1 Das CGI-Interface verwenden

Dokument-ID: 108416_de_01
Dokument-Bezeichnung: AH DE MGUARD CGI INTERFACE

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

Inhalt dieses Dokuments

In diesem Dokument wird die Verwendung des CGI-Interface des mGuard-Geräts (eine zusätzliche HTTPS-Schnittstelle) beschrieben.

1.1 Einleitung 1
1.2 Verwendung 2
1.3 Voraussetzungen und Einschränkungen 5
1.4 Interface nph-vpn.cgi 6
1.5 Interface nph-diag.cgi 21
1.6 Interface nph.action.cgi 22
1.7 Interface nph.status.cgi 24

1.1 Einleitung

Die zusätzlichen HTTPS-Schnittstellen sind als CGI-Skripte (**C**ommon **G**ateway **I**nterface) umgesetzt und bieten folgende Merkmale und Funktionen:

Einige Befehle werden synchron ausgeführt: ihr Rückgabecode gibt Auskunft darüber, ob der Befehl erfolgreich ausgeführt wurde oder nicht. Beim Aufbau einer VPN-Verbindung wird der Fortschritt für jeden wichtigen Schritt angezeigt.

nph-vpn.cgi / nph-diag.cgi

- Zugriff von einem konventionellen HTTPS-Client.
- Aktivierung/Deaktivierung einer VPN-Verbindung.
- Ermittlung des Verbindungsstatus einer VPN-Verbindung.
- Ausführung eines "Download-Tests", um zu überprüfen, ob der mGuard die Konfigurationsdatei von dem angegebenen HTTPS-Server herunterladen kann.
- Ermittlung der Firmware-Version und Hardware-Revision des mGuards.
- Herunterladen eines Support-*Snapshots*.

nph-action.cgi / nph-status.cgi

Die CGI-Interfaces *nph-action.cgi* und *nph-status.cgi* bieten einen erweiterten Funktionsumfang (siehe Kapitel 1.6, "Interface nph.action.cgi" und Kapitel 1.7, "Interface nph.status.cgi").

1.2 Verwendung

Die CGI-Skripte auf dem mGuard können über HTTPS über die gleiche IP-Adresse und den gleichen Port erreicht werden, auf denen die Weboberfläche verfügbar ist. Sie müssen nur eine andere URL verwenden. Jeder Zugriff auf ein CGI-Skript führt einen bestimmten Befehl aus. Jeder Befehl antwortet mit einem UTF-8-Text im *Body* der HTTP-Antwort. Die Ausnahme bildet der Befehl *snapshot*, der binäre Daten zurückgibt. Einige Fehlerzustände werden im SSL in der jeweiligen HTTP-Antwort angezeigt. Der HTTP-Statuscode 401, zum Beispiel, zeigt eine fehlgeschlagene Autorisierung an.

1.2.1 Verfügbare Befehle

nph-vpn.cgi / nph-diag.cgi

Tabelle 1-1 Über CGI-Skripte verfügbare Befehle

CGI-Skript	Befehl	Zweck
nph-vpn.cgi	*synup*	Aktivierung einer VPN-Verbindung (synchroner Befehl)
	syndown	Deaktivierung einer VPN-Verbindung (synchroner Befehl)
	synstat	Bestimmung des Status einer VPN-Verbindung (synchroner Befehl)
	sysinfo	Ermittlung der Firmware-Version und Hardware-Revision auf dem mGuard
	up	Aktivierung einer VPN-Verbindung (asynchroner Befehl)
	down	Deaktivierung einer VPN-Verbindung (asynchroner Befehl)
	status	Bestimmung des Status einer VPN-Verbindung (asynchroner Befehl)
	clear	Löscht die Instanz einer VPN-Verbindung
nph-diag.cgi	*testpull*	Veranlasst einen "Download-Test" von einem HTTPS-Server
	snapshot	Herunterladen eines *Snapshots* vom mGuard

nph-action.cgi / nph-status.cgi

Für die Befehle, die über die CGI-Skripte *nph-action.cgi* und *nph-status.cgi* verfügbar sind, siehe Kapitel 1.6, "Interface nph.action.cgi" und Kapitel 1.7, "Interface nph.status.cgi".

1.2.2 Befehlssyntax

Die Verwendung des Kommandozeilen-Tools *wget* funktioniert nur im Zusammenspiel mit mGuard-Firmwareversionen < 8.4.0. Ab mGuard-Firmwareversion 8.4.0 kann das Kommandozeilen-Tool *curl* verwendet werden (Parameter und Optionen abweichend!).

Beispiel:

wget --no-check-certificate "https://admin:mGuard@192.168.1.1/nph-vpn.cgi?name=Athen&cmd=up"

curl --insecure "https://admin:mGuard@192.168.1.1/nph-vpn.cgi?name=Athen&cmd=up"

Die Option --no-check-certificate (*wget*) bzw. --insecure (*curl*) sorgt dafür, dass das HTTPS-Zertifikat des mGuards nicht weiter geprüft wird.

Die Befehlszeile hat bei Verwendung des Dienstprogrammes *wget* folgende Syntax:

*wget […] 'https://***MGUARD/CGI-SCRIPT***?cmd=***COMMAND***'**
*wget […] 'https://***MGUARD/CGI-SCRIPT***?cmd=***COMMAND***&name=***VPN_NAME***'**
*wget […] 'https://***MGUARD/CGI-SCRIPT***?cmd=***COMMAND***&channel=***LNET_RNET***'**

Bei Verwendung des Dienstprogrammes *curl* hat die Befehlszeile folgende Syntax:

*curl […] 'https://***MGUARD/CGI-SCRIPT***?cmd=***COMMAND***'**
*curl […] 'https://***MGUARD/CGI-SCRIPT***?cmd=***COMMAND***&name=***VPN_NAME***'**
*curl […] 'https://***MGUARD/CGI-SCRIPT***?cmd=***COMMAND***&channel=***LNET_RNET***'**

Tabelle 1-2 Befehlssyntax

wget […] oder curl […]	Dienstprogramm zum Erstellen der HTTPS-Anfrage und der benötigten Argumente. Beachten Sie bitte das Handbuch zum Dienstprogramm.
MGUARD	IP-Adresse und Portnummer, auf denen der mGuard auf eingehende HTTPS-Anfragen horcht. Der IP-Adresse können Benutzername und Passwort vorangestellt werden. **[<Benutzername>:<Passwort>@]<IP-Adresse>[:<Port>]** Beispiel: admin:mGuard@192.168.1.254:443
CGI-SCRIPT	Name des aufzurufenden CGI-Skriptes, entweder *nph-vpn.cgi* oder *nph-diag.cgi*.
COMMAND	Auszuführender Befehl, auf den folgenden Seiten beschrieben.
VPN_NAME	Name der VPN-Verbindung, die aktiviert oder deaktiviert oder deren Status erfasst werden soll. Befehle: *synup, syndown, synstat, up, down, status.*
LNET_RNET	Lokales und Remote-VPN-Netzwerk. Befehle: status, clear.

