unit)
`mru`	MRU (Maximum Receive Unit)
`icmp_ping`	IP-Adresse oder Domainname für zusätzlichen ICMP-Ping

[ipsec dialout]	*FW 2.4.0*
start_ipsec	0 = IPsec für Dial-Out-Verbindungen deaktiviert (default)
	1 = IPsec für Dial-Out-Verbindungen aktiviert
remote_peer	IP-Adresse oder Domainname der Gegenstelle
remote_net	Lokales Subnetz der Gegenstelle
remote_netmask	Netzmaske des lokalen Subnetzes der Gegenstelle
remote_id	ID der Gegenstelle
	Objektwert muss in Hochkommas übergeben werden!
local_id	Eigene ID
	Objektwert muss in Hochkommas übergeben werden!
auth_mode	main = Authentifizierungsmodus Main wird verwendet (default)
	aggressive = Authentifizierungsmodus Aggressive wird verwendet
ike_cipher	3des = IKE-Verschlüsselungsalgorithmus DES EDE3 (default)
	aes128 = IKE-Verschlüsselungsalgorithmus AES 128 Bit
	aes192 = IKE-Verschlüsselungsalgorithmus AES 192 Bit
	aes256 = IKE-Verschlüsselungsalgorithmus AES 256 Bit
ike_hash	sha1 = IKE-Hash-Algorithmus SHA1 (default)
	md5 = IKE-Hash-Algorithmus MD5
ike_dh	modp768 = Diffie-Hellman-Gruppe für IKE ist DH 768
	modp1024 = Diffie-Hellman-Gruppe für IKE ist DH 1024 (default)
	modp1536 = Diffie-Hellman-Gruppe für IKE ist DH 1536
ipsec_cipher	3des = IPsec-Verschlüsselungsalg. DES EDE3 (default)
	aes128 = IPsec-Verschlüsselungsalg. AES 128 Bit
	aes192 = IPsec-Verschlüsselungsalg. AES 192 Bit
	aes256 = IPsec-Verschlüsselungsalg. AES 256 Bit
ipsec_hash	sha1 = IPsec-Hash-Algorithmus SHA1 (default)
	md5 = IPsec-Hash-Algorithmus MD5
key_attempts	Maximale Verbindungsversuche (0 = unendlich)
nat_traversal	on = NAT-Traversal ist aktiviert (default)
	off = NAT-Traversal ist deaktiviert
	forced = NAT-Traversal wird erzwungen
keep_alive	Intervall der Keep-Alive-Pakete (in Sekunden, default: 10)
pfs	0 = Perfect-Forward-Secrecy ist deaktiviert
	1 = Perfect-Forward-Secrecy ist aktiviert (default)
dpd_interval	Intervall für Dead-Peer-Detection (in Sekunden, default: 30)

`dpd_timeout`	Timeout für Dead-Peer-Detection (in Sekunden, default: 120)
`dpd_action`	clear = Abbauen der Verbindung bei Dead-Peer-Detection
	hold = Halten der Verbindung bei Dead-Peer-Detection
	restart = Neu starten der Verbindung bei Dead-Peer-Detection (default)
`key_lifetime`	Intervall für Schlüsselerneuerung (in Sekunden, default: 3600)
`icmp_ping`	IP-Adresse oder Domainname für zusätzlichen ICMP-Ping
`auth_type`	cert = Authentifizierung mit Zertifikaten
	psk = Authentifizierung mit Passphrase (PSK)
`psk`	Passphrase (PSK)
	Objektwert muss in Hochkommas übergeben werden!
`masquerade`	0 = Pakete durch den Tunnel nicht maskieren
	1 = Pakete durch den Tunnel maskieren (default)
`ca_certificate`	CA-Zertifikat
`public_certificate`	Öffentliches Zertifikat
`private_key`	Privater Schlüssel

[ipsec dialout]	*ab FW 2.5.0; <x> = 1-10*
start_ipsec	0 = IPsec für Dial-Out-Verbindungen deaktiviert (default)
	1 = IPsec für Dial-Out-Verbindungen aktiviert
nat_traversal	on = NAT-Traversal ist aktiviert (default)
	off = NAT-Traversal ist deaktiviert
	forced = NAT-Traversal wird erzwungen
keep_alive	Intervall der Keep-Alive-Pakete (in Sekunden, default: 10)
start_tunnel<x>	0 = IPsec-Tunnel <x> deaktiviert (default)
	1 = IPsec-Tunnel <x> aktiviert
	10<X> = Fallback für Tunnel <X> *(ab FW 2.12.0)*
tunnel_name<x>	Name für IPsec-Tunnel <x>
remote_peer<x>	IP-Adresse oder Domainname der Gegenstelle
local_net<x>	Eigenes Subnetz
local_netmask<x>	Netzmaske des eigenen Subnetzes
remote_net<x>	Lokales Subnetz der Gegenstelle
remote_netmask<x>	Netzmaske des lokalen Subnetzes der Gegenstelle
remote_id<x>	ID der Gegenstelle
	Objektwert muss in Hochkommas übergeben werden!
local_id<x>	Eigene ID
	Objektwert muss in Hochkommas übergeben werden!
auth_mode<x>	main = Authentifizierungsmodus Main wird verwendet (default)
	aggressive = Authentifizierungsmodus Aggressive wird verwendet
ike_cipher<x>	3des = IKE-Verschlüsselungsalg. DES EDE3 (default)
	aes128 = IKE-Verschlüsselungsalg. AES 128 Bit
	aes192 = IKE-Verschlüsselungsalg. AES 192 Bit
	aes256 = IKE-Verschlüsselungsalg. AES 256 Bit
ike_hash<x>	sha1 = IKE-Hash-Algorithmus SHA1 (default)
	md5 = IKE-Hash-Algorithmus MD5
ike_dh<x>	modp768 = Diffie-Hellman-Gruppe für IKE ist DH 768
	modp1024 = Diffie-Hellman-Gruppe für IKE ist DH 1024 (default)
	modp1536 = Diffie-Hellman-Gruppe für IKE ist DH 1536
ipsec_cipher<x>	3des = IPsec-Verschlüsselungsalg. DES EDE3 (default)
	aes128 = IPsec-Verschlüsselungsalg. AES 128 Bit
	aes192 = IPsec-Verschlüsselungsalg. AES 192 Bit
	aes256 = IPsec-Verschlüsselungsalg. AES 256 Bit
ipsec_hash<x>	sha1 = IPsec-Hash-Algorithmus SHA1 (default)
	md5 = IPsec-Hash-Algorithmus MD5

`key_attempts<x>`	Maximale Verbindungsversuche (0 = unendlich)
`masquerade<x>`	0 = Pakete durch den Tunnel nicht maskieren
	1 = Pakete durch den Tunnel maskieren (default)
`dpd_interval<x>`	Intervall für Dead-Peer-Detection (in Sekunden, default: 30)
`dpd_timeout<x>`	Timeout für Dead-Peer-Detection (in Sekunden, default: 120)
`dpd_action<x>`	clear = Abbauen der Verbindung bei Dead-Peer-Detection
	hold = Halten der Verbindung bei Dead-Peer-Detection
	restart = Neu starten der Verbindung bei Dead-Peer-Detection (default)
`pfs<x>`	0 = Perfect-Forward-Secrecy ist deaktiviert
	1 = Perfect-Forward-Secrecy ist aktiviert (default)
`key_lifetime<x>`	Intervall für Schlüsselerneuerung (in Sekunden, default: 3600)
	(bis FW 2.12.3)
`icmp_ping<x>`	IP-Adresse oder Domainname für zusätzlichen ICMP-Ping
`auth_type<x>`	cert = Authentifizierung mit Zertifikaten
	psk = Authentifizierung mit Passphrase (PSK)
`psk<x>`	Passphrase (PSK)
	Objektwert muss in Hochkommas übergeben werden!
`ca_certificate<x>`	CA-Zertifikat
`public_certificate<x>`	Öffentliches Zertifikat
`private_key<x>`	Privater Schlüssel
`ipsec_lifetime<x>`	Intervall für IPsec SA Schlüsselerneuerung (in Sekunden, default: 3600)
	(ab FW 2.12.3)
`ike_lifetime<x>`	Intervall für IKE SA Schlüsselerneuerung (in Sekunden, default: 86400)
	(ab FW 2.12.3)
`local_protocol<x>`	Zugelassenes Protokoll am lokalen Ende des Tunnels (IANA-Nummer)
	(ab FW 2.12.3)
`local_port<x>`	Zugelassener Port am lokalen Ende des Tunnels
	(ab FW 2.12.3)
`remote_protocol<x>`	Zugelassenes Protokoll am Gegenstellen-Ende des Tunnels (IANA-Nummer)
	(ab FW 2.12.3)
`remote_port<x>`	Zugelassener Port am Gegenstellen-Ende des Tunnels
	(ab FW 2.12.3)

[gre dialout]	*ab FW 2.11.0*
start_gre_tunnel	0 = GRE-Tunnel für Dial-Out-Verbindungen deaktiviert (default)
	1 = GRE-Tunnel für Dial-Out-Verbindungen aktiviert
remote_ip	IP-Adresse oder Domainname der Gegenstelle
local_ip	Eigene IP-Adresse
tunnel_ip	Lokale Tunnel-IP-Adresse
tunnel_netmask	Optionale Netzmaske der lokalen Tunnel-IP-Adresse
mtu	MTU (Maximum Transmission Unit)
ttl	TTL (Time to Live, default: 0)
list	a = Neue Einträge werden an bestehende Liste angehängt
	d = Bestehende Liste wird gelöscht (default)
new_entry	Neuer Routeneintrag, der folgende Unterobjekte übergibt:
net	Netzwerkadresse der Route
netmask	Netzmaske der Route
gateway	Gateway der Route

[lanext]	
lan_ext_mode	off = LAN (ext)-Schnittstelle deaktiviert (default)
	bridge = LAN (ext) verhält sich wie ein weiterer Switch-Port
	dsl = PPPoE-Verbindung aktiviert
	pppoa = PPPoA-Verbindung aktiviert *(nur ADSL)*
	dhcp = DHCP-Client aktiviert
	static = IP-Adresse statisch einstellen
ip	IP-Adresse der LAN (ext)-Schnittstelle (default: 192.168.2.1)
netmask	Netzmaske der LAN (ext)-Schnittstelle (default: 255.255.255.0)
slaac_active	0 = SLAAC deaktiviert
	1 = SLAAC aktiviert (default)
	(ab FW 2.10.0)
ipv6	IPv6-Adresse des Routers (default: random)
	(ab FW 2.10.0)
prefix_length	Länge des IPv6-Adress-Prefix (7-64, default: 64)
	(ab FW 2.10.0)
add_dhcp_ips	0 = IP-Adresse wird nicht für jeden Host-Eintrag angefordert (default)
	1 = IP-Adresse wird für jeden Host-Eintrag angefordert
	(ab FW 2.11.0)

`lan_ext_medium`	ethernet = LAN (ext) verhält sich wie in LAN (ext) Modus konfiguriert (default) wlan = LAN (ext)-Schnittstelle wird WLAN-Client zugeordnet, Buchse LAN (ext) verhält sich wie ein weiterer Switch-Port, Einstellung in LAN (ext) Modus ist nicht relevant *(bei WLAN-Routern ab FW 2.12.7)*
[sdsl]	*bei SDSL-Routern*
`mode_ch1`	cpe = Gerät wird in der Betriebsart CPE betrieben (default) co = Gerät wird in der Betriebsart CO betrieben
`annex`	b = Gerät verwendet Annex B zur Modulation (default) a = Gerät verwendet Annex A zur Modulation
`aggregate`	0 = Kanäle werden nicht gebündelt (default) 1 = Kanäle werden gebündelt
`min_rate_ch1`	Minimale Geschwindigkeit auf Kanal 1 in Bit/s (default: 192000, mögliche Werte siehe Web-Interface)
`max_rate_ch1`	Maximale Geschwindigkeit auf Kanal 1 in Bit/s (default: 5696000, mögliche Werte siehe Web-Interface)
`line_probing_ch1`	0 = Maximale Geschwindigkeit wird nicht selbständig ausgehandelt 1 = Maximale Geschwindigkeit wird selbständig ausgehandelt (default)
`min_rate_ch2`	Minimale Geschwindigkeit auf Kanal 2 in Bit/s (default: 192000, mögliche Werte siehe Web-Interface)
`max_rate_ch2`	Maximale Geschwindigkeit auf Kanal 2 in Bit/s (default: 5696000, mögliche Werte siehe Web-Interface)
`line_probing_ch2`	0 = Maximale Geschwindigkeit wird nicht selbständig ausgehandelt 1 = Maximale Geschwindigkeit wird selbständig ausgehandelt (default)

[redundant]	*nicht bei LAN-Routern o. redundantem Kommunikationsgerät*
start_redundant	0 = Redundantes WAN deaktiviert (default)
	1 = Redundantes WAN aktiviert
check_interval	Zeitintervall der Verbindungsüberprüfung (in Minuten, default: 5)
check_type	dns = Verbindungsprüfung über DNS-Abfrage (default)
	ping = Verbindungsprüfung über Ping
	link = Verbindungsprüfung über Link-Verlust *(ab FW 2.12.0)*
dns_target	Ziel der Verbindungsprüfung über DNS-Abfrage
ping_target	Ziel der Verbindungsprüfung über Ping
fallback_interval	Intervall für Zurückschalten auf LAN (ext) (in Minuten, default: 10)

