Innominate

Anwenderhandbuch

mGuard

Software-Release 7.5

2012-11-22

Bezeichnung: UM DE MGUARD 7.5

Revision: 06

Artikel-Nr.: —

Dieses Handbuch ist gültig für das mGuard Software-Release 7.5
bei Verwendung mit den folgenden Geräten der mGuard-Familie:

- mGuard rs4000
- mGuard rs2000
- mGuard centerport
- mGuard industrial rs
- mGuard smart²
- mGuard smart
- mGuard pci² SD
- mGuard pci
- mGuard blade
- mGuard delta²
- mGuard delta
- EAGLE mGuard

Bitte beachten Sie folgende Hinweise

Zielgruppe des Handbuchs

Der in diesem Handbuch beschriebene Produktgebrauch richtet sich ausschließlich an

– Elektrofachkräfte oder von Elektrofachkräften unterwiesene Personen, die mit den geltenden Normen und sonstigen Vorschriften zur Elektrotechnik und insbesondere mit den einschlägigen Sicherheitskonzepten vertraut sind.
– qualifizierte Anwendungsprogrammierer und Software-Ingenieure, die mit den einschlägigen Sicherheitskonzepten zur Automatisierungstechnik sowie den geltenden Normen und sonstigen Vorschriften vertraut sind.

Erklärungen zu den verwendeten Symbolen und Signalwörtern

Dieses Symbol kennzeichnet Gefahren, die zu Personenschäden führen können. Beachten Sie alle Hinweise, die mit diesem Hinweis gekennzeichnet sind, um mögliche Personenschäden zu vermeiden.

Es gibt drei verschiedene Gruppen von Personenschäden, die mit einem Signalwort gekennzeichnet sind.

GEFAHR Hinweis auf eine gefährliche Situation, die – wenn sie nicht vermieden wird – einen Personenschaden bis hin zum Tod zur Folge hat.

WARNUNG Hinweis auf eine gefährliche Situation, die – wenn sie nicht vermieden wird – einen Personenschaden bis hin zum Tod zur Folge haben kann.

VORSICHT Hinweis auf eine gefährliche Situation, die – wenn sie nicht vermieden wird – eine Verletzung zur Folge haben kann.

Dieses Symbol mit dem Signalwort **ACHTUNG** und der dazugehörige Text warnen vor Handlungen, die einen Schaden oder eine Fehlfunktion des Gerätes, der Geräteumgebung oder der Hard-/Software zur Folge haben können.

Dieses Symbol und der dazugehörige Text vermitteln zusätzliche Informationen oder verweisen auf weiterführende Informationsquellen.

Allgemeine Nutzungsbedingungen für Technische Dokumentation

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

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

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

Notes on CE identification

Die Konformitätserklärungen werden in Übereinstimmung mit den EU-Direktiven für die zuständigen Behörden an folgender Stelle bereitgehalten:

Innominate Security Technologies AG
Rudower Chaussee 13
12489 Berlin
Deutschland
Tel. +49 (0)30 92 10 28-0

FCC Note

This note applies to the following devices:
mGuard rs4000, mGuard rs2000, mGuard centerport, mGuard industrial rs, mGuard smart^2, mGuard smart, mGuard pci, mGuard pci^2 SD, mGuard delta, mGuard delta^2, and EAGLE mGuard.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class A digital device, persuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Herausgeber

Innominate Security Technologies AG

Rudower Chaussee 13
12489 Berlin
Deutschland
Tel.: +49 (0)30 92 10 28-0
contact@innominate.com

www.innominate.com

Innominate Dokumentennummer: UG207501C11-038

Inhaltsverzeichnis

1 Einleitung

Der mGuard sichert IP-Datenverbindungen. Dazu vereinigt das Gerät folgende Funktionen:

– Netzwerkkarte (mGuard pci² SD, mGuard pci), Switch (mGuard delta)
– VPN-Router (VPN - **V**irtuelles **P**rivates **N**etzwerk) für sichere Datenübertragung über öffentliche Netze (Hardware-basierte DES-, 3DES- und AES-Verschlüsselung, IPsec Protokoll)
– Konfigurierbare Firewall für den Schutz vor unberechtigtem Zugriff. Der dynamische Paketfilter untersucht Datenpakete anhand der Ursprungs- und Zieladresse und blockiert unerwünschten Datenverkehr.

Die Konfiguration des Gerätes erfolgt einfach mit einem Web-Browser.

Weiterführende Informationen finden Sie auf der Webseite von Innominate: www.innominate.com.

Netzwerk-Features

– Stealth (Auto, Static, Multi), Router (Static, DHCP-Client), PPPoE (für DSL), PPTP (für DSL) und Modem
– VLAN
– DHCP-Server/Relay auf den internen und externen Netzwerkschnittstellen
– DNS-Cache auf der internen Netzwerkschnittstelle
– Administration über HTTPS und SSH
– Optionales Umschreiben von DSCP/TOS-Werten (Quality of Service)
– Quality of Service (QoS)
– LLDP
– MAU-Management
– SNMP

Firewall-Features

– Stateful Packet Inspection
– Anti-Spoofing
– IP-Filter
– L2-Filter (nur im Stealth Mode)
– NAT mit FTP-, IRC- und PPTP-Unterstützung (nur in den Router-Modi)
– 1:1-NAT (nur im Netzwerk-Modus *Router*)
– Port-Weiterleitung (nicht im Netzwerk-Modus *Stealth*)
– Individuelle Firewall-Regeln für verschiedene Nutzer (Benutzerfirewall)
– Individuelle Regelsätze als Aktion (Ziel) von Firewall-Regeln (ausgenommen Benutzerfirewall oder VPN-Firewall)

Anti-Virus-Features

– CIFS-Integritätsprüfung von Netzwerklaufwerken auf Veränderung von bestimmten Datei-Typen (z. B. von ausführbaren Dateien).
– Anti-Virus-Scan-Connector zur Unterstützung der zentralen Überwachung von Netzlaufwerken mit Viren-Scannern

VPN-Features

- Protokoll: IPsec (Tunnel- und Transport-Mode)
- IPsec-Verschlüsselung in Hardware mit DES (56 Bit), 3DES (168 Bit), AES (128, 192, 256 Bit)
- Paket-Authentifizierung: MD5, SHA-1
- Internet-Key-Exchange (IKE) mit Main- und Quick-Mode
- Authentisierung über
  - Pre-Shared-Key (PSK)
  - X.509v3-Zertifikate mit Public-Key-Infrastruktur (PKI) mit Certification Authority (CA), optionaler Certificate Revocation List (CRL) und Filtermöglichkeit nach Subjects

  oder
  - Zertifikat der Gegenstelle, z. B. selbstunterschriebene Zertifikate
- Erkennen wechselnder IP-Adressen von Gegenstellen über DynDNS
- NAT-Traversal (NAT-T)
- Dead-Peer-Detection (DPD): Erkennung von IPsec-Verbindungsabbrüchen
- IPsec/L2TP-Server: Anbindung von IPsec/L2TP-Clients
- IPsec-Firewall und 1:1-NAT
- Standard-Route über VPN
- Weiterleiten von Daten zwischen VPNs (Hub and Spoke)
- Abhängig von der Lizenz: bis zu 250 VPN-Kanäle, bei mGuard centerport bis zu 1000 aktive VPN-Kanäle
- Hardware-Beschleunigung für die Verschlüsselung im VPN (außer mGuard centerport)

Weitere Features

- Remote Logging
- Router-/Firewall-Redundanz (Die Funktion „Firewall-Redundanz“ steht in der Firmware-Version 7.0 nicht zur Verfügung.)
- Administration unter Benutzung von SNMP v1-v3 und Innominate Device Manager (IDM)
- PKI-Unterstützung für HTTPS/SSH Remote Access
- Kann über die LAN-Schnittstelle als NTP- und DNS-Server agieren

Support

Bei Problemen mit Ihrem mGuard wenden Sie sich bitte an Ihren Händler.

Zusätzliche Informationen zum Gerät, sowie Release Notes und Software-Updates finden Sie unter folgender Internet-Adresse: www.innominate.com.

1.1 Geräteversionen

Den **mGuard** gibt es in folgenden Geräteausführungen, deren Funktionen weitgehend identisch sind. Alle Geräte sind unabhängig davon einsetzbar, welche Prozessor-Technologie und welches Betriebssystem die angeschlossenen Rechner benutzen.

mGuard rs4000/ mGuard rs2000

Der **mGuard rs4000** ist ein Security Router mit intelligenter Firewall und optionalem IPsec-VPN (zehn bis 250 Tunnel). Er ist für den Einsatz in der Industrie mit hohen Ansprüchen an die dezentrale Sicherheit und Hochverfügbarkeit konzipiert.

Der **mGuard rs2000** ist eine Variante mit einfacher Firewall und integriertem IPsec-VPN (maximal zwei Tunnel). Der Funktionsumfang ist auf das Wesentliche reduziert. Er eignet sich für sichere Fernwartungsszenarien in der Industrie und ermöglicht eine schnelle Inbetriebnahme von robusten, industrietauglichen Feldgeräten für einen störungsfreien, autarken Betrieb.

Beide Varianten unterstützen einen auswechselbaren Konfigurationsspeicher in Form einer SD-Karte. (Die SD-Karten sind nicht im Lieferumfang enthalten). Das lüfterlose Metallgehäuse wird auf eine Tragschiene montiert.

Folgende Konnektivitätsoptionen stehen zur Verfügung

mGuard rs4000: (LAN/WAN)		**mGuard rs2000: (LAN/WAN)**	
TX/TX	Ethernet/Ethernet	TX/TX-VPN	Ethernet/Ethernet + VPN
TX/TX-VPN	Ethernet/Ethernet + VPN		

Bild 1-1 mGuard rs4000/mGuard rs2000

mGuard centerport

mGuard centerport ist in drei Geräteversionen lieferbar, die sich in der Anzahl unterstützter, gleichzeitig aktiver VPN-Tunnel unterscheiden: mGuard centerport, mGuard centerport 250, mGuard centerport 1000.

Innominate mGuard centerport ist ein High-End Firewall / VPN Gateway im 19-Zoll-Format, ideal positioniert als zentrale Netzwerkinfrastruktur für Teleservice-Lösungen. Mit seinen Gigabit Ethernet Schnittstellen und entsprechendem Durchsatz als Router und Stateful Inspection Firewall ist das Gerät auch für den Einsatz im Backbone industrieller Netze geeignet. Als Gateway für Virtuelle Private Netze unterstützt es die VPN-Anbindung beliebig vieler Systeme in VPN Tunnel-Gruppen mit bis zu 1.000 gleichzeitig aktiven Tunneln, alle terminiert an einer einzigen öffentlichen IP-Adresse. Ohne Lastverteilung auf multiple Interfaces leistet es dabei über 300 MBit / s verschlüsselten VPN-Datendurchsatz für gesicherte Teleservices wie Remote Support, Ferndiagnose, Fernwartung und Condition Monitoring großer Mengen von Maschinen und Anlagen über das Internet.

mGuard centerport ist mit der vollständig auf seine Multi-core x86 Prozessorarchitektur portierten mGuard firmware (Version 7.0.0 oder neuer) ausgestattet und natürlich voll kompatibel mit allen mGuard VPN Feldgeräten und dem Innominate Device Manager.

Bild 1-2 mGuard centerport

mGuard industrial rs

Der **mGuard industrial rs** ist in drei Geräteversionen lieferbar:

– mit integriertem Modem
– mit integriertem ISDN-Terminaladapter
– ohne diese Geräte

Er ist dadurch hybrid nutzbar als Firewall/VPN-Router sowohl über Ethernet als auch für serielle Wählverbindungen. Der Namenszusatz „rs“ besagt, dass dieses Gerät in besonderer Weise für gesicherte Remote Services (Ferndiagnose, Fernkonfiguration, Teleservice) geeignet ist. Das Gerät ist für die Montage auf Tragschienen (gemäß DIN EN 60715) konzipiert und ist damit vor allem für den Einsatz im industriellem Umfeld geeignet. .

Bild 1-3 mGuard industrial rs

VPN-Tunnel können per Software- oder Hardware-Schalter initiiert werden. Die Versorgungsspannung ist redundant anschließbar (9 V DC ... 36 V DC).

mGuard smart²

Der **mGuard smart²** ist die kleinste Geräteausführung. Er kann z. B. einfach zwischen Rechner oder lokalem Netz (an LAN-Port des mGuards) und einem vorhandenem Router (an WAN-Port des mGuards) gesteckt werden, ohne dass beim bestehenden System Konfigurationsänderungen oder Treiberinstallationen erforderlich sind. Er ist konzipiert für den schnellen Einsatz im Büro oder unterwegs.

Der mGuard smart² ist eine Weiterentwicklung des **mGuard smart**. In diesem Handbuch wird zur Vereinfachung weitgehend mGuard smart² für beide Ausführungen verwendet. Die beschriebenen Eigenschaften gelten ebenfalls für den mGuard smart. Wenn es Abweichungen zum mGuard smart gibt, wird darauf hingewiesen.

Bild 1-4 mGuard smart²

mGuard pci² SD

Der mGuard pci² SD hat die Form einer PCI-kompatiblen Steckkarte. Es gibt ihn in zwei Ausführungen:

– mGuard pci² SD für Geräte oder Maschinen mit PCI- Bus
– mGuard pcie² SD für Geräte oder Maschinen mit PCI-Express-Bus

In diesem Handbuch wird zur Vereinfachung mGuard pci² SD für beide Ausführungen verwendet.

Der mGuard pci² SD eignet sich für die dezentrale Absicherung von Industrie- und Panel-PCs, einzelnen Maschinen oder Industrie-Robotern. Er verfügt über einen Konfigurationsspeicher in Form einer wechselbaren SD-Karte, die an der Frontseite gut zugänglich ist.

Bild 1-5 mGuard pci² SD

mGuard pci

Diese in einem PCI-Steckplatz einsetzbare Karte **mGuard pci** bietet im *Treibermodus* dem Rechner, in dem die Karte installiert ist, alle mGuard-Funktionen und fungiert zusätzlich als normale Netzwerkkarte.

Im *Power-over-PCI-Modus* kann eine bereits im Rechner vorhandene Netzwerkkarte oder ein anderer Rechner/ein anderes Netz angeschlossen werden.

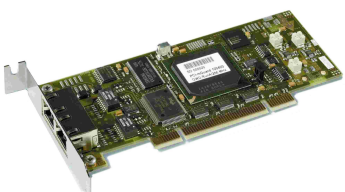


Bild 1-6 mGuard pci

mGuard blade

Das **mGuard bladepack** besteht aus dem mGuard bladebase, das problemlos in Standard 3-U-Racks (19 Zoll) eingebaut werden kann und bis zu 12 mGuard blades zuzüglich einem mGuard blade-Controller aufnimmt. Damit eignet sich diese Geräteausführung vor allem im industriellem Umfeld, um mehrere Server-Systeme individuell und unabhängig voneinander schützen zu können.

Eine zusätzliche serielle Schnittstelle ermöglicht die Fernkonfiguration über eine Telefon-Wählverbindung oder einen Terminal.

Bild 1-7 mGuard blade

mGuard delta²

Der **mGuard delta²** ist prädestiniert für den Einsatz im Desktop-Bereich, in Verteilerräumen, Netzwerkschränken und anderen produktionsnahen Umgebungen mit geringen Anforderungen an eine industrielle Härtung.

Einzelteilnehmer oder Netzwerksegmente können sicher vernetzt und umfassend geschützt werden. Der mGuard delta² eignet sich als Firewall zwischen Büro- und Produktionsnetzen sowie als Security- Router für kleine und mittlere Arbeitsgruppen.

Bild 1-8 mGuard delta²

mGuard delta

Als kompakter LAN Switch (Ethernet/Fast Ethernet) ist der **mGuard delta** für den Anschluss von bis zu 4 LAN-Segmenten konzipiert. Damit eignet sich das Gerät besonders in logisch segmentierten Netzwerkumgebungen, bei denen sich die lokal angeschlossenen Rechner/Netze die mGuard-Funktionen teilen.

Eine zusätzliche serielle Schnittstelle ermöglicht die Konfiguration über eine Telefon-Wählverbindung oder einen Terminal. Mit seinem robusten Metallgehäuse ist der mGuard delta nicht nur als Desktop-Gerät sondern auch zur Unterbringung in Verteilerräumen geeignet.

Bild 1-9 mGuard delta

EAGLE mGuard

Der **EAGLE mGuard** ist für die Montage auf Tragschienen (gemäß DIN EN 60715) konzipiert und ist damit vor allem für den Einsatz im industriellem Umfeld geeignet.

Der optionale Konfigurationsanschluss und die Option zur Herstellung einer Telefon-Wählverbindung über die V.24-Schnittstelle eröffnen weitere Einsatzmöglichkeiten.

Bild 1-10 EAGLE mGuard

2 Typische Anwendungsszenarien

In diesem Kapitel werden verschiedene Anwendungsszenarien für den mGuard skizziert.

- Stealth-Modus
- Netzwerkrouter
- DMZ
- VPN-Gateway
- WLAN über VPN
- Auflösen von Netzwerkkonflikten

2.1 Stealth-Modus

Im **Stealth-Modus** kann der mGuard zwischen einen einzelnen Rechner und das übrige Netzwerk gesetzt werden.

Die Einstellungen (z. B. für Firewall und VPN) können mit einem Web-Browser unter der URL https://1.1.1.1/ vorgenommen werden.

Auf dem Rechner selbst müssen keine Konfigurationsänderungen durchgeführt werden.

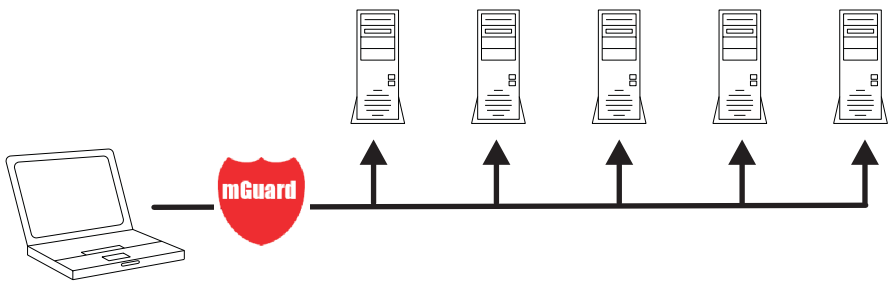


Bild 2-1 Stealth-Modus

2.2 Netzwerkrouter

Der mGuard kann für mehrere Rechner als **Netzwerkrouter** die Internetanbindung bereitstellen und das Firmennetz dabei mit seiner Firewall schützen.

Dazu kann einer der folgenden Netzwerk-Modi des mGuards genutzt werden:

– *Router*, wenn der Internet-Anschluss z. B. über einen DSL-Router oder eine Standleitung erfolgt.
– *PPPoE*, wenn der Internet-Anschluss z. B. per DSL-Modem erfolgt und das PPPoE-Protokoll verwendet wird (z. B. in Deutschland).
– *PPTP*, wenn der Internet-Anschluss z. B. per DSL-Modem erfolgt und das PPTP-Protokoll verwendet wird (z. B. in Österreich).
– *Modem*, wenn der Internet-Anschluss über ein seriell angeschlossenes Modem (Hayes- bzw. AT-Befehlssatz kompatibel) erfolgt.

Bei Rechnern im Intranet muss der mGuard als Standard-Gateway festgelegt sein.

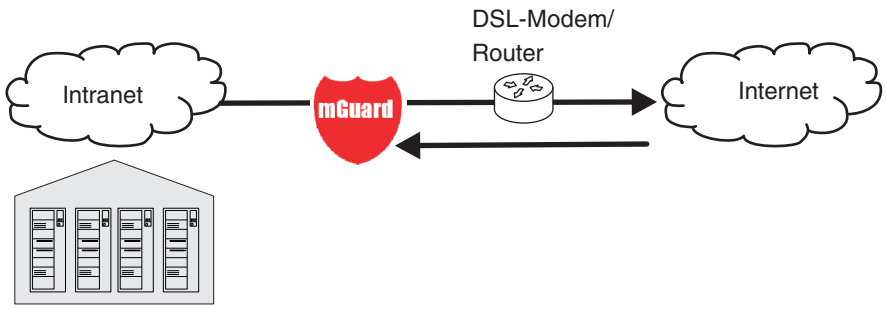


Bild 2-2 Netzwerkrouter

2.3 DMZ

Eine **DMZ** (Demilitarized Zone, deutsch: entmilitarisierte Zone) ist ein geschütztes Netzwerk, das zwischen zwei anderen Netzen liegt. Zum Beispiel kann sich die Webpräsenz einer Firma so in der DMZ befinden, dass nur aus dem Intranet heraus mittels FTP neue Seiten auf den Server kopiert werden können. Der lesende Zugriff per HTTP auf die Seiten ist jedoch auch aus dem Internet heraus möglich.

Die IP-Adressen innerhalb der DMZ können öffentlich oder privat sein, wobei der mit dem Internet verbundene mGuard die Verbindungen mittels Port-Weiterleitung an die privaten Adressen innerhalb der DMZ weiterleitet.

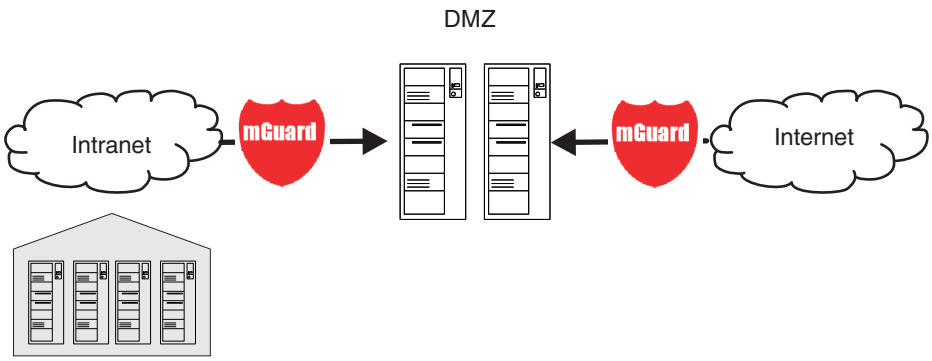


Bild 2-3 DMZ

2.4 VPN-Gateway

Beim **VPN-Gateway** soll Mitarbeitern einer Firma ein verschlüsselter Zugang zum Firmennetz von zu Hause oder von unterwegs zur Verfügung gestellt werden. Der mGuard übernimmt dabei die Rolle des VPN-Gateways.

Auf den externen Rechnern muss dazu eine IPsec-fähige VPN-Client-Software installiert werden und das Betriebssystem muss diese Funktionalität unterstützen. Es kann z. B. Windows 2000/XP eingesetzt werden oder der Rechner wird mit einem mGuard ausgerüstet.

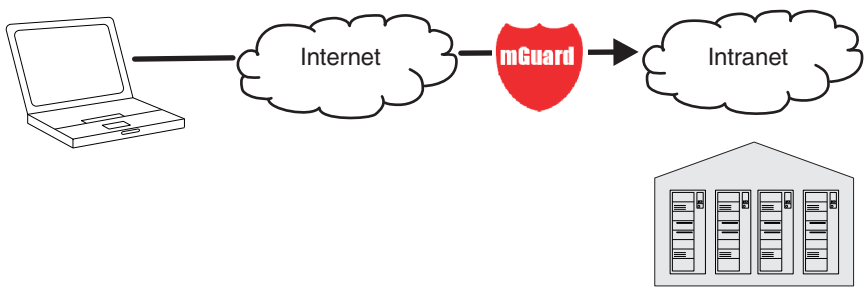


Bild 2-4 VPN-Gateway

2.5 WLAN über VPN

Beim **WLAN über VPN** sollen zwei Gebäude einer Firma über eine mit IPsec geschützte WLAN-Strecke miteinander verbunden werden. Vom Nebengebäude soll zudem der Internetzugang des Hauptgebäudes mitgenutzt werden können.

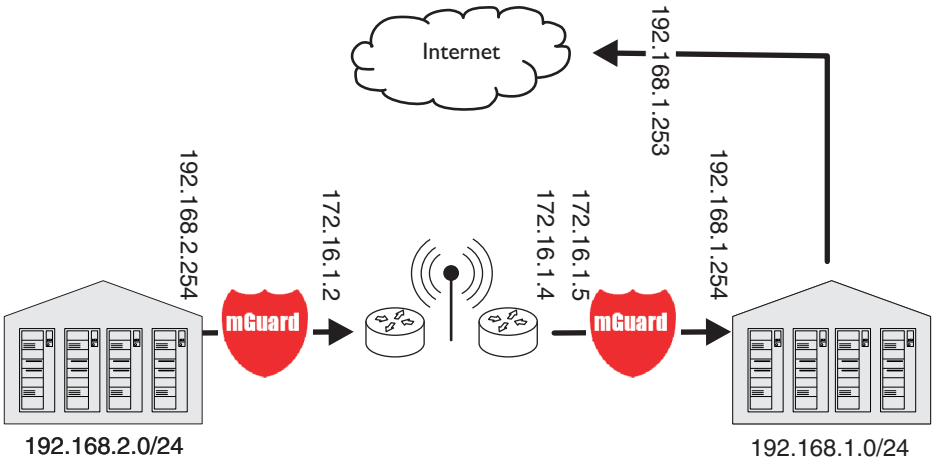


Bild 2-5 WLAN über VPN

In diesem Beispiel wurden die mGuards in den *Router-M*odus geschaltet und für das WLAN ein eigenes Netz mit 172.16.1.x Adressen eingerichtet.

Da vom Nebengebäude aus das Internet über das VPN erreichbar sein soll, wird hier eine Standard-Route über das VPN eingerichtet:

Tunnelkonfiguration im Nebengebäude

Verbindungstyp	Tunnel (Netz <-> Netz)
Adresse des lokalen Netzes	192.168.2.0/24
Adresse des gegenüberliegenden Netzes	0.0.0.0/0

Im Hauptgebäude wird das entsprechende Gegenstück der Verbindung konfiguriert:

Tunnelkonfiguration im Hauptgebäude

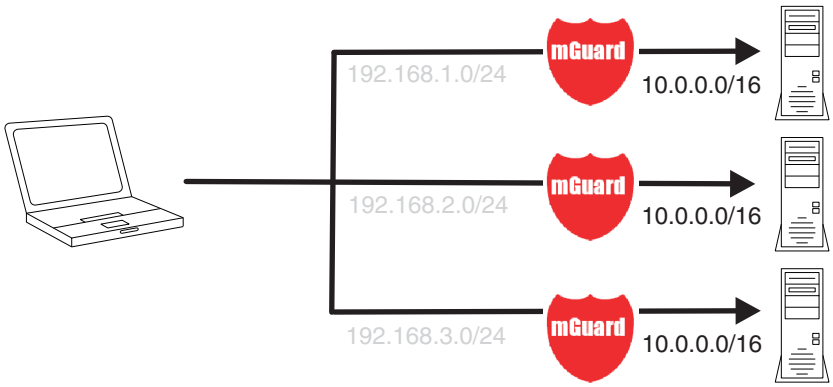
Verbindungstyp	Tunnel (Netz <-> Netz)
Lokales Netz	0.0.0.0
Adresse des gegenüberliegenden Netzes	192.168.2.0/24

Die Standard-Route eines mGuards führt normalerweise über den WAN-Port. In diesem Fall jedoch ist das Internet über den LAN Port erreichbar:

Standard-Gateway im Hauptgebäude:

IP-Adresse des Standard-Gateways	192.168.1.253

2.6 Auflösen von Netzwerkkonflikten



Auflösen von Netzwerkkonflikten

Im Beispiel sollen die Netzwerke auf der rechten Seite von dem Netzwerk oder Rechner auf der linken Seite erreichbar sein. Aus historischen oder technischen Gründen überschneiden sich jedoch die Netzwerke auf der rechten Seite.

Mit Hilfe der mGuards und ihrem 1-zu-1-NAT-Feature können diese Netze nun auf andere Netze umgeschrieben werden, so dass der Konflikt aufgelöst wird.

(1-zu-1-NAT kann im normalen Routing und in IPsec-Tunneln genutzt werden.)

3 Bedienelemente und Anzeigen

3.1 mGuard rs4000/rs2000

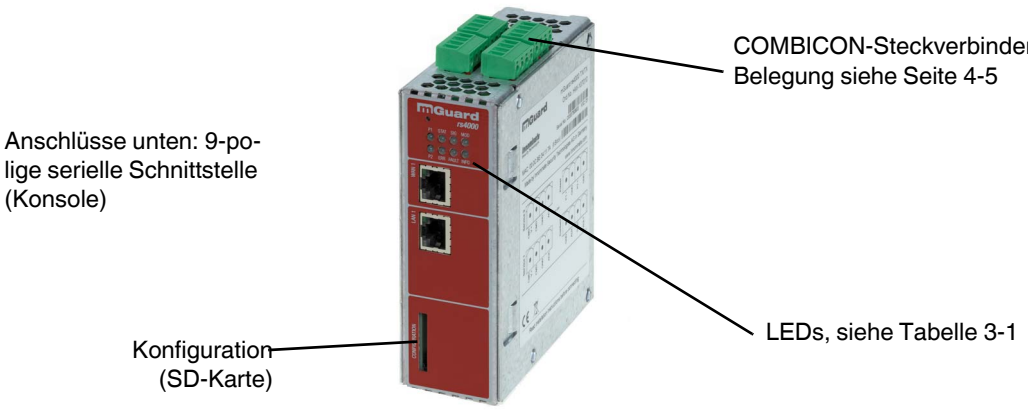


Bild 3-1 Bedienelemente und Anzeigen vom mGuard rs4000

Tabelle 3-1 Anzeigen vom mGuard rs4000 und rs2000

LED	Zustand		Bedeutung
P1	grün	Ein	Stromversorgung 1 ist aktiv
P2	grün	Ein	Stromversorgung 2 ist aktiv (mGuard rs2000: unbelegt)
STAT	grün	Blinkt	**Heartbeat**. Das Gerät ist korrekt angeschlossen und funktioniert.
ERR	rot	Blinkt	**Systemfehler**. Führen Sie einen Neustart durch. – Dazu die Rescue-Taste kurz (1,5 Sek.) drücken. – Alternativ: das Gerät kurz von der Stromversorgung trennen und wieder anschließen. Falls der Fehler weiterhin auftritt, starten Sie die *Recovery-Prozedur* (siehe Seite 8-2) oder wenden Sie sich an Ihren Händler.
STAT+ ERR	abwechselnd grün-rot blinkend		**Bootvorgang**. Nach Anschluss des Gerätes an die Stromversorgungsquelle. Nach einigen Sekunden wechselt diese Anzeige zu Heartbeat.
SIG	–		(nicht belegt)
FAULT	rot	Ein	Der Meldeausgang ist aufgrund eines Fehlers offen (siehe „mGuard rs4000/rs2000 installieren“ auf Seite 4-4). (Während eines Neustarts ist der Meldeausgang unterbrochen.)
MOD	grün	Ein	Verbindung per Modem hergestellt
INFO	grün	Ein	Konfigurierte VPN-Verbindung ist aufgebaut
		Blinkt	Konfigurierte VPN-Verbindung wird auf- oder abgebaut
LAN	grün	Ein	Die LAN/WAN LEDs befinden sich in den LAN/WAN-Buchsen (10/100 und Duplex-Anzeige) **Ethernetstatus**. Zeigt den Status des LAN- bzw. WAN-Ports. Sobald das Gerät am entsprechenden Netzwerk angeschlossen ist, zeigt kontinuierliches Leuchten an, dass eine Verbindung zum Netzwerk-Partner im LAN bzw. WAN besteht. Beim Übertragen von Datenpaketen erlischt kurzzeitig die LED.
WAN	grün	Ein	

3.2 mGuard centerport

Frontseite

Bild 3-2 Bedienelemente und Anzeigen vom mGuard centerport - Frontseite

Tabelle 3-2 Anzeigen vom mGuard centerport

LED	Zustand	Bedeutung
Grün	Ein	Leuchtet, wenn das System eingeschaltet ist
Orange	Ein	Leuchtet, während Festplattenzugriff stattfindet

Frontklappe geöffnet

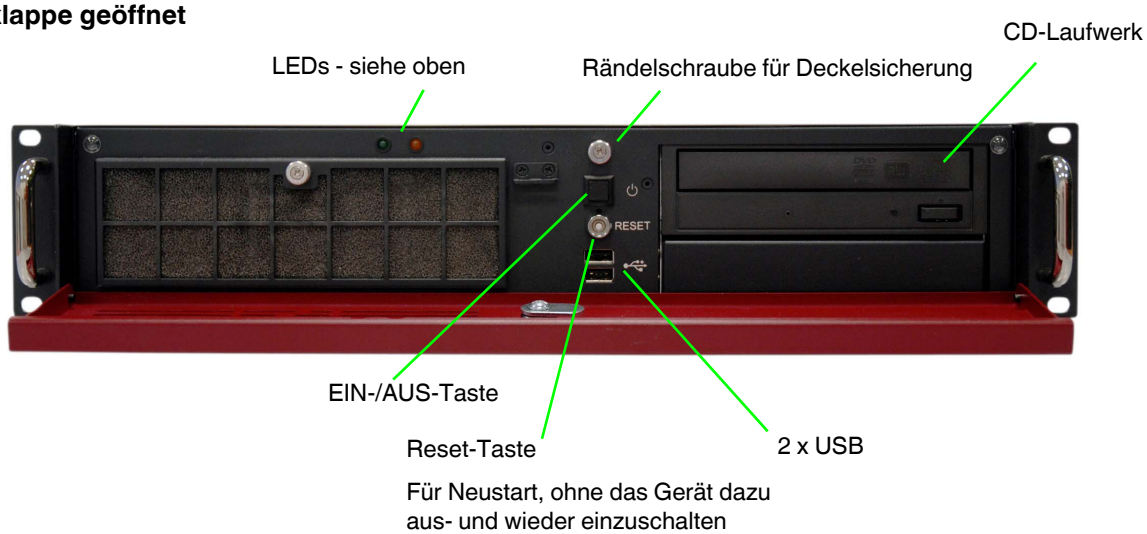


Bild 3-3 Bedienelemente vom mGuard centerport bei geöffneter Frontklappe

3.3 mGuard industrial rs

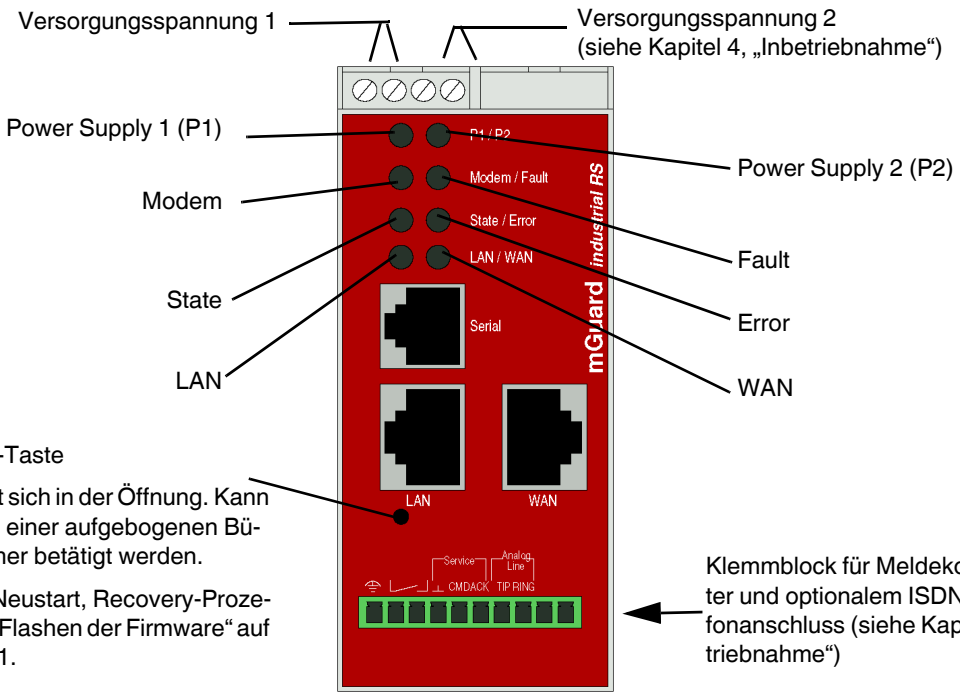


Bild 3-4 Bedienelemente und Anzeigen vom mGuard industrial rs

Tabelle 3-3 Anzeigen vom mGuard industrial rs

LED	Zustand		Bedeutung
P1	grün	Ein	Stromversorgung 1 ist aktiv
P2	grün	Ein	Stromversorgung 2 ist aktiv
Modem	grün	Ein	Verbindung per Modem hergestellt
Fault	rot	Ein	Der Meldekontakt ist aufgrund eines Fehlers offen (siehe „mGuard industrial rs installieren“ auf Seite 4-12, unter „„Meldekontakt“ auf Seite 4-16“). (Während eines Neustarts ist der Meldekontakt unterbrochen.)
State	grün	Blinkt	**Heartbeat**. Das Gerät ist korrekt angeschlossen und funktioniert.
Error	rot	Blinkt	**Systemfehler**. Führen Sie einen Neustart durch. – Dazu die Rescue-Taste kurz (1,5 Sek.) drücken. – Alternativ: das Gerät kurz von der Stromversorgung trennen und wieder anschließen. Falls der Fehler weiterhin auftritt, starten Sie die *Recovery-Prozedur* (siehe „Recovery-Prozedur ausführen“ auf Seite 8-2) oder wenden Sie sich an Ihren Händler.
State + Error	abwechselnd grün-rot blinkend		**Bootvorgang**. Nach Anschluss des Gerätes an die Stromversorgungsquelle. Nach einigen Sekunden wechselt diese Anzeige zu Heartbeat.
LAN	grün	Ein	**Ethernetstatus**. Zeigt den Status des LAN- bzw. WAN-Ports. Sobald das Gerät am entsprechenden Netzwerk angeschlossen ist, zeigt kontinuierliches Leuchten an, dass eine Verbindung zum Netzwerk-Partner im LAN bzw. WAN besteht. Beim Übertragen von Datenpaketen erlischt kurzzeitig die LED.
WAN	grün	Ein	

3.4 mGuard smart²/mGuard smart

Bild 3-5 Bedienelemente und Anzeigen vom mGuard smart²

Tabelle 3-4 Anzeigen vom mGuard smart²

LED	Zustand		Bedeutung
1	grün	Ein	LAN: Verbindung zum Netzwerk-Partner besteht
		Blinkt	LAN: Datenübertragung aktiv
2	rot/grün	Blinkt	**Bootvorgang**. Nach Anschluss des Gerätes an die Stromversorgungsquelle. Nach einigen Sekunden wechselt diese Anzeige zu Heartbeat.
	grün	Blinkt	**Heartbeat**. Das Gerät ist korrekt angeschlossen und funktioniert.
	rot	Blinkt	**Systemfehler**. Führen Sie einen Neustart durch. • Dazu die Rescue-Taste kurz (1,5 Sek.) drücken. • Alternativ: das Gerät kurz von der Stromversorgung trennen und wieder anschließen. Falls der Fehler weiterhin auftritt, starten Sie die *Recovery-Prozedur* (siehe „Recovery-Prozedur ausführen“ auf Seite 8-2) oder wenden Sie sich an Ihren Händler.
3	grün	Ein	WAN: Verbindung zum Netzwerk-Partner besteht
		Blinkt	WAN: Datenübertragung aktiv
1, 2, 3	diverse LED-Leuchtcodes		**Recovery-Modus**. Nach Drücken der **Rescue**-Taste. Siehe „Neustart, Recovery-Prozedur und Flashen der Firmware“ auf Seite 8-1.

3.5 mGuard pci² SD

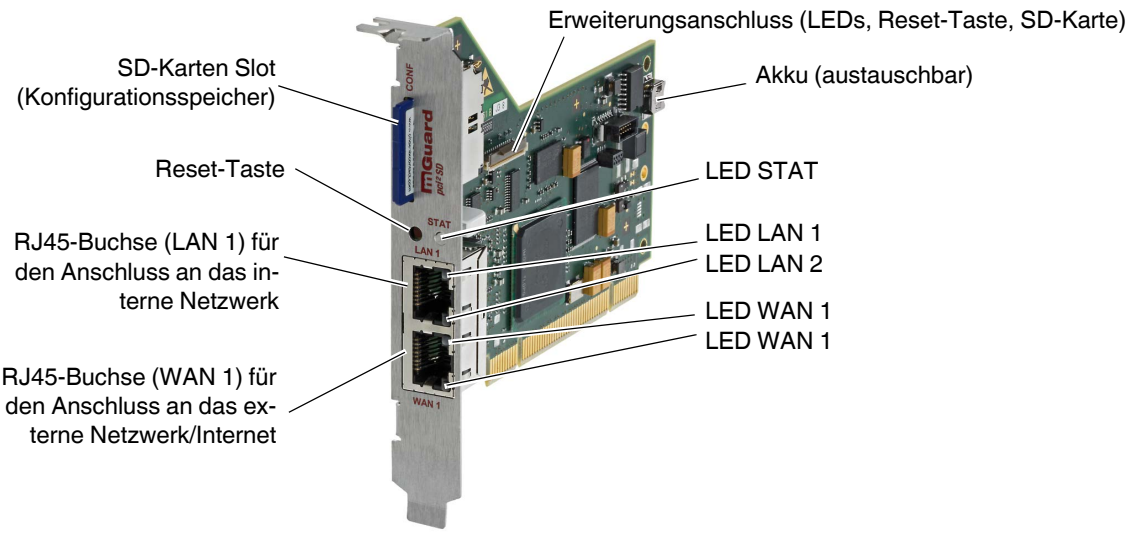


Bild 3-6 Bedienelemente und Anzeigen vom mGuard pci² SD

Tabelle 3-5 Anzeigen vom mGuard pci² SD

LEDs	Zustand		Bedeutung
WAN 1 **LAN 1**	grün	Ein	Vollduplex
		Aus	Halbduplex
WAN 2 **LAN 2**	gelb	Ein	10 MBit/s
		Blinkt	10 MBit/s, Datenübertragung aktiv
	grün	Ein	100 MBit/s
		Blinkt	100 MBit/s, Datenübertragung aktiv
LAN 1 **LAN 2** **WAN 1**	diverse LED-Leuchtcodes		**Recovery-Prozedur/Flashen** Siehe „Neustart, Recovery-Prozedur und Flashen der Firmware“ auf Seite 8-1.
STAT	rot/grün	Blinkt	**Bootprozess.** Nach Anschluss des Gerätes an die Stromversorgungsquelle. Nach einigen Sekunden wechselt diese Anzeige zu Heartbeat.
	grün	Blinkt	**Heartbeat**. Der mGuard ist korrekt angeschlossen und funktionsfähig.
	rot	Blinkt	**Systemfehler**. Führen Sie einen Neustart durch. • Dazu die Reset-Taste kurz (1,5 Sek.) drücken. • Alternativ: das Gerät kurz von der Stromversorgung trennen und wieder anschließen. Falls der Fehler weiterhin auftritt, starten Sie die *Recovery-Prozedur* (siehe „Recovery-Prozedur ausführen“ auf Seite 8-2) oder wenden Sie sich an Ihren Händler.

3.6 mGuard pci

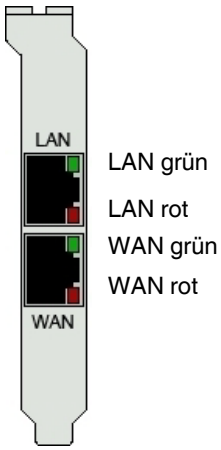


Bild 3-7 Bedienelemente und Anzeigen vom mGuard pci

Tabelle 3-6 Anzeigen vom mGuard pci

LEDs	Zustand		Bedeutung
WAN, LAN	rot	Blinkt	**Bootvorgang**. Nach dem Starten oder Neustarten des Rechners.
WAN	rot	Blinkt	**Systemfehler**. Führen Sie einen Neustart durch. • Dazu die Rescue-Taste kurz (1,5 Sek.) drücken. • Alternativ: das Gerät kurz von der Stromversorgung trennen und wieder anschließen. Falls der Fehler weiterhin auftritt, starten Sie die *Recovery-Prozedur* (siehe „Recovery-Prozedur ausführen“ auf Seite 8-2) oder wenden Sie sich an Ihren Händler.
WAN, LAN	grün	Ein oder Blinkt	**Ethernetstatus**. Zeigt den Status vom LAN bzw. WAN Interface. Sobald das Gerät angeschlossen ist, zeigt kontinuierliches Leuchten an, dass eine Verbindung zum Netzwerk-Partner besteht. Bei der Übertragung von Datenpaketen erlischt kurzzeitig die LED.
WAN **LAN**	rot/grün grün	div. LED-Leuchtcodes	**Recovery-Modus**. Nach Drücken der **Rescue**-Taste*****. Siehe „Neustart, Recovery-Prozedur und Flashen der Firmware“ auf Seite 8-1

***** Beim mGuard pci befindet sich die Rescue-Taste auf der Platine (siehe „Hardware einbauen“ auf Seite 4-25).

3.7 mGuard blade

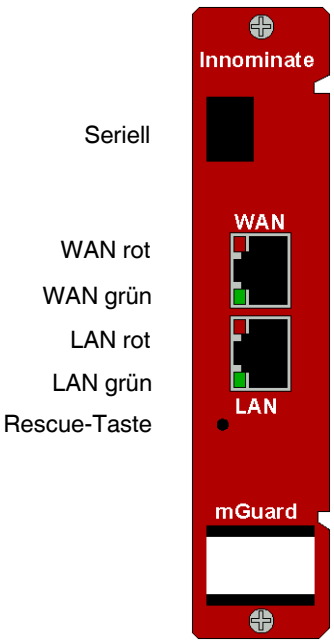


Bild 3-8 Bedienelemente und Anzeigen vom mGuard blade

Tabelle 3-7 mGuard blade

LED	Zustand		Bedeutung
WAN, LAN	rot	Blinkt	**Bootvorgang**. Nach dem Starten oder Neustarten des Rechners.
WAN	rot	Blinkt	**Systemfehler**. Führen Sie einen Neustart durch. • Dazu die Rescue-Taste kurz (1,5 Sek.) drücken Falls der Fehler weiterhin auftritt, starten Sie die *Recovery-Prozedur* (siehe „Recovery-Prozedur ausführen“ auf Seite 8-2) oder wenden Sie sich an Ihren Händler.
WAN, LAN	grün	Ein oder Blinkt	**Ethernetstatus**. Zeigt den Status vom LAN bzw. WAN Interface. Sobald das Gerät angeschlossen ist, zeigt kontinuierliches Leuchten an, dass eine Verbindung zum Netzwerk-Partner besteht. Bei der Übertragung von Datenpaketen erlischt kurzzeitig die LED.
WAN **LAN**	rot/grün grün	div. LED-Leuchtcodes	**Recovery-Modus**. Nach Drücken der **Rescue**-Taste. Siehe „Neustart, Recovery-Prozedur und Flashen der Firmware“ auf Seite 8-1

3.8 mGuard delta²

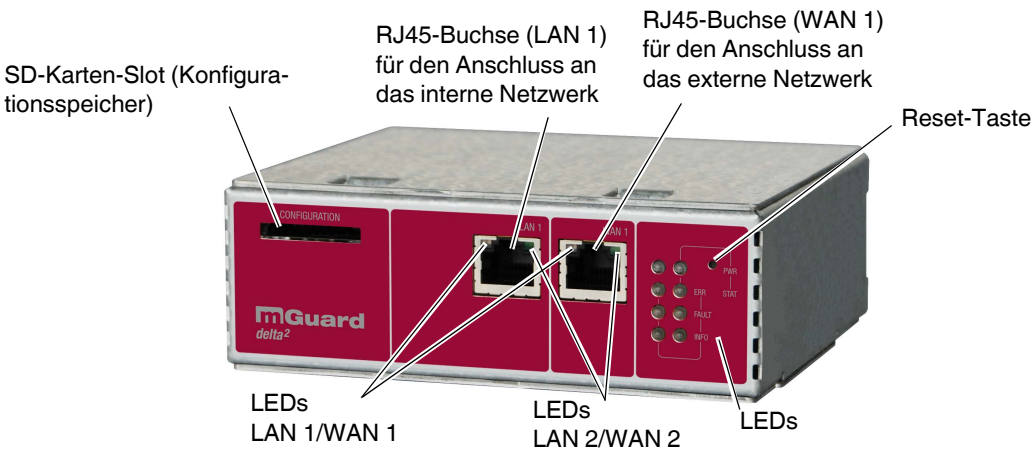


Bild 3-9 Bedienelemente und Anzeigen vom

Tabelle 3-8 Anzeigen vom mGuard delta²

LEDs	Zustand		Bedeutung
WAN 1	grün	Ein	Vollduplex
LAN 1		Aus	Halbduplex
WAN 2	gelb	Ein	10 MBit/s
LAN 2		Blinkt	10 MBit/s, Datenübertragung aktiv
	grün	Ein	100 MBit/s
		Blinkt	100 MBit/s, Datenübertragung aktiv
PWR	grün	Ein	Versorgungsspannung o.k.
STAT	grün	Blinkt	Der mGuard ist betriebsbereit.
ERR	rot	Ein	Systemfehler
FAULT	rot	Ein	mGuard im Zustand Booten oder Flashen
INFO			Nicht belegt

3.9 mGuard delta

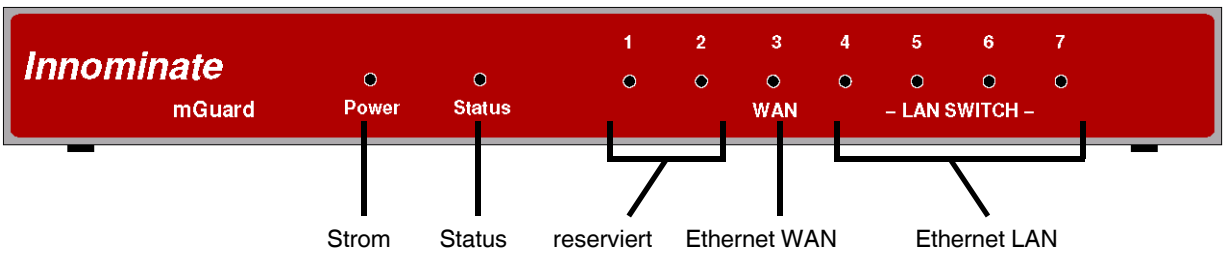


Bild 3-10 Bedienelemente und Anzeigen vom mGuard delta

Tabelle 3-9 Anzeigen vom mGuard delta

LED	Zustand	Bedeutung
Power	Ein	**Die Stromversorgung ist aktiv.**
Status	Ein	Der mGuard startet.
	Heartbeat (aufleuchten, aufleuchten, Pause, ...)	Der mGuard ist bereit.
1, 2	–	**Reserviert**
3 (WAN)	Ein	**Link vorhanden**
	Blinkt	Datentransfer
4-7 (LAN)	Ein	Link vorhanden
	Blinkt	Datentransfer

3.10 EAGLE mGuard

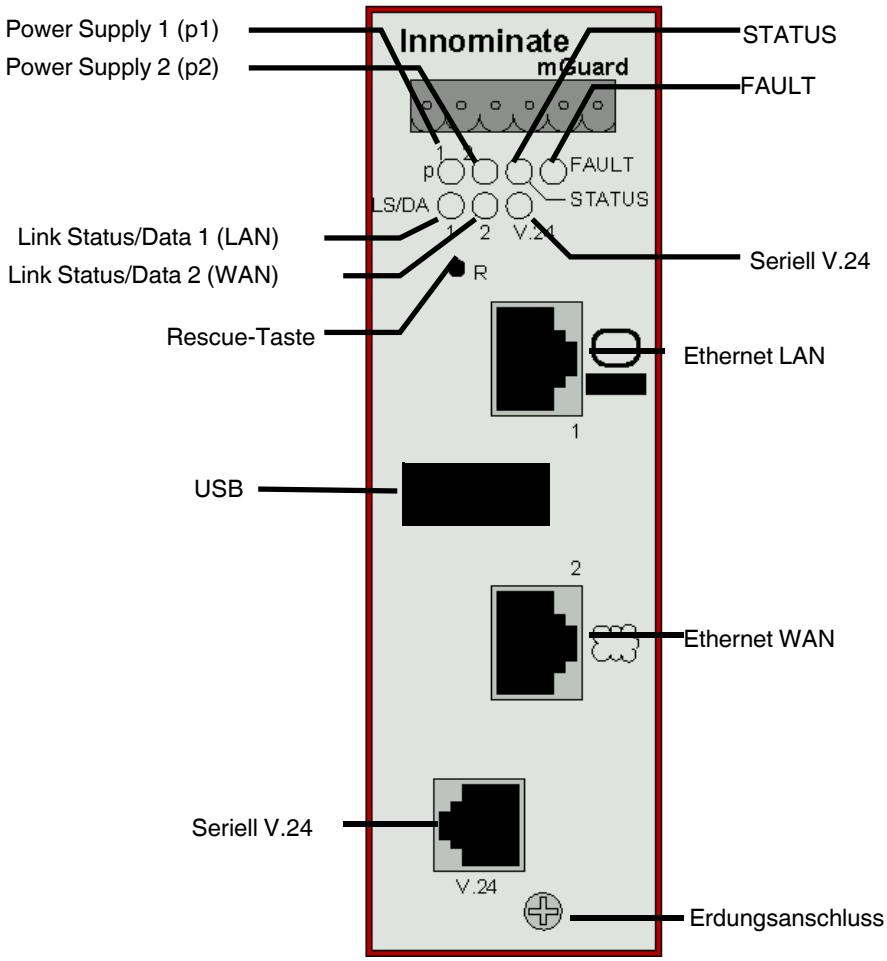


Bild 3-11 Bedienelemente und Anzeigen vom EAGLE mGuard

Tabelle 3-10 Anzeigen vom EAGLE mGuard

LED	Zustand		Bedeutung
p1, p2	grün	Ein	**Die Stromversorgung 1 bzw. 2 ist aktiv.**
STATUS	grün	Ein	Der mGuard ist bereit.
		Blinkt	Der mGuard startet.
FAULT	rot	Ein	**Der Meldekontakt ist infolge eines Fehlers offen** (siehe „mGuard blade installieren“ auf Seite 4-30 und unter „Meldekontakt“ auf Seite 4-16“).
LS/DA 1/2 V.24	grün	Ein	**Link vorhanden**
	gelb	Blinkt	Datentransfer

4 Inbetriebnahme

4.1 Sicherheitshinweise

Um den ordnungsgemäßen Betrieb sicherzustellen und die Sicherheit der Umgebung und von Personen zu gewährleisten, muss der mGuard richtig installiert, betrieben und gewartet werden.

WARNUNG: Bestimmungsgemäßer Gebrauch

Bitte verwenden Sie den mGuard ausschließlich auf die dafür vorgesehene Art und für geeignete Zwecke.

WARNUNG: An RJ45-Buchsen nur LAN-Installationen anschließen

Schließen Sie die Netzwerk-Ports des mGuards nur an LAN-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des mGuards verbunden werden.

Bitte beachten Sie auch die weiteren gerätespezifischen Sicherheitshinweise in den folgenden Abschnitten.

Allgemeine Hinweise zur Benutzung

ACHTUNG: Anschlusshinweise

- Beim mGuard pci² SD/mGuard pci muss ihr PC einen freien PCI-Slot (3,3 V oder 5 V) bereitstellen.
- Anschlusskabel nicht knicken. Den Netzwerkstecker nur zum Verbinden mit einem Netzwerk benutzen.

ACHTUNG: Umgebungsbedingungen passend auswählen

- Umgebungstemperatur:
  +5 °C ... +40 °C (mGuard blade)
  0 °C ... +40 °C (mGuard smart², mGuard delta², mGuard delta)
  0 °C ... +50 °C (mGuard centerport)
  0 °C ... +55 °C (mGuard industrial rs)
  0 °C ... +60 °C (mGuard pci² SD mit Akku, EAGLE mGuard)
  0 °C ... +70 °C (mGuard pci² SD ohne Akku, mGuard pci)
  -20°C ... +60°C (mGuard rs4000/mGuard rs2000)
- Maximale Luftfeuchtigkeit, nicht kondensierend:
  20 % ... 90 %(mGuard smart², mGuard pci, mGuard centerport)
  10 % ... 95 %, (mGuard industrial rs, EAGLE mGuard, mGuard blade)
  5 % ... 95 %, (mGuard rs4000/mGuard rs2000, mGuard pci² SD, mGuard delta², mGuard delta)

Nicht direktem Sonnenlicht oder dem direkten Einfluss einer Wärmequelle aussetzen, um Überhitzung zu vermeiden.

ACHTUNG: Reinigen

Zum Reinigen des Gerätegehäuses ein weiches Tuch verwenden. Kein aggressives Lösungsmittel auftragen.

Schritte zur Inbetriebnahme

Um das Gerät in Betrieb zu nehmen, führen Sie folgende Schritte in der angegebenen Reihenfolge aus:

Schritt	Ziel	Seite
1	Lieferumfang prüfen	Seite 4-3
	Release Notes lesen	
2	Gerät anschließen	
	mGuard rs 4000/mGuard rs 2000	Seite 4-4
	mGuard centerport	Seite 4-8
	mGuard industrial rs	Seite 4-12
	mGuard smart^2/mGuard smart	Seite 4-19
	mGuard pci^2 SD	Seite 4-20
	mGuard pci	Seite 4-21
	mGuard blade	Seite 4-30
	mGuard delta^2	Seite 4-32
	mGuard delta	Seite 4-33
	Eagle mGuard	Seite 4-34
3	Das Gerät konfigurieren, soweit erforderlich.	Seite 5-4
	Gehen Sie dazu die einzelnen Menüoptionen durch, die Ihnen der mGuard mit seiner Konfigurationsoberfläche bietet.	
	Lesen Sie deren Erläuterungen in diesem Handbuch, um zu entscheiden, welche Einstellungen für Ihre Betriebsumgebung erforderlich oder gewünscht sind.	

4.2 Lieferumfang prüfen

Prüfen Sie vor Inbetriebnahme die Lieferung auf Vollständigkeit

Zum Lieferumfang gehören

- Das Gerät mGuard rs4000, mGuard rs2000, mGuard centerport, mGuard industrial rs, mGuard smart^2, mGuard pci^2 SD, mGuard pci, mGuard blade, mGuard delta^2, mGuard delta, oder EAGLE mGuard
- Packungsbeilage

Zum mGuard rs4000 und mGuard rs2000 gehören zusätzlich:

- COMBICON-Steckerbinder für den Stromanschluss und Ein-/Ausgänge (aufgesteckt)

Zum mGuard centerport gehören zusätzlich:

- 2 x Schlüssel für Frontklappenschloss
- 2 x AC-Netzanschlusskabel
- Gummifüße (selbstklebend)

Zum mGuard industrial rs gehören zusätzlich:

- Klemmblock für den Stromanschluss (aufgesteckt)
- Klemmblock für den Meldekontakt, Taster und optionaler ISDN- oder Telefonanschluss
- 2 Abdeckkappen für RJ45-Buchsen

Zum mGuard blade gehören zusätzlich:

- 19'' mGuard bladebase
- ein mGuard blade als Controller
- zwei Netzteile
- zwei Netzkabel
- 12 Leerblenden
- 12 Beschriftungsplättchen M1 bis M12
- Schrauben zur Montage der mGuard bladebase

Zum mGuard delta^2 gehören zusätzlich:

- eine 12 V DC-Stromversorgung inkl. diverser Länder-Adapter

Zum mGuard delta gehören zusätzlich:

- eine 5 V DC-Stromversorgung
- zwei UTP-Ethernetkabel

4.3 mGuard rs4000/rs2000 installieren

4.3.1 Montage/Demontage

Montage

Das Gerät wird in betriebsbereitem Zustand ausgeliefert. Für die Montage und Anschluss ist folgender Ablauf zweckmäßig:

- Montieren Sie den mGuard rs4000/rs2000 auf eine geerdete 35-mm-Tragschiene nach DIN EN 60715.

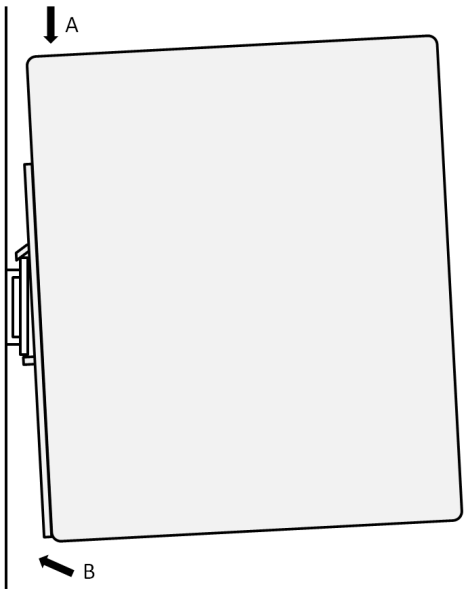


Bild 4-1 Montage des mGuard rs4000/rs2000 auf einer Tragschiene

- Hängen Sie dazu die obere Rastführung des mGuard rs4000/rs2000 in die Tragschiene ein und drücken Sie den mGuard rs4000/rs2000 dann nach unten gegen die Tragschiene, bis er einrastet.

Demontage

- Anschlüsse abnehmen bzw. trennen.
- Um den mGuard rs4000/rs2000 von der Tragschiene zu demontieren, stecken Sie einen Schraubendreher waagerecht unterhalb des Gehäuses in den Verriegelungsschieber, ziehen diesen – ohne den Schraubendreher zu kippen – nach unten und klappen den mGuard rs4000/rs2000 nach oben.

4.3.2 Netzwerkverbindung anschließen

WARNUNG: Schließen Sie die Netzwerk-Ports des mGuards nur an LAN-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des mGuards verbunden werden.

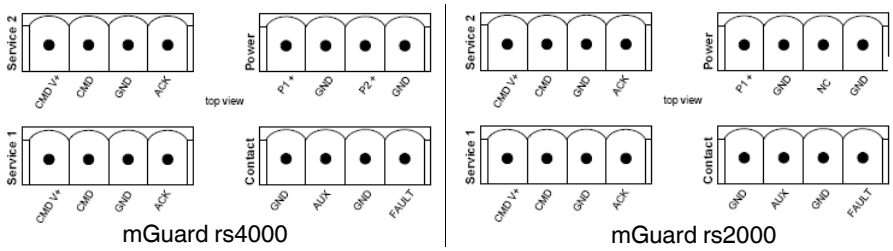
- Verbinden Sie den mGuard mit dem Netzwerk. Dazu benötigen Sie ein geeignetes UTP-Kabel (CAT5), das nicht zum Lieferumfang gehört.
- Verbinden Sie die interne Netzwerkschnittstelle LAN 1 des mGuards mit der entsprechenden Ethernet-Netzwerkkarte des Konfigurationsrechners oder einem validen Netzwerk-Anschluss des internen Netzwerks (LAN).

4.3.3 Service-Kontakte

WARNUNG: Die Service-Kontakte (GND, CMD, CMD V+, ACK) dürfen an keine externe Spannungsquelle angeschlossen werden, sondern sind wie hier beschrieben zu verbinden.