Beispiele

wget […] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?cmd=synup&name=Service'
curl […] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?cmd=synup&name=Service'

– Unter Linux und anderen UNIX-Betriebssystemen beginnt und endet der mit https:// beginnende String mit einem einfachen Anführungszeichen (‘). Unter anderen Betriebssystemen wie Windows können doppelte Anführungszeichen (") verwendet werden.
– Wenn der VPN-Name Sonderzeichen wie das Leerzeichen enthält, müssen diese entsprechend den URL-Kodierregeln in Anführungszeichen gesetzt werden.
– Beinhaltet die URL wie in den oben genannten Beispielen das Passwort, müssen Sie sich darüber im Klaren sein, dass ein Eindringling das Passwort aus der Prozessliste oder dem Verlauf der Befehlszeile auslesen kann. Es ist ratsam, den Benutzer mit dem Benutzernamen "*user*" zu verwenden. Dieser Benutzer hat die Rechte, eine VPN-Verbindung zu aktivieren oder deaktivieren oder ihren Status zu ermitteln, indem er die in diesem Dokument beschriebenen CGI-Skripte aufruft. Dieser Benutzer hat aber nicht das Recht, sich über HTTPS oder SSH auf dem mGuard einzuloggen oder Konfigurationsänderungen vorzunehmen.

1.2.3 Zugriffsrechte

Tabelle 1-3 Zugriffsrechte

Befehl	**Benutzer**				
	root	**admin**	**user**	**netadmin**	**audit**
up, down, synup, syndown	x	x	x	-	-
status, synstat, sysinfo	x	x	x	x	x
status & channel, clear (central VPN gateway)	x	x	-	-	-
testpull, snapshot	x	x	-	-	-

1.3 Voraussetzungen und Einschränkungen

Beim Ausführen der Skripte nph-vpn.cgi, nph-diag.cgi, nph-status.cgi und nph-action.cgi, dürfen nur folgende Zeichen für Benutzernamen, Passwörter und andere definierte Namen (z.B. die Benennung einer VPN-Verbindung) verwendet werden:

– Buchstaben: A - Z, a - z
– Ziffern: 0 - 9
– Sonderzeichen: - . _ ~

Andere Sonderzeichen, z. B. das Leerzeichen oder das Fragezeichen, müssen entsprechend codiert werden (URL-Kodierung).

Die Verwendung des Kommandozeilen-Tools *wget* funktioniert nur im Zusammenspiel mit mGuard-Firmwareversionen < 8.4.0. Ab mGuard-Firmwareversion 8.4.0 kann das Kommandozeilen-Tool *curl* verwendet werden (Parameter und Optionen abweichend!).

Beispiel:

wget --no-check-certificate "https://admin:mGuard@192.168.1.1/nph-vpn.cgi?name=Athen&cmd=up"

curl --insecure "https://admin:mGuard@192.168.1.1/nph-vpn.cgi?name=Athen&cmd=up"

Die Option --no-check-certificate (*wget*) bzw. --insecure (*curl*) sorgt dafür, dass das HTTPS-Zertifikat des mGuards nicht weiter geprüft wird.

1.3.1 Voraussetzungen

Die Befehle *synup*, *syndown*, *up* und *down* können nur für das Auslösen einer VPN-Verbindung verwendet werden, wenn diese wie folgt konfiguriert ist:

1. Die VPN-Verbindung ist deaktiviert (Menü **IPsec VPN >> Verbindungen**).
2. Mindestens ein Tunnel der VPN-Verbindung ist aktiviert (Menü **VPN >> Verbindungen**, Registerkarte *Allgemein*, Abschnitt *Transport- und Tunneleinstellungen*).
3. Die Verbindungsinitialisierung muss auf *Initiiere* oder *Initiiere bei Datenverkehr* gestellt sein (Menü **VPN >> Verbindungen**, Registerkarte *Allgemein*, Abschnitt *Optionen*).

1.3.2 Einschränkungen

– Befehle, die über das CGI-Interface ausgeführt werden, können mit anderen Aktivitäten des mGuard sowie mit anderen über andere Schnittstellen ausgeführten Befehlen kollidieren.
– Eine VPN-Verbindung sollte entweder durch CMD-Kontakt oder über das CGI-Interface ausgelöst werden. Eine Kombination aus beiden Varianten wird nicht unterstützt.
– Die Befehle *synup*, *syndown*, *up* und *down* werden nicht für VPN-Verbindungen unterstützt, die auf eingehende VPN-Verbindungen warten (*Verbindungsinitiierung* = *Warte*).
– Das CGI sollte nicht während eines Firmware-Updates oder eines Neustarts des mGuard verwendet werden.

1.4 Interface nph-vpn.cgi

1.4.1 cmd=(up|down), name=<VPN-Name>

Diese Befehle aktivieren oder deaktivieren die angegebene VPN-Verbindung. Der Name der VPN-Verbindung muss mit dem Parameter *name* angegeben werden.

Aufgrund der asynchronen Ausführung dieser Befehle gibt der Rückgabewert keine Informationen über den Status der VPN-Verbindung. Daher sollte diesen Befehlen eine Ausführung des Befehls Status folgen, um den Status der VPN-Verbindung zu bestimmen.

Beispiele:

*wget […] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?***cmd=up***&name=Service'*
*wget […] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?***cmd=down***&name=Service'*

Diese Befehle geben einen der folgenden Werte im HTTP-Antworttext zurück:

Rückgabewert	Bedeutung
unknown	Eine VPN-Verbindung mit dem angegebenen Namen existiert nicht.
void	Die VPN-Verbindung ist inaktiv, entweder aufgrund eines Fehlers oder weil sie nicht mithilfe des CGI-Interface aktiviert wurde.
ready	Die VPN-Verbindung ist bereit, selbst Tunnel aufzubauen oder eingehende Anfragen zum Tunnelaufbau zu erlauben.
active	Mindestens ein VPN-Tunnel der VPN-Verbindung ist für die Verbindung aufgebaut.

1.4.2 cmd=status, [name=(<VPN-Name>|*)]

Abhängig vom Parameter *name*, ermittelt dieser Befehl entweder den Status

1. einer angegebenen VPN-Verbindung (name=[VPN-Name]) oder
2. den aller konfigurierten VPN-Verbindungen (name=*), oder
3. den aller aktivierten oder über *synup* aktivierten VPN-Verbindungen (Parameter *name* nicht angegeben) samt zusätzlicher Informationen.

Im Falle von (1) oder (2) gibt der Befehl einen der folgenden Werte zurück:

Rückgabewert	Bedeutung
unknown	Eine VPN-Verbindung mit dem angegebenen Namen existiert nicht.
void	Die VPN-Verbindung ist inaktiv, entweder aufgrund eines Fehlers oder weil sie nicht mithilfe des CGI-Interface aktiviert wurde.
ready	Die VPN-Verbindung ist bereit, selbst Tunnel aufzubauen oder eingehende Anfragen zum Tunnelaufbau zu erlauben.
active	Mindestens ein VPN-Tunnel der VPN-Verbindung ist für die Verbindung aufgebaut.

1.4.2.1 cmd=status, name=<VPN-Name>

Dieser Befehl ermittelt den Status der angegebenen VPN-Verbindung.

Beispiel:

*wget […] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?***cmd=status***&name=Service1'*

Rückgabewert
active

1.4.2.2 cmd=status, name=*

Dieser Befehl ermittelt den Status aller konfigurierten VPN-Verbindungen.

Beispiel:

*wget […] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?***cmd=status***&name=*'*

Rückgabewert
Service 1: active
Service 2: void

1.4.2.3 cmd=status (ohne Parameter *name*)

Dieser Befehl ermittelt den Status aller aktivierten VPN-Verbindungen samt zusätzlicher Informationen.