[dsl]	
username	Benutzername für Einwahl bei DSL-Provider
	Objektwert muss in Hochkommas übergeben werden!
password	Kennwort für Einwahl bei DSL-Provider
	Objektwert muss in Hochkommas übergeben werden!
idletime	Maximale Leerlaufzeit (in Sekunden, default: 20, 0 = unbegrenzt)
maxtime	Maximale Verbindungszeit (in Sekunden, default: 0, 0 = unbegrenzt)
mtu	MTU (Maximum Transmission Unit)
mru	MRU (Maximum Receive Unit)
fetch_dns	0 = Keine DNS-Server-Adresse anfordern
	1 = DNS-Server-Adresse anfordern (default)
flat	0 = Standleitungsbetrieb deaktiviert (default)
	1 = Standleitungsbetrieb aktiviert
check_interval	Zeitintervall der Verbindungsüberprüfung (in Minuten, default: 60)
check_type	dns = Verbindungsprüfung über DNS-Abfrage (default)
	ping = Verbindungsprüfung über Ping
dns_target	Ziel der Verbindungsprüfung über DNS-Abfrage
ping_target	Ziel der Verbindungsprüfung über Ping
auto_daily_start	0 = Täglicher automatischer Verbindungsaufbau deaktiviert (default)
	1 = Täglicher automatischer Verbindungsaufbau
auto_hour_start	Täglicher autom. Verbindungsaufbau um (Stunde, 00-23)
auto_minutes_start	Täglicher autom. Verbindungsaufbau um (Minute, 00-59)

`auto_daily_stop`	0 = Täglicher automatischer Verbindungsabbau deaktiviert (default) 1 = Täglicher automatischer Verbindungsabbau
`auto_hour_stop`	Täglicher autom. Verbindungsabbau um (Stunde, 00-23)
`auto_minutes_stop`	Täglicher autom. Verbindungsabbau um (Minute, 00-59)
`vpi`	Virtual Path Identifier (0-256; default = 1) *(nur ADSL)*
`vci`	Virtual Channel Identifier (0-65535; default = 1) *(nur ADSL)*
`multiplex`	llc = Multiplex-Verfahren Logical Link Control (default) vcmux = Multiplex-Verfahren Virtual Circuit Multiplexing *(nur ADSL)*
`renegotiate`	0 = Eine bestehende PPP-Verbindung wird im Fehlerfall nicht abgebaut 1 = Eine bestehende PPP-Verbindung wird im Fehlerfall abgebaut bevor eine neue Verbindung aufgebaut wird (default) *(ab FW 2.11.0)*
`ipv6`	0 = IPv6-Adresse und –Prefix beziehen (default) 1 = IPv6-Adresse und -Prefix nicht beziehen *(ab FW 2.12.0)*
`vlan`	VLAN-Tag für Ethernet-Pakete über PPPoE (0-4096) *(ab FW 2.12.9)*

[wlan]	*nur WLAN-Router*	
start_wlan	0 =	WLAN deaktiviert (default)
	1 =	WLAN aktiviert
	(bis FW 2.12.6)	
ssid	SSID der WLAN-Basisstation	
security	none =	Keine Verschlüsselung aktiviert
	psk =	PSK-Verschlüsselung aktiviert
	802.1x =	Authentifizierung nach 802.1x aktiviert
encryption	wpa2 =	WPA2-Verschlüsselung aktiviert (default)
	wpa =	WPA-Verschlüsselung aktiviert
	wpa12 =	WPA bzw. WPA2-Verschlüsselung aktiviert
	wep =	WEP-Verschlüsselung aktiviert
wep_key_nr	Index des bei WEP verwendeten Schlüssels (1-4; default = 1)	
psk	WLAN-Schlüssel	
	Objektwert muss in Hochkommas übergeben werden!	
eap_method	tls =	EAP-Authentifizierung mit TLS (default)
	ttls_md5 =	EAP-Authentifizierung mit TTLS/MD5
	ttls_pap =	EAP-Authentifizierung mit TTLS/PAP
	ttls_chap =	EAP-Authentifizierung mit TTLS/CHAP
	ttls_mschap =	EAP-Authentifizierung mit TTLS/MSCHAP
	ttls_mschapv2 =	EAP-Authentifizierung mit TTLS/MSCHAPv2
	peap_mschapv2 =	EAP-Authentifizierung mit PEAP/MSCHAPv2
eap_encryption	wpa2 =	WPA2-Verschlüsselung aktiviert (default)
	wpa =	WPA-Verschlüsselung aktiviert
	wpa12 =	WPA bzw. WPA2-Verschlüsselung aktiviert
eap_identity	Identität für EAP-Authentifizierung	
	Objektwert muss in Hochkommas übergeben werden!	
eap_password	Passwort für EAP-Authentifizierung	
	Objektwert muss in Hochkommas übergeben werden!	
eap_anonym_identity	Anonyme Identität für EAP-Authentifizierung	
	Objektwert muss in Hochkommas übergeben werden!	
ca_certificate<x>	CA-Zertifikat	
public_certificate<x>	Öffentliches Zertifikat	
private_key<x>	Privater Schlüssel	

[routing lan]

`default_route`	0 = Keine Default-Route setzen (default)
	1 = Default-Route setzen
`default_gateway`	IP-Adresse des Default-Gateways
`nat_incoming`	0 = NAT für eingehende Pakete deaktiviert
	1 = NAT für eingehende Pakete aktiviert (default)
`nat_outgoing`	0 = NAT für ausgehende Pakete deaktiviert
	1 = NAT für ausgehende Pakete aktiviert (default)
`list`	a = Neue Einträge werden an bestehende Liste angehängt
	d = Bestehende Liste wird gelöscht (default)
`default6_route`	0 = Keine IPv6-Default-Route setzen (default)
	1 = IPv6-Default-Route setzen
	(ab FW 2.10.0)
`default6_gateway`	IPv6-Adresse des Default-Gateways
	(ab FW 2.10.0)
`new_entry`	Neuer Routeneintrag, der folgende Unterobjekte übergibt:
`net`	Netzwerkadresse der Route für IPv4
`netmask`	Netzmaske der Route für IPv4
`gateway`	Gateway der Route für IPv4
`ipv6`	Netzwerkadresse der Route für IPv6
	(ab FW 2.10.0)
`prefix_length`	Netzmaske der Route für IPv6
	(ab FW 2.10.0)
`gateway6`	Gateway der Route für IPv6
	(ab FW 2.10.0)

[dialfilters lan]

`start_dialfilter`	0 = Wählfilter für LAN (ext)-Schnittstelle deaktiviert (default)
	1 = Wählfilter für LAN (ext)-Schnittstelle aktiviert
`list`	a = Neue Einträge werden an bestehende Liste angehängt
	d = Bestehende Liste wird gelöscht (default)
`new_entry`	Neue Wählfilterregel, die folgende Unterobjekte übergibt:
`protocol`	icmp = ICMP-Protokoll wird verwendet
	udp = UDP-Protokoll wird verwendet
	tcp = TCP-Protokoll wird verwendet
`source_ip`	IP-Adresse des Absenders
`source_netmask`	Netzmaske des Absenders
`dest_port`	Port des Empfängers
`dest_ip`	IP-Adresse des Empfängers
`dest_netmask`	Netzmaske des Empfängers
`dns`	0 = DNS-Anfragen der Absender-IP-Adresse dürfen keine Verbindung initiieren (default)
	1 = DNS-Anfragen der Absender-IP-Adresse dürfen eine Verbindung initiieren

[firewall lan]

`start_firewall`	0 = Firewall für LAN (ext)-Schnittstelle deaktiviert (default)
	1 = Firewall für LAN (ext)-Schnittstelle aktiviert
`start_firewall6`	0 = Firewall für IPv6-Dial-In-Verbindungen deaktiviert
	1 = Firewall für IPv6-Dial-In-Verbindungen aktiviert (default)
	(ab FW 2.10.0)
`list`	a = Neue Einträge werden an bestehende Liste angehängt
	d = Bestehende Liste wird gelöscht (default)
`new_entry`	Neue zugelassene Verbindung, die folgende Unterobjekte übergibt:
`protocol`	tcp = TCP-Protokoll wird verwendet
	udp = UDP-Protokoll wird verwendet
	icmp = ICMP-Protokoll wird verwendet
	icmpv6 = ICMPv6-Protokoll wird verwendet *(ab FW 2.12.0)*
	esp = ESP-Protokoll wird verwendet *(ab FW 2.12.0)*
	ah = AH-Protokoll wird verwendet *(ab FW 2.12.0)*
	gre = GRE-Protokoll wird verwendet *(ab FW 2.12.0)*
	all = Alle Protokolle sind zugelassen *(ab FW 2.12.0)*

`direction`	in = Nur eingehende Verbindungen sind zugelassen out = Nur ausgehende Verbindungen sind zugelassen both = Ein- und ausgehende Verbindungen sind zugelassen
`source_ip`	IP-Adresse des Absenders
`source_netmask`	Netzmaske des Absenders
`dest_port`	Port des Empfängers (oder Anfang des Portbereichs *(ab FW 2.6.0)*)
`dest_port_end`	Ende des Portbereichs des Empfängers *(ab FW 2.6.0)*
`dest_ip`	IP-Adresse des Empfängers
`dest_netmask`	Netzmaske des Empfängers
`ip_version`	ipv4 = Regel kann nur für IPv4-Verbindungen angelegt werden ipv6 = Regel kann nur für IPv6-Verbindungen angelegt werden all = Regel kann für IPv4-und IPv6-Verbindungen angelegt werden *(ab FW 2.12.0)*

[portforward lan]

start_portforwarding	0 = Port-Forwarding für LAN (ext)-Schnittstelle deaktiviert
	1 = Port-Forwarding für LAN (ext)-Schnittstelle aktiviert (default)
exposed_host	IP-Adresse des „Exposed Host“
list	a = Neue Einträge werden an bestehende Liste angehängt
	d = Bestehende Liste wird gelöscht (default)
new_entry	Neue zugelassene Verbindung, die folgende Unterobjekte übergibt:
protocol	tcp = TCP-Protokoll wird verwendet
	udp = UDP-Protokoll wird verwendet
	icmp = ICMP-Protokoll wird verwendet
	esp = ESP-Protokoll wird verwendet
	ah = AH-Protokoll wird verwendet *(ab FW 2.12.0)*
	gre = GRE-Protokoll wird verwendet *(ab FW 2.12.0)*
source_port_start	Beginn des Port-Bereichs für die Weiterleitung
source_port_end	Ende des Port-Bereichs für die Weiterleitung
dest_ip	IP-Adresse des Weiteleitungsziels
dest_port	Port des Weiteleitungsziels
apply	always = Regel gilt immer
	wan = Regel gilt für WAN-Verbindungen
	openvpn = Regel gilt für OpenVPN-Verbindungen
	(ab FW 2.12.6)

[openvpn server lan]

start_openvpn_server	0 = OpenVPN-Server für LAN (ext)-Schnittstelle deaktiviert (default)
	1 = OpenVPN-Server für LAN (ext)-Schnittstelle aktiviert
lport	Lokaler Port des Tunnels (default: 1194)
rport	Gegenstellen-Port des Tunnels (default: 1194)
protocol	udp = UDP-Protokoll wird verwendet
	tcp = TCP-Protokoll wird verwendet
push_server_route	0 = Server-Netz den Clients mitteilen deaktiviert
	1 = Server-Netz den Clients mitteilen aktiviert (default)
	(ab FW 2.6.0)
float	0 = Float (Gegenstelle darf IP-Adresse ändern) deaktiviert
	1 = Float (Gegenstelle darf IP-Adresse ändern) aktiviert (default)
comp_lzo	0 = LZO-Komprimierung deaktiviert
	1 = LZO-Komprimierung aktiviert (default)