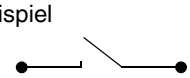
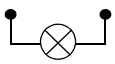
Beachten Sie, dass mit der Firmware-Version 7.4 und 7.5 nur die Kontakte „Service 1“ belegt sind. Die Kontakte „Service 2“ werden mit einer späteren Firmware-Version verfügbar sein.

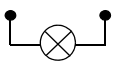
Die COMBICON-Stecker der Sevice-Kontakte können während des Betriebs des mGuard entfernt oder aufgesetzt werden.



Service 2	CMD V+	CMD	GND	ACK
	nicht verwendet	nicht verwendet	nicht verwendet	nicht verwendet

Power	P1+	GND	P2+	GND
	+24 V	+0 V	+24 V	+0 V
	siehe Kapitel 4.3.4		nur beim mGuard rs4000 siehe Kapitel 4.3.4	

Service 1	CMD V+	CMD	GND	ACK
	Externer Steuerungsschalter, Pin 1	Externer Steuerungsschalter, Pin 2	Meldeausgang (-)	Meldeausgang (+)
	Beispiel 		Beispiel 	

Contact	GND	AUX	GND	FAULT
	nicht verwendet	nicht verwendet	Meldeausgang (-)	Meldeausgang (+)[1]
			Beispiel 	

[1] 11 V ... 36 V bei ordnungsgemäßem Betrieb, bei Fehler spannungsfrei

Zwischen die **Service-Kontakte CMD V+ und CMD** kann ein **Taster** oder ein **Ein-/Aus-Schalter** (z. B. Schlüsselschalter) angeschlossen werden.

Zwischen den **Kontakten GND (-) und ACK (+)** kann eine handelsübliche Lampe (24 V) angeschlossen werden. Der Kontakt ist dauerkurzschlussfest und liefert maximal 250 mA.

Der **Taster** oder **Ein-/Aus-Schalter** dient zum Auf- und Abbau einer zuvor definierten VPN-Verbindung. Der Ausgang signalisiert den Status der VPN-Verbindung (siehe „IPsec VPN >> Global“ auf Seite 6-179 unter Optionen).

Bedienung eines angeschlossenen Tasters

- Zum Aufbau der VPN-Verbindung den Taster einige Sekunden gedrückt halten, bis der Signal-Ausgang blinkt. Erst dann den Taster loslassen.

  Das Blinken signalisiert, dass der mGuard das Kommando zum Aufbau der VPN-Verbindung erhalten hat und dabei ist, die VPN-Verbindung aufzubauen. Sobald die VPN-Verbindung steht, leuchtet der Signal-Ausgang kontinuierlich.
- Zum Abbau der VPN-Verbindung den Taster einige Sekunden gedrückt halten, bis der Signal-Ausgang blinkt oder erlischt. Erst dann den Taster loslassen.

  Sobald der Signal-Ausgang nicht mehr leuchtet, ist die VPN-Verbindung abgebaut.

Bedienung eines angeschlossenen Ein/Aus-Schalters

- Zum Aufbau der VPN-Verbindung den Schalter auf EIN stellen.
- Zum Abbau der VPN-Verbindung den Schalter auf AUS stellen.

INFO-LED

Ist der Signal-Ausgang auf AUS, wird dadurch generell signalisiert, dass die definierte VPN-Verbindung nicht besteht. Die VPN-Verbindung wurde entweder nicht aufgebaut oder ist wegen eines Fehlers ausgefallen.

Ist die INFO-LED auf EIN, besteht die VPN-Verbindung.

Blinkt die INFO-LED, wird die VPN-Verbindung gerade auf- oder abgebaut.

Meldekontakt (Meldeausgang)

Der Meldekontakt überwacht die Funktion des mGuards rs4000/rs2000 und ermöglicht damit eine Ferndiagnose. Bei dem Meldekontakt entspricht die Spannung der angelegten Versorgungsspannung. Bei der Überwachung der Ausgangsspannung wird folgendes gemeldet:

- Der Ausfall mindestens einer der beiden Versorgungsspannungen.
- Eine Unterschreitung des Grenzwertes bei der Stromversorgung des mGuards rs4000/rs2000 (Versorgungsspannung 1 und/oder 2 ist kleiner als 11 V).
- Überwachung des Link-Status der Ethernet-Anschlüsse, wenn dies konfiguriert worden ist. Im Lieferzustand wird die Verbindung nicht überwacht. Sie können die Überwachung einstellen (siehe„Meldekontakt“ auf Seite 6-6).
- Ein Fehler beim Selbsttest.

Während eines Neustarts ist der Meldekontakt abgeschaltet, bis der mGuard rs4000/rs2000 vollständig den Betrieb aufgenommen hat. Das gilt auch, wenn der Meldekontakt in der Software-Konfiguration unter „Manuelle Konfiguration“ auf „Geschlossen“ gestellt ist.

4.3.4 Versorgungsspannung anschließen

WARNUNG: Der mGuard rs4000/rs2000 ist für den Betrieb an einer Gleichspannung von 11 V DC ... 36 V DC/SELV, max. 1,5 A vorgesehen.

Entsprechend dürfen an die Versorgungsanschlüsse sowie an den Meldekontakt nur SELV-Spannungskreise mit den Spannungsbeschränkungen nach EN 60950-1 angeschlossen werden.

Der Anschluss der Versorgungsspannung erfolgt über einen COMBICON-Steckverbinder, der sich oben auf dem Gerät befindet.

Wenn Sie den COMBICON-Stecker während des Betriebs des mGuard entfernen oder aufgesetzen, führt das unmittelbar zum Ausschalten des mGuards.

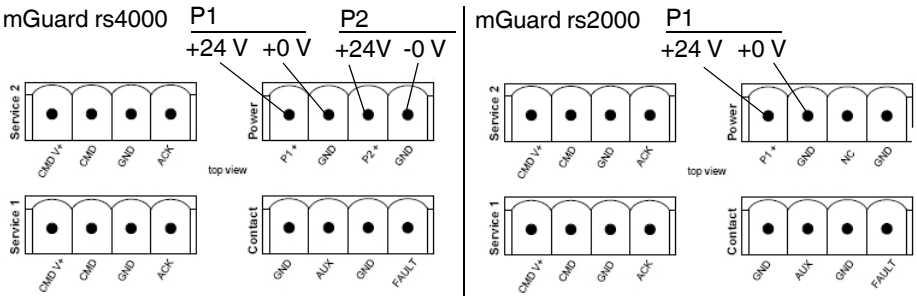


Bild 4-2 Versorgungsspannung anschließen: mGuard rs4000/mGuard rs2000

Der mGuard rs4000 hat eine redundante Versorgungsspannung. Wenn Sie nur eine Versorgungsspannung anschließen, erhalten Sie eine Fehlermeldung.

- Nehmen Sie die COMBICON-Stecker für Stromversorgung und Servicekontakte ab.
- Schließen Sie die Service-Kontakte nicht an eine externe Spannungsquelle an.
- Verdrahten Sie die Versorgungsspannungsleitungen mit dem entsprechenden COMBICON-Stecker (P1/P2) des mGuards. Ziehen Sie die Schrauben der Schraubklemmen mit 0,5 ... 0,8 Nm an.
- Stecken Sie die COMBICON-Stecker auf die vorgesehenen COMBICON-Buchsen auf der Oberseite des mGuards (siehe Bild 4-2).

Die Status-Anzeige P1 leuchtet grün, wenn die Versorgungsspannung korrekt anschlossen ist. Beim mGuard rs4000 leuchtet zusätzlich die Status-Anzeige P2 bei redundantem Anschluss der Versorgungsspannung.

Der mGuard bootet die Firmware. Die Status-Anzeige STAT blinkt grün. Der mGuard ist betriebsbereit, sobald die LEDs der Ethernet-Buchsen leuchten. Zusätzlich leuchten die Status-Anzeigen P1/P2 grün und die Status-Anzeige STAT blinkt grün im Heartbeat.

Redundante Spannungsversorgung (mGuard rs4000)

Die Versorgungsspannung ist redundant anschließbar. Beide Eingänge sind entkoppelt. Es besteht keine Lastverteilung. Bei redundanter Einspeisung versorgt das Netzgerät mit der höheren Ausgangsspannung den mGuard rs4000 alleine. Die Versorgungsspannung ist galvanisch vom Gehäuse getrennt.

Bei nicht redundanter Zuführung der Versorgungsspannung meldet der mGuard rs4000 über den Meldekontakt den Ausfall einer Versorgungsspannung. Sie können diese Meldung verhindern, indem Sie die Versorgungsspannung über beide Eingänge P1/P2 zuführen oder eine geeignete Drahtbrücke zwischen den Anschlüssen P1 und P2 anbringen.

4.4 mGuard centerport installieren und booten

Rückseite

Nicht bezeichnete Anschlüsse / Buchsen werden nicht verwendet.

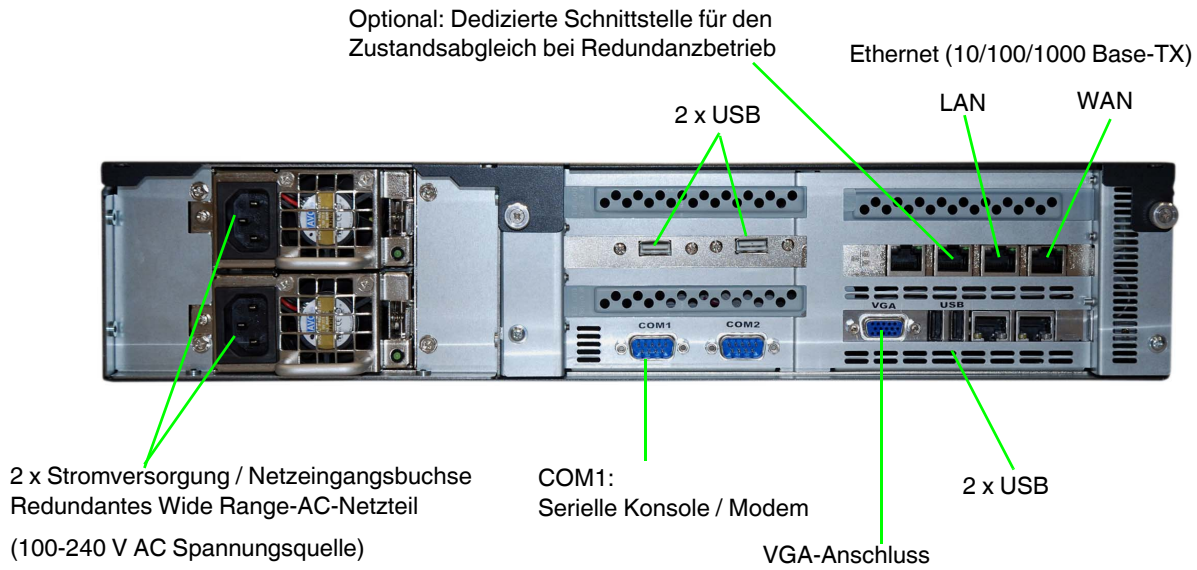


Bild 4-3 mGuard centerport Rückseite

4.4.1 Das Gerät anschließen

1. Optional:
   Das Gerät in einen 19“-Industrieschrank einbauen - siehe „Gehäuse“ auf Seite 4-10.
2. Beide Netzteile über die beiden Netzeingangsbuchsen am Netz bzw. an der Stromversorgungsquelle (100-240 VAC) anschließen.
3. Netzwerkverbindungen anschließen - siehe „Netzwerkverbindungen anschließen“ auf Seite 4-9.
4. Optional:
   Am **VGA-Anschluss** einen PC-Monitor anschließen (nicht im Lieferumfang).
   An einem der **USB**-Anschlüsse eine PC-Tastatur anschließen (nicht im Lieferumfang).
   Bildschirm und Tastatur müssen nur angeschlossen werden,
   – um beim Starten (Booten) von mGuard centerport eine der Boot-Optionen zu nutzen - siehe „Boot-Optionen - bei angeschlossenem Bildschirm und Tastatur“ auf Seite 4-10,
   – um eine Rescue-Prozedur oder Recovery-Prozedur durchzuführen. Siehe „Neustart, Recovery-Prozedur und Flashen der Firmware“ auf Seite 8-1
   Tastatur und Monitor brauchen nicht angeschlossen sein, um das Gerät zu starten und zu betreiben.

4.4.2 Netzwerkverbindungen anschließen

WARNUNG:
Schließen Sie die Netzwerk-Ports des mGuards nur an LAN-Installationen an.

Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des mGuards verbunden werden.

LAN-Port

- Verbinden Sie den lokalen Rechner oder das lokale Netzwerk mittels eines UTP-Ethernetkabels (CAT5) mit dem LAN-Port des mGuards.

WAN-Port

- Benutzen Sie ein UTP-Kabel (CAT5).
- Schließen Sie das externe Netzwerk über die WAN-Buchse an, z. B. WAN, Internet. (Über dieses Netz werden die Verbindungen zum entfernten Gerät bzw. Netz hergestellt.)

COM1: Serial-Port

ACHTUNG: Die serielle Schnittstelle (D-SUB-Buchse) darf nicht direkt mit Fernmeldeanschlüssen verbunden werden. Zum Anschluss eines seriellen Terminals oder eines Modems ist ein serielles Kabel mit D-SUB-Stecker zu verwenden. Die maximale Leitungslänge des seriellen Kabels beträgt 30m.

Der Serial-Port (serielle Schnittstelle) kann so benutzt werden, wie es unter „Serial-Port“ auf Seite 4-18 beschrieben ist.

4.4.3 Frontklappe

Das Sicherheitsschloss der Frontklappe ermöglicht das sichere Verschließen der Frontklappe, so dass der Zugriff auf die Laufwerke, die Reset-Taste und den EIN-/AUS-Schalter verwehrt ist. Die beiden mitgelieferten Schlüssel sicher aufbewahren.

Frontseite geöffnet

Bild 4-4 mGuard centerport Frontseite bei geöffneter Frontklappe

4.4.4 Gehäuse

Das Gehäuse des mGuard centerports ist von der Firma Kontron und wird als KISS 2U-Plattform bezeichnet. Unter der Internetadresse www.kontron.de finden Sie u.a. Informationen zu den folgenden Punkten:

– Montage in einen 19“-Industrieschrank
– Montage von Gehäusefüßen
– 19"-Winkel vom Gerät abnehmen
– Wartung und Pflege

4.4.5 mGuard centerport starten (booten)

- EIN-/AUS-Taste drücken.

De mGuard centerport bootet die Firmware und ist betriebsbereit.

4.4.5.1 Boot-Optionen - bei angeschlossenem Bildschirm und Tastatur

Ist ein Bildschirm und eine Tastatur am Gerät angeschlossen, gibt es folgende Optionen:

– Nach dem Einschalten,
– nach einem Neustart oder
– nach Drücken der Reset-Taste

werden auf dem Bildschirm zunächst die Boot-Meldungen des BIOS angezeigt, dann für einige Sekunden das Boot-Menü vom mGuard centerport.

Soll das Boot-Menü länger angezeigt bleiben, drücken Sie auf der Tastatur am besten eine der Richtungstasten: ↑, ↓, ← oder →.

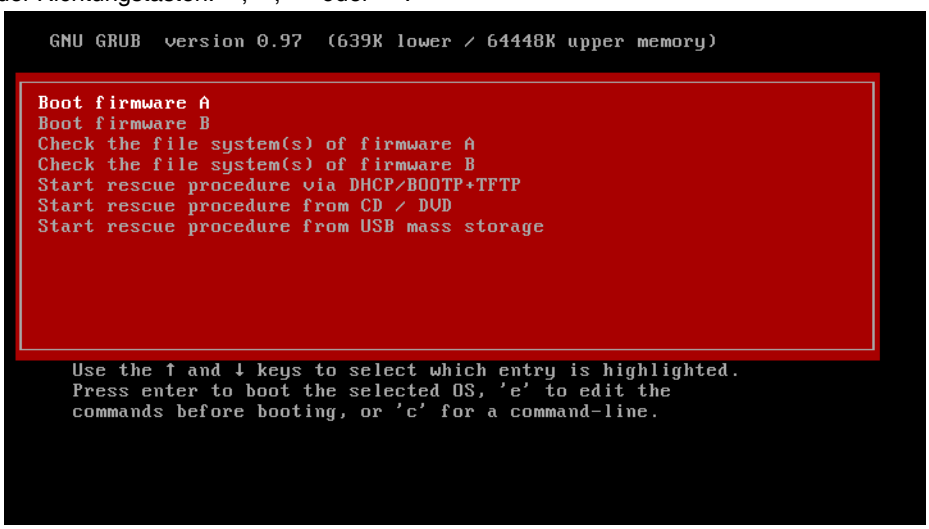


Bild 4-5 Boot-Menü mGuard centerport

Zum Auswählen und Inkraftsetzen einer der Boot-Optionen wie folgt vorgehen:

1. Mit den Richtungstasten ↓ bzw. ↑ eine der angezeigten Optionen auswählen.
2. Dann die **Enter-**Taste drücken.

Nachfolgend werden die Boot-Optionen erläutert:

Boot firmware A

Starten der primären auf dem Gerät befindlichen Firmware-Version „A“. Das ist die Standardeinstellung: Sie tritt in Kraft, wenn der Benutzer beim Starten nicht eingreift.

Boot firmware B

Wird von der aktuellen Firmware-Version nicht unterstützt.

Check the file system(s) of firmware A

Überprüft und repariert gegebenenfalls alle Dateisysteme der Firmware.
Dieser Menüpunkt braucht nur im besonderen Bedarfsfall bei entsprechender Kenntnis des Benutzers oder auf Anweisung des Supports Ihres Händlers verwendet werden. Die Firmware des mGuards überprüft und repariert die Dateisysteme bei Bedarf auch während des normalen Startvorganges. Die Firmware verwendet ihre Dateisysteme in sehr robuster Weise bei ausgeschaltetem Cache des Massenspeichermediums, so dass in der Regel kein Reparaturbedarf entsteht.

Check the file system(s) of firmware B

Wird von der aktuellen Firmware-Version nicht unterstützt.

Start rescue procedure via DHCP/BootP+TFTP

Siehe „Neustart, Recovery-Prozedur und Flashen der Firmware“ auf Seite 8-1.

Start rescue procedure from CD /DVD

Siehe „Neustart, Recovery-Prozedur und Flashen der Firmware“ auf Seite 8-1.

Start rescue procedure from USB mass storage

Siehe „Neustart, Recovery-Prozedur und Flashen der Firmware“ auf Seite 8-1.

4.5 mGuard industrial rs installieren

WARNUNG: Das Gehäuse darf nicht geöffnet werden.

WARNUNG: Die Schirmungsmasse der anschließbaren Twisted Pair-Leitungen ist elektrisch leitend mit der Frontblende verbunden.

WARNUNG: Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu treffen. Der Innominate mGuard industrial rs darf bei Aufstellung in Wohn- und Büroumgebungen ausschließlich in Schaltschränken mit Brandschutzeigenschaften gemäß EN 60950-1 betrieben werden.

4.5.1 Montage/Demontage

Montage

Das Gerät wird in betriebsbereitem Zustand ausgeliefert. Für die Montage und Anschluss ist folgender Ablauf zweckmäßig:

- Ziehen Sie den Klemmblock unten vom mGuard industrial rs ab und verdrahten Sie die Meldeleitungen und die weiteren Anschlüsse, soweit nötig (siehe „Anschlussmöglichkeiten Klemmblock unten“ auf Seite 4-14).
- Ziehen Sie die Schrauben der Schraubklemmen mit mindestens 0,22 Nm an.

  Warten Sie mit dem Einsetzen des Klemmenblocks.
- Montieren Sie den mGuard industrial rs auf eine geerdete 35-mm-Tragschiene nach DIN EN 60715.

  Das Gerät leitet die per Tragschiene gelieferte Erdung durch zum linken Kontakt (Erdungsanschluss) der unteren Klemmleiste.

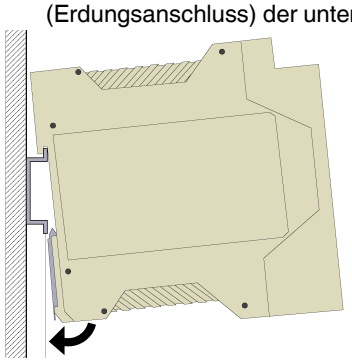


Bild 4-6 Montage des mGuard industrial rs´ auf einer Tragschiene

- Hängen Sie dazu die obere Rastführung des mGuard industrial rs’ in die Tragschiene ein und drücken Sie den mGuard industrial rs dann nach unten gegen die Tragschiene, so dass er einrastet.
- Setzen Sie den verdrahteten Klemmblock ein.
- Schließen Sie am Klemmblock oben die Versorgungsspannung an (siehe „Versorgungsspannung anschließen“ auf Seite 4-13).
- Nehmen Sie am LAN-Port bzw. WAN-Port die erforderlichen Netzwerkanschlüsse vor (siehe „Netzwerkverbindung anschließen“ auf Seite 4-14).
- Schließen Sie gegebenenfalls am SERIAL-Port das entsprechende Gerät an (siehe „Serial-Port“ auf Seite 4-18).

Demontage

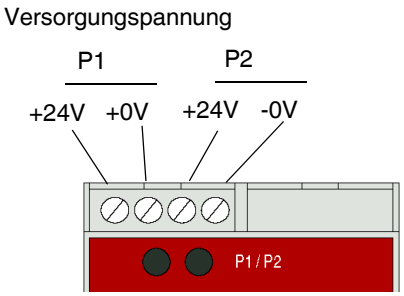
- Anschlüsse abnehmen bzw. trennen.
- Um den mGuard industrial rs von der Tragschiene zu demontieren, stecken Sie einen Schraubendreher waagerecht unterhalb des Gehäuses in den Verriegelungsschieber, ziehen diesen – ohne den Schraubendreher zu kippen – nach unten und klappen den mGuard industrial rs nach oben

4.5.2 Versorgungsspannung anschließen

WARNUNG: Der mGuard industrial rs ist für den Betrieb an einer Gleichspannung von 9 V DC ... 36 V DC/SELV, max. 0,5 A vorgesehen.

Entsprechend dürfen an die Versorgungsanschlüsse sowie an den Meldekontakt nur SELV-Spannungskreise mit den Spannungsbeschränkungen gemäß EN 60950-1 angeschlossen werden.

Der Anschluss der Versorgungsspannung erfolgt über einen Klemmblock mit Schraubverriegelung, der sich oben auf dem Gerät befindet.



Versorgungsspannung

– NEC Class 2 power source 12 V DC bzw. 24 V DC
– -25 % +33 % Sicherheitskleinspannung (SELV/PELV, redundante Eingänge entkoppelt)
– Maximal 5 A
– Pufferzeit min. 10 ms bei 24 V DC

Redundante Spannungsversorgung

Die Versorgungsspannung ist redundant anschließbar. Beide Eingänge sind entkoppelt. Es besteht keine Lastverteilung. Bei redundanter Einspeisung versorgt das Netzgerät mit der höheren Ausgangsspannung den mGuard industrial rs alleine. Die Versorgungsspannung ist galvanisch vom Gehäuse getrennt.

Bei nicht redundanter Zuführung der Versorgungsspannung meldet der mGuard industrial rs über den Meldekontakt den Ausfall einer Versorgungsspannung. Sie können diese Meldung verhindern, indem Sie die Versorgungsspannung über beide Eingänge zuführen.

4.5.3 Netzwerkverbindung anschließen

WARNUNG: Schließen Sie die Netzwerk-Ports des mGuards nur an LAN-Installationen an.

Zum Aufbau von Netzwerkverbindungen sind Kabel mit Knickschutzhülle an den Steckern zu verwenden.

Unbenutzte Buchsen sind mit den mitgelieferten Staubschutzkappen abzudecken.

Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des mGuards verbunden werden.

LAN-Port

- Verbinden Sie den lokalen Rechner oder das lokale Netzwerk mittels eines UTP-Ethernetkabels (CAT5) mit dem LAN-Port des mGuards.

  Ist Ihr Rechner bereits an einem Netzwerk angeschlossen, dann patchen Sie den mGuard zwischen die bereits bestehende Netzwerkverbindung.

Beachten Sie, dass die Konfiguration zunächst nur über das LAN-Interface erfolgen kann und die Firewall des mGuards industrial rs den gesamten IP-Datenverkehr vom WAN zum LAN-Interface unterbindet.

WAN-Port

- Benutzen Sie ein UTP-Kabel (CAT5).
- Schließen Sie das externe Netzwerk über die WAN-Buchse an, z. B. WAN, Internet. (Über dieses Netz werden die Verbindungen zum entfernten Gerät/Netz hergestellt.)

Es ist keine Treiber-Installation erforderlich.

Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administrator-Passwort zu ändern.

Anschlussmöglichkeiten Klemmblock unten

Der mGuard industrial rs ist in drei Versionen lieferbar, äußerlich unterscheidbar anhand der Anschlussmöglichkeiten bei der Klemmleiste unten:

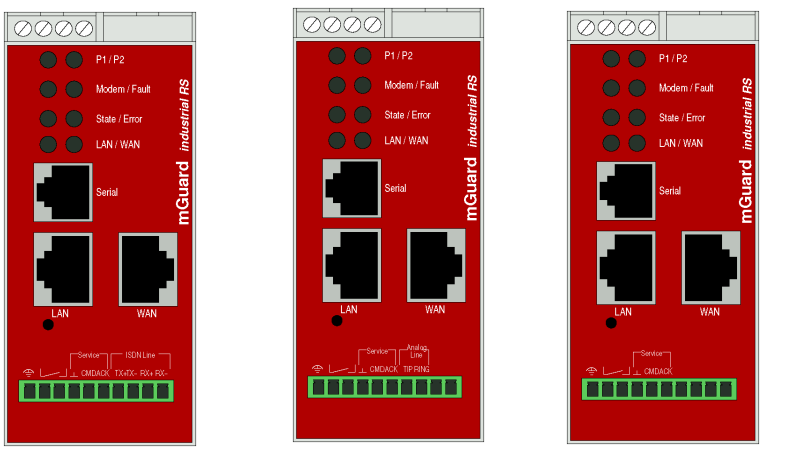


Bild 4-7 mGuard industrial rs: Klemmleiste unten

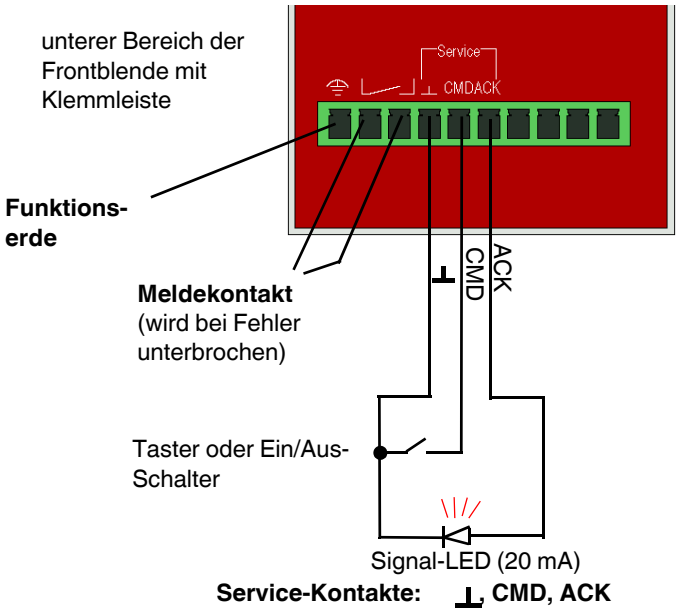


Bild 4-8 mGuard industrial rs: **ohne** Modem/ISDN-Terminaladapter

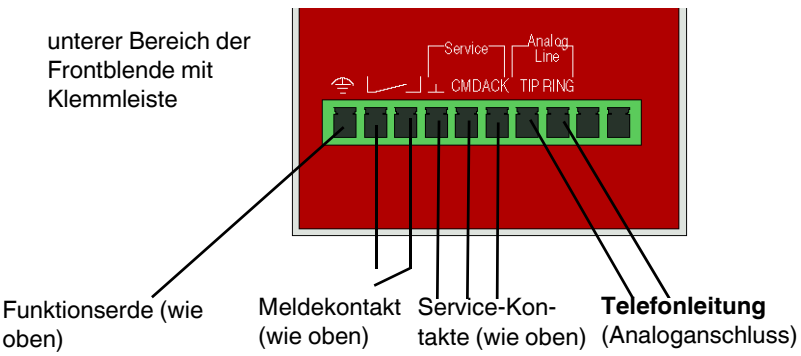


Bild 4-9 mGuard industrial rs **mit Modem**

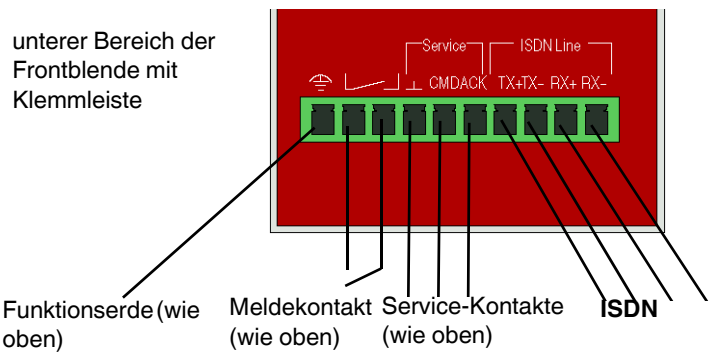


Bild 4-10 mGuard industrial rs **mit ISDN-Terminaladapter**

Funktionserde

Die Funktionserde kann für Ihre Zwecke verwendet werden. Dieser Anschluss ist leitend mit der Rückseite des mGuard industrial rs' verbunden. Die Erdung des mGuard industrial rs' erfolgt bei Montage auf einer Tragschiene mit der Metallklemme, über die er über seine Rückseite mit der Tragschiene verbunden ist. Die Tragschiene muss geerdet sein.

Meldekontakt

WARNUNG: An den Meldekontakt dürfen nur SELV-Spannungskreise mit den Spannungsbeschränkungen gemäß EN 60950-1 angeschlossen werden.

Der Meldekontakt dient der Funktionsüberwachung des mGuard industrial rs' und ermöglicht damit eine Ferndiagnose. Über den potentialfreien Meldekontakt (Relaiskontakt, Ruhestromschaltung) wird durch Kontaktunterbrechung folgendes gemeldet:

– Der Ausfall mindestens einer der zwei Versorgungsspannungen.
– Eine Grenzwertunterschreitung bei der Stromversorgung des mGuard industrial rs' (Versorgungsspannung 1 und/oder 2 ist kleiner als 9 V).
– Der fehlerhafte Link-Status mindestens eines Ports. Die Meldung des Link-Status kann beim mGuard industrial rs pro Port über das Management maskiert werden.

  Im Lieferzustand erfolgt keine Verbindungsüberwachung.
– Fehler beim Selbsttest.

Während eines Neustarts ist der Meldekontakt unterbrochen, bis der mGuard vollständig den Betrieb aufgenommen hat. Das gilt auch, wenn der Meldekontakt per Software-Konfiguration manuell auf *Geschlossen* gestellt ist.

Service-Kontakte

WARNUNG: Die Service-Kontakte (_I_, CMD, ACK) dürfen an keine externe Spannungsquelle angeschlossen werden, sondern sind wie hier beschrieben zu verbinden.

Zwischen die **Service-Kontakte CMD und** _I_ kann ein **Taster** oder ein **Ein-/Aus-Schalter** (z. B. Schlüsselschalter) angeschlossen werden.

Zwischen den **Kontakten ACK (+) und** _I_ **(-)** kann eine handelsübliche **LED** (bis 3,5 V) oder ein entsprechender Optokoppler angeschlossen werden. Der Kontakt ist kurzschlussfest und liefert maximal 20 mA. Die LED beziehungsweise der Optokoppler muss ohne Vorwiderstand angeschlossen werden (Verdrahtung siehe Bild 4-8 bis Bild 4-10).

Der **Taster** oder **Ein-/Aus-Schalter** dient zum Auf- und Abbau einer zuvor definierten VPN-Verbindung. Die LED signalisiert den Status der VPN-Verbindung (siehe „IPsec VPN >> Global“ auf Seite 6-179 unter Optionen).

Bedienung eines angeschlossenen Tasters

- Zum Aufbau der VPN-Verbindung den Taster einige Sekunden gedrückt halten, bis die Signal-LED blinkt. Erst dann den Taster loslassen.

  Das Blinken signalisiert, dass der mGuard das Kommando zum Aufbau der VPN-Verbindung erhalten hat und dabei ist, die VPN-Verbindung aufzubauen. Sobald die VPN-Verbindung steht, leuchtet die Signal-LED kontinuierlich.
- Zum Abbau der VPN-Verbindung den Taster einige Sekunden gedrückt halten, bis die Signal-LED blinkt oder erlischt. Erst dann den Taster loslassen.

  Sobald die Signal-LED nicht mehr leuchtet, ist die VPN-Verbindung abgebaut.

Bedienung eines angeschlossenen Ein/Aus-Schalters

- Zum Aufbau der VPN-Verbindung den Schalter auf EIN stellen.
- Zum Abbau der VPN-Verbindung den Schalter auf AUS stellen.

Signal-LED

Ist die Signal-LED auf AUS, wird dadurch generell signalisiert, dass die definierte VPN-Verbindung nicht besteht. Die VPN-Verbindung wurde entweder nicht aufgebaut oder ist wegen eines Fehlers ausgefallen.

Ist die Signal-LED auf EIN, besteht die VPN-Verbindung.

Blinkt die Signal-LED, wird die VPN-Verbindung gerade auf- oder abgebaut.

Analog Line (bei integriertem Modem)

WARNUNG: Die analogen Anschlüsse (TIP, RING) dürfen nur an die dafür vorgesehene Fernmeldeleitung angeschlossen werden.

Die Kontakte TIP und RING sind für den Anschluss ans Telefon-Festnetz (Analoganschluss).

Für die auf der Frontblende angegebenen Kontaktbezeichnungen sind in Deutschland auch folgende Bezeichnungen gebräuchlich:

TIP = a **RING = b**

ISDN-Line (bei integriertem ISDN-Terminaladapter)

WARNUNG: Die ISDN-Anschlüsse (TX+, TX-, RX+, RX-) dürfen nur an einen ISDN S0 Bus angeschlossen werden.

Die Kontakte TX+, TX-, RX+ und RX– sind für den Anschluss an ISDN gedacht und bezeichnen den mGuard industrial rs als Teilnehmer am ISDN. Die folgende Tabelle beschreibt die Zuordnung der Kontakte zu 8-poligen-Verbindungen sowohl für Stecker als auch Dosen, zum Beispiel RJ45:

Tabelle 4-1 Zuordnung der Kontakte zu 8-poligen-Verbindungen

Pol-Nummer	TE (mGuard)
3	TX+
4	RX+
5	RX-
6	TX-

Beim direkten Anschluss an einen ISDN-NTBA müssen die mGuard-Anschlüsse wie folgt verbunden werden:

NTBA a1 -----> mGuard Pin 9 (Rx+)

NTBA a2 -----> mGuard Pin 7 (Tx+)

NTBA b1 -----> mGuard Pin 10 (Rx-)

NTBA b2 -----> mGuard Pin 8 (Tx-)

Serial-Port

WARNUNG: Die serielle Schnittstelle (RJ12-Buchse) darf nicht direkt mit den Fernmeldeanschlüssen verbunden werden. Zum Anschluss eines seriellen Terminals oder eines Modems ist ein serielles Kabel mit RJ12-Stecker zu verwenden. Die maximale Leitungslänge des seriellen Kabels beträgt 30 m.

Der Serial-Port (serielle Schnittstelle) kann wie folgt verwendet werden:

Zum Konfigurieren des mGuards über die serielle Schnittstelle. Dazu gibt es zwei Möglichkeiten:

– An die serielle Schnittstelle des mGuards wird direkt ein PC angeschlossen (über dessen serielle Schnittstelle). Dann kann der PC-Benutzer mittels eines Terminalprogramms über die Kommandozeile den mGuard konfigurieren.
– Oder an die serielle Schnittstelle des mGuards wird ein Modem angeschlossen, das am Telefonnetz (Festnetz oder GSM-Netz) angeschlossen ist. Dann kann der Benutzer eines entfernten PCs, der ebenfalls mit einem Modem am Telefonnetz angeschlossen ist, zum mGuard eine PPP-Wählverbindung (PPP = Point-to-Point Protocol) herstellen und ihn per Web-Browser konfigurieren.

Zur Abwicklung des Datenverkehrs statt über die WAN-Schnittstelle des mGuards über die serielle Schnittstelle. In diesem Fall ist an die serielle Schnittstelle ein Modem anzuschließen.

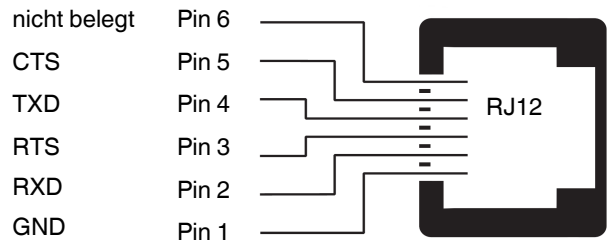


Bild 4-11 Pin-Belegung der RJ12-Buchse (Serial-Port)

Beim mGuard industrial rs mit eingebautem Modem oder ISDN-Terminaladapter kann der Datenverkehr statt über die WAN-Schnittstelle über die Anschlüsse *Analog Line* bzw. *ISDN Line* erfolgen.

4.6 mGuard smart²/mGuard smart anschließen

LAN-Port

Ethernet-Stecker zum direkten Anschließen an das zu schützende Gerät bzw. Netz (**lokales** Gerät oder Netz).

USB-Stecker

Zum Anschließen an die USB-Schnittstelle eines Rechners.

Dient der Stromversorgung (Werkseinstellung).

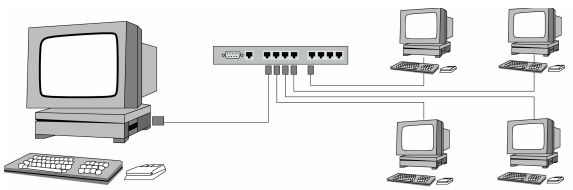
Der mGuard smart² (nicht der mGuard smart) kann auch so konfiguriert werden, dass über den USB-Stecker eine serielle Konsole zur Verfügung steht (siehe Kapitel 6.4.1.5).

WAN-Port

Buchse zum Anschließen an das externe Netzwerk, z. B. WAN, Internet. (Über dieses Netz werden die Verbindungen zum entfernten Gerät bzw. Netz hergestellt.)

Benutzen Sie ein UTP-Kabel (CAT5).

vorher:



nachher:

(Links kann auch ein LAN sein.)

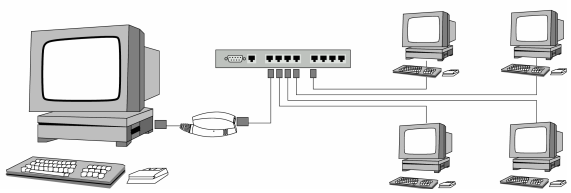


Bild 4-12 mGuard smart²: Anschuss im Netzwerk**.**

Wenn Ihr Rechner bereits an einem Netzwerk angeschlossen ist, dann stecken Sie den mGuard smart² zwischen die Netzwerkschnittstelle des Rechners (= dessen Netzwerkkarte) und das Netzwerk.

Es ist keine Treiber-Installation erforderlich.

Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administrator-Passwort zu ändern.

WARNUNG: Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu treffen.

4.7 mGuard pci² SD installieren

WARNUNG: Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen.

WARNUNG: Die sichere Trennung von berührungsgefährlichen Stromkreisen ist nur gewährleistet, wenn die angeschlossenen Geräte die Anforderungen der VDE 0106-101 (Sichere Trennung) erfüllen. Für die sichere Trennung sind die Zuleitungen getrennt von berührungsgefährlichen Stromkreisen zu führen oder zusätzlich zu isolieren.

4.7.1 Hardware einbauen

ACHTUNG: Elektrostatische Entladung!

Berühren Sie vor dem Einbau den freien Metallrahmen des PCs, in den Sie den mGuard pci² SD einbauen wollen, um Ihren Körper elektrostatisch zu entladen.

Das Gerät enthält Bauelemente, die durch elektrostatische Entladung beschädigt oder zerstört werden können. Beachten Sie beim Umgang mit dem Gerät die notwendigen Sicherheitsmaßnahmen gegen elektrostatische Entladung (ESD) gemäß EN 61340-5-1 und IEC 61340-5-1.

mGuard pci² SD: Aufbau

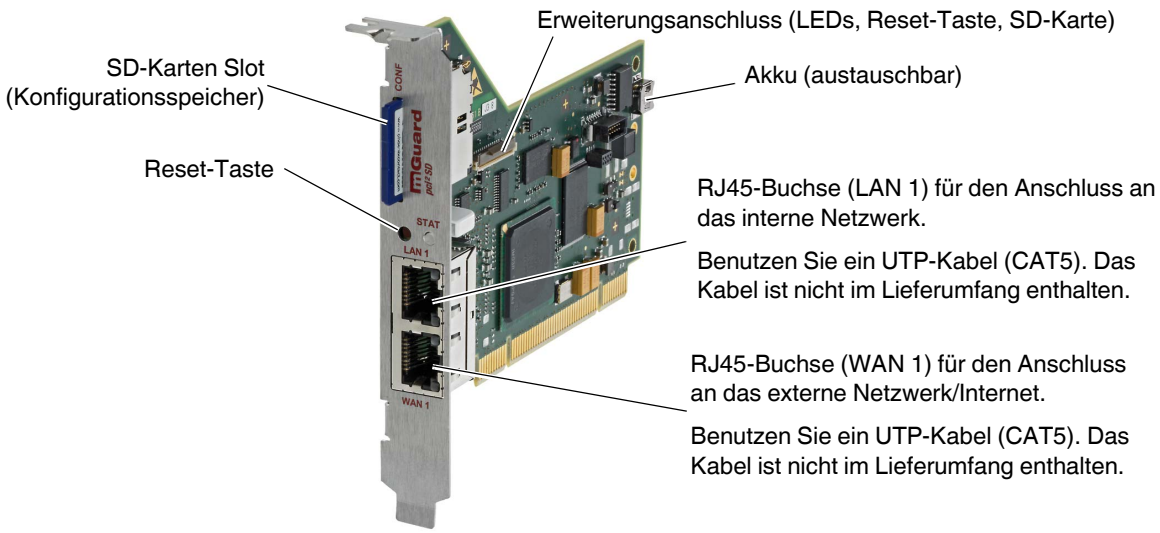


Bild 4-13 Aufbau mGuard pci² SD

- Bauen Sie den mGuard pci² SD in einen freien PCI- (mGuard pci²) oder PCI-Express- (mGuard pcie²) Steckplatz ein. Beachten Sie dabei die Hinweise in der Dokumentation zu Ihrem System.

4.8 mGuard pci installieren

WARNUNG: Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen.

WARNUNG: Akzeptabilitätsbedingungen

Das Gerät ist für den Einbau in einen PC im sekundären Signalkreis konzipiert worden und deshalb sind keine Tests durchgeführt worden. Tests müssen vom Anwender bewertet werden.

Die Temperatur der Leiterplatte darf 105 °C nicht überschreiten.

Auswahl Treibermodus oder Power-over-PCI-Modus

Es gibt zwei Betriebsmodi: *Treibermodus* und *Power-over-PCI-Modus.*

- Entscheiden Sie vor dem Einbau in Ihren PC, in welchem Modus Sie den mGuard pci betreiben möchten.
- Der mGuard wird per Jumper auf den gewünschten Modus geschaltet.

Treibermodus

Der mGuard pci kann wie eine normale Netzwerkkarte verwendet werden. Dann stellt diese Netzwerkkarte zusätzlich die mGuard-Funktionen zur Verfügung.

In diesem Fall muss der mitgelieferte Treiber installiert werden.

Power-over-PCI-Modus

Wenn die Netzwerkkarten-Funktionalität des mGuards nicht gebraucht wird oder nicht verwendet werden soll, kann der mGuard pci hinter eine vorhandene Netzwerkkarte (desselben Rechners oder eines anderen) quasi wie ein mGuard Standalone-Gerät angeschlossen werden. Tatsächlich steckt der mGuard pci in dieser Betriebsart nur deswegen im PCI-Slot eines Rechners, um mit Strom versorgt zu werden und ein Gehäuse zu haben. Diese Betriebsart des mGuards wird *Power-over-PCI-Modus* genannt.

Ein Treiber wird nicht installiert.

4.8.1 Treibermodus

In diesem Modus muss später ein Treiber für die PCI-Schnittstelle des mGuard pci (verfügbar für Windows XP/2000 und Linux) auf dem Computer installiert werden. Im Treibermodus wird keine weitere Netzwerkkarte für den Computer benötigt.

Stealth-Modus im Treibermodus (Werkseinstellung)

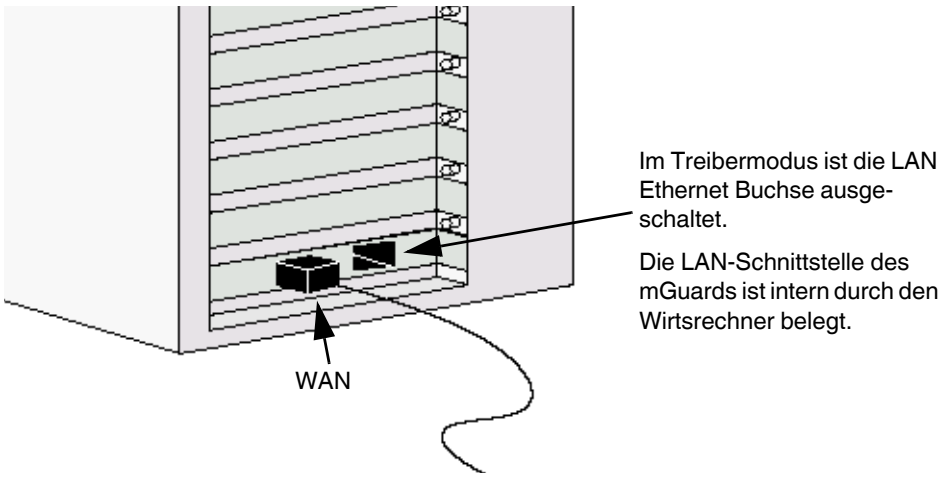


Bild 4-14 Treibermodus: Stealth-Modus

Im *Stealth*-Modus verhält sich der mGuard wie eine normale Netzwerkkarte.

Die IP-Adresse, die für die Netzwerkschnittstelle des Betriebssystems konfiguriert wird (= LAN-Port), übernimmt der mGuard auch für seinen WAN-Port. Somit tritt der mGuard für den Datenverkehr vom und zum Rechner als eigenes Gerät mit eigener Adresse gar nicht in Erscheinung.

Im Stealth-Modus ist es nicht möglich PPPoE oder PPTP zu verwenden.

Router -Modus im Treibermodus

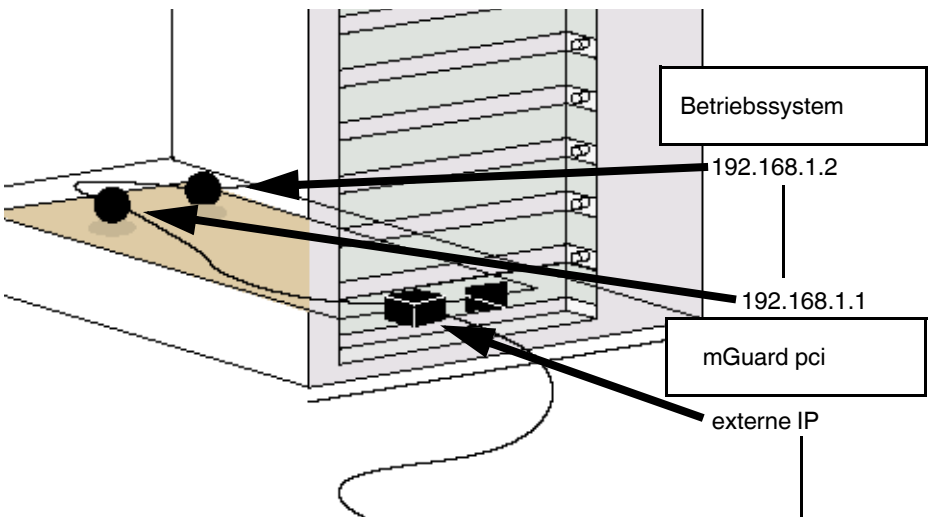


Bild 4-15 Treibermodus: Router-Modus

Befindet sich der mGuard im *Router*-Modus (oder *PPPoE*- oder *PPTP*-Modus), bildet er mit dem Betriebssystem des Rechners, in dem der mGuard installiert ist, quasi ein eigenes Netzwerk.

Für die IP-Konfiguration der Netzwerkschnittstelle des Betriebssystems bedeutet das Folgendes: Dieser muss eine IP-Adresse zugewiesen werden, die sich von der internen IP-Adresse des mGuards (gemäß werkseitiger Voreinstellung 192.168.1.1) unterscheidet.

(Dieser Zusammenhang wird in der obiger Zeichnung durch zwei schwarze Kugeln verdeutlicht.)

Eine dritte IP-Adresse wird für die Schnittstelle des mGuards zum WAN verwendet. Über diese geht die Verbindung zu einem externen Netz (z. B. Internet).

4.8.2 Power-over-PCI-Modus

Stealth-Modus im Power-over-PCI-Modus

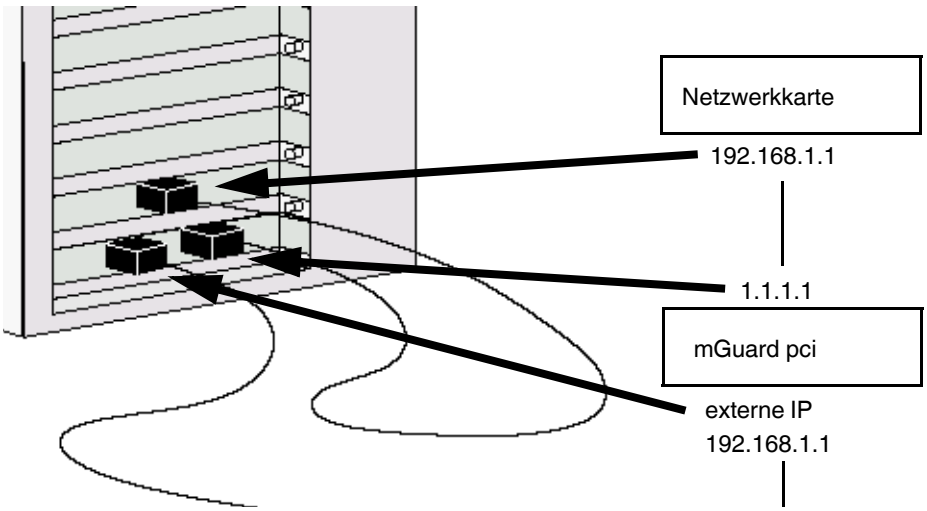


Bild 4-16 Power-over-PCI-Modus: Stealth-Modus

Da im Power-over-PCI-Modus die Netzwerkkarten-Funktionalität des mGuard pci ausgeschaltet ist, wird für ihn keine Treibersoftware installiert.

An den LAN Port des mGuard pci wird eine bereits installierte Netzwerkkarte angeschlossen, die sich im gleichen oder in einem anderen Computer befindet (siehe „Hardware einbauen“ auf Seite 4-25).

Im *Stealth*-Modus wird die IP-Adresse, die für die Netzwerkschnittstelle des Betriebssystems (= LAN Port) konfiguriert ist, vom mGuard auch für seinen WAN-Port übernommen. Somit tritt der mGuard für den Datenverkehr vom und zum Rechner als eigenes Gerät mit eigener Adresse gar nicht in Erscheinung.

Im Stealth-Modus ist es nicht möglich PPPoE oder PPTP zu verwenden.

Router-Modus im Power-over-PCI-Modus

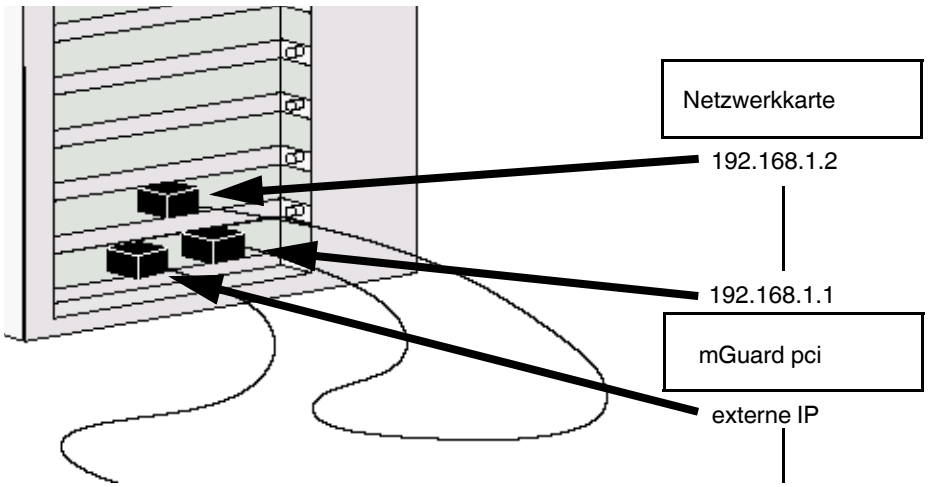


Bild 4-17 Power-over-PCI-Modus: Router-Modus

Befindet sich der mGuard im *Router*-Modus (oder *PPPoE* oder *PPTP* Modus), arbeiten der mGuard und die an seiner LAN-Buchse angeschlossene Netzwerkkarte – installiert im selben Rechner oder einem anderen – wie ein eigenes Netzwerk.

Für die IP-Konfiguration der Netzwerkschnittstelle des Betriebssystem des Rechners, in dem die Netzwerkkarte installiert ist, bedeutet das Folgendes: Dieser Netzwerkschnittstelle muss eine IP-Adresse zugewiesen werden, die sich von der internen IP-Adresse des mGuards (werkseitige Voreinstellung 192.168.1.1) unterscheidet.

Eine dritte IP-Adresse wird für die Schnittstelle des mGuards zum WAN verwendet. Über diese geht die Verbindung zu einem externen Netz (z. B. Internet).

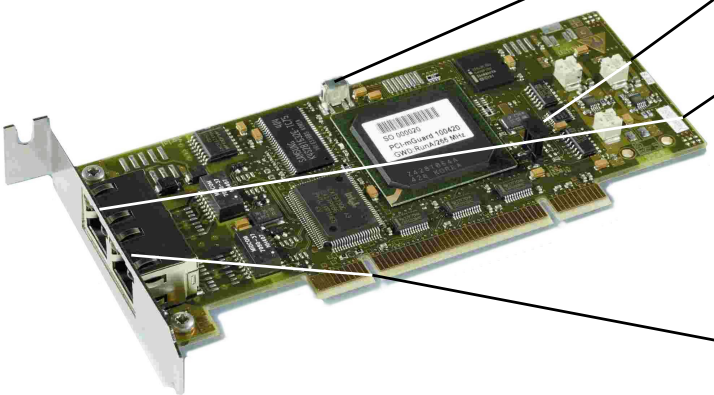
4.8.3 Hardware einbauen

ACHTUNG: Elektrostatische Entladung!

Berühren Sie vor dem Einbau den freien Metallrahmen des PCs, in den Sie den mGuard pci einbauen wollen, um Ihren Körper elektrostatisch zu entladen.

Das Gerät enthält Bauelemente, die durch elektrostatische Entladung beschädigt oder zerstört werden können. Beachten Sie beim Umgang mit dem Gerät die notwendigen Sicherheitsmaßnahmen gegen elektrostatische Entladung (ESD) gemäß EN 61340-5-1 und IEC 61340-5-1.

mGuard pci: Aufbau



(1) Rescue-Schalter

(2) Jumper zum Aktivieren/Deaktivieren des Treibermodus

(3) LAN Port

Ist im Treibermodus deaktiviert. Im Power-over-PCI-Modus wird hier die Netzwerkkarte desselben oder eines anderen zu schützenden Rechners oder das zu schützende Netzwerk angeschlossen.

(4) WAN-Port

Verbindungen zum externen Netz (z. B. Internet) werden über diese Schnittstelle aufgebaut. Gemäß Firewall-Werkseinstellung sind hier eingehende Verbindungen gesperrt. Verwenden Sie ein UTP-Kabel (CAT5).

Vorgehensweise

- Konfigurieren Sie den mGuard pci für den *Treibermodus* oder *Power-over-PCI-Modus*. (siehe „Auswahl Treibermodus oder Power-over-PCI-Modus“ auf Seite 4-21)
- Setzen Sie dazu den Jumper (2) an die entsprechende Position:

Treibermodus **Power-over-PCI-Modus**

Bild 4-18 Jumper für Treiber- oder Power-over-PCI-Modus

- Schalten Sie den Computer sowie andere angeschlossene Peripheriegeräte aus.
- Beachten Sie die Sicherheitshinweisen zur elektrostatischen Entladung.

- Ziehen Sie das Stromkabel.
- Öffnen Sie die Abdeckung des Computers. Bitte folgenden Sie dabei der Beschreibung im Handbuch des Computers.
- Wählen Sie einen freien PCI -Steckplatz (3,3 V oder 5 V) für den mGuard pci.
- Entfernen Sie das dazugehörige Slotblech durch Lösen der entsprechenden Schraube und Herausziehen des Slotblechs.

  Bewahren Sie die Schraube für das Festschrauben der mGuard pci Karte auf.
- Richten Sie die Steckerleiste der mGuard pci-Karte vorsichtig über der Buchsenleiste des PCI-Steckplatzes auf dem Motherboard aus, und drücken Sie anschließend die Karte gleichmäßig in die Buchsenleiste hinein.
- Schrauben Sie das Slotblech der Karte fest.
- Schließen Sie die Abdeckung des Computers wieder.
- Schließen Sie das Stromkabel des Computers wieder an und schalten Sie diesen ein.

4.8.4 Treiber installieren

Nur wenn der mGuard pci im *Treibermodus* arbeitet, ist die Installation eines Treibers erforderlich und möglich (siehe „Treibermodus“ auf Seite 4-21).

Voraussetzungen

- Falls noch nicht geschehen, führen Sie die unter „Hardware einbauen“ auf Seite 4-25 beschriebenen Schritte aus.
- Sie haben die Treiberdateien auf einem Datenträger.

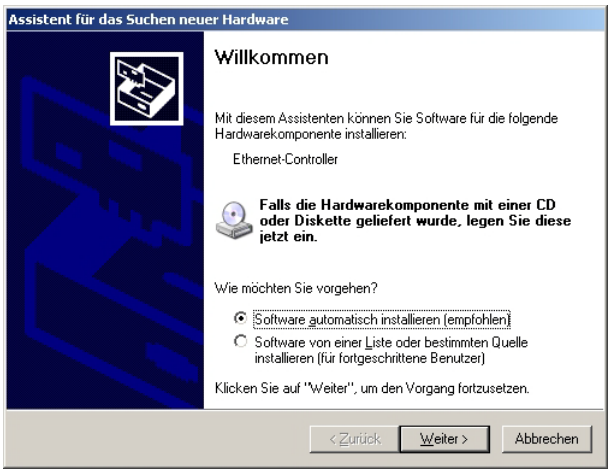
Falls nicht:

- Laden Sie die Treiberdateien im Download-Bereich der Website www.innominate.com herunter.
- Entpacken Sie das ZIP-Archiv.
- Kopieren Sie die entpackten Dateien auf einen Datenträger, z. B. CD-ROM, USB-Speicherstick.

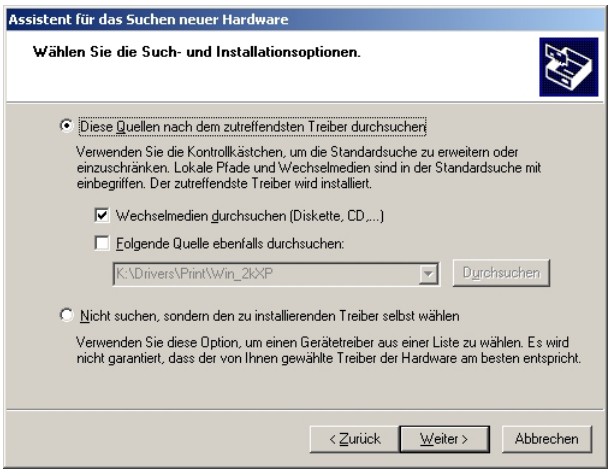
Unter Windows XP

- Nach dem Einbau der Hardware den Computer einschalten.
- Melden Sie sich mit Administratorrechten an und warten Sie, bis das folgende Fenster erscheint:

1



2



3

4

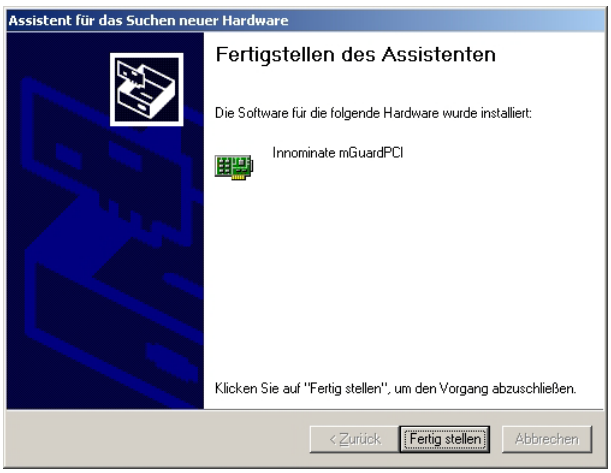


Bild 4-19 Treiberinstallation unter Windows XP

1. Nach Einlegen des Datenträgers wählen Sie „Software von einer Liste oder bestimmten Quelle installieren (für fortgeschrittene Benutzer)“ und klicken Sie auf „Weiter“.
2. Klicken Sie auf „Weiter“.
3. Klicken Sie auf „Installation fortsetzen“.
4. Klicken Sie auf „Fertig stellen“.