Beispiel:

wget […] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?cmd=status'

(Parameter *name* nicht angegeben)

Rückgabewert	
fullname	Service1
name	MAI0003584192_1 instance
leftnet	192.168.1.0/24
leftgw	10.1.0.48
leftnatport	
leftid	O=Innominate, OU=Support, CN=mGuard 3
leftproto	
leftport	
rightnet	192.168.2.0/24
rightgw	77.245.33.67
rightnatport	
rightid	O=Innominate, OU=Support, CN=Central Gateway
rightproto	
rightport	

Rückgabewert	
isakmp	6
isakmp-txt	STATE_MAIN_I4 (ISAKMP-SA established)
isakmp-ltime	157s
isakmp-algo	3DES_CBC_192-MD5-MODP1536
ipsec	7
ipsec-txt	STATE_QUICK_I2 (sent QI2, IPsec-SA aufgebaut)
ipsec-ltime	25526s
ipsec-algo	3DES_0-HMAC_MD5

Der Status der VPN-Verbindung *Service2* wird in diesem Beispiel nicht zurückgegeben, da diese Verbindung nicht aktiviert ist.

1.4.3 cmd=(synup|synstat|syndown), name=<VPN-Name>

Diese Befehle aktivieren, deaktivieren oder ermitteln den Status der angegebenen VPN-Verbindung. Anders als die Befehle *-up*, *-down* und *-status* werden diese Befehle synchron ausgeführt, weshalb der Vorgang zurückgegeben wird, sobald ein bestimmter Status erreicht wurde.

Das erste Zeichen der Antwort gibt an, ob der Vorgang erfolgreich ausgeführt wurde. Dem Rest der Antwortzeile können weitere Informationen entnommen werden. Der Antworttext besteht nur aus einer Zeile, außer beim Befehl *synup*, der eine VPN-Verbindung aufbaut. Für diesen Befehl enthält der Antworttext Fortschrittsmeldungen bezüglich des Aufbaus der VPN-Verbindung sowie eine finale Meldung mit dem Gesamtergebnis.

1.4.3.1 Format der Antwortmeldung

Jede Meldung hat das Format: <TYP> <CODE> <MESSAGE BODY>

TYP	Meldungstyp, ein Zeichen: P, R oder F: **P** – Fortschrittsmeldung (nur für den Befehl *synup*) **R** – Finale Meldung, Vorgang erfolgreich abgeschlossen **F** – Finale Meldung, Vorgang abgeschlossen mit Fehler
CODE	Maximal 12 Zeichen, eine Abkürzung dessen, was in diesem Schritt getan wurde (für Fortschrittsmeldungen) oder des Endergebnisses (für finale Meldungen). Bitte beachten Sie das nächste Kapitel.
MESSAGE BODY	Eine Folge von Textfeldern, abgegrenzt durch Leerzeichen. Jedes Feld besteht aus einem Kennzeichner und einem Wert, getrennt durch ein Gleichheitszeichen. Zu Beginn des MESSAGE BODY steht oft das Feld "uptime=..." oder "tstamp=...". “uptime=” gibt die Betriebszeit des mGuard in Sekunden mit Nachkommastellen seit der letzten Inbetriebnahme an. “tstamp=” gibt das Datum und den Zeitpunkt an, zu der die Meldung generiert wurde.

1.4.3.2 Antwortcode

Die Antwort kann eine der folgenden Codes enthalten:

Antwortcode	Beschreibung
EAMBIGUOUS	Der angegebene Name der VPN-Verbindung war zweideutig, da mehrere VPN-Verbindungen den gleichen Namen haben.
EBUSY	Das gerufene GDI-Skript ist derzeit mit einer anderen Aufgabe beschäftigt oder ist aufgrund eines laufenden Firmware-Updates gesperrt.
ECONFPULL	Der Test-Download eines Konfigurationsprofils vom HTTPS-Servers ist fehlgeschlagen.
EINVAL	Der CGI-Befehl oder die Parameter enthalten Syntaxfehler.
EVLOOKUPGW	Der Hostname des Remote-VPN-Gateways konnte nicht in eine IP-Adresse aufgelöst werden.
EVLOOKUPROUT	Kein Pfad zur IP-Adresse des Remote-VPN-Gateways bekannt.
ENOENT	Das angegebene Objekt existiert nicht (z.B. existiert keine VPN-Verbindung mit dem angegebenen Namen).
ESYNVPN001	Die VPN-Verbindung wurde erfolgreich aufgebaut, wurde dann aber unterbrochen (z.B. aufgrund einer Netzwerkunterbrechung). Die Verbindung muss deaktiviert und neu aufgebaut werden. Verwenden Sie den Befehl *synstat*, um den Status der VPN-Verbindung zu ermitteln.
EVDIFFALG1	Während des Handshaking zu Beginn des Aufbaus der VPN-Verbindung (Negotiation von ISAKMP-SA) konnten sich die Geräte nicht auf die Stärke der Schlüssel oder die kryptographischen Algorithmen, die in der ersten Phase verwendet werden, einigen.
EVDIFFALG2	Während des Handshaking zu Beginn des Aufbaus der VPN-Verbindung (Negotiation von IPsec-SA) konnten sich die Geräte nicht auf die Stärke der Schlüssel oder die kryptographischen Algorithmen, die in der zweiten Phase verwendet werden, einigen.
EVIFDOWN	Die Netzwerkschnittstelle, über die die VPN-Verbindungen aufgebaut werden sollen, verfügt über keinen Uplink.
EVPEERNOENT1	Die Remote-VPN-Gegenstelle kennt keine VPN-Verbindung, die den Kriterien für die erste IKE-Phase (Negotiation von ISAKMP-SA) entspricht. Vermutlich ist die Konfiguration des mGuard oder der Gegenstelle nicht korrekt.
EVPEERNOENT2	Die Remote-VPN-Gegenstelle kennt keine VPN-Verbindung, die den Kriterien für die zweite IKE-Phase (Negotiation von IPsec-SA) entspricht. Vermutlich ist die Konfiguration des mGuard oder der Gegenstelle nicht korrekt.
EVTOUT1RESP	Der mGuard hat auf seine erste Meldung zum Aufbau der VPN-Verbindung keine Antwort der VPN-Gegenstelle erhalten.
EVTOUTWRESP	Der mGuard hat keine Antwort der Remote-VPN-Gegenstelle erhalten, nachdem diese auf mindestens eine Meldung geantwortet hatte.
OKCONFPULL	Der Test-Download eines Konfigurationsprofils vom HTTPS-Servers war erfolgreich.
OKVACT	Die VPN-Verbindung war beim Aufruf des Befehls *synup* bereits aufgebaut.
OKVDOWN	Die VPN-Verbindung wurde erfolgreich deaktiviert.
OKVNOTACT	Die VPN-Verbindung, die mit dem Befehl *syndown* deaktiviert werden sollte, war schon deaktiviert.
OKVST1	Der Status der angegebenen VPN-Verbindung wurde erfolgreich ermittelt.
OKVUP	Die VPN-Verbindung wurde erfolgreich aufgebaut.

1.4.3.3 cmd=synup

Dieser Befehl aktiviert eine VPN-Verbindung. Der Name der VPN-Verbindung muss mit dem Parameter *name* angegeben werden. Dieser Befehl wird synchron ausgeführt und gibt zurück, sobald ein bestimmter Status erreicht wurde. Der Antworttext enthält Fortschrittsmeldungen bezüglich des Aufbaus der VPN-Verbindung sowie eine finale Meldung mit dem Gesamtergebnis.