`masquerade`	0 = Pakete vor Tunneln nicht maskieren	
	1 = Pakete vor Tunneln maskieren (default)	
`cipher`	BF-CBC =	Verschlüsselungsalgorithmus Blowfish 128 Bit (default)
	DES-CBC =	Verschlüsselungsalg. DES 64 Bit
	DES-EDE-CBC =	Verschlüsselungsalg. DES EDE 128 Bit
	DES-EDE3-CBC =	Verschlüsselungsalg. DES EDE3 192 Bit
	DESX-CBC =	Verschlüsselungsalg. DESX 192 Bit
	CAST5-CBC =	Verschlüsselungsalg. CAST5 128 Bit
	IDEA-CBC =	Verschlüsselungsalg. IDEA 128 Bit
	RC2-CBC =	Verschlüsselungsalg. RC2 128 Bit
	RC2-40-CBC =	Verschlüsselungsalg. RC2 40 Bit
	RC2-64-CBC =	Verschlüsselungsalg. RC2 64 Bit
	AES-128-CBC =	Verschlüsselungsalg. AES 128 Bit
	AES-192-CBC =	Verschlüsselungsalg. AES 192 Bit
	AES-256-CBC =	Verschlüsselungsalg. AES 256 Bit
	none =	Keine Verschlüsselung *(ab FW 2.8.0)*
`verb`	Ausführlichkeit der Meldungen im Verb.-Log (default: 3, 0-9)	
`fragment`	Maximale Größe der Tunnelpakete (in Bytes)	
`reneg`	Intervall für Schlüsselerneuerung (in Sekunden, default: 3600)	
`ping`	Intervall für Ping-Versand an Gegenstelle (in Sekunden, default: 30)	
`restart`	Intervall für Ping-Restart (in Sekunden, default: 60)	
`auth_type`	static = Keine Authentifizierung oder mit statischem Schlüssel	
	cert = Authentifizierung mit Zertifikaten	
`client_to_client`	0 = Kommunikation zwischen Clients nicht erlauben (default)	
	1 = Kommunikation zwischen Clients erlauben	
`pool_ip`	IP-Adressen-Pool für die Clients	
`pool_netmask`	Netzmaske des IP-Adressen-Pools	
`list`	a = Neue Einträge werden an bestehende Liste angehängt	
	d = Bestehende Liste wird gelöscht (default)	
`remote_peer`	IP-Adresse oder Domainname der Gegenstelle	
`remote_peer2`	IP-Adresse oder Domainname der alternativen Gegenstelle	
`local_vpn_ip`	IP-Adresse des VPN-Tunnels lokal	
`remote_vpn_ip`	IP-Adresse des VPN-Tunnels der Gegenstelle	
`remote_net`	Netzadresse des Netzwerks hinter dem VPN-Tunnel	

`remote_netmask`	Netzmaske des Netzwerks hinter dem VPN-Tunnel
`pool_ip6`	IPv6-Adressen-Pool für die Clients *(ab FW 2.10.0)*
`pool_netmask6`	Netzmaske des IPv6-Adressen-Pools *(ab FW 2.10.0)*
`local_vpn_ip6`	IPv6-Adresse des VPN-Tunnels lokal *(ab FW 2.10.0)*
`remote_vpn_ip6`	IPv6-Adresse des VPN-Tunnels der Gegenstelle *(ab FW 2.10.0)*
`remote_net6`	IPv6-Netzadresse des Netzwerks hinter dem VPN-Tunnel *(ab FW 2.10.0)*
`remote_netmask6`	IPv6-Netzmaske des Netzwerks hinter dem VPN-Tunnel *(ab FW 2.10.0)*
`tls_auth`	0 = Statischer Schlüssel wird nicht zusätzlich zur Authentifizierung mit Zertifikaten verwendet (default) 1 = Statischer Schlüssel wird zusätzlich zur Authentifizierung mit Zertifikaten verwendet *(ab FW 2.12.3)*
`key_direction`	none = Keine Benutzungsrichtung des Schlüssels vorgegeben (default) 0 = Benutzungsrichtung des Schlüssels ist „0“ 1 = Benutzungsrichtung des Schlüssels ist „1“ *(ab FW 2.12.3)*
`hash`	sha1 = Hash-Algorithmus SHA-1 (default) sha224 = Hash-Algorithmus SHA-224 sha256 = Hash-Algorithmus SHA-256 sha384 = Hash-Algorithmus SHA-384 sha512 = Hash-Algorithmus SHA-512 none = Kein Hash-Algorithmus verwendet *(ab FW 2.12.7)*
`new_entry`	Neuer Routeneintrag zu Client-Netzwerk, der folgende Unterobjekte übergibt:
`common_name`	„Common Name“ im Zertifikat des Clients
`net`	Netzwerkadresse des Clients
`netmask`	Netzmaske des Clients
`vpn_ip`	VPN-IP-Adresse des Clients
`dh_parameters`	Diffie-Hellman-Parametersatz
`crl`	Certificate Revocation List
`ca_certificate`	CA-Zertifikat
`public_certificate`	Öffentliches Zertifikat des Servers

`private_key`	Privater Schlüssel des Servers
`static_key`	Statischer Schlüssel

[openvpn client lan]

`start_openvpn_client`	0 = OpenVPN-Client für LAN (ext)-Schnittstelle deaktiviert (default)
	1 = OpenVPN-Client für LAN (ext)-Schnittstelle aktiviert
`remote_peer`	IP-Adresse oder Domainname der Gegenstelle
`remote_peer2`	IP-Adresse oder Domainname der alternativen Gegenstelle
`lport`	Lokaler Port des Tunnels (default: 1194)
`rport`	Gegenstellen-Port des Tunnels (default: 1194)
`protocol`	udp = UDP-Protokoll wird verwendet
	tcp = TCP-Protokoll wird verwendet
`defaultroute`	0 = Default-Route deaktiviert (default)
	1 = Default-Route aktiviert
	(ab FW 2.6.0)
`bind`	0 = Nobind (lokale Adresse und Port fixieren) deaktiviert
	1 = Nobind (lokale Adresse und Port fixieren) aktiviert (default)
`float`	0 = Float (Gegenstelle darf IP-Adresse ändern) deaktiviert
	1 = Float (Gegenstelle darf IP-Adresse ändern) aktiviert (default)
`comp_lzo`	0 = LZO-Komprimierung deaktiviert
	1 = LZO-Komprimierung aktiviert (default)
`masquerade`	0 = Pakete vor Tunneln nicht maskieren
	1 = Pakete vor Tunneln maskieren (default)

`cipher`	BF-CBC =	Verschlüsselungsalgorithmus Blowfish 128 Bit (default)
	DES-CBC =	Verschlüsselungsalg. DES 64 Bit
	DES-EDE-CBC =	Verschlüsselungsalg. DES EDE 128 Bit
	DES-EDE3-CBC =	Verschlüsselungsalg. DES EDE3 192 Bit
	DESX-CBC =	Verschlüsselungsalg. DESX 192 Bit
	CAST5-CBC =	Verschlüsselungsalg. CAST5 128 Bit
	IDEA-CBC =	Verschlüsselungsalg. IDEA 128 Bit
	RC2-CBC =	Verschlüsselungsalg. RC2 128 Bit
	RC2-40-CBC =	Verschlüsselungsalg. RC2 40 Bit
	RC2-64-CBC =	Verschlüsselungsalg. RC2 64 Bit
	AES-128-CBC =	Verschlüsselungsalg. AES 128 Bit
	AES-192-CBC =	Verschlüsselungsalg. AES 192 Bit
	AES-256-CBC =	Verschlüsselungsalg. AES 256 Bit
	none =	Keine Verschlüsselung *(ab FW 2.8.0)*
`verb`	Ausführlichkeit der Meldungen im Verb.-Log (default: 3, 0-9)	
`fragment`	Maximale Größe der Tunnelpakete (in Bytes)	
`reneg`	Intervall für Schlüsselerneuerung (in Sekunden, default: 3600)	
`ping`	Intervall für Ping-Versand an Gegenstelle (in Sekunden, default: 30)	
`restart`	Intervall für Ping-Restart (in Sekunden, default: 60)	
`icmp_ping`	IP-Adresse oder Domainname für zusätzlichen ICMP-Ping	
`auth_type`	static =	Keine Authentifizierung oder mit statischem Schlüssel
	cert =	Authentifizierung mit Zertifikaten
`username`	Benutzername des Clients für Anmeldung am OpenVPN-Server	
	Objektwert muss in Hochkommas übergeben werden!	
`password`	Kennwort des Clients für Anmeldung am OpenVPN-Server	
	Objektwert muss in Hochkommas übergeben werden!	
`check_server_cert`	0 =	Überprüfung des Zertifikatstyps der Gegenstelle deaktiviert (default)
	1 =	Überprüfung des Zertifikatstyps der Gegenstelle aktiviert
`local_vpn_ip`	IP-Adresse des VPN-Tunnels lokal	
`remote_vpn_ip`	IP-Adresse des VPN-Tunnels der Gegenstelle	
`remote_net`	Netzadresse des Netzwerks hinter dem VPN-Tunnel	
`remote_netmask`	Netzmaske des Netzwerks hinter dem VPN-Tunnel	

`local_vpn_ip6`	IPv6-Adresse des VPN-Tunnels lokal *(ab FW 2.10.0)*
`remote_vpn_ip6`	IPv6-Adresse des VPN-Tunnels der Gegenstelle *(ab FW 2.10.0)*
`remote_net6`	IPv6-Netzadresse des Netzwerks hinter dem VPN-Tunnel *(ab FW 2.10.0)*
`remote_netmask6`	IPv6-Netzmaske des Netzwerks hinter dem VPN-Tunnel *(ab FW 2.10.0)*
`proxy_name`	IP-Adresse oder Domainname des Proxy-Servers *(ab FW 2.11.0)*
`proxy_type`	http = HTTP-Proxy wird verwendet socks5 = SOCKS5-Proxy wird verwendet *(ab FW 2.11.0)*
`proxy_port`	Port des Proxy-Servers *(ab FW 2.11.0)*
`proxy_user`	Benutzername für den Proxy-Servers *(ab FW 2.11.0)* Objektwert muss in Hochkommas übergeben werden!
`proxy_password`	Passwort für den Proxy-Servers *(ab FW 2.11.0)* Objektwert muss in Hochkommas übergeben werden!
`tls_auth`	0 = Statischer Schlüssel wird nicht zusätzlich zur Authentifizierung mit Zertifikaten verwendet (default) 1 = Statischer Schlüssel wird zusätzlich zur Authentifizierung mit Zertifikaten verwendet *(ab FW 2.12.3)*
`key_direction`	none = Keine Benutzungsrichtung des Schlüssels vorgegeben (default) 0 = Benutzungsrichtung des Schlüssels ist „0“ 1 = Benutzungsrichtung des Schlüssels ist „1“ *(ab FW 2.12.3)*
`hash`	sha1 = Hash-Algorithmus SHA-1 (default) sha224 = Hash-Algorithmus SHA-224 sha256 = Hash-Algorithmus SHA-256 sha384 = Hash-Algorithmus SHA-384 sha512 = Hash-Algorithmus SHA-512 none = Kein Hash-Algorithmus verwendet *(ab FW 2.12.7)*
`ca_certificate`	CA-Zertifikat
`public_certificate`	Öffentliches Zertifikat des Clients
`private_key`	Privater Schlüssel des Clients
`static_key`	Statischer Schlüssel

[pptp server lan]	*ab FW 2.6.0*	
start_pptp_server	0 = PPTP-Server für LAN (ext)-Schnittstelle deaktiviert (default)	
	1 = PPTP-Server für LAN (ext)-Schnittstelle aktiviert	
authentication	none	Keine Authentifizierung
	pap	Authentifizierung über PAP
	chap	Authentifizierung über CHAP
	mschap	Authentifizierung über MS-CHAP
	mschap-v2	Authentifizierung über MS-CHAP-v2 (default)
encryption	none	Keine Verschlüsselung
	mppe-40	Verschlüsselung über MPPE-40
	mppe-128	Verschlüsselung über MPPE-128
mtu	MTU (Maximum Transmission Unit)	
mru	MRU (Maximum Receive Unit)	
local_ip	IPv4-Adresse des VPN-Tunnels lokal	
remote_vpn_ip_start	IP-Adressen-Pool für die Clients (Anfang des Adressbereichs)	
remote_vpn_ip_end	IP-Adressen-Pool für die Clients (Ende des Adressbereichs)	
list	a = Neue Einträge werden an bestehende Liste angehängt	
	d = Bestehende Liste wird gelöscht (default)	
new_entry	Neuer Benutzereintrag, der folgende Unterobjekte übergibt:	
username	Benutzername des Benutzers	
password	Kennwort des Benutzers	
[pptp client lan]	*ab FW 2.6.0*	
start_pptp_client	0 = PPTP-Client für LAN (ext)-Schnittstelle deaktiviert (default)	
	1 = PPTP-Client für LAN (ext)-Schnittstelle aktiviert	
remote_peer	IP-Adresse oder Domainname der Gegenstelle	
username	Benutzername des Clients für Anmeldung am PPTP-Server	
	Objektwert muss in Hochkommas übergeben werden!	
password	Kennwort des Clients für Anmeldung am PPTP-Server	
	Objektwert muss in Hochkommas übergeben werden!	
encryption	none	Keine Verschlüsselung
	mppe-40	Verschlüsselung über MPPE-40
	mppe-128	Verschlüsselung über MPPE-128
defaultroute	0 = Default-Route deaktiviert (default)	
	1 = Default-Route aktiviert	

`remote_net`	Lokales Subnetz der Gegenstelle
`remote_netmask`	Netzmaske des lokalen Subnetzes der Gegenstelle
`mtu`	MTU (Maximum Transmission Unit)
`mru`	MRU (Maximum Receive Unit)
`icmp_ping`	IP-Adresse oder Domainname für zusätzlichen ICMP-Ping