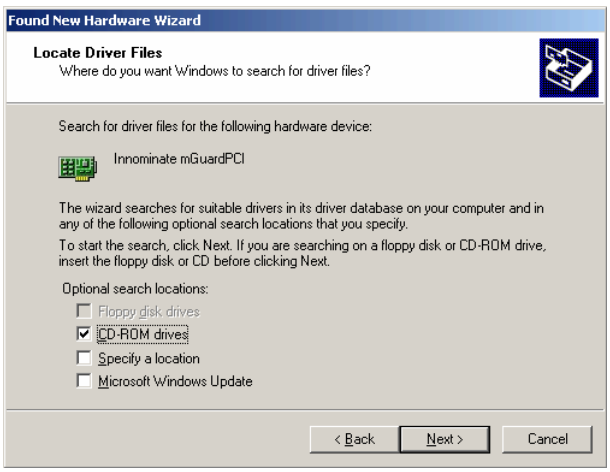
Unter Windows 2000

- Nach Einbau der Hardware den Computer einschalten.
- Melden sich mit Administratorrechten an und warten Sie, bis das folgende Fenster erscheint:

1

2

3



4

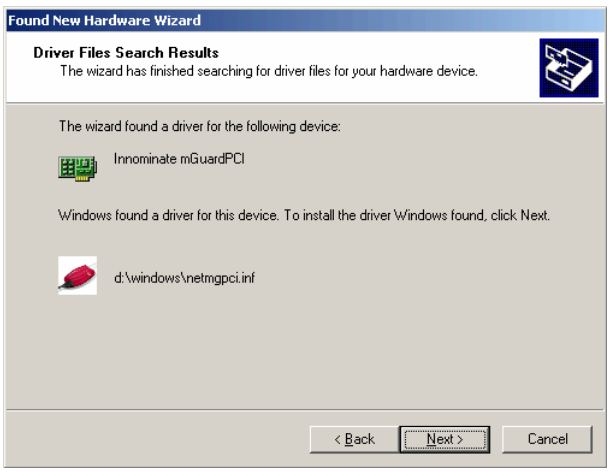


Bild 4-20 Treiberinstallation unter Windows 2000 (1)

1. Klicken Sie auf „Next“.
2. Wählen Sie „Search for a suitable driver for my device (recommended)“ und klicken Sie auf „Next“.
3. Wählen Sie „Specify a location“ und klicken Sie auf „Weiter“.
4. Klicken Sie auf „Next“.

5

6

Bild 4-21 Treiberinstallation unter Windows 2000 (2)

5. Klicken Sie auf „Yes“.
6. Klicken Sie auf „Finish“.

Unter Linux

Der Linuxtreiber ist im Sourcecode verfügbar und muss vor Verwendung übersetzt werden:

- Bauen und übersetzen Sie zunächst den Linuxkernel (2.4.25) im Verzeichnis /usr/src/linux
- Entpacken Sie die Treiber des ZIP-Archivs ins Verzeichnis /usr/src/pci-driver
- Führen Sie die folgenden Kommandos aus
  cd /usr/src/pci-driver
  make LINUXDIR=/usr/src/linux
  install -m0644 mguard.o /lib/modules/2.4.25/kernel/drivers/net/
  depmod -a
- Der Treiber kann nun mit dem folgenden Kommando geladen werden:
  modprobe mguard

4.9 mGuard blade installieren

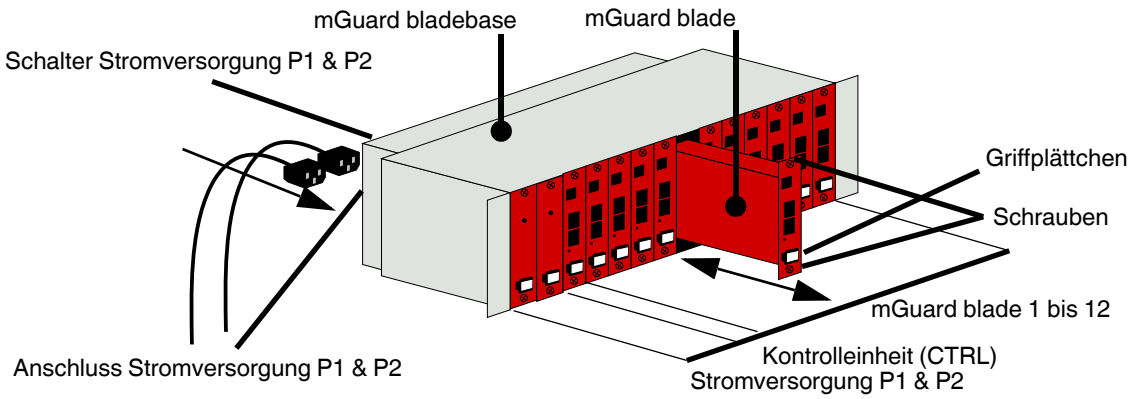


Bild 4-22 mGuard blade installieren

ACHTUNG: Achten Sie unbedingt darauf, dass eine ausreichende Luftzirkulation für das bladepack sichergestellt ist!

Bei Stapelung von mehreren bladepacks müssen ein oder mehrere Zoll Lüftereinschübe vorgesehen werden, damit die aufgestaute Warmluft abgeführt werden kann!

mGuard bladebase installieren

- Bauen Sie die mGuard bladebase in das Rack ein, z. B. in der Nähe des Patchfeldes.
- Versehen Sie die beiden Stromversorgungen und die Kontrolleinheit an der Vorderseite von links nach rechts mit den Griffplättchen „P1“, „P2“ und „Ctrl“.
- Verbinden Sie die beiden Stromversorgungen auf der Rückseite der mGuard bladebase mit 100 V oder 220/240 V.
- Schalten Sie die beiden Stromversorgungen ein.
- Die LEDs an der Vorderseite der Stromversorgungen leuchten nun grün.

mGuard blade installieren

Die mGuard bladebase braucht beim Ein- und Ausbau eines mGuard blade nicht ausgeschaltet zu werden.

- Lösen Sie an der Blende bzw. am zu ersetzenden mGuard blade die obere und untere Schraube.
- Nehmen Sie die Blende ab bzw. ziehen Sie das alte mGuard blade heraus.
- Setzen Sie das neue mGuard blade mit der Leiterplatte in die Kunststoffführungen und schieben Sie es vollständig in das mGuard bladebase hinein.
- Sichern Sie das mGuard blade durch leichtes Anziehen der Schrauben.
- Ersetzen Sie das leere Griffplättchen durch das mit der passenden Nummer aus dem Zubehör der mGuard bladebase, oder ersetzen Sie es durch das des ausgetauschten mGuard blade. Dazu das Plättchen seitlich hinein- bzw. herausschieben.

Kontrolleinheit (CTRL Slot)

Direkt neben den beiden Stromversorgungen befindet sich der CTRL-Slot. Ein darin betriebener mGuard blade arbeitet als Controller (Kontrolleinheit) für alle anderen mGuard blades.

Bei der ersten Installation eines mGuard blade in den „CTRL“ Slot konfiguriert sich das blade in eine Kontrolleinheit wie folgt um:

– Die Benutzeroberfläche wird für den Betrieb als Controller umkonfiguriert.
– Er schaltet sich in den Router-Modus mit der lokalen IP-Adresse 192.168.1.1.
– Die Funktionen Firewall, CIFS-Integrity-Monitoring und VPN werden zurückgesetzt und deaktiviert.

mGuard blade anschließen

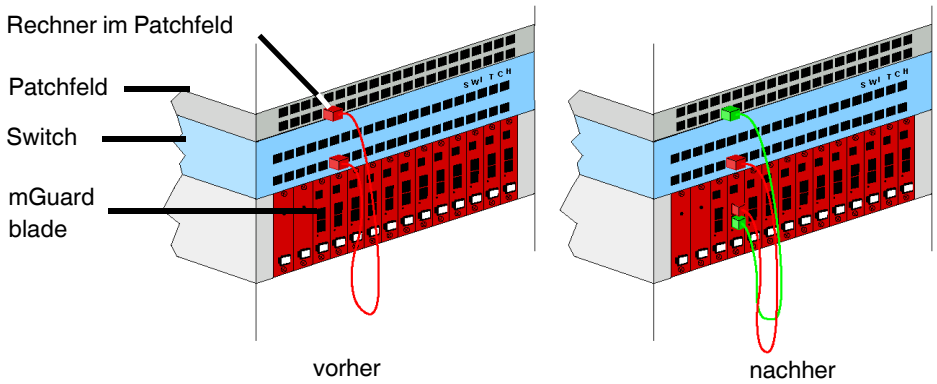


Bild 4-23 mGuard blade ans Netzwerk anschließen

ACHTUNG: Wenn Ihr Rechner bereits an einem Netzwerk angeschlossen ist, dann patchen Sie das mGuard blade zwischen die bereits bestehende Netzwerkverbindung.

Beachten Sie, dass die Konfiguration zunächst nur vom lokalen Rechner aus über das LAN-Interface erfolgen kann und die Firewall des mGuards allen IP-Datenverkehr vom WAN zum LAN Interface unterbindet.

Es ist keine Treiber-Installation erforderlich.

Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administrator-Passwort zu ändern.

Serial-Port

ACHTUNG: Die serielle Schnittstelle (RJ12-Buchse) darf nicht direkt mit Fernmeldeanschlüssen verbunden werden. Zum Anschluss eines seriellen Terminals oder eines Modems ist ein serielles Kabel mit RJ12-Stecker zu verwenden. Die maximale Leitungslänge des seriellen Kabels beträgt 30m.

Der Serial-Port (serielle Schnittstelle) kann so benutzt werden, wie es unter „Serial-Port“ auf Seite 4-18 beschrieben ist.

4.10 mGuard delta² anschließen

ACHTUNG: Hinweise zu Montage und Installation

Schließen Sie die RJ45-Ethernet-Ports des mGuards nur an passende Netzwerk-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen. Diese dürfen Sie nicht mit den RJ45-Anschlüssen des mGuards verbinden.

Die sichere Trennung von berührungsgefährlichen Stromkreisen ist nur gewährleistet, wenn die angeschlossenen Geräte die Anforderungen der VDE 0106-101 (Sichere Trennung) erfüllen. Für die sichere Trennung sind die Zuleitungen getrennt von berührungsgefährlichen Stromkreisen zu führen oder zusätzlich zu isolieren.

4.10.1 Mit dem Netzwerk verbinden

- Verbinden Sie den mGuard mit dem Netzwerk. Dazu benötigen Sie ein geeignetes UTP-Kabel (CAT5), das nicht zum Lieferumfang gehört.
- Verbinden Sie die interne Netzwerkschnittstelle LAN 1 des mGuards mit der entsprechenden Ethernet-Netzwerkkarte des Konfigurationsrechners oder einem validen Netzwerk-Anschluss des internen Netzwerks (LAN).

4.10.2 Versorgungsspannung anschließen

- Verbinden Sie das Weitbereichs-Netzteil des mGuards mit einer geeigneten Stromversorgung. Schließen Sie den Niederspannungs-Stecker des Netzteils auf der Rückseite des mGuards an.

Bild 4-24 Niederspannungs-Stecker des Netzteils

Die Status-Anzeige PWR leuchtet grün, wenn die Versorgungsspannung korrekt angeschlossen ist.

Der mGuard bootet die Firmware. Die Status-Anzeige STAT blinkt grün.

Der mGuard ist betriebsbereit, sobald die LAN/WAN-LEDs der Ethernet-Buchsen leuchten.

Zusätzlich leuchten die Status-Anzeigen PWR grün und die Status-Anzeige STAT blinkt grün im Heartbeat.

4.11 mGuard delta anschließen

WARNUNG: Die serielle Schnittstelle (DE-9 Steckverbindung) darf nicht direkt mit Fernmeldeanschlüssen verbunden werden. Zum Anschluss eines seriellen Terminals oder eines Modems ist ein serielles Kabel mit einer DE-9 Steckverbinder zu verwenden.

Die maximale Leitungslänge des seriellen Kabels beträgt 30 m.

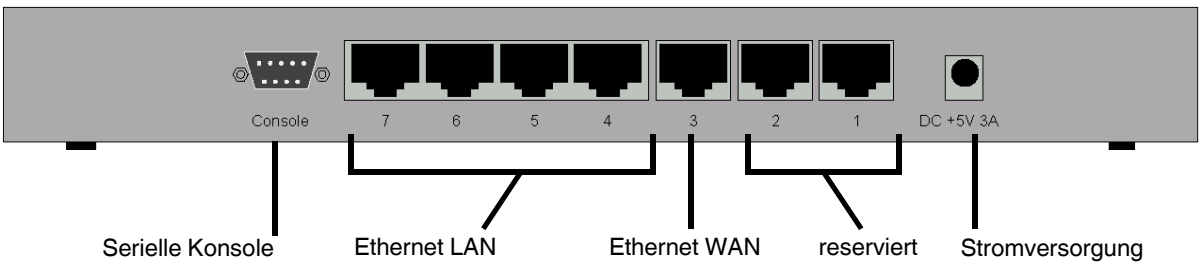


Bild 4-25 Anschlüsse mGuard delta

mGuard delta anschließen

- Verbinden Sie die Stromversorgung (5 V DC, 3 A) mit der Buchse „DC +5V, 3A“ des mGuard deltas.
- Verbinden Sie den lokalen Computer oder das lokale Netzwerk mittels eines UTP-Ethernetkabels (CAT5) mit einem der Ethernet-LAN-Anschlüsse (4 bis 7) des mGuard deltas.

4.12 EAGLE mGuard installieren

WARNUNG: Das Gehäuse darf nicht geöffnet werden.

WARNUNG: Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu treffen. Der EAGLE mGuard darf bei Aufstellung in Wohn- und Büroumgebungen ausschließlich in Schaltschränken mit Brandschutzeigenschaften gemäß EN 60950-1 betrieben werden.

ACHTUNG: Die Schirmungsmasse der anschließbaren Industrial Twisted Pair-Leitungen ist elektrisch leitend mit der Frontblende verbunden.

Versorgungspannung und Meldekontakt anschließen

Klemmblock

Der Anschluss der Versorgungsspannung und des Meldekontaktes erfolgt über einen 6-poligen Klemmblock.

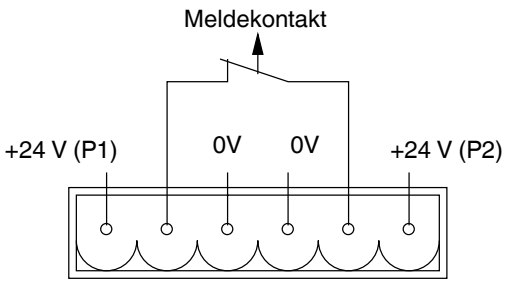


Bild 4-26 Klemmenblock

WARNUNG: Der EAGLE mGuard ist für den Betrieb mit Sicherheitskleinspannung ausgelegt. Entsprechend dürfen an die Versorgungsspannungsanschlüsse sowie an den Meldekontakt nur PELV-Spannungskreise oder wahlweise SELV-Spannungskreise mit den Spannungsbeschränkungen gemäß EN 60950-1 angeschossen werden.

Der EAGLE mGuard kann an einer Gleichspannung von 9,6 ... 60 V DC, max. 1 A beziehungsweise an einer Wechselspannung von 18 ... 30 V AC, max. 1 A betrieben werden. Verwenden Sie die Pins +24V und 0V zum Anschluss von Wechselspannung.

Betriebsspannung

- NEC Class 2 power source 12 V DC bzw. 24 V DC, -25 % +33 %
- Sicherheitskleinspannung (SELV/PELV, redundante Eingänge entkoppelt),
- max. 5 A. Pufferzeit min. 10 ms bei 24 V DC.

Redundante Spannungsversorgung

Die Versorgungsspannung ist redundant anschließbar. Beide Eingänge sind entkoppelt. Es besteht keine Lastverteilung. Bei redundanter Einspeisung versorgt das Netzgerät mit der höheren Ausgangsspannung den EAGLE mGuard alleine.

Die Versorgungsspannung ist galvanisch vom Gehäuse getrennt.

Inbetriebnahme

- Mit dem Anschluss der Versorgungsspannung über den 6-poligen Klemmblock nehmen Sie den EAGLE mGuard in Betrieb.
- Verriegeln Sie den Klemmblock mit der seitlichen Verriegelungsschraube.

Meldekontakt

WARNUNG: Der Meldekontakt darf nur an PELV-Spannungskreise oder wahlweise SELV-Spannungskreise mit den Spannungsbeschränkungen gemäß EN 60950-1 angeschlossen werden.

Der Meldekontakt dient der Funktionsüberwachung des EAGLE mGuard und ermöglicht damit eine Ferndiagnose. Über den potentialfreien Meldekontakt (Relaiskontakt, Ruhestromschaltung) wird durch Kontaktunterbrechung folgendes gemeldet:

– Der Ausfall mindestens einer der zwei Versorgungsspannungen.
– Eine dauerhafte Störung im EAGLE mGuard (interne 3,3 V DC-Spannung, Versorgungsspannung 1 oder 2 < 9,6 V, …).
– Der fehlerhafte Link-Status mindestens eines Ports. Die Meldung des Link-Status kann beim EAGLE mGuard pro Port über das Management maskiert werden.

  Im Lieferzustand erfolgt keine Verbindungsüberwachung.
– Fehler beim Selbsttest.

Bei nicht redundanter Zuführung der Versorgungsspannung meldet der EAGLE mGuard den Ausfall einer Versorgungsspannung. Sie können diese Meldung verhindern, indem Sie die Versorgungsspannung über beide Eingänge zuführen.

Erdungsanschluss

- Zur Erdung des EAGLE mGuard ist ein separater Schraubanschluss vorhanden.

Serial-Port

WARNUNG: Die serielle Schnittstelle (RJ12-Buchse) darf nicht direkt mit Fernmeldeanschlüssen verbunden werden. Zum Anschluss eines seriellen Terminals oder eines Modems ist ein serielles Kabel mit RJ12-Stecker zu verwenden. Die maximale Leitungslänge des seriellen Kabels beträgt 30 m.

Der Serial-Port (serielle Schnittstelle) kann so benutzt werden, wie es unter „Serial-Port“ auf Seite 4-18 beschrieben ist. Doch die Belegung der Kontakte ist unterschiedlich wie es die folgende Abbildung zeigt:.

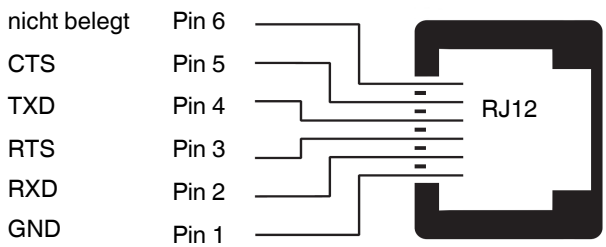


Bild 4-27 Pin-Belegung der RJ12-Buchse (Serial-Port)

Montage

Das Gerät wird in betriebsbereitem Zustand ausgeliefert. Für die Montage ist folgender Ablauf zweckmäßig:

- Ziehen Sie den Klemmblock vom EAGLE mGuard ab und verdrahten Sie die Versorgungsspannungs- und Meldeleitungen.

- Montieren Sie den EAGLE mGuard auf einer 35-mm-Tragschiene nach DIN EN 60715.

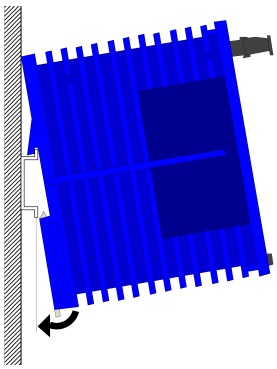


Bild 4-28 EAGLE mGuard: Tragschienenmontage

- Hängen Sie die obere Rastführung des EAGLE mGuard in die Tragschiene ein und drücken Sie den EAGLE mGuard dann nach unten gegen die Tragschiene, so dass er einrastet.
- Schließen Sie das Gerät an das lokale Netz oder den lokalen Rechner an, das/der geschützt werden soll (LAN).
- Über die Buchse zum Anschließen an das externe Netzwerk (WAN) den Anschluss ans externe Netzwerk vornehmen, z. B. Internet. (Über dieses Netzwerk werden die Verbindungen zum entfernten Gerät bzw. entfernten Netz hergestellt.)
- Die Erdung der Frontblende des Gehäuses des EAGLE mGuard erfolgt über den Erdungsanschluss.

Netzwerkverbindung

ACHTUNG: Wenn Ihr Rechner bereits an einem Netzwerk angeschlossen ist, dann patchen Sie den EAGLE mGuard zwischen die bereits bestehende Netzwerkverbindung.

Beachten Sie, dass die Konfiguration zunächst nur über das LAN Interface erfolgen kann und die Firewall des EAGLE mGuard den gesamten IP-Datenverkehr vom WAN zum LAN Interface unterbindet.

Es ist keine Treiber-Installation erforderlich.

Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administrator-Passwort zu ändern.

Beide Netzwerkschnittstellen des EAGLE mGuard sind für den Anschluss an einen Rechner konfiguriert.

Beim Anschluss an einen **Hub** ist Folgendes zu beachten:

Bei deaktivierter *Autonegotiation* Funktion wird auch die Auto-MDIX Funktion deaktiviert, d. h. der Port des EAGLE mGuard muss entweder an den Uplink-Port des Hub oder mittels eines Cross-Link-Kabels mit dem Hub verbunden werden.

Demontage

Um den EAGLE mGuard von der Tragschiene zu demontieren, fahren Sie mit einem Schraubendreher waagerecht unterhalb des Gehäuses in den Verriegelungsschieber, ziehen diesen – ohne den Schraubendreher zu kippen – nach unten und klappen den EAGLE mGuard nach oben.

5 Konfiguration vorbereiten

5.1 Anschlussvoraussetzungen

mGuard rs4000/rs2000

- Der mGuard rs4000/rs2000 muss an mindestens einem aktiven Netzteil angeschlossen sein.
- **Bei lokaler Konfiguration:** Der Rechner, mit dem Sie die Konfiguration vornehmen, muss an der LAN-Buchse des mGuards angeschlossen sein.
- **Bei Fernkonfiguration:** Der mGuard muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Der mGuard muss angeschlossen sein, d. h. die erforderlichen Verbindungen müssen funktionieren.

mGuard centerport

- Beim mGuard centerport müssen beide Netzteile an der Stromversorgungsquelle / am Netz angeschlossen sein. (Ist nur 1 Netzteil angeschlossen, kann das Gerät zwar betrieben werden, aber es wird ein akustisches Signal ausgegegen.)
- **Bei lokaler Konfiguration:** Der Rechner, mit dem Sie die Konfiguration vornehmen, muss an der LAN-Buchse des mGuards angeschlossen sein.
- **Bei Fernkonfiguration:** Der mGuard muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Der mGuard muss angeschlossen sein, d. h. die erforderlichen Verbindungen müssen funktionieren.

mGuard industrial rs

- Der mGuard industrial rs muss an mindestens einem aktiven Netzteil angeschlossen sein.
- **Bei lokaler Konfiguration:** Der Rechner, mit dem Sie die Konfiguration vornehmen, muss an der LAN-Buchse des mGuards angeschlossen sein.
- **Bei Fernkonfiguration:** Der mGuard muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Der mGuard muss angeschlossen sein, d. h. die erforderlichen Verbindungen müssen funktionieren.

mGuard smart²

- Der mGuard smart² muss eingeschaltet sein, d. h. er muss per USB-Kabel an einen eingeschalteten Rechner (oder Netzteil) angeschlossen sein, so dass er mit Strom versorgt wird.
- **Bei lokaler Konfiguration:** Der Rechner, mit dem Sie die Konfiguration vornehmen, muss entweder
  - am LAN Port des mGuard angeschlossen sein,
  - oder er muss über das lokale Netzwerk mit dem mGuard verbunden sein.
- **Bei Fernkonfiguration:** Der mGuard muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Der mGuard muss angeschlossen sein, d. h. die erforderlichen Verbindungen müssen funktionieren.

mGuard pci² SD

- **Bei lokaler Konfiguration:** Der Rechner, mit dem Sie die Konfiguration vornehmen, muss folgende Voraussetzungen erfüllen:
  - Der Rechner muss am LAN-Anschluss des mGuards angeschlossen sein oder über das lokale Netzwerk mit dem mGuard verbunden sein.
- **Bei Fernkonfiguration:** Der mGuard muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Der mGuard muss angeschlossen sein, d. h. die erforderlichen Verbindungen müssen funktionieren.

mGuard pci

- **Bei lokaler Konfiguration:** Der Rechner, mit dem Sie die Konfiguration vornehmen, muss folgende Voraussetzungen erfüllen:
  - **mGuard im** *Treibermodus*: Auf dem Rechner muss der mGuard pci-Treiber installiert sein.
  - **mGuard im** *Power-over-PCI-Modus*: Der Rechner muss am LAN-Anschluss des mGuards angeschlossen sein oder über das lokale Netzwerk mit dem mGuard verbunden sein.
- **Bei Fernkonfiguration:** Der mGuard muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Der mGuard muss angeschlossen sein, d. h. die erforderlichen Verbindungen müssen funktionieren.

mGuard blade

- Der mGuard blade muss in der mGuard bladebase montiert sein, und mindestens eines der Netzteile der bladebase muss in Betrieb sein.
- **Bei lokaler Konfiguration:** Der Rechner, mit dem Sie die Konfiguration vornehmen, muss entweder
  - an der LAN-Buchse des mGuard angeschlossen sein,
  - oder der Rechner muss über das Netzwerk mit dem mGuard verbunden sein.
- **Bei Fernkonfiguration:** Der mGuard muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Der mGuard muss angeschlossen sein, d. h. die erforderlichen Verbindungen müssen funktionieren.

mGuard delta²

- Der mGuard delta² muss an seine Stromversorgung angeschlossen sein.
- **Bei lokaler Konfiguration**: Der Rechner, mit dem Sie die Konfiguration vornehmen, muss an der LAN-Buchse des mGuards angeschlossen sein.
- **Bei Fernkonfiguration**: Der mGuard muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Der mGuard muss angeschlossen sein, d. h. die erforderlichen Verbindungen müssen funktionieren.

mGuard delta

- Der mGuard delta muss an seine Stromversorgung angeschlossen sein.
- **Bei lokaler Konfiguration:** Der Rechner, mit dem Sie die Konfiguration vornehmen, muss entweder
  - am LAN Switch (Ethernetbuchse 4 bis 7) des mGuards angeschlossen sein,
  - oder er muss über das lokale Netzwerk mit dem mGuard verbunden sein.
- **Bei Fernkonfiguration:** Der mGuard muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Der mGuard muss angeschlossen sein, d. h. die erforderlichen Verbindungen müssen funktionieren.

EAGLE mGuard

- Der EAGLE mGuard muss an mindestens einem aktiven Netzteil angeschlossen sein.
- **Bei lokaler Konfiguration:** Der Rechner, mit dem Sie die Konfiguration vornehmen, muss entweder
  - an der LAN-Buchse des mGuard angeschlossen sein,
  - oder der Rechner muss über das Netzwerk mit dem mGuard verbunden sein.
- **Bei Fernkonfiguration:** Der mGuard muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Der mGuard muss angeschlossen sein, d. h. die erforderlichen Verbindungen müssen funktionieren.

5.2 Lokale Konfiguration bei Inbetriebnahme (EIS)

Die Erstinbetriebnahme von mGuard-Produkten, die im Stealth-Modus ausgeliefert werden, ist ab der Firmware-Version 7.2 deutlich vereinfacht worden. Ab dieser Version ermöglicht das EIS (**E**asy **I**nitial **S**etup) Verfahren eine Inbetriebnahme über voreingestellte oder benutzerdefinierte Management-Adressen und das auch ohne Verbindung mit einem externen Netzwerk.

Der mGuard wird per Web-Browser konfiguriert, der auf dem zum Konfigurieren verwendeten Rechner ausgeführt wird (z. B. MS Internet-Explorer ab Version 8, Mozilla Firefox ab Version 3.6, Google Chrome oder Apple Safari).

ACHTUNG: Der verwendete Web-Browser muss SSL-Verschlüsselung (d. h. HTTPS) unterstützen.

Der mGuard ist gemäß Werkseinstellung unter folgenden Adressen erreichbar:

Tabelle 5-1 Voreingestellte Adressen

Werkseinstellung	Netzwerk-Modus	Management-IP #1	Management-IP #2
mGuard rs4000/rs2000	Stealth	https://1.1.1.1/	https://192.168.1.1/
mGuard industrial rs	Stealth	https://1.1.1.1/	https://192.168.1.1/
mGuard smart^2	Stealth	https://1.1.1.1/	https://192.168.1.1/
mGuard pci^2 SD	Stealth	https://1.1.1.1/	https://192.168.1.1/
mGuard pci	Stealth	https://1.1.1.1/	https://192.168.1.1/
mGuard blade	Stealth	https://1.1.1.1/	https://192.168.1.1/
mGuard delta^2	Stealth	https://1.1.1.1/	https://192.168.1.1/
EAGLE mGuard	Stealth	https://1.1.1.1/	https://192.168.1.1/
mGuard centerport	Router		https://192.168.1.1/
mGuard blade-Controller	Router		https://192.168.1.1/
mGuard delta	Router		https://192.168.1.1/

Die mGuards, die im Netzwerk-Modus Stealth ausgeliefert werden, sind auf die Stealth-Konfiguration „mehrere Clients“ voreingestellt. In diesem Modus müssen Sie, wenn Sie VPN-Verbindungen nutzen wollen, eine Management IP-Adresse und ein Standard-Gateway konfigurieren (siehe Seite 6-74). Alternativ können Sie eine andere Stealth-Konfiguration als „mehrere Clients“ wählen oder einen anderen Netzwerk-Modus verwenden.

Die Konfiguration bei der Inbetriebnahme wird in zwei Kapiteln beschrieben:

– für Geräte, die im Netzwerk-Modus „Stealth“ ausgeliefert werden, in Kapitel 5.2.1, ab Seite 5-5
– für Geräte, die im Netzwerk-Modus „Router“ ausgeliefert werden, in Kapitel 5.2.2, auf Seite 5-10

5.2.1 mGuard mit Werkseinstellung Stealth-Modus konfigurieren

Bei der ersten Inbetriebnahme von Geräten, die im Stealth-Modus ausgeliefert werden, ist der mGuard unter zwei Adressen erreichbar:

– https://192.168.1.1/ (siehe Seite 5-5)
– https://1.1.1.1/ (siehe Seite 5-6)

Alternativ kann per BootP (zum Beispiel mit IPAssign.exe) eine IP-Adresse zugewiesen werden (siehe „IP-Adresse per BootP zuweisen“ auf Seite 5-7).

Der mGuard ist unter der Adresse https://192.168.1.1/ erreichbar, wenn die externe Netzwerkschnittstelle beim Starten nicht verbunden ist.

Der mGuard kann von Rechnern über https://1.1.1.1/ erreicht werden, wenn diese direkt oder indirekt am LAN-Port des mGuards angeschlossen sind. Dazu muss der mGuard mit LAN- und WAN-Port in ein funktionierendes Netzwerk eingebunden sein, bei dem das Standard-Gateway über den WAN-Port erreichbar ist.

– Nach einem Zugriff über die IP-Adresse 192.168.1.1 und einer erfolgreichen Anmeldung wird die IP-Adresse 192.168.1.1 als Management IP-Adresse fest eingestellt.
– Nach einem Zugriff über die IP-Adresse 1.1.1.1 oder nach der Zuweisung einer IP-Adresse per BootP steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

Beim **mGuard pci²** und **mGuard pci** weicht die Inbetriebnahme von der hier beschriebenen Vorgehensweise ab.

Zur Anfangskonfiguration des
– mGuard pci² SD siehe „mGuard pci² SD bei Inbetriebnahme konfigurieren“ auf Seite 5-11.
– mGuard pci siehe „mGuard pci bei Inbetriebnahme konfigurieren“ auf Seite 5-15.

5.2.1.1 IP-Adresse 192.168.1.1

Bei Geräten, die im Stealth-Modus ausgeliefert werden, ist der mGuard über die LAN-Schnittstelle unter der IP-Adresse 192.168.1.1 innerhalb des Netzwerks 192.168.1.0/24 erreichbar, wenn eine dieser Bedingungen zutrifft.

– Der mGuard ist im Auslieferungszustand.
– Der mGuard wurde über die Web-Oberfläche auf die Werkseinstellung zurückgesetzt (siehe „Konfigurationsprofile“ auf Seite 6-41) und neu gestartet.
– Die Rescue-Prozedur (Flashen des mGuards) oder die Recovery-Prozedur wurden ausgeführt (siehe Kapitel 8).

Für einen Zugriff auf die Konfigurationsoberfläche kann es nötig sein, die Netzwerk-Konfiguration Ihres Computers anzupassen.

Unter **Windows XP** gehen Sie dazu wie folgt vor:

• Auf „Start, Systemsteuerung, Netzwerkverbindungen“ klicken.
• Das Symbol des LAN-Adapters mit der rechten Maustaste klicken, so dass sich das Kontextmenü öffnet.
• Im Kontextmenü „Eigenschaften“ klicken.
• Im Dialogfeld „Eigenschaften von LAN-Verbindung lokales Netz“ die Registerkarte „Allgemein“ wählen.

- Unter „Diese Verbindung verwendet folgende Elemente“ den Eintrag „Internetprotokoll (TCP/IP)“ markieren.
- Dann auf die Schaltfläche „Eigenschaften“ klicken, so dass folgendes Dialogfenster angezeigt wird:

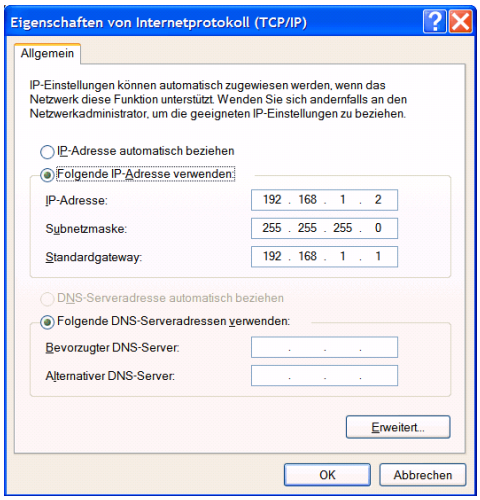


Bild 5-1 Eigenschaften von Internetprotokoll (TCP/IP)

- Aktivieren Sie zunächst „Folgende IP-Adressen verwenden“ und geben dann zum Beispiel folgende Adressen ein:

IP-Adresse:	192.168.1.2
Subnetzmaske:	255.255.255.0
Standard-Gateway:	192.168.1.1

Je nach dem, wie Sie den mGuard konfigurieren, müssen Sie gegebenenfalls anschließend die Netzwerkschnittstelle des lokal angeschlossenen Rechners bzw. Netzes entsprechend anpassen.

5.2.1.2 IP-Adresse https://1.1.1.1/

Bei konfigurierter Netzwerkschnittstelle

Damit der mGuard über die Adresse **https://1.1.1.1/** angesprochen werden kann, muss er an eine konfigurierte Netzwerkschnittstelle angeschlossen sein. Das ist der Fall, wenn man ihn zwischen eine bestehende Netzwerkverbindung steckt (siehe Bild 4-12 auf Seite 4-19) und dabei das Standard-Gateway über den WAN-Port des mGuards erreichbar ist.

In diesem Fall wird der Web-Browser nach Eingabe der Adresse https://1.1.1.1/ die Verbindung zur Konfigurations-Oberfläche des mGuards herstellen (siehe „Lokale Konfigurationsverbindung herstellen“ auf Seite 5-17). Fahren Sie in diesem Falle dort fort.

Nach einem Zugriff über die IP-Adresse 1.1.1.1 steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

5.2.1.3 IP-Adresse per BootP zuweisen

Nach der Zuweisung einer IP-Adresse per BootP steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

Für die IP-Adressvergabe nutzt der mGuard das BootP-Protokoll. Sie können die IP-Adresse auch über BootP zuweisen. Das Internet stellt eine Vielzahl von BootP-Servern zur Verfügung. Sie können ein beliebiges dieser Programme für die Adressvergabe nutzen.

Dieses Kapitel erklärt die IP-Adressvergabe mit Hilfe der Windows-Software „IP Assignment Tool“ (IPAssign.exe). Diese Software steht entweder unter der Adresse www.phoenixcontact.net/catalog zum kostenlosen Download bereit oder unter der Adresse www.innominate.com im Bereich „Downloads > Software“.

Hinweise zu BootP

Bei der ersten Inbetriebnahme sendet der mGuard ununterbrochen bis zum Erhalt einer gültigen IP-Adresse BootP-Requests aus. Sobald der mGuard eine korrekte IP-Adresse erhält, werden keine weiteren BootP-Requests gesendet. Danach steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

Nachdem der mGuard eine BootP-Antwort erhalten hat, sendet er keine BootP-Anfragen aus, auch nicht nach einem Neustart. Damit der mGuard erneut BootP-Requests sendet, muss entweder die Werkseinstellung wiederhergestellt oder eine der Prozeduren (Recovery oder Flash) ausgeführt werden.

Voraussetzungen

Der mGuard ist mit einem Rechner mit Microsoft Windows-Betriebssystem verbunden.

Vergabe der IP-Adresse mit IPAssign.exe

Schritt 1: Programm herunterladen und ausführen

- Wählen Sie im Internet den Link www.innominate.com/downloads.
- Unter „Software & Sonstiges“ finden Sie das BootP IP-Adressierungs-Werkzeug von Innominate.
- Doppelklicken Sie auf die Datei „IPAssign_mGuard.exe“.
- Wählen Sie im sich öffnenden Fenster die Schaltfläche „Ausführen“.

Alternativ finden Sie das Werkzeug „IPAssign.exe“ auch bei Phoenix Contact an folgender Stelle:

- Wählen Sie im Internet den Link www.phoenixcontact.net/catalog.
- Geben Sie in der Suchmaske z. B. die Artikel-Nummer 2832700 ein.

Unter „Konfigurationsdatei“ finden Sie das BootP IP-Adressierungs-Tool.

- Doppelklicken Sie auf die Datei „IPAssign.exe“.
- Wählen Sie im sich öffnenden Fenster die Schaltfäche „Ausführen“.

Schritt 2: „IP Assignment Wizard“

Das Programm wird geöffnet und der Startbildschirm des Adressierungs-Tools erscheint.

Das Programm ist in großen Teilen aus Gründen der Internationalität in Englisch gehalten. Die Schaltflächen des Programms passen sich an die landesspezifischen Einstellungen an.

Auf dem Startbildschirm wird die IP-Adresse des PCs angezeigt. Dies hilft in den weiteren Schritten bei der Adressierung des mGuards.

- Wählen Sie auf die Schaltfläche „Weiter“.

Schritt 3: „IP Address Request Listener“

Im sich öffnenden Fenster werden alle Geräte, die einen BootP-Request senden, gelistet und warten auf eine neue IP-Adresse.

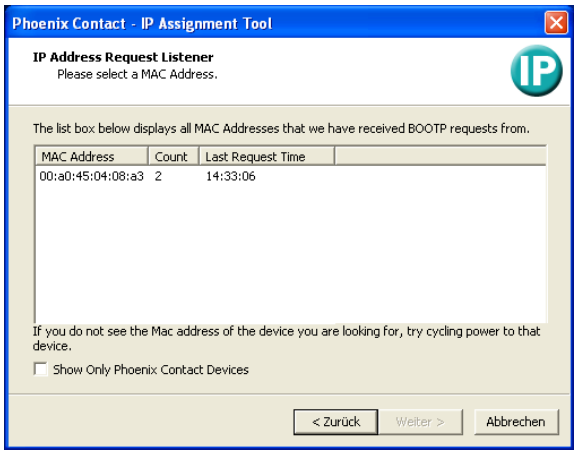


Bild 5-2 Fenster „IP Address Request Listener“

Im gezeigten Beispiel hat der mGuard die MAC-ID 00.A0.45.04.08.A3.

- Wählen Sie das Gerät, dem Sie eine IP-Adresse vergeben wollen, aus.
- Wählen Sie die Schaltfäche „Weiter“.

Schritt 4: „SET IP Address“

Im sich öffnenden Fenster werden folgende Informationen angegeben:

– IP-Adresse des PCs
– MAC-Adresse des ausgewählten Geräts
– IP-Parameter des ausgewählten Geräts
(IP-Adresse, Subnetzmaske und Gateway-Adresse)
– Eventuelle fehlerhafte Einstellungen

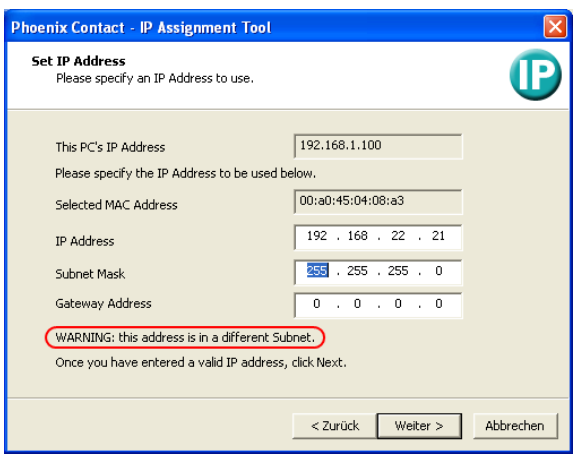


Bild 5-3 Fenster „Set IP Address“ mit fehlerhaften Einstellungen

- Passen Sie die IP-Parameter an Ihre Gegebenheiten an.

Wenn keine Unstimmigkeiten mehr erkannt werden, erscheint die Information, dass eine gültige IP-Adresse eingestellt wurde.

- Wählen Sie die Schaltfäche „Weiter“.

Schritt 5: „Assign IP Address“

Das Programm versucht, die eingestellte IP-Parameter an den mGuard zu übertragen.

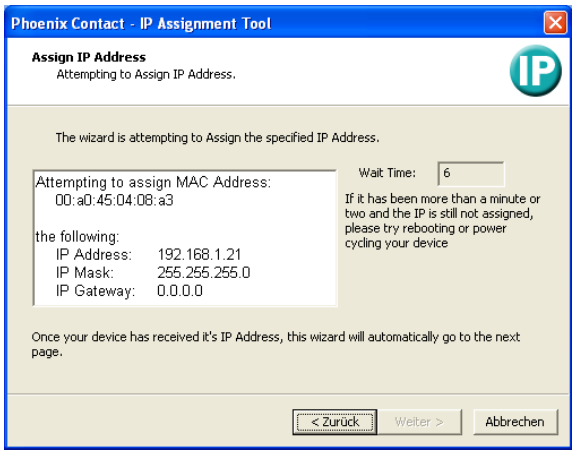


Bild 5-4 Fenster „Assign IP Address“

Nach erfolgreicher Übertragung öffnet sich das nächste Fenster.

Schritt 6: Abschluss der IP-Adressvergabe

Das folgenden Fenster informiert Sie über den erfolgreichen Abschluss der IP-Adressvergabe. Sie erhalten eine Übersicht darüber, welche IP-Parameter an das Gerät mit der angezeigten MAC-Adresse übertragen wurden.

Wenn Sie IP-Parameter für weitere Geräte vergeben wollen:

- Wählen Sie die Schaltfäche „Zurück“.

Wenn Sie die IP-Adressvergabe beenden wollen:

- Wählen Sie die Schaltfäche „Fertig stellen.

Die hier eingestellten IP-Parameter können Sie bei Bedarf in der mGuard Web-Oberfläche unter Netzwerk >> Interfaces ändern (siehe Seite 6-64).

5.2.2 mGuard mit Werkseinstellung Router-Modus konfigurieren

Bei Auslieferung oder nach Zurücksetzen auf die Werkseinstellung oder Flashen des mGuards ist er über die LAN Schnittstelle (bei mGuard delta die LAN-Schnittstellen 4 bis 7) unter der IP-Adresse 192.168.1.1 innerhalb des Netzwerks 192.168.1.0/24 erreichbar.

Für einen Zugriff auf die Konfigurationsoberfläche kann es daher nötig sein, die Netzwerk-Konfiguration Ihres Computers anzupassen.

Unter **Windows XP** gehen Sie dazu wie folgt vor:

- Auf „Start, Systemsteuerung, Netzwerkverbindungen“ klicken.
- Das Symbol des LAN-Adapters mit der rechten Maustaste klicken, so dass sich das Kontextmenü öffnet.
- Im Kontextmenü „Eigenschaften“ klicken.
- Im Dialogfeld „Eigenschaften von LAN-Verbindung lokales Netz“ die Registerkarte „Allgemein“ wählen.
- Unter „Diese Verbindung verwendet folgende Elemente“ den Eintrag „Internetprotokoll (TCP/IP)“ markieren.
- Dann auf die Schaltfläche „Eigenschaften“ klicken, so dass folgendes Dialogfenster angezeigt wird:

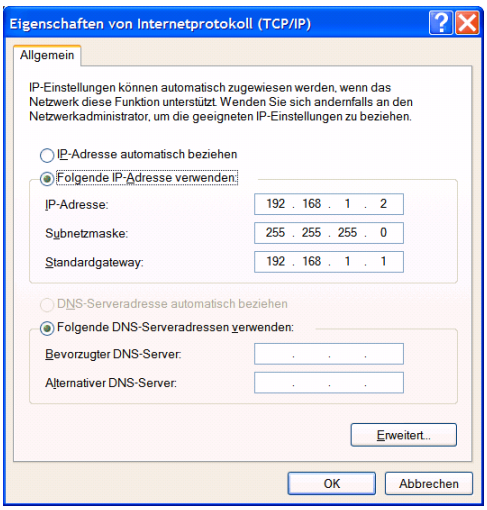


Bild 5-5 Eigenschaften von Internetprotokoll (TCP/IP)

- Aktivieren Sie zunächst „Folgende IP-Adressen verwenden“ und geben dann zum Beispiel folgende Adressen ein:

IP-Adresse:	192.168.1.2
Subnetzmaske:	255.255.255.0
Standard-Gateway:	192.168.1.1

Je nach dem, wie Sie den mGuard konfigurieren, müssen Sie gegebenenfalls anschließend die Netzwerkschnittstelle des lokal angeschlossenen Rechners bzw. Netzes entsprechend anpassen.

5.2.3 mGuard pci² SD bei Inbetriebnahme konfigurieren

Der mGuard pci² SD kann auf drei unterschiedliche Arten in Betrieb genommen werden:

– Gerät im Stealth-Modus in Betrieb nehmen (Standard)
– Gerät über temporäre Management IP-Adresse in Betrieb nehmen
– Gerät per BootP in Betrieb nehmen

5.2.3.1 Gerät im Stealth-Modus in Betrieb nehmen (Standard)

Schalten Sie den mGuard pci² SD zwischen eine bestehende Netzwerkverbindung.

Sie benötigen dafür geeignete UTP-Kabel (CAT5) für den Anschluss an die LAN- und WAN-Schnittstelle. Die Kabel sind nicht im Lieferumfang enthalten.

- Verbinden Sie die interne Netzwerkschnittstelle (LAN 1) des mGuard pci² SD mit der entsprechenden Ethernet-Netzwerkkarte des Konfigurationsrechners oder einem validen Netzwerkanschluss des internen Netzwerks.
- Verbinden Sie die externe Netzwerkschnittstelle (WAN 1) des mGuard pci² SD mit dem externen Netzwerk, z. B. dem Internet.

Die Status-Anzeige STAT leuchtet grün, wenn die Versorgungsspannung korrekt angeschlossen ist.

Der mGuard bootet die Firmware. Die Status-Anzeige STAT blinkt währenddessen grün.

Der mGuard ist betriebsbereit, sobald die unteren LEDs der Ethernet-Buchsen leuchten. Zusätzlich blinkt die Status-Anzeige STAT grün im Heartbeat.

Sie können eine fehlende Verbindung zum internen oder externen Netzwerk dadurch erkennen, dass die unteren LEDs in den Ethernet-Buchsen nicht leuchten. Wenn keine LED leuchtet, fehlt die Versorgungsspannung.

Der mGuard wird per Web-Browser konfiguriert, der auf dem lokal angeschlossenen Rechner (z. B. dem Schützling) ausgeführt wird (z. B. MS Internet-Explorer ab Version 8, Mozilla Firefox ab Version 3.6, Google Chrome oder Apple Safari).

ACHTUNG: Der verwendete Web-Browser muss SSL-Verschlüsselung (d. h. HTTPS) unterstützen.

Der mGuard ist voreingestellt unter der folgenden Adresse erreichbar: https://1.1.1.1/

mGuard pci² SD konfigurieren

- Geben Sie im Browser die folgende Adresse ein: https://1.1.1.1/

Die Verbindung zum mGuard pci² SD wird hergestellt. (Wenn nicht, siehe Kapitel 5.2.3.2).

Ein Sicherheitshinweis wegen eines angeblich ungültigen/nicht vertrauenswürdigen Zertifikats wird angezeigt. Diese Meldung resultiert aus der Verwendung eines mGuard-eigenen Zertifikats von Innominate, das dem Browser noch unbekannt ist, aber zur Verschlüsselung der Kommunikation benötigt wird.

- Quittieren Sie den Hinweis mit
  „Dieses Zertifikat immer/temporär akzeptieren“ (Mozilla Firefox),
  „Laden dieser Website fortsetzen“ (MS Internet Explorer),
  „Trotzdem Fortfahren“ (Google Chrome).
- Quittieren Sie den entsprechenden Sicherheitshinweis mit „Ja“.

Das Login-Fenster wird angezeigt.

Bild 5-6 Login

- Wählen Sie die Zugangsart „Administration“ und geben Sie Ihren Benutzernamen und Ihr Passwort ein.

Für Administration ist werkseitig voreingestellt (Groß- und Kleinschreibung beachten):

Benutzername:	admin
Passwort:	mGuard

Zur Konfiguration machen Sie auf den einzelnen Seiten der Oberfläche des mGuards die gewünschten bzw. erforderlichen Angaben (siehe „Konfiguration“ auf Seite 6-1).

Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administrator-Passwort zu ändern (siehe „Authentifizierung >> Administrative Benutzer“ auf Seite 6-121).

5.2.3.2 mGuard pci² SD über eine temporäre Management IP-Adresse in Betrieb nehmen

Wenn im Erstinbetriebnahme-Modus der mGuard pci² SD ohne ein funktionierendes externes Netzwerk angeschlossen wird, so ist das Gerät unter der Adresse https://1.1.1.1/ **nicht** erreichbar.

Der mGuard pci² SD ist in diesem Fall automatisch über die Management IP-Adresse 192.168.1.1/24 erreichbar. Das gilt sowohl für die interne (LAN 1) als auch externe (WAN 1) Netzwerkschnittstelle. Ein Adressenkonflikt an der externen Netzwerkschnittstelle ist nicht möglich, solange WAN 1 nicht an ein funktionierendes Netzwerk angeschlossen wird. Diese Management IP-Adresse ist normalerweise nicht persistent.

Wenn nach dem Hochfahren des mGuard pci² SD die externe Netzwerkschnittstelle (WAN 1) nachträglich verbunden wird, bleibt die Management IP-Adresse bestehen. In diesem Fall ist ein Adressenkonflikt mit bereits bestehenden Adressen im externen Netzwerk möglich.

mGuard pci² SD ohne externes Netzwerk in Betriebe nehmen

- Verbinden Sie die interne Netzwerkschnittstelle (LAN 1) des mGuard pci² SD mit der entsprechenden Ethernet-Netzwerkkarte des Konfigurationsrechners oder einem validen Netzwerk-Anschluss des internen Netzwerks.
- Trennen Sie die externe Netzwerkschnittstelle (WAN 1) des mGuard pci² SD vom externen Netzwerk (WAN).
- Schalten Sie das System ein. Die LED STAT leuchtet grün, wenn die Versorgungsspannung korrekt angeschlossen ist.

Der mGuard bootet die Firmware. Die LED STAT blinkt grün.

Konfigurationsrechner anpassen

Um den mGuard pci² für die Konfiguration erreichen zu können, müssen Sie den Konfigurationsrechner an die Management IP-Adresse des mGuard pci² SD angepassen

Beispiel für Microsoft Windows XP:

- Stellen Sie im Dialogfeld „Eigenschaften von Internetprotokoll (TCP/IP)“ der betreffenden Netzwerkschnittstelle des Konfigurationsrechners Folgendes ein:

IP-Adresse:	192.168.1.10
Subnetzmaske:	255.255.255.0
Standard-Gateway:	192.168.1.2

- Geben Sie im Browser die zugewiesene Adresse ein: https://192.168.1.1/
- Konfigurieren Sie den mGuard wie unter „mGuard pci² SD konfigurieren“ auf Seite 5-12 beschrieben.

5.2.3.3 mGuard pci² SD per BootP in Betrieb nehmen

Der mGuard pci² startet bei der Erstinbetriebnahme immer zusätzlich einen BootP-Clienten an der internen Netzwerkschnittstelle (LAN 1). Der BootP-Client ist kompatibel zu den BootP-Servern „IPAssign“ von Phoenix Contact sowie „DHCPD“ unter Linux.

Diese Software steht entweder unter der Adresse www.phoenixcontact.net/catalog zum kostenlosen Download bereit oder unter der Adresse www.innominate.com im Bereich „Downloads > Software“.

Die IP-Adressvergabe mit Hilfe von IPAssign wird in Kapitel „IP-Adresse per BootP zuweisen“ auf Seite 5-7 ausführlich beschrieben.

Wenn ein nicht konfigurierter mGuard pci² SD nach dem Hochfahren einen BootP-Server erreicht, dann wird dem mGuard pci² SD über das BootP-Protokoll eine IP-Adresse, eine Subnetzmaske und optional ein Standard-Gateway der internen Netzwerkschnittstelle zugewiesen. Diese Parameter werden persistent im Gerät gespeichert, welches dann ab sofort darunter erreichbar ist.

- Geben Sie im Browser die per BootP zugewiesene Adresse ein: z. B. https://192.168.1.1/

Konfigurieren Sie den mGuard wie unter „mGuard pci² SD konfigurieren“ auf Seite 5-12 beschrieben.

5.2.4 mGuard pci bei Inbetriebnahme konfigurieren

Installieren der PCI-Karte

- Wenn Sie die PCI-Karte noch nicht in ihrem Computer installiert haben, folgen Sie zunächst den unter „Hardware einbauen“ auf Seite 4-25 beschriebenen Schritten.

Installieren der Treiber

- Wenn Sie den mGuard für den **Treibermodus** konfiguriert haben, stellen Sie sicher, dass die Treiber wie unter „Treiber installieren“ auf Seite 4-26 beschrieben installiert sind.

Konfiguration der Netzwerkschnittstelle

Wenn Sie den mGuard

– im **Treibermodus** betreiben und die LAN-Schnittstelle (= Netzwerkschnittstelle des Computers) noch nicht konfiguriert wurde, oder

– im **Power-over-PCI-Modus** betreiben und die Netzwerkschnittstelle des Computers, der am LAN Interface des mGuards angeschlossenen ist, noch nicht konfiguriert wurde

dann müssen Sie diese Netzwerkschnittstelle konfigurieren, bevor Sie den mGuard konfigurieren können.

Unter **Windows XP** konfigurieren Sie die Netzwerkschnittstelle wie folgt:

- Auf „Start, Systemsteuerung, Netzwerkverbindungen“ klicken.
- Das Symbol des LAN-Adapters mit der rechten Maustaste klicken, so dass sich das Kontextmenü öffnet. Im Kontextmenü „Eigenschaften“ klicken.
- Im Dialogfeld „Eigenschaften von LAN-Verbindung lokales Netz“ die Registerkarte „Allgemein“ wählen.
- Unter „Diese Verbindung verwendet folgende Elemente“ den Eintrag „Internetprotokoll (TCP/IP)“ markieren.
- Dann die Schaltfläche „Eigenschaften“ klicken, so dass folgendes Dialogfenster angezeigt wird:

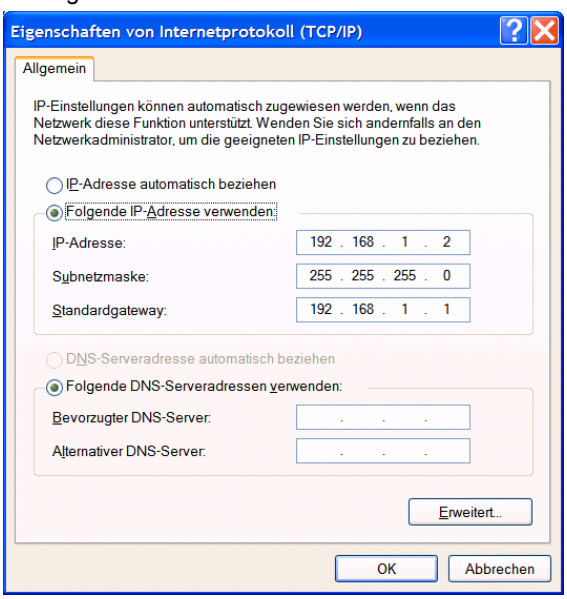


Bild 5-7 Eigenschaften von Internetprotokoll (TCP/IP)

Standard-Gateway

Nachdem Sie die Netzwerkschnittstelle konfiguriert haben, sollten Sie die Konfigurationsoberfläche des mGuards mit einem Web-Browser unter der URL „https://1.1.1.1/“ erreichen können.

Wenn dies nicht möglich ist, dann ist möglicherweise das Standard-Gateway ihres Computers nicht erreichbar. In diesem Fall muss es ihrem Computer wie folgt vorgetäuscht werden:

Standard-Gateway initialisieren

Ermitteln Sie die zurzeit gültige Standard-Gateway-Adresse.

- Unter **Windows XP** folgen Sie dazu den unter „Konfiguration der Netzwerkschnittstelle“ auf Seite 5-15 beschriebenen Schritten, um das Dialogfeld „Eigenschaften von Internetprotokoll (TCP/IP)“ zu öffnen.
- Falls in diesem Dialogfeld keine IP-Adresse des Standard-Gateway angegeben ist, z. B. weil „IP-Adresse automatisch beziehen“ aktiviert ist, dann geben Sie eine IP-Adresse manuell ein.

  Dazu aktivieren Sie zunächst „Folgende IP-Adressen“ verwenden und geben dann zum Beispiel folgende Adressen ein:

IP-Adresse:	192.168.1.2	Auf keinen Fall dem Konfigurations-Rechner eine Adresse wie 1.1.1.2 geben!
Subnetzmaske:	255.255.255.0	
Standard-Gateway:	192.168.1.1	

- Auf DOS-Ebene (Menü „Start, Alle Programme, Zubehör, Eingabeaufforderung“) geben Sie ein:

  arp -s <IP-Adresse des Standard-Gateway> 00-aa-aa-aa-aa-aa
  Beispiel:
  Sie haben als Standard-Gateway-Adresse ermittelt oder festgelegt: 192.168.1.1
  Dann lautet der Befehl:
  arp -s 192.168.1.1 00-aa-aa-aa-aa-aa
- Zur Konfiguration stellen Sie jetzt die Konfigurationsverbindung her (siehe „Lokale Konfigurationsverbindung herstellen“ auf Seite 5-17).
- Nach der Konfiguration stellen Sie das Standard-Gateway wieder zurück. Dazu entweder den Konfigurations-Rechner neu starten oder auf DOS-Ebene folgendes Kommando eingeben:

  arp -d

Je nach dem, wie Sie den mGuard konfigurieren, müssen Sie gegebenenfalls anschließend die Netzwerkschnittstelle des lokal angeschlossenen Rechners bzw. Netzes entsprechend anpassen.

5.3 Lokale Konfigurationsverbindung herstellen

Web-basierte Administratoroberfläche

Der mGuard wird per Web-Browser (z. B. Mozilla Firefox, MS Internet-Explorer, Google Chrome oder Apple Safari) konfiguriert, der auf dem Konfigurations-Rechner ausgeführt wird.

ACHTUNG: Der verwendete Web-Browser muss SSL-Verschlüsselung (d. h. HTTPS) unterstützen.

Der mGuard wird je nach Modell entweder im Netzwerk-Modus *Stealth* oder *Router* ausgeliefert und ist dem entsprechend unter einer der folgenden Adressen erreichbar:

Tabelle 5-2 Voreingestellte Adressen

Werkseinstellung	Netzwerk-Modus	Management-IP #1	Management-IP #2
mGuard rs4000/rs2000	Stealth	https://1.1.1.1/	https://192.168.1.1/
mGuard industrial rs	Stealth	https://1.1.1.1/	https://192.168.1.1/
mGuard smart^2	Stealth	https://1.1.1.1/	https://192.168.1.1/
mGuard pci^2 SD	Stealth	https://1.1.1.1/	https://192.168.1.1/
mGuard pci	Stealth	https://1.1.1.1/	https://192.168.1.1/
mGuard blade	Stealth	https://1.1.1.1/	https://192.168.1.1/
mGuard delta^2	Stealth	https://1.1.1.1/	https://192.168.1.1/
EAGLE mGuard	Stealth	https://1.1.1.1/	https://192.168.1.1/
mGuard centerport	Router		https://192.168.1.1/
mGuard blade-Controller	Router		https://192.168.1.1/
mGuard delta	Router		https://192.168.1.1/

Gehen Sie wie folgt vor:

- Starten Sie einen Web-Browser.

  (Zum Beispiel: Mozilla Firefox, MS Internet-Explorer, Google Chrome oder Apple Safari; der Web-Browser muss SSL-Verschlüsselung (d. h. HTTPS) unterstützen.)
- Achten Sie darauf, dass der Browser beim Starten nicht automatisch eine Verbindung wählt, weil sonst die Verbindungsaufnahme zum mGuard erschwert werden könnte.

Im **MS Internet Explorer** nehmen Sie diese Einstellung wie folgt vor:

- Menü „Extras, Internetoptionen...“, Registerkarte „Verbindungen“:
- Unter „DFÜ- und VPN-Einstellungen“ muss „Keine Verbindung wählen“ aktiviert sein.
- In der Adresszeile des Web-Browsers geben Sie die Adresse des mGuards vollständig ein (siehe Tabelle 5-2).

Sie gelangen zur Administrator-Webseite des mGuards.

Wenn Sie nicht zur Administrator-Webseite des mGuards gelangen

Falls Sie die konfigurierte Adresse vergessen haben

Falls die Adresse des mGuards im *Router- PPPoE-* oder *PPTP-*Modus auf einen anderen Wert gesetzt ist, und Sie kennen die aktuelle Adresse nicht, dann müssen Sie beim mGuard die **Recovery**-Prozedur ausführen, sodass die oben angegebenen Werkseinstellungen bezüglich der IP-Adresse des mGuards wieder in Kraft treten (siehe „Recovery-Prozedur ausführen“ auf Seite 8-2).

Falls die Administrator-Webseite nicht angezeigt wird

Sollte auch nach wiederholtem Versuch der Web-Browser melden, dass die Seite nicht angezeigt werden kann, versuchen Sie Folgendes:

- Prüfen Sie, ob der Standard-Gateway des angeschlossenen Konfigurations-Rechners initialisiert ist (siehe „Lokale Konfiguration bei Inbetriebnahme (EIS)“ auf Seite 5-4).
- Bestehende Firewalls gegebenenfalls deaktivieren.
- Achten Sie darauf, dass der Browser keinen Proxy Server verwendet.

  Im **MS Internet Explorer** (Version 8) nehmen Sie diese Einstellung wie folgt vor: Menü „Extras, Internetoptionen...“, Registerkarte „Verbindungen“.

  Unter „LAN-Einstellungen“ auf die Schaltfläche „Einstellungen“ klicken.

  Im Dialogfeld „Einstellungen für lokales Netzwerk (LAN)“ dafür sorgen, dass unter Proxyserver der Eintrag „Proxyserver für LAN verwenden nicht“ aktiviert ist.
- Falls andere LAN-Verbindungen auf dem Rechner aktiv sind, deaktivieren Sie diese für die Zeit der Konfiguration.

  Dazu unter Menü „Start, Einstellungen, Systemsteuerung, Netzwerkverbindungen“ bzw. „Netzwerk- und DFÜ-Verbindungen“ das betreffende Symbol mit der rechten Maustaste klicken und im Kontextmenü „Deaktivieren“ wählen.