Beispiel: Aktivierung der VPN-Verbindung mit dem Namen Service

wget […] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?cmd=synup&name=Service'

Antwort:

```
P synup name=Service1
P deviceinfo uptime=9508.73 tstamp= 20120907095258a serial=2004010272 hostname=mguard
P vpnconn uptime=9508.79 id=MAI0003584192 gw=77.245.33.67
P dnslookup uptime=9508.83 ip=77.245.33.67
P routeinfo uptime=9508.87 via=ext1(10.1.0.48) ifstate=up
...
P IKEv1 uptime=9509.33 newstate=main-i2
...
P IKEv1 uptime=9509.88 newstate=main-i4
P IKEv1 uptime=9509.93 isakmp-sa=established id=#13
...
P IKEv1 uptime=9510.31 newstate=quick-i2 dpd=on
P IKEv1 uptime=9510.34 ipsec-sa=established id=#14 msg=IPsec SA 1 out of 1 is established on this side.
R OKVUP uptime=9510.36 msg=The connection is established on this side.
```

Wenn der mGuard den Befehl *synup* ausführt, führt er folgende Schritte aus:

1. Auflösung des Namens des Remote-VPN-Gateways in eine IP-Adresse (falls erforderlich).
2. Bestimmung der Netzwerkschnittstelle, über die die VPN-Verbindung aufgebaut werden soll und ihrer Konnektivität.

Die Ergebnisse beider Schritte werden in den Zeilen *dnslookup* und *routeinfo* angezeigt. Nur wenn diese Schritte erfolgreich durchgeführt wurden, baut der mGuard die VPN-Verbindung weiter auf. Erhält der mGuard keine Antwort von der Remote-VPN-Gegenstelle, sendet er einen *IKE-Ping* um zu überprüfen, ob die Gegenstelle verfügbar ist, und gibt das Ergebnis aus.

Antwortmuster

Eine Antwort des Befehls *synup* besteht aus mehreren Fortschrittsmeldungen und einer finalen Meldung mit dem Gesamtergebnis. Folgende Struktur zeigt den Fall einer erfolgreich aufgebauten VPN-Verbindung.

Antwort bestehend aus Fortschrittsmeldungen *(pogress messages = P)* und einer finalen Meldung *(final message = R).*

P synup name=**vpn_name**
P deviceinfo uptime=… tstamp=… serial=**XXXX** hostname=**string**
P vpnconn uptime=… id=**vNNN** gw=**hostname/IP**
P dnslookup uptime=… ip=**IP**
P routeinfo uptime=… via=**IF(IP)** ifstate=**up/down/error**
P IKEv1 uptime=… newstate=**status** [**key=value**…] send=…
P IKEv1 uptime=… state=**status** [**key=value** …] rcvd=…
P IKEv1 uptime=… newstate=**status**
P IKEv1 uptime=… newstate=**status** [**key=value** …] send=…
P IKEv1 uptime=… state=status [**key=value** …] rcvd=…
P IKEv1 uptime=… newstate=**status**
P IKEv1 uptime=… isakmp-sa=**status** [**key=value** …] info=…
P IKEv1 uptime=… newstate=**status** [**key=value**…] send=…
P IKEv1 uptime=… state=**status** [key=value …] rcvd=…
P IKEv1 uptime=… newstate=**status**
P IKEv1 uptime=… newstate=**status** [**key=value** …] send=…
P IKEv1 uptime=… ipsec-sa=**status** [**key=value** …] info=…
R OKVUP tstamp=… msg=VPN connection is established.

Fortschrittsmeldungen

Die Antwort beginnt immer mit den fünf Fortschrittsmeldungen *synup, deviceinfo*, *vpnconn*, *dnslookup* und *routeinfo*:

synup	Zeigt den gegebenen Befehl *synup* mit seinem Parameter *name* an

<table>
<tr><td>deviceinfo</td><td colspan="4">Diese Meldung gibt Informationen zum mGuard. Das Format dieser Meldung ist:
P deviceinfo uptime=… tstamp=… serial=XXXX hostname=string
Die Bedeutung der Felder ist wie folgt:</td></tr>
<tr><td></td><td>uptime=</td><td colspan="3">Betriebszeit des mGuard seit der letzten Inbetriebnahme. Der Wert wird in Sekunden mit Nachkommastellen angezeigt. Beispiel: uptime=75178.32</td></tr>
<tr><td></td><td>tstamp=</td><td colspan="3">Datum und Zeitpunkt, zu dem die Meldung generiert wurde. Format: JJJJMMTThhmmssx, dem Datum folgen die Zeit (UTC) und ein Kleinbuchstabe. Die Bedeutung der Buchstaben ist wie folgt:</td></tr>
<tr><td></td><td></td><td>JJJJ</td><td colspan="2">4 Ziffern geben das Jahr an</td></tr>
<tr><td></td><td></td><td>MM</td><td colspan="2">2 Ziffern geben den Monat an</td></tr>
<tr><td></td><td></td><td>TT</td><td colspan="2">2 Ziffern geben den Tag im Monat an</td></tr>
<tr><td></td><td></td><td>hh</td><td colspan="2">2 Ziffern geben die Stunde des Tages an</td></tr>
<tr><td></td><td></td><td>mm</td><td colspan="2">2 Ziffern geben die Minute der Stunde an</td></tr>
<tr><td></td><td></td><td>ss</td><td colspan="2">2 Ziffern geben die Sekunde der Minute an</td></tr>
<tr><td></td><td></td><td>x</td><td colspan="2">Kleinbuchstaben geben den Status der Systemzeit und des Datums des mGuard an.</td></tr>
<tr><td></td><td></td><td></td><td>a</td><td>Systemzeit und -datum noch nicht synchronisiert.</td></tr>
<tr><td></td><td></td><td></td><td>b</td><td>Systemzeit wurde manuell eingestellt oder mittels eines unpräzisen Zeitstempels synchronisiert, der alle 2 Stunden im Dateisystem des mGuard gemeldet ist.</td></tr>
<tr><td></td><td></td><td></td><td>c</td><td>Die Systemzeit wurde mithilfe der gepufferten Echtzeituhr synchronisiert, die manuell oder einmalig über NTP synchronisiert wurde.</td></tr>
<tr><td></td><td></td><td></td><td>d</td><td>Systemzeit einmalig mit einem NTP-Server synchronisiert.</td></tr>
<tr><td></td><td></td><td></td><td>e</td><td>Systemzeit regelmäßig mit einem NTP-Server synchronisiert.</td></tr>
<tr><td></td><td></td><td></td><td colspan="2">Trifft mehr als ein Fall zu, wird der letzte der alphabetischen Reihenfolge angezeigt.</td></tr>
<tr><td></td><td colspan="4">serial= Seriennummer des Gerätes. Leerzeichen werden durch Unterstriche ersetzt.</td></tr>
<tr><td></td><td colspan="4">hostname= Hostname des mGuard.</td></tr>
</table>

vpnconn	Spezielle Konfigurationseigenschaften der VPN-Verbindung. Das Format dieser Meldung ist wie folgt: **P vpnconn uptime=… id=vNNN gw=hostname/IP** Die Bedeutung der Felder ist wie folgt:		
	uptime=	Betriebszeit des mGuard seit der letzten Inbetriebnahme. Der Wert wird in Sekunden mit Nachkommastellen angezeigt. Beispiel: uptime=75178.32	
	id=	Der interne Name der VPN-Verbindung auf dem mGuard, unter dem die Verbindung aufrecht erhalten wird.	
	gw=	Remote-VPN-Gateway der VPN-Verbindung.	

dnslookup	Ergebnis der Auflösung des Hostnames der Remote-VPN-Gegenstelle in eine IP-Adresse. Das Format dieser Meldung ist wie folgt: **P dnslookup uptime=… ip=IP** Die Bedeutung der Felder ist wie folgt:		
	uptime=	Betriebszeit des mGuard seit der letzten Inbetriebnahme. Der Wert wird in Sekunden mit Nachkommastellen angezeigt. Beispiel: uptime=75178.32	
	ip=	IP-Adresse der VPN-Gegenstelle.	