[ipsec lan]	*FW 2.4.0*
start_ipsec	0 = IPsec für LAN (ext)-Schnittstelle deaktiviert (default)
	1 = IPsec für LAN (ext)-Schnittstelle aktiviert
remote_peer	IP-Adresse oder Domainname der Gegenstelle
remote_net	Lokales Subnetz der Gegenstelle
remote_netmask	Netzmaske des lokalen Subnetzes der Gegenstelle
remote_id	ID der Gegenstelle
	Objektwert muss in Hochkommas übergeben werden!
local_id	Eigene ID
	Objektwert muss in Hochkommas übergeben werden!
auth_mode	main = Authentifizierungsmodus Main wird verwendet (default)
	aggressive = Authentifizierungsmodus Aggressive wird verwendet
ike_cipher	3des = IKE-Verschlüsselungsalgorithmus DES EDE3 (default)
	aes128 = IKE-Verschlüsselungsalgorithmus AES 128 Bit
	aes192 = IKE-Verschlüsselungsalgorithmus AES 192 Bit
	aes256 = IKE-Verschlüsselungsalgorithmus AES 256 Bit
ike_hash	sha1 = IKE-Hash-Algorithmus SHA1 (default)
	md5 = IKE-Hash-Algorithmus MD5
ike_dh	modp768 = Diffie-Hellman-Gruppe für IKE ist DH 768
	modp1024 = Diffie-Hellman-Gruppe für IKE ist DH 1024 (default)
	modp1536 = Diffie-Hellman-Gruppe für IKE ist DH 1536
ipsec_cipher	3des = IPsec-Verschlüsselungsalg. DES EDE3 (default)
	aes128 = IPsec-Verschlüsselungsalg. AES 128 Bit
	aes192 = IPsec-Verschlüsselungsalg. AES 192 Bit
	aes256 = IPsec-Verschlüsselungsalg. AES 256 Bit
ipsec_hash	sha1 = IPsec-Hash-Algorithmus SHA1 (default)
	md5 = IPsec-Hash-Algorithmus MD5
key_attempts	Maximale Verbindungsversuche (0 = unendlich)
nat_traversal	on = NAT-Traversal ist aktiviert (default)
	off = NAT-Traversal ist deaktiviert
	forced = NAT-Traversal wird erzwungen
keep_alive	Intervall der Keep-Alive-Pakete (in Sekunden, default: 10)
pfs	0 = Perfect-Forward-Secrecy ist deaktiviert
	1 = Perfect-Forward-Secrecy ist aktiviert (default)
dpd_interval	Intervall für Dead-Peer-Detection (in Sekunden, default: 30)

`dpd_timeout`	Timeout für Dead-Peer-Detection (in Sekunden, default: 120)
`dpd_action`	clear = Abbauen der Verbindung bei Dead-Peer-Detection
	hold = Halten der Verbindung bei Dead-Peer-Detection
	restart = Neu starten der Verbindung bei Dead-Peer-Detection (default)
`key_lifetime`	Intervall für Schlüsselerneuerung (in Sekunden, default: 3600)
`icmp_ping`	IP-Adresse oder Domainname für zusätzlichen ICMP-Ping
`auth_type`	cert = Authentifizierung mit Zertifikaten
	psk = Authentifizierung mit Passphrase (PSK)
`psk`	Passphrase (PSK)
	Objektwert muss in Hochkommas übergeben werden!
`masquerade`	0 = Pakete durch den Tunnel nicht maskieren
	1 = Pakete durch den Tunnel maskieren (default)
`ca_certificate`	CA-Zertifikat
`public_certificate`	Öffentliches Zertifikat
`private_key`	Privater Schlüssel

[ipsec lan]	*ab FW 2.5.0; <x> = 1-10*
start_ipsec	0 = IPsec für LAN (ext)-Schnittstelle deaktiviert (default)
	1 = IPsec für LAN (ext)-Schnittstelle aktiviert
nat_traversal	on = NAT-Traversal ist aktiviert (default)
	off = NAT-Traversal ist deaktiviert
	forced = NAT-Traversal wird erzwungen
keep_alive	Intervall der Keep-Alive-Pakete (in Sekunden, default: 10)
start_tunnel<x>	0 = IPsec-Tunnel <x> deaktiviert (default)
	1 = IPsec-Tunnel <x> aktiviert
	10<X> = Fallback für Tunnel <X> *(ab FW 2.12.0)*
tunnel_name<x>	Name für IPsec-Tunnel <x>
remote_peer<x>	IP-Adresse oder Domainname der Gegenstelle
local_net<x>	Eigenes Subnetz
local_netmask<x>	Netzmaske des eigenen Subnetzes
remote_net<x>	Lokales Subnetz der Gegenstelle
remote_netmask<x>	Netzmaske des lokalen Subnetzes der Gegenstelle
remote_id<x>	ID der Gegenstelle
	Objektwert muss in Hochkommas übergeben werden!
local_id<x>	Eigene ID
	Objektwert muss in Hochkommas übergeben werden!
auth_mode<x>	main = Authentifizierungsmodus Main wird verwendet (default)
	aggressive = Authentifizierungsmodus Aggressive wird verwendet
ike_cipher<x>	3des = IKE-Verschlüsselungsalgorithmus DES EDE3 (default)
	aes128 = IKE-Verschlüsselungsalgorithmus AES 128 Bit
	aes192 = IKE-Verschlüsselungsalgorithmus AES 192 Bit
	aes256 = IKE-Verschlüsselungsalgorithmus AES 256 Bit
ike_hash<x>	sha1 = IKE-Hash-Algorithmus SHA1 (default)
	md5 = IKE-Hash-Algorithmus MD5
ike_dh<x>	modp768 = Diffie-Hellman-Gruppe für IKE ist DH 768
	modp1024 = Diffie-Hellman-Gruppe für IKE ist DH 1024 (default)
	modp1536 = Diffie-Hellman-Gruppe für IKE ist DH 1536
ipsec_cipher<x>	3des = IPsec-Verschlüsselungsalg. DES EDE3 (default)
	aes128 = IPsec-Verschlüsselungsalg. AES 128 Bit
	aes192 = IPsec-Verschlüsselungsalg. AES 192 Bit
	aes256 = IPsec-Verschlüsselungsalg. AES 256 Bit

ipsec_hash<x>	sha1 = IPsec-Hash-Algorithmus SHA1 (default) md5 = IPsec-Hash-Algorithmus MD5
key_attempts<x>	Maximale Verbindungsversuche (0 = unendlich)
masquerade<x>	0 = Pakete durch den Tunnel nicht maskieren 1 = Pakete durch den Tunnel maskieren (default)
dpd_interval<x>	Intervall für Dead-Peer-Detection (in Sekunden, default: 30)
dpd_timeout<x>	Timeout für Dead-Peer-Detection (in Sekunden, default: 120)
dpd_action<x>	clear = Abbauen der Verbindung bei Dead-Peer-Detection hold = Halten der Verbindung bei Dead-Peer-Detection restart = Neu starten der Verbindung bei Dead-Peer-Detection (default)
pfs<x>	0 = Perfect-Forward-Secrecy ist deaktiviert 1 = Perfect-Forward-Secrecy ist aktiviert (default)
key_lifetime<x>	Intervall für Schlüsselerneuerung (in Sekunden, default: 3600) *(bis FW 2.12.3)*
icmp_ping<x>	IP-Adresse oder Domainname für zusätzlichen ICMP-Ping
auth_type<x>	cert = Authentifizierung mit Zertifikaten psk = Authentifizierung mit Passphrase (PSK)
psk<x>	Passphrase (PSK) Objektwert muss in Hochkommas übergeben werden!
ca_certificate<x>	CA-Zertifikat
public_certificate<x>	Öffentliches Zertifikat
private_key<x>	Privater Schlüssel
ipsec_lifetime<x>	Intervall für IPsec SA Schlüsselerneuerung (in Sekunden, default: 3600) *(ab FW 2.12.3)*
ike_lifetime<x>	Intervall für IKE SA Schlüsselerneuerung (in Sekunden, default: 86400) *(ab FW 2.12.3)*
local_protocol<x>	Zugelassenes Protokoll am lokalen Ende des Tunnels (IANA-Nummer) *(ab FW 2.12.3)*
local_port<x>	Zugelassener Port am lokalen Ende des Tunnels *(ab FW 2.12.3)*
remote_protocol<x>	Zugelassenes Protokoll am Gegenstellen-Ende des Tunnels (IANA-Nummer) *(ab FW 2.12.3)*

`remote_port<x>`	Zugelassener Port am Gegenstellen-Ende des Tunnels *(ab FW 2.12.3)*
[ipforward]	*ab FW 2.11.0*
`start_ipforward`	0 = IP-Forwarding für LAN (ext)-Schnittstelle deaktiviert (default) 1 = IP-Forwarding für LAN (ext)-Schnittstelle aktiviert
`list`	a = Neue Einträge werden an bestehende Liste angehängt d = Bestehende Liste wird gelöscht (default)
`new_entry`	Neue zugelassene Verbindung, die folgende Unterobjekte übergibt:
`source_ip`	Quell-IP-Adresse für die Weiterleitung
`source_netmask`	Netzmaske der Quell-IP-Adresse für die Weiterleitung
`dest_ip`	IP-Adresse des Weiteleitungsziels
[gre lan]	*ab FW 2.11.0*
`start_gre_tunnel`	0 = GRE-Tunnel für Lan (ext)-Verbindungen deaktiviert (default) 1 = GRE-Tunnel für Lan (ext)-Verbindungen aktiviert
`remote_ip`	IP-Adresse oder Domainname der Gegenstelle
`local_ip`	Eigene IP-Adresse
`tunnel_ip`	Lokale Tunnel-IP-Adresse
`tunnel_netmask`	Optionale Netzmaske der lokalen Tunnel-IP-Adresse
`mtu`	MTU (Maximum Transmission Unit)
`ttl`	TTL (Time to Live, default: 0)
`list`	a = Neue Einträge werden an bestehende Liste angehängt d = Bestehende Liste wird gelöscht (default)
`new_entry`	Neuer Routeneintrag, der folgende Unterobjekte übergibt:
`net`	Netzwerkadresse der Route
`netmask`	Netzmaske der Route
`gateway`	Gateway der Route
[inputs]	*nur bei Geräten mit Ein-/Ausgängen*
`in2`	off = Eingang 2 hat keine Funktion (default) dialout = Dial-Out-Verbindung mit Eingang 2 aufbauen openvpn = OpenVPN-Tunnel mit Eingang 2 aufbauen ipsec = IPsec-Tunnel mit Eingang 2 aufbauen serial = Ausgehende Seriell-Ethernet-Verbindung mit Eingang 2 aufbauen

`in2_dial_exclusive`	0 = Dial-Out-Verbindung nicht exklusiv aufbauen (default)
	1 = Dial-Out-Verbindung exklusiv aufbauen
`in2_dial_stop`	0 = Dial-Out-Verbindung nicht abbauen wenn Eingang wieder offen (default)
	1 = Dial-Out-Verbindung abbauen wenn Eingang wieder offen
`in2_openvpn_exclusive`	0 = OpenVPN-Tunnel nicht exklusiv aufbauen (default)
	1 = OpenVPN-Tunnel exklusiv über Eingang aufbauen
`in2_openvpn_stop`	0 = OpenVPN-Tunnel nicht abbauen wenn Eingang wieder offen (default)
	1 = OpenVPN-Tunnel abbauen wenn Eingang wieder offen
`in2_pptpn_exclusive`	0 = PPTP-Tunnel nicht exklusiv aufbauen (default)
	1 = PPTP-Tunnel exklusiv über Eingang aufbauen
`in2_pptp_stop`	0 = PPTP-Tunnel nicht abbauen wenn Eingang wieder offen (default)
	1 = PPTP-Tunnel abbauen wenn Eingang wieder offen
`in2_ipsec_exclusive`	0 = IPsec-Tunnel nicht exklusiv aufbauen (default)
	1 = IPsec-Tunnel exklusiv über Eingang aufbauen
`in2_ipsec_stop`	0 = IPsec-Tunnel nicht abbauen wenn Eingang wieder offen (default)
	1 = IPsec-Tunnel abbauen wenn Eingang wieder offen
`in2_serial_stop`	0 = Seriell-Ethernet-Verbindung nicht abbauen wenn Eingang wieder offen (default)
	1 = Seriell-Ethernet-Verbindung abbauen wenn Eingang wieder offen