Bei erfolgreichem Verbindungsaufbau

Nach erfolgreicher Verbindungsaufnahme erscheint dieser Sicherheitshinweis (MS Internet Explorer):

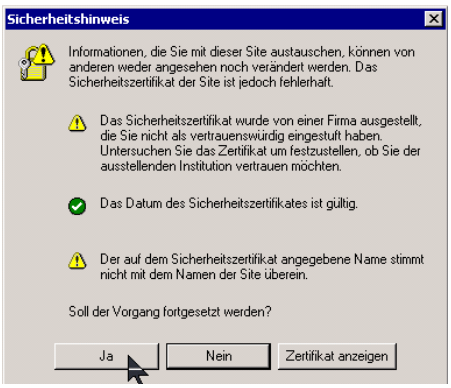


Bild 5-8 Sicherheitshinweis

Erläuterung:

Da das Gerät nur über verschlüsselte Zugänge administrierbar ist, wird es mit einem selbstunterzeichneten Zertifikat ausgeliefert.

- Quittieren Sie den entsprechenden Sicherheitshinweis mit „Ja“.

Das Login-Fenster wird angezeigt.

Bild 5-9 Login

Die Zugangsart „Benutzerfirewall“ steht beim **mGuard rs2000 nicht** zur Verfügung.

- Wählen Sie die Zugangsart — Administration oder Benutzerfirewall — und geben Sie Ihren Benutzernamen und Ihr Passwort ein, die für diese Zugangsart festgelegt sind. (Benutzerfirewall siehe „Netzwerksicherheit >> Benutzerfirewall“ auf Seite 6-161)

Für Administration ist werkseitig voreingestellt (Groß- und Kleinschreibung beachten):

Benutzername:	admin
Passwort:	mGuard

Zur Konfiguration machen Sie auf den einzelnen Seiten der Oberfläche des mGuards die gewünschten bzw. erforderlichen Angaben (siehe „Konfiguration“ auf Seite 6-1).

Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administrator-Passwort zu ändern (siehe „Authentifizierung >> Administrative Benutzer“ auf Seite 6-121).

5.4 Fernkonfiguration

Voraussetzung

Der mGuard muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.

Standardmäßig ist die Möglichkeit zur Fernkonfiguration ausgeschaltet.

Um die Möglichkeit zur Fernkonfiguration einzuschalten (siehe „Verwaltung >> Web-Einstellungen“ auf Seite 6-23 und „Zugriff“ auf Seite 6-24).

Vorgehensweise

Um von einem entfernten Rechner aus den mGuard über seine Web-Oberfläche zu konfigurieren, stellen Sie von dort die Verbindung zum mGuard her.

Gehen Sie wie folgt vor:

- Starten Sie dazu auf dem entfernten Rechner den Web-Browser (z. B. Mozilla Firefox, MS Internet-Explorer, Google Chrome oder Apple Safari; der Web-Browser muss HTTPS unterstützen).
- Als Adresse geben Sie an: Die IP-Adresse, unter der der mGuard von extern über das Internet bzw. WAN erreichbar ist, gegebenenfalls zusätzlich die Port-Nummer.

Beispiel

Ist dieser mGuard über die Adresse https://123.45.67.89/ über das Internet zu erreichen, und ist für den Fernzugang die Port-Nummer 443 festgelegt, dann muss bei der entfernten Gegenstelle im Web-Browser folgende Adresse angegeben werden: https://123.45.67.89/

Bei einer anderen Port-Nummer ist diese hinter der IP-Adresse anzugeben, z. B.: https://123.45.67.89:442/

Konfiguration

- Zur Konfiguration machen Sie auf den einzelnen Seiten der mGuard-Oberfläche die gewünschten bzw. erforderlichen Angaben (siehe „Konfiguration“ auf Seite 6-1).

6 Konfiguration

6.1 Bedienung

Sie können über das Menü auf der linken Seite die gewünschte Konfiguration anklicken, z. B. „Verwaltung, Lizenzierung“.

Dann wird im Hauptfenster die Seite angezeigt. Meistens in Form von einer oder mehrerer Registerkarten auf denen Sie Einstellungen vornehmen können. Gliedert sich eine Seite in mehrere Registerkarten, können Sie oben auf die Registerkartenzunge (auch *Tab* genannt) klicken, um zu blättern.

Arbeiten mit Registerkarten

- Sie können auf der betreffenden Registerkarte die gewünschten Einträge machen (siehe auch „Arbeiten mit sortierbaren Tabellen“ auf Seite 6-1).
- 

Damit die Einstellungen vom Gerät übernommen werden, müssen Sie auf die Schaltfläche **Übernehmen** klicken.

  Nach der Übernahme vom System erhalten Sie eine (bestätigende) Rückmeldung. Damit sind die neuen Einstellungen in Kraft. Sie bleiben auch nach einem Neustart (Reset) in Kraft.
- 

Befindet sich unten rechts die Schaltfläche **Zurück**, kehren Sie durch Klicken auf diese Schaltfläche auf die Seite zurück, von der Sie gekommen sind.

Bei Eingabe unzulässiger Werte

Wenn Sie einen unzulässigen Wert (z. B. eine unzulässige Zahl in einer IP-Adresse) angegeben haben und dann auf die Schaltfläche **Übernehmen** klicken, wird die Schrift des betreffenden Registerkarten-Titels in Rot dargestellt. Das erleichtert Ihnen das Finden des Fehlers.

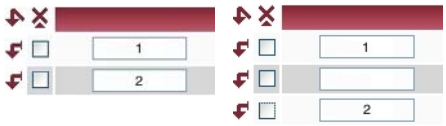
Arbeiten mit sortierbaren Tabellen

Viele Einstellungen werden als Datensätze gespeichert. Entsprechend werden Ihnen die einstellbaren Parameter und deren Werte in Form von Tabellenzeilen präsentiert. Wenn mehrere Firewall-Regeln gesetzt sind, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Gegebenenfalls ist also auf die Reihenfolge der Einträge zu achten. Durch das Verschieben von Tabellenzeilen nach unten oder oben kann die Reihenfolge geändert werden.

Bei Tabellen können Sie

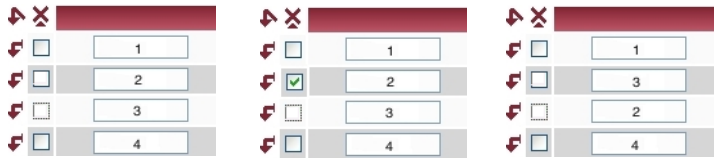
- Zeilen einfügen, um einen neuen Datensatz mit Einstellungen anzulegen (z. B. die Firewall-Einstellungen für eine bestimmte Verbindung)
- Zeilen verschieben (d. h. umsortieren) und
- Zeilen löschen, um den gesamten Datensatz zu löschen.

Einfügen von Zeilen



1. Klicken Sie auf den Pfeil , unter dem Sie eine neue Zeile einfügen wollen.
2. Die neue Zeile ist eingefügt.
   Jetzt können Sie in der Zeile Werte eintragen oder angeben

Verschieben von Zeilen



1. Markieren Sie eine oder mehrere Zeilen, die Sie verschieben wollen.
2. Klicken Sie auf den Pfeil , unter den Sie die markierten Zeilen verschieben wollen.
3. Die Zeilen sind verschoben.

Löschen von Zeilen

1. Markieren Sie die Zeilen, die Sie löschen wollen.
2. Klicken Sie auf das Zeichen zum Löschen
3. Die Zeilen sind gelöscht.

Arbeiten mit nicht sortierbaren Tabellen

Tabellen, bei denen die Reihenfolge der in ihnen enthaltenen Datensätze technisch keine Rolle spielt, sind nicht sortierbar. Es ist also nicht möglich, Zeilen einzufügen oder zu verschieben. Bei solchen Tabellen können Sie

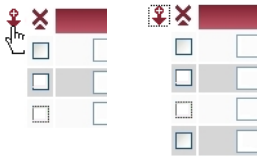
– Zeilen löschen und
– Zeilen am Tabellenende anfügen, um einen neuen Datensatz mit Einstellungen anzulegen (z. B. Benutzerfirewall-Templates)

Entsprechend unterscheiden sich die Symbole zum Einfügen einer neuer Tabellenzeile:

– für Anfügen bei **nicht** sortierbarer Tabelle

– für Einfügen bei einer sortierbaren Tabelle

Anfügen von Zeilen (nicht sortierbare Tabelle)



1. Klicken Sie auf den Pfeil  , um eine neue Zeile anzufügen.
2. Die neue Zeile wird unter der bestehenden Tabelle angefügt.
   Jetzt können Sie in der Zeile Werte eintragen oder angeben.

Schaltflächen

Folgende Schaltflächen stehen auf dem Seitenkopf auf allen Seiten zur Verfügung:

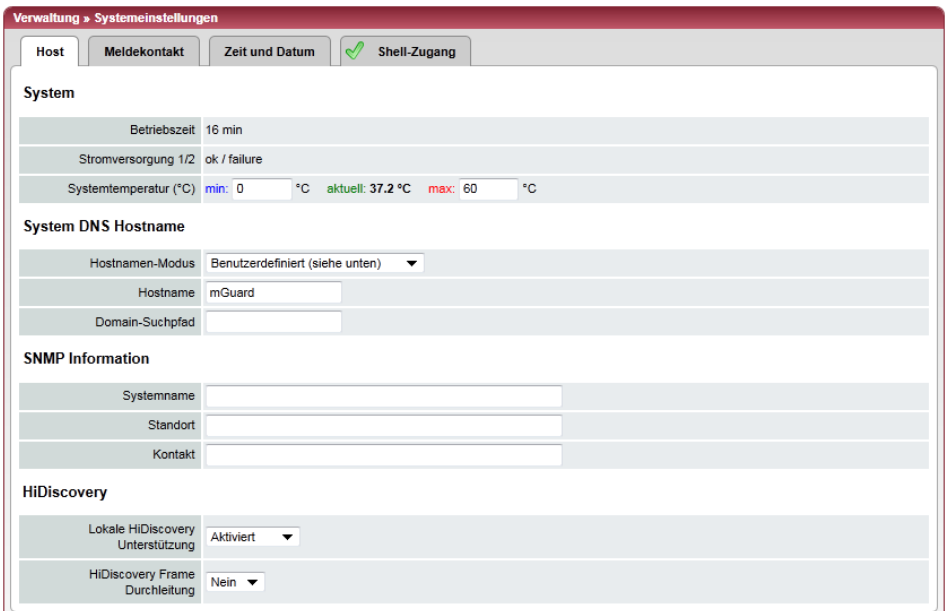
Logout 	Zum Abmelden nach einem Konfigurations-Zugriff auf den mGuard. Führt der Benutzer kein Logout durch, wird ein Logout automatisch durchgeführt, sobald keine Aktivität mehr stattfindet und die durch die Konfiguration festgelegte Zeit abgelaufen ist. Ein erneuter Zugriff kann dann nur durch erneutes Anmelden (Login) erfolgen.
Reset 	Optionale Schaltfläche. Zurücksetzen auf die alten Werte. Wenn Sie auf einer Konfigurationsseite Werte eingetragen haben und diese noch nicht mit **Übernehmen** in Kraft gesetzt haben, können Sie mit **Reset** die Seite auf die alten Werte zurücksetzen. Diese Schaltfläche ist nur dann im Kopfbereich der Seite eingeblendet, wenn der Gültigkeitsbereich der **Übernehmen**-Schaltfläche auf *„seitenübergreifend“* gestellt ist (siehe „Verwaltung >> Web-Einstellungen“ auf Seite 6-23).
Übernehmen 	Optionale Schaltfläche. Wirkt wie die Schaltfläche **Übernehmen**, gilt aber seitenübergreifend. Diese Schaltfläche ist nur dann im Kopfbereich der Seite eingeblendet, wenn der Gültigkeitsbereich der **Übernehmen**-Schaltfläche auf *„seitenübergreifend“* gestellt ist (siehe „Verwaltung >> Web-Einstellungen“ auf Seite 6-23).

6.2 Menü Verwaltung

Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administrator-Passwort zu ändern (siehe „Authentifizierung >> Administrative Benutzer“ auf Seite 6-121). Solange dies noch nicht geschehen ist, erhalten Sie oben auf der Seite einen Hinweis darauf.

6.2.1 Verwaltung >> Systemeinstellungen

6.2.1.1 Host

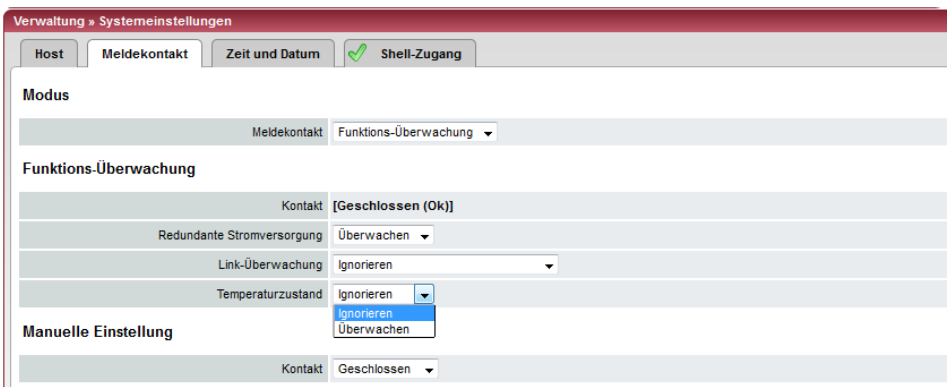


Verwaltung >> Systemeinstellung >> Host	
System	
	Betriebszeit Bisherige Laufzeit des Geräts seit dem letzten Neustart.
	(nur mGuard rs4000/rs2000, mGuard centerport, mGuard industrial rs, EAGLE mGuard)
	Stromversorgung 1/2 Zustand der beiden Netzteile (nicht beim mGuard rs2000)
	(nur mGuard rs4000/rs2000, mGuard centerport, mGuard industrial rs, EAGLE mGuard, mGuard smart²)
	Systemtemperatur (°C) Wenn der hier angegebene Temperaturbereich unter- bzw. überschritten wird, dann wird ein SNMP-Trap ausgelöst.
	(nur mGuard centerport)
	CPU-Temperatur (°C) Wenn der hier angegebene Temperaturbereich unter- bzw. überschritten wird, dann wird ein SNMP-Trap ausgelöst.

Verwaltung >> Systemeinstellung >> Host [...]		
System DNS Hostname	**Hostnamen-Modus**	Mit *Hostname Modus* und *Hostname* können Sie dem mGuard einen Namen geben. Dieser wird dann z. B. beim Einloggen per SSH angezeigt (siehe „Verwaltung >> Systemeinstellungen“ auf Seite 6-4, „Shell-Zugang“ auf Seite 6-12). Eine Namensgebung erleichtert die Administration mehrerer mGuards. **Benutzerdefiniert (siehe unten)** (Standard) Der im Feld „Hostname“ eingetragene Name wird als Name für den mGuard gesetzt. Arbeitet der mGuard im *Stealth*-Modus, muss als „Hostname-Modus“ die Option „Benutzer definiert“ gewählt werden. **Provider definiert (z. B. via DHCP)** Sofern der Netzwerk-Modus ein externes Setzen des Hostnamens erlaubt wie z. B. bei DHCP, dann wird der vom Provider übermittelte Name für den mGuard gesetzt.
	Hostname	Ist unter „Hostname-Modus“ die Option „Benutzer definiert“ ausgewählt, dann tragen Sie hier den Namen ein, den der mGuard erhalten soll. Sonst, d. h. wenn unter „Hostname-Modus“ die Option „Provider definiert“ (z. B. via DHCP) ausgewählt ist, wird ein Eintrag in diesem Feld ignoriert.
	Domain-Suchpfad	Erleichtert dem Benutzer die Eingabe eines Domain-Namens: Gibt der Benutzer den Domain-Name gekürzt ein, ergänzt der mGuard seine Eingabe um den angegebenen Domain-Suffix, der hier unter „Domain-Suchpfad“ festgelegt wird.
SNMP-Information	**Systemname**	Ein für Verwaltungszwecke frei vergebbarer Name für den mGuard, z. B. „Hermes“, „Pluto“. (Unter SNMP: sysName)
	Standort	Frei vergebbare Bezeichnung des Installationsortes, z. B. „Halle IV, Flur 3“, „Schaltschrank“. (Unter SNMP: sysLocation)
	Kontakt	Angabe einer für den mGuard zuständigen Kontaktperson, am besten mit Telefonnummer. (Unter SNMP: sysContact)
Tastatur	**(nur mGuard centerport)** 	
	Tastenanordnung	Auswahlliste zum Auswählen der passenden Tastenanordnung
	Wiederholrate	Legt fest, wie viele Zeichen die Tastatur pro Sekunde generiert, wenn dieselbe Taste gedrückt gehalten wird. (Standard: 30)

Verwaltung >> Systemeinstellung >> Host [...]		
HiDiscovery	**Wiederholverzögerung**	Legt fest, wie lange auf der Tastatur eine Taste gedrückt gehalten werden muss, bis die Wiederholfunktion in Kraft tritt, so dass so viele Zeichen pro Sekunde generiert werden, wie oben unter **Wiederholrate** festgelegt ist. (Standard: 250)
		HiDiscovery ist ein Protokoll zur Unterstützung der initialen Inbetriebnahme von neuen Netzwerkgeräten und ist im *Stealth*-Modus für das lokale Interface (LAN) des mGuards verfügbar.
	Lokale HiDiscovery Unterstützung	**Aktiviert** Das HiDiscovery-Protokoll ist aktiviert. **Nur lesend** Das HiDiscovery-Protokoll ist aktiviert, der mGuard kann jedoch nicht darüber konfiguriert werden. **Deaktiviert** Das HiDiscovery-Protokoll ist deaktiviert.
	HiDiscovery Frame Durchleitung: Ja / Nein	Steht diese Option auf **Ja**, dann werden HiDiscovery Frames vom LAN-Port nach außen über den WAN-Port weitergeleitet.

6.2.1.2 Meldekontakt



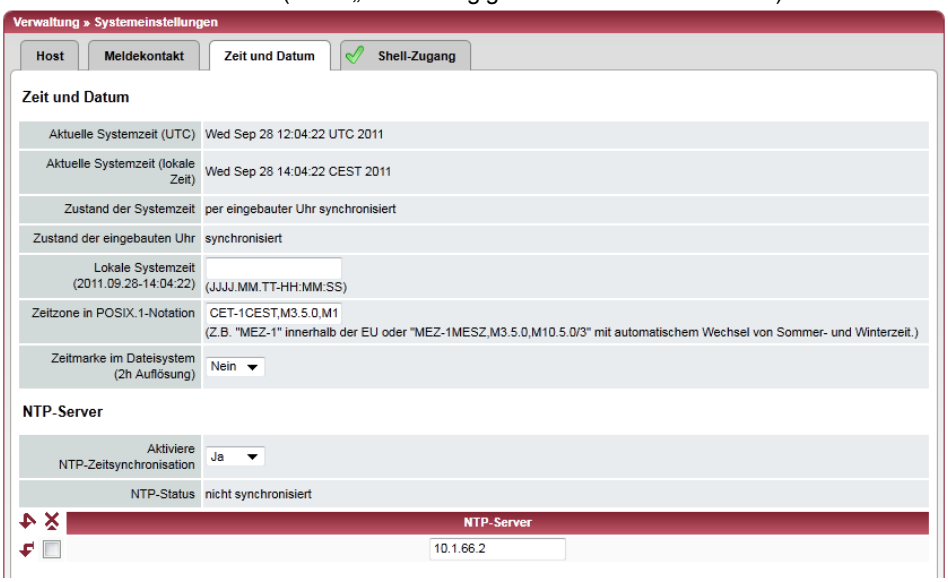
Der Meldekontakt ist ein Relais, mit welchem der mGuard Fehlerzustände signalisieren kann (siehe auch „Meldekontakt (Meldeausgang)“ auf Seite 4-6, 4-16 und 4-35)

Verwaltung >> Systemeinstellung >> Meldekontakt		
Modus	(nur mGuard rs4000/rs2000, mGuard industrial rs, EAGLE mGuard)	
	Meldekontakt	Der Meldekontakt kann automatisch durch die **Funktions-Überwachung** geschaltet werden (Standard), oder durch **Manuelle Einstellung**. Siehe auch: „mGuard rs4000/rs2000 installieren“ auf Seite 4-4, „mGuard industrial rs installieren“ auf Seite 4-12 und „mGuard blade installieren“ auf Seite 4-30.
Funktions-Überwachung	**Kontakt**	Zeigt den Zustand des Meldekontakts an. Entweder **Offen (Fehler)** oder **Geschlossen (Ok)**.

Verwaltung >> Systemeinstellung >> Meldekontakt[...]		
	Redundante Stromversorgung	Bei **Ignorieren** hat der Zustand der Stromversorgung keinen Einfluss auf den Meldekontakt. Bei **Überwachen** wird der Meldekontakt geöffnet, wenn eine der zwei Versorgungsspannungen ausfällt.
	Link-Überwachung	Überwachung des Link-Status der Ethernetanschlüsse. Mögliche Einstellungen sind: – Ignorieren – Nur Intern (trusted) überwachen – Nur Extern (untrusted) überwachen – Beide überwachen
	Temperaturzustand	Der Meldekontakt meldet eine Über- oder Untertemperatur. Der zulässige Bereich wird unter *„Systemtemperatur (°C)“* im Menü *Verwaltung >> Systemeinstellung >> Host* eingestellt. Bei **Ignorieren** hat die Temperatur keinen Einfluss auf den Meldekontakt. Bei **Überwachen** wird der Meldekontakt geöffnet, wenn die Temperatur den zulässigen Bereich verlässt.
	Verbindungsstatus der Redundanz	Nur wenn die Funktion „Redundanz“ genutzt wird (siehe Kapitel 7). Bei **Ignorieren** hat die Konnektivitätsprüfung keinen Einfluss auf den Meldekontakt. Bei **Überwachen** wird der Meldekontakt geöffnet, wenn die Konnektivitätsprüfung fehlschlägt. Das ist unabhängt davon, ob der mGuard aktiv oder im Bereitschaftszustand ist.
Manuelle Einstellung	**Kontakt**	Wenn oben unter **Meldekontakt** die Einstellung **Manuelle Einstellung** gewählt wurde, so kann man ihn hier auf **Geschlossen** oder **Offen (Alarm)** stellen.

6.2.1.3 Zeit und Datum

Stellen Sie Zeit und Datum korrekt ein, da sonst der mGuard bestimmte zeitabhängige Aktivitäten nicht starten kann (siehe „Zeitabhängige Aktivitäten“ auf Seite 6-9).



Verwaltung >> Systemeinstellung >> Zeit und Datum		
Zeit und Datum	**Aktuelle Systemzeit (UTC)**	Anzeige der aktuellen Systemzeit in Universal Time Coordinates (UTC). Solange die **NTP-Zeitsynchronisation** noch nicht aktiviert ist (s. u.), und **Zeitmarken im Dateisystem** deaktiviert sind, beginnt die Uhr mit dem 1. Januar 2000.
	Aktuelle Systemzeit (lokale Zeit)	Anzeige: Soll die eventuell abweichende aktuelle Ortszeit angezeigt werden, müssen Sie unter **Zeitzone in POSIX.1-Notation...** (s. u.) den entsprechenden Eintrag machen.
	Zustand der Systemzeit	Anzeige: Zeigt an, ob die Systemzeit des mGuards zur Laufzeit des mGuards einmal mit einer tatsächlich aktuell gültigen Zeit synchronisiert wurde. Solange hier angezeigt wird, dass die Systemzeit des mGuards nicht synchronisiert ist, führt der mGuard keine zeitgesteuerten Aktivitäten aus. Das sind Folgende:

Verwaltung >> Systemeinstellung >> Zeit und Datum [...]

Zeitabhängige Aktivitäten

– **Zeitgesteuertes Holen der Konfiguration von einem Konfigurations-Server:**
  Dies ist der Fall, wenn unter dem Menüpunkt *Verwaltung >> Zentrale Verwaltung* , *Konfiguration holen* für die Einstellung **Schedule** die Einstellung *Zeitgesteuert* ausgewählt ist (siehe „Verwaltung >> Konfigurationsprofile“ auf Seite 6-41, „Konfiguration holen“ auf Seite 6-56).
– **Das Unterbrechen der Verbindung zu bestimmter Uhrzeit beim Netzwerk-Modus PPPoE:**
  Dies ist der Fall, wenn unter dem Menüpunkt *Netzwerk >> Interfaces , Allgemein* der **Netzwerk-Modus** auf PPPoE und der **Automatische Reconnect** auf Ja gesetzt ist (siehe 6.4.1 „Netzwerk >> Interfaces“, „Netzwerk-Modus = Router, Router-Modus = PPPoE“ auf Seite 6-86).
– **Anerkennung von Zertifikaten, solange die Systemzeit noch nicht synchronisiert ist:**
  Dies ist der Fall, wenn unter dem Menüpunkt Authentifizierung >> Zertifikate , *Zertifikatseinstellungen* für die Option **Beachte den Gültigkeitszeitraum von Zertifikaten und CRLs** die Einstellung *Warte auf Synchronisation der Systemzeit* ausgewählt ist (siehe Kapitel 6.5.4 und „Zertifikatseinstellungen“ auf Seite 6-134).
– **CIFS-Integritätsprüfung:**
  Die automatische regelmäßige Prüfung der Netzlaufwerke wird nur dann gestartet, wenn der mGuard eine gültige Zeit und ein gültiges Datum hat (siehe folgender Abschnitt).

Die Systemzeit kann durch verschiedene Ereignisse gestellt oder synchronisiert werden:

– Der mGuard besitzt eine eingebaute Uhr, und diese wurde mindestens einmal mit der aktuellen Zeit synchronisiert. Nur wenn das Feld **Zustand der eingebauten Uhr** sichtbar ist, hat der mGuard eine eingebaute Uhr. An der dortigen Anzeige lässt sich ablesen, ob sie synchronisiert ist. Eine synchronisierte eingebaute Uhr sorgt dafür, dass der mGuard auch nach einem Neustart eine synchronisierte Systemzeit hat.
– Der Administrator hat zur Laufzeit dem mGuard die aktuelle Zeit mitgeteilt, indem er im Feld **Lokale Systemzeit** eine entsprechende Eingabe gemacht hat.
– Der Administrator hat die Einstellung **Zeitmarke im Dateisystem** auf *Ja* gestellt und dem mGuard entweder per NTP (siehe unten unter *NTP-Server*) die aktuelle Systemzeit erfahren lassen oder per Eingabe in **Lokale Systemzeit** selbst eingestellt. Dann wird der mGuard auch ohne eingebaute Uhr nach einem Neustart sofort seine Systemzeit mit Hilfe des Zeitstempels synchronisieren (auch wenn sie danach eventuell noch einmal per NTP genauer eingestellt wird).
– Der Administrator hat unten unter **NTP-Server** die NTP-Zeitsynchronisation aktiviert und die Adressen von mindestens einem NTP-Server angegeben, und der mGuard hat erfolgreich Verbindung zu mindestens einem der festgelegten NTP-Server aufgenommen. Bei funktionierendem Netzwerk geschieht dies in wenigen Sekunden nach dem Neustart. Die Anzeige im Feld **NTP-Status** wechselt eventuell erheblich später erst auf „synchronisiert“ (siehe dazu die Erklärung weiter unten zu **NTP-Status)**.

Verwaltung >> Systemeinstellung >> Zeit und Datum [...]

Zustand der eingebauten Uhr

(bei *mGuard rs4000/rs2000, mGuard centerport, mGuard industrial rs*, *mGuard delta* und bei *mGuard smart²*, aber nicht bei *mGuard smart*)

Der Zustand der eingebauten Uhr ist nur sichtbar, wenn der mGuard eine Uhr besitzt, die auch dann weiter läuft, wenn der mGuard nicht mit Strom versorgt wird und eingeschaltet ist. Die Anzeige gibt an, ob die Uhr einmal mit der aktuellen Zeit synchronisiert wurde. Die eingebaute Uhr wird immer dann synchronisiert, wenn die Systemzeit des mGuards synchronisiert wurde.

Wenn die Uhr einmal synchronisiert ist, wechselt ihr Zustand nur dann wieder auf „nicht synchronisiert“, wenn die Firmware neu auf das Gerät aufgebracht wird (siehe Kapitel 8.3) oder wenn bei ausgeschaltetem Gerät

– der Kondensator (mGuard industrial rs),
– die Batterie (mGuard centerport, mGuard delta),
– oder der Akku (mGuard rs4000/rs2000, mGuard smart²)

die eingebaute Uhr zwischenzeitlich nicht mehr hinreichend unter Spannung hielt.

Lokale Systemzeit

Hier können Sie die Zeit des mGuards setzen, falls kein NTP-Server eingestellt wurde (s. u.) oder aber der NTP-Server nicht erreichbar ist.

Das Datum und die Zeit werden in dem Format JJJJ.MM.TT-HH:MM:SS angegeben:

JJJJ	Jahr
MM	Monat
TT	Tag
HH	Stunde

Zeitzone in POSIX.1-Notation...

Soll oben unter *Aktuelle Systemzeit* nicht die mittlere Greenwich-Zeit angezeigt werden sondern Ihre aktuelle Ortszeit (abweichend von der mittleren Greenwich-Zeit), dann tragen Sie hier ein, um wieviel Stunden bei Ihnen die Zeit voraus bzw. zurück ist.

Beispiele: In Berlin ist die Uhrzeit der mittleren Greenwich-Zeit um 1 Stunde voraus. Also tragen Sie ein: MEZ-1.

In New York geht die Uhr bezogen auf die mittlere Greenwich-Zeit um 5 Stunden nach. Also tragen Sie ein: MEZ+5.

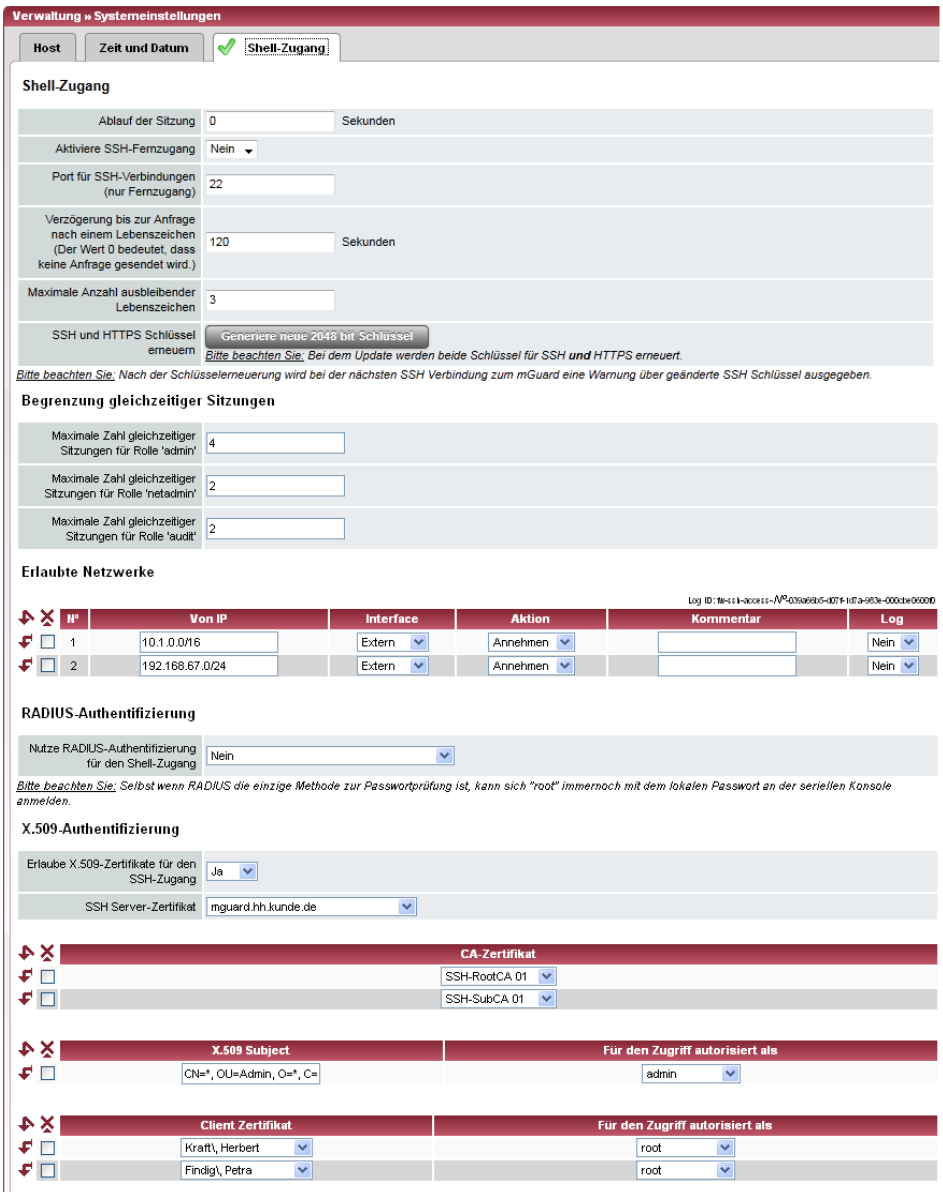
Wichtig ist allein die Angabe -1, -2 oder +1 usw., weil nur sie ausgewertet wird; die davor stehenden Buchstaben nicht. Sie können „MEZ“ oder beliebig anders lauten, z. B. auch „UTC“.

Wünschen Sie die Anzeige der MEZ-Uhrzeit (= gültig für Deutschland) mit automatischer Umschaltung auf Sommer- bzw. Winterzeit geben Sie ein:
MEZ-1MESZ,M3.5.0,M10.5.0/3

Verwaltung >> Systemeinstellung >> Zeit und Datum [...]		
	Zeitmarke im Dateisystem (2h Auflösung): Ja / Nein	Ist dieser Schalter auf **Ja** gesetzt, schreibt der mGuard alle zwei Stunden die aktuelle Systemzeit in seinen Speicher. Wird der mGuard aus- und wieder eingeschaltet, wird nach dem Einschalten eine Uhrzeit in diesem 2-Stunden-Zeitfenster angezeigt und nicht eine Uhrzeit am 1. Januar 2000.
NTP-Server	(NTP - Network Time Protocol) Der mGuard kann für Rechner, die an seinem LAN-Port angeschlossen sind, als NTP-Server fungieren. In diesem Fall sind die Rechner so zu konfigurieren, dass als Adresse des NTP-Servers die lokale Adresse des mGuards angegeben ist. Wenn der mGuard im *Stealth*-Modus betrieben wird, muss bei den Rechnern die Management IP-Adresse des mGuards verwendet werden (sofern diese konfiguriert ist), oder es muss die IP-Adresse 1.1.1.1 als lokale Adresse des mGuards angegeben werden. Damit der mGuard als NTP-Server fungieren kann, muss er selber das aktuelle Datum und die aktuelle Uhrzeit von einem NTP-Server (= Zeit-Server) beziehen. Dazu muss die Adresse von mindestens einem NTP-Server angegeben werden. Zusätzlich muss dieses Feature aktiviert sein.	
	Aktiviere NTP-Zeitsynchronisation: Ja / Nein	Sobald das NTP aktiviert ist, bezieht der mGuard Datum und Uhrzeit von einem oder mehreren Zeit-Server(n) und synchronisiert sich mit ihm bzw. ihnen. Die initiale Zeitsynchronisation kann bis zu 15 Minuten dauern. Während dieser Zeitspanne vollzieht der mGuard immer wieder Vergleiche zwischen der Zeitangabe des externen Zeit-Servers und der eigenen Uhrzeit, um diese so präzise wie möglich abzustimmen. Erst dann kann der mGuard als NTP-Server für die an seiner LAN-Schnittstelle angeschlossenen Rechner fungieren und ihnen die Systemzeit liefern. Eine initiale Zeitsynchronisation mit dem externen Zeit-Server erfolgt nach jedem Booten, es sei denn, der mGuard verfügt über eine eingebaute Uhr (*mGuard rs4000/rs2000*, *mGuard centerport, mGuard industrial rs*, *mGuard delta* und *mGuard smart²*, nicht *mGuard smart*). Nach der initialen Zeitsynchronisation vergleicht der mGuard regelmäßig die Systemzeit mit den Zeit-Servern. In der Regel erfolgen Nachjustierungen nur noch im Sekundenbereich.
	NTP-Status	Anzeige des aktuellen NTP-Status. Gibt an, ob sich der auf dem mGuard selbst laufende NTP-Server mit hinreichender Genauigkeit mit den konfigurierten NTP-Servern synchronisiert hat. Wenn die Systemuhr des mGuards vor der Aktivierung der NTP-Zeitsynchronisation noch nie synchronisiert war, kann die Synchronisierung bis zu 15 Minuten dauern. Dennoch stellt der NTP-Server die Systemuhr des mGuards nach wenigen Sekunden auf die aktuelle Zeit um, sobald er erfolgreich einen der konfigurierten NTP-Server kontaktiert hat. Dann betrachtet der mGuard seine Systemzeit auch bereits als synchronisiert. Nachjustierungen erfolgen in der Regel nur noch im Sekundenbereich.

Verwaltung >> Systemeinstellung >> Zeit und Datum [...]	
NTP-Server	Geben Sie hier einen oder mehrere Zeit-Server an, von denen der mGuard die aktuelle Zeitangabe beziehen soll. Falls Sie mehrere Zeit-Server angeben, verbindet sich der mGuard automatisch mit allen, um die aktuelle Zeit zu ermitteln.

6.2.1.4 Shell-Zugang



Wird eingeblendet, wenn *Erlaube X.509-Zertifikate für den SSH-Zugang* auf **Ja** gesetzt ist

Die Konfiguration des mGuards darf nicht gleichzeitig über den Web-Zugriff, den Shell-Zugang oder SNMP erfolgen. Eine zeitgleiche Konfiguration über die verschiedenen Zugangsmethoden führt möglicherweise zu unerwarteten Ergebnissen.

Verwaltung >> Systemeinstellungen >> Shell-Zugang

Shell-Zugang

Bei eingeschaltetem SSH-Fernzugang kann der mGuard **von entfernten Rechnern aus** über die Kommandozeile konfiguriert werden.

Standardmäßig ist diese Option ausgeschaltet.

ACHTUNG: Wenn Sie Fernzugriff ermöglichen, achten Sie darauf, dass sichere Passwörter für *root* und *admin* festgelegt sind.

Für SSH-Fernzugang machen Sie folgende Einstellungen:

Ablauf der Sitzung (Sekunden)

Gibt an, nach wie viel Zeit (in Sekunden) der Inaktivität die Sitzung automatisch beendet wird, d. h. ein automatisches Ausloggen stattfindet. Bei Einstellung von 0 (= Werkseinstellung) findet kein automatisches Beenden der Sitzung statt.

Der angegebene Wert gilt auch, wenn der Benutzer den Shell-Zugang über die serielle Schnittstelle anstatt über das SSH-Protokoll verwendet.

Die Wirkung der Einstellung des Feldes „Ablauf der Sitzung“ wird vorübergehend ausgesetzt, wenn die Bearbeitung eines Shell-Kommandos die eingestellte Anzahl von Sekunden überschreitet.

Im Unterschied hierzu kann die Verbindung auch abgebrochen werden, wenn die Funktionsfähigkeit der Verbindung nicht mehr gegeben ist, siehe „Verzögerung bis zur Anfrage nach einem Lebenszeichen“ auf Seite 6-14.

Aktiviere SSH-Fernzugang: Ja / Nein

Wollen Sie SSH-Fernzugriff ermöglichen, setzen Sie diesen Schalter auf **Ja**. SSH-Zugriff über *Intern* (d. h. aus dem direkt angeschlossenen LAN oder vom direkt angeschlossenen Rechner aus) ist unabhängig von der Schalterstellung möglich.

Um Zugriffsmöglichkeiten auf den mGuard differenziert festzulegen, müssen Sie auf dieser Seite unter **Erlaubte Netzwerke** die Firewall-Regeln für die verfügbaren Interfaces entsprechend definieren.

Verwaltung >> Systemeinstellungen >> Shell-Zugang [...]		
	Port für SSH-Verbindungen (nur Fernzugang)	Standard: 22 Wird diese Port-Nummer geändert, gilt die geänderte Port-Nummer nur für Zugriffe über das Interface *Extern, Extern 2, VPN* und *Einwahl*. Für internen Zugriff gilt weiterhin 22. Die entfernte Gegenstelle, die den Fernzugriff ausübt, muss beim Login gegebenenfalls die Port-Nummer angeben, die hier festgelegt ist. Beispiel: Ist dieser mGuard über die Adresse 123.124.125.21 über das Internet zu erreichen, und ist für den Fernzugang gemäß Standard die Port-Nummer 22 festgelegt, dann muss bei der entfernten Gegenstelle im SSH-Client (z. B. PuTTY oder OpenSSH) diese Port-Nummer evtl. nicht angegeben werden. Bei einer anderen Port-Nummer (z. B. 2222) ist diese anzugeben, z. B.: ssh -p 2222 123.124.125.21
	Verzögerung bis zur Anfrage nach einem Lebenszeichen	Default: 120 Sekunden Einstellbar sind Werte von 0 bis 3600 Sekunden. Positive Werte bedeuten, dass der mGuard innerhalb der verschlüsselten SSH-Verbindung eine Anfrage an die Gegenstelle sendet, ob sie noch erreichbar ist. Die Anfrage wird gesendet, wenn für die angegebene Anzahl von Sekunden keine Aktivität von der Gegenstelle bemerkt wurde (zum Beispiel durch Netzwerkverkehr innerhalb der verschlüsselten Verbindung). Der hier eingetragene Wert bezieht sich auf die Funktionsfähigkeit der verschlüsselten SSH-Verbindung. Solange diese gegeben ist, wird die SSH-Verbindung vom mGuard wegen dieser Einstellungen nicht beendet, selbst wenn der Benutzer während dieser Zeit keine Aktion ausführt. Da die Anzahl der gleichzeitig geöffneten Sitzungen begrenzt ist (siehe *Begrenzung gleichzeitiger Sitzungen*), ist es wichtig, abgelaufene Sitzungen zu beenden. Deshalb wird ab Version 7.4.0 die Anfrage nach einem Lebenszeichen auf 120 Sekunden voreingestellt. Bei maximal drei Anfragen nach einem Lebenszeichen, wird eine abgelaufende Sitzung nach sechs Minuten entdeckt und entfernt. In vorherigen Versionen war die Voreinstellung „0“. Das bedeutet, dass keine Anfragen nach einem Lebenszeichen gesendet werden. Wenn es wichtig ist, dass kein zusätzlicher Traffic erzeugt wird, können Sie den Wert anpassen. Bei der Einstellung „0“ in Kombination mit der „*Begrenzung gleichzeitiger Sitzungen* “ kann es geschehen, dass ein weiterer Zugriff blockiert wird, wenn zu viele Sitzungen durch Netzwerkfehler unterbrochen aber nicht geschlossen wurden.

Verwaltung >> Systemeinstellungen >> Shell-Zugang [...]

	Maximale Anzahl ausbleibender Lebenszeichen	Gibt an, wie oft Antworten auf Anfragen nach Lebenszeichen der Gegenstelle ausbleiben dürfen. Wenn z. B. alle 15 Sekunden nach einem Lebenszeichen gefragt werden soll und dieser Wert auf 3 eingestellt ist, dann wird die SSH-Verbindung gelöscht, wenn nach circa 45 Sekunden immer noch kein Lebenszeichen gegeben wurde.
	SSH und HTTPS Schlüssel erneuern	**Generiere neue 2048 bit Schlüssel** Schlüssel, die mit einer älteren Firmware erstellt worden sind, sind möglicherweise schwach und sollten erneuert werden. • Klicken Sie auf diese Schaltfläche, um neue Schlüssel zu erzeugen. • Beachten Sie die Fingerprints der neu generierten Schlüssel. • Loggen Sie sich über HTTPS ein und vergleichen Sie die Zertifikat-Informationen, die vom Browser zur Verfügung gestellt werden.
Begrenzung gleichzeitiger Sitzungen	Beim administrativen Zugang zum mGuard über SSH gibt es je nach vordefiniertem Benutzer eine Begrenzung der Anzahl von gleichzeitigen Sitzungen. Pro Sitzung wird etwa 0,5 MB Speicherplatz benötigt. Der Benutzer „root“ hat einen uneingeschränkten Zugang. Beim administrativen Zugang über einen anderen Benutzer *(admin, netadmin* und *audit)* ist die Anzahl der gleichzeitigen Sitzungen eingeschränkt. Sie können die Anzahl hier festlegen. Die Einschränkung hat keine Auswirkung auf bereits bestehende Sitzungen, sondern nur auf neu aufgebaute Zugriffe.	
	Maximale Zahl gleichzeitiger Sitzungen für die Rolle „admin“	2 bis 2147483647 Für "admin" sind mindestens 2 gleichzeitig erlaubte Sitzungen erforderlich, damit sich "admin" nicht selbst aussperrt.
	Maximale Zahl gleichzeitiger Sitzungen für die Rolle „netadmin“	0 bis 2147483647 Bei „0“ ist keine Sitzung erlaubt. Es kann sein, dass der Benutzer „netadmin“ nicht verwendet wird.
	Maximale Zahl gleichzeitiger Sitzungen für die Rolle „audit“	0 bis 2147483647 Bei „0“ ist keine Sitzung erlaubt. Es kann sein, dass der Benutzer „audit“ nicht verwendet wird.
Erlaubte Netzwerke		

N°	Von IP	Interface	Aktion	Kommentar	Log
1	10.1.0.0/16	Extern	Annehmen		Nein
2	192.168.67.0/24	Extern	Annehmen		Nein

Verwaltung >> Systemeinstellungen >> Shell-Zugang [...]

Listet die eingerichteten Firewall-Regeln auf. Sie gelten für eingehende Datenpakete eines SSH-Fernzugriffs.

Sind mehrere Firewall-Regeln gesetzt, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Sollten nachfolgend in der Regelliste weitere Regeln vorhanden sein, die auch passen würden, werden diese ignoriert.

Die hier angegebenen Regeln treten nur in Kraft, wenn der Schalter **Aktiviere SSH-Fernzugang** auf **Ja** steht. Weil Zugriffe von *Intern* auch möglich sind, wenn dieser Schalter auf **Nein** steht, tritt für diesen Fall eine Firewall-Regel, die den Zugriff von *Intern* verwehren würde, nicht in Kraft.

Bei den Angaben haben Sie folgende Möglichkeiten:

Von IP

Geben Sie hier die Adresse des Rechners oder Netzes an, von dem der Fernzugang erlaubt beziehungsweise verboten ist.

Bei den Angaben haben Sie folgende Möglichkeiten:

IP-Adresse: **0.0.0.0/0** bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise, siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 6-261

Interface

Extern / Intern / Extern 2 / VPN / Einwahl

Extern 2 und *Einwahl* nur bei Geräten mit serieller Schnittstelle, Siehe „Netzwerk >> Interfaces“ auf Seite 6-64.

Gibt an, für welches Interface die Regel gelten soll.

Sind keine Regeln gesetzt oder greift keine Regel, gelten folgende Standardeinstellungen:

SSH-Zugriff ist erlaubt über *Intern*, *VPN* und *Einwahl*. Zugriffe über *Extern* und *Extern 2* werden verwehrt.

Legen Sie die Zugriffsmöglichkeiten nach Bedarf fest.

ACHTUNG: Wenn Sie Zugriffe über *Intern, VPN* oder *Einwahl* verwehren wollen, müssen Sie das explizit durch entsprechende Firewall-Regeln bewirken, in der Sie als Aktion z. B. *Verwerfen* festlegen.

Damit Sie sich nicht aussperren, müssen Sie eventuell gleichzeitig den Zugriff über ein anderes Interface explizit mit *Annehmen* erlauben, bevor Sie durch Klicken auf die **Übernehmen**-Schaltfläche die neue Einstellung in Kraft setzen. Sonst muss bei Aussperrung die Recovery-Prozedur durchgeführt werden.

Verwaltung >> Systemeinstellungen >> Shell-Zugang [...]		
	Aktion	Möglichkeiten: – **Annehmen** bedeutet, die Datenpakete dürfen passieren. – **Abweisen** bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat *Abweisen* dieselbe Wirkung wie *Verwerfen*.) – **Verwerfen** bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information über deren Verbleib erhält.
	Kommentar	Ein frei wählbarer Kommentar für diese Regel.
	Log	Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel – das Ereignis protokolliert werden soll – *Log* auf **Ja** setzen – oder das Ereignis nicht protokolliert werden soll – *Log* auf **Nein** setzen (werkseitige Voreinstellung).

Verwaltung >> Systemeinstellungen >> Shell-Zugang [...]

RADIUS-Authentifizierung

Dieser Menüpunkt gehört nicht zum Funktionsumfang vom mGuard rs2000.

Nutze RADIUS-Authentifizierung für den Shell-Zugang

Bei **Nein** wird das Passwort der Benutzer, die sich über den Shell-Zugang einloggen, über die lokale Datenbank auf dem mGuard geprüft.

Wählen Sie **Ja**, damit Benutzer über einen RADIUS-Server authentifiziert werden. Dies gilt für Anwender, die über den Shell-Zugang mit Hilfe von SSH oder einer seriellen Konsole auf den mGuard zugreifen wollen. Nur bei den vordefinierten Benutzern *(root, admin, netadmin* und *audit)* wird das Passwort lokal geprüft.

Wenn Sie unter **X.509-Authentifizierung** den Punkt **Erlaube X.509-Zertifikate für den SSH-Zugang** auf **Ja** stellen, kann alternativ das X.509-Authentifizierungsverfahren verwendet werden. Welches Verfahren von einem Benutzer tatsächlich verwendet wird, hängt davon ab, wie er seinen SSH-Client verwendet.

Wenn Sie eine RADIUS-Authentifizierung das erste Mal einrichten, wählen Sie **Ja**.

Die Auswahl von **Als einzige Methode zur Passwortprüfung** ist nur für erfahrene Anwender geeignet, da Sie damit den Zugang zum mGuard komplett sperren können.

Wenn Sie planen, die RADIUS-Authentifizierung **als einzige Methode zur Passwortprüfung** einzurichten, empfehlen wir Ihnen ein „Customized Default Profile“ anzulegen, das die Authentifizierungsmethode zurücksetzt.

Die vordefinierten Benutzer *(root, admin, netadmin* und *audit)* können sich dann nicht mehr per SSH oder serieller Konsole beim mGuard anmelden.

Einzige Ausnahme: Eine Authentifizierung über eine extern erreichbare serielle Konsole bleibt möglich, wenn das lokale Passwort für den Benutzernamen *root* korrekt eingegeben wird.

X.509-Authentifizierung

Verwaltung >> Systemeinstellungen >> Shell-Zugang

X.509-Authentifizierung

Dieser Menüpunkt gehört nicht zum Funktionsumfang vom mGuard rs2000.

Erlaube X.509-Zertifikate für den SSH-Zugang

- Bei **Nein** werden zur Authentifizierung nur die herkömmlichen Authentifizierungsverfahren (Benutzername und Passwort bzw. privater und öffentlicher Schlüssel) erlaubt, nicht das X.509-Authentifizierungsverfahren.
- Bei **Ja** kann zur Authentifizierung zusätzlich zum herkömmlichen Authentifizierungsverfahren (wie es auch bei **Nein** verwendet wird) das X.509-Authentifizierungsverfahren verwendet werden.
- Bei **Ja** ist festzulegen,
  - wie sich der mGuard gemäß X.509 beim SSH-Client authentisiert, siehe **SSH Server-Zertifikat (1)**
  - wie der mGuard den entfernten SSH-Client gemäß X.509 authentifiziert, siehe **SSH Server-Zertifikat (2)**

SSH-Server-Zertifikat (1)

Legt fest, wie sich der mGuard beim SSH-Client ausweist.

In der Auswahlliste eines der Maschinenzertifikate auswählen oder den Eintrag *Keines*.

Keines:

Bei Auswahl von *Keines* authentisiert sich der SSH-Server des mGuards nicht per X.509-Zertifikat gegenüber dem SSH-Client, sondern er benutzt einen Server-Schlüssel und verhält sich damit so wie ältere Versionen des mGuards.

Wird eines der Maschinenzertifikate ausgewählt, wird dem SSH-Client das zusätzlich angeboten, so dass dieser es sich aussuchen kann, ob er das herkömmliche Authentifizierungsverfahren oder das gemäß X.509 anwenden will.

Die Auswahlliste stellt die Maschinenzertifikate zur Wahl, die in den mGuard unter Menüpunkt *Authentifizierung >> Zertifikate* geladen worden sind (siehe Seite 6-128).

Verwaltung >> Systemeinstellungen >> Shell-Zugang [...]

SSH-Server-Zertifikat (2)

Legt fest wie der mGuard den SSH-Client authentifiziert

Nachfolgend wird festgelegt, wie der mGuard die Authentizität des SSH-Clients prüft.

Die Tabelle unten zeigt, welche Zertifikate dem mGuard zur Authentifizierung des SSH-Clients zur Verfügung stehen müssen, wenn der SSH-Client bei Verbindungsaufnahme eines der folgenden Zertifikatstypen vorzeigt:

– ein von einer CA signiertes Zertifikat
– ein selbst signiertes Zertifikat

Zum Verständnis der nachfolgenden Tabelle siehe Kapitel Kapitel 6.5.4, „Authentifizierung >> Zertifikate“.

Authentifizierung bei SSH

Die Gegenstelle zeigt vor:	Zertifikat (personenbezogen) von **CA signiert**	Zertifikat (personenbezogen) **selbst signiert**
Der mGuard authentifiziert die Gegenstelle anhand von...	⇕	⇕
	...allen CA-Zertifikaten, die mit dem von der Gegenstelle vorgezeigten Zertifikat die Kette bis zum Root-CA-Zertifikat bilden ggf. PLUS Gegenstellen-Zertifikaten, **wenn** sie als Filter verwendet werden	Gegenstellen-Zertifikat

Nach dieser Tabelle sind die Zertifikate zur Verfügung zu stellen, die der mGuard zur Authentifizierung des jeweiligen SSH-Clients heranziehen muss.

Die nachfolgenden Anleitungen gehen davon aus, dass die Zertifikate bereits ordnungsgemäß im mGuard installiert sind (siehe Kapitel 6.5.4, „Authentifizierung >> Zertifikate“).

Ist unter Menüpunkt *Authentifizierung >> Zertifikate , Zertifikatseinstellungen* die Verwendung von Sperrlisten (= CRL-Prüfung) aktiviert, wird jedes von einer CA signierte Zertifikat, das SSH-Clients „vorzeigen“, auf Sperrung geprüft.

Verwaltung >> Systemeinstellungen >> Shell-Zugang

CA-Zertifikat

Die Konfiguration ist nur dann erforderlich, wenn der SSH-Client ein von einer CA signiertes Zertifikat vorzeigt.

Es sind alle CA-Zertifikate zu konfigurieren, die der mGuard benötigt, um mit den von SSH-Clients vorgezeigten Zertifikaten jeweils die Kette bis zum jeweiligen Root-CA-Zertifikat zu bilden.

Die Auswahlliste stellt die CA-Zertifikate zur Wahl, die in den mGuard unter Menüpunkt *Authentifizierung >> Zertifikate* geladen worden sind.

Verwaltung >> Systemeinstellungen >> Shell-Zugang [...]

X.509-Subject

Ermöglicht die Filtersetzung in Bezug auf den Inhalt des Feldes *Subject* im Zertifikat, das vom SSH-Client vorgezeigt wird. Dadurch ist es möglich, den Zugriff von SSH-Clients, die der mGuard auf Grundlage von Zertifikatsprüfungen im Prinzip akzeptieren würde, zu beschränken bzw. freizugeben:

- Beschränkung auf bestimmte *Subjects* (d. h. Personen) und/oder auf *Subjects*, die bestimmte Merkmale (Attribute) haben, oder
- Freigabe für alle Subjects (siehe Glossar unter *„Subject, Zertifikat“ auf Seite 9-5).*

Das Feld *X.509-Subject* darf nicht leer bleiben.

Freigabe für alle Subjects (d. h. Personen):

Mit * (Sternchen) im Feld *X.509-Subject* legen Sie fest, dass im vom SSH-Client vorgezeigten Zertifikat beliebige Subject-Einträge erlaubt sind. Dann ist es überflüssig, das im Zertifikat jeweils angegebene Subject zu kennen oder festzulegen.

Beschränkung auf bestimmte Subjects (d. h. Personen) oder auf Subjects, die bestimmte Merkmale (Attribute) haben:

Im Zertifikat wird der Zertifikatsinhaber im Feld *Subject* angegeben, dessen Eintrag sich aus mehreren Attributen zusammensetzt. Diese Attribute werden entweder als Object Identifier ausgedrückt (z. B.: 132.3.7.32.1) oder, geläufiger, als Buchstabenkürzel mit einem entsprechenden Wert.

Beispiel: CN=Max Muster, O=Fernwartung GmbH, C=DE

Sollen bestimmte Attribute des Subjects ganz bestimmte Werte haben, damit der mGuard den SSH-Client akzeptiert, muss das entsprechend spezifiziert werden. Die Werte der anderen Attribute, die beliebig sein können, werden dann durch das Wildcard ***** (Sternchen) angegeben.

Beispiel: CN=*, O=*, C=DE (mit oder ohne Leerzeichen zwischen Attributen)

Bei diesem Beispiel müsste im Zertifikat im Subject das Attribut „C=DE“ stehen. Nur dann würde der mGuard den Zertifikatsinhaber (= Subject) als Kommunikationspartner akzeptieren. Die anderen Attribute könnten in den zu filternden Zertifikaten beliebige Werte haben.

Wird ein Subject-Filter gesetzt, muss zwar die Anzahl, nicht aber die Reihenfolge der angegebenen Attribute mit der übereinstimmen, wie sie in den Zertifikaten gegeben ist, auf die der Filter angewendet werden soll.

Auf Groß- und Kleinschreibung achten.

Es können mehrere Filter gesetzt werden, die Reihenfolge ist irrelevant.

Verwaltung >> Systemeinstellungen >> Shell-Zugang [...]

Für den Zugriff autorisiert als	Alle Benutzer / root / admin / netadmin / audit Zusätzlicher Filter, der festlegt, dass der SSH-Client für eine bestimmte Verwaltungsebene autorisiert sein muss, um Zugriff zu erhalten. Der SSH-Client zeigt bei Verbindungsaufnahme nicht nur sein Zertifikat vor, sondern gibt auch den Systembenutzer an, für den die SSH-Sitzung eröffnet werden soll (*root, admin, netadmin, audit*). Nur wenn diese Angabe mit der übereinstimmt, die hier festgelegt wird, erhält er Zugriff. Mit der Einstellung *Alle Benutzer* ist der Zugriff für jeden der vorgenannten Systembenutzer möglich.  Die Einstellmöglichkeiten *netadmin* und *audit* beziehen sich auf Zugriffsrechte mit dem Innominate Device Manager.
Client-Zertifikat	Die Konfiguration ist in den folgenden Fällen erforderlich: – SSH-Clients zeigen jeweils ein selbst signiertes Zertifikat vor. – SSH-Clients zeigen jeweils ein von einer CA signiertes Zertifikat vor. Es soll eine Filterung erfolgen: Zugang erhält nur der, dessen Zertifikats-Kopie im mGuard als Gegenstellen-Zertifikat installiert ist und in dieser Tabelle dem mGuard als *Client-Zertifikat* zur Verfügung gestellt wird. Dieser Filter ist dem *Subject*-Filter darüber **nicht** nachgeordnet, sondern ist auf gleicher Ebene angesiedelt, ist also dem *Subject*-Filter mit einem logischen ODER beigeordnet. Der Eintrag in diesem Feld legt fest, welches Gegenstellen-Zertifikat der mGuard heranziehen soll, um die Gegenstelle, den SSH-Client, zu authentifizieren. Dazu in der Auswahlliste eines der Gegenstellen-Zertifikate auswählen. Die Auswahlliste stellt die Gegenstellen-Zertifikate zur Wahl, die in den mGuard unter Menüpunkt *Authentifizierung >> Zertifikate* geladen worden sind.

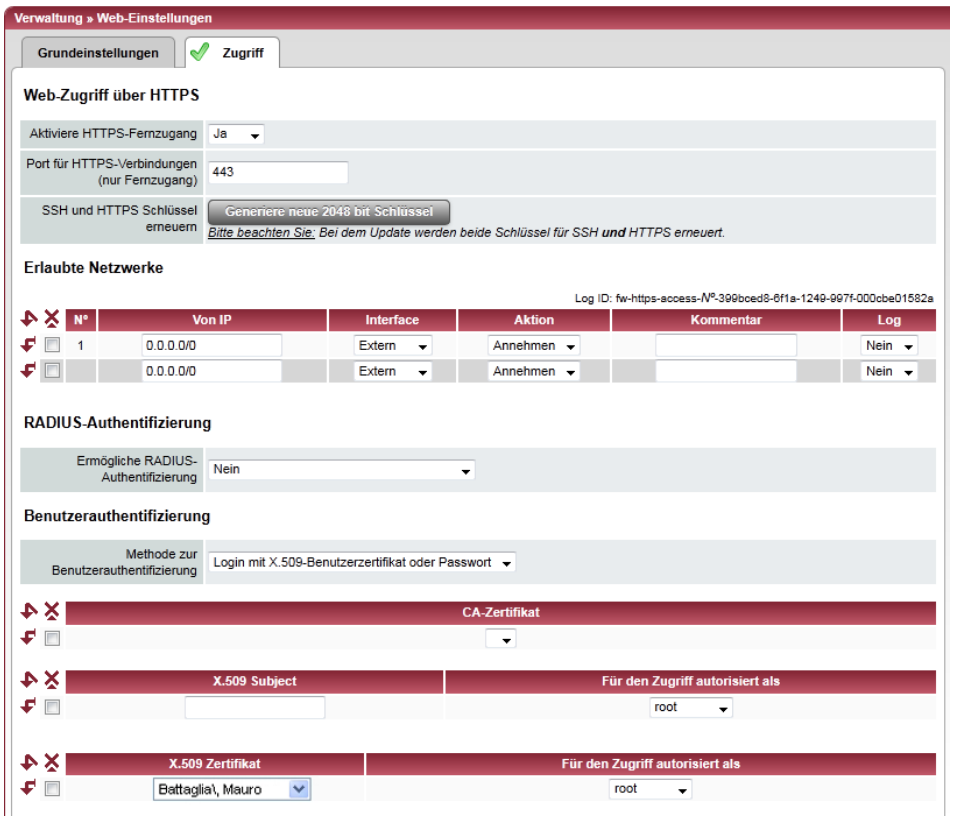
Verwaltung >> Systemeinstellungen >> Shell-Zugang [...]		
	Für den Zugriff autorisiert als	Alle Benutzer / root / admin / netadmin / audit Filter, der festlegt, dass der SSH-Client für eine bestimmte Verwaltungsebene autorisiert sein muss, um Zugriff zu erhalten. Der SSH-Client zeigt bei Verbindungsaufnahme nicht nur sein Zertifikat vor, sondern gibt auch den Systembenutzer an, für den die SSH-Sitzung eröffnet werden soll (*root, admin, netadmin, audit*). Nur wenn diese Angabe mit der übereinstimmt, die hier festgelegt wird, erhält er Zugriff. Mit der Einstellung *Alle Benutzer* ist der Zugriff für jeden der vorgenannten Systembenutzer möglich. Die Einstellmöglichkeiten *netadmin* und *audit* beziehen sich auf Zugriffsrechte mit dem Innominate Device Manager.