routeinfo	Netzwerkschnittstelle, über die der mGuard versucht, die VPN-Verbindung und den Schnittstellenstatus aufzubauen. Das Format dieser Meldung ist wie folgt: **P routeinfo uptime=… via=IF(IP) ifstate=up/down/error** Die Bedeutung der Felder ist wie folgt:		
	uptime=	Betriebszeit des mGuard seit der letzten Inbetriebnahme. Der Wert wird in Sekunden mit Nachkommastellen angezeigt. Beispiel: uptime=75178.32	
	via=	Netzwerkschnittstelle, über die der mGuard versucht, die VPN-Verbindung aufzubauen. Mögliche Werte sind "ext1", "ext2", "int" "dmz0" und "dial-in".	
	ifstate=	Status der Netzwerkschnittstelle. Mögliche Werte sind:	
		up	Netzwerkschnittstelle betriebsbereit.
		down	Netzwerkschnittstelle wird betriebsbereit, sobald der Verkehr ankommt, der durch sie weitergeleitet werden soll.
		error	Netzwerkschnittstelle nicht betriebsbereit. In diesem Fall gibt der Befehl *synup* in der finalen Meldung EVIFDOWN zurück.

Der mGuard kann die Verbindung zur Remote-VPN-Gegenstelle nicht aufbauen, obwohl die vorherigen Schritte erfolgreich ausgeführt wurden; der mGuard prüft mithilfe eines IKE-Pings, ob die Remote-Site auf IKE-Meldungen antwortet. Die Prüfung wird ausgelassen wenn die IKE-Meldung schon während des Verbindungsaufbaus mit der Gegenstelle ausgetauscht wurde.

<table>
<tr><td rowspan="6">ikeping</td><td colspan="3">Ergebnis des IKE-Ping. Das Format dieser Meldung ist wie folgt:
P ikeping uptime=… to=IP:PORT via=IF response=yes|no|error
Die Bedeutung der Felder ist wie folgt:</td></tr>
<tr><td>uptime=</td><td colspan="2">Betriebszeit des mGuard seit der letzten Inbetriebnahme. Der Wert wird in Sekunden mit Nachkommastellen angezeigt. Beispiel: uptime=75178.32</td></tr>
<tr><td>to=</td><td colspan="2">IP-Adresse und Portnummer des IKE-Ping-Ziels.</td></tr>
<tr><td>via=</td><td colspan="2">Netzwerkschnittstelle, über die der IKE-Ping gesendet wurde. Mögliche Werte sind: "ext1", "ext2", "int", "dmz0" und "dial-in".</td></tr>
<tr><td rowspan="4">response=</td><td colspan="2">Gibt Auskunft darüber, ob der mGuard rechtzeitig eine Antwort auf den IKE-Ping erhalten hat. Mögliche Werte:</td></tr>
<tr><td>yes</td><td>Der mGuard hat eine Antwort der VPN-Gegenstelle erhalten.</td></tr>
<tr><td>no</td><td>Der mGuard hat innerhalb eines bestimmten Zeitraums keine Antwort der VPN-Gegenstelle erhalten.</td></tr>
<tr><td>error</td><td>Der mGuard konnte keinen IKE-Ping senden.</td></tr>
</table>

Weitere Fortschrittsmeldungen werden während des Aufbaus der VPN-Verbindung angezeigt. Im Falle eines Versagens wird direkt eine finale Meldung angezeigt.

<table>
<tr><td>IKEv1</td><td colspan="3">Diese Meldung wird angezeigt wenn
– der mGuard ein IKEv1-Paket erhalten oder gesendet hat,
– eine Phase des Verbindungsaufbaus abgeschlossen ist.
Die Meldung kann mehrere Textfelder mit Werten enthalten. Einige von ihnen können die angebotenen oder ausgewählten Kryptoalgorithmen anzeigen.
Das Format dieser Meldung ist wie folgt:
P IKEv1 uptime=… newstate=state [key=value …] send=…
P IKEv1 uptime=… state=state [key=value …] rcvd=…
P IKEv1 uptime=… newstate=state
P IKEv1 uptime=… isakmp-sa=status id=NN info=… oder
P IKEv1 uptime=… ipsec-sa=established id=NN info=…
Die Bedeutung der Felder, die auftreten können, ist wie folgt:</td></tr>
<tr><td></td><td>uptime=</td><td colspan="2">Betriebszeit des mGuard seit der letzten Inbetriebnahme. Der Wert wird in Sekunden mit Nachkommastellen angezeigt. Zum Beispiel: uptime=75178.32</td></tr>
<tr><td></td><td>newstate=</td><td colspan="2">Statusänderung während des Aufbaus der VPN-Verbindung. Der Wert ist der Name des neuen Status.</td></tr>
<tr><td></td><td>state=</td><td colspan="2">Aktueller Status der VPN-Verbindung.</td></tr>
<tr><td></td><td>send=</td><td colspan="2">Details zu einem gesendeten Paket.</td></tr>
<tr><td></td><td>rcvd=</td><td colspan="2">Details zu einem erhaltenen Paket.</td></tr>
<tr><td></td><td rowspan="3">isakmp-sa=</td><td colspan="2">Abschlussstatus der ersten Phase. Mögliche Werte sind:</td></tr>
<tr><td>established</td><td>Eine neue ISAKMP Security Association (ISAKMP-SA) wurde aufgebaut.</td></tr>
<tr><td>reused</td><td>Eine geeignete ISAKMP-SA wurde bereits für eine andere VPN-Verbindung aufgebaut. Sie wurde für diese wieder verwendet.</td></tr>
<tr><td></td><td>ipsec-sa=</td><td colspan="2">Abschlussstatus der zweiten Phase. Der Wert ist immer "established" (aufgebaut).</td></tr>
<tr><td></td><td>id=</td><td colspan="2">Kennzeichner der ersten oder zweiten Phase. Diese Kennzeichner werden während der Laufzeit intern vom mGuard verwendet. Wird eine ISAKMP-SA wiederverwendet, kann der Kennzeichner für die Suche nach dem Befehl synup verwendet werden, der sie aufgebaut hat.</td></tr>
</table>

Finale Meldung

Wurde die VPN-Verbindung erfolgreich aufgebaut, gibt der Befehl entweder **OKVUP** oder **OKVACT** zurück.

Andernfalls wird einer der folgenden Werte zurückgegeben: **EINVAL, EAMBIGUOUS, ENOENT, ESYNVPN001, EBUSY, EVLOOKUPGW, EVLOOKUPROUT, EVIFDOWN, EVTOUT1RESP, EVTOUTWRESP, EVDIFFALG1, EVDIFFALG2, EVPEERNOENT1, EVPEERNOENT2.**

Erklärungen zu diesen Codes entnehmen Sie bitte „Antwortcode“ auf Seite 9.

1.4.3.4 cmd=synstat

Dieser Befehl ermittelt den Status einer VPN-Verbindung. Der Name der VPN-Verbindung muss mit dem Parameter *name* angegeben werden.