[outputs]	*nur bei Geräten mit Ein-/Ausgängen*
out1_set	idle = Ausgang 1 in Ruhestellung (default)
	operated = Ausgang 1 in Arbeitsstellung
out2_set	idle = Ausgang 2 in Ruhestellung (default)
	operated = Ausgang 2 in Arbeitsstellung
out1_daily_operated	0 = Ausgang 1 nicht täglich in Arbeitsstellung schalten (default)
	1 = Ausgang 1 täglich in Arbeitsstellung schalten
out1_daily_operated_hour	Ausgang 1 täglich in Arbeitsst. schalten um (Stunde, 00-23)
out1_daily_operated_min	Ausgang 1 täglich in Arbeitsst. schalten um (Minute, 00-59)
out1_daily_idle	0 = Ausgang 1 nicht täglich in Ruhestellung schalten (default)
	1 = Ausgang 1 täglich in Ruhestellung schalten
out1_daily_idle_hour	Ausgang 1 täglich in Ruhest. schalten um (Stunde, 00-23)
out1_daily_idle_min	Ausgang 1 täglich in Ruhest. schalten um (Minute, 00-59)
out2_daily_operated	0 = Ausgang 2 nicht täglich in Arbeitsstellung schalten (default)
	1 = Ausgang 2 täglich in Arbeitsstellung schalten
out2_daily_operated_hour	Ausgang 2 täglich in Arbeitsst. schalten um (Stunde, 00-23)
out2_daily_operated_min	Ausgang 2 täglich in Arbeitsst. schalten um (Minute, 00-59)
out2_daily_idle	0 = Ausgang 2 nicht täglich in Ruhestellung schalten (default)
	1 = Ausgang 2 täglich in Ruhestellung schalten
out2_daily_idle_hour	Ausgang 2 täglich in Ruhest. schalten um (Stunde, 00-23)
out2_daily_idle_min	Ausgang 2 täglich in Ruhest. schalten um (Minute, 00-59)
out1	off = Ausgang 1 hat keine automatische Funktion (default)
	ppp = Ausgang 1 schaltet auf Arbeitsstellung wenn eine PPP-Verbindung besteht
out2	off = Ausgang 2 hat keine automatische Funktion (default)
	openvpn = Ausgang 2 schaltet auf Arbeitsstellung wenn ein OpenVPN-Tunnel besteht
	pptp = Ausgang 2 schaltet auf Arbeitsstellung wenn ein PPTP-Tunnel besteht *(ab FW 2.10.0)*
	ipsec = Ausgang 2 schaltet auf Arbeitsstellung wenn ein IPsec-Tunnel besteht
	serial2 = Ausgang 2 schaltet auf Arbeitsstellung wenn eine Seriell-Ethernet-Verbindung besteht

[switch port]	*nur bei MoRoS und MLR*
active1	0 = Switch-Port 1 deaktiviert
	1 = Switch-Port 1 aktiviert (default)
active2	0 = Switch-Port 2 deaktiviert
	1 = Switch-Port 2 aktiviert (default)
active3	0 = Switch-Port 3 deaktiviert
	1 = Switch-Port 3 aktiviert (default)
active4	0 = Switch-Port 4 deaktiviert
	1 = Switch-Port 4 aktiviert (default)
autoneg1	0 = Auto-Negotiation für Switch-Port 1 deaktiviert
	1 = Auto-Negotiation für Switch-Port 1 aktiviert (default)
autoneg2	0 = Auto-Negotiation für Switch-Port 2 deaktiviert
	1 = Auto-Negotiation für Switch-Port 2 aktiviert (default)
autoneg3	0 = Auto-Negotiation für Switch-Port 3 deaktiviert
	1 = Auto-Negotiation für Switch-Port 3 aktiviert (default)
autoneg4	0 = Auto-Negotiation für Switch-Port 4 deaktiviert
	1 = Auto-Negotiation für Switch-Port 4 aktiviert (default)
speed1	10 = Fixe Geschwindigkeit von Switch-Port 1 ist 10 MBit/s
	100 = Fixe Geschwindigkeit von Switch-Port 1 ist 100 MBit/s
speed2	10 = Fixe Geschwindigkeit von Switch-Port 2 ist 10 MBit/s
	100 = Fixe Geschwindigkeit von Switch-Port 2 ist 100 MBit/s
speed3	10 = Fixe Geschwindigkeit von Switch-Port 3 ist 10 MBit/s
	100 = Fixe Geschwindigkeit von Switch-Port 3 ist 100 MBit/s
speed4	10 = Fixe Geschwindigkeit von Switch-Port 4 ist 10 MBit/s
	100 = Fixe Geschwindigkeit von Switch-Port 4 ist 100 MBit/s
duplex1	half = Protokoll von Switch-Port 1 ist Half-Duplex
	full = Protokoll von Switch-Port 1 ist Full-Duplex
duplex2	half = Protokoll von Switch-Port 2 ist Half-Duplex
	full = Protokoll von Switch-Port 2 ist Full-Duplex
duplex3	half = Protokoll von Switch-Port 3 ist Half-Duplex
	full = Protokoll von Switch-Port 3 ist Full-Duplex
duplex4	half = Protokoll von Switch-Port 4 ist Half-Duplex
	full = Protokoll von Switch-Port 4 ist Full-Duplex

[switch led]	*nur bei MoRoS und MLR*	
`led_green`	100 =	Grüne LED zeigt Geschwindigkeit 100 MBit/s an (default)
	link =	Grüne LED zeigt Verbindung (Link) an
	full =	Grüne LED zeigt Full-Duplex-Protokoll an
	collision =	Grüne LED zeigt Kollision an
	rxtx =	Grüne LED zeigt RX/TX-Aktivität an
	duplex_collision =	Grüne LED zeigt Full-Duplex / Kollision an
	link_activity =	Grüne LED zeigt Verbindung / Aktivität an
`led_red`	100 =	Rote LED zeigt Geschwindigkeit 100 MBit/s an (default)
	link =	Rote LED zeigt Verbindung (Link) an
	full =	Rote LED zeigt Full-Duplex-Protokoll an
	collision =	Rote LED zeigt Kollision an
	rxtx =	Rote LED zeigt RX/TX-Aktivität an
	duplex_collision =	Rote LED zeigt Full-Duplex / Kollision an
	link_activity =	Rote LED zeigt Verbindung / Aktivität an

[switch vlan]	*nur bei MoRoS und MLR*
`start_vlan`	0 = VLAN-Konfiguration deaktiviert (default)
	1 = VLAN-Konfiguration aktiviert
`vlana_port1`	0 = Port 1 gehört nicht zu VLAN A (default)
	1 = Port 1 gehört zu VLAN A
`vlana_port2`	0 = Port 2 gehört nicht zu VLAN A (default)
	1 = Port 2 gehört zu VLAN A
`vlana_port3`	0 = Port 3 gehört nicht zu VLAN A (default)
	1 = Port 3 gehört zu VLAN A
`vlana_port4`	0 = Port 4 gehört nicht zu VLAN A (default)
	1 = Port 4 gehört zu VLAN A
`vlana_port5`	0 = Router gehört nicht zu VLAN A (default)
	1 = Router gehört zu VLAN A
`vlanb_port1`	0 = Port 1 gehört nicht zu VLAN B (default)
	1 = Port 1 gehört zu VLAN B
`vlanb_port2`	0 = Port 2 gehört nicht zu VLAN B (default)
	1 = Port 2 gehört zu VLAN B

`vlanb_port3`	0 = Port 3 gehört nicht zu VLAN B (default)
	1 = Port 3 gehört zu VLAN B
`vlanb_port4`	0 = Port 4 gehört nicht zu VLAN B (default)
	1 = Port 4 gehört zu VLAN B
`vlanb_port5`	0 = Router gehört nicht zu VLAN B (default)
	1 = Router gehört zu VLAN B
`vlanc_port1`	0 = Port 1 gehört nicht zu VLAN C (default)
	1 = Port 1 gehört zu VLAN C
`vlanc_port2`	0 = Port 2 gehört nicht zu VLAN C (default)
	1 = Port 2 gehört zu VLAN C
`vlanc_port3`	0 = Port 3 gehört nicht zu VLAN C (default)
	1 = Port 3 gehört zu VLAN C
`vlanc_port4`	0 = Port 4 gehört nicht zu VLAN C (default)
	1 = Port 4 gehört zu VLAN C
`vlanc_port5`	0 = Router gehört nicht zu VLAN C (default)
	1 = Router gehört zu VLAN C
`vland_port1`	0 = Port 1 gehört nicht zu VLAN D (default)
	1 = Port 1 gehört zu VLAN D
`vland_port2`	0 = Port 2 gehört nicht zu VLAN D (default)
	1 = Port 2 gehört zu VLAN D
`vland_port3`	0 = Port 3 gehört nicht zu VLAN D (default)
	1 = Port 3 gehört zu VLAN D
`vland_port4`	0 = Port 4 gehört nicht zu VLAN D (default)
	1 = Port 4 gehört zu VLAN D
`vland_port5`	0 = Router gehört nicht zu VLAN D (default)
	1 = Router gehört zu VLAN D
`vlan_ida`	VLAN-ID des VLAN A
`vlan_idb`	VLAN-ID des VLAN B
`vlan_idc`	VLAN-ID des VLAN C
`vlan_idd`	VLAN-ID des VLAN D
`port1_tag`	insert = VLAN-Tag für Port 1 einfügen
	remove = VLAN-Tag für Port 1 entfernen (default)
`port2_tag`	insert = VLAN-Tag für Port 2 einfügen
	remove = VLAN-Tag für Port 2 entfernen (default)
`port3_tag`	insert = VLAN-Tag für Port 3 einfügen
	remove = VLAN-Tag für Port 3 entfernen (default)
`port4_tag`	insert = VLAN-Tag für Port 4 einfügen
	remove = VLAN-Tag für Port 4 entfernen (default)

[switch mirror]	*nur bei MoRoS und MLR*
sniffer_port	off = Sniffer-Port deaktiviert (default)
	1 = Port 1 ist Sniffer-Port
	2 = Port 2 ist Sniffer-Port
	3 = Port 3 ist Sniffer-Port
	4 = Port 4 ist Sniffer-Port
tx_port	off = TX spiegeln an Sniffer-Port deaktiviert (default)
	1 = Port 1 sendet Sendedaten an Sniffer-Port
	2 = Port 2 sendet Sendedaten an Sniffer-Port
	3 = Port 3 sendet Sendedaten an Sniffer-Port
	4 = Port 4 sendet Sendedaten an Sniffer-Port
rx_port	off = RX spiegeln an Sniffer-Port deaktiviert (default)
	1 = Port 1 sendet Empfangsdaten an Sniffer-Port
	2 = Port 2 sendet Empfangsdaten an Sniffer-Port
	3 = Port 3 sendet Empfangsdaten an Sniffer-Port
	4 = Port 4 sendet Empfangsdaten an Sniffer-Port
[serial ethernet basic]	*nicht bei EBW*
start_serial	0 = Seriell-Ethernet-Gateway für RS232 deaktiviert (default)
	1 = Seriell-Ethernet-Gateway für RS232 aktiviert
connection_mode	demand = Verbindung auf Anforderung aktiviert (default)
	flat = Standleitungsmodus aktiviert
increase_interval	0 = Wartezeit zwischen Verbindungsversuchen nicht erhöhen (default)
	1 = Wartezeit zwischen Verbindungsversuchen erhöhen
ipt	0 = IPT nicht verwenden (default)
	1 = IPT verwenden
	(ab FW 2.5.0)
incoming	0 = Eingehende Verbindung nicht annehmen
	1 = Eingehende Verbindung annehmen (default)
	(bis FW 2.12.2)
incoming	off = Eingehende Verbindungen nicht annehmen
	tcp = Eingehende TCP-Verbindung annehmen (default)
	modbus = Eingehende Modbus TCP-Verbindungen annehmen
	(ab FW 2.12.3)
listen_port	Port, der auf eingehende Verbindungen überwacht wird

`outgoing`	off = Ausgehende Verbindung nicht aktiviert (default) atd = Ausgehende Verbindung ausgelöst durch Wählbefehl ATD char = Ausgehende Verbindung ausgelöst durch serielles Zeichen wan = Ausgehende Verbindung ausgelöst durch WAN-Verbindung
`outgoing_server`	IP-Adresse oder Domain-Name des primären Ziels
`outgoing_port`	Port des primären Ziels
`outgoing_ipt`	IPT-Rufnummer des primären Ziels
`outgoing_server2`	IP-Adresse oder Domain-Name des sekundären Ziels
`outgoing_port2`	Port des sekundären Ziels
`outgoing_ipt2`	IPT-Rufnummer des sekundären Ziels
`auth_incoming`	off = Keine VCom-Authentifizierung für eingehende Verbindungen (default) udp = VCom-Authentifizierung über UDP für eingehende Verbindungen tcp = VCom-Authentifizierung über TCP für eingehende Verbindungen
`auth_outgoing`	off = Keine VCom-Authentifizierung für ausgehende Verbindungen (default) udp = VCom-Authentifizierung über UDP für ausgehende Verbindungen tcp = VCom-Authentifizierung über TCP für ausgehende Verbindungen
`local_exclusive`	0 = Eingehende Verbindungen nicht beschränken (default) 1 = Eingehende Verbindungen auf lokales Netzwerk beschränken *(ab FW 2.12.9)*