6.2.2 Verwaltung >> Web-Einstellungen

6.2.2.1 Grundeinstellungen

Verwaltung >> Web-Einstellungen >> Grundeinstellungen		
Grundeinstellungen	**Sprache**	Ist in der Sprachauswahlliste **(Automatisch)** ausgewählt, übernimmt das Gerät die Spracheinstellung aus dem Browser des Rechners.
	Ablauf der Sitzung (Sekunden)	Sekunden der Inaktivität, nach denen der Benutzer von der Web-Schnittstelle des mGuards automatisch abgemeldet wird. Mögliche Werte: 15 bis 86400 (= 24 Stunden)
	Gültigkeitsbereich der Schaltfläche „Übernehmen“	Mit **Pro Seite** wird festgelegt, dass Sie auf jeder Seite, auf der Sie Änderungen vorgenommen haben, jeweils die Schaltfläche **Übernehmen** zu klicken haben, damit die Einstellungen vom mGuard übernommen und in Kraft gesetzt werden. Mit **Seitenübergreifend** wird festgelegt, dass Sie nach Vornahme von Änderungen auf mehreren Seiten nur einmalig **Übernehmen** klicken müssen.

6.2.2.2 Zugriff



Nur eingeblendet bei *Login mit X.509-Benutzerzertifikat*

Die Konfiguration des mGuards darf nicht gleichzeitig über den Web-Zugriff, den Shell-Zugang oder SNMP erfolgen. Eine zeitgleiche Konfiguration über die verschiedenen Zugangsmethoden führt möglicherweise zu unerwarteten Ergebnissen.

Bei eingeschaltetem Web-Zugriff per HTTPS-Protokoll kann der mGuard über seine Web-basierte Administratoroberfläche **von entfernten Rechnern aus** konfiguriert werden. Das heißt, auf dem entfernten Rechner wird der Browser benutzt, um den mGuard zu konfigurieren.

Standardmäßig ist diese Option ausgeschaltet.

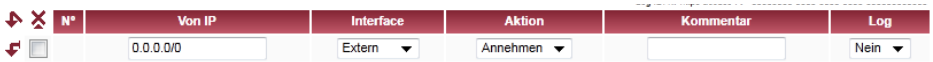
ACHTUNG: Wenn Sie Fernzugriff ermöglichen, achten Sie darauf, dass sichere Passwörter für *root* und *admin* festgelegt sind.

Um HTTPS-Fernzugang zu ermöglichen, machen Sie nachfolgende Einstellungen:

Verwaltung >> Web-Einstellungen >> Zugriff		
Web-Zugriff über HTTPS	**Aktiviere HTTPS-Fernzugang: Ja / Nein**	Wollen Sie HTTPS-Fernzugriff ermöglichen, setzen Sie diesen Schalter auf **Ja**. HTTPS-Fernzugriff über *Intern* (d. h. aus dem direkt angeschlossenen LAN oder vom direkt angeschlossenen Rechner aus) ist unabhängig von dieser Schalterstellung möglich. Um Zugriffsmöglichkeiten auf den mGuard differenziert festzulegen, müssen Sie auf dieser Seite unter **Erlaubte Netzwerke** die Firewall-Regeln für die verfügbaren Interfaces entsprechend definieren. Zusätzlich müssen gegebenenfalls unter **Benutzerauthentifizierung** die Authentifizierungsregeln gesetzt werden.
	Port für HTTPS-Verbindungen (nur Fernzugang)	Standard: 443 Wird diese Port-Nummer geändert, gilt die geänderte Port-Nummer nur für Zugriffe über das Interface *Extern, Extern 2, VPN* und *Einwahl*. Für internen Zugriff gilt weiterhin 443. Die entfernte Gegenstelle, die den Fernzugriff ausübt, muss bei der Adressenangabe hinter der IP-Adresse gegebenenfalls die Port-Nummer angeben, die hier festgelegt ist. Beispiel: Ist dieser mGuard über die Adresse 123.124.125.21 über das Internet zu erreichen, und ist für den Fernzugang die Port-Nummer 443 festgelegt, dann muss bei der entfernten Gegenstelle im Web-Browser diese Port-Nummer nicht hinter der Adresse angegeben werden. Bei einer anderen Port-Nummer ist diese hinter der IP-Adresse anzugeben, z. B.: https://123.124.125.21:442/  Der mGuard authentisiert sich bei der Gegenstelle, in diesem Fall dem Browser des Bedieners, mit einem selbst signiertem Maschinenzertifikat. Es handelt sich um ein von Innominate einmalig für jeden mGuard ausgestelltes Zertifikat. Das heißt, jeder mGuard wird mit einem einzigartigen selbstunterzeichneten Maschinenzertifikat ausgeliefert.
	SSH und HTTPS Schlüssel erneuern	**Generiere neue 2048 bit Schlüssel** Schlüssel, die mit einer älteren Firmware erstellt worden sind, sind möglicherweise schwach und sollten erneuert werden. • Klicken Sie auf diese Schaltfläche, um neue Schlüssel zu erzeugen. • Beachten Sie die Fingerprints der neu generierten Schlüssel. • Loggen Sie sich über HTTPS ein und vergleichen Sie die Zertifikat-Informationen, die vom Browser zur Verfügung gestellt werden.

Verwaltung >> Web-Einstellungen >> Zugriff [...]

Erlaubte Netzwerke



Listet die eingerichteten Firewall-Regeln auf. Sie gelten für eingehende Datenpakete eines HTTPS-Fernzugriffs.

Sind mehrere Firewall-Regeln gesetzt, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Sollten nachfolgend in der Regelliste weitere Regeln vorhanden sein, die auch passen würden, werden diese ignoriert.

Die hier angegebenen Regeln treten nur in Kraft, wenn der Schalter **Aktiviere HTTPS-Fernzugang** auf **Ja** steht. Weil Zugriffe von *Intern* auch möglich sind, wenn dieser Schalter auf **Nein** steht, tritt für diesen Fall eine Firewall-Regel, die den Zugriff von *Intern* verwehren würde, nicht in Kraft.

Bei den Angaben haben Sie folgende Möglichkeiten:

Von IP

Geben Sie hier die Adresse des Rechners oder Netzes an, von dem der Fernzugang erlaubt beziehungsweise verboten ist.

IP-Adresse: **0.0.0.0/0** bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise – siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 6-261

Interface

Extern / Intern / Extern 2 / VPN / Einwahl[1]

Gibt an, für welches Interface die Regel gelten soll.

Sind keine Regeln gesetzt oder greift keine Regel, gelten folgende Standardeinstellungen:

HTTPS-Zugriff ist erlaubt über *Intern, VPN* und *Einwahl*. Zugriffe über *Extern* und *Extern 2* werden verwehrt.

Legen Sie die Zugriffsmöglichkeiten nach Bedarf fest.

Wenn Sie Zugriffe über *Intern, VPN* oder *Einwahl* verwehren wollen, müssen Sie das explizit durch entsprechende Firewall-Regeln bewirken, in der Sie als Aktion z. B. *Verwerfen* festlegen. **Damit Sie sich nicht aussperren**, müssen Sie eventuell gleichzeitig den Zugriff über ein anderes Interface explizit mit *Annehmen* erlauben, bevor Sie durch Klicken auf die **Übernehmen**-Schaltfläche die neue Einstellung in Kraft setzen. Sonst muss bei Aussperrung die Recovery-Prozedur durchgeführt werden.

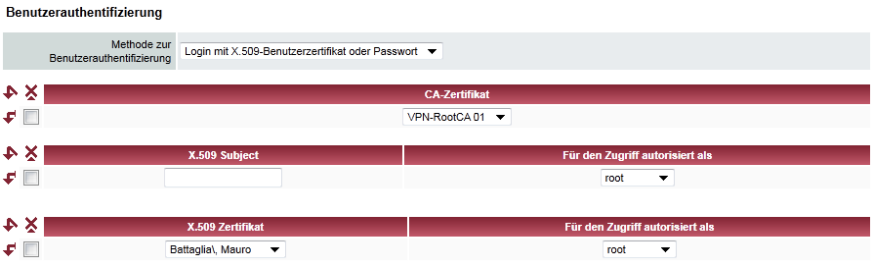
Verwaltung >> Web-Einstellungen >> Zugriff [...]		
	Aktion	– **Annehmen** bedeutet, die Datenpakete dürfen passieren. – **Abweisen** bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat *Abweisen* dieselbe Wirkung wie *Verwerfen*.) – **Verwerfen** bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information über deren Verbleib erhält.
	Kommentar	**Ein frei wählbarer Kommentar für diese Regel.**
	Log	Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel – das Ereignis protokolliert werden soll – *Log* auf **Ja** setzen – oder das Ereignis nicht protokolliert werden soll – *Log* auf **Nein** setzen (werkseitige Voreinstellung).
RADIUS-Authentifizierung Dieser Menüpunkt gehört nicht zum Funktionsumfang vom mGuard rs2000.	**Ermögliche RADIUS-Authentifizierung**	Bei **Nein** wird das Passwort der Benutzer, die sich über HTTPS einloggen, über die lokale Datenbank geprüft. Nur wenn **Nein** ausgewählt ist, kann die **Methode zur Benutzerauthentifizierung** auf **Login nur mit X.509-Benutzerzertifikat** gesetzt werden. Wählen Sie **Ja**, damit die Benutzer über den RADIUS-Server authentifiziert werden. Nur bei den vordefinierten Benutzern (*root*, *admin*, *netadmin*, *audit* und *user)* wird das Passwort lokal geprüft. Die Auswahl von **Als einzige Methode zur Passwortprüfung** ist nur für erfahrene Anwender geeignet, da Sie damit den Zugang zum mGuard komplett sperren können. Wenn Sie eine RADIUS-Authentifizierung das erste Mal einrichten, wählen Sie **Ja**. Wenn Sie planen, die RADIUS-Authentifizierung **als einzige Methode zur Passwortprüfung** einzurichten, empfehlen wir Ihnen ein „Customized Default Profile“ anzulegen, das die Authentifizierungsmethode zurücksetzt. Wenn Sie die RADIUS-Authentifizierung als einzige Methode zur Passwortprüfung ausgewählt haben, dann ist der Zugang zum mGuard unter Umständen nicht mehr möglich. Dies gilt z. B. wenn Sie einen falschen RADIUS-Server einrichten oder den mGuard umsetzen. Die vordefinierten Benutzer (*root*, *admin*, *netadmin*, *audit* und *user)* werden dann nicht mehr akzeptiert.

[1] *Extern 2* und *Einwahl* nur bei Geräten mit serieller Schnittstelle (siehe „Netzwerk >> Interfaces“ auf Seite 6-64).

Verwaltung >> Web-Einstellung >> Zugriff

Benutzerauthentifizierung

Dieser Menüpunkt gehört nicht zum Funktionsumfang vom mGuard rs2000.



Legt fest, wie der lokale mGuard die entfernte Gegenstelle authentifiziert

Methode zur Benutzerauthentifizierung

Login mit Passwort

Legt fest, dass sich der aus der Ferne zugreifende Bediener des mGuards mit Angabe seines Passwortes beim mGuard anmelden muss. Das Passwort ist festgelegt unter Menü *Authentifizierung >> Administrative Benutzer* (siehe Seite 6-121). Außerdem gibt es die Möglichkeit der RADIUS-Authentifizierung (siehe Seite 6-126).

Je nach dem, mit welcher Benutzerkennung der Bediener sich anmeldet (User- oder Administrator-Passwort), hat er entsprechende Rechte, den mGuard zu bedienen bzw. zu konfigurieren.

Login mit X.509-Benutzerzertifikat oder Passwort

- Die Benutzerauthentifizierung erfolgt per Login mit Passwort (siehe oben), oder
- der Browser des Benutzers authentisiert sich mit Hilfe eines X.509-Zertifikates und einem dazugehörigen privaten Schlüssel. Dazu sind unten weitere Angaben zu machen.

Welche Methode zur Anwendung kommt, hängt vom Web-Browser des von entfernt zugreifenden Benutzers ab. Die zweite Option kommt dann zur Anwendung, wenn der Web-Browser dem mGuard ein Zertifikat anbietet.

Login nur mit X.509-Benutzerzertifikat

Der Browser des Benutzers muss sich mit Hilfe eines X.509-Zertifikates und dem zugehörigen privaten Schlüssel authentisieren. Dazu sind weitere Angaben zu machen.

Bevor Sie die Einstellung *Login nur mit X.509-Benutzerzertifikat* in Kraft setzen, unbedingt erst die Einstellung *Login mit X.509-Benutzerzertifikat oder Passwort* wählen und testen.

Erst wenn sichergestellt ist, dass diese Einstellung funktioniert, auf *Login nur mit X.509-Benutzerzertifikat* umstellen. **Sonst könnte es passieren, dass Sie sich selbst aussperren!**

Diese Vorsichtsmaßnahme unbedingt immer dann treffen, wenn unter **Benutzerauthentifizierung** Einstellungen geändert werden.

Ist als **Methode der Benutzerauthentifizierung**

– Login nur mit X.509-Benutzerzertifikat, oder
– Login mit X.509-Benutzerzertifikat oder Passwort festgelegt

dann wird nachfolgend festgelegt, wie der mGuard den aus der Ferne zugreifenden Benutzer gemäß X.509 zu authentifizieren hat.

Die Tabelle unten zeigt, welche Zertifikate dem mGuard zur Authentifizierung des per HTTPS zugreifenden Benutzers zur Verfügung stehen müssen, wenn der Benutzer bzw. dessen Browser bei Verbindungsaufnahme eines der folgenden Zertifikatstypen vorzeigt:

– ein von einer CA signiertes Zertifikat
– ein selbst signiertes Zertifikat

Zum Verständnis der nachfolgenden Tabelle siehe „Authentifizierung >> Zertifikate“ auf Seite 6-128.

X.509-Authentifizierung bei HTTPS

Die Gegenstelle zeigt vor:	Zertifikat (personenbezogen) von **CA signiert**[1]	Zertifikat (personenbezogen) **selbst signiert**
Der mGuard authentifiziert die Gegenstelle anhand von...	⇕	⇕
	...allen CA-Zertifikaten, die mit dem von der Gegenstelle vorgezeigten Zertifikat die Kette bis zum Root-CA-Zertifikat bilden ggf. PLUS Gegenstellen-Zertifikaten, **wenn** sie als Filter verwendet werden.	Gegenstellen-Zertifikat

[1] Die Gegenstelle kann zusätzlich Sub-CA-Zertifikate anbieten. In diesem Fall kann der mGuard mit den angebotenen CA-Zertifikaten und den bei ihm selber konfigurierten CA-Zertifikaten die Vereinigungsmenge bilden, um die Kette zu bilden. Auf jeden Fall muss aber das zugehörige Root-Zertifikat auf dem mGuard zur Verfügung stehen.

Nach dieser Tabelle sind nachfolgend die Zertifikate zur Verfügung zu stellen, die der mGuard benutzen muss, um einen von entfernt per HTTPS zugreifenden Benutzer bzw. dessen Browser zu authentifizieren.

Die nachfolgenden Anleitungen gehen davon aus, dass die Zertifikate bereits ordnungsgemäß im mGuard installiert sind (siehe „Authentifizierung >> Zertifikate“ auf Seite 6-128).

Ist unter Menüpunkt Authentifizierung >> Zertifikate *, Zertifikatseinstellungen* die Verwendung von Sperrlisten (= CRL-Prüfung) aktiviert, wird jedes von einer CA signierte Zertifikat, das HTTPS-Clients „vorzeigen“, auf Sperrung geprüft.

Verwaltung >> Web-Einstellung >> Zugriff

CA-Zertifikat

Die Konfiguration ist nur erforderlich, wenn der Benutzer, der per HTTPS zugreift, ein von einer CA signiertes Zertifikat vorzeigt.

Es sind alle CA-Zertifikate zu konfigurieren, die der mGuard benötigt, um mit den von Benutzern vorgezeigten Zertifikaten jeweils die Kette bis zum jeweiligen Root-CA-Zertifikat zu bilden.

Sollte der Browser des aus der Ferne zugreifenden Benutzers zusätzlich CA-Zertifikate anbieten, die zur Bildung dieser Kette beitragen, dann ist es nicht notwendig, dass genau diese CA-Zertifikate beim mGuard installiert und an dieser Stelle referenziert werden.

Es muss aber auf jeden Fall das zugehörige Root-CA-Zertifikat beim mGuard installiert und zur Verfügung gestellt (= referenziert) sein.

Bei Auswahl anzuwendender CA-Zertifikate oder bei der Änderung der Auswahl oder Filtersetzung sollten Sie vor Inkraftsetzen der (neuen) Einstellung unbedingt erst die Einstellung *Login mit X.509-Benutzerzertifikat oder Passwort* als *Methode zur Benutzerauthentifizierung* wählen und testen.

Erst wenn sichergestellt ist, dass diese Einstellung funktioniert, auf *Login nur mit X.509-Benutzerzertifikat* umstellen. **Sonst könnte es passieren, dass Sie sich selbst aussperren!**

Diese Vorsichtsmaßnahme unbedingt immer dann treffen, wenn unter **Benutzerauthentifizierung** Einstellungen geändert werden.

Verwaltung >> Web-Einstellung >> Zugriff[...]

X.509-Subject

Ermöglicht die Filtersetzung in Bezug auf den Inhalt des Feldes *Subject* im Zertifikat, das vom Browser/HTTPS-Client vorgezeigt wird.

Dadurch ist es möglich, den Zugriff von Browser/HTTPS-Client, die der mGuard auf Grundlage von Zertifikatsprüfungen im Prinzip akzeptieren würde, wie folgt zu beschränken bzw. freizugeben:

– Beschränkung auf bestimmte *Subjects* (d. h. Personen) und/oder auf *Subjects*, die bestimmte Merkmale (Attribute) haben, oder
– Freigabe für alle Subjects (siehe Glossar unter „Subject, Zertifikat“ auf Seite 9-5*)*.

Das Feld *X.509-Subject* darf nicht leer bleiben.

Freigabe für alle Subjects (d. h. Personen):

Mit * (Sternchen) im Feld *X.509-Subject* legen Sie fest, dass im vom Browser/HTTPS-Client vorgezeigten Zertifikat beliebige Subject-Einträge erlaubt sind. Dann ist es überflüssig, das im Zertifikat jeweils angegebene Subject zu kennen oder festzulegen.

Verwaltung >> Web-Einstellung >> Zugriff[...]

Beschränkung auf bestimmte Subjects (d. h. Personen) und/oder auf Subjects, die bestimmte Merkmale (Attribute) haben:

Im Zertifikat wird der Zertifikatsinhaber im Feld *Subject* angegeben, dessen Eintrag sich aus mehreren Attributen zusammensetzt. Diese Attribute werden entweder als Object Identifier ausgedrückt (z. B.: 132.3.7.32.1) oder, geläufiger, als Buchstabenkürzel mit einem entsprechenden Wert.

Beispiel: CN=Max Muster, O=Fernwartung GmbH, C=DE

Sollen bestimmte Attribute des Subjects ganz bestimmte Werte haben, damit der mGuard den Browser akzeptiert, muss das entsprechend spezifiziert werden. Die Werte der anderen Attribute, die beliebig sein können, werden dann durch das Wildcard * (Sternchen) angegeben.

Beispiel: CN=*, O=*, C=DE (mit oder ohne Leerzeichen zwischen Attributen)

Bei diesem Beispiel müsste im Zertifikat im Subject das Attribut „C=DE“ stehen. Nur dann würde der mGuard den Zertifikatsinhaber (= Subject) als Kommunikationspartner akzeptieren. Die anderen Attribute könnten in den zu filternden Zertifikaten beliebige Werte haben.

Wird ein Subject-Filter gesetzt, muss zwar die Anzahl, nicht aber die Reihenfolge der angegebenen Attribute mit der übereinstimmen, wie sie in den Zertifikaten gegeben ist, auf die der Filter angewendet werden soll.

Auf Groß- und Kleinschreibung achten.

Es können mehrere Filter gesetzt werden, die Reihenfolge der Filter ist irrelevant.

Bei HTTPS gibt der Browser des zugreifenden Benutzers nicht an, mit welchen Benutzer- bzw. Administratorrechten dieser sich anmeldet. Diese Rechtevergabe erfolgt bei der Filtersetzung hier (unter „Für den Zugriff autorisiert“).

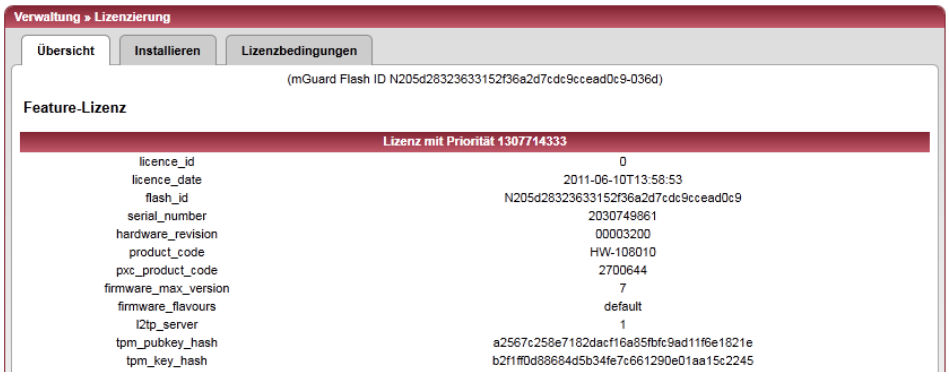
Das hat folgende Konsequenz: Gibt es mehrere Filter, die einen bestimmten Benutzer „durchlassen“, tritt der erste Filter in Kraft. Und der Benutzer erhält das Zugriffsrecht, das ihm in diesem Filter zugesprochen wird. Und das könnte sich unterscheiden von Zugriffsrechten, die ihm in weiter unten stehenden Filtern zugeordnet sind.

Sind nachfolgend in der Tabelle mit der Spalte **X.509-Zertifikat** Gegenstellen-Zertifikate als Filter konfiguriert, dann haben diese Filter Vorrang gegenüber den Filtersetzungen hier.

Verwaltung >> Web-Einstellung >> Zugriff[...]	
Für den Zugriff autorisiert als	**Alle Benutzer / root / admin / netadmin / audit** Legt fest, welche Benutzer- bzw. Administratorrechte dem aus der Ferne zugreifenden Bediener eingeräumt werden. Für eine Beschreibung der Berechtigungsstufen *root, admin* und *user* siehe „Authentifizierung >> Administrative Benutzer“ auf Seite 6-121. Die Berechtigungsstufen *netadmin* und *audit* beziehen sich auf Zugriffsrechte bei Zugriffen mit dem Innominate Device Manager.
X.509-Zertifikat	Die Konfiguration ist in den folgenden Fällen erforderlich: – Von entfernt zugreifende Benutzer zeigen jeweils ein selbst signiertes Zertifikat vor. – Von entfernt zugreifende Benutzer zeigen jeweils ein von einer CA signiertes Zertifikat vor. Es soll eine Filterung erfolgen: Zugang erhält nur der, dessen Zertifikats-Kopie im mGuard als Gegenstellen-Zertifikat installiert ist und in dieser Tabelle dem mGuard als *X.509-Zertifikat* zur Verfügung gestellt wird. Dieser Filter hat Vorrang gegenüber dem *Subject*-Filter in der Tabelle darüber, sofern verwendet. Der Eintrag in diesem Feld legt fest, welches Gegenstellen-Zertifikat der mGuard heranziehen soll, um die Gegenstelle, den Browser des von entfernt zugreifenden Benutzers, zu authentifizieren. Dazu in der Auswahlliste eines der Gegenstellen-Zertifikate auswählen. Die Auswahlliste stellt die Gegenstellen-Zertifikate zur Wahl, die in den mGuard unter Menüpunkt Authentifizierung >> Zertifikate geladen worden sind.
Für den Zugriff autorisiert als	**root / admin / netadmin / audit / user** Legt fest, welche Nutzer- bzw. Administratorrechte dem aus der Ferne zugreifenden Bediener eingeräumt werden. Für eine Beschreibung der Berechtigungsstufen *root, admin* und *user* siehe „Authentifizierung >> Administrative Benutzer“ auf Seite 6-121**.** Die Berechtigungsstufen *netadmin* und *audit* beziehen sich auf Zugriffsrechte mit dem Innominate Device Manager.

6.2.3 Verwaltung >> Lizenzierung

6.2.3.1 Übersicht



Ab Version 5.0 des mGuards bleiben Lizenzen auch nach Flashen der Firmware installiert.

Beim Flashen von Geräten mit älteren Firmware-Versionen auf Versionen 5.0.0 oder später werden weiterhin Lizenzen gelöscht. Dann muss vor dem Flashen erst die Lizenz für die Nutzung des neuen Updates erworben werden, damit beim Flashen die erforderliche Lizenz-Datei zur Verfügung steht.

Das gilt für Major-Release Upgrades, also z. B. bei einem Upgrade von Version 4.x.y zu Version 5.x.y zu Version 6.x.y usw. (siehe „Flashen der Firmware / Rescue-Prozedur“ auf Seite 8-3).

Verwaltung >> Lizenzierung >> Übersicht		
Grundeinstellungen	**Feature-Lizenz**	Zeigt an, welche Funktionen die eingespielten mGuard-Lizenzen beinhalteten, z. B. die Anzahl der ermöglichten VPN-Tunnel, ob Remote Logging unterstützt wird, usw.

6.2.3.2 Installieren

Dieses Funktion steht **nicht** auf dem **mGuard rs2000** zur Verfügung.

Sie können nachträglich Ihre erworbene mGuard-Lizenz um weitere Funktionen ergänzen.

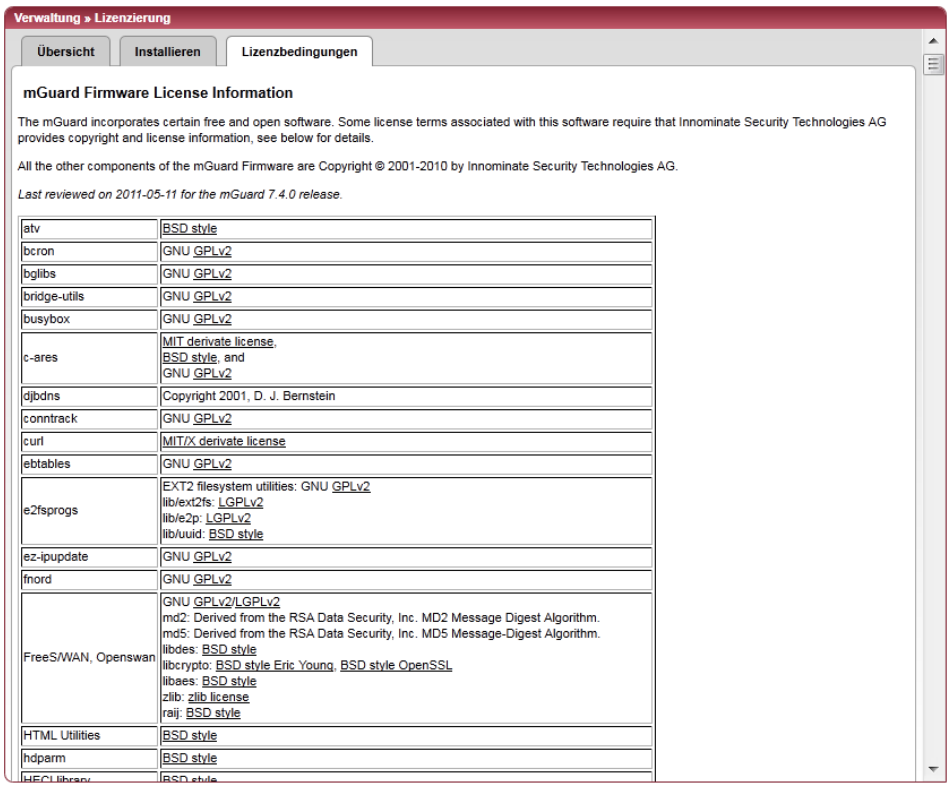
Im Voucher, den Sie beim Kauf des mGuards erhalten oder zusätzlich erworben haben, finden Sie eine Voucher-Seriennummer und einen Voucher-Schlüssel.

Damit können Sie

– die erforderliche Feature-Lizenzdatei anfordern und dann
– die Lizenzdatei, die Sie daraufhin erhalten, installieren.

Verwaltung >> Lizenzierung >> Installieren		
Automatische Lizenzinstallation	**Vouchernummer/Voucherschlüssel**	Geben Sie hier die Seriennummer, die auf dem Voucher aufgedruckt ist, sowie den dazugehörigen Voucherschlüssel ein, und klicken Sie anschließend **Online-Lizenzabruf**. Der mGuard baut nun eine Verbindung über das Internet auf und installiert bei einem gültigen Voucher die zugehörige Lizenz auf dem mGuard.
	Lizenzen wiederherstellen	Kann benutzt werden, falls die im mGuard installierten Lizenzen gelöscht wurde. Klicken Sie dazu auf die Schaltfläche **Online-Lizenzwiederherstellung**. Dann werden die Lizenzen, die zuvor für diesen mGuard ausgestellt waren, über das Internet vom Server geholt und installiert.
Manuelle Lizenzinstallation	**Bestellte Lizenz** **Dateiname**	Nach Klicken auf die Schaltfläche **Editiere Lizenzformular** wird über eine Internet-Verbindung ein Formular bereit gestellt, über das Sie die gewünschte Lizenz bestellen können und in deren Felder Sie die folgenden Informationen eingeben: – **Voucher-Serial-Number:** Die Seriennummer, die auf Ihrem Voucher gedruckt ist – **Voucher-Key:** Der Voucherschlüssel auf ihrem Voucher – **Flash-ID:** Wird automatisch vorausgefüllt Nach dem Absenden des Formulars wird die Lizenzdatei zum Herunterladen bereitgestellt und kann mit einem weiteren Schritt im mGuard installiert werden. **Lizenzdatei installieren** Um eine Lizenz einzuspielen, speichern Sie zunächst die Lizenz-Datei als separate Datei auf Ihrem Rechner und gehen dann wie folgt vor: • Hinter dem Feld *Dateiname* die Schaltfläche **Durchsuchen...** klicken, die Datei selektieren und öffnen, so dass ihr Pfad- bzw. Dateiname im Feld *Dateiname* angezeigt wird. • Dann die Schaltfläche **Installiere Lizenzdatei** klicken.

6.2.3.3 Lizenzbedingungen



Listet die Lizenzen der Fremd-Software auf, die im mGuard verwendet wird. Es handelt sich meistens um Open-Source-Software.

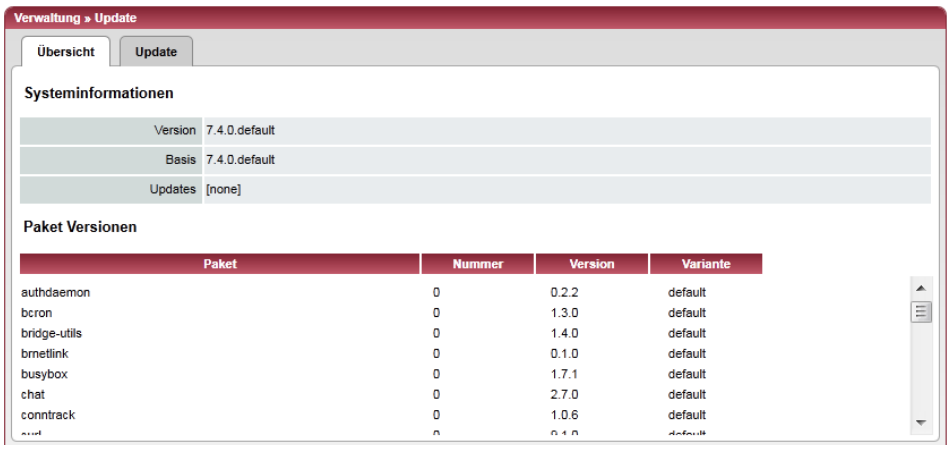
6.2.4 Verwaltung >> Update

Ab Version 5.0.0 der mGuard-Firmware muss vor der Installation eines Major-Release-Upgrades (z. B. von Version 4.x.y auf 5.x.y oder von Version 5.x.y auf Version 6.x.y) für das betreffende Gerät erst eine Lizenz erworben werden.

Die Lizenz muss vor der Durchführung des Firmware-Updates auf dem Gerät installiert werden (siehe „Verwaltung >> Lizenzierung“ auf Seite 6-34 und „Installieren“ auf Seite 6-34).

Minor-Release-Upgrades (bedeutet: gleichbleibende Hauptversion, z. B. innerhalb von 5.x.y) können bis auf Weiteres ohne Lizenz installiert werden.

6.2.4.1 Übersicht



Verwaltung >> Update >> Übersicht		
Systeminformation	**Version**	Die aktuelle Software-Version des mGuards.
	Basis	Die Software-Version, mit der dieser mGuard ursprünglich geflasht wurde.
	Updates	Liste der Updates, die zur Basis hinzu installiert worden sind.
Paket Versionen	Listet die einzelnen Software-Module des mGuards auf. Gegebenenfalls für Supportzwecke interessant.	

6.2.4.2 Update

Firmware-Updates mit eingeschalteter Firewall-Redundanz

Updates von Version 7.3.1 an aufwärts können durchgeführt werden, während ein mGuard-Redundanzpaar angeschlossen und in Betrieb ist.

Ausnahme hiervon sind die folgenden Geräte:

– mGuard industrial rs
– mGuard smart
– mGuard pci
– mGuard blade
– mGuard delta

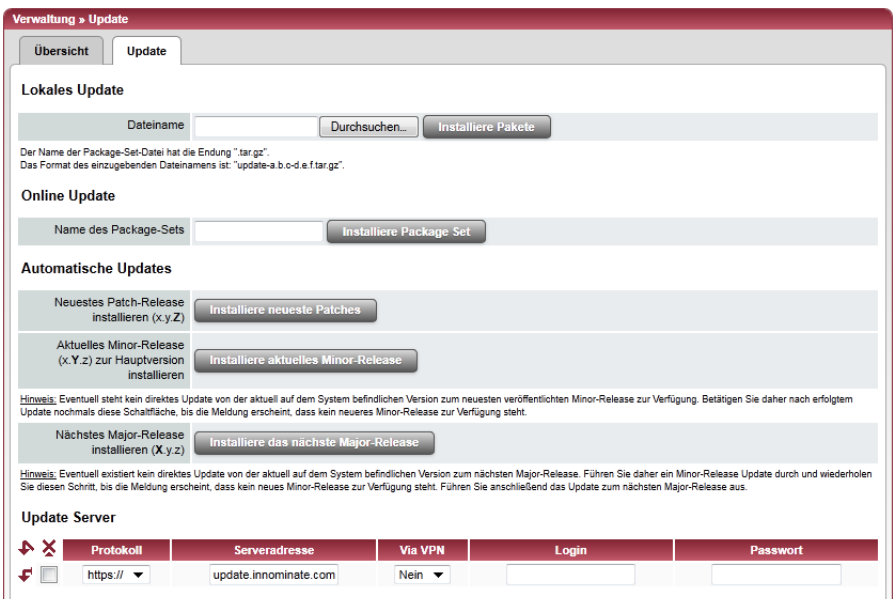
Sie müssen nacheinander ein Update erhalten, während das entsprechende redundante Gerät abgekoppelt ist.

Wenn die Firewall-Redundanz aktiviert ist, können beide mGuards eines Redundanzpaares gleichzeitig ein Update erhalten. Die mGuards, die ein Paar bilden, entscheiden selbstständig, welcher mGuard das Update zuerst durchführt, während der andere mGuard aktiv bleibt. Wenn der aktive mGuard innerhalb von 25 Minuten nachdem er den Update-Befehl erhalten hat, nicht booten kann (weil der andere mGuard noch nicht übernommen hat), bricht er das Update ab und läuft mit der vorhandenen Firmware-Version weiter.

Firmware-Update durchführen

Um ein Firmware-Update durchzuführen, gibt es zwei Möglichkeiten:

1. Sie haben die aktuelle Package-Set-Datei auf Ihrem Rechner (der Dateiname hat die Endung „.tar.gz“) und Sie führen ein lokales Update durch.
2. Der mGuard lädt ein Firmware-Update Ihrer Wahl über das Internet vom Update-Server herunter und installiert es.



ACHTUNG: Sie dürfen während des Updates auf keinen Fall die Stromversorgung des mGuards unterbrechen! Das Gerät könnte ansonsten beschädigt werden und nur noch durch den Hersteller reaktiviert werden können.

	Abhängig von der Größe des Updates, kann dieses mehrere Minuten dauern.
	Falls zum Abschluss des Updates ein Neustart erforderlich sein sollte, werden Sie durch eine Nachricht darauf hingewiesen.
	Ab Version 5.0.0 der mGuard-Firmware muss vor der Installation eines Major-Release-Upgrades (z. B. von Version 5.x.y auf 6.x.y oder von Version 6.x.y auf Version 7.x.y) für das betreffende Gerät erst eine Lizenz erworben werden. Die Lizenz muss vor der Durchführung des Firmware-Updates auf dem Gerät installiert werden (siehe „Verwaltung >> Lizenzierung“ auf Seite 6-34, „Installieren“ auf Seite 6-34). Minor-Release-Upgrades (bedeutet: gleichbleibende Hauptversion, z. B. innerhalb von 7.x.y) können bis auf Weiteres ohne Lizenz installiert werden.

Verwaltung >> Update		
Lokales Update	**Dateiname**	Zur Installation von Paketen gehen Sie wie folgt vor: • Die Schaltfläche **Durchsuchen...** klicken, die Datei selektieren und öffnen, so dass ihr Pfad- bzw. Dateiname im Feld *Dateiname* angezeigt wird. Das Format des Dateinamens muss lauten: update-a.b.c-d.e.f.default.<Plattform>.tar.gz **Beispiel**: update-7.0.0-7.0.1.default.ixp4xx_be.tar.gz • Dann die Schaltfläche **Installiere Pakete** klicken.
Online Update		Um ein Online-Update durchzuführen, gehen Sie wie folgt vor: • Stellen Sie sicher, dass unter **Update-Server** mindestens ein gültiger Eintrag vorhanden ist. Die dafür nötigen Angaben haben Sie von Ihrem Lizenzgeber erhalten. • Geben Sie den Namen des Package-Sets ein. z. B. „update-6.1.x-7.2.0“. • Dann die Schaltfläche **Installiere Package Set** klicken.
Automatische Updates	Dieses ist eine Variante des Online-Updates, bei welcher der mGuard das benötigte Package-Set eigenständig ermittelt.	
	Neustes Patch-Release installieren (x.y.Z)	Patch-Releases beheben Fehler der vorherigen Versionen und haben eine Versionsnummer, welche sich nur in der dritten Stelle ändern. Zum Beispiel ist 4.0.1 ein Patch-Release zur Version 4.0.0.
	Aktuelles Minor-Release zur Hauptversion installieren (x.Y.z)	Minor- und Major-Releases ergänzen den mGuard um neue Eigenschaften oder enthalten Änderungen am Verhalten des mGuards. Ihre Versionsnummer ändert sich in der ersten oder zweiten Stelle.
	Nächstes Major-Release installieren (X.y.z)	Zum Beispiel ist 4.1.0 ein Major- bzw. Minor-Release zu den Versionen 3.1.0 bzw. 4.0.1.

Verwaltung >> Update [...]

Update-Server

Legen Sie fest, von welchen Servern ein Update vorgenommen werden darf.

Die Liste der Server wird von oben nach unten abgearbeitet, bis ein verfügbarer Server gefunden wird. Die Reihenfolge der Einträge legt also deren Priorität fest.

Alle konfigurierten Update-Server müssen die selben Updates zur Verfügung stellen.

Bei den Angaben haben Sie folgende Möglichkeiten:

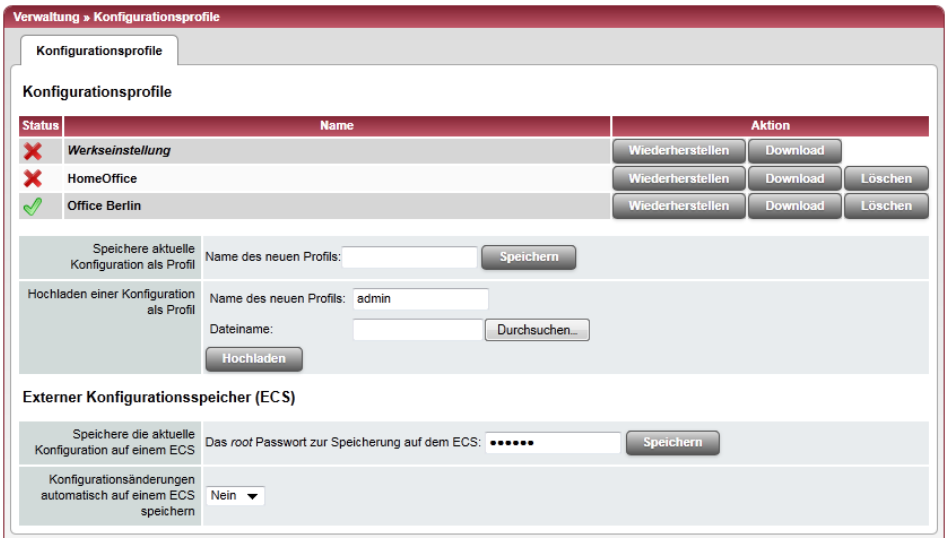
Protokoll	Das Update der kann entweder per HTTPS oder HTTP erfolgen.
Server Adresse	Hostnamen des Servers, der die Update-Dateien bereitstellt.
Via VPN	Das Update wird über den VPN-Tunnel durchgeführt. Default: Nein.

Updates via VPN werden nicht unterstützt, wenn der relevante VPN-Tunnel in der Konfiguration ausgeschaltet wurde (siehe Kapitel 6.8.2, *IPsec VPN >> Verbindungen*) und über den Servicekontakt oder die CGI-Schnittstelle nur temporär geöffnet wurde.

Login	Login für den Server.
Passwort	Passwort für den Login.

6.2.5 Verwaltung >> Konfigurationsprofile

6.2.5.1 Konfigurationsprofile



Sie haben die Möglichkeit, die Einstellungen des mGuards als Konfigurationsprofil unter einem beliebigen Namen im mGuard zu speichern. Sie können mehrere solcher Konfigurationsprofile anlegen, so dass Sie nach Bedarf zwischen verschiedenen Profilen wechseln können, z. B. wenn der mGuard in unterschiedlichen Umgebungen eingesetzt wird.

Darüber hinaus können Sie Konfigurationsprofile als Dateien auf ihrem Konfigurationsrechner abspeichern. Umgekehrt besteht die Möglichkeit, eine so erzeugte Konfigurationsdatei in den mGuard zu laden und zu aktivieren.

Zusätzlich können Sie jederzeit die *Werkseinstellung* (wieder) in Kraft setzen.

Konfigurationsprofile können beim mGuard rs4000/rs2000, mGuard delta^2, mGuard pci^2 SD, EAGLE mGuard und beim mGuard centerport auch auf einem externen Konfigurationsspeicher (ECS) wie SD-Karte (mGuard rs4000/rs2000, mGuard delta^2, mGuard pci^2 SD) bzw. V.24/USB-Speicherstick (EAGLE mGuard, mGuard centerport) abgelegt werden (siehe „Profile auf externem Speichermedium: mGuard rs4000/2000, mGuard delta^2, mGuard pci^2 SD, EAGLE mGuard, mGuard centerport“ auf Seite 6-43).

Beim Abspeichern eines Konfigurationsprofils werden die Passwörter, die zur Authentifizierung des administrativen Zugriffs auf den mGuard dienen, nicht mitgespeichert.

Es ist möglich, ein Konfigurationsprofil zu laden und in Kraft zu setzen, das unter einer älteren Firmware-Version erstellt wurde. Umgekehrt trifft das nicht zu: Ein unter einer neueren Firmware-Version erstelltes Konfigurationsprofil sollte nicht geladen werden.

Verwaltung >> Konfigurationsprofile	
Konfigurationsprofile	Die Seite zeigt oben eine Liste von Konfigurationsprofilen, die im mGuard gespeichert sind, z. B. das Konfigurationsprofil *Werkseinstellung*. Sofern vom Benutzer Konfigurationsprofile gespeichert worden sind (siehe unten), werden diese hier aufgeführt.  **Aktives Konfigurationsprofil:** Das Konfigurationsprofil, das zurzeit in Kraft ist, hat vorne im Eintrag das *Active*-Symbol . Sie können Konfigurationsprofile, die im mGuard gespeichert sind: – in Kraft setzen – als Datei auf dem angeschlossenen Konfigurations-Rechner speichern – löschen – anzeigen **Konfigurationsprofil anzeigen:** • In der Liste den Namen des Konfigurationsprofils anklicken. **Die Werkseinstellung oder ein vom Benutzer im mGuard gespeichertes Konfigurationsprofil in Kraft setzen** • Rechts neben dem Namen des betreffenden Konfigurationsprofils auf die Schaltfläche **Wiederherstellen** klicken. Das betreffende Konfigurationsprofil wird aktiviert. **Konfigurationsprofil als Datei auf dem Konfigurations-Rechner speichern** • Rechts neben dem Namen des betreffenden Konfigurationsprofils auf die Schaltfläche **Download** klicken. • Legen Sie im angezeigten Dialogfeld den Dateinamen und Ordner fest, unter bzw. in dem das Konfigurationsprofil als Datei gespeichert werden soll. (Sie können die Datei beliebig benennen.) **Konfigurationsprofil löschen:** • Rechts neben dem Namen des betreffenden Konfigurationsprofils auf die Schaltfläche **Löschen** klicken.  Das Profil *Werkseinstellung* kann nicht gelöscht werden.
Speichere aktuelle Konfiguration als Profil	**Aktuelle Konfiguration als Konfigurationsprofil im mGuard speichern** • Hinter „Speichere aktuelle Konfiguration als Profil“ in das Feld *Name des neuen Profils* den gewünschten Profil-Namen eintragen. • Auf die Schaltfläche **Speichern** klicken. Das Konfigurationsprofil wird im mGuard gespeichert, und der Name des Profils wird in der Liste der bereits im mGuard gespeicherten Profile angezeigt.

Verwaltung >> Konfigurationsprofile [...]

Hochladen einer Konfiguration als Profil	**Hochladen eines Konfigurationsprofils, das auf dem Konfigurations-Rechner in einer Datei gespeichert ist**	
	Voraussetzung: Sie haben nach dem oben beschriebenem Verfahren ein Konfigurationsprofil als Datei auf dem Konfigurations-Rechners gespeichert. • Hinter „Hochladen einer Konfiguration als Profil“ in das Feld *Name des neuen Profils* den gewünschten Profil-Namen eintragen. • Auf die Schaltfläche **Durchsuchen...** klicken und im angezeigten Dialogfeld die betreffende Datei selektieren und öffnen. • Auf die Schaltfläche **Hochladen** klicken. Das Konfigurationsprofil wird in den mGuard geladen, und der in Schritt 1 vergebene Name wird in der Liste der bereits im mGuard gespeicherten Profile angezeigt.	
Externer Konfigurationsspeicher (ECS)	**Speichere die aktuelle Konfiguration auf einem ECS**	*Nur beim mGuard rs4000/rs2000,* mGuard delta^2, mGuard pci^2 SD, *EAGLE mGuard und mGuard centerport* Beim Austausch durch ein Ersatzgerät kann das Konfigurationsprofil des ursprünglichen Gerätes mit Hilfe des ECS übernommen werden. Voraussetzung hierfür ist, dass das Ersatzgerät noch „root“ als Passwort für den Benutzer „root“ verwendet. Wenn das Root-Passwort auf dem Ersatzgerät ungleich „root“ ist, dann muss dieses Passwort in das Feld **Das root Passwort zur Speicherung auf dem ECS** eingegeben werden. (siehe „Profil auf externem Speichermedium speichern“)
	Konfigurationsänderungen automatisch auf einem ECS speichern	*Nur beim mGuard rs4000/rs2000,* mGuard delta^2, mGuard pci^2 SD, *EAGLE mGuard und mGuard centerport* Bei **Ja** werden die Konfigurationsänderungen automatisch auf einem ECS gespeichert, so dass auf dem ECS stets das aktuell verwendete Profil gespeichert ist. Automatisch abgespeicherte Konfigurationsprofile werden von einem mGuard beim Starten nur angewendet, wenn der mGuard als Passwort für den „root“-Benutzer noch das ursprüngliche Passwort (ebenfalls „root“) eingestellt hat (siehe „Profil vom externen Speichermedium laden“ auf Seite 6-44). Auch wenn der ECS ist nicht angeschlossen, voll oder defekt ist, werden Konfigurationsänderungen ausgeführt. Entsprechende Fehlermeldungen erscheinen im Logging (siehe Kapitel 6.12.2). Die Aktivierung der neuen Einstellung verlängert die Reaktionszeit der Bedienoberfläche, wenn Einstellungen geändert werden.

Profile auf externem Speichermedium: mGuard rs4000/2000, mGuard delta^2, mGuard pci^2 SD, EAGLE mGuard, mGuard centerport

EAGLE mGuard: Konfigurationsprofile können auch auf einem externen Konfigurationsspeicher (ECS) abgelegt werden.

mGuard centerport und **EAGLE mGuard** mit **USB-Schnittstelle**: Konfigurationsprofile können auch auf einem USB-Speicherstick abgelegt werden. Dieser muss die folgenden Eigenschaften haben:

– VFAT-Dateisystem auf der ersten primären Partition, mindestens 64 MB freie Speicherkapazität.

mGuard rs4000/rs2000, mGuard delta², mGuard pci² SD: Konfigurationsprofile können auch auf einer SD-Karte (bis zu 2 GB Kapazität) abgelegt werden. Diese muss die folgenden Eigenschaften besitzen:

– VFAT-Dateisystem auf der ersten primären Partition, mindestens 64 MB freie Speicherkapazität.

– Zertifiziert und freigegeben durch die Innominate Security Technologies AG (aktuelle Freigabeliste unter www.innominate.com).

Profil auf externem Speichermedium speichern

- **EAGLE mGuard**: Den ECS an die V.24 Buchse (ACA11) oder USB-Buchse (ACA21) anschließen.
- **mGuard centerport** und **EAGLE mGuard mit USB-Schnittstelle**: Den USB-Stick in die USB-Buchse einstecken.
- **mGuard rs4000/rs2000, mGuard delta², mGuard pci² SD**: SD-Karte in den SD-Slot auf der Frontseite einsetzen.
- Wenn das Root-Passwort auf dem mGuard, auf welchem das Profil später wieder eingelesen werden soll, ungleich „root“ ist, dann muss dieses Passwort in das Feld **Das root Passwort zur Speicherung auf dem ECS** eingegeben werden.
- Auf die Schaltfläche **Speichern** klicken.

  Beim EAGLE mGuard: Die LED STATUS und die LED V.24 blinken, bis das Speichern beendet ist.

Profil vom externen Speichermedium laden

- **EAGLE mGuard**: Den ECS an die V.24 Buchse (ACA11) oder USB-Buchse (ACA21) anschließen.
- **mGuard centerport** und **EAGLE mGuard mit USB-Schnittstelle**: Den USB-Stick in die USB-Buchse einstecken.
- **mGuard rs4000/rs2000, mGuard delta², mGuard pci² SD**: SD-Karte in den SD-Slot auf der Frontseite einsetzen.
- Bei eingestecktem Speichermedium den mGuard starten.
- Das Root-Passwort des mGuards muss entweder „root“ lauten, oder es muss dem Passwort entsprechen, das während des Speicherns des Profils angegeben wurde.

  Beim EAGLE mGuard: Die LED STATUS und die LED V.24 blinken, bis das Speichern beendet ist.

Das vom Speichermedium geladene Konfigurationsprofil wird in den mGuard geladen und in Kraft gesetzt.

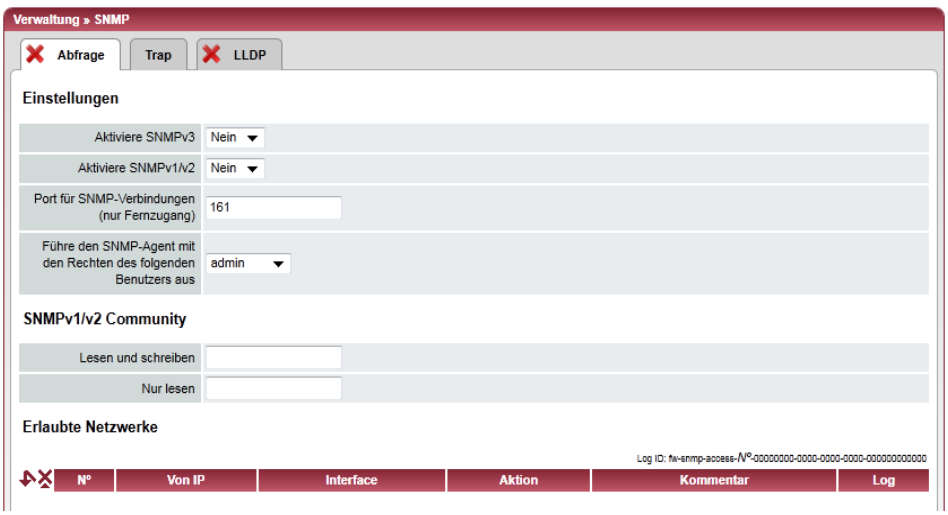
Das geladene Konfigurationsprofil erscheint nicht in der Liste der im mGuard gespeicherten Konfigurationsprofile.

Die Konfiguration auf dem externen Speichermedium enthält auch die Passwörter für die Benutzer *root*, *admin*, *netadmin*, *audit* und *user*. Diese werden beim Laden vom externen Speichermedium ebenfalls übernommen.

6.2.6 Verwaltung >> SNMP

Die Konfiguration des mGuards darf nicht gleichzeitig über den Web-Zugriff, den Shell-Zugang oder SNMP erfolgen. Eine zeitgleiche Konfiguration über die verschiedenen Zugangsmethoden führt möglicherweise zu unerwarteten Ergebnissen.

6.2.6.1 Abfrage



Das SNMP (Simple Network Management Protocol) wird vorzugsweise in komplexeren Netzwerken benutzt, um den Zustand und den Betrieb von Geräten zu überwachen.

Das SNMP gibt es in mehreren Entwicklungsstufen: SNMPv1/SNMPv2 und SNMPv3.

Die älteren Versionen SNMPv1/SNMPv2 benutzen keine Verschlüsselung und gelten als nicht sicher. Daher ist davon abzuraten, SNMPv1/SNMPv2 zu benutzen.

SNMPv3 ist unter dem Sicherheitsaspekt deutlich besser, wird aber noch nicht von allen Management-Konsolen unterstützt.

Ist SNMPv3 oder SNMPv1/v2 aktiviert, wird das oben auf der Registerkartenzunge durch ein grünes Signalfeld angezeigt. Sonst, d. h. bei nicht aktivem SNMPv3 und SNMPv1/v2 ist das Signalfeld auf Rot.

Die Bearbeitung einer SNMP-Anfrage kann länger als eine Sekunde dauern. Dieser Wert entspricht jedoch dem Standard-Timeout-Wert einiger SNMP-Management-Applikationen.

- Setzen Sie aus diesem Grund den Timeout-Wert Ihrer Management Applikation auf Werte zwischen 3 und 5 Sekunden, falls Timeout-Probleme auftreten sollten.

Verwaltung >> SNMP >> Abfrage		
Einstellungen	**Aktiviere SNMPv3: Ja / Nein**	Wollen Sie zulassen, dass der mGuard per SNMPv3 überwacht werden kann, setzen Sie diesen Schalter auf **Ja**. Um Zugriffs- bzw. Überwachungsmöglichkeiten auf den mGuard differenziert festzulegen, müssen Sie auf dieser Seite unter **Erlaubte Netzwerke** die Firewall-Regeln für die verfügbaren Interfaces entsprechend definieren. Für den Zugang per SNMPv3 ist eine Authentifizierung mittels Login und Passwort notwendig. Die Werkseinstellungen für die Login-Parameter lauten: **Login**: admin **Passwort**: SnmpAdmin (Bitte beachten Sie die Groß-/Kleinschreibung!) Für die Authentifizierung wird MD5 unterstützt, für die Verschlüsselung DES. Die Login-Parameter für SNMPv3 können nur mittels SNMPv3 geändert werden.
	Aktiviere SNMPv1/v2: Ja / Nein	Wollen Sie zulassen, dass der mGuard per SNMPv1/v2 überwacht werden kann, setzen Sie diesen Schalter auf **Ja**. Zusätzlich müssen Sie unter **SNMPv1/v2-Community** die Login-Daten angeben. Um Zugriffs- bzw. Überwachungsmöglichkeiten auf den mGuard differenziert festzulegen, müssen Sie auf dieser Seite unter **Erlaubte Netzwerke** die Firewall-Regeln für die verfügbaren Interfaces entsprechend definieren.
	Port für SNMP-Verbindungen	Standard: 161 Wird diese Port-Nummer geändert, gilt die geänderte Port-Nummer nur für Zugriffe über das Interface *Extern, Extern 2, VPN* und *Einwahl*. Für internen Zugriff gilt weiterhin 161. Die entfernte Gegenstelle, die den Fernzugriff ausübt, muss bei der Adressenangabe gegebenenfalls die Port-Nummer angeben, die hier festgelegt ist.
SNMPv1/v2-Community	**Lesen und schreiben**	Geben Sie in diese Felder die erforderlichen Login-Daten ein.
	Nur lesen	Geben Sie in diese Felder die erforderlichen Login-Daten ein.
Erlaubte Netzwerke	Listet die eingerichteten Firewall-Regeln auf. Sie gelten für eingehende Datenpakete eines SNMP-Zugriffs. Die hier angegebenen Regeln treten nur in Kraft, wenn der Schalter **Aktiviere SNMPv3** oder **Aktiviere SNMPv1/v2** auf **Ja** steht. Sind mehrere Firewall-Regeln gesetzt, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Sollten nachfolgend in der Regelliste weitere Regeln vorhanden sein, die auch passen würden, werden diese ignoriert.	

Verwaltung >> SNMP >> Abfrage[...]

Von IP

Geben Sie hier die Adresse des Rechners oder Netzes an, von dem der Fernzugang erlaubt beziehungsweise verboten ist.

Bei den Angaben haben Sie folgende Möglichkeiten:

- Eine IP-Adresse.
- Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise (siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 6-261).
- **0.0.0.0/0** bedeutet alle Adressen.

Interface

Extern / Intern / Extern 2 / VPN / Einwahl[1]

Gibt an, für welches Interface die Regel gelten soll.

Sind keine Regeln gesetzt oder greift keine Regel, gelten folgende Standardeinstellungen:

SNMP-Überwachung ist erlaubt über *Intern, VPN* und *Einwahl*.

Zugriffe über *Extern* und *Extern 2* werden verwehrt.

Legen Sie die Überwachungsmöglichkeiten nach Bedarf fest.

ACHTUNG: Wenn Sie Zugriffe über *Intern, VPN* oder *Einwahl* verwehren wollen, müssen Sie das explizit durch entsprechende Firewall-Regeln bewirken, in der Sie als Aktion z. B. *Verwerfen* festlegen. **Damit Sie sich nicht aussperren**, müssen Sie eventuell gleichzeitig den Zugriff über ein anderes Interface explizit mit *Annehmen* erlauben, bevor Sie durch Klicken auf die **Übernehmen**-Schaltfläche die neue Einstellung in Kraft setzen. Sonst muss bei Aussperrung die Recovery-Prozedur durchgeführt werden.

Aktion

Annehmen bedeutet, dass die Datenpakete passieren dürfen.

Abweisen bedeutet, dass die Datenpakete zurückgewiesen werden, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat *Abweisen* dieselbe Wirkung wie *Verwerfen*.)

Verwerfen bedeutet, dass die Datenpakete nicht passieren dürfen. Sie werden verschluckt, so dass der Absender keine Information über deren Verbleib erhält.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

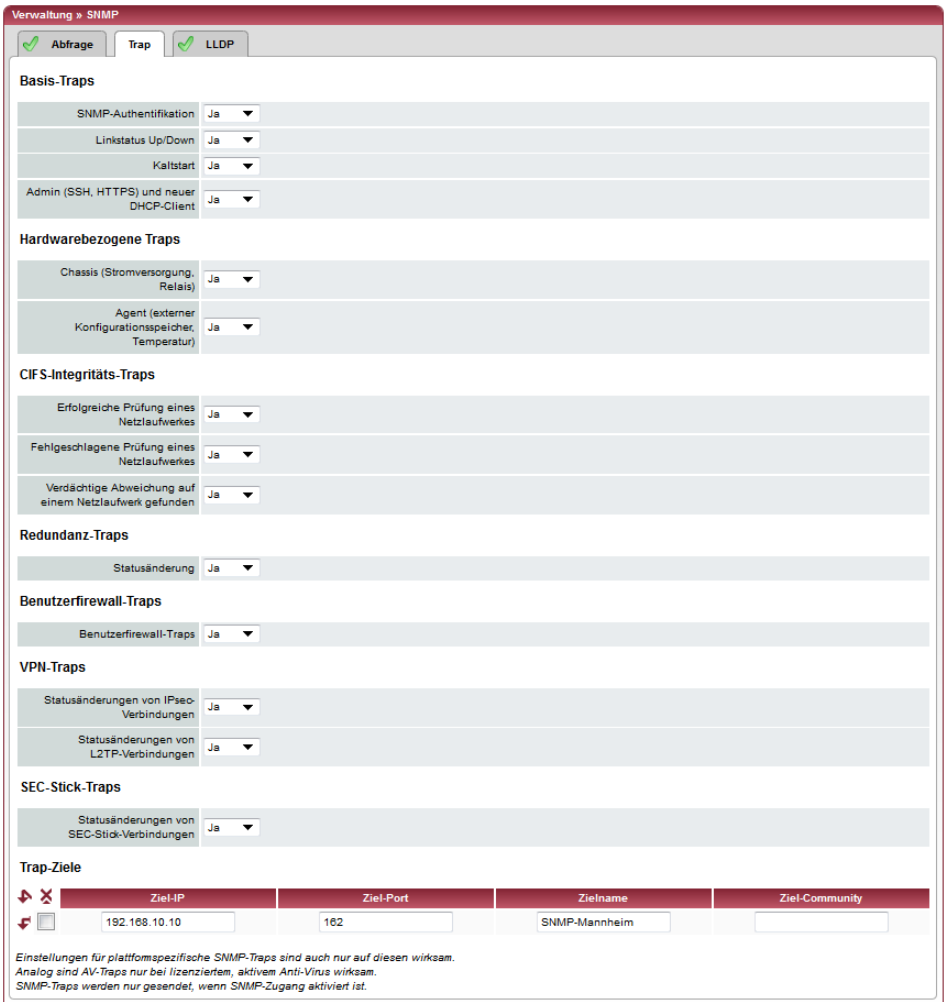
Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

- das Ereignis protokolliert werden soll – *Log* auf **Ja** setzen
- oder das Ereignis nicht protokolliert werden soll – *Log* auf **Nein** setzen (werkseitige Voreinstellung).