Beispiel: Ermittlung des Status der VPN-Verbindung mit dem Namen *Service*

wget […] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?cmd=synstat&name=Service'

Antwort:

```
R OKVST1 id=MAI0003584192 enabled=no activated=yes ike=OK ipsec=OK
```

Konnte der Status der VPN-Verbindung erfolgreich ermittelt werden, wird **OKVST1** mit folgender zusätzlicher Information zurückgegeben:

OKVST1	Der mGuard hat den Status der VPN-Verbindung erfolgreich ermittelt. Das Format dieser Meldung ist wie folgt: **R OKVST1 id=id enabled=yesno1 activated=yesno2 ike=stat1 ipsec=stat2** Die Bedeutung der Felder ist wie folgt:		
	id=	Interner Kennzeichner (*internal identifier*) der VPN-Verbindung, der während der Laufzeit vom mGuard verwendet wird. Dies ist nicht der konfigurierte Name der VPN-Verbindung.	
	enabled=	Zeigt an, ob die VPN-Verbindung auf dem mGuard als "*enabled*" (aktiviert) konfiguriert ist oder nicht. Mögliche Werte sind:	
		yes	VPN-Verbindung aktiviert.
		no	VPN-Verbindung deaktiviert.
	activated=	Zeigt an, ob die VPN-Verbindung "aushilfsweise aktiv" ist, was der Fall ist, wenn die VPN-Verbindung mit den Befehlen **synup** oder **up** durch das *CGI-Script nph-vpn.cgi* oder mit CMD-Kontakt aufgebaut wurde. Mögliche Werte sind:	
		yes	Aushilfsweise aktiv
		no	Nicht aushilfsweise aktiv
	ike=	Status der zu dieser VPN-Verbindung gehörenden ISAKMP Security Association (ISAKMP-SA). Dieses Feld ist nur vorhanden, wenn die VPN-Verbindung "aushilfsweise aktiv" ist. Mögliche Werte sind:	
		NAME	ISAKMP-SA wird aufgebaut. ISAKMP-SA hat den Status **NAME**. Der Wert von **NAME** unterscheidet sich von den anderen Werten "OK", "EXP" oder "DEAD".
		OK	ISAKMP-SA ist aufgebaut und kann verwendet werden.
		EXP	ISAKMP-SA abgelaufen. Wurde noch nicht erneuert.
		DEAD	ISAKMP-SA existiert nicht für diese VPN-Verbindung.
	ipsec=	Status der zu dieser VPN-Verbindung gehörenden IPsec ISAKMP Security Association (IPsec-SA). Wird nur angezeigt, wenn die VPN-Verbindung "aushilfsweise aktiv" ist. Mögliche Werte und ihre Bedeutungen:	
		NAME	IPsec-SA wird aufgebaut. IPsec-SA hat den Status **NAME**. Der Wert von **NAME** unterscheidet sich von den anderen Werten "OK", "EXP" oder "DEAD".
		OK	IPsec-SA ist aufgebaut und kann verwendet werden.
		EXP	IPsec-SA abgelaufen. Wurde noch nicht erneuert.
		DEAD	IPsec-SA existiert nicht für diese VPN-Verbindung.

Konnte der Status der VPN-Verbindung nicht erfolgreich ermittelt werden, wird einer der folgenden Werte zurückgegeben: **EINVAL, EAMBIGUOUS, ENOENT**.

Erklärungen zu diesen Codes entnehmen Sie bitte „Antwortcode“ auf Seite 9.

1.4.3.5 cmd=syndown

Dieser Befehl deaktiviert eine VPN-Verbindung. Der Name der VPN-Verbindung muss mit dem Parameter *name* angegeben werden.

Beispiel: Deaktivierung der VPN-Verbindung mit dem Namen *Service*

wget […] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?cmd=syndown&name=Service'

Antwort:

```
R OKVDOWN
```

Wurde die VPN-Verbindung erfolgreich deaktiviert, gibt der Befehl entweder **OKVDOWN** oder **OKVNOTACT** zurück.

Andernfalls wird einer der folgenden Werte zurück gegeben: **EINVAL, EAMBIGUOUS, ENOENT.**

Erklärungen zu diesen Codes entnehmen Sie bitte „Antwortcode“ auf Seite 9.

1.4.4 Zentrale VPN-Gateway-Befehle

Die in den vorhergehenden Kapitels erklärten Befehle werden auf Remote-mGuards verwendet, die VPN-Verbindungen zu einem zentralen VPN-Gateway aufbauen. Zwei weitere Befehle sind speziell für die Verwendung auf einem zentralen VPN-Gateway verfügbar, das das Feature *VPN-Tunnelgruppe* verwendet. *VPN-Tunnelgruppe* ermöglicht es vielen Remote-mGuards, eine VPN-Verbindung zu einer einzelnen konfigurierten VPN-Verbindung auf dem zentralen VPN-Gateway aufzubauen.

Eine *VPN-Tunnelgruppenverbindung* hat *%any* als Gegenstellenadresse und das angegebene VPN-Netzwerk ist ein großes Netzwerk (z.B. 192.168.0.0/16), inklusive aller Netzwerke der Remote-mGuards (z.B. 192.168.**1**.0/24, 192.168.**2**.0/24, 192.168.**3**.0/24 etc.).

Die VPN-Verbindung nimmt gleichzeitig ISAKMP-SAs von vielen unterschiedlichen Remote-mGuards an. Es wird erwartet, dass jeder Remote-mGuard eine oder mehrere IPsec-SAs im Tunnelmodus aufbaut, wo der Remote-mGuard ein eindeutiges Subnetz des konfigurierten Remote-Netzwerkes für jedes Tunnelende anfordert.

Hat das zentrale VPN-Gateway nur eine konfigurierte *VPN-Tunnelgruppe*, mit der sich alle Remote-mGuards verbinden, kann nicht ermittelt werden, ob eine aktive Verbindung zu einem einzelnen Remote-mGuard besteht. Natürlich kann *cmd=status* ohne Angabe des VPN-Verbindungsnamens verwendet werden (siehe Kapitel 1.4.2.3), aber dieser Befehl würde den Status aller Tunnel ermitteln, was für die Statusabfrage für einen einzelnen Tunnel nicht effizient ist.

Manchmal soll der Administrator des zentralen VPN-Gateways eine bestimmte VPN-Gegenstelle von der VPN-Verbindung löschen. Das ist besonders hilfreich, wenn die VPN-Gegenstelle aus welchen Interoperabilitätsgründen auch immer keinen neuen Tunnel aufbauen kann. IPsec ist ein Standard, aber manchmal erfüllen die Geräte anderer Anbieter nicht alle Anforderungen dieses Standards. Ohne die Option, eine spezifische VPN-Verbindung zu löschen, muss die gesamte *VPN-Tunnelgruppen*konfiguration neu gestartet werden. Das würde dazu führen, dass alle VPN-Tunnel verworfen und wieder aufgebaut werden müssen.

1.4.4.1 cmd=status, channel=<LNet:RNet>

Dieser Befehl ermittelt den Status des angegebenen VPN-Tunnels. *LNet* steht für das lokale VPN.Netzwerk, *RNet* für das VPN-Netzwerk der Gegenstelle.

Rückgabewert	Bedeutung
unknown	Dieser Rückgabewert kann zwei Ursachen haben: – Derzeit besteht kein passender Tunnel. Es besteht weder ein konfigurierter und aktiver Tunnel mit den angegebenen Netzwerken noch ein passender aufgebauter Tunnel einer *VPN-Tunnelgruppe*. – Ein passender Kanal ist aufgrund eines Fehlers inaktiv (zum Beispiel weil das externe Netzwerk gestört ist oder weil der Hostname der Gegenstelle nicht in eine IP-Adresse aufgelöst werden konnte (DNS)).
ready	Die Verbindung lässt eingehende Anfragen bezüglich des Tunnelaufbaus zu.
active	Der Tunnel ist aufgebaut.

Beispiel: *wget […] 'https://admin:mGuard@77.245.33.67/nphvpn.cgi?cmd=status&channel=10.1.0.0/16:192.168.23.0/24'*

Antwort:

```
active
```

1.4.4.2 cmd=clear, channel=<LNet:RNet>

Dieser Befehl löscht den angegebenen VPN-Tunnel. *LNet* steht für das lokale VPN-Netzwerk, *RNet* für das VPN-Netzwerk der Gegenstelle.