[serial ethernet interfaces]	*nicht bei EBW*
speed	Geschwindigkeit der seriellen RS232-Schnittstelle (110, 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Bit/s; default: 115200)
databits	Datenbits auf der seriellen Schnittstelle (7, 8; default: 8)
parity	Parität der seriellen Schnittstelle (O, E, N; default: N)
stopbits	Stoppbits auf der seriellen Schnittstelle (1, 2; default: 1)
flowctrl	hard = Hardware-Datenflusskontrolle aktiviert (default)
	soft = Software-Datenflusskontrolle aktiviert
	none = Keine Datenflusskontrolle aktiviert
ctl	0 = Steuerleitungen nicht benutzen
	1 = Steuerleitungen benutzen (default)
	(nur MoRoS und MLR)
reset_ctl	0 = Steuerleitungen nach Verbindungsende nicht zurücksetzen
	1 = Steuerleitungen nach Verbindungsende zurücksetzen (default)
	(nur MoRoS und MLR)
blocksize	Maximale TCP-Blockgröße (in Bytes, default: 512)
aggregationtime	Aggregation-Timeout (in Millisekunden, default: 100)
idletime	Maximale Leerlaufzeit (in Sekunden, default: 20, 0 = unbegrenzt)
keepalive_interval	Intervall der Keep-Alive-Pakete (in Sekunden, default: 0)
telnet	0 = Telnet-Protokoll wird nicht verwendet
	1 = Telnet-Protokoll wird verwendet (default)
serial_device	1 = Schnittstelle „Serial 1“ (RS232) wird verwendet
	2 = Schnittstelle „Serial 2“ (Logo/RS485) wird verwendet
	(nur IMON mit FW 2.11.x)
dtr_on_connect	0 = DTR wird bei Verbindung nicht gesetzt (default)
	1 = DTR-Leitung wird bei Verbindung nicht gesetzt
	(ab FW 2.12.7)
maxtime	Maximale *Verbindungszeit* (in Sekunden, default: 0)
	(ab FW 2.12.7)
[serial ethernet modem]	*nicht bei EBW*
modem_emulation	0 = Modem-Emulator für RS232 deaktiviert
	1 = Modem-Emulator für RS232 aktiviert (default)
ate	0 = Echo (ATE) deaktiviert
	1 = Echo (ATE) aktiviert (default)
atq	0 = Rückmeldungen (ATQ) deaktiviert (default)
	1 = Rückmeldungen (ATQ) aktiviert

`atv`	0 = Ausführliche Rückmeldungen (ATV) deaktiviert
	1 = Ausführliche Rückmeldungen (ATV) aktiviert (default)
`ats0`	Anzahl an Klingelzeichen bis zur Rufannahme (default: 1)
`default_at_answer`	Standardantwort bei unbekannten Kommandos
	Objektwert muss in Hochkommas übergeben werden!
`hangup_on_atz`	0 = Verbindung bei ATZ nicht beenden (default)
	1 = Verbindung bei ATZ beenden
	(ab FW 2.12.6)
`connect_message`	Meldung bei Verbindungsaufbau (default: CONNECT)
	(ab FW 2.12.9)
`at_answer_list`	AT-Antwortliste
`[ serial ethernet 2 basic ]`	*nur IMON*
`start_serial`	0 = Seriell-Ethernet-Gateway für Logo/RS485 deaktiviert (default)
	1 = Seriell-Ethernet-Gateway für Logo/RS485 aktiviert
`connection_mode`	demand = Verbindung auf Anforderung aktiviert (default)
	flat = Standleitungsmodus aktiviert
`increase_interval`	0 = Wartezeit zwischen Verbindungsversuchen nicht erhöhen (default)
	1 = Wartezeit zwischen Verbindungsversuchen erhöhen
`ipt`	0 = IPT nicht verwenden (default)
	1 = IPT verwenden
`incoming`	0 = Eingehende Verbindung nicht annehmen
	1 = Eingehende Verbindung annehmen (default)
	(bis FW 2.12.2)
`incoming`	off = Eingehende Verbindungen nicht annehmen
	tcp = Eingehende TCP-Verbindung annehmen (default)
	modbus = Eingehende Modbus TCP-Verbindungen annehmen
	(ab FW 2.12.3)
`listen_port`	Port, der auf eingehende Verbindungen überwacht wird
`outgoing`	off = Ausgehende Verbindung nicht aktiviert (default)
	atd = Ausgehende Verbindung ausgelöst durch Wählbefehl ATD
	char = Ausgehende Verbindung ausgelöst durch serielles Zeichen
	wan = Ausgehende Verbindung ausgelöst durch WAN-Verbindung
`outgoing_server`	IP-Adresse oder Domain-Name des primären Ziels
`outgoing_port`	Port des primären Ziels

`outgoing_ipt`	IPT-Rufnummer des primären Ziels
`outgoing_server2`	IP-Adresse oder Domain-Name des sekundären Ziels
`outgoing_port2`	Port des sekundären Ziels
`outgoing_ipt2`	IPT-Rufnummer des sekundären Ziels
`auth_incoming`	off = Keine VCom-Authentifizierung für eingehende Verbindungen (default) udp = VCom-Authentifizierung über UDP für eingehende Verbindungen tcp = VCom-Authentifizierung über TCP für eingehende Verbindungen
`auth_outgoing`	off = Keine VCom-Authentifizierung für ausgehende Verbindungen (default) udp = VCom-Authentifizierung über UDP für ausgehende Verbindungen tcp = VCom-Authentifizierung über TCP für ausgehende Verbindungen
`local_exclusive`	0 = Eingehende Verbindungen nicht beschränken (default) 1 = Eingehende Verbindungen auf lokales Netzwerk beschränken *(ab FW 2.12.9)*
`[ serial ethernet 2 interfaces ]`	*nur IMON*
`speed`	Geschwindigkeit der seriellen Logo/RS485-Schnittstelle (110, 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Bit/s; default: 115200)
`databits`	Datenbits auf der seriellen Schnittstelle (7, 8; default: 8)
`parity`	Parität der seriellen Schnittstelle (O, E, N; default: N)
`stopbits`	Stoppbits auf der seriellen Schnittstelle (1, 2; default: 1)
`flowctrl`	soft = Software-Datenflusskontrolle aktiviert (default) none = Keine Datenflusskontrolle aktiviert
`blocksize`	Maximale TCP-Blockgröße (in Bytes, default: 512)
`aggregationtime`	Aggregation-Timeout (in Millisekunden, default: 100)
`idletime`	Maximale Leerlaufzeit (in Sekunden, default: 20, 0 = unbegrenzt)
`keepalive_interval`	Intervall der Keep-Alive-Pakete (in Sekunden, default: 0)
`telnet`	0 = Telnet-Protokoll wird nicht verwendet 1 = Telnet-Protokoll wird verwendet (default)
`dtr_on_connect`	0 = DTR wird bei Verbindung nicht gesetzt (default) 1 = DTR-Leitung wird bei Verbindung nicht gesetzt *(ab FW 2.12.7)*
`maxtime`	Maximale *Verbindungszeit* (in Sekunden, default: 0) *(ab FW 2.12.7)*

[serial ethernet 2 modem]	*nur IMON*
modem_emulation	0 = Modem-Emulator für Logo/RS485 deaktiviert
	1 = Modem-Emulator für Logo/RS485 aktiviert (default)
ate	0 = Echo (ATE) deaktiviert
	1 = Echo (ATE) aktiviert (default)
atq	0 = Rückmeldungen (ATQ) deaktiviert (default)
	1 = Rückmeldungen (ATQ) aktiviert
atv	0 = Ausführliche Rückmeldungen (ATV) deaktiviert
	1 = Ausführliche Rückmeldungen (ATV) aktiviert (default)
ats0	Anzahl an Klingelzeichen bis zur Rufannahme (default: 1)
default_at_answer	Standardantwort bei unbekannten Kommandos
	Objektwert muss in Hochkommas übergeben werden!
hangup_on_atz	0 = Verbindung bei ATZ nicht beenden (default)
	1 = Verbindung bei ATZ beenden
	(ab FW 2.12.6)
connect_message	Meldung bei Verbindungsaufbau (default: CONNECT)
	(ab FW 2.12.9)
at_answer_list	AT-Antwortliste

[message]

email_address	E-Mail-Adresse des E-Mail-Accounts
real_name	Name des Inhabers des E-Mail-Accounts
	Objektwert muss in Hochkommas übergeben werden!
server	SMTP-Server-Adresse
port	SMTP-Port (default: 25)
username	Benutzername des E-Mail-Accounts
	Objektwert muss in Hochkommas übergeben werden!
password	Kennwort des E-Mail-Accounts
	Objektwert muss in Hochkommas übergeben werden!
scn	SCN für SIM-Karte *(nicht bei LAN-Routern)*
scn2	SCN für SIM-Karte 2 *(nur bei Mobilfunk-Routern)*
sms_protocol	0 = Gegenstelle ist Modem *(nur bei Modem-Routern)*
	1 = Gegenstelle ist Mobiltelefon (PET/IXO/TAP 8N1) *(nur bei Modem-Routern)*
	1 = TAP-Protokoll *(nur bei ISDN-Routern)*
	2 = Gegenstelle ist Mobiltelefon (EMI/UCP 7E1) *(nur bei Modem-Routern)*
	2 = UGP-Protokoll *(nur bei ISDN-Routern)*
	3 = Gegenstelle ist Mobiltelefon (PET/IXO/TAP 7E1) *(nur bei Modem-Routern)*
	4 = Gegenstelle ist Mobiltelefon (EMI/UCP 8N1) *(nur bei Modem-Routern)*
	5 = Gegenstelle ist Fax *(nur bei Modem-Routern)*
	6 = Gegenstelle ist SMS an Festnetz *(nur bei Modem-Routern)*
start_sms_reception	0 = SMS-Empfang deaktiviert (default)
	1 = SMS-Empfang aktiviert
acknowledge_sms	0 = SMS-Quittierung deaktiviert (default)
	1 = SMS-Quittierung aktiviert
sms_reception_password	Kennwort für den SMS-Empfang
	Objektwert muss in Hochkommas übergeben werden!
forward_sms_to_sandbox	0 = SMS-Weiterleitung zur Sandbox deaktiviert (default)
	1 = SMS-Weiterleitung zur Sandbox aktiviert
snmp_version	2 = SNMPv2c aktiviert (default)
	3 = SNMPv3 aktiviert
snmp_community	Community-String für SNMPv2c (default: public)
	Objektwert muss in Hochkommas übergeben werden!
snmp_username	Benutzername für SNMPv3
	Objektwert muss in Hochkommas übergeben werden!

`snmp_auth_hash`	none = Keine SNMP-Authentifizierung (default)
	md5 = SNMP-Authentifizierung über MD5
	sha = SNMP-Authentifizierung über SHA
`snmp_auth_password`	Kennwort für die SNMP-Authentifizierung
	Objektwert muss in Hochkommas übergeben werden!
`snmp_privacy_cipher`	none = Keine SNMP-Verschlüsselung (default)
	des = SNMP-Verschlüsselung über DES
	aes = SNMP-Verschlüsselung über AES
`snmp_privacy_password`	Kennwort für die SNMP-Verschlüsselung
	Objektwert muss in Hochkommas übergeben werden!
`use_ssl_tls`	0 = Keine SSL/TLS-Verschlüsselung verwenden (default)
	1 = SSL/TLS-Verschlüsselung verwenden

[email]

`start_email`	0 = Versand von E-Mail-Meldungen deaktiviert
	1 = Versand von E-Mail-Meldungen aktiviert (default)
`list`	a = Neue Einträge werden an bestehende Liste angehängt
	d = Bestehende Liste wird gelöscht (default)
`new_entry`	Neue Regel für E-Mail-Versand, die folgende Unterobjekte übergibt:
`recipient`	E-Mail-Adresse des Empfängers
`cause`	1 = Meldungsversand bei Systemstart
	2 = … bei Aufbau eines OpenVPN-Tunnels
	3 = … bei Aufbau eines IPsec-Tunnels
	4 = … bei einfachem Alarm an Eingang 1
	5 = … bei einem Puls an Eingang 1
	6 = … bei zwei Pulsen an Eingang 1
	7 = … bei drei Pulsen an Eingang 1
	8 = … bei vier Pulsen an Eingang 1
	9 = … bei fünf Pulsen an Eingang 1
	10 = .. bei sechs Pulsen an Eingang 1
	11 = … bei sieben Pulsen an Eingang 1
	12 = … bei acht Pulsen an Eingang 1
	13 = … bei neun Pulsen an Eingang 1
	14 = … bei zehn Pulsen an Eingang 1
	15 = … bei Aufbau einer Dial-Out-Verb.
	16 = … bei Aufbau einer Dial-In-Verb.
	17 = .. bei Umschalten der SIM-Karten
	18 = … bei Aufbau einer DSL-Verbindung
	19 = … bei Beziehen einer IP-Adresse per DCHP