1 *Extern 2* und *Einwahl* nur bei Geräten mit serieller Schnittstelle (siehe „Netzwerk >> Interfaces“ auf Seite 6-64).

6.2.6.2 Trap



Bei bestimmten Ereignissen kann der mGuard SNMP-Traps versenden. SNMP-Traps werden nur gesendet, wenn die SNMP-Anfrage aktiviert ist.

Die Traps entsprechen SNMPv1. Im Folgenden sind die zu jeder Einstellung zugehörigen Trap-Informationen aufgelistet, deren genaue Beschreibung in der zum mGuard gehörenden MIB zu finden ist.

Werden SNMP-Traps über einen VPN-Kanal zur Gegenstelle gesendet, dann muss sich die IP-Adresse der Gegenstelle in dem Netzwerk befinden, das in der Definition der VPN-Verbindung als **Remote**-Netzwerk angegeben ist.

Die interne IP-Adresse (im Stealth-Modus die **Stealth Management IP-Adresse** bzw. **Virtuelle IP**) muss sich in dem Netzwerk befinden, das in der Definition der VPN-Verbindung als **Lokal** angegeben ist (siehe „VPN-Verbindung / VPN-Verbindungskanäle definieren“ auf Seite 6-190).

– Ist dabei die Option **Aktiviere 1-zu-1-NAT des lokalen Netzwerkes in ein internes Netz** auf **Ja** gestellt (siehe „1-zu-1-NAT“ auf Seite 6-203), gilt Folgendes:

  Die interne IP-Adresse (im Stealth-Modus die **Stealth Management IP-Adresse** bzw. **Virtuelle IP**) muss sich in dem Netzwerk befinden, das mit **Interne Netzwerkadresse für lokales 1-zu-1-NAT** angegeben ist.

– Ist dabei die Option **Aktiviere 1-zu-1-NAT des gegenüberliegenden Netzwerkes auf ein anders Netz** auf **Ja** gestellt (siehe „1-zu-1-NAT“ auf Seite 6-203), gilt Folgendes:

  Die IP-Adresse des Trap-Empfängers muss sich in dem Netzwerk befinden, das in der Definition der VPN-Verbindung als **Remote** angegeben ist.

Verwaltung >> SNMP >> Trap		
Basis-Traps	**SNMP-Authentifikation**	Traps aktivieren **Ja / Nein** – enterprise-oid : mGuardInfo – generic-trap : authenticationFailure – specific-trap : 0 Wird gesendet, falls eine Station versucht, unberechtigt auf den SNMP-Agenten des mGuards zuzugreifen.
	Linkstatus Up/Down	Traps aktivieren **Ja / Nein** – enterprise-oid : mGuardInfo – generic-trap : linkUp, linkDown – specific-trap : 0 Wird gesendet, wenn die Verbindung zu einem Port unterbrochen (linkDown) bzw. wiederhergestellt (linkUp) wird.
	Kaltstart	Traps aktivieren **Ja / Nein** – enterprise-oid : mGuardInfo – generic-trap : coldStart – specific-trap : 0 Wird nach Kalt- oder Warmstart gesendet.
	Admin (SSH, HTTPS) Traps und neuer DHCP-Client:	Traps aktivieren **Ja / Nein** – enterprise-oid : mGuard – generic-trap : enterpriseSpecific – specific-trap : mGuardHTTPSLoginTrap (1) – additional : mGuardHTTPSLastAccessIP Dieser Trap wird gesendet, wenn jemand erfolgreich oder vergeblich (z. B. mit einem falschen Passwort) versucht hat, eine HTTPS-Sitzung zu öffnen. Der Trap enthält die IP-Adresse, von der der Versuch stammte. – enterprise-oid : mGuard – generic-trap : enterpriseSpecific – specific-trap : mGuardShellLoginTrap (2) – additional : mGuardShellLastAccessIP Dieser Trap wird gesendet, wenn jemand die Shell öffnet per SSH oder über die serielle Schnittstelle. Der Trap enthält die IP-Adresse der Login-Anfrage. Wurde diese Anfrage über die serielle Schnittstelle abgesetzt, lautet der Wert 0.0.0.0.

Verwaltung >> SNMP >> Trap[...]		
		– enterprise-oid : mGuard – generic-trap : enterpriseSpecific – specific-trap : 3 – additional : mGuardDHCPLastAccessMAC Dieser Trap wird gesendet, wenn eine DHCP-Anfrage von einem unbekannten Client eingegangen ist. – enterprise-oid : mGuard – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapSSHLogin – additional : mGuardTResSSHUsername mGuardTResSSHRemoteIP Dieser Trap wird gesendet, wenn jemand per SSH auf den mGuard zugreift. – enterprise-oid : mGuard – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapSSHLogout – additional : mGuardTResSSHUsername mGuardTResSSHRemoteIP Dieser Trap wird gesendet, wenn ein Zugriff per SSH auf den mGuard beendet wird.
Hardwarebezogene Traps (nur mGuard rs4000/rs2000, mGuard industrial rs und EAGLE mGuard)	**Chassis (Stromversorgung, Relais)**	Traps aktivieren **Ja / Nein** – enterprise-oid : mGuardTrapSenderIndustrial – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapIndustrialPowerStatus (2) – additional : mGuardTrapIndustrialPowerStatus Wird gesendet, wenn das System einen Stromausfall registriert. – enterprise-oid : mGuardTrapSenderIndustrial – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapSignalRelais (3) – additional : mGuardTResSignalRelaisState (mGuardTEsSignlalRelaisReason, mGuardTResSignal RelaisReasonIdx) Wird gesendet nach geändertem Meldekontakt und gibt den dann aktuellen Status an (0 = Aus, 1 = Ein).

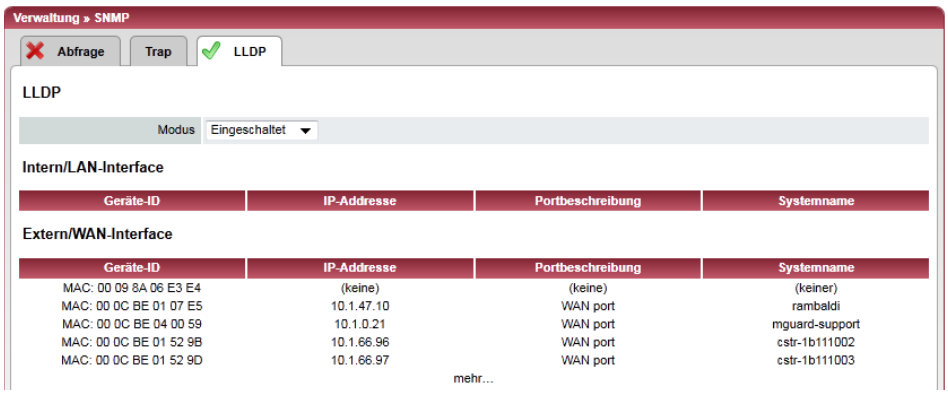
Verwaltung >> SNMP >> Trap[...]		
	Agent (externer Konfigurationsspeicher, Temperatur)	Traps aktivieren **Ja / Nein** – enterprise-oid : mGuardTrapIndustrial – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapIndustrialTemperature (1) – additional : mGuardSystemTemperature, mGuardTrapIndustrialTempHiLimit, mGuardTrapIndustrialLowLimit Bei Überschreitung der festgelegten Grenzwerte gibt der Trap die Temperatur an. – enterprise-oid : mGuardTrapIndustrial – genericTrap : enterpriseSpecific – specific-trap : mGuardTrapAutoConfigAdapterState (4) – additional : mGuardTrapAutoConfigAdapter Change Dieser Trap wird nach Zugriff auf den ECS gesendet.
mGuard blade Controller-Traps (nur blade)	**Statusänderung von Blades**	(Umstecken, Ausfall): Traps aktivieren **Ja / Nein** – enterprise-oid : mGuardTrapBladeCTRL – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapBladeCtrlPowerStatus (2) – additional : mGuardTrapBladeRackID, mGuardTrapBladeSlotNr, mGuardTrapBladeCtrlPowerStatus Trap wird gesendet, wenn der Stromversorgungsstatus des Blade Pack wechselt. – enterprise-oid : mGuardTrapBladeCTRL – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapBladeCtrlRunStatus (3) – additional : mGuardTrapBladeRackID, mGuardTrapBladeSlotNr, mGuardTrapBladeCtrlRunStatus Trap wird gesendet, wenn der Blade-Ausführungsstatus wechselt
	Rekonfiguration von Blades	(Backup/Restore) Traps aktivieren **Ja / Nein** – enterprise-oid : mGuardTrapBladeCtrlCfg – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapBladeCtrlCfgBackup (1) – additional : mGuardTrapBladeRackID, mGuardTrapBladeSlotNr, mGuardTrapBladeCtrlCfgBackup Trap bei Auslösung des Konfigurations-Backups zum mGuard blade-Controller.

Verwaltung >> SNMP >> Trap[...]		
		– enterprise-oid : mGuardTrapBladeCtrlCfg – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapBladeCtrlCfgRestored 2 – additional : mGuardTrapBladeRackID, mGuardTrapBladeSlotNr, mGuardTrapBladeCtrlCfgRestored Trap bei Auslösung der Konfigurations-Wiederherstellung vom mGuard blade-Controller.
CIFS-Integritäts-Traps Dieser Menüpunkt gehört nicht zum Funktionsumfang vom mGuard rs2000.	**Erfolgreiche Prüfung eines Netzlaufwerkes**	Traps aktivieren **Ja / Nein** – enterprise-oid : mGuardTrapCIFSScan – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapCIFSScanInfo (1) – additional : mGuardTResCIFSShare, mGuardTResCIFSScanError, mGuardTResCIFSNumDiffs Dieser Trap wird gesendet, wenn die CIFS-Integritätsprüfung erfolgreich abgeschlossen worden ist.
	Fehlgeschlagene Prüfung eines Netzlaufwerkes	Traps aktivieren **Ja / Nein** – enterprise-oid : mGuardTrapCIFSScan – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapCIFSScanFailure (2) – additional : mGuardTResCIFSShare, mGuardTResCIFSScanError, mGuardTResCIFSNumDiffs Dieser Trap wird gesendet, wenn CIFS-Integritätsprüfung fehlgeschlagen ist.
	Verdächtige Abweichung auf einem Netzwerk gefunden	Traps aktivieren **Ja / Nein** – enterprise-oid : mGuardTrapCIFSScan – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapCIFSScanDetection (3) – additional : mGuardTResCIFSShare, mGuardTResCIFSScanError, mGuardTResCIFSNumDiffs Dieser Trap wird gesendet, wenn bei der CIFS-Integritätsprüfung eine Abweichung festgestellt worden ist.
Benutzerfirewall-Traps Dieser Menüpunkt gehört nicht zum Funktionsumfang vom mGuard rs2000.	**Benutzerfirewall-Traps**	Traps aktivieren **Ja / Nein**. – enterprise-oid : mGuardTrapUserFirewall – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapUserFirewallLogin (1) – additional : mGuardTResUserFirewallUsername, mGuardTResUserFirewallSrcIP, mGuardTResUserFirewallAuthenticationMethod Trap bei Einloggen eines Benutzers der Benutzer-Firewall.

Verwaltung >> SNMP >> Trap[...]		
		– enterprise-oid : mGuardTrapUserFirewall – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapUserFirewallLogout (2) – additional : mGuardTResUserFirewallUsername, mGuardTResUserFirewallSrcIP, mGuardTResUserFirewallLogoutReason Trap bei Ausloggen eines Benutzers der Benutzer-Firewall – enterprise-oid : mGuardTrapUserFirewall – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapUserFirewallAuthError TRAP-TYPE (3) – additional : mGuardTResUserFirewallUsername, mGuardTResUserFirewallSrcIP, mGuardTResUserFirewallAuthenticationMethod Trap bei Authentifizierungs-Fehler.
VPN-Traps	**Statusänderungen von IPsec-Verbindungen**	Traps aktivieren **Ja / Nein**. – enterprise-oid : mGuardTrapVPN – genericTrap : enterpriseSpecific – specific-trap : mGuardTrapVPNIKEServerStatus (1) – additional : mGuardTResVPNStatus Trap beim Starten und Stoppen des IPsec-IKE-Servers – enterprise-oid : mGuardTrapVPN – genericTrap : enterpriseSpecific – specific-trap : mGuardTrapVPNIPsecConnStatus (2) – additional : mGuardTResVPNName, mGuardTResVPNIndex, mGuardTResVPNPeer, mGuardTResVPNStatus, mGuardTResVPNType, mGuardTResVPNLocal, mGuardTResVPNRemote Trap bei Zustandsänderung einer IPsec-Verbindung – enterprise-oid : mGuard – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapVPNIPsecConnStatus Dieser Trap wird gesendet, wenn eine Verbindung aufgebaut oder getrennt wird. Er wird nicht gesendet, wenn der mGuard dabei ist, eine Verbindungsanfrage für diese Verbindung zu akzeptieren.

Verwaltung >> SNMP >> Trap[...]		
	Statusänderungen von L2TP-Verbindungen	Traps aktivieren **Ja / Nein**. – enterprise-oid : mGuardTrapVPN – genericTrap : enterpriseSpecific – specific-trap : mGuardTrapVPNL2TPConnStatus (3) – additional : mGuardTResVPNName, mGuardTResVPNIndex, mGuardTResVPNPeer, mGuardTResVPNStatus, mGuardTResVPNLocal, mGuardTResVPNRemote Trap bei Zustandsänderung einer L2TP-Verbindung
SNMP-Trap-Ziele	**Traps können an mehrere Ziele versendet werden.**	
	Ziel-IP	IP-Adresse, an welche der Trap gesendet werden soll.
	Ziel-Port	Standard: 162 Ziel-Port, an welchen der Trap gesendet werden soll
	Zielname	Ein optionaler beschreibender Name für das Ziel. Hat keinen Einfluss auf die generierten Traps.
	Ziel-Community	Name der SNMP-Community, der der Trap zugeordnet ist.

6.2.6.3 LLDP

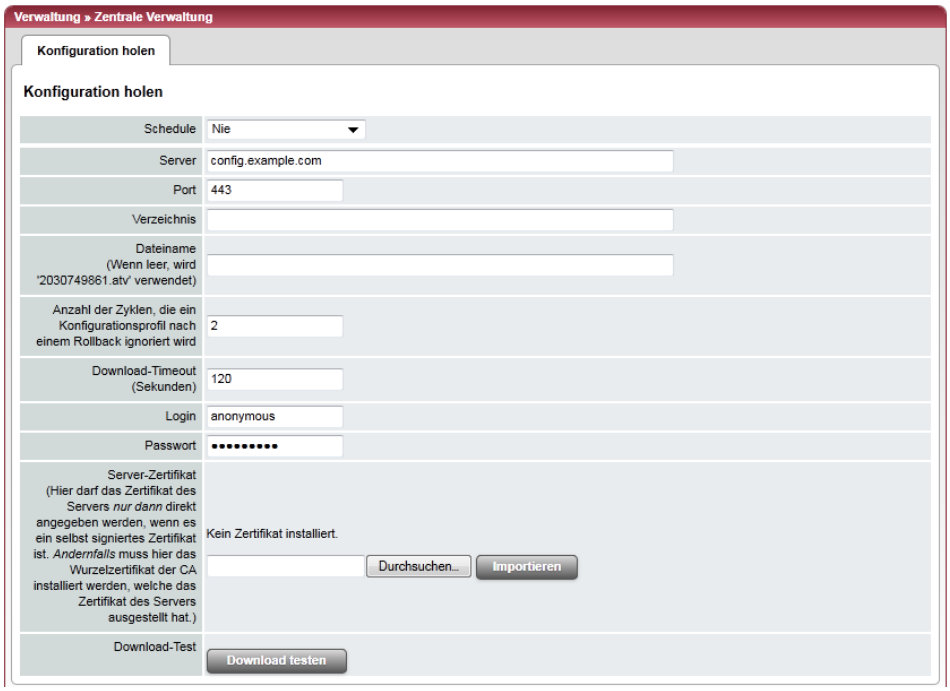


Mit LLDP (Link Layer Discovery Protocol, IEEE 802.1AB/D13) kann mit geeigneten Abfragemethoden die (Ethernet) Netzwerk-Infrastruktur automatisch ermittelt werden. Auf Ethernet-Ebene (Layer 2) werden dazu periodisch Multicasts versandt. Aus deren Antworten werden dann Tabellen der ans Netz angeschlossenen Systeme erstellt, die über SNMP abgefragt werden können.

Verwaltung >> SNMP >> LLDP		
LLDP	**Modus**	**Eingeschaltet / Ausgeschaltet** Der LLDP-Service bzw. -Agent kann hier global ein- bzw. ausgeschaltet werden. Ist die Funktion eingeschaltet, wird das oben auf der Registerkartenzunge durch ein grünes Signalfeld angezeigt. Ist das Signalfeld auf Rot, ist die Funktion ausgeschaltet.
Intern/LAN-Interface **Extern/WAN-Interface**	**Geräte-ID**	Eine eindeutige ID des gefundenen Rechners; üblicherweise eine seiner MAC-Adressen.
	IP-Adresse	IP-Adresse des gefundenen Rechners über die der Rechner per SNMP administriert werden kann.
	Portbeschreibung	Ein Text, welcher die Netzwerkschnittstelle beschreibt, über welche der Rechner gefunden wurde.
	Systemname	Hostname des gefundenen Rechners.
	Schaltfläche: Aktualisieren	Um gegebenenfalls die angezeigten Daten auf den aktuellen Stand zu bringen, auf die Schaltfläche **Aktualisieren** klicken.

6.2.7 Verwaltung >> Zentrale Verwaltung

6.2.7.1 Konfiguration holen



Der mGuard kann sich in einstellbaren Zeitintervallen neue Konfigurationsprofile von einem HTTPS Server holen, wenn der Server sie dem mGuard als Datei zur Verfügung stellt (Datei-Endung: .atv). Wenn sich die jeweils zur Verfügung gestellte Konfiguration von der aktuellen Konfiguration des mGuards unterscheidet, wird die verfügbare Konfiguration automatisch heruntergeladen und aktiviert.

Verwaltung >> Zentrale Verwaltung >> Konfiguration holen		
Konfiguration holen	**Schedule**	Geben Sie hier an, ob - und wenn ja - wann bzw. in welchen Zeitabständen der mGuard versuchen soll, eine neue Konfiguration vom Server herunterzuladen und bei sich in Kraft zu setzen. Öffnen Sie dazu die Auswahlliste und wählen Sie den gewünschten Wert. Bei Auswahl von **Zeitgesteuert** wird unterhalb ein neues Feld eingeblendet. In diesem geben Sie an, ob täglich oder an einem bestimmten Wochentag regelmäßig und zu welcher Uhrzeit eine neue Konfiguration vom Server heruntergeladen werden soll. Das zeitgesteuerte Herunterladen einer neuen Konfiguration kann erst nach Synchronisation der Systemzeit erfolgen (siehe „Verwaltung >> Systemeinstellungen“ auf Seite 6-4, „Zeit und Datum“ auf Seite 6-8). Die Zeitsteuerung setzt die ausgewählte Zeit in Bezug auf die eventuell konfigurierte Zeitzone.
	Server	IP-Adresse oder Hostname des Servers, welcher die Konfigurationen bereitstellt.

Verwaltung >> Zentrale Verwaltung >> Konfiguration holen[...]

Verzeichnis	Das Verzeichnis (Ordner) auf dem Server, in dem die Konfiguration liegt.
Dateiname	Der Name der Datei in dem oben definierten Verzeichnis. Falls an dieser Stelle kein Dateiname definiert ist, wird die Seriennummer des mGuards inklusive der Endung „.atv“ verwendet.
Anzahl der Zyklen, die ein Konfigurationsprofil nach einem Rollback ignoriert wird	Standard: 10 Nach Holen einer neuen Konfiguration könnte es im Prinzip passieren, dass nach Inkraftsetzen der neuen Konfiguration der mGuard nicht mehr erreichbar ist und damit eine neue, korrigierende Fernkonfiguration nicht mehr möglich ist. Um das auszuschließen, unternimmt der mGuard folgende Prüfung:

Sofort nach Inkraftsetzen der geholten Konfiguration versucht der mGuard auf Grundlage dieser neuen Konfiguration, die Verbindung zum Konfigurations-Server nochmals herzustellen und das neue, bereits in Kraft gesetzte Konfigurationsprofil erneut herunterzuladen.

Wenn das gelingt, bleibt die neue Konfiguration in Kraft.

Wenn diese Prüfung negativ ausfällt - aus welchen Gründen auch immer -, geht der mGuard davon aus, dass das gerade in Kraft gesetzte neue Konfigurationsprofil fehlerhaft ist. Für Identifizierungszwecke merkt sich der mGuard dessen MD5-Summe. Dann führt der mGuard ein Rollback durch.

Rollback bedeutet, dass die letzte (funktionierende) Konfiguration wiederhergestellt wird. Das setzt voraus, dass in der neuen (nicht funktionierenden) Konfiguration die Anweisung steht, ein Rollback durchzuführen, wenn ein neues geladenes Konfigurationsprofil sich in dem oben beschriebenen Prüfungsverfahren als fehlerhaft erweist.

Wenn nach der im Feld **Schedule** (und **Zeitgesteuert**) festgelegten Zeit der mGuard erneut und zyklisch versucht, ein neues Konfigurationsprofil zu holen, wird er ein solches nur unter folgendem Auswahlkriterium annehmen: Das zur Verfügung gestellte Konfigurationsprofil **muss sich unterscheiden** von dem Konfigurationsprofil, das sich für den mGuard zuvor als fehlerhaft erwiesen hat und zum Rollback geführt hat.

(Dazu vergleicht der mGuard die bei ihm gespeicherte MD5-Summe der alten, für ihn fehlerhaften und verworfenen Konfiguration mit der MD5-Summe des angebotenen neuen Konfigurationsprofils.)

Wird dieses Auswahlkriterium **erfüllt**, d. h. es wird ein neueres Konfigurationsprofil angeboten, holt sich der mGuard dieses Konfigurationsprofil, setzt es in Kraft und prüft es gemäß des oben beschriebenen Verfahrens - und setzt es bei nicht bestandener Prüfung per Rollback wieder außer Kraft.

Verwaltung >> Zentrale Verwaltung >> Konfiguration holen[...]

Wird dieses Auswahlkriterium **nicht erfüllt** (weil immer noch das selbe Konfigurationsprofil angeboten wird), bleibt für die weiteren zyklischen Abfragen dieses Auswahlkriterium so lange in Kraft, wie in diesem Feld (**Anzahl der Zyklen...**) festgelegt ist.

Ist die hier festgelegte Anzahl von Zyklen abgelaufen, ohne dass das auf dem Konfigurations-Server angebotene Konfigurationsprofil verändert wurde, setzt der mGuard das unveränderte neue („fehlerhafte“) Konfigurationsprofil ein weiteres Mal in Kraft, obwohl es sich als „fehlerhaft“ erwiesen hatte. Das geschieht um auszuschließen, dass das Misslingen der Prüfung durch äußere Faktoren (z. B. Netzwerkausfall) bedingt war.

Der mGuard versucht dann erneut, auf Grundlage der erneut eingesetzten neuen Konfiguration die Verbindung zum Konfigurations-Server herzustellen und erneut das neue, jetzt in Kraft gesetzte Konfigurationsprofil herunterzuladen. Wenn das misslingt, erfolgt wieder ein Rollback, und für die weiteren Zyklen zum Laden einer neuen Konfiguration wird erneut das Auswahlkriterium in Kraft gesetzt - so oft, wie in diesem Feld (**Anzahl der Zyklen...**) festgelegt ist.

Wird im Feld **Anzahl der Zyklen...** als Wert **0** (Null) festgelegt, hat das zur Folge, dass das Auswahlkriterium - das angebotene Konfigurationsprofil wird ignoriert, wenn es unverändert geblieben ist - niemals in Kraft tritt. Dadurch könnte das 2. der nachfolgend aufgeführten Ziele nicht realisiert werden.

Dieser Mechanismus hat folgende Ziele:

1. Nach Inkraftsetzen einer neuen Konfiguration muss sichergestellt sein, dass der mGuard sich weiterhin vom entfernten Standort aus konfigurieren lässt.
2. Bei eng gesetzten Zyklen (z. B. bei **Schedule** = 15 Minuten) muss verhindert werden, dass der mGuard stur ein möglicherweise fehlerhaftes Konfigurationsprofil in zu kurzen Abständen immer wieder erneut testet. Das könnte dazu führen, dass der mGuard so mit sich selbst beschäftigt ist, dass ein administrativer Eingriff von außen behindert oder verhindert wird.
3. Es muss mit großer Wahrscheinlichkeit ausgeschlossen werden, dass äußere Faktoren (z. B. Netzwerkausfall) den mGuard bewogen haben, eine Neukonfiguration als fehlerhaft zu betrachten. .

Von Innominate wird eine Application Note zur Verfügung gestellt. Darin ist beschrieben, wie über ein Konfigurationsprofil ein Rollback angewiesen werden kann. (Application Notes stehen im Download-Bereich von www.innominate.com bereit.)

Download-Timeout (Sekunden)	Standard: 120. Gibt an, wie lange während eines Downloads der Konfigurationsdatei ein Timeout (Zeit der Inaktivität) maximal dauern darf. Bei Überschreitung wird der Download abgebrochen. Ob und wann ein nächster Download-Versuch stattfindet, richtet sich nach der Einstellung von *Schedule* (s. o.).
Login	Login (Benutzername), den der HTTPS Server abfragt.
Passwort	Passwort, das der HTTPS Server abfragt.
Server-Zertifikat	Das Zertifikat, mit dem der mGuard prüft, dass das vom Konfigurations-Server „vorgezeigte“ Zertifikat echt ist. Es verhindert, dass von einem nicht autorisierten Server falsche Konfigurationen auf dem mGuard installiert werden.

Verwaltung >> Zentrale Verwaltung >> Konfiguration holen[...]

Hier darf entweder

– ein selbst signiertes Zertifikat des Konfigurations-Servers angegeben werden oder

– das Wurzelzertifikat der CA (Certification Authority), welche das Zertifikat des Servers ausgestellt hat. Das gilt dann, wenn es sich beim Zertifikat des Konfigurations-Servers um ein von einer CA signiertes Zertifikat handelt (statt um ein selbst signiertes)

Wenn die hinterlegten Konfigurationsprofile auch den privaten VPN-Schlüssel für die VPN-Verbindung oder VPN-Verbindungen mit PSK enthalten, sollten folgende Bedingungen erfüllt sein:

– Das Passwort sollte aus mindestens 30 zufälligen Groß- und Kleinbuchstaben sowie Ziffern bestehen, um unerlaubten Zugriff zu verhindern.

– Der HTTPS Server sollte über den angegebenen Login nebst Passwort nur Zugriff auf die Konfiguration dieses einen mGuard ermöglichen. Ansonsten könnten sich die Benutzer anderer mGuards Zugriff verschaffen.

Die unter Server angegebene IP-Adresse bzw. der Hostname muss im Server-Zertifikat als Common-Name (CN) angegeben sein.

Selbstunterschriebene Zertifikate (self-signed) sollten nicht die „key-usage“ Erweiterung verwenden.

Zum Installieren eines Zertifikats wie folgt vorgehen:

Voraussetzung: Die Zertifikatsdatei ist auf dem angeschlossenen Rechner gespeichert

- **Durchsuchen...** klicken, um die Datei zu selektieren.
- **Importieren** klicken.

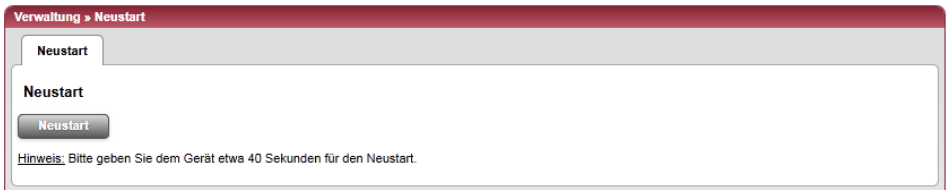
Download-Test

- Durch Klicken auf die Schaltfläche **Download testen** können Sie testen – ohne die geänderten Parameter zu speichern oder das Konfigurationsprofil zu aktivieren – ob die angegebenen Parameter funktionieren. Das Ergebnis des Tests wird in der rechten Spalte angezeigt.

Stellen Sie sicher, dass das Profil auf dem Server keine unerwünschten mit „GAI_PULL_“ beginnenden Variablen enthält, welche die hier vorgenommene Konfiguration überschreiben.

6.2.8 Verwaltung >> Neustart

6.2.8.1 Restart



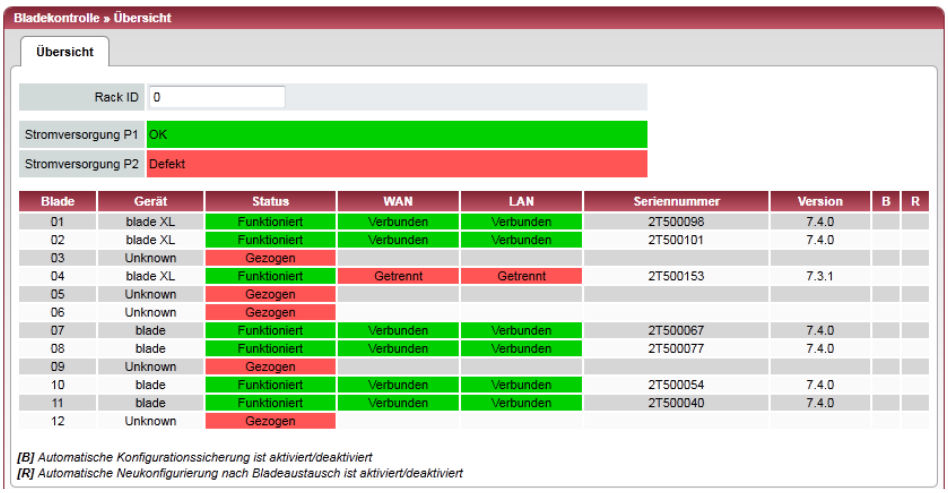
Startet den mGuard neu. Hat den selben Effekt, als wenn Sie die Stromzufuhr vorübergehend unterbrechen, so dass der mGuard aus- und wieder eingeschaltet wird.

Ein Neustart (= Reboot) ist erforderlich im Fehlerfall. Außerdem kann ein Neustart nach einem Software-Update erforderlich sein.

6.3 Menü Bladekontrolle

Dieses Menü steht nur auf dem **mGuard blade-Controller** zur Verfügung.

6.3.1 Bladekontrolle >> Übersicht



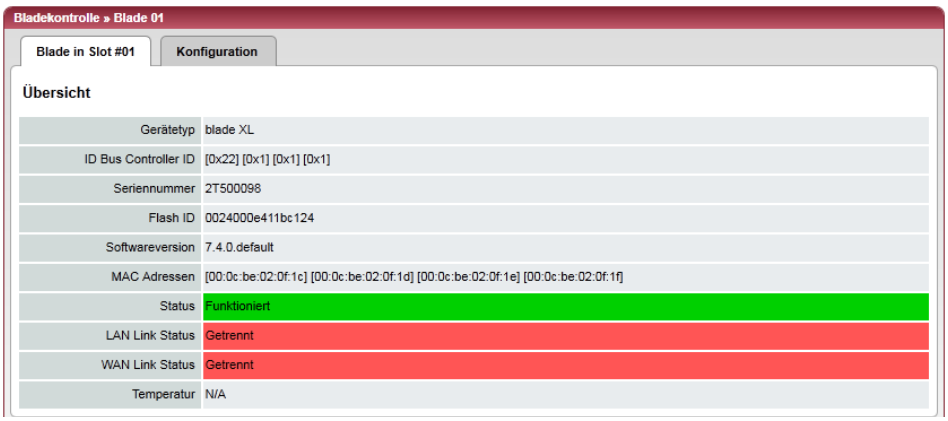
Bladekontrolle >> Übersicht		
Übersicht	**Rack ID**	Die ID des Racks, in dem sich der mGuard befindet. Auf dem Controller kann dieser Wert für alle blades konfiguriert werden.
	Stromversorgung P1/P2	Status der Netzteile P1 und P2. – OK – Gezogen – Defekt – Fataler Fehler
	Blade	Nummer des Slots, in welchem das mGuard blade steckt.
	Gerät	Name des Geräts, z. B. „blade“ oder „blade XL“.
	Status	– **Funktioniert -** Das Gerät in dem Slot ist funktionsbereit. – **Gesteckt -** Das Gerät ist vorhanden, aber noch nicht bereit, z. B. weil es gerade beim Starten ist. – **Gezogen -** In dem Slot wurde kein Gerät entdeckt.
	WAN	Status des WAN-Ports.
	LAN	Status des LAN-Ports.
	Seriennummer	Seriennummer des mGuards.
	Version	Softwareversion des mGuards.
	B	**Backup**: Für diesen Slot ist die automatische Konfigurationssicherung auf dem Controller aktiviert/deaktiviert.

Bladekontrolle >> Übersicht [...]		
	R	**Restore**: Für diesen Slot ist das automatische Zurückspielen der Konfiguration nach Austausch des mGuards aktiviert/deaktiviert.

6.3.2 Bladekontrolle >> Blade 01 bis 12

Diese Seiten zeigen für jeden installierten mGuard Statusinformationen an und erlauben das Speichern und Zurückspielen der Konfiguration des jeweiligen mGuards.

6.3.2.1 Blade in slot #...



Bladekontrolle >> Blade xx >> Blade in slot xx		
Übersicht	**Gerätetyp**	Name des Geräts, z. B. „blade“ oder „blade XL“.
	ID Bus Controller-ID	ID dieses Slots am Steuerbus der bladebase.
	Seriennummer	Seriennummer des mGuards.
	Flash-ID	Flash-ID des Flashspeichers des mGuards.
	Software-Version	Die Version der auf dem mGuard installierten Software.
	MAC-Adressen	Alle vom mGuard verwendeten MAC-Adressen.
	Status	Status des mGuards.
	LAN-Status	Status des LAN-Ports.
	WAN-Status	Status des WAN-Ports.
	Temperatur	N/A = nicht verfügbar

6.3.2.2 Konfiguration

Bladekontrolle>> Blade xx >> Konfiguration

Konfiguration

Für jeden blade wird der Status der gespeicherten Konfiguration angezeigt:

[Keine Konfiguration vorhanden]

[Veraltet]

[Aktuell]

[Datei wird kopiert]

[Blade wurde ausgewechselt]

[---] Kein Blade vorhanden

Konfigurationssicherung [Blade #__ -> Controller]

- **Automatisch:** Kurz nach einer Konfigurationsänderung des mGuards wird die neue Konfiguration automatisch auf dem Controller gespeichert.
- **Manuell:** Die Konfiguration kann mit **Sichern** auf dem Controller gesichert werden.
- Mit **Zurückspielen** kann die auf dem Controller gesicherte Konfiguration in den mGuard übertragen werden.

Wurde nach einer manuellen Konfigurationssicherung das Blade umkonfiguriert, aber die neue Konfiguration nicht erneut gesichert, ist die im Controller gespeicherte Konfiguration veraltet. Dies wird auf der Registerkarte *Konfiguration* durch „Konfiguration [Veraltet]“ angezeigt.

Das ist als Hinweis auf ein Versäumnis zu verstehen: Sorgen Sie in diesem Fall für die Konfigurationssicherung auf den Controller.

Neukonfiguration bei Austausch des mGuard blades

Beim Austausch eines mGuards in diesem Slot wird die auf dem Controller gespeicherte Konfiguration auf das neue Gerät in diesem Slot übertragen.

Konfigurationssicherung des Blade #__ löschen

Löscht die auf dem Controller gespeicherte Konfiguration für das Gerät in diesem Slot.

Hochladen der Konfiguration vom Client

Hochladen und Speichern des angegebenen Konfigurationsprofils für diesen Slot auf dem Controller.

Herunterladen der Konfiguration zum Client

Lädt das auf dem Controller gespeicherte Konfigurationsprofil für diesen Slot auf den Konfigurations-PC.

6.4 Menü Netzwerk

6.4.1 Netzwerk >> Interfaces

Der mGuard verfügt über folgende von außen zugängliche Interfaces (Schnittstellen):

	Ethernet: Intern: LAN Extern: WAN	Serielle Schnittstelle	Eingebautes Modem	Serielle Konsole über USB[1]
mGuard smart	**ja**	**nein**	**nein**	**nein**
mGuard smart[2]	**ja**	**nein**	**nein**	**ja**
mGuard rs4000/rs2000, mGuard centerport, mGuard industrial rs, mGuard pci[2] SD, mGuard pci, mGuard blade, mGuard delta, mGuard delta[2], EAGLE mGuard	**ja**	**ja**	**nein**	**nein**
optional: mGuard industrial rs	**ja**	**ja**	**ja**	**nein**

[1] Siehe „Serielle Konsole über USB“ auf Seite 6-101.

Der LAN-Port wird an einen Einzelrechner oder das lokale Netzwerk (= intern) angeschlossen. Der WAN-Port ist für den Anschluss an das externe Netz. Bei Geräten mit serieller Schnittstelle kann der Anschluss ans externe Netz auch oder zusätzlich über die serielle Schnittstelle mittels eines Modems erfolgen. Alternativ kann die serielle Schnittstelle auch wie folgt benutzt werden: für ppp-Einwahl ins lokale Netz oder für Konfigurationszwecke. Bei Geräten mit eingebautem Modem (Analog-Modem oder ISDN-Terminaladapter) kann zusätzlich das Modem benutzt werden, um Zugriffsmöglichkeiten zu kombinieren.

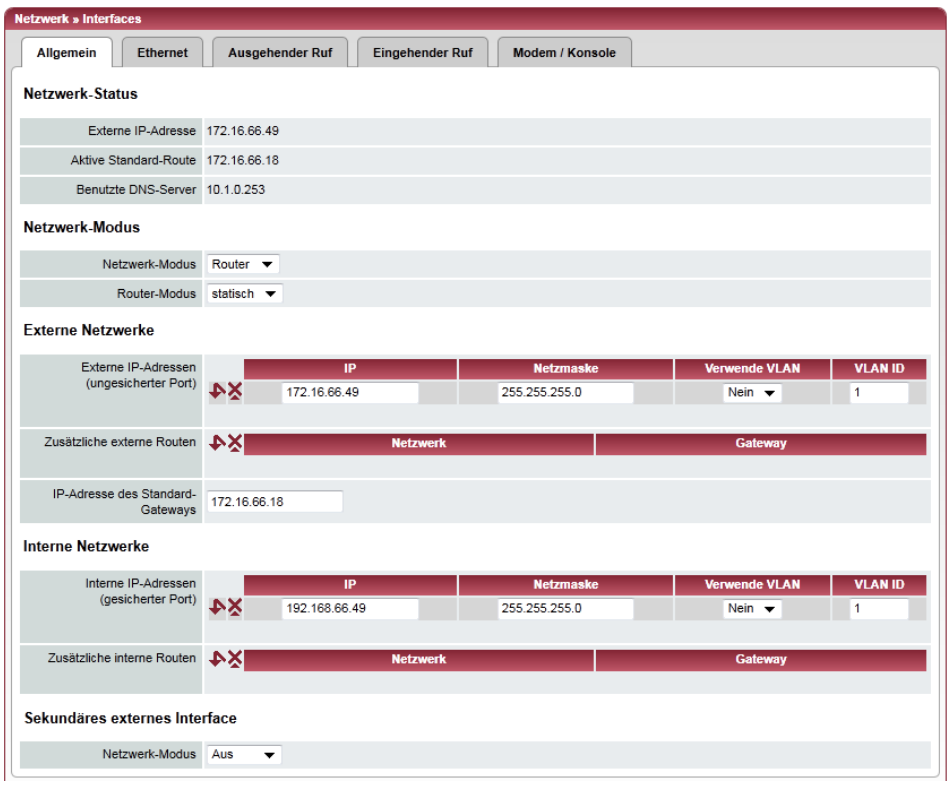
Die Details dazu müssen auf den Registerkarten *Allgemein, Ethernet, Ausgehender Ruf, Eingehender Ruf* und *Modem / Konsole* konfiguriert werden. Für weitere Erläuterungen zur Nutzungsmöglichkeit der seriellen Schnittstelle (und eines eingebauten Modems) siehe „Modem / Konsole“ auf Seite 6-100.

Anschließen der Netzwerk-Schnittstelle

Schließen Sie den EAGLE mGuard über ein normales Ethernet-Patch-Kabel an den PC an. Auf diese Weise wird eine korrekte Verbindung ermöglicht, auch wenn Auto-MDIX und Autonegotiation ausgeschaltet sind.

Der EAGLE mGuard hat eine DCE-Netzwerk-Schnittstelle, während alle anderen mGuard-Plattformen DTE-Schnittstellen haben. Schließen Sie diese mGuards mit einem gekreuzten Ethernet-Kabel an. Allerdings ist hier das Auto-MDIX dauerhaft eingeschaltet, so dass es keine Rolle spielt, wenn der Parameter Autonegotiation ausgeschaltet wird.

6.4.1.1 Allgemein



Netzwerk>> Interfaces >> Allgemein		
Netzwerk-Status	**Externe IP-Adresse - Adresse des WAN-Ports**	Nur Anzeige: Die Adressen, unter denen der mGuard von Geräten des externen Netzes aus erreichbar ist. Sie bilden die Schnittstelle zu anderen Teilen des LAN oder zum Internet. Findet hier der Übergang zum Internet statt, werden die IP-Adressen normalerweise vom Internet Service Provider (ISP) vorgegeben. Wird dem mGuard eine IP-Adresse dynamisch zugeteilt, können Sie hier die gerade gültige IP-Adresse nachschlagen. Im *Stealth*-Modus übernimmt der mGuard die Adresse des lokal angeschlossenen Rechners als seine externe IP.
	Status des Netzwerk-Modus	Anzeige des Status des ausgewählten Netzwerk Modus.
	Aktive Standard-Route	Nur Anzeige: Hier wird die IP-Adresse angezeigt, über die der mGuard versucht, ihm unbekannte Netze zu erreichen. Hier kann insbesondere dann „(none)“ stehen, wenn sich der mGuard im *Stealth*-Modus befindet.
	Benutzte DNS-Server	Nur Anzeige: Hier wird der Name der DNS-Server angezeigt, die vom mGuard zur Namensauflösung benutzt werden. Diese Information kann nützlich sein, wenn der mGuard z. B. die DNS-Server verwendet, welche ihm vom Internet Service Provider vorgegeben werden.

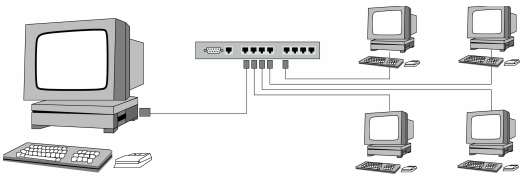
Netzwerk>> Interfaces >> Allgemein[...]		
Netzwerk-Modus	**Netzwerk-Modus**	**Stealth / Router** Der mGuard muss auf den Netzwerk-Modus gestellt werden, der seiner Einbindung in das Netzwerk entspricht (siehe auch „Typische Anwendungsszenarien“ auf Seite 2-1). Je nach dem, auf welchen Netzwerk-Modus der mGuard gestellt ist, ändert sich auch die Seite mit den auf ihr angebotenen Konfigurationsparametern. Siehe: „Stealth (Werkseinstellung mGuard rs4000/rs2000, mGuard industrial rs, mGuard smart², mGuard pci² SD, mGuard pci, mGuard delta², EAGLE mGuard)“ auf Seite 6-67 und „Netzwerk-Modus: Stealth“ auf Seite 6-71 „Router (Werkseinstellung mGuard centerport, mGuard blade-Controller, mGuard delta)“ auf Seite 6-68 und „Netzwerk-Modus: Router“ auf Seite 6-82
Router-Modus	Nur, wenn Netzwerk-Modus „Router“ gewählt worden ist.	**statisch / DHCP / PPPoE / PPTP / Modem[1] / Eingebautes Modem[1]** Siehe: „Router-Modus: statisch“ auf Seite 6-69 und „Netzwerk-Modus: Router, Router-Modus = PPTP“ auf Seite 6-87 „Router-Modus: DHCP“ auf Seite 6-69 und „Netzwerk-Modus = Router, Router-Modus = DHCP“ auf Seite 6-85 „Router-Modus: PPPoE“ auf Seite 6-69 und „Netzwerk-Modus = Router, Router-Modus = PPPoE“ auf Seite 6-86 „Router-Modus: PPTP“ auf Seite 6-69 und „Netzwerk-Modus: Router, Router-Modus = PPTP“ auf Seite 6-87 „Router-Modus: Modem“ auf Seite 6-70 und „Netzwerk-Modus = Router, Router-Modus = Modem / Eingebautes Modem“ auf Seite 6-88 „Router-Modus: Eingebautes Modem“ auf Seite 6-70 und „Netzwerk-Modus = Router, Router-Modus = Modem / Eingebautes Modem“ auf Seite 6-88

1 *M*odem/Eingebautes Modem steht nicht bei allen mGuard-Modellen zur Verfügung (siehe „Netzwerk >> Interfaces“ auf Seite 6-64)

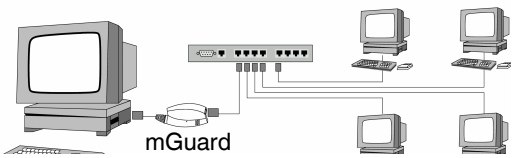
Stealth (Werkseinstellung mGuard rs4000/rs2000, mGuard industrial rs, mGuard smart², mGuard pci² SD, mGuard pci, mGuard delta², EAGLE mGuard)

Der *Stealth*-Modus wird verwendet, um einen einzelnen Computer oder ein lokales Netzwerk mit dem mGuard zu schützen. Wesentlich ist Folgendes: Ist der mGuard im Netzwerk-Modus *Stealth*, wird er in das bestehende Netzwerk eingefügt (siehe Abbildung), ohne dass die bestehende Netzwerkkonfiguration der angeschlossenen Geräte geändert wird.

vorher:



nachher:



(Links kann auch ein LAN sein.)

Der mGuard analysiert den laufenden Netzwerkverkehr und konfiguriert dementsprechend seine Netzwerkanbindung eigenständig und arbeitet transparent, d. h. ohne dass die Rechner umkonfiguriert werden müssen.

Wie auch in den anderen Modi stehen die Sicherheitsfunktionen Firewall und VPN zur Verfügung.

Von extern gelieferte DHCP-Daten werden an den angeschlossenen Rechner durchgelassen.

Eine auf dem Rechner installierte Firewall muss ICMP-Echo-Requests (Ping) zulassen, wenn der mGuard Dienste wie VPN, DNS, NTP, etc. bereit stellen soll.

Im *Stealth*-Modus hat der mGuard die interne IP-Adresse 1.1.1.1, welche vom Rechner erreichbar ist, wenn das auf dem Rechner konfigurierte Standard-Gateway erreichbar ist.

Im Netzwerk-Modus *Stealth* kann zusätzlich ein sekundäres externes Interface konfiguriert werden (siehe „Sekundäres externes Interface“ auf Seite 6-75).

Für die weitere Konfiguration des Netzwerk-Modus *Stealth* siehe „Netzwerk-Modus: Stealth“ auf Seite 6-71.

Router (Werkseinstellung mGuard centerport, mGuard blade-Controller, mGuard delta)

Befindet sich der mGuard im *Router*-Modus, arbeitet er als Gateway zwischen verschiedenen Teilnetzen und hat dabei ein externes Interface (= WAN-Port) und ein internes Interface (= LAN-Port) mit jeweils mindestens einer IP-Adresse.

WAN-Port

Über seinen WAN-Port ist der mGuard ans Internet oder an Teile des LAN angeschlossen, die als „extern“ gelten.

– mGuard smart^2: Der WAN-Port ist die Ethernet-Buchse.

LAN-Port

Über seinen LAN-Port ist der mGuard an ein lokales Netzwerk oder an einen Einzelrechner angeschlossen:

– mGuard smart^2: Der LAN-Port ist der Ethernet-Stecker.
– mGuard pci: Im *Treibermodus* wird der LAN-Port durch die Netzwerkschnittstelle des Betriebssystems gebildet, die das Betriebssystem zur Netzwerkkarte - hier der mGuard pci - hat.

  Im *Power-over-PCI-Modus* ist der LAN-Port durch die LAN-Buchse des mGuard pci gegeben.

Wie auch in den anderen Modi stehen die Sicherheitsfunktionen Firewall und VPN zur Verfügung.

Wird der mGuard im *Router*-Modus betrieben, muss er bei lokal angeschlossenen Rechnern als Standard-Gateway festgelegt sein.

Das heißt, dass bei diesen Rechnern die IP-Adresse des LAN-Ports des mGuards als Adresse des Standard-Gateway anzugeben ist.

Wenn der mGuard im *Router*-Modus betrieben wird und die Verbindung zum Internet herstellt, dann sollte NAT aktiviert werden (siehe „Netzwerk >> NAT“ auf Seite 6-107).

Nur dann erhalten die Rechner im angeschlossenen lokalen Netz über den mGuard Zugriff auf das Internet. Ist NAT nicht aktiviert, können eventuell nur VPN-Verbindungen genutzt werden.

Im Netzwerk-Modus *Router* kann zusätzlich ein sekundäres externes Interface konfiguriert werden (siehe „Sekundäres externes Interface“ auf Seite 6-75).

Es gibt mehrere Router-Modi, je nach Internetanbindung:

– statisch
– DHCP
– PPPoE
– PPPT
– Modem
– Eingebautes Modem

Router-Modus: statisch

Die IP-Adresse ist fest eingestellt.

Router-Modus: DHCP

Die IP-Adresse wird über DHCP vergeben.

Router-Modus: PPPoE

Der *PPPoE*-Modus entspricht dem Router-Modus mit DHCP – mit einem Unterschied: Für den Anschluss ans externe Netzwerk (Internet, WAN) wird das PPPoE-Protokoll verwendet, das von vielen DSL-Modems (bei DSL-Internetzugang) verwendet wird. Die externe IP-Adresse, unter der der mGuard von entfernten Gegenstellen aus erreichbar ist, wird vom Provider festgelegt.

Wird der mGuard im *PPPoE*-Modus betrieben, muss bei lokal angeschlossenen Rechnern der mGuard als Standard-Gateway festgelegt sein.

Das heißt, dass bei diesen Rechnern die IP-Adresse des LAN-Ports des mGuards als Adresse des Standard-Gateway anzugeben ist.

Arbeitet der mGuard im *PPPoE*-Modus, muss NAT aktiviert werden, um Zugriff auf das Internet zu erhalten.

Ist NAT nicht aktiviert, können eventuell nur VPN-Verbindungen genutzt werden.

Für die weitere Konfiguration des Netzwerk-Modus *PPPoE* siehe „Netzwerk-Modus = Router, Router-Modus = PPPoE“ auf Seite 6-86.

Router-Modus: PPTP

Ähnlich dem *PPPoE*-Modus. In Österreich zum Beispiel wird statt des PPPoE-Protokolls das PPTP-Protokoll zur DSL-Anbindung verwendet.

(PPTP ist das Protokoll, das ursprünglich von Microsoft für VPN-Verbindungen benutzt worden ist.)

Wird der mGuard im *PPTP*-Modus betrieben, muss bei lokal angeschlossenen Rechnern der mGuard als Standard-Gateway festgelegt sein.

Dass heißt, dass bei diesen Rechnern die IP-Adresse des LAN-Ports des mGuards als Standard-Gateway anzugeben ist.

Wird der mGuard im *PPTP*-Modus betrieben, sollte NAT aktiviert werden, um aus dem lokalen Netz heraus Zugriff auf das Internet zu erhalten (siehe „Netzwerk >> NAT“ auf Seite 6-107).

Ist NAT nicht aktiviert, können eventuell nur VPN-Verbindungen genutzt werden.

Für die weitere Konfiguration des Netzwerk-Modus *PPTP* siehe „Netzwerk-Modus: Router, Router-Modus = PPTP“ auf Seite 6-87.

Router-Modus: Modem

Nur bei *mGuard industrial rs* **ohne** eingebautes Modem, *mGuard rs4000/2000*, mGuard centerport, *mGuard blade, mGuard delta,* mGuard delta[2], *EAGLE mGuard*

Wird der Netzwerk-Modus *Modem* gewählt, wird die externe Ethernet-Schnittstelle des mGuards deaktiviert, und der Datenverkehr vom und zum WAN läuft über die von außen zugängliche serielle Schnittstelle (Serial Port) des mGuards.

An den Serial Port wird ein externes Modem angeschlossen, das die Verbindung ins Telefonnetz herstellt. Die Anbindung an WAN oder das Internet erfolgt dann (per externem Modem) über das Telefonnetz.

Wenn Sie die Adresse des mGuards ändern (z. B. durch Wechsel des Netzwerk-Modus von *Stealth* auf *Router*), dann ist das Gerät nur noch unter der neuen Adresse zu erreichen. Erfolgte die Änderung der Konfiguration über den LAN-Port, so erhalten Sie eine Rückmeldung über die neue Adresse, bevor die Änderung aktiv wird. Bei Konfigurationsänderungen über den WAN-Port erhalten Sie keine Rückmeldung.

Wenn Sie den Modus auf *Router* oder *PPPoE* oder *PPTP* stellen und dann die IP-Adresse des LAN-Ports und/oder die lokale Netzmaske ändern, achten Sie unbedingt darauf, dass Sie korrekte Werte angeben. Sonst ist der mGuard unter Umständen nicht mehr erreichbar.

Für die weitere Konfiguration des Netzwerk-Modus *Eingebautes Modem / Modem* siehe „Netzwerk-Modus = Router, Router-Modus = Modem / Eingebautes Modem“ auf Seite 6-88.

Router-Modus: Eingebautes Modem

Nur bei *mGuard industrial rs* **mit** eingebautem Modem oder ISDN-Terminaladapter

Wird der Netzwerk-Modus *Eingebautes Modem* gewählt, wird die externe Ethernet-Schnittstelle des mGuards deaktiviert, und der Datenverkehr vom und zum WAN läuft über das im mGuard eingebaute Modem bzw. den eingebauten ISDN-Terminaladapter. Dieses bzw. dieser muss am Telefonnetz angeschlossen sein. Die Anbindung ans Internet erfolgt dann über das Telefonnetz.

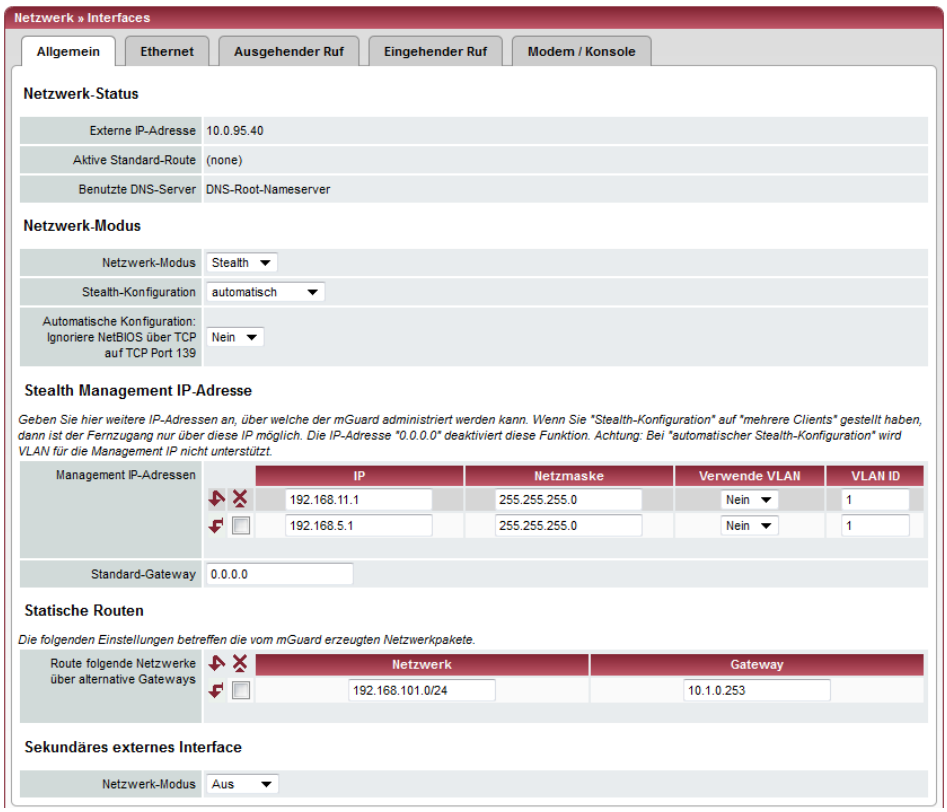
Nach Auswahl von *Eingebautes Modem* werden die Felder zur Festlegung der Parameter für eine Modemverbindung eingeblendet.

Für die weitere Konfiguration des Netzwerk-Modus *Eingebautes Modem / Modem* (siehe „Netzwerk-Modus = Router, Router-Modus = Modem / Eingebautes Modem“ auf Seite 6-88).

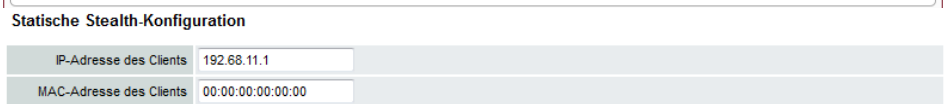
Netzwerk-Modus: Stealth

Werkseinstellung mGuard rs4000/rs2000, mGuard industrial rs, mGuard smart², mGuard pci² SD, mGuard pci, mGuard delta², EAGLE mGuard

Wenn als Netzwerk-Modus „Stealth“ ausgewählt ist ...



... und für Stealth-Konfiguration „statisch“



Netzwerk >> Interfaces >> Allgemein (Netzwerk-Modus = „Stealth“)

Netzwerk-Modus

Gilt nur, wenn als Netzwerk-Modus „Stealth“ ausgewählt ist.

Stealth-Konfiguration — **automatisch / statisch / mehrere Clients**

automatisch

Der mGuard analysiert den Netzwerkverkehr, der über ihn läuft, und konfiguriert dementsprechend seine Netzwerkanbindung eigenständig. Er arbeitet transparent.

Netzwerk >> Interfaces >> Allgemein (Netzwerk-Modus = „Stealth“) [...]		
		statisch Wenn der mGuard keinen über ihn laufenden Netzwerkverkehr analysieren kann, z. B. weil zum lokal angeschlossenen Rechner nur Daten ein-, aber nicht ausgehen, dann muss die *Stealth-Konfiguration* auf **statisch** gesetzt werden. In diesem Fall stellt die Seite unten weitere Eingabefelder zur statischen Stealth-Konfiguration zur Verfügung. **mehrere Clients** (Standard) Wie bei **automatisch**, es können jedoch mehr als nur ein Rechner am LAN-Port (gesicherter Port) des mGuards angeschlossen sein und somit mehrere IP-Adressen am LAN-Port (gesicherter Port) des mGuards verwendet werden.
	Automatische Konfiguration: Ignoriere NetBIOS über TCP auf TCP-Port 139:	**Nein / Ja** Nur bei automatischer Stealth-Konfiguration: Hat ein Windows-Rechner mehr als eine Netzwerkkarte installiert, kann es vorkommen, dass er in den von ihm ausgehenden Datenpaketen abwechselnd unterschiedliche IP-Adressen als Absenderadresse benutzt. Das betrifft Netzwerkpakete, die der Rechner an den TCP-Port 139 (NetBIOS) sendet. Da der mGuard aus der Absenderadresse die Adresse des Rechners ermittelt (und damit die Adresse, unter der der mGuard erreichbar ist), müsste der mGuard entsprechend hin- und herschalten, was den Betrieb erheblich stören würde. Um das zu verhindern, setzen Sie diesen Schalter auf **Ja**, sofern Sie den mGuard an einem Rechner angeschlossen haben, der diese Eigenarten aufweist.

Netzwerk >> Interfaces >> Allgemein (Netzwerk-Modus = „Stealth“) [...]

Stealth Management IP-Adresse

Hier können Sie eine weitere IP-Adresse angeben, über welche der mGuard administriert werden kann.

Wenn

– unter *Stealth-Konfiguration* die Option **mehrere Clients** gewählt ist oder
– der Client ARP-Anfragen nicht beantwortet oder
– kein Client vorhanden ist,

dann ist der Fernzugang über HTTPS, SNMP und SSH **nur** über diese Adresse möglich.

Bei *statischer* Stealth-Konfiguration kann die *Stealth Management IP-Adresse* immer erreicht werden, auch wenn der Client-PC seine Netzwerkkarte nicht aktiviert hat.

Ist das sekundäre externe Interface aktiviert (siehe „Sekundäres externes Interface“ auf Seite 6-75) gilt Folgendes:

Sind die Routing-Einstellungen in der Weise in Kraft, dass der Datenverkehr zur **Stealth Management IP-Adresse** über das sekundäre externe Interface geroutet würde, wäre damit eine Ausschlusssituation gegeben, d. h. der mGuard wäre nicht mehr lokal administrierbar.

Um das zu verhindern hat der mGuard einen Mechanismus eingebaut, der dafür sorgt, dass in einem solchen Fall die Stealth Management IP-Adresse vom lokal angeschlossenem Rechner (oder Netz) erreichbar bleibt.

Netzwerk >> Interfaces >> Allgemein (Netzwerk-Modus = „Stealth“) [...]		
	Management IP-Adressen	**IP** IP-Adresse, unter welcher der mGuard erreichbar und administrierbar sein soll. Die IP-Adresse „0.0.0.0“ deaktiviert die Management IP-Adresse. Ändern Sie zuerst die Management IP-Adresse, bevor Sie zusätzliche Adressen angeben. **Netzmaske** Die Netzmaske zu obiger IP-Adresse. **Verwende VLAN: Ja / Nein** IP-Adresse und Netzmaske des VLAN-Ports. Wenn die IP-Adresse innerhalb eines VLANs liegen soll, setzen Sie diese Option auf **Ja**. **VLAN-ID** – Eine VLAN-ID zwischen 1 und 4095. – Eine Erläuterung finden Sie unter „VLAN“ auf Seite 9-8. – Falls Sie Einträge aus der Liste löschen wollen: Der erste Eintrag kann nicht gelöscht werden. Im Multi-Stealth-Mode kann der externe DHCP-Server des mGuards nicht genutzt werden, wenn eine VLAN ID als Management IP zugewiesen ist.
	Standard-Gateway	Das Standard-Gateway des Netzes, in dem sich der mGuard befindet.
Statische Routen	In den Stealth-Modi „automatisch“ und „statisch“ übernimmt der mGuard das Standard-Gateway des Rechners, der an seinen LAN-Port angeschlossen ist. Dies gilt nicht, wenn eine Management IP-Adresse mit Standard-Gateway konfiguriert ist. Für Datenpakete ins WAN, die der mGuard selber erzeugt, können alternative Routen festgelegt werden. Dazu gehören u. a. die Pakete folgender Datenverkehre: – das Herunterladen von Zertifikats-Sperrlisten (CRL) – das Herunterladen einer neuen Konfiguration – die Kommunikation mit einem NTP-Server (zur Zeit-Synchronisation) – das Versenden und Empfangen verschlüsselter Datenpakete von VPN-Verbindungen – Anfragen an DNS-Server – Syslog-Meldungen – das Herunterladen von Firmware-Updates – das Herunterladen von Konfigurationsprofilen von einem zentralen Server (sofern konfiguriert) – SNMP-Traps	

Netzwerk >> Interfaces >> Allgemein (Netzwerk-Modus = „Stealth“) [...]