Rückgabewert	Bedeutung
unknown	Derzeit besteht kein passender Tunnel.
Deleting connection ...	Der Tunnel wird gelöscht.

Beispiel:

wget […] 'https://admin:mGuard@77.245.33.67/nph-vpn.cgi?cmd=clear&channel=10.1.0.0/16:192.168.23.0/24'

Antwort:

```
002 "MAI1693250436_1"[2] 77.245.32.76: deleting connection "MAI1693250436_1"[2] instance  with peer 77.245.32.76 {isakmp=#0/ipsec=#0} cleared
```

1.4.5 cmd=sysinfo

Dieser Befehl ermittelt die Softwareversion, den Hardwarenamen und die Hardware-Revision auf dem mGuard.

Beispiel:

wget […] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?cmd=sysinfo'

Antwort:

```
mGuardProductName=mGuard smart2
mGuardHardware=MGUARD2
mGuardHardwareVersion=00003000
mGuardVersion=7.5.0.default
```

1.5 Interface nph-diag.cgi

1.5.1 cmd=snapshot

Der *Body* der durch den Befehl snapshot produzierten HTTP-Antwort hat binären Inhalt. Er sollte in eine Datei gespeichert werden, vorzugsweise als snapshot.tar.gz. Wird wget verwendet, nutzen Sie dafür die Option *output-document* (*wget … --output-document=snapshot.tar.gz …*).

Der Snapshot enthält die aktuelle Konfiguration des mGuard, seine Laufzeitparameter und alle Log-Einträge. Die Datei enthält außerdem die in diesem Dokument beschriebenen VPN-Diagnosemeldungen der letzten 100 (maximal) VPN-Verbindungsaufbauten, wenn die VPN-Verbindung durch CMD-Kontakt oder durch das Skript nph-vpn.cgi ausgelöst wurde und wenn die Optionen **Archiviere Diagnosemeldungen zu VPN-Verbindungen** (Menü **IPsec VPN >> Global**, Registerkarte *Optionen*) aktiviert sind. Diese Datei enthält keine privaten Informationen wie z. B. private Schlüssel oder Passwörter.

Beispiel: *wget […] 'https://admin:mGuard@192.168.1.1/nph-diag.cgi?cmd=snapshot'*

1.5.2 cmd=testpull

Der mGuard kann sich in einstellbaren Zeitintervallen neue Konfigurationsprofile von einem HTTPS Server holen, wenn der Server sie dem mGuard als Konfigurationsprofil (*.atv) zur Verfügung stellt. Unterscheidet sich eine neue mGuard-Konfiguration von der aktuellen Konfiguration, wird sie automatisch heruntergeladen und aktiviert. Diese Option wird über die Weboberflache im Menü **Verwaltung >> Zentrale Verwaltung** konfiguriert.

Mit diesem Befehl kann geprüft werden, ob eine Konfigurationsdatei vom Konfigurationsserver gemäß den aktuellen Einstellungen des mGuard heruntergeladen werden kann. Der mGuard wendet das Profil nicht an, wenn dieser Befehl erfolgreich ausgeführt wurde. Dieser Befehl gibt in der HTTP-Antwort einen der folgenden Werte zurück:

OKCONFPULL	Der mGuard hat die Konfiguration erfolgreich heruntergeladen. Das Format dieser Meldung ist: **R OKCONFPULL d=digest** Die Bedeutung der Felder ist wie folgt:	
	digest	Alphanumerischer String, den der mGuard an den IDM (MGUARD DM, MGUARD Device Manager) mit der HTTP-Anfrage schickt, um anzuzeigen, welche Version der Konfigurationsdatei heruntergeladen wurde.
ECONFPULL	Download der Konfigurationsdatei fehlgeschlagen. Das Format dieser Meldung ist wie folgt: **F ECONFPULL http-code=code msg=message** Die Bedeutung der Felder ist wie folgt:	
	code	Vom HTTPS-Server zurückgegebener HTTP-Statuscode. Leer, wenn der HTTP-Statuscode aufgrund eines Fehlers auf einem anderen Layer, z.B. auf dem Secure Socket Layer (SSL) nicht übertragen werden konnte.
	message	Diese Meldung gibt den Grund für den Fehler an und kann weitere Informationen enthalten. Sie enthält weiterhin die Fehlermeldung des HTTPS-Servers, wenn der HTTP-Statuscode unbekannt ist.

Beispiel: *wget […] 'https://admin:mGuard@192.168.1.1/nph-diag.cgi?cmd=testpull'*
Antwort:

```
R OKCONFPULL tstamp=20120515094007e d=d12851f0b9801e0df45c5794c7f392c5
```

1.6 Interface nph.action.cgi

Benutzer „root“ und „admin“

Die folgenden Befehle können durch die Benutzer **root** und **admin** ausgeführt werden.

Zeilenaktionen (Row actions)

https://admin:mGuard@192.168.1.1/nph-action.cgi?action=<ACTION>&name=<NAME>

https://admin:mGuard@192.168.1.1/nph-action.cgi?action=<ACTION>&rowid=<ROWID>

Tabelle 1-4 **Zeilenaktionen** – Parameter

Parameter	Beschreibung
name	Verbindungsname, Regelsätze, Integritätsprüfung
rowid	Eindeutige ID aus der Konfiguration (gaiconfig --goto VPN_CONNECTION:0 --get-rowid)

Tabelle 1-5 **Zeilenaktionen** – Aktion

Aktion	Beschreibung
fwrules/inactive	Deaktiviert einen Firewall-Regelsatz
fwrules/active	Aktiviert einen Firewall-Regelsatz
vpn/stop	Stoppt wie „nph-vpn.cgi“ ebenfalls eine IPsec-Verbindung, aber mit geringerer Komplexität
vpn/start	Startet wie „nph-vpn.cgi“ ebenfalls eine IPsec-Verbindung, aber mit geringerer Komplexität
openvpn/stop	Stoppt eine OpenVPN-Verbindung
openvpn/start	Startet eine OpenVPN-Verbindung
cifsim/validaterep	Validiert einen CIFS/IM-Scanbericht
cifsim/check-start	Startet eine CIFS/IM-Prüfung
cifsim/init-start	Erzeugt eine neue CIFS/IM-Integritätsdatenbank
cifsim/cancel	Beendet einen laufenden CIFS/IM-Job
cifsim/erase-db	Löscht die CIFS/IM-Datenbank
cifsim/access-scan	Startet die Zugriffsüberprüfung eines Netzlaufwerks

Benutzerfirewall-Logout

https://admin:mGuard@192.168.1.1/nph-action.cgi?action=userfw/logout&name=<NAME> &ip=<IP>

Tabelle 1-6 Benutzerfirewall-Logout – Parameter

Parameter	Beschreibung
name	Benutzerkennung des eingeloggten Benutzers der Benutzerfirewall
ip	Die aktuelle IP-Adresse des eingeloggten Benutzers der Benutzerfirewall

Tabelle 1-7 Benutzerfirewall-Logout – Aktion

Aktion	Beschreibung
userfw/logout	Meldet den angemeldeten Firewall-Benutzer ab (*Logout*)

Einfache Befehle

(Parameter *name* oder *ID* sind nicht erforderlich)

https://admin:mGuard@192.168.1.1/nph-action.cgi?action=<ACTION>

Tabelle 1-8 Einfache Befehle – Aktionen

Aktion	Beschreibung
switch/purge-arlt	Setzt die Address-Resolution-Tabelle des internen Switch zurück
switch/reset-phy-counters	Setzt den PHY-Zähler des internen Switch zurück

Benutzer „mobile“, „root“ und „admin“

Die folgenden Befehle können durch die Benutzer **mobile**, **root** und **admin** ausgeführt werden. Der Benutzer **mobile** ist ab Firmware-Version 8.3.0 verfügbar.