20 = … bei Umschalten auf integriertes Kommunikationsgerät

21 = … bei Zurückschalten auf die LAN (ext)-Schnittstelle

22 = … wenn internes Kommunikationsgerät nicht bereit ist

23 = … wenn automatisches Update erfolgt

24 = … bei Empfang einer neuen SMS

25 = … wenn SIM-Karte 1 aktiv ist

26 = … wenn SIM-Karte 2 aktiv ist

27 = … bei Aufbau eines PPTP-Tunnels

28 = … bei Link-Aufbau an LAN-Port 1

29 = … bei Link-Aufbau an LAN-Port 2

30 = … bei Link-Aufbau an LAN-Port 3

31 = … bei Link-Aufbau an LAN-Port 4

32 = … bei Link-Aufbau an LAN (ext)-Port

33 = … bei Link-Abbau an LAN-Port 1

34 = … bei Link-Abbau an LAN-Port 2

35 = … bei Link-Abbau an LAN-Port 3

36 = … bei Link-Abbau an LAN-Port 4

37 = … bei Link-Abbau an LAN (ext)-Port

38 = … bei Änderung der Konfiguration

39 = … wenn lokales Paket von der Firewall verworfen wird

40 = … wenn remote-Paket von der Firewall verworfen wird

41 = … bei fehlerhafter Authentifizierung am Web-Interface

42 = … bei Aufbau einer WWAN-Verbindung

43 = … wenn lokales Paket vom MAC-Filter verworfen wird

`attach`	0 = Kein Anhang wird an E-Mail angehängt
	1 = Systemmeldungen werden an E-Mail angehängt
	2 = System-Log wird an E-Mail angehängt
	3 = Mobilfunk-Log wird an E-Mail angehängt
	4 = OpenVPN Dial-In-Client-Log wird an E-Mail angeh.
	5 = OpenVPN Dial-In-Server-Log wird an E-Mail angeh.
	6 = OpenVPN Dial-Out-Client-Log wird an E-Mail angeh.
	7 = OpenVPN Dial-Out-Server-Log wird an E-Mail angeh.
	8 = OpenVPN LAN (ext)-Client-Log wird an E-Mail angehängt
	9 = OpenVPN LAN (ext)-Server-Log wird an E-Mail angehängt
	10 = IPsec LAN (ext)-Log wird an E-Mail angehängt
	11 = IPsec Dial-In-Log wird an E-Mail angehängt
	12 = IPsec Dial-Out-Log wird an E-Mail angehängt
	13 = Seriell-Ethernet-Gateway-Log wird an E-Mail angeh.
	14 = Auto-Update-Log wird an E-Mail angehängt
	15 = Text-Config-Log wird an E-Mail angehängt
	16 = IPT-Log wird an E-Mail angehängt
	17 = SDSL-Log wird an E-Mail angehängt
	18 = PPTP Dial-In-Client-Log wird an E-Mail angehängt
	19 = PPTP Dial-In-Server-Log wird an E-Mail angehängt
	20 = PPTP Dial-Out-Client-Log wird an E-Mail angehängt
	21 = PPTP Dial-Out-Server-Log wird an E-Mail angehängt
	22 = PPTP LAN (ext)-Client-Log wird an E-Mail angehängt
	23 = PPTP LAN (ext)-Server-Log wird an E-Mail angeh.
	24 = Router Advertiser-Log wird an E-Mail angehängt
	32 = ASCII-Konfigurationsdatei wird an E-Mail angehängt
`status`	0 = Keine Statusseite an E-Mail-Meldung anhängen (default)
	1 = Statusseite an E-Mail-Meldung anhängen
`text`	Text der E-Mail-Meldung

[sms]

`start_sms`	0 = Versand von SMS-Meldungen deaktiviert
	1 = Versand von SMS-Meldungen aktiviert (default)
`list`	a = Neue Einträge werden an bestehende Liste angehängt
	d = Bestehende Liste wird gelöscht (default)
`new_entry`	Neue Regel für SMS-Versand, die folgende Unterobjekte übergibt:
`recipient`	Telefonnummer des Empfängers

`cause`

1 = Meldungsversand bei Systemstart
2 = … bei Aufbau eines OpenVPN-Tunnels
3 = … bei Aufbau eines IPsec-Tunnels
4 = … bei einfachem Alarm an Eingang 1
5 = … bei einem Puls an Eingang 1
6 = … bei zwei Pulsen an Eingang 1
7 = … bei drei Pulsen an Eingang 1
8 = … bei vier Pulsen an Eingang 1
9 = … bei fünf Pulsen an Eingang 1
10 = .. bei sechs Pulsen an Eingang 1
11 = … bei sieben Pulsen an Eingang 1
12 = … bei acht Pulsen an Eingang 1
13 = … bei neun Pulsen an Eingang 1
14 = … bei zehn Pulsen an Eingang 1
15 = … bei Aufbau einer Dial-Out-Verb.
16 = … bei Aufbau einer Dial-In-Verb.
17 = .. bei Umschalten der SIM-Karten
18 = … bei Aufbau einer DSL-Verbindung
19 = … bei Beziehen einer IP-Adresse per DCHP
20 = … bei Umschalten auf integriertes Kommunikationsgerät
21 = … bei Zurückschalten auf die LAN (ext)-Schnittstelle
22 = … wenn internes Kommunikationsgerät nicht bereit ist
23 = … wenn automatisches Update erfolgt
24 = … bei Empfang einer neuen SMS
25 = … wenn SIM-Karte 1 aktiv ist
26 = … wenn SIM-Karte 2 aktiv ist
27 = … bei Aufbau eines PPTP-Tunnels
28 = … bei Link-Aufbau an LAN-Port 1
29 = … bei Link-Aufbau an LAN-Port 2
30 = … bei Link-Aufbau an LAN-Port 3
31 = … bei Link-Aufbau an LAN-Port 4
32 = … bei Link-Aufbau an LAN (ext)-Port
33 = … bei Link-Abbau an LAN-Port 1
34 = … bei Link-Abbau an LAN-Port 2
35 = … bei Link-Abbau an LAN-Port 3
36 = … bei Link-Abbau an LAN-Port 4
37 = … bei Link-Abbau an LAN (ext)-Port
38 = … bei Änderung der Konfiguration

	39 = … wenn lokales Paket von der Firewall verworfen wird
	40 = … wenn remote-Paket von der Firewall verworfen wird
	41 = … bei fehlerhafter Authentifizierung am Web-Interface
	42 = … bei Aufbau einer WWAN-Verbindung
	43 = … wenn lokales Paket vom MAC-Filter verworfen wird
`text`	Text der SMS-Meldung
`[ snmp traps ]`	
`start_snmptrap`	0 = Versand von SNMP-Traps deaktiviert
	1 = Versand von SNMP-Traps aktiviert (default)
`list`	a = Neue Einträge werden an bestehende Liste angehängt
	d = Bestehende Liste wird gelöscht (default)
`new_entry`	Neue Regel für SNMP-Trap-Versand, die folgende Unterobjekte übergibt:
`recipient_ip`	IP-Adresse oder Domainname des Empfängers
`recipient_port`	Port des Empfängers

`cause`

1 = Meldungsversand bei Systemstart
2 = … bei Aufbau eines OpenVPN-Tunnels
3 = … bei Aufbau eines IPsec-Tunnels
4 = … bei einfachem Alarm an Eingang 1
5 = … bei einem Puls an Eingang 1
6 = … bei zwei Pulsen an Eingang 1
7 = … bei drei Pulsen an Eingang 1
8 = … bei vier Pulsen an Eingang 1
9 = … bei fünf Pulsen an Eingang 1
10 = .. bei sechs Pulsen an Eingang 1
11 = … bei sieben Pulsen an Eingang 1
12 = … bei acht Pulsen an Eingang 1
13 = … bei neun Pulsen an Eingang 1
14 = … bei zehn Pulsen an Eingang 1
15 = … bei Aufbau einer Dial-Out-Verb.
16 = … bei Aufbau einer Dial-In-Verb.
17 = .. bei Umschalten der SIM-Karten
18 = … bei Aufbau einer DSL-Verbindung
19 = … bei Beziehen einer IP-Adresse per DCHP
20 = … bei Umschalten auf integriertes Kommunikationsgerät
21 = … bei Zurückschalten auf die LAN (ext)-Schnittstelle
22 = … wenn internes Kommunikationsgerät nicht bereit ist
23 = … wenn automatisches Update erfolgt
24 = … bei Empfang einer neuen SMS
25 = … wenn SIM-Karte 1 aktiv ist
26 = … wenn SIM-Karte 2 aktiv ist
27 = … bei Aufbau eines PPTP-Tunnels
28 = … bei Link-Aufbau an LAN-Port 1
29 = … bei Link-Aufbau an LAN-Port 2
30 = … bei Link-Aufbau an LAN-Port 3
31 = … bei Link-Aufbau an LAN-Port 4
32 = … bei Link-Aufbau an LAN (ext)-Port
33 = … bei Link-Abbau an LAN-Port 1
34 = … bei Link-Abbau an LAN-Port 2
35 = … bei Link-Abbau an LAN-Port 3
36 = … bei Link-Abbau an LAN-Port 4
37 = … bei Link-Abbau an LAN (ext)-Port
38 = … bei Änderung der Konfiguration

	39 = … wenn lokales Paket von der Firewall verworfen wird
	40 = … wenn remote-Paket von der Firewall verworfen wird
	41 = … bei fehlerhafter Authentifizierung am Web-Interface
	42 = … bei Aufbau einer WWAN-Verbindung
	43 = … wenn lokales Paket vom MAC-Filter verworfen wird

[dns]

`dns`	IPv4-Adresse des ersten DNS-Servers
`dns2`	IPv4-Adresse des zweiten DNS-Servers
`dns_v6`	IPv6-Adresse des ersten DNS-Servers *(ab FW 2.10.0)*
`dns2_v6`	IPv6-Adresse des zweiten DNS-Servers *(ab FW 2.10.0)*
`start_dns_relay`	0 = DNS-Relay deaktiviert 1 = DNS-Relay aktiviert (default) *(ab FW 2.11.0)*

[dyndns]

`start_dyndns`	0 = Dynamisches DNS-Update deaktiviert (default)	
	1 = Dynamisches DNS-Update aktiviert	
`provider`	dyndns =	DynDNS als DynDNS-Provider (default)
	dyndns-custom =	DynDNS custom als DynDNS-Provider
	dyndns-static =	DynDNS static als DynDNS-Provider
	dhs =	DHS als DynDNS-Provider
	ods =	ODS als DynDNS-Provider
	tzo =	TZO als DynDNS-Provider
	easydns =	easyDNS als DynDNS-Provider
	dyns =	DyNS als DynDNS-Provider
	zoneedit =	zoneedit als DynDNS-Provider
	own =	Benutzerdefinierter DynDNS-Provider
`server`	Benutzerdefinierter DynDNS-Server Wird ein Provider aus der Liste gewählt, darf kein Server angegeben werden!	
`domain`	Domainname beim DynDNS-Provider	
`username`	Benutzername beim DynDNS-Provider Objektwert muss in Hochkommas übergeben werden!	

`password`	Kennwort beim DynDNS-Provider Objektwert muss in Hochkommas übergeben werden!
`freedns_hash_<x>`	Hash-Wert für freedns.afraid.org-Konfiguration (<x> = 1-5)
`freedns_ipv6_<x>`	0 = IPv6-Adresse des Routers beim DNS-Server nicht hinterlegen (default) 1 = IPv6-Adresse des Routers beim DNS-Server hinterlegen (<x> = 1-5)

[dhcp]

`start_dhcpserver`	0 = DHCP-Server deaktiviert (default) 1 = DHCP-Server aktiviert
`dhcp_ip_start`	Erste IP-Adresse des Adress-Pools
`dhcp_ip_end`	Letzte IP-Adresse des Adress-Pools
`leasetime`	Gültigkeitsdauer der IP-Adressen (in Sek., default: 3600)
`alternate_dns`	IP-Adresse des alternativen DNS-Servers für die DHCP-Clients
`list`	a = Neue Einträge werden an bestehende Liste angehängt d = Bestehende Liste wird gelöscht (default)
`alternate_router`	IP-Adresse des alternativen Default-Gateway *(ab FW 2.11.0)*
`new_entry`	Neue Zuordnung von MAC-Adresse und IP-Adresse, die folgende Unterobjekte übergibt:
`mac`	MAC-Adresse (ohne Doppelpunkte)
`ip`	IP-Adresse

[proxy]

start_proxy	0 = Proxy-Server deaktiviert (default)
	1 = Proxy-Server aktiviert
port	Port des Proxy-Servers (default: 8888)
timeout	Timeout für inaktive Verbindungen (in Sek., default: 600)
max_clients	Maximale Anzahl an erlaubten Clients (default: 10)
min_spare	Minimale Anzahl an freien Proxy-Servern (default: 1)
max_spare	Maximale Anzahl an freien Proxy-Servern (default: 5)
filter	0 = Proxy-Filter deaktiviert (default)
	1 = Proxy-Filter aktiviert
list	a = Neue Einträge werden an bestehende Liste angehängt
	d = Bestehende Liste wird gelöscht (default)
new_entry	Neuer Eintrag in die Liste der erlaubten URLs oder IP-Adressen des Proxy-Filters

[ipt] *ab FW 2.5.0*

start_ipt	0 = IPT-Slave deaktiviert (default)
	1 = IPT-Slave aktiviert
master	IP-Adresse oder Domainname des primären IPT-Master
port	Port des primären IPT-Master
username	Benutzername für Anmeldung am primären IPT-Master
	Objektwert muss in Hochkommas übergeben werden!
password	Passwort für Anmeldung am primären IPT-Master
	Objektwert muss in Hochkommas übergeben werden!
master2	IP-Adresse oder Domainname des sekundären IPT-Master
port2	Port des sekundären IPT-Master
username2	Benutzername für Anmeldung am sekundären IPT-Master
	Objektwert muss in Hochkommas übergeben werden!
password2	Passwort für Anmeldung am sekundären IPT-Master
	Objektwert muss in Hochkommas übergeben werden!
device_identifier	IPT Device-Identifier (default: INS_<MAC-Adresse>)
increase_interval	0 = Wartezeit zwischen Verbindungsversuchen nicht erhöhen (default)
	1 = Wartezeit zwischen Verbindungsversuchen erhöhen
response_timeout	Timeout für IPT-Response (in Sekunden, default: 30)
receive_timeout	Timeout für IPT-Zeichen (in Sekunden, default: 15)
scrambled	0 = IPT-Verschleierung nicht verwenden (default)
	1 = IPT-Verschleierung verwenden
challenge_key	IPT-Challenge Scramble Key
fix_key	IPT-Fix Scramble Key

[snmp agent]	*ab FW 2.6.0*
start_snmpd	0 = SNMP-Agent deaktiviert (default)
	1 = SNMP-Agent aktiviert
local_exclusiv	0 = SNMP nur lokal zulassen deaktiviert
	1 = SNMP nur lokal zulassen aktiviert (default)
port	Port des SNMP-Agent für den Empfang von Anfragen
system_contact	Eintrag für Kontakt-Informationen des SNMP-Agent
	Objektwert muss in Hochkommas übergeben werden!
system_description	Eintrag für Beschreibung des SNMP-Agent
	Objektwert muss in Hochkommas übergeben werden!
use_v1_v2c	0 = SNMP-Version v1 und v2c deaktiviert
	1 = SNMP-Version v1 und v2c aktiviert (default)
community	Community-String für SNMPv2c (default: public)
	Objektwert muss in Hochkommas übergeben werden!
use_v3	0 = SNMP-Version v3 deaktiviert (default)
	1 = SNMP-Version v3 aktiviert
username	Benutzername für SNMPv3
	Objektwert muss in Hochkommas übergeben werden!
auth_hash	none = Keine SNMP-Authentifizierung (default)
	md5 = SNMP-Authentifizierung über MD5
	sha = SNMP-Authentifizierung über SHA
auth_password	Kennwort für die SNMP-Authentifizierung
	Objektwert muss in Hochkommas übergeben werden!
privacy_cipher	none = Keine SNMP-Verschlüsselung (default)
	des = SNMP-Verschlüsselung über DES
	aes = SNMP-Verschlüsselung über AES
privacy_password	Kennwort für die SNMP-Verschlüsselung
	Objektwert muss in Hochkommas übergeben werden!