Soll diese Option genutzt werden, machen Sie nachfolgend die entsprechenden Angaben. Wird sie nicht genutzt, werden die betreffenden Datenpakete über das beim Client festgelegte Standard-Gateway geleitet.

Netzwerk	Das Netzwerk in CIDR-Schreibweise angeben (siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 6-261).
Gateway	Das Gateway, über welches dieses Netzwerk erreicht werden kann. Die hier festgelegten Routen gelten für Datenpakete, die der mGuard selber erzeugt, als unbedingte Routen. Diese Festlegung hat Vorrang vor sonstigen Einstellungen (siehe auch „Netzwerk-Beispielskizze“ auf Seite 6-262).

Statische Stealth-Konfiguration

IP-Adresse des Clients	Die IP-Adresse des am LAN-Port angeschlossenen Rechner.
MAC-Adresse des Clients	Das ist die physikalische Adresse der Netzwerkkarte des lokalen Rechners, an dem der mGuard angeschlossen ist. • Die MAC-Adresse ermitteln Sie wie folgt: Auf der DOS-Ebene (Menü Start, Alle Programme, Zubehör, Eingabeaufforderung) folgenden Befehl eingeben: ***ipconfig /all***

Die Angabe der MAC-Adresse ist nicht unbedingt erforderlich. Denn der mGuard kann die MAC-Adresse automatisch vom Client erfragen. Hierfür muss die MAC-Adresse 0:0:0:0:0:0 eingestellt werden. Zu beachten ist, dass der mGuard aber erst dann Netzwerkpakete zum Client hindurchleiten kann, nachdem er die MAC-Adresse vom Client ermitteln konnte.

Ist im statischen Stealth-Modus weder eine *Stealth Management IP-Adresse* noch die *MAC-Adresse des Clients* konfiguriert, werden DAD ARP Anfragen auf dem internen Interface versendet (siehe RFC2131, Abschnitt 4.4.1)

Sekundäres externes Interface

Dieser Menüpunkt gehört nicht zum Funktionsumfang vom mGuard rs2000.

Nur bei Netzwerk-Modus *Router* **mit** Router-Modus *Statisch* oder Netzwerk-Modus *Stealth*.

Nur bei *mGuard rs4000, mGuard centerport*, *mGuard industrial rs*, *mGuard blade, EAGLE mGuard, mGuard delta*:

In diesen Netzwerk-Modi kann die serielle Schnittstelle des mGuards als zusätzliches **sekundäres externes Interface** konfiguriert werden.

Über das sekundäre externe Interface kann *permanent* oder *aushilfsweise* Datenverkehr ins externe Netz (WAN) geführt werden.

Bei aktiviertem sekundärem externen Interface gilt Folgendes:

Netzwerk >> Interfaces >> Allgemein (Netzwerk-Modus = „Stealth“) [...]

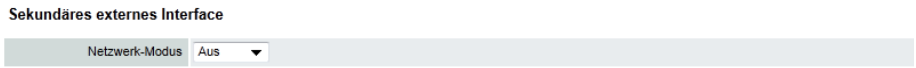
Im Netzwerk-Modus *Stealth*

Nur der vom mGuard erzeugte Datenverkehr wird dem Routing unterzogen, das für das sekundäre externe Interface festgelegt ist, nicht der Datenverkehr, der von einem lokal angeschlossenem Rechner ausgeht. Auch kann auf lokal angeschlossene Rechner nicht von entfernt zugegriffen werden, nur ein Fernzugriff auf den mGuard selber ist - bei entsprechender Konfiguration - möglich.

VPN-Datenverkehr kann - wie im Netzwerk-Modus Router - von und zu den lokal angeschlossenen Rechnern fließen. Denn dieser wird vom mGuard verschlüsselt und gilt daher als vom mGuard erzeugt.

Im Netzwerk-Modus *Router*

Alle Datenverkehre, also die von und zu lokal angeschlossenen Rechnern und die, welche vom mGuard erzeugt werden, können über das sekundäre externe Interface ins externe Netz (WAN) geführt werden.



Netzwerk-Modus: Aus / Modem

Aus

(Standard). Wählen Sie diese Einstellung, wenn die Betriebsumgebung des mGuards kein sekundäres externes Interface braucht. Dann können Sie die serielle Schnittstelle (oder das eingebaute Modem - falls vorhanden) für andere Zwecke nutzen (siehe „Modem / Konsole“ auf Seite 6-100).

Modem/Eingebautes Modem

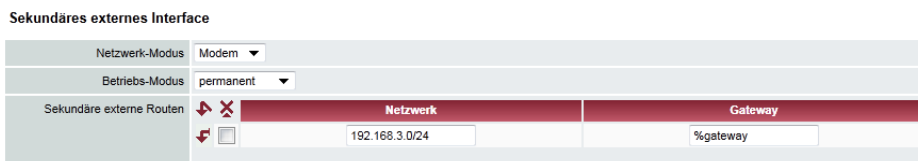
Bei Auswahl einer dieser Optionen wird der Datenverkehr ins externe Netz (WAN) über das sekundäre externe Interface geführt, entweder *permanent* oder *aushilfsweise*.

Das sekundäre externe Interface wird über die serielle Schnittstelle des mGuards und ein daran angeschlossenes externes Modem gebildet.

Betriebs-Modus

permanent / aushilfsweise

Nach Auswahl des Netzwerk-Modus *Modem* oder *Eingebautes Modem* für das sekundäre externe Interface muss der Betriebs-Modus des sekundären externen Interface festgelegt werden.



Netzwerk >> Interfaces >> Allgemein (Netzwerk-Modus = „Stealth“) [...]

	permanent Datenpakete, deren Ziel den Routing-Einstellungen entspricht, die für das sekundäre externe Interface festgelegt sind, werden immer über dieses externe Interface geleitet. Das sekundäre externe Interface ist immer aktiviert. **aushilfsweise** Datenpakete, deren Ziel den Routing-Einstellungen entspricht, die für das sekundäre externe Interface festgelegt sind, werden nur dann über dieses externe Interface geleitet, wenn zusätzlich weitere zu definierende Bedingungen erfüllt werden. Nur dann wird das sekundäre externe Interface aktiviert, und die Routing-Einstellungen für das sekundäre externe Interface treten in Kraft (siehe „Tests zur Aktivierung“ auf Seite 6-79).
Sekundäre externe Routen	**Netzwerk** Machen Sie hier die Angabe für das Routing zum externen Netzwerk. Sie können mehre Routing-Angaben machen. Datenpakete, die für diese Netze bestimmt sind, werden dann über das sekundäre externe Interface zum entsprechenden Netz - *permanent* oder *aushilfsweise* - geleitet. Gateway Geben Sie hier die IP-Adresse des Gateways an, über das die Vermittlung in das vorgenannte externe Netzwerk erfolgt - sofern diese IP-Adresse bekannt ist. Bei Einwahl ins Internet über die Telefonnummer des Internet Service Providers wird die Adresse des Gateways normalerweise erst nach Einwahl bekannt. In diesem Fall ist **%gateway** als Platzhalter in das Feld einzutragen.

Betriebs-Modus: permanent/aushilfsweise

Sowohl in der Betriebsart **permanent** als auch in der Betriebsart **aushilfsweise** muss dem mGuard für das sekundäre externe Interface das Modem zur Verfügung stehen, damit der mGuard über das am Modem angeschlossene Telefonnetz eine Verbindung zum WAN (Internet) herstellen kann.

Welche Datenpakete über das **primäre externe Interface** (Ethernet-Schnittstelle) und welche Datenpakete über das **sekundäre externe Interface** gehen, entscheiden die Routing-Einstellungen, die für diese beiden externen Interfaces in Kraft sind. Ein Datenpaket kann also grundsätzlich nur das Interface nehmen, dessen Routing-Einstellung für das vom Datenpaket angesteuerte Ziel passend ist.

Für die Anwendung von Routing-Angaben gelten folgende Regeln:

Sind mehrere Routing-Angaben für des Ziel eines Datenpaketes passend, entscheidet das kleinste in den Routing-Angaben definierte Netz, das auf ein Datenpaket-Ziel passt, welche Route dieses Paket nimmt.

Beispiel:

- Die externe Route des **primären** externen Interface ist z. B. mit 10.0.0.0/8 angegeben, die externe Route des **sekundären** externen Interface mit 10.1.7.0/24. Dann werden Datenpakete zum Netz 10.1.7.0/24 über das sekundäre externe Interface geleitet, obwohl für sie die Routing-Angabe für das primäre externe Interface auch passt. Begründung: Die Routing-Angabe für das sekundäre externe Interface bezeichnet ein kleineres Netz (10.1.7.0/24 < 10.0.0.0/8).
- (Diese Regel gilt nicht im Netzwerk-Modus *Stealth* in Bezug auf die Stealth Management IP-Adresse (siehe Hinweis unter „Stealth Management IP-Adresse“ auf Seite 6-73).
- Sind die Routing-Angaben für das primäre und das sekundäre externe Interface identisch, dann „gewinnt“ das sekundäre externe Interface, d. h. die Datenpakete mit passender Zieladresse werden über das sekundäre externe Interface geleitet.
- Die Routing-Einstellungen für das sekundäre externe Interface treten nur dann in Kraft, wenn das sekundäre externe Interface aktiviert ist. Das ist insbesondere dann zu berücksichtigen, wenn die Routing-Angaben für des primäre und das sekundäre externe Interface sich überschneiden oder gleich sind und durch die Priorität des sekundären externen Interface eine Filterwirkung mit folgendem Effekt erzielt wird: Datenpakete, die aufgrund ihres Zieles sowohl für das primäre als auch das sekundäre externe Interface passen, gehen auf jeden Fall über das sekundäre externe Interface, aber nur, wenn dieses aktiviert ist.
- „Aktiviert“ bedeutet im Betriebs-Modus **aushilfsweise** Folgendes: Nur wenn bestimmte Bedingungen erfüllt werden, wird das sekundäre externe Interface aktiviert, und erst dann wirken sich die Routing-Einstellungen des sekundären externen Interface aus.
- Die Netzwerkadresse 0.0.0.0/0 bezeichnet generell das größte definierbare Netz, also das Internet

Im Netzwerk-Modus Router kann das lokale Netz, das am mGuard angeschlossen ist, über das sekundäre externe Interface erreicht werden, sofern die Firewall-Einstellungen so festgelegt sind, dass sie das zulassen.

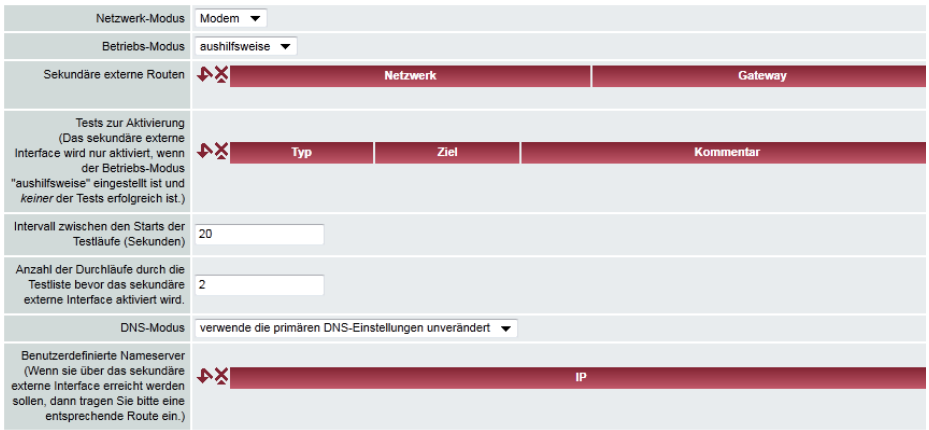
Fortsetzung Netzwerk >> Interfaces >> Allgemein; Fortsetzung Sekundäres externes Interface

Sekundäres externes Interface (Fortsetzung)

Netzwerk-Modus = Modem

Betrieb-Modus = aushilfsweise

Tests zur Aktivierung



Ist der Betriebs-Modus des sekundären externen Interface auf **aushilfsweise** gestellt, dann wird durch periodisch durchgeführte Ping-Tests Folgendes überprüft: Ist ein bestimmtes Ziel oder sind bestimmte Ziele erreichbar, wenn Datenpakete dorthin ihren Weg aufgrund aller für den mGuard festgelegten Routing-Einstellungen - außer der für das sekundäre externe Interface - nehmen? Nur wenn **keiner** der Ping-Tests erfolgreich ist, geht der mGuard davon aus, dass es zurzeit nicht möglich ist, das/die Ziel(e) über das primäre externe Interface (= Ethernet-Schnittstelle oder WAN-Port des mGuards) zu erreichen. In diesem Fall wird das sekundäre externe Interface aktiviert, so dass - bei entsprechender Routing-Einstellung für das sekundäre externe Interface - die Datenpakete über dieses Interface geleitet werden.

Das sekundäre externe Interface bleibt so lange aktiviert, bis bei nachfolgenden Ping-Tests der mGuard ermittelt, dass das bzw. die Ziel(e) wieder erreichbar sind. Wird diese Bedingung erfüllt, werden die Datenpakete wieder über das **primäre** externe Interface geleitet und das **sekundäre** externe Interface wird deaktiviert.

Die fortlaufend durchgeführten Ping-Tests dienen also dazu zu überprüfen, ob bestimmte Ziele über das primäre externe Interface erreichbar sind. Bei Nichterreichbarkeit wird das sekundäre externe Interface für die Dauer der Nichterreichbarkeit aktiviert.

Typ / Ziel

Legen Sie den Ping-**Typ** des Ping-Request-Pakets fest, das der mGuard zum Gerät mit der IP-Adresse aussenden soll, die Sie unter **Ziel** angeben.

Sie können mehrere solcher Ping-Tests auch zu unterschiedlichen Zielen konfigurieren.

Erfolg / Misserfolg:

Ein Ping-Test gilt dann als erfolgreich absolviert, wenn der mGuard innerhalb von 4 Sekunden eine positive Reaktion auf das ausgesandte Ping-Request Paket erhält. Bei einer positiven Reaktion gilt die Gegenstelle als erreichbar.

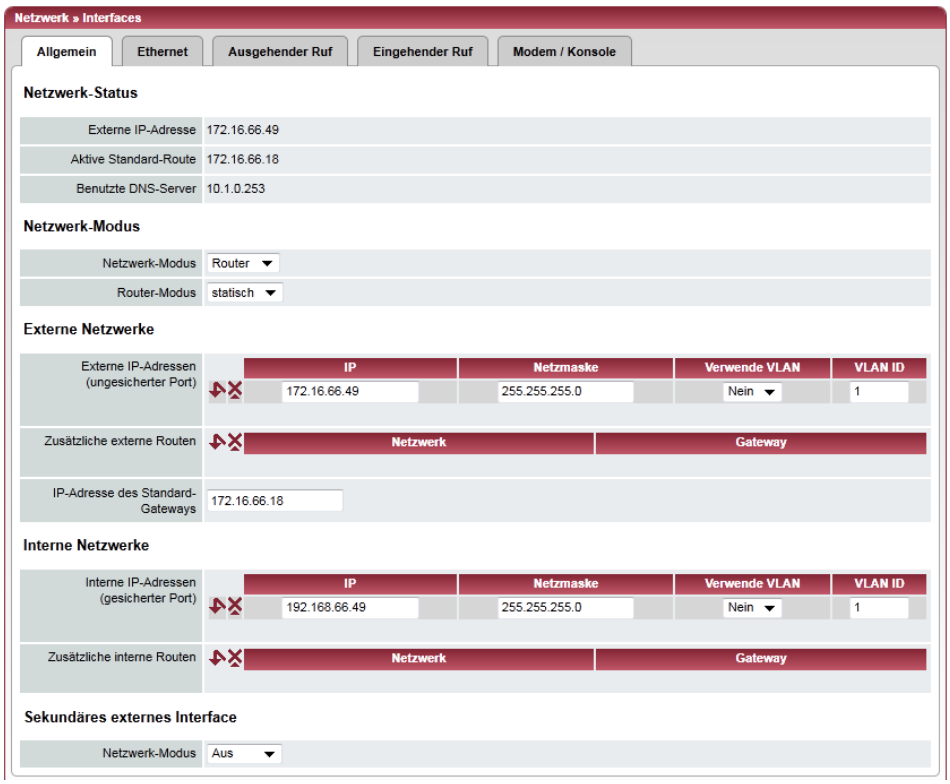
Fortsetzung Netzwerk >> Interfaces >> Allgemein; Fortsetzung Sekundäres externes Interface

	Ping-Typen: – IKE-Ping: Ermittelt, ob unter der angegebenen IP-Adresse ein VPN-Gateway erreichbar ist. – ICMP-Ping: Ermittelt, ob unter der angegebenen IP-Adresse ein Gerät erreichbar ist. Der gebräuchlichste Ping-Test. Die Reaktion auf solche Ping-Tests ist bei manchen Geräten aber ausgeschaltet, so dass sie nicht reagieren, obwohl sie erreichbar sind. – DNS-Ping: Ermittelt, ob unter der angegebenen IP-Adresse ein funktionierender DNS-Server erreichbar ist. An den DNS-Server mit der angegebenen IP-Adresse wird eine generische Anfrage gerichtet, auf die jeder DNS-Server - sofern erreichbar - eine Antwort gibt. Bei der Programmierung von Ping-Tests ist Folgendes zu beachten: Es ist sinnvoll, mehrere Ping-Tests zu programmieren. Denn es könnte sein, dass ein einzelner getesteter Dienst gerade gewartet wird. Solch ein Fall sollte nicht die Auswirkung haben, dass das sekundäre externe Interface aktiviert und eine Kosten verursachende Wählverbindung über das Telefonnetz hergestellt wird. Da durch die Ping-Tests Netzwerkverkehr erzeugt wird, sollte deren Anzahl und die Häufigkeit ihrer Durchführung angemessen festgelegt werden. Auch sollte vermieden werden, dass das sekundäre externe Interface zu frühzeitig aktiviert wird. Bei den einzelnen Ping-Requests gilt eine Timeout-Zeit von 4 Sekunden. Das bedeutet, dass nach dem Starten eines Ping-Tests der nächste Ping-Test nach 4 Sekunden startet, wenn der vorige negativ war. Zur Berücksichtigung dieser Aspekte nehmen Sie die nachfolgenden Einstellungen vor.
Intervall zwischen den Starts der Testläufe (Sekunden)	Die oben unter **Tests zur Aktivierung...** definierten Ping-Tests werden nacheinander durchgeführt. Die einmalige sequentielle Durchführung der definierten Ping-Tests wird als *Testlauf* bezeichnet. Testläufe werden in Zeitabständen kontinuierlich wiederholt. Das in diesem Feld angegebene Intervall gibt an, wie lange der mGuard nach dem Start eines Testlaufs abwartet, um den nächsten Testlauf zu starten. Die Testläufe werden nicht unbedingt vollständig abgearbeitet: Sobald ein Ping-Test eines Testlaufs erfolgreich ist, werden die folgenden Ping-Tests desselben Testlaufs ausgelassen. Dauert ein Testlauf länger als das festgelegte Intervall, dann wird der nächste Testlauf direkt im Anschluss gestartet.

Fortsetzung Netzwerk >> Interfaces >> Allgemein; Fortsetzung Sekundäres externes Interface	
Anzahl der Durchläufe durch die Testliste, bevor das sekundäre externe Interface aktiviert wird	Gibt an, wie viele nacheinander durchgeführte Testläufe mit negativem Ausgang es geben muss, damit der mGuard das sekundäre externe Interface aktiviert. Ein Testlauf hat dann einen negativen Ausgang, wenn **keiner** der darin enthaltenen Ping-Tests erfolgreich war. Die hier festgelegte Anzahl gibt auch an, wie oft nach Aktivierung des sekundären externen Interface die Testläufe in Folge erfolgreich sein müssen, damit es wieder deaktiviert wird.
DNS-Modus	Nur relevant bei aktiviertem sekundären externem Interface im Betriebs-Modus **aushilfsweise**: Der hier ausgewählte DNS-Modus legt fest, welche DNS-Server der mGuard verwendet für aushilfsweise herzustellende Verbindungen über das sekundäre externe Interface. – Verwende die primären DNS-Einstellungen unverändert – DNS-Root-Nameserver – Provider definiert (via PPP-Auswahl) – Benutzerdefiniert (unten stehende Liste) **Verwende die primären DNS-Einstellungen unverändert** Es werden die DNS-Server benutzt, welche unter Netzwerk --> DNS-Server (siehe „Netzwerk >> NAT“ auf Seite 6-107) definiert sind. **DNS-Root-Nameserver** Anfragen werden an die Root-Nameserver im Internet gerichtet, deren IP-Adressen im mGuard gespeichert sind. Diese Adressen ändern sich selten. **Provider definiert (via PPP-Auswahl)** Es werden die Domain Name Server des Internet Service Providers benutzt, der den Zugang zum Internet zur Verfügung stellt. **Benutzerdefiniert (unten stehende Liste)** Ist diese Einstellung gewählt, nimmt der mGuard mit den Domain Name Servern Verbindung auf, die in der nachfolgenden Liste *Benutzerdefinierte Nameserver* aufgeführt sind.
Benutzer definierte Nameserver	In dieser Liste können Sie die IP-Adressen von Domain Name Servern erfassen. Diese benutzt der mGuard bei der Kommunikation über das sekundäre externe Interface - sofern dieses aushilfsweise aktiviert ist und der **DNS-Modus** (s. o.) für diesen Fall mit *Benutzerdefiniert* angegeben ist.

Netzwerk-Modus: Router

Werkseinstellung mGuard centerport, mGuard delta und mGuard blade-Controller

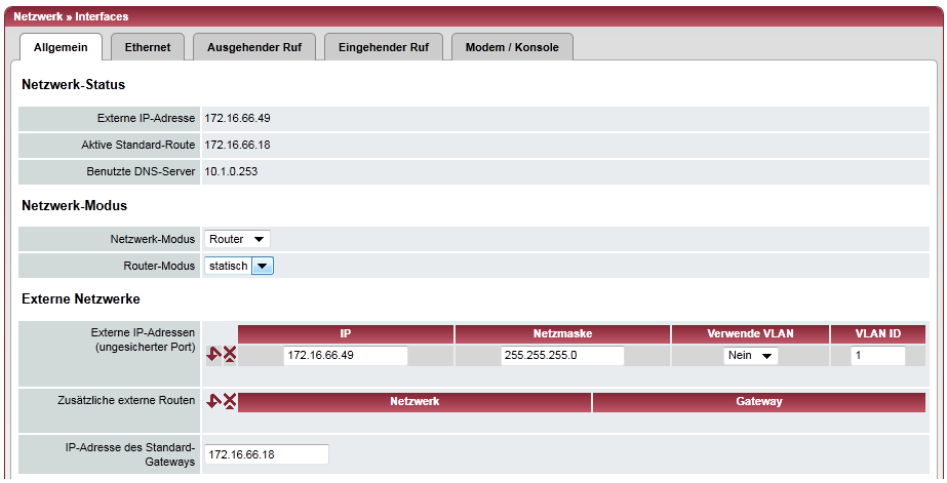


Wenn als Netzwerk-Modus „Router“ und Router-Modus „statisch“ ausgewählt ist (siehe Seite 6-84)

Netzwerk >> Interfaces >> Allgemein (Netzwerk-Modus = „Router“)		
Interne Netzwerke	**Interne IP-Adressen (gesicherter Port)**	Interne IP ist die IP-Adresse, unter der der mGuard von Geräten des lokal angeschlossenen Netzes erreichbar ist. Im **Router**-/**PPPoE**-/**PPTP**-/**Modem**-Modus ist werkseitig voreingestellt: – IP-Adresse: **192.168.1.1** – Netzmaske: **255.255.255.0** Sie können weitere Adressen festlegen, unter der der mGuard von Geräten des lokal angeschlossenen Netzes angesprochen werden kann. Das ist zum Beispiel dann hilfreich, wenn das lokal angeschlossene Netz in Subnetze unterteilt wird. Dann können mehrere Geräte aus verschiedenen Subnetzen den mGuard unter unterschiedlichen Adressen erreichen.
	IP	IP-Adresse, unter welcher der mGuard über seinen LAN-Port erreichbar sein soll.
	Netzmaske	Die Netzmaske des am LAN-Port angeschlossenen Netzes.
	Verwende VLAN	Wenn die IP-Adresse innerhalb eines VLANs liegen soll, ist diese Option auf **Ja** zu setzen.

Netzwerk >> Interfaces >> Allgemein (Netzwerk-Modus = „Router“)[...]		
	VLAN-ID	– Eine VLAN-ID zwischen 1 und 4095. – Eine Erläuterung des Begriffes „VLAN“ befindet sich im Glossar auf 9-8. – Falls Sie Einträge aus der Liste löschen wollen: Der erste Eintrag kann nicht gelöscht werden.
	Zusätzliche interne Routen	Sind am lokal angeschlossen Netz weitere Subnetze angeschlossen, können Sie zusätzliche Routen definieren.
	Netzwerk	Das Netzwerk in CIDR-Schreibweise angeben (siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 6-261)
	Gateway	Das Gateway, über welches dieses Netzwerk erreicht werden kann. Siehe auch „Netzwerk-Beispielskizze“ auf Seite 6-262
Sekundäres externes Interface	Siehe „Sekundäres externes Interface“ auf Seite 6-75	

Netzwerk-Modus = Router, Router-Modus = statisch



Netzwerk >> Interfaces >> Allgemein (Netzwerk-Modus = „Router“, Router-Modus = „statisch“)		
Externe Netzwerke	**Externe IPs (ungesicherter Port)**	Die Adressen, unter denen der mGuard von Geräten erreichbar ist, die sich auf Seiten des WAN-Ports befinden. Findet hier der Übergang zum Internet statt, wird die externe IP-Adresse des mGuards vom Internet Service Provider (ISP) vorgegeben. **IP/Netzmaske** – IP-Adresse und Netzmaske des WAN-Ports. **Verwende VLAN: Ja / Nein** – Wenn die IP-Adresse innerhalb eines VLANs liegen soll, ist diese Option auf **Ja** zu setzen. **VLAN-ID** – Eine VLAN-ID zwischen 1 und 4095. – Eine Erläuterung finden Sie unter „VLAN“ auf Seite 9-8. – Falls Sie Einträge aus der Liste löschen wollen: Der erste Eintrag kann nicht gelöscht werden.
	Zusätzliche externe Routen	Zusätzlich zur Standard-Route über das unten angegebene Standard-Gateway können Sie weitere externe Routen festlegen. **Netzwerk / Gateway** (Siehe „Netzwerk-Beispielskizze“ auf Seite 6-262)

Netzwerk >> Interfaces >> Allgemein (Netzwerk-Modus = „Router“, Router-Modus = „statisch“)	
	IP-Adresse des Standard-Gateways Hier kann die IP-Adresse eines Gerätes im lokalen Netz (angeschlossen am LAN-Port) oder die IP-Adresse eines Gerätes im externen Netz (angeschlossen am WAN-Port) angegeben werden. Wenn der mGuard den Übergang zum Internet herstellt, wird diese IP-Adresse vom Internet Service Provider (ISP) vorgegeben. Wird der mGuard innerhalb des LANs eingesetzt, wird die IP-Adresse des Standard-Gateways vom Netzwerk-Administrator vorgegeben. Wenn das lokale Netz dem externen Router nicht bekannt ist, z. B. im Falle einer Konfiguration per DHCP, dann sollten Sie unterNetzwerk >> NAT Ihr lokales Netz angeben (siehe Seite 6-107).
Interne Netzwerke	Siehe „Interne Netzwerke“ auf Seite 6-82.
Sekundäres externes Interface	Siehe „Sekundäres externes Interface“ auf Seite 6-75

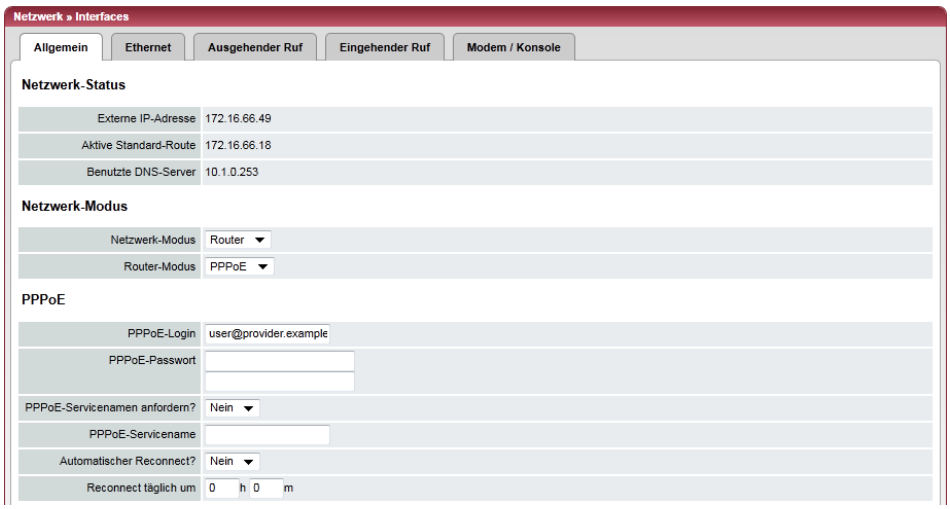
Netzwerk-Modus = Router, Router-Modus = DHCP

Es gibt bei Netzwerk-Modus = Router, Router-Modus = „DHCP“ keine zusätzlichen Einstellmöglichkeiten.

Netzwerk >> Interfaces >> Allgemein (Netzwerk-Modus = „Router“, Router-Modus = „DHCP“)	
Interne Netzwerke	Siehe „Interne Netzwerke“ auf Seite 6-82.
Sekundäres externes Interface	Siehe „Sekundäres externes Interface“ auf Seite 6-75

Netzwerk-Modus = Router, Router-Modus = PPPoE

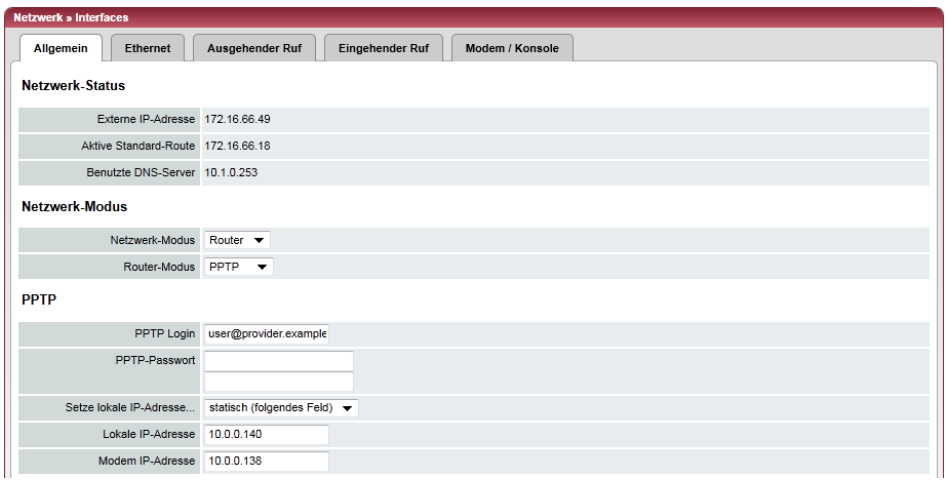
Wenn als Netzwerk-Modus Router und als Router-Modus „PPPoE“ ausgewählt ist



Netzwerk >> Interfaces >> Allgemein (Netzwerk-Modus = Router, Router-Modus = „PPPoE“)		
PPPoE	**Für Zugriffe ins Internet gibt der Internet Service Provider (ISP) dem Benutzer einen Benutzernamen (Login) und ein Passwort. Diese werden abfragt, wenn Sie eine Verbindung ins Internet herstellen wollen.**	
	PPPoE-Login	Benutzername (Login), den der Internet Service Provider (ISP) anzugeben fordert, wenn Sie eine Verbindung ins Internet herstellen wollen.
	PPPoE-Passwort	Passwort, das der Internet Service Provider anzugeben fordert, wenn Sie eine Verbindung ins Internet herstellen wollen.
	PPPoE-Servicenamen anfordern?	Bei **Ja** fordert der PPPoE-Client des mGuards den unten genannten Servicenamen beim PPPoE-Server an. Ansonsten wird der PPPoE-Servicename nicht verwendet.
	PPPoE-Servicename	PPPoE-Servicename
	Automatisches Reconnect?	Bei **Ja** geben Sie im nachfolgenden Feld **Reconnect täglich um** die Uhrzeit an. Dieses Feature dient dazu, das von vielen Internet Providern sowieso erzwungene Trennen und Wiederverbinden mit dem Internet in eine Zeit zu legen, wenn es den Geschäftsbetrieb nicht stört. Bei Einschalten dieser Funktion greift diese nur dann, wenn die Synchronisation mit einem Zeit-Server erfolgt ist (siehe „Verwaltung >> Systemeinstellungen“ auf Seite 6-4, „Zeit und Datum“ auf Seite 6-8).
	Reconnect täglich um	Angabe der Uhrzeit, falls *Automatisches Reconnect* (s. o.) stattfindet.
Interne Netzwerke	Siehe „Interne Netzwerke“ auf Seite 6-82.	
Sekundäres externes Interface	Siehe „Sekundäres externes Interface“ auf Seite 6-75	

Netzwerk-Modus: Router, Router-Modus = PPTP

Wenn als Netzwerk-Modus „Router“ und als Router-Modus „PPTP“ ausgewählt ist



Netzwerk >> Interfaces >> Allgemein (Netzwerk-Modus = Router, Router-Modus = „PPTP“)		
PPTP	**Für Zugriffe ins Internet gibt der Internet Service Provider (ISP) dem Benutzer einen Benutzernamen (Login) und ein Passwort. Diese werden abfragt, wenn Sie eine Verbindung ins Internet herstellen wollen.**	
	PPTP-Login	Benutzername (Login), den der Internet Service Provider anzugeben fordert, wenn Sie eine Verbindung ins Internet herstellen wollen.
	PPTP-Passwort	Passwort, das der Internet Service Provider anzugeben fordert, wenn Sie eine Verbindung ins Internet herstellen wollen.
	Setze lokale IP-Adresse...:	**über DHCP:** Werden die Adressdaten für den Zugang zum PPTP-Server vom Internet Service Provider per DHCP geliefert, wählen Sie **über DHCP**. Dann ist kein Eintrag unter **Lokale IP-Adresse** zu machen. **statisch (folgendes Feld):** Werden die Adressdaten für den Zugang zum PPTP-Server **nicht** per DHCP vom Internet Service Provider geliefert, dann muss die lokale IP-Adresse angegeben werden.
	Lokale IP-Adresse	IP-Adresse, unter der der mGuard vom PPTP-Server aus zu erreichen ist.
	Modem IP-Adresse	Das ist die Adresse des PPTP-Servers des Internet Service Providers.
Interne Netzwerke	Siehe „Interne Netzwerke“ auf Seite 6-82.	
Sekundäres externes Interface	Siehe „Sekundäres externes Interface“ auf Seite 6-75	
Dieser Menüpunkt gehört nicht zum Funktionsumfang vom mGuard rs2000.		

Netzwerk-Modus = Router, Router-Modus = Modem / Eingebautes Modem

Nur *mGuard rs4000*, *mGuard centerport*, *mGuard industrial rs*, *mGuard blade,* mGuard delta[2], *mGuard delta, EAGLE mGuard*

Netzwerk >> Interfaces >> Allgemein (Netzwerk-Modus = Router, Router-Modus = „Modem/Eingebautes Modem“)

Modem/Eingebautes Modem

Der Netzwerk-Modus **Modem** ist verfügbar bei:

mGuard centerport, mGuard industrial rs, mGuard blade, EAGLE mGuard, mGuard delta

Der Netzwerk-Modus **Eingebautes Modem** ist zusätzlich verfügbar bei:

mGuard industrial rs, wenn dieser über ein eingebautes Modem oder einen eingebauten ISDN-Terminaladapter verfügt (optional).

Bei allen oben aufgeführten Geräten wird im Netzwerk-Modus *Modem* bzw. *Eingebautes Modem* der Datenverkehr statt über den WAN-Port des mGuards über die serielle Schnittstelle geleitet, und von dort

- A – entweder über die von außen zugängliche serielle Schnittstelle (Serial Port), an die ein externes Modem angeschlossen werden muss
- B – über das eingebaute Modem / den eingebauten ISDN-Terminaladapter (beim mGuard industrial rs, wenn dieser entsprechend ausgestattet ist).

Sowohl bei Möglichkeit A als auch bei B wird per Modem bzw. ISDN-Terminaladapter über das Telefonnetz die Verbindung zum Internet Service Provider und damit ins Internet hergestellt.

Im Netzwerk-Modus *Modem* steht die serielle Schnittstelle des mGuards nicht für die ppp-Einwahloption und nicht für Konfigurationszwecke zur Verfügung (siehe „Modem / Konsole“ auf Seite 6-100).

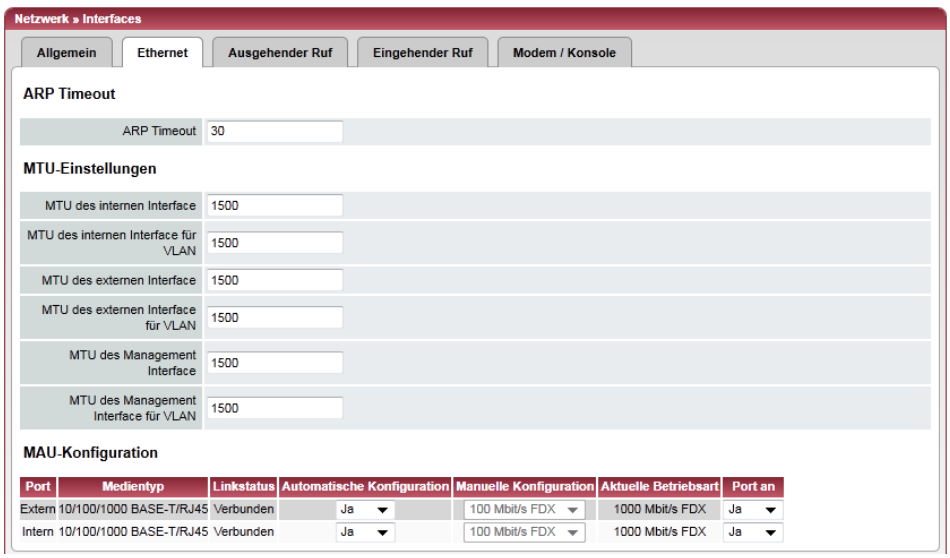
Nach Auswahl des Netzwerk-Modus **Modem**[1] geben Sie auf der Registerkarte **Ausgehender Ruf** und/oder **Eingehender Ruf** die für die Modemverbindung erforderlichen Parameter an (siehe „Ausgehender Ruf“ auf Seite 6-91 und „Eingehender Ruf“ auf Seite 6-97).

Auf der Registerkarte *Modem / Konsole* nehmen Sie Anschlusseinstellungen für ein externes Modem vor (siehe „Modem / Konsole“ auf Seite 6-100).

Die Konfiguration der internen Netzwerke wird im nächsten Abschnitt erklärt.

1 Beim mGuard industrial rs auch **Eingebautes Modem** (nur beim mGuard industrial rs mit eingebautem Modem oder ISDN-Terminaladapter - als Option verfügbar)

6.4.1.2 Ethernet

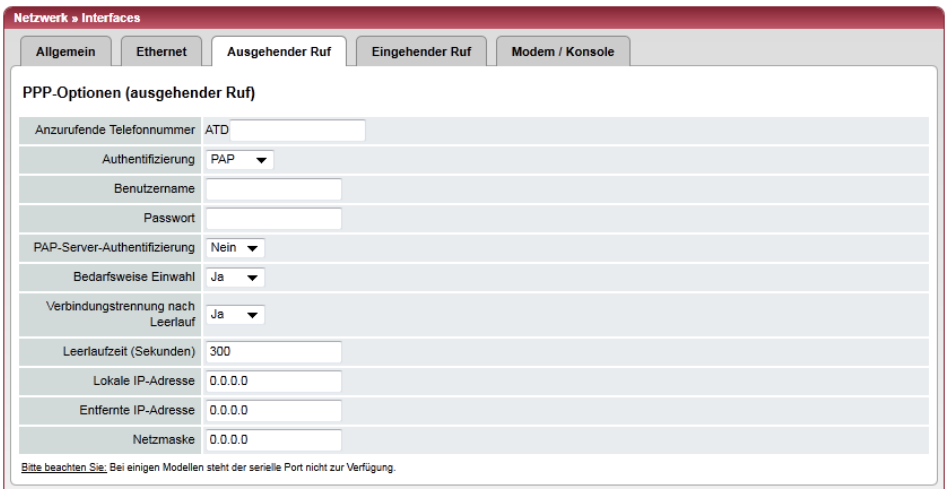


Netzwerk >> Interfaces >> Ethernet		
ARP Timeout	**ARP-Timeout**	Lebensdauer der Einträge in der ARP-Tabelle in Sekunden.
MTU-Einstellungen	**MTU des ... Interface**	Die Maximum Transfer Unit (MTU) beschreibt die maximale IP-Paketlänge, die beim betreffenden Interface benutzt werden darf. Bei VLAN-Interface: Da die VLAN Pakete 4 Byte länger als Pakete ohne VLAN sind, haben bestimmte Treiber Probleme mit der Verarbeitung der größeren Pakete. Eine Reduzierung der MTU auf 1496 kann dieses Problem beseitigen.
MAU-Konfiguration	Konfiguration und Statusanzeige der Ethernetanschlüsse:	
	Port	Name des Ethernetanschlusses, auf welchen sich die Zeile bezieht.
	Medientyp	Medientyp des Ethernetanschlusses.
	Linkstatus	– **Verbunden**: Die Verbindung ist aufgebaut. – **Nicht verbunden**: Die Verbindung ist nicht aufgebaut.

Netzwerk >> Interfaces >> Ethernet	
Automatische Konfiguration	– **Ja**: Versuche die benötigte Betriebsart automatisch zu ermitteln. – **Nein**: Verwende die vorgegebene Betriebsart aus der Spalte „Manuelle Konfiguration“.  Beim Anschluss des EAGLE mGuards an einen Hub ist Folgendes zu beachten: Bei deaktivierter *Automatischer Konfiguration* wird auch die Auto-MDIX-Funktion deaktiviert, d. h. der Port des EAGLE mGuards muss entweder an den Uplink-Port des Hub oder mittels eines Cross-Link-Kabels mit dem Hub verbunden werden.
Manuelle Konfiguration	Die gewünschte Betriebsart, wenn *Automatische Konfiguration* auf *Nein* gestellt ist.
Aktuelle Betriebsart	Die aktuelle Betriebsart des Netzwerkanschlusses.
Port On	**Ja / Nein** Schaltet den Ethernetanschluss auf Ein oder Aus. Die Funktion **Port on** wird **nicht** unterstützt von: – mGuard centerport Die Funktion **Port on** wird mit Einschränkung unterstützt von: – mGuard delta: hier lässt sich die interne Seite (Switch-Ports) nicht abschalten – mGuard pci: hier lässt sich im Treibermodus die interne Netzwerkschnittstelle nicht abschalten (wohl aber im Power-over-PCI-Modus).

6.4.1.3 Ausgehender Ruf

Nur *mGuard rs4000*, *mGuard centerport*, *mGuard industrial rs*, *mGuard blade,* mGuard delta[2], *mGuard delta, EAGLE mGuard*



Netzwerk >> Interfaces >> Ausgehender Ruf

PPP-Optionen (ausgehender Ruf)

Dieser Menüpunkt gehört nicht zum Funktionsumfang vom mGuard rs2000.

Ist nur dann zu konfigurieren, wenn der mGuard

- über das primäre externe Interface (Netzwerk-Modus *Modem* oder *Eingebautes Modem*) **oder**
- über das sekundäre externe Interface (zusätzlich im Netzwerk-Modus *Stealth* oder *Router* verfügbar)

eine Datenverbindung ins WAN (Internet) herstellen können soll (Ausgehender Ruf).

Anzurufende Telefonnummer

Telefonnummer des Internet Service Providers. Nach Herstellung der Telefonverbindung wird darüber die Verbindung ins Internet hergestellt.

Befehlssyntax:

Zusammen mit dem bereits vorangestellten Modemkommando ATD zum Wählen ergibt sich für das angeschlossene Modem z. B. folgende Wählsequenz: ATD765432

Standardmäßig wird das kompatiblere Pulswahlverfahren benutzt, das auf jeden Fall funktioniert.

Es können Wählsonderzeichen in die Wählsequenz aufgenommen werden.

Netzwerk >> Interfaces >> Ausgehender Ruf [...]

HAYES-Wählsonderzeichen

– **W :** Weist das Modem an, an dieser Stelle eine Wählpause einzulegen, bis das Freizeichen zu hören ist.

  Wird verwendet, wenn das Modem an einer Nebenstellenanlage angeschlossen ist, bei der für Anrufe „nach draußen“ mit einer bestimmten Nummer (z. B. 0) zunächst das externe Festnetz (das Amt) geholt werden muss und erst dann die Telefonnummer des gewünschten Teilnehmers gewählt werden kann.

  Beispiel: ATD0W765432

– **T** : Wechsel auf Tonwahlverfahren.

  Soll bei Anschluss an einen tonwahlfähigen Telefonanschluss das schnellere Tonwahlverfahren verwendet werden, setzen Sie das Wählsonderzeichen T vor die Rufnummer. Beispiel: ATDT765432

Authentifizierung

PAP / CHAP / Keine

PAP = Password Authentication Protocol, CHAP = Challenge Handshake Authentication Protocol. Das sind Bezeichnungen für Verfahren zur sicheren Übertragung von Authentifizierungsdaten über das Point-to-Point Protocol.

Wenn der Internet Service Provider verlangt, dass sich der Benutzer mit Benutzername und Passwort anmeldet, wird PAP oder CHAP als Authentifizierungsverfahren benutzt. Benutzername und Passwort sowie eventuell weitere Angaben, die der Benutzer für den Aufbau einer Verbindung ins Internet angeben muss, werden dem Benutzer vom Internet Service Provider mitgeteilt.

Je nach dem, ob **PAP** oder **CHAP** oder **Keine** ausgewählt wird, erscheinen unterhalb die entsprechenden Felder. In diese tragen Sie die entsprechenden Daten ein.

Wenn die Authentifizierung per PAP erfolgt:

Authentifizierung	PAP
Benutzername	
Passwort	
PAP-Server-Authentifizierung	Nein
Bedarfsweise Einwahl	Ja
Verbindungstrennung nach Leerlauf	Ja
Leerlaufzeit (Sekunden)	300
Lokale IP-Adresse	0.0.0.0
Entfernte IP-Adresse	0.0.0.0
Netzmaske	0.0.0.0

Benutzername

Benutzername, zur Anmeldung beim Internet-Service-Provider, um Zugang zum Internet zu erhalten.

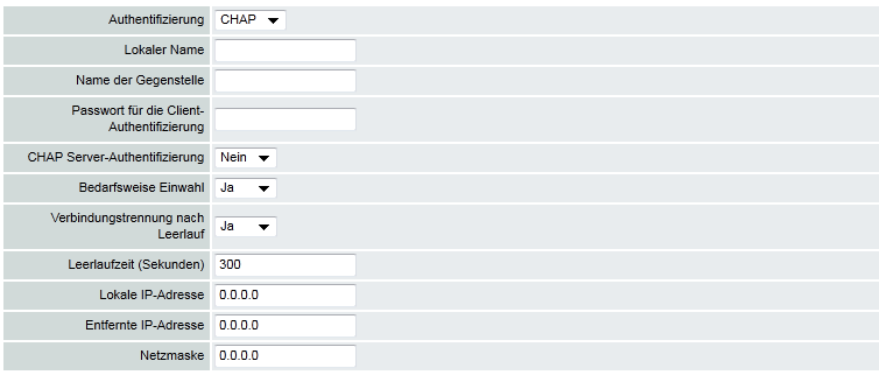
Passwort

Passwort, zur Anmeldung beim Internet-Service-Provider angegeben, um Zugang zum Internet zu erhalten.

Netzwerk >> Interfaces >> Ausgehender Ruf [...]

PAP-Server-Authentifizierung	**Ja/Nein** Bei **Ja** werden die nachfolgen 2 Eingabefelder eingeblendet:
Benutzername des Servers **Passwort des Servers**	Benutzername und Passwort, die der mGuard beim Server abfragt. Nur wenn der Server die verabredete Benutzernamen/Passwort-Kombination liefert, erlaubt der mGuard die Verbindung.
Nachfolgend aufgeführte Felder	Siehe unter „Wenn als Authentifizierung „Keine“ festgelegt wird“ auf Seite 6-94.

Wenn die Authentifizierung per CHAP erfolgt:



Lokaler Name	Ein Name für den mGuard, mit dem er sich beim Internet Service Provider meldet. Eventuell hat der Service Provider mehrere Kunden und muss durch die Nennung des Namens erkennen können, wer sich bei ihm einwählen will. Nachdem der mGuard sich mit diesem Namen beim Internet Service Provider angemeldet hat, vergleicht der Service Provider dann auch das angegebene Passwort für die Client-Authentifizierung (siehe unten). Nur wenn der Name dem Service Provider bekannt ist und das Passwort stimmt, kann die Verbindung erfolgreich aufgebaut werden.
Name der Gegenstelle	Ein Name, den der Internet Service Provider dem mGuard nennen wird, um sich zu identifizieren. Der mGuard wird keine Verbindung zum Service Provider aufbauen, wenn dieser nicht den richtigen Namen nennt.
Passwort für die Client-Authentifizierung	Passwort, das zur Anmeldung beim Internet Service Provider angegeben werden muss, um Zugang zum Internet zu erhalten.
CHAP-Server-Authentifizierung:	**Ja/Nein** Bei **Ja** werden die nachfolgen 2 Eingabefelder eingeblendet:
Passwort für die Server-Authentifizierung	Passwort, das der mGuard beim Server abfragt. Nur wenn der Server das verabredete Passwort liefert, erlaubt der mGuard die Verbindung.

Netzwerk >> Interfaces >> Ausgehender Ruf [...]		
	Nachfolgend aufgeführte Felder	Siehe unter „Wenn als Authentifizierung „Keine“ festgelegt wird“ auf Seite 6-94.
	Wenn als Authentifizierung „Keine“ festgelegt wird	In diesem Fall werden die Felder ausgeblendet, die die Authentifizierungsmethoden PAP oder CHAP betreffen.

Es bleiben dann nur die Felder unterhalb sichtbar, die weitere Einstellungen festlegen.

Weitere gemeinsame Einstellungen

Netzwerk >> Interfaces >> Ausgehender Ruf		
PPP Optionen (abgehender Ruf)	**Bedarfsweise Einwahl**	Ja / Nein

Ob *Ja* oder *Nein*: Es ist immer der mGuard, der die Telefonverbindung aufbaut.

Bei **Ja** (Standard): Diese Einstellung ist sinnvoll bei Telefonverbindungen, deren Kosten nach der Verbindungsdauer berechnet werden.

Der mGuard befiehlt dem Modem erst dann, eine Telefonverbindung aufzubauen, wenn auch wirklich Netzwerkpakete zu übertragen sind. Er weist dann auch das Modem an, die Telefonverbindung wieder abzubauen, sobald für eine bestimmte Zeit keine Netzwerkpakete mehr zu übertragen gewesen sind (siehe Wert in *Verbindungstrennung nach Leerlauf*). Auf diese Weise bleibt der mGuard allerdings nicht ständig von außerhalb, d. h. für eingehende Datenpakete, erreichbar.

Netzwerk >> Interfaces >> Ausgehender Ruf [...]

Der mGuard baut über das Modem auch oft oder sporadisch dann eine Verbindung auf bzw. hält eine Verbindung länger, wenn folgende Bedingungen zutreffen:

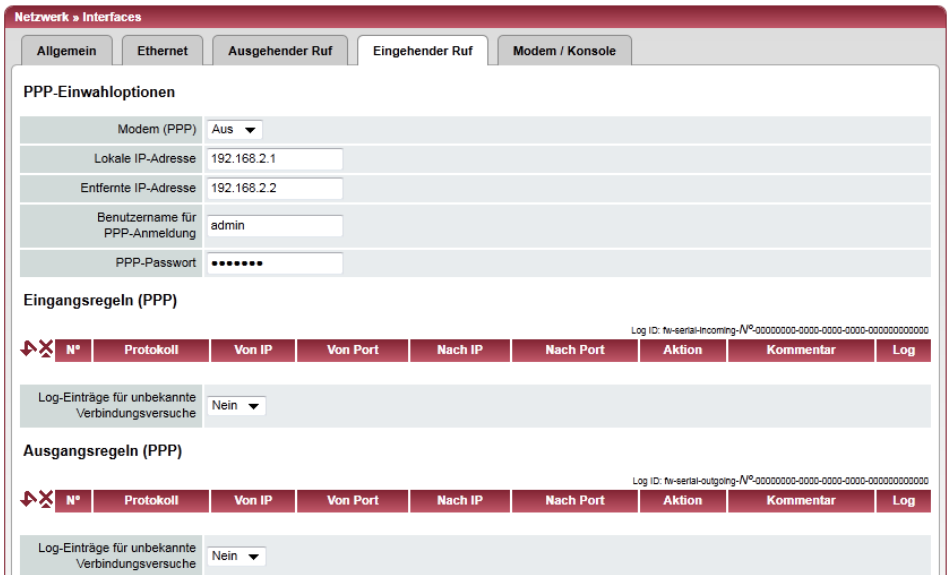
- Oft: Der mGuard ist so konfiguriert, dass er seine Systemzeit (Datum und Uhrzeit) regelmäßig mit einem externen NTP-Server synchronisiert.
- Sporadisch: Der mGuard agiert als DNS-Server und muss für einen Client eine DNS-Anfrage durchführen.
- Nach einem Neustart: Eine aktive VPN-Verbindung ist auf **Initiiere** gestellt. Dann wird jedesmal nach einem Neustart des mGuards eine Verbindung aufgebaut.
- Nach einem Neustart: Bei einer aktiven VPN-Verbindung ist das Gateway der Gegenstelle als Hostname angegeben. Dann muss der mGuard nach einem Neustart bei einem DNS-Server die zum Hostnamen gehörige IP-Adresse anfordern.
- Oft: Es sind VPN-Verbindungen eingerichtet und es werden regelmäßig DPD-Nachrichten gesendet (siehe „Dead Peer Detection“ auf Seite 6-216).
- Oft: Der mGuard ist so konfiguriert ist, dass er seine externe IP-Adresse regelmäßig einem DNS-Service, z. B. DynDNS, mitteilt, damit er unter seinem Hostnamen erreichbar bleibt.
- Oft: Die IP-Adressen von VPN-Gateways von Gegenstellen müssen beim DynDNS-Service angefordert bzw. durch Neuanfragen auf dem aktuellen Stand gehalten werden.
- Sporadisch: Der mGuard ist so konfiguriert, dass SNMP-Traps zum entfernten Server gesendet werden.
- Sporadisch: Der mGuard ist so konfiguriert, dass er den Fernzugriff per HTTPS, SSH oder SNMP zulässt und annimmt. (Dann sendet der mGuard Antwortpakete an jede IP-Adresse, von der ein Zugriffsversuch erfolgt (sofern die Firewall-Regeln den Zugriff zulassen würden)).
- Oft: Der mGuard ist so konfiguriert, dass er in regelmäßigen Abständen Verbindung zu einem HTTPS Server aufnimmt, um gegebenenfalls ein dort vorliegendes Konfigurationsprofil herunterzuladen (siehe „Verwaltung >> Zentrale Verwaltung“ auf Seite 6-56).

Bei **Nein** baut der mGuard mit Hilfe des angeschlossenen Modems so früh wie möglich nach seinem Neustart oder nach Aktivierung des Netzwerk-Modus *Modem* die Telefonverbindung auf. Diese bleibt dann dauerhaft bestehen, unabhängig davon, ob Daten übertragen werden oder nicht. Wird die Telefonverbindung dennoch unterbrochen, versucht der mGuard, sie sofort wiederherzustellen. So entsteht eine ständige Verbindung, also praktisch eine Standleitung. Auf diese Weise bleibt der mGuard auch ständig von außerhalb, d. h. für eingehende Datenpakete, erreichbar.

Netzwerk >> Interfaces >> Ausgehender Ruf [...]		
	Verbindungstrennung nach Leerlauf	**Ja / Nein** Wird nur beachtet, wenn *Bedarfsweise Einwahl* auf **Ja** gestellt ist. Bei **Ja** (Standard) trennt der mGuard die Telefonverbindung, sobald über die unter *Leerlaufzeit* angegebene Zeitdauer kein Datenverkehr stattfindet. Zur Trennung der Telefonverbindung gibt der mGuard dem angeschlossenen Modem das entsprechende Kommando. Bei **Nein** gibt der mGuard dem angeschlossenen Modem kein Kommando, die Telefonverbindung zu trennen.
	Leerlaufzeit (Sekunden)	Standard: 300. Findet nach Ablauf der hier angegebenen Zeit weiterhin kein Datenverkehr statt, kann der mGuard die Telefonverbindung trennen (siehe oben unter *Verbindungstrennung nach Leerlauf*).
	Lokale IP-Adresse	IP-Adresse der seriellen Schnittstelle des mGuards, die jetzt als WAN-Schnittstelle fungiert. Wird diese IP-Adresse vom Internet Service Provider dynamisch zugewiesen, übernehmen Sie den voreingestellten Wert: 0.0.0.0. Sonst, d. h. bei Zuteilung einer festen IP-Adresse, tragen Sie diese hier ein.
	Entfernte IP-Adresse	IP-Adresse der Gegenstelle. Bei Anbindung ans Internet ist das die IP-Adresse des Internet Service Providers, über die der Zugang ins Internet bereit gestellt wird. Da für die Verbindung das Point-to-Point Protocol (PPP) verwendet wird, muss im Normalfall diese IP-Adresse nicht spezifiziert werden, so dass Sie den voreingestellten Wert übernehmen: 0.0.0.0.
	Netzmaske	Die hier anzugegebene Netzmaske gehört zu den beiden IP-Adressen *Lokale IP-Adresse* und *Entfernte IP-Adresse*. Üblich ist, dass entweder alle drei Werte (*Lokale IP-Adresse, Entfernte IP-Adresse, Netzmaske*) fest eingestellt werden oder auf dem Wert 0.0.0.0 verbleiben. Auf der Registerkarte *Modem / Konsole* nehmen Sie Anschlusseinstellungen für ein externes Modem vor (siehe „Modem / Konsole“ auf Seite 6-100).

6.4.1.4 Eingehender Ruf

Nur *mGuard rs4000, mGuard centerport*, *mGuard industrial rs*, *mGuard blade,* mGuard delta[2]*,mGuard delta, EAGLE mGuard*



Netzwerk >> Interfaces >> Eingehender Ruf

PPP-Einwahloptionen

Dieser Menüpunkt gehört nicht zum Funktionsumfang vom mGuard rs2000.

Nur *mGuard rs4000, mGuard centerport*, *mGuard industrial rs*, *mGuard blade,* mGuard delta[2]*, mGuard delta, EAGLE mGuard*

Ist nur dann zu konfigurieren, wenn der mGuard die ppp-Einwahl erlauben soll, entweder über

– ein an der seriellen Schnittstelle angeschlossenes Modem oder
– ein eingebautes Modem (beim mGuard industrial rs als Option verfügbar).

Die ppp-Einwahl kann für Zugriffe ins LAN (oder auf den mGuard für Konfigurationszwecke) genutzt werden (siehe „Modem / Konsole“ auf Seite 6-100).

Wird das Modem für ausgehende Rufe verwendet, indem es als primäre externe Schnittstelle (Netzwerk-Modus *Modem)* des mGuards oder als dessen sekundäre externe Schnittstelle (wenn aktiviert im Netzwerk-Modus *Stealth* oder *Router*) fungiert, steht es nicht für die ppp-Einwahloption zur Verfügung.

Modem (PPP)

Nur *mGuard rs4000, mGuard industrial rs* **(ohne eingebautes Modem/ISDN-TA),** *mGuard blade, EAGLE mGuard, mGuard delta*

Aus / Ein

Der Schalter **muss** auf Aus stehen, wenn keine serielle Schnittstelle für die ppp-Einwahloption genutzt werden soll.

Steht dieser Schalter auf **Ein**, steht die ppp-Einwahloption zur Verfügung. Die Anschlusseinstellungen für das angeschlossene externe Modem sind auf der Registerkarte *Modem / Konsole* vorzunehmen.