Mobile Aktionen (Benutzer: mobile / root / admin)

– **Nur mGuard-Firmwareversion 8.3:**
https://admin:mGuard@192.168.1.1/nph-action.cgi?action=gsm/call&dial=<NUMBER>&timeout=<TIMEOUT>

– **mGuard-Firmwareversion 8.3 und 8.4:**
https://admin:mGuard@192.168.1.1/nph-action.cgi?action=gsm/sms&dial=<NUMBER> &msg=<MESSAGE>

Tabelle 1-9 Mobile Aktionen – Parameter

Parameter	Beschreibung
dial	Ziel-Telefonnummer
timeout	Zeit bis zur Beendigung des Anrufs (in Sekunden)
msg	Inhalt der Kurznachricht (ohne Sonderzeichen und Umlaute)

Tabelle 1-10 Mobile Aktionen – Aktionen

Akion	Beschreibung
gsm/call	Startet einen Telefonanruf
gsm/sms	Sendet eine Textnachricht (SMS)

1.7 Interface nph.status.cgi

Die folgenden Befehle können durch die Benutzer **root** und **admin** ausgeführt werden.

Tabelle 1-11 CGI-Status

Parameter	Beschreibung
/network/modem/state	**Status des Modems**
https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/network/modem/state	
Antwort: *online* | *offline*	
/network/ntp_state	**Status der NTP-Zeitsynchronisation**
https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/network/ntp_state	
Antwort: *disabled* | *not_synced* | *synchronized*	
/system/time_sync	**Status der Systemzeitsynchronisation**
https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/system/time_sync	
Antwort: *not_synced* | *manually* | *stamp* | *rtc* | *ntp* | *gps* | *gpslost*	
/ecs/status	**Status des ECS-Speichers**
https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/ecs/status	
Antwort: "1" für nicht präsent, "2" für entfernt, "3" für präsent und in Synchronisation, "4" für nicht in Synchronisation und "8" für allgemeiner Fehler	
/vpn/con	**Status einer VPN-Verbindung**
https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/vpn/con&name=<Verbindungsname>	
Antwort: – */vpn/con/<rowid>/armed=[yes|no]* Zeigt an, ob die Verbindung gestartet wurde oder nicht. – */vpn/con/<rowid>/ipsec=[down|some|up]* Zeigt den IPsec-Status. – */vpn/con/<rowid>/isakmp=[up|down]* Zeigt den ISAKMP-Status. – */vpn/con/<rowid>/sa_count=<number>* Anzahl aufgebauter Tunnel – */vpn/con/<rowid>/sa_count_conf=<number>* Anzahl konfigurierter aktivierter Tunnel	
/fwrules	**Status eines Firewall-Regelsatzes**
https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/fwrules&name=<Regelsatz>	
Antwort: – */fwrules/<rowid>/expires=<seconds since 1.1.1970>* Ablaufzeit – 0 für keine Ablaufzeit – */fwrules/<rowid>/state=[inactive|active]* Aktivitätsstatus des Firewall-Regelsatzes	
/cifs/im	**Status eines Netzlaufwerks in Bezug auf CIFS**
https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/cifs/im&name=<Netzlaufwerksname>	

Tabelle 1-11 CGI-Status

Parameter	Beschreibung
Antwort:	
Aktuell laufende Überprüfung	
– */cifs/im/<rowid>/curr/all=<number>* Anzahl der Dateien	
– */cifs/im/<rowid>/curr/end=<seconds>* Ablaufzeit der aktuell laufenden Überprüfung in Sekunden seit dem 1.1.1970	
– */cifs/im/<rowid>/curr/numdiffs=<number>* Aktuell gefundene Anzahl von Abweichungen.	
– */cifs/im/<rowid>/curr/operation=[none|suspend|check|idb_build]* Aktueller Vorgang	
– */cifs/im/<rowid>/curr/scanned=<number>* Anzahl aktuell überprüfter Dateien	
– */cifs/im/<rowid>/curr/start=<seconds>* Startzeit in Sekunden seit dem 1.1.1970	
Letzte abgeschlossene Überprüfung	
– */cifs/im/<rowid>/last/duration=<number>* Dauer der letzten Überprüfung in Sekunden	
– */cifs/im/<rowid>/last/numdiffs=<number>* Anzahl der Unterschiede, die bei der letzten Überprüfung gefunden wurden.	
– */cifs/im/<rowid>/last/start=<seconds> start time in seconds since 1.1.1970* Startzeitpunkt der letzten abgeschlossenen Überprüfung in Sekunden sei dem 1.1.1970	
– */cifs/im/<rowid>/last/result*=<siehe unten „Letzte Ergebnisse“>	
Log-Ergebnisse	
– */cifs/im/<rowid>/log/fname=<filename of the log file>*	
– */cifs/im/<rowid>/log/hash=<sha1 hash>*	
– */cifs/im/<rowid>/log/result*=<siehe unten „Log-Ergebnisse“>	

Tabelle 1-11 CGI-Status

Parameter	Beschreibung
Letzte Ergebnisse	
– *-1:* Das Netzlaufwerk wurde noch nie überprüft. Eine Integritätsdatenbank liegt wahrscheinlich nicht vor. – *0:* Die letzte Überprüfung wurde erfolgreich abgeschlossen. – *1:* Der Vorgang wurde aufgrund eines nicht erwarteten Ereignisses abgebrochen. Bitte prüfen Sie die Log-Dateien. – *2:* Die letzte Überprüfung wurde nach Ablauf eines Timeouts abgebrochen. – *3:* Die Integritätsdatenbank ist nicht vorhanden oder unvollständig. – *4:* Die Signatur der Integritätsdatenbank ist ungültig. – *5:* Die Integritätsdatenbank wurde mit einem anderen Prüfsummen-Algorithmus erstellt. – *6:* Die Integritätsdantenbank liegt in der falschen Version vor. – *7:* Das zu überprüfende Netzlaufwerk ist nicht verfügbar. – *8:* Das Netzlaufwerk, das als Prüfsummenspeicher verwendet werden soll, ist nicht verfügbar. – *11:* Eine Datei konnte aufgrund eines I/O-Fehlers nicht gelesen werden (siehe Prüfbericht). – *12:* Der Verzeichnisbaum konnte aufgrund eines I/O-Fehlers nicht vollständig durchlaufen werden (siehe Prüfbericht).	
Log-Ergebnisse	
– *unchecked* – Die Signatur wurde noch nicht verifiziert. – *valid* – Die Signatur ist gültig. – *Emissing* – FEHLER: Der Prüfbericht fehlt. – *Euuid_mismatch* – FEHLER: Der Prüfbericht gehört nicht zu diesem Gerät oder ist nicht aktuell. – *Ealgo_mismatch* – FEHLER: Der Prüfbericht wurde mit einem anderen Prüfsummenalgorithmus erstellt. – *Etampered* – FEHLER: Der Prüfbericht wurde verfälscht. – *Eunavail* – FEHLER: Der Prüfbericht ist nicht verfügbar. Prüfen Sie, ob das Netzlaufwerk eingebunden (mounted) ist. – *Eno_idb* – Eine Prüfbericht liegt aufgrund einer fehlenden Integritätsdatenbank nicht vor.	