[radvd]	*ab FW 2.10.0*
start_radvd	0 = Router-Advertiser deaktiviert (default)
	1 = Router-Advertiser aktiviert
preference	low = Router-Advertiser-Präferenz niedrig
	medium = Router-Advertiser-Präferenz mittel (default)
	high = Router-Advertiser-Präferenz hoch
list	a = Neue Einträge werden an bestehende Liste angehängt
	d = Bestehende Liste wird gelöscht (default)
new_entry	Neuer Routeneintrag, der folgende Unterobjekte übergibt:
net	IPv6-Adress-Prefix
prefix_length	Länge des IPv6-Adress-Prefix (7-64, default: 64)

[mcip]	*ab FW 2.10.0*
incoming	0 = Eingehende TCP-Verbindungen nicht annehmen (default)
	1 = Eingehende TCP-Verbindungen annehmen
listen_port	Port an dem die eingehenden TCP-Verbindungen angenommen werden (default: 4424)
oid_in1	Objekt-ID für Eingang 1 (1001-65534)
	(nur bei Geräten mit Ein-/Ausgängen)
oid_in2	Objekt-ID für Eingang 2 (1001-65534)
	(nur bei Geräten mit Ein-/Ausgängen)
oid_out1	Objekt-ID für Ausgang 1 (1001-65534)
	(nur bei Geräten mit Ein-/Ausgängen)
oid_out2	Objekt-ID für Ausgang 2 (1001-65534)
	(nur bei Geräten mit Ein-/Ausgängen)
oid_led_com_green	Objekt-ID für LED COM grün (1001-65534)
oid_led_com_orange	Objekt-ID für LED COM orange (1001-65534)
oid_led_status_green	Objekt-ID für LED Status grün (1001-65534)
local_exclusive	0 = MCIP-Verbindungen auch aus dem WAN zulassen
	1 = MCIP-Verbindungen nur lokal zulassen (default)

[settime]	
day	Systemzeit stellen auf Tag (01-31)
mon	Systemzeit stellen auf Monat (01-12)
year	Systemzeit stellen auf Jahr
hour	Systemzeit stellen auf Stunde (00-23)
min	Systemzeit stellen auf Minute (00-59)

`timezone`	UTC =	Zeitzone UTC
	GMT =	Zeitzone GMT
	GMT-1 =	Zeitzone GMT -1
	GMT+1 =	Zeitzone GMT +1
	GMT-2 =	Zeitzone GMT -2
	GMT+2 =	Zeitzone GMT +2
	GMT-3 =	Zeitzone GMT -3
	GMT+3 =	Zeitzone GMT +3
	GMT-4 =	Zeitzone GMT -4
	GMT+4 =	Zeitzone GMT +4
	GMT-5 =	Zeitzone GMT -5
	GMT+5 =	Zeitzone GMT +5
	GMT-6 =	Zeitzone GMT -6
	GMT+6 =	Zeitzone GMT +6
	GMT-7 =	Zeitzone GMT -7
	GMT+7 =	Zeitzone GMT +7
	GMT-8 =	Zeitzone GMT -8
	GMT+8 =	Zeitzone GMT +8
	GMT-9 =	Zeitzone GMT -9
	GMT+9 =	Zeitzone GMT +9
	GMT-10 =	Zeitzone GMT -10
	GMT+10 =	Zeitzone GMT +10
	GMT-11 =	Zeitzone GMT -11
	GMT+11 =	Zeitzone GMT +11
	GMT-12 =	Zeitzone GMT -12
	GMT+12 =	Zeitzone GMT +12
	GMT-13 =	Zeitzone GMT -13
	GMT-14 =	Zeitzone GMT -14
	Europe/Amsterdam =	Zeitzone Europe/Amsterdam
	Europe/Andorra =	Zeitzone Europe/Andorra
	Europe/Athens =	Zeitzone Europe/Athens
	Europe/Belfast =	Zeitzone Europe/Belfast
	Europe/Belgrade =	Zeitzone Europe/Belgrade
	Europe/Berlin =	Zeitzone Europe/Berlin
	Europe/Bratislava =	Zeitzone Europe/Bratislava
	Europe/Brussels =	Zeitzone Europe/Brussels
	Europe/Bucharest =	Zeitzone Europe/Bucharest
	Europe/Budapest =	Zeitzone Europe/Budapest
	Europe/Chisinau =	Zeitzone Europe/Chisinau

Europe/Copenhagen =	Zeitzone Europe/Copenhagen
Europe/Dublin =	Zeitzone Europe/Dublin
Europe/Eire =	Zeitzone Europe/Eire
Europe/Gibraltar =	Zeitzone Europe/Gibraltar
Europe/Helsinki =	Zeitzone Europe/Helsinki
Europe/Iceland =	Zeitzone Europe/Iceland
Europe/Istanbul =	Zeitzone Europe/Istanbul
Europe/Kaliningrad =	Zeitzone Europe/Kaliningrad
Europe/Kiev =	Zeitzone Europe/Kiev
Europe/Lisbon =	Zeitzone Europe/Lisbon
Europe/Ljubljana =	Zeitzone Europe/Ljubljana
Europe/London =	Zeitzone Europe/London
Europe/Luxembourg =	Zeitzone Europe/Luxembourg
Europe/Madrid =	Zeitzone Europe/Madrid
Europe/Malta =	Zeitzone Europe/Malta
Europe/Minsk =	Zeitzone Europe/Minsk
Europe/Monaco =	Zeitzone Europe/Monaco
Europe/Moscow =	Zeitzone Europe/Moscow
Europe/Nicosia =	Zeitzone Europe/Nicosia
Europe/Oslo =	Zeitzone Europe/Oslo
Europe/Paris =	Zeitzone Europe/Paris
Europe/Poland =	Zeitzone Europe/Poland
Europe/Portugal =	Zeitzone Europe/Portugal
Europe/Prague =	Zeitzone Europe/Prague
Europe/Regensburg =	Zeitzone Europe/Regensburg (default)
Europe/Riga =	Zeitzone Europe/Riga
Europe/Rome	Zeitzone Europe/Rome
Europe/Samara =	Zeitzone Europe/Samara
Europe/San_Marino =	Zeitzone Europe/San Marino
Europe/Sarajevo =	Zeitzone Europe/Sarajevo
Europe/Simferopol =	Zeitzone Europe/Simferopol
Europe/Skopje =	Zeitzone Europe/Skopje
Europe/Sofia =	Zeitzone Europe/Sofia
Europe/Stockholm =	Zeitzone Europe/Stockholm
Europe/Tallinn =	Zeitzone Europe/Tallinn
Europe/Tirane =	Zeitzone Europe/Tirane
Europe/Tiraspol =	Zeitzone Europe/Tiraspol
Europe/Turkey =	Zeitzone Europe/Turkey

	Europe/Uzhgorod =	Zeitzone Europe/Uzhgorod
	Europe/Vaduz =	Zeitzone Europe/Vaduz
	Europe/Vatican =	Zeitzone Europe/Vatican
	Europe/Vienna =	Zeitzone Europe/Vienna
	Europe/Vilnius =	Zeitzone Europe/Vilnius
	Europe/Warsaw =	Zeitzone Europe/Warsaw
	Europe/Zagreb =	Zeitzone Europe/Zagreb
	Europe/Zaporozhye =	Zeitzone Europe/Zaporozhye
	Europe/Zurich =	Zeitzone Europe/Zurich
`ntp_server`	Adresse des verwendeten NTP-Zeit-Servers	
`start_ntp_client`	0 = Keine Uhrsynchronisierung über NTP-Zeit-Server	
	1 = Uhrsynchronisierung über NTP-Zeit-Server (default)	
`daily_sync`	0 = Keine tägliche Zeitsynchronisierung (default)	
	1 = Tägliche Zeitsynchronisierung zur angegebenen Uhrzeit	
`daily_sync_hour`	Stunde der täglichen Zeitsynchronisierung (00-24)	
`daily_sync_min`	Minute der täglichen Zeitsynchronisierung (00-59)	
`update_now`	0 = Uhrzeit nicht sofort synchronisieren (default)	
	1 = Uhrzeit sofort synchronisieren	
	(ab FW 2.11.0)	
`start_ntp_server`	0 = Lokaler Zeit-Server deaktiviert (default)	
	1 = Lokaler Zeit-Server aktiviert	
	(ab FW 2.11.0)	

[reset daily]

`reset_daily`	0 = Täglicher Neustart deaktiviert (default)
	1 = Täglicher Neustart aktiviert
`hour`	Täglicher Neustart um (Stunde, 00-23)
`min`	Täglicher Neustart um (Minute, 00-59)

[update]

`start_auto_update`	0 = Automatisches tägliches Update deaktiviert (default)
	1 = Automatisches tägliches Update aktiviert
`timing_type`	mac = Update-Zeitpunkt abhängig von MAC (default)
	manual = Update zu fester Uhrzeit
	wan = Update nach jedem WAN-Verbindungsaufbau *(ab FW 2.8.0)*
`time_hour`	Update um (Stunde, 00-23)
`time_min`	Update um (Minute, 00-59)
`protocol`	http = Download über HTTP-Protokoll (default)
	ftp = Download über FTP-Protokoll
`uri`	IP-Adresse oder Domain-Name des Download-Servers
`port`	Port am Download-Server (default: 80)
`username`	Benutzername für Zugriff auf die Update-Dateien
	Objektwert muss in Hochkommas übergeben werden!
`password`	Kennwort für Zugriff auf die Update-Dateien
	Objektwert muss in Hochkommas übergeben werden!
`update_now`	0 = Nicht sofort nach Updates suchen (default)
	1 = Sofort nach Updates suchen

[sandbox] *nicht bei EBW bis FW 2.12.8 und RSM*

`start_sandbox`	0 = Sandbox deaktiviert (default)
	1 = Sandbox aktiviert
`serial`	0 = RS232-Schnittstelle „Serial 1“ nicht für Sandbox reserviert (default)
	1 = RS232-Schnittstelle „Serial 1“ für Sandbox reserviert
`serial2`	0 = Logo/RS485-Schnittstelle „Serial 2“ nicht für Sandbox reserviert (default)
	1 = Logo/RS485-Schnittstelle „Serial 2“ für Sandbox reserviert
	(nur IMON ab FW 2.11.0)
`install`	0 = Gespeichertes Sandbox-Image nicht installieren (default)
	1 = Gespeichertes Sandbox-Image installieren
`password`	Kennwort für den Sandbox-Benutzer „user“
	Objektwert muss in Hochkommas übergeben werden!
`ascii_config`	0 = ASCII-Konfiguration aus der Sandbox nicht zugelassen (default)
	1 = ASCII-Konfiguration aus der Sandbox zugelassen
	(ab FW 2.8.0)

`gps`	0 = GPS-Verwendung in der Sandbox nicht zugelassen (default) 1 = GPS-Verwendung in der Sandbox zugelassen *(nur bei Geräten mit GPS-Empfänger)*
`antenna`	passive = Passive GPS-Antenne wird verwendet active = Aktive GPS-Antenne wird verwendet (default) *(nur bei Geräten mit GPS-Empfänger)*
`i2c`	0 = I²C-Schnittstelle nicht für Sandbox reserviert (default) 1 = I²C-Schnittstelle für Sandbox reserviert *(nur QLM-E/G/H/W)*
`auto_install`	0 = Neues Image beim automatischen Update nicht installieren (default) 1 = Neues Image beim automatischen Update installieren *(ab FW 2.12.9)*