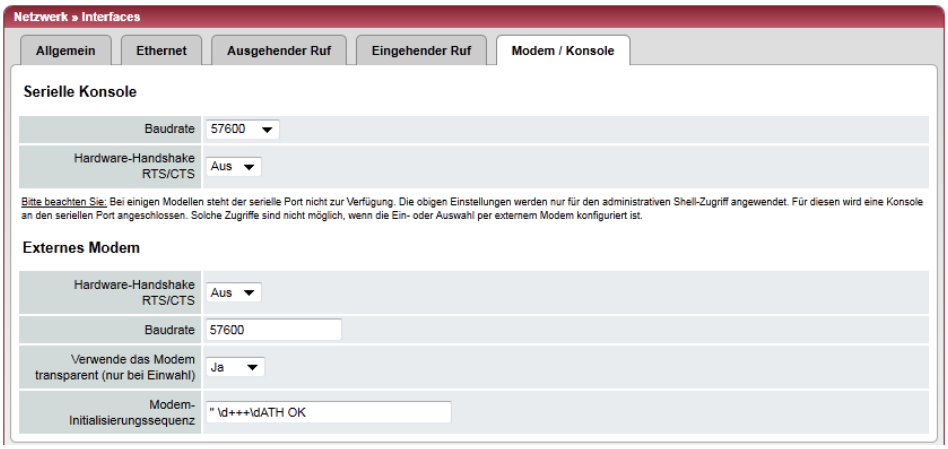
Netzwerk >> Interfaces >> Eingehender Ruf [...]		
	Modem (PPP)	**Nur** *mGuard industrial rs* **(mit eingebautem Modem / ISDN-TA)** **Aus / Eingebautes Modem / Externes Modem** Der Schalter **muss** auf **Aus** stehen, wenn die serielle Schnittstelle nicht für die ppp-Einwahloption genutzt werden soll. Steht dieser Schalter auf **Externes Modem**, steht die PPP-Einwahloption zur Verfügung. Dann muss an der seriellen Schnittstelle ein externes Modem angeschlossen sein. Die Anschlusseinstellungen für das angeschlossene externe Modem sind auf der Registerkarte *Modem / Konsole* vorzunehmen. Steht dieser Schalter auf **Eingebautes Modem**, steht die PPP-Einwahloption zur Verfügung. In diesem Fall erfolgt die Modemverbindung nicht über die auf seiner Frontseite befindliche Buchse *Serial* sondern über die Klemmleiste unten, über die das eingebaute Modem bzw. der eingebaute ISDN-Terminaladapter mit dem Telefonnetz verbunden wird. Die Anschlusseinstellungen für das eingebaute Modem sind auf der Registerkarte *Modem / Konsole* vorzunehmen. Bei Nutzung der Option **Eingebautes Modem** ist es zusätzlich möglich, die serielle Schnittstelle zu benutzen. Zu dessen Nutzungsmöglichkeiten siehe „Modem / Konsole“ auf Seite 6-100.
	Lokale IP-Adresse	IP-Adresse des mGuards, unter der er bei einer PPP-Verbindung erreichbar ist.
	Entfernte IP-Adresse	IP-Adresse der Gegenstelle von der PPP-Verbindung.
	Benutzername für PPP-Anmeldung	Anmeldename, welchen die PPP-Gegenstelle angeben muss, um per PPP-Verbindung Zugriff auf den mGuard zu bekommen.
	PPP-Passwort	Das Passwort, welches die PPP-Gegenstelle angeben muss, um per PPP-Verbindung Zugriff auf den mGuard zu bekommen.
Eingangsregeln (PPP)	Firewall-Regeln für PPP-Verbindungen zum LAN Interface. Sind mehrere Firewall-Regeln gesetzt, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Sollten nachfolgend in der Regelliste weitere Regeln vorhanden sein, die auch passen würden, werden diese ignoriert. Bei den Angaben haben Sie folgende Möglichkeiten:	
	Protokoll	**Alle** bedeutet: TCP, UDP, ICMP, GRE und andere IP-Protokolle
	Von / Nach IP	**0.0.0.0/0** bedeutet alle IP-Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise (siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 6-261).

Netzwerk >> Interfaces >> Eingehender Ruf [...]	
Von / Nach Port	(wird nur ausgewertet bei den Protokollen TCP und UDP) **any** bezeichnet jeden beliebigen Port. **startport:endport** (z. B. 110:120) bezeichnet einen Portbereich. Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben: (z. B. 110 für pop3 oder pop3 für 110).
Aktion	**Annehmen** bedeutet, die Datenpakete dürfen passieren. **Abweisen** bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. **Verwerfen** bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information über deren Verbleib erhält.
Kommentar	Ein frei wählbarer Kommentar für diese Regel.
Log	Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel – das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen – oder nicht - *Log* auf **Nein** setzen (werkseitige Voreinstellung).
Log-Einträge für unbekannte Verbindungsversuche	Ja / Nein Bei **Ja** werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden.
Ausgangsregeln (Port)	Firewall-Regeln für ausgehende PPP-Verbindungen vom LAN Interface. Die Parameter entsprechen denen von *Eingangsregeln (PPP)*. Diese Ausgangsregeln gelten für Datenpakete, die bei einer durch PPP-Einwahl initiierten Datenverbindung nach draußen gehen.

6.4.1.5 Modem / Konsole

Nur *mGuard rs4000/rs2000, mGuard centerport, mGuard industrial rs, mGuard smart*[2] (**nicht** *mGuard smart*), *mGuard blade,* mGuard delta[2], *mGuard delta, EAGLE mGuard.*

Einige mGuard-Modelle verfügen über eine von außen zugängliche serielle Schnittstelle, der mGuard industrial rs optional zusätzlich über ein eingebautes Modem (siehe „Netzwerk >> Interfaces“ auf Seite 6-64).



Nutzungsarten der seriellen Schnittstelle

Die serielle Schnittstelle kann alternativ wie folgt genutzt werden:

Primäres externes Interface (Dieser Menüpunkt gehört nicht zum Funktionsumfang vom mGuard rs2000)

Als **primäres externes Interface**, wenn unter *Netzwerk >> Interfaces* , auf der Registerkarte *Allgemein* als Netzwerk-Modus *Modem* eingestellt ist (siehe „Netzwerk >> Interfaces“ auf Seite 6-64 und „Allgemein“ auf Seite 6-65).

In diesem Fall wird der Datenverkehr nicht über den WAN-Port (= Ethernet-Schnittstelle) abgewickelt, sondern über die serielle Schnittstelle.

Sekundäres externes Interface (Dieser Menüpunkt gehört nicht zum Funktionsumfang vom mGuard rs2000)

Als **sekundäres externes Interface**, wenn unter *Netzwerk >> Interfaces* , Registerkarte *Allgemein* das *sekundäre externe Interface* aktiviert und *Modem* ausgewählt ist (siehe „Netzwerk >> Interfaces“ auf Seite 6-64 und „Allgemein“ auf Seite 6-65).

In diesem Fall wird Datenverkehr - permanent oder aushilfsweise - über die serielle Schnittstelle abgewickelt.

Einwahl ins LAN oder für Konfigurationszwecke (Dieser Menüpunkt gehört nicht zum Funktionsumfang vom mGuard rs2000)

Für die **Einwahl ins LAN oder für Konfigurationszwecke** (siehe auch „Eingehender Ruf“ auf Seite 6-97). Es gibt folgende Möglichkeiten:

– An die serielle Schnittstelle des mGuards wird ein Modem angeschlossen, das am Telefonnetz (Festnetz oder GSM-Netz) angeschlossen ist.

  (Beim mGuard industrial rs **mit** eingebautem Modem oder ISDN-Terminaladapter erfolgt der Anschluss ans Telefonnetz über die Klemmleiste unten am Gerät.)

  Dann kann von einem entfernten PC, der ebenfalls mit einem Modem oder ISDN-Adapter am Telefonnetz angeschlossen ist, zum mGuard eine PPP-Wählverbindung (PPP = Point-to-Point Protocol) aufgebaut werden.

  Diese Verwendungsart wird als PPP-Einwahloption bezeichnet. Sie kann für den Zugriff ins LAN benutzt werden, das sich hinter dem mGuard befindet, oder für die Konfiguration des mGuards. In Firewall-Auswahllisten wird für diese Verbindungsart die Interface-Bezeichnung *Einwahl* verwendet.

Damit Sie mit einem Windows-Rechner über die Wählverbindung auf das LAN zugreifen können, muss auf diesem Rechner eine Netzwerkverbindung eingerichtet sein, in der die Wählverbindung zum mGuard definiert ist. Außerdem muss für diese Verbindung die IP-Adresse des mGuards (oder dessen Hostname) als Gateway definiert werden, damit die Verbindungen ins LAN darüber geroutet werden.

Um auf die Web-Konfigurationsoberfläche des mGuards zuzugreifen, müssen Sie in die Adressenzeile des Web-Browser die IP-Adresse des mGuards (oder dessen Hostname) eingeben.

– Die serielle Schnittstelle des mGuards wird mit der seriellen Schnittstelle eines PCs verbunden.

  Auf dem PC wird mittels eines Terminalprogramms die Verbindung zum mGuard gestellt und die Konfiguration wird über die Kommandozeile des mGuards durchgeführt.

Sofern an der seriellen Schnittstelle ein externes Modem angeschlossen ist, sind gegebenenfalls weiter unten unter *Externes Modem* die passenden Einstellungen zu machen, unabhängig davon, für welche Nutzungsart Sie die serielle Schnittstelle und das an ihr angeschlossene Modem einsetzen.

Netzwerk >> Interfaces >> Modem/Konsole

Serielle Konsole

Die nachfolgende Einstellungen für *Baudrate* und *Hardware-Handshake* gelten nur für eine Konfigurationsverbindung, wenn wie oben beschrieben ein Terminal bzw. ein PC mit Terminalprogramm an der seriellen Schnittstelle angeschlossen wird.

Die Einstellungen sind nicht gültig, wenn ein externes Modem angeschlossen wird. Die Einstellung dafür erfolgt weiter unten unter *Externes Modem*.

Baudrate	Über die Auswahlliste wird festgelegt, mit welcher Übertragungsgeschwindigkeit die serielle Schnittstelle arbeiten soll.
Hardware-Handshake RTS/CTS	**Aus / Ein** Bei **Ein** findet eine Flusssteuerung durch RTS- und CTS-Signale statt.
Serielle Konsole über USB (nur beim mGuard smart², gilt nicht für den mGuard smart)	**Nein / Ja** Bei **Nein** nutzt der mGuard smart² den USB-Anschluss ausschließlich zur Stromversorgung. Bei **Ja** stellt der mGuard smart² zusätzlich über die USB-Schnittstelle eine serielle Schnittstelle für den angeschlossenen Rechner zur Verfügung. Auf dem Rechner kann mit Hilfe eines Terminal-Programmes auf die serielle Schnittstelle zugegriffen werden. Über die serielle Schnittstelle stellt der mGuard smart² eine Konsole zur Verfügung, die dann im Terminal-Programm genutzt werden kann. Unter Windows benötigen Sie einen speziellen Treiber. Dieser kann direkt vom mGuard herunter geladen werden. Der Link hierzu befindet sich rechts neben dem Auswahlmenü „Serielle Konsole über USB“.

Externes Modem

Dieser Menüpunkt gehört nicht zum Funktionsumfang vom mGuard rs2000.

Hardware-Handshake RTS/CTS	**Aus / Ein** Bei **Ein** findet bei der PPP-Verbindungen Flusssteuerung durch RTS- und CTS-Signale statt.

Netzwerk >> Interfaces >> Modem/Konsole		
	Baudrate	Standard: 57600. Übertragungsgeschwindigkeit für die Kommunikation zwischen mGuard und Modem, die über das serielle Verbindungskabel zwischen den beiden Geräten verläuft. Der Wert sollte so hoch eingestellt werden, wie es das Modem unterstützt. Ist der Wert niedriger eingestellt als die Geschwindigkeit, welche das Modem auf der Telefonleitung erreichen kann, dann wird die Telefonleitung nicht voll ausgenutzt.
	Verwende das Modem transparent (nur bei Einwahl):	**Ja / Nein** Wird das externe Modem zur Einwahl verwendet (siehe Seite 6-97), dann bedeutet die Einstellung **Ja**, dass der mGuard das Modem nicht initialisiert. Die nachfolgend konfigurierte Modem-Initialisierungssequenz wird nicht beachtet. So kann entweder ein Modem angeschlossen werden, das von selbst Anrufe annimmt (Standard-Profil des Modems beinhaltet „Auto-Answer“), oder es kann anstelle des Modems ein Null-Modem-Kabel zu einem Computer und darüber das PPP-Protokoll verwendet werden.
	Modem-Initialisierungssequenz	Gibt die Initialisierungssequenz an, die der mGuard zum angeschlossenen Modem sendet. Standard: *” |d+++|dATH OK* Gegebenenfalls im Handbuch zum Modem nachschlagen, wie die Initialisierungssequenz für diese Modem lautet.
	Die Initialisierungssequenz ist eine Folge von Zeichenketten, die vom Modem erwartet werden und von Befehlen, die daraufhin an das Modem gesendet werden, damit das Modem eine Verbindung aufbauen kann.	

Die voreingestellte Initialisierungssequenz hat folgende Bedeutung:

” (zwei einfache, direkt hintereinander gesetzte Anführungsstriche)	Die leere Zeichenkette inerhalb der Anführungsstriche bedeutet, dass der mGuard am Anfang keine Information vom angeschlossene Modem erwartet, sondern direkt den folgenden Text an das Modem sendet.
|d+++|dATH	Diese Zeichenkette sendet der mGuard an das Modem, um dessen Bereitschaft zum Annehmen von Kommandos festzustellen.
OK	Gibt an, dass der mGuard vom Modem die Zeichenkette ***OK*** als Antwort auf ***|d+++|dATH*** erwartet.

Bei vielen Modem-Modellen ist es möglich, Modem-Voreinstellungen im Modem selber abzuspeichern. Doch sollte auf diese Möglichkeit besser verzichtet werden.

Initialisierungssequenzen sollten statt dessen lieber extern, d. h. beim mGuard konfiguriert werden. Dann kann bei einem Defekt des Modems dieses schnell und problemlos ausgetauscht werden, ohne auf Modem-Voreinstellungen zu achten.

Soll das externe Modem für eingehende Rufe verwendet werden, ohne dass die Modem-Voreinstellungen darauf ausgelegt sind, dann müssen Sie dem Modem mitteilen, dass es hereinkommende Rufe nach dem Klingeln annehmen soll.

Bei Verwendung des erweiterten HAYES-Befehlssatzes geschieht dies durch das Anhängen der Zeichen „ ***AT&S0=1 OK***“ (ein Leerzeichen gefolgt von „***AT&S0=1***“, gefolgt von einem Leerzeichen, gefolgt von „***OK***“) an die Initialisierungssequenz.

Manches externe Modem benötigt gemäß seiner Werkseinstellungen zur korrekten Funktion die physikalische Verbindung mit der DTR-Leitung der seriellen Schnittstelle.

Weil die mGuard-Modelle diese Leitung an der externen seriellen Schnittstelle nicht zur Verfügung stellen, muss dann die obige Initialisierungssequenz um die anzuhängenden Zeichen „ ***AT&D0 OK***“ (ein Leerzeichen gefolgt von „***AT&D0***“, gefolgt von einem Leerzeichen, gefolgt von „***OK***“) erweitert werden. Gemäß des erweiterten HAYES-Befehlssatz bedeutet diese Sequenz, dass das Modem die DTR-Leitung nicht verwendet.

Soll das externe Modem für ausgehende Rufe verwendet werden, ist es an einer Nebenstellenanlage angeschlossen, und erzeugt diese Nebenstellenanlage kein Freizeichen nach dem Abheben, dann muss das Modem angewiesen werden, vor dem Wählen nicht auf ein Freizeichen zu warten.

In diesem Fall erweitern Sie die Initialisierungssequenz um die anzuhängenden Zeichen „ ***ATX3 OK***“ (ein Leerzeichen gefolgt von „***ATX3***“, gefolgt von einem Leerzeichen, gefolgt von „***OK***“).

In dem Fall sollten Sie in die *Anzurufende Telefonnummer* nach der Ziffer zur Amtsholung das Steuerzeichen „***W***“ einfügen, damit auf das Freizeichen gewartet wird.

Beim mGuard industrial rs mit eingebautem Modem / eingebautem ISDN-Modem (ISDN-Terminaladapter)

Der mGuard industrial rs verfügt optional über ein eingebautes Analog-Modem / einen eingebauten ISDN-Terminaladapter. Das eingebaute Modem bzw. der eingebaute ISDN-Terminaladapter kann wie folgt benutzt werden:

Primäres externes Interface

– Als **primäres externes Interface**, wenn unter *Netzwerk* >> *Interfaces* , auf der Registerkarte *Allgemein* als Netzwerk-Modus *Eingebautes Modem* eingestellt ist (siehe „Netzwerk >> Interfaces“ auf Seite 6-64 und „Allgemein“ auf Seite 6-65). In diesem Fall wird der Datenverkehr nicht über den WAN-Port (= Ethernet-Schnittstelle) abgewickelt, sondern über dieses Modem.

Sekundäres externes Interface

– Als **sekundäres externes Interface**, wenn unter *Netzwerk* >> *Interfaces* , Registerkarte *Allgemein* das *sekundäre externe Interface* aktiviert und *Eingebautes Modem* ausgewählt ist (siehe „Netzwerk >> Interfaces“ auf Seite 6-64 und „Allgemein“ auf Seite 6-65). In diesem Fall wird Datenverkehr auch über die serielle Schnittstelle abgewickelt.

PPP-Einwahloption

– für die PPP-Einwahloption (siehe „Nutzungsarten der seriellen Schnittstelle“ auf Seite 6-100)

Beachten Sie, dass die serielle Schnittstelle des Gerätes zusätzlich vergleichbare Nutzungsmöglichkeiten zur Verfügung stellt (siehe oben). So kann beim *mGuard industrial rs* mit eingebautem Modem z. B. der normale Datenverkehr über eine Modemverbindung erfolgen (Netzwerk-Modus *Modem*) und gleichzeitig eine zweite Modemverbindung für die PPP-Einwahloption genutzt werden.

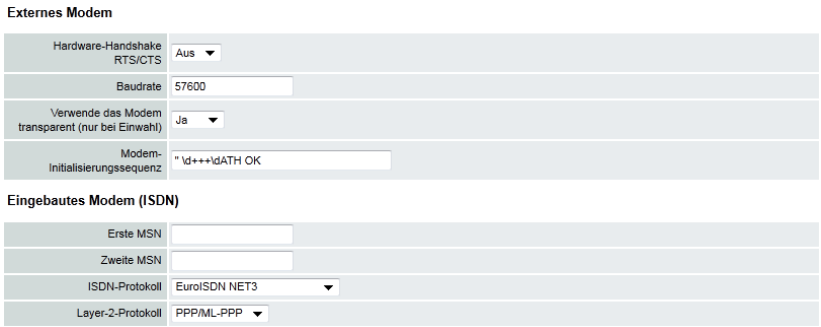
Beim mGuard industrial rs mit eingebautem Modem

Zusätzlich beim mGuard industrial rs mit eingebautem Modem (analog)

Netzwerk >> Interfaces >> Modem/Konsole (Beim mGuard industrial rs mit eingebautem Modem)		
Externes Modem	**Wie beim** *mGuard industrial rs* **(ohne eingebautes Modem), mGuard centerport,** *mGuard blade, EAGLE mGuard* **und** *mGuard delta:*	
	Konfiguration wie oben für **Externes Modem** (siehe „Externes Modem“ auf Seite 6-101).	
Eingebautes Modem (analog)	**Staat**	Hier muss der Staat angegeben werden, in dem der mGuard mit seinem eingebautem Modem betrieben wird. Nur dann ist gewährleistet, dass sich das eingebaute Modem gemäß der in diesem Staat gültigen Fernmeldevorschriften verhält und z. B. Rufton und Wählton richtig erkennt und entsprechend reagiert.
	Nebenstelle (bzgl. Amtsholung)	Ja / Nein Bei **Nein** erwartet der mGuard bei Anschaltung ans Telefonnetz den Wählton, wenn der mGuard die Gegenstelle anwählen will. Bei **Ja** erwartet der mGuard keinen Wählton sondern beginnt gleich mit der Anwahl der Gegenstelle. Dieses Verhalten kann notwendig sein, wenn das eingebaute Modem des mGuards an einer privaten Nebenstellenanlage angeschlossen ist, bei der beim „Abheben“ kein Wählton ausgegeben wird. Wenn zur Anwahl nach draußen (Amtsholung) eine bestimmte Nummer, z. B. „0“ gewählt werden muss, ist diese der anzuwählenden Telefonnummer der gewünschten Gegenstelle voran zu stellen.
	Lautstärke (eingebauter Lautsprecher)	
	Lautsprechernutzung	Diese beiden Einstellungen legen fest, was der eingebaute Lautsprecher des mGuards wiedergeben soll und in welcher Lautstärke.

Beim mGuard industrial rs mit eingebautem ISDN-Terminaladapter

Zusätzlich beim mGuard industrial rs mit eingebautem Modem (ISDN)

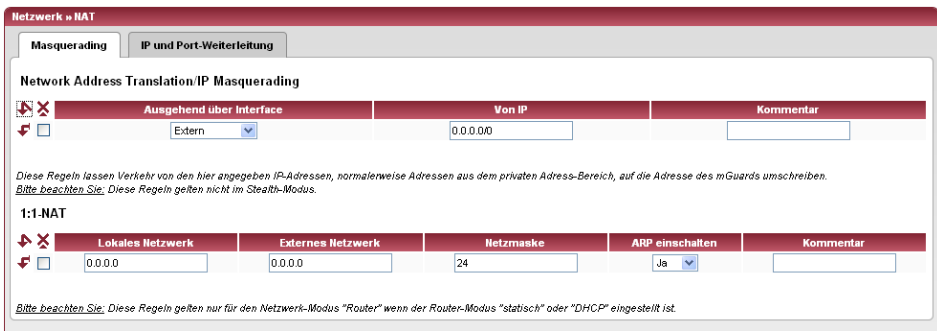


Netzwerk >> Interfaces >> Modem/Konsole (Beim mGuard industrial rs mit ISDN-Terminaladapter)

Externes Modem	**Wie beim** *mGuard industrial rs* **(ohne eingebautes Modem),** *mGuard rs4000,* **mGuard centerport,** *mGuard blade, EAGLE mGuard* **und** *mGuard delta:*	
	Konfiguration wie oben für **Externes Modem** (siehe „Externes Modem“ auf Seite 6-101).	
Eingebautes Modem (ISDN)	**Erste MSN**	Bei ausgehenden Rufen überträgt der mGuard die hier eingetragene MSN (Multiple Subscriber Number) zur angerufenen Gegenstelle. Außerdem ist der mGuard unter dieser MSN für eingehende Anrufe erreichbar (sofern Einwahl ermöglicht ist (siehe Registerkarte *Allgemein*)). Max. 25 Ziffern/Zeichen; folgende Sonderzeichen können verwendet werden: *****, **#**, **:** (Doppelpunkt)
	Zweite MSN	Soll der mGuard für Einwahl (sofern ermöglicht) zusätzlich unter einer anderen Nummer erreichbar sein, tragen Sie hier eine zweite MSN ein.
	ISDN-Protokoll	In Deutschland und vielen anderen europäischen Länder wird das ISDN-Protokoll EuroISDN verwendet, auch NET3 genannt. Ansonsten ist länderspezifisch festgelegt, welches ISDN-Protokoll benutzt wird. Muss gegebenenfalls bei der zuständigen Telefongesellschaft erfragt werden
	Layer-2-Protokoll	Das Regelwerk, über das sich der ISDN-Terminaladapter des lokalen mGuard mit seiner ISDN-Gegenstelle verständigt. Das ist im Allgemeinen das ISDN-Modem des Internet Service Providers, über das die Verbindung ins Internet hergestellt wird. Muss beim Internet Service Provider erfragt werden. Sehr häufig wird PPP/ML-PPP verwendet.

6.4.2 Netzwerk >> NAT

6.4.2.1 Masquerading



Netzwerk >> NAT >> Masquerading

Network Address Translation / IP-Masquerading

Listet die festgelegten Regeln für NAT (**N**etwork **A**ddress **T**ranslation) auf.

Das Gerät kann bei ausgehenden Datenpaketen die in ihnen angegebenen Absender-IP-Adressen aus seinem internen Netzwerk auf seine eigene externe Adresse umschreiben, eine Technik, die als NAT (Network Address Translation) bezeichnet wird (siehe auch NAT (Network Address Translation) im Glossar).

Diese Methode wird z. B. benutzt, wenn die internen Adressen extern nicht geroutet werden können oder sollen, z. B. weil ein privater Adressbereich wie 192.168.x.x oder die interne Netzstruktur verborgen werden soll.

Die Methode kann auch dazu genutzt werden, um externe Netzwerkstrukturen den internen Geräten zu verbergen. Dazu können Sie unter **Ausgehend über Interface** die Auswahl **Intern** einstellen. Die Einstellung **Intern** ermöglicht die Kommunikation zwischen zwei separaten IP-Netzen, bei denen die IP-Geräte keine (sinnvolle) Standard-Route bzw. differenziertere Routing-Einstellungen konfiguriert haben (z. B. SPSsen ohne entsprechende Einstellung). Dazu müssen unter **1:1-NAT** die entsprechenden Einstellungen vorgenommen werden.

Dieses Verfahren wird auch *IP-Masquerading* genannt.

Werkseinstellung: Es findet kein NAT statt.

Arbeitet der mGuard im *PPPoE/PPTP*-Modus, muss NAT aktiviert werden, um Zugriff auf das Internet zu erhalten. Ist NAT nicht aktiviert, können nur VPN-Verbindungen genutzt werden.

Bei der Verwendung von mehreren statischen IP-Adressen für den WAN-Port wird immer die erste IP-Adresse der Liste für IP-Masquerading verwendet.

Im Stealth-Modus werden die Regeln nicht angewendet.

Ausgehend über Interface

Extern / Extern 2 / Alle Externen[1] / Intern

Gibt an, über welches Interface die Datenpakete ausgehen, damit sich die Regel auf sie bezieht. Mit **Alle Externen** sind die Interfaces **Extern** und **Extern 2** gemeint

Netzwerk >> NAT >> Masquerading [...]

Es wird eine Maskierung definiert, die im Router-Modus für Netzwerk-Datenströme gilt. Diese Datenströme werden so initiiert, dass sie zu einem Zielgerät führen, das über die ausgewählte Netzwerkschnittstelle des mGuards erreichbar ist.

Dafür ersetzt der mGuard in allen zugehörigen Datenpaketen die IP-Adresse des Initiators durch eine geeignete IP-Adresse der ausgewählten Netzwerkschnittstelle. Die Wirkung ist analog zu den anderen Werten derselben Variablen. Dem Ziel des Datenstroms bleibt die IP-Adresse des Initiators verborgen. Insbesondere benötigt das Ziel keine Routen, nicht einmal eine Standard-Route (Standard-Gateway), um in so einem Datenstrom zu antworten.

Stellen Sie die Firewall so ein, dass die gewünschten Verbindungen erlaubt sind. Für Ein- und Ausgangsregeln gilt, dass die Quelladresse noch dem ursprünglichen Absender entspricht, wenn die Firewall-Regeln angewendet werden.

Beachten Sie bei den Einstellungen „Extern / Extern 2 / Alle Externen“ die Ausgangsregeln (siehe „Ausgangsregeln“ auf Seite 6-147).

Beachten Sie bei der Einstellung „Intern“ die Eingangsregeln (siehe „Eingangsregeln“ auf Seite 6-145).

Von IP

0.0.0.0/0 bedeutet, alle internen IP-Adressen werden dem NAT-Verfahren unterzogen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise (siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 6-261).

Kommentar

Kann mit kommentierendem Text gefüllt werden.

1:1-NAT

Listet die festgelegten Regeln für 1-zu-1-NAT (Network Address Translation) auf.

Bei 1-zu-1-NAT werden die Absender-IP-Adressen so ausgetauscht, dass jede einzelne gegen eine bestimmte andere ausgetauscht wird, und nicht wie beim IP-Masquerading gegen eine für alle Datenpakete identische. So wird ermöglicht, dass der mGuard die Adressen des internen Netzes in das externe Netz spiegeln kann.

Beispiel:

Der mGuard ist über seinen LAN-Port an Netzwerk 192.168.0.0/24 angeschlossen, mit seinem WAN-Port an Netzwerk 10.0.0.0/24. Durch das 1:1-NAT lässt sich der LAN-Rechner 192.168.0.8 im externen Netz unter der IP-Adresse 10.0.0.8 erreichen.

192.168.0.0/24 **10.0.0.0/24**

Der mGuard beansprucht die für „Externes Netzwerk“ angegebenen IP-Adressen für die Geräte in seinem „Lokalen Netzwerk“. Der mGuard antwortet stellvertretend für die Geräte aus dem „Lokalen Netzwerk“ mit ARP-Antworten zu allen Adressen aus dem angegebenen „Externen Netzwerk“. Die unter „Externes Netzwerk“ angegebenen IP-Adressen müssen also frei sein. Sie dürfen nicht für andere Geräte vergeben oder gar in Benutzung sein, weil sonst im externen Netzwerk ein IP-Adressenkonflikt entsteht. Dies gilt selbst dann, wenn zu einer oder mehreren IP-Adressen aus dem angegebenen „Externen Netzwerk“ gar kein Gerät im „Internen Netzwerk" existiert.

Netzwerk >> NAT >> Masquerading [...]

Werkseinstellung: Es findet kein 1:1-NAT statt.

	1:1-NAT kann nicht auf das Interface *Extern 2* angewendet werden.
	1:1-NAT wird nur im Netzwerk-Modus *Router* angewendet.

Lokales Netzwerk	Die Adresse des Netzwerks am LAN-Port.
Externes Netzwerk	Die Adresse des Netzwerks am WAN-Port.
Netzmaske	Die Netzmaske als Wert zwischen 1 und 32 für die lokale und externe Netzwerkadresse (siehe auch „CIDR (Classless Inter-Domain Routing)“ auf Seite 6-261).
Kommentar	Kann mit kommentierendem Text gefüllt werden.

[1] *Extern 2* und *Alle Externen* nur bei Geräten mit serieller Schnittstelle: mGuard rs4000/2000, mGuard centerport, mGuard industrial rs, mGuard blade, EAGLE mGuard, mGuard delta (siehe „Sekundäres externes Interface“ auf Seite 6-75).

6.4.2.2 IP und Port-Weiterleitung

Netzwerk >> NAT >> IP und Port-Weiterleitung

IP und Port-Weiterleitung

Listet die festgelegten Regeln zur Port-Weiterleitung (DNAT = Destination-NAT) auf.

Bei Port-Weiterleitung geschieht Folgendes: Der Header eingehender Datenpakete aus dem externen Netz, die an die externe IP-Adresse (oder eine der externen IP-Adressen) des mGuards sowie an einen bestimmten Port des mGuards gerichtet sind, werden so umgeschrieben, dass sie ins interne Netz an einen bestimmten Rechner und zu einem bestimmten Port dieses Rechners weitergeleitet werden. D. h. die IP-Adresse und Port-Nummer im Header eingehender Datenpakete werden geändert.

Dieses Verfahren wird auch Destination-NAT genannt.

Port-Weiterleitung kann nicht angewendet werden bei Verbindungen, die über das Interface *Extern 2*[1] initiiert werden.

[1] *Extern 2* nur bei Geräten mit serieller Schnittstelle

Die hier eingestellten Regeln haben gegenüber den Einstellungen unter Netzwerksicherheit >> Paketfilter >> Eingangsregeln Vorrang.

Protokoll: TCP / UDP / GRE

Geben Sie hier das Protokoll an, auf den sich die Regel beziehen soll.

GRE

IP-Pakete des GRE-Protokolls können weitergeleitet werden. Allerdings wird nur eine GRE-Verbindung zur gleichen Zeit unterstützt. Wenn mehr als ein Gerät GRE-Pakete an die selbe externe IP-Adresse sendet, kann der mGuard möglicherweise Antwortpakete nicht korrekt zurückleiten. Wir empfehlen, GRE-Pakete nur von bestimmten Sendern weiterzuleiten. Das können solche sein, für deren Quelladresse eine Weiterleitungsregel eingerichtet ist, indem im Feld „Von IP“ die Adresse des Senders eingetragen wird, zum Beispiel 193.194.195.196/32.

Von IP

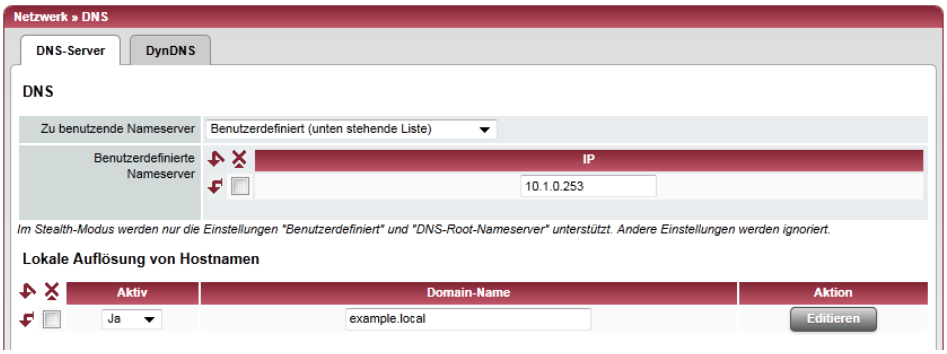
Absenderadresse, für die Weiterleitungen durchgeführt werden sollen.

0.0.0.0/0 bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise (siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 6-261)

Netzwerk >> NAT >> IP und Port-Weiterleitung [...]	
Von Port	Absenderport, für den Weiterleitungen durchgeführt werden sollen. **any** bezeichnet jeden beliebigen Port. Er kann entweder über die Port-Nummer oder über den entsprechenden Servicenamen angegeben werden, z. B. *pop3* für Port 110 oder *http* für Port 80
Eintreffend auf IP	– Geben Sie hier die externe IP-Adresse (oder eine der externen IP-Adressen) des mGuards an, **oder** – verwenden Sie Variable: **%extern** (wenn ein dynamischer Wechsel der externen IP-Adresse des mGuards erfolgt, so dass die externe IP-Adresse nicht angebbar ist). Die Angabe von **%extern** bezieht sich bei der Verwendung von mehreren statischen IP-Adressen für den WAN-Port immer auf die erste IP-Adresse der Liste.
Eintreffend auf Port	Original-Ziel-Port, der in eingehenden Datenpaketen angegeben ist. Er kann entweder über die Port-Nummer oder über den entsprechenden Servicenamen angegeben werden, z. B. *pop3* für Port 110 oder *http* für Port 80. Beim Protokoll „GRE“ ist diese Angabe irrelevant. Sie wird vom mGuard ignoriert.
Weiterleiten an IP	Interne IP-Adresse, an die die Datenpakete weitergeleitet werden sollen und auf die die Original-Zieladressen umgeschrieben werden.
Weiterleiten an Port	Port, an den die Datenpakete weitergeleitet werden sollen und auf den die Original-Port-Angaben umgeschrieben werden. Er kann entweder über die Port-Nummer oder über den entsprechenden Servicenamen angegeben werden, z. B. *pop3* für Port 110 oder *http* für Port 80. Beim Protokoll „GRE“ ist diese Angabe irrelevant. Sie wird vom mGuard ignoriert.
Kommentar	Ein frei wählbarer Kommentar für diese Regel.
Log	Für jede einzelne Port-Weiterleitungs-Regel können Sie festlegen, ob bei Greifen der Regel – das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen – oder nicht - *Log* auf **Nein** setzen (werkseitige Voreinstellung).

6.4.3 Netzwerk >> DNS

6.4.3.1 DNS-Server



Netzwerk >> DNS >> DNS-Server

DNS

Soll der mGuard von sich aus eine Verbindung zu einer Gegenstelle aufbauen (zum Beispiel VPN-Gateway oder NTP-Server) und wird ihm diese in Form eines Hostnamens angegeben (d. h. in der Form www.example.com), dann muss der mGuard ermitteln, welche IP-Adresse sich hinter dem Hostnamen verbirgt. Dazu nimmt er Verbindung zu einem Domain Name Server (DNS) auf, um dort die zugehörige IP-Adresse zu erfragen. Die zum Hostnamen ermittelte IP-Adresse wird im Cache gespeichert, damit sie bei weiteren Hostnamensauflösungen direkt, d. h. schneller gefunden werden kann.

Durch die Funktion *Lokale Auflösung von Hostnamen* kann der mGuard außerdem so konfiguriert werden, dass er selber DNS-Anfragen für lokal verwendete Hostnamen beantwortet, indem er auf ein internes, zuvor konfiguriertes Verzeichnis zugreift.

Die lokal angeschlossenen Clients können (manuell oder per DHCP) so konfiguriert werden, dass als Adresse des zu benutzenden DNS-Servers die lokale Adresse des mGuards verwendet wird. Wird der mGuard im *Stealth*-Modus betrieben, muss bei den Clients die Management IP-Adresse des mGuards verwendet werden (sofern diese konfiguriert ist), oder es muss die IP-Adresse 1.1.1.1 als lokale Adresse des mGuards angegeben werden.

Zu benutzende Nameserver

- **DNS-Root-Nameserver**
  Anfragen werden an die Root-Nameserver im Internet gerichtet, deren IP-Adressen im mGuard gespeichert sind. Diese Adressen ändern sich selten.
- **Provider-definiert (z. B. via PPPoE oder DHCP)**
  Es werden die Domain Name Server des Internet Service Providers benutzt, der den Zugang zum Internet zur Verfügung stellt. Wählen Sie diese Einstellung nur dann, wenn der mGuard im *PPPoE*-, im *PPTP*-, *Modem*-Modus oder im *Router*-Modus mit DHCP arbeitet.
- **Benutzerdefiniert (unten stehende Liste)**
  Ist diese Einstellung gewählt, nimmt der mGuard mit den Domain Name Servern Verbindung auf, die in der Liste *Benutzer definierte Nameserver* aufgeführt sind.

Benutzerdefinierte Nameserver

In dieser Liste können Sie die IP-Adressen von Domain Name Servern erfassen. Sollen diesen vom mGuard benutzt werden, muss oben unter **Zu benutzende Nameserver** die Option *Benutzer definiert (unten stehende Liste)* eingestellt sein.

Netzwerk >> DNS >> DNS-Server [...]

Lokale Auflösung von Hostnamen

Sie können zu verschiedenen Domain-Namen jeweils mehrere Einträge mit Zuordnungspaaren von Hostnamen und IP-Adressen konfigurieren.

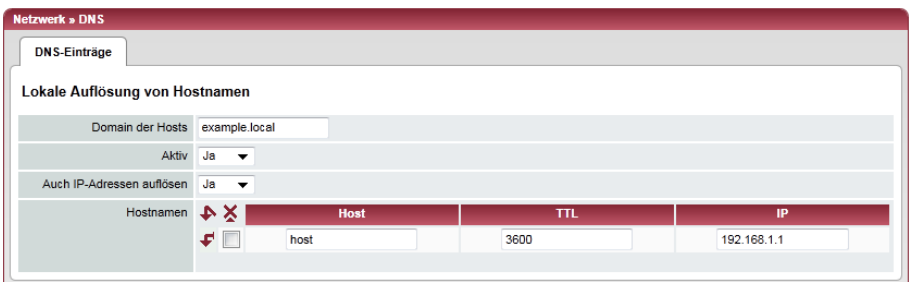
Sie haben die Möglichkeit, Zuordnungspaare von Hostnamen und IP-Adressen neu zu definieren, zu ändern (editieren) und zu löschen. Ferner können Sie für eine Domain die Auflösung von Hostnamen aktivieren oder deaktivieren. Und Sie können eine Domain mit all ihren Zuordnungspaaren löschen.

Tabelle mit Zuordnungspaaren für eine Domain anlegen:

- Eine neue Zeile öffnen und in dieser auf die Schaltfläche **Editieren** klicken.

Zuordnungspaare, die zu einer Domain gehören, ändern oder löschen:

- In der betreffenden Tabellenzeile auf **Editieren** klicken.
  Nach Klicken auf **Editieren** wird die Registerkarte für *DNS-Einträge* angezeigt:



Domain der Hosts
Der Name kann frei vergeben werden, muss aber den Regeln für die Vergabe von Domain-Namen folgen. Wird jedem Hostnamen zugeordnet.

Aktiv
Ja / Nein

Schaltet die Funktion *Lokale Auflösung von Hostnamen* für die im Feld darüber angegebene Domain auf Ein (**Ja**) oder auf Aus (**Nein**).

Auch IP-Adressen auflösen
Nein: Der mGuard löst nur Hostnamen auf, d. h. liefert zu Hostnamen die zugeordnete IP-Adresse.

Ja: Wie bei Nein. Zusätzlich ist es möglich, für eine IP-Adresse die zugeordneten Hostnamen geliefert zu bekommen.

Hostnamen
Die Tabelle kann beliebig viele Einträge aufnehmen.

Ein Hostname darf mehreren IP-Adressen zugeordnet werden. Einer IP-Adresse dürfen mehrere Hostnamen zugeordnet werden.

TTL
Abkürzung für **T**ime **T**o **L**ive. Angabe in Sekunden. Standard: 3600 (= 1 Stunde)

Gibt an, wie lange abgerufene Zuordnungspaare im Cache des abrufenden Rechners gespeichert bleiben dürfen.

IP
Die IP-Adresse, die dem Hostnamen in dieser Tabellenzeile zugeordnet wird.

Domäne mit allen Zuordnungspaaren löschen
Den entsprechenden Tabelleneintrag löschen.

Beispiel: Lokale Auflösung von Hostnamen

Die Funktion „Lokale Auflösung von Hostnamen“ findet z. B. in folgendem Szenario Anwendung:

Ein Werk betreibt mehrere gleich aufgebaute Maschinen, jede als eine sogenannte Zelle. Die lokalen Netze der Zellen A, B und C sind jeweils per mGuard über das Internet mit dem Werksnetz verbunden. In jeder Zelle befinden sich mehrere Steuerungselemente, die über ihre IP-Adressen angesprochen werden können. Dabei werden je Zelle unterschiedliche Adressräume verwendet.

Ein Service-Techniker soll in der Lage sein, sich bei Maschine A, B oder C vor Ort mit seinem Notebook an das dort vorhandene lokale Netz anzuschließen und mit den einzelnen Steuerungen zu kommunizieren. Damit der Techniker nicht für jede einzelne Steuerung in Maschine A, B oder C deren IP-Adresse kennen und eingeben muss, sind den IP-Adressen der Steuerungen jeweils Hostnamen nach einheitlichem Schema zugeordnet, die der Service-Techniker verwendet. Dabei sind die bei den Maschinen A, B und C verwendeten Hostnamen identisch, d. h. zum Beispiel, dass die Steuerung der Verpackungsmaschine in allen drei Maschinen den Hostnamen „pack“ hat. Jeder Maschine ist aber ein individueller Domain-Name zugeordnet, z. B. cell-a.example.com.

Der Service-Techniker kann sein Notebook bei Maschine A, B oder C ans lokale Netz anschließen und in jedem dieser Netze dieselben Hostnamen benutzen, um mit den entsprechenden Maschinensteuerungen zu kommunizieren.

Das Notebook kann die zu verwendende IP-Adresse, den Nameserver und die Domain vom mGuard per DHCP erhalten.

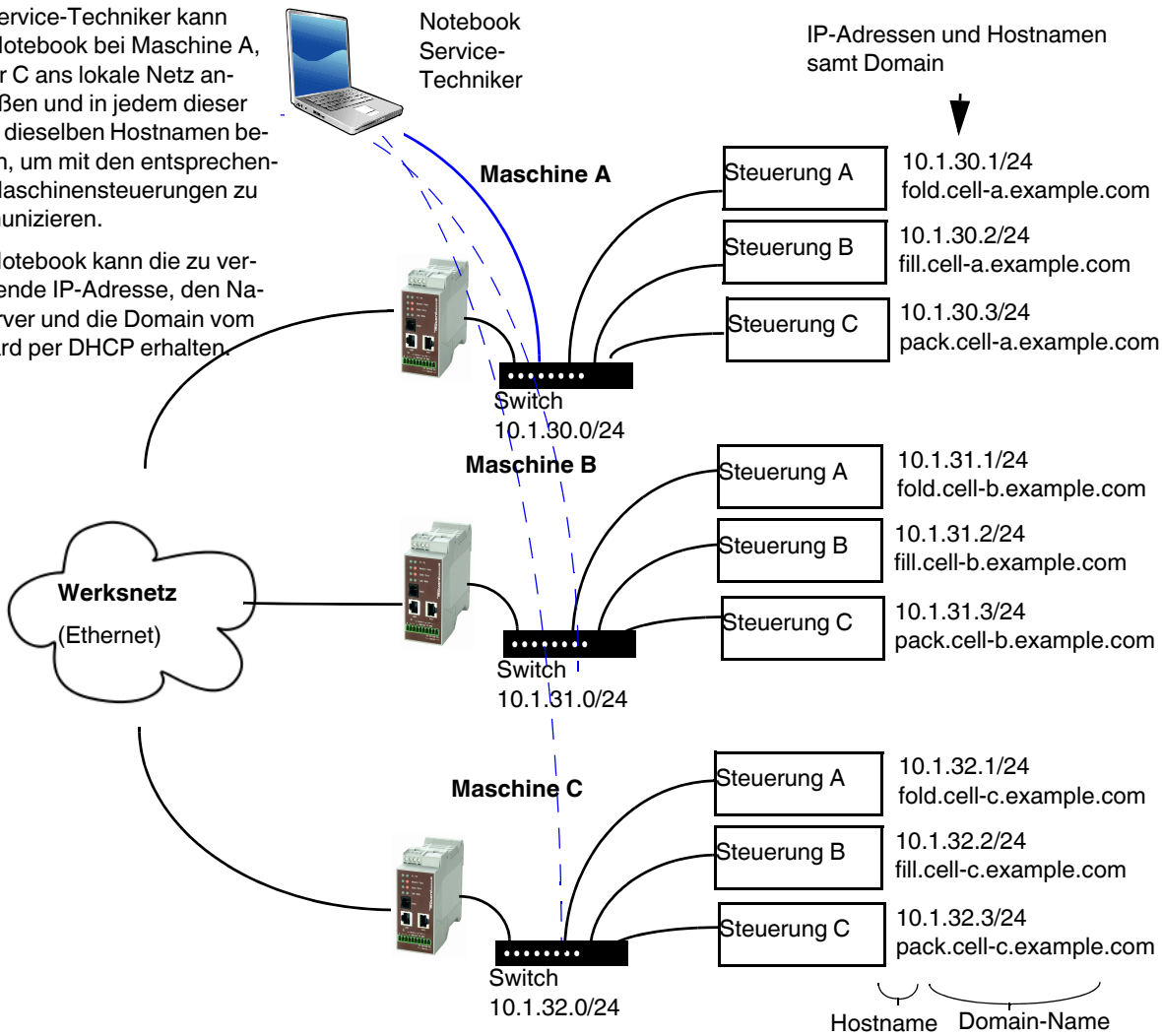
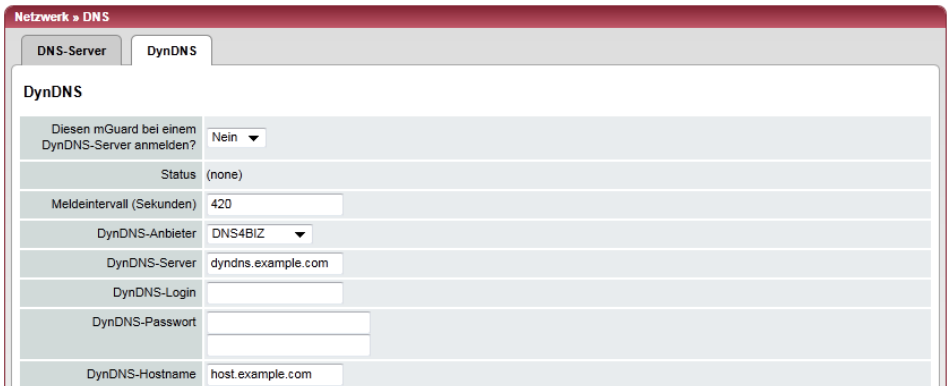


Bild 6-1 Lokale Auflösung von Hostnamen

6.4.3.2 DynDNS



Netzwerk >> DNS >> DynDNS

DynDNS

Zum Aufbau von VPN-Verbindungen muss mindestens die IP-Adresse eines der Partner bekannt sein, damit diese miteinander Kontakt aufnehmen können. Diese Bedingung ist nicht erfüllt, wenn beide Teilnehmer ihre IP-Adressen dynamisch von ihrem Internet Service Provider zugewiesen bekommen. In diesem Fall kann aber ein DynDNS-Service wie z. B. DynDNS.org oder DNS4BIZ.com helfen. Bei einem DynDNS-Service wird die jeweils gültige IP-Adresse unter einem festen Namen registriert.

Sofern Sie für einen vom mGuard unterstützten DynDNS-Service registriert sind, können Sie in diesem Dialogfeld die entsprechenden Angaben machen.

Diesen mGuard bei einem DynDNS-Server anmelden?

Wählen Sie **Ja**, wenn Sie beim DynDNS-Anbieter entsprechend registriert sind, und der mGuard den Service benutzen soll. Dann meldet der mGuard die aktuelle IP-Adresse, die gerade dem eigenen Internet-Anschluss vom Internet Service Provider zugewiesen ist, an den DynDNS-Service.

Meldeintervall (Sekunden)

Standard: 420 (Sekunden).

Immer wenn sich die IP-Adresse des eigenen Internet-Anschlusses ändert, informiert der mGuard den DynDNS-Service über die neue IP-Adresse. Aus Zuverlässigkeitsgründen erfolgt diese Meldung zusätzlich in dem hier festgelegten Zeitintervall.

Bei einigen DynDNS-Anbietern wie z. B. DynDNS.org hat diese Einstellung keine Wirkung, da dort ein zu häufiges Melden zur Löschung des Accounts führen kann.

DynDNS-Anbieter

Die zur Auswahl gestellten Anbieter unterstützen das Protokoll, das auch der mGuard unterstützt.

Wählen Sie den Namen des Anbieters, bei dem Sie registriert sind, z. B. DynDNS.org, TinyDynDNS, DNS4BIZ

DynDNS-Server

Name des Servers des ausgewählten DynDNS-Anbieters.

DynDNS-Login, DynDNS-Passwort

Geben Sie hier den Benutzernamen und das Passwort ein, das Ihnen vom DynDNS-Anbieter zugeteilt worden ist.

DynDNS-Hostname

Der für diesen mGuard gewählte Hostname beim DynDNS-Service - sofern Sie einen DynDNS-Dienst benutzen und oben die entsprechenden Angaben gemacht haben.

Unter diesem Hostnamen ist dann der mGuard erreichbar.

6.4.4 Netzwerk >> DHCP

Mit dem Dynamic Host Configuration Protocol (DHCP) kann den direkt am mGuard angeschlossenen Rechner automatisch die hier eingestellte Netzwerkkonfiguration zugeteilt werden. Unter *Internes DHCP* können Sie DHCP-Einstellungen für das interne Interface (= LAN-Port) vornehmen und unter *Externes DHCP* die DHCP-Einstellungen für das externe Interface (= WAN-Port). Der Menüpunkt „Externes DHCP“ gehört nicht zum Funktionsumfang vom mGuard rs2000.

Der DHCP-Server funktioniert auch im *Stealth*-Modus.

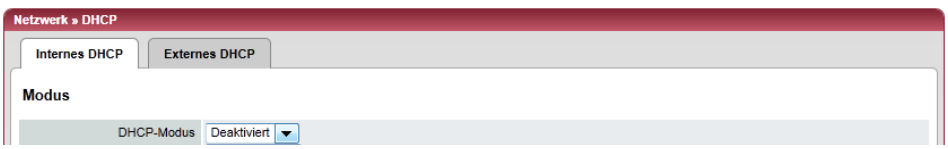
Im Multi-Stealth-Mode kann der externe DHCP-Server des mGuards nicht genutzt werden, wenn eine VLAN ID als Management IP zugewiesen ist.

IP-Konfiguration bei Windows-Rechnern: Wenn Sie den DHCP-Server des mGuards starten, können Sie die lokal angeschlossenen Rechner so konfigurieren, dass sie ihre IP-Adressen automatisch beziehen.

Dazu unter Windows XP

- Im Start-Menü „Systemsteuerung, Netzwerkverbindungen“ wählen.
- Das Symbol des LAN-Adapters mit der rechten Maustaste anklicken und im Kontextmenü auf „Eigenschaften“ klicken.
- Auf der Registerkarte „Allgemein“ unter „Diese Verbindung verwendet folgende Elemente“ den Eintrag „Internetprotokoll (TCP/IP“) markieren und auf die Schaltfläche „Eigenschaften“ klicken.
- Machen Sie im Dialogfeld „Eigenschaften von Internetprotokoll (TCP/IP)“ die entsprechenden Angaben bzw. Einstellungen.

6.4.4.1 Internes / Externes DHCP



Netzwerk >> DHCP >> Internes DHCP

Modus

DHCP-Modus — **Deaktiviert / Server / Relay**

Setzen Sie diesen Schalter auf **Server**, wenn der mGuard als eigenständiger DHCP-Server arbeiten soll. Dann werden unten auf der Registerkarte entsprechende Einstellmöglichkeiten eingeblendet (siehe „Server“).

Setzen Sie ihn auf **Relay**, wenn der mGuard DHCP-Anfragen an einen anderen DHCP-Server weiterleiten soll. Dann werden unten auf der Registerkarte entsprechende Einstellmöglichkeiten eingeblendet (siehe „Relay“).

Im *Stealth*-Modus des mGuards wird der DHCP-Modus *Relay* nicht unterstützt. Wenn der mGuard im *Stealth*-Modus betrieben wird und der DHCP-Modus *Relay* ausgewählt ist, dann wird diese Einstellung ignoriert.

Aufgrund der Natur des Stealth-Modus werden DHCP-Anfragen des Rechners und die entsprechenden Antworten jedoch durchgeleitet.

Wenn der Schalter auf **Deaktiviert** steht, beantwortet der mGuard keine DHCP-Anfragen.

DHCP-Modus — **Server**

Ist als DHCP-Modus *Server* ausgewählt, werden unten auf der Seite entsprechende Einstellmöglichkeiten wie folgt eingeblendet.

Netzwerk >> DHCP >> Internes DHCP[...]		
DHCP-Server-Optionen	**Dynamischen IP-Adresspool aktivieren**	Setzen Sie diesen Schalter auf **Ja**, wenn sie den weiter unten durch *DHCP-Bereichsanfang* bzw. *DHCP-Bereichsende* angegebenen IP-Adresspool verwenden wollen (siehe unten). Setzen Sie diesen Schalter auf Nein, wenn nur statische Zuweisungen anhand der MAC-Adressen vorgenommen werden sollen (siehe unten). **Bei aktiviertem dynamischen IP-Adresspool:** Bei aktiviertem DHCP-Server und aktiviertem dynamischem IP-Adresspool können Sie die Netzwerkparameter angeben, die vom Rechner benutzt werden sollen: **DHCP-Bereichsanfang und -ende** Anfang und Ende des Adressbereichs, aus dem der DHCP-Server des mGuards den lokal angeschlossenen Rechnern IP-Adressen zuweisen soll.
	DHCP-Lease-Dauer	Zeit in Sekunden, für die eine dem Rechner zugeteilte Netzwerkkonfiguration gültig ist. Kurz vor Ablauf dieser Zeit sollte ein Client seinen Anspruch auf die ihm zugeteilte Konfiguration erneuern. Ansonsten wird diese u.U. anderen Rechnern zugeteilt.
	Lokale Netzmaske	Legt die Netzmaske der Rechner fest. Voreingestellt ist: 255.255.255.0
	Broadcast-Adresse	Legt die Broadcast-Adresse der Rechner fest.
	Standard-Gateway	Legt fest, welche IP-Adresse beim Rechner als Standard-Gateway benutzt wird. In der Regel ist das die interne IP-Adresse des mGuards.
	DNS-Server	Adresse des Servers, bei dem Rechner über den Domain Name Service (DNS) Hostnamen in IP-Adressen auflösen lassen können. Wenn der DNS-Dienst des mGuards genutzt werden soll, dann die interne IP-Adresse des mGuards angeben.
	WINS-Server	Adresse des Servers, bei dem Rechner über den Windows Internet Naming Service (WINS) Hostnamen in Adressen auflösen können.
	Statische Zuordnung [anhand der MAC-Adresse]	Die **MAC-Adresse** Ihres Rechners finden Sie wie folgt heraus: **Windows 95/98/ME**: • Starten Sie **winipcfg** in einer DOS-Box. **Windows NT/2000/XP**: • Starten Sie **ipconfig /all** in einer Eingabeaufforderung. Die MAC-Adresse wird als „Physikalische Adresse“ angezeigt. **Linux**: • Rufen Sie in einer Shell **/sbin/ifconfig** oder **ip link show** auf.

Netzwerk >> DHCP >> Internes DHCP[...]

Bei den Angaben haben Sie folgende Möglichkeiten:

– MAC-Adresse des Clients/Rechners (ohne Leerzeichen oder Bindestriche).

– IP-Adresse des Client**s**

IP-Adresse des Clients

Die statische IP-Adresse des Rechners, die der MAC-Adresse zugewiesen werden soll.

Die statischen Zuweisungen haben Vorrang vor dem dynamischen IP-Adresspool.

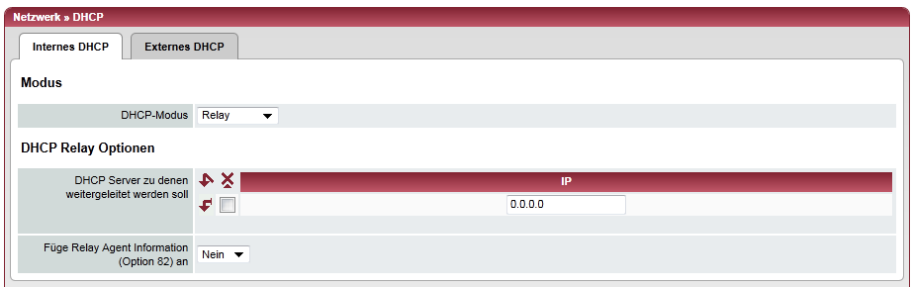
Statische Zuweisungen dürfen sich nicht mit dem dynamischen IP-Adresspool überschneiden.

Eine IP-Adresse darf nicht in mehreren statischen Zuweisungen verwendet werden, ansonsten wird diese IP-Adresse mehreren MAC-Adressen zugeordnet.

Es sollte nur ein DHCP-Server pro Subnetz verwendet werden.

DHCP-Modus **Relay**

Ist als DHCP-Modus *Relay* ausgewählt, werden unten auf der Seite entsprechende Einstellmöglichkeiten wie folgt eingeblendet.



DHCP-Relay-Optionen

Im *Stealth*-Modus des mGuards wird der DHCP-Modus *Relay* nicht unterstützt. Wird der mGuard im *Stealth*-Modus betrieben und ist der DHCP-Modus *Relay* ausgewählt, wird diese Einstellung ignoriert. Aufgrund der Natur des Stealth-Modus werden DHCP-Anfragen des Rechners und die entsprechenden Antworten jedoch durchgeleitet.

DHCP-Server, zu denen weitergeleitet werden soll

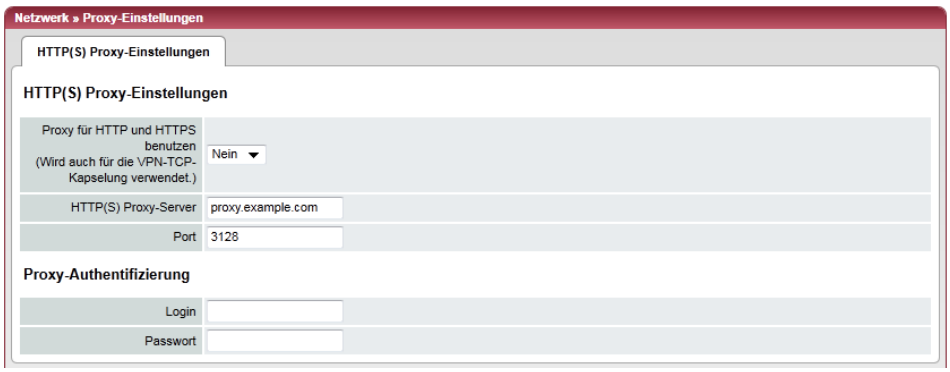
Eine Liste von einem oder mehreren DHCP-Servern, an welche DHCP-Anfragen weitergeleitet werden sollen.

Füge Relay-Agent-Information (Option 82) an

Beim Weiterleiten können zusätzliche Informationen nach RFC 3046 für die DHCP-Server angefügt werden, an welche weitergeleitet wird.

6.4.5 Netzwerk >> Proxy-Einstellungen

6.4.5.1 HTTP(S) Proxy- Einstellungen



Für folgende vom mGuard selbst ausgeführte Aktivitäten kann hier ein Proxy Server angegeben werden:

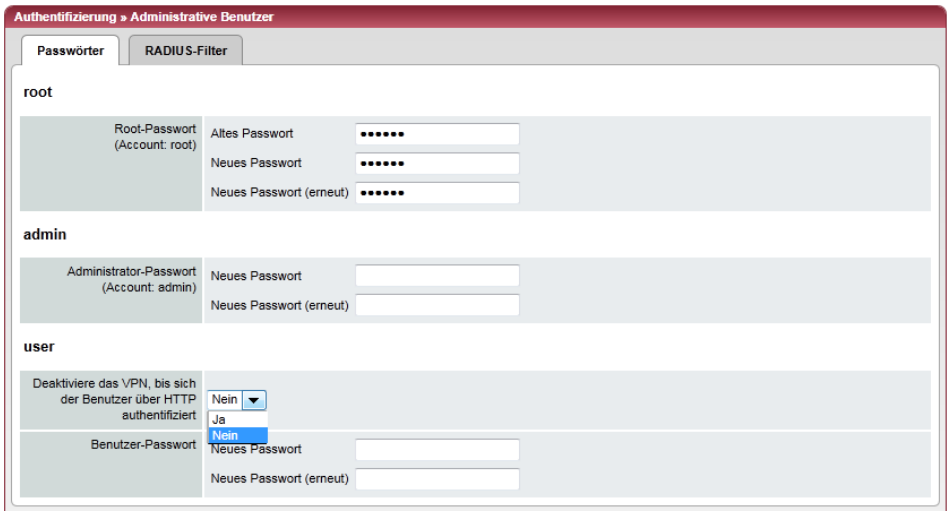
- CRL-Download
- Firmware-Update
- regelmäßiges Holen des Konfigurationsprofils von zentraler Stelle
- Wiederherstellung von Lizenzen

Netzwerk >> Proxy-Einstellungen >> HTTP(S) Proxy-Einstellungen		
HTTP(S) Proxy-Einstellungen	**Proxy für HTTP und HTTPS benutzen:**	Bei **Ja** gehen Verbindungen, bei denen das Protokoll HTTP oder HTTPS verwendet wird, über einen Proxy Server, dessen Adresse und Port in den nächsten beiden Feldern festzulegen ist.
	HTTP(S) Proxy Server	Hostname oder IP-Adresse des Proxy Servers.
	Port	Nummer des zu verwendenden Ports, z. B. 3128.
Proxy-Authentifizierung	**Login**	Benutzername zur Anmeldung beim Proxy Server.
	Passwort	Passwort zur Anmeldung beim Proxy Server.

6.5 Menü Authentifizierung

6.5.1 Authentifizierung >> Administrative Benutzer

6.5.1.1 Passwörter

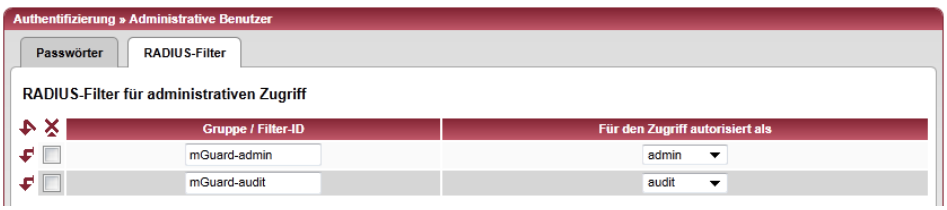


Unter *Administrative Benutzer* sind die Benutzer zu verstehen, die je nach Berechtigungsstufe das Recht haben, den mGuard zu konfigurieren (Berechtigungsstufe *Root* und *Administrator*) oder zu benutzen (Berechtigungsstufe *User*).

Authentifizierung >> Administrative Benutzer >> Passwörter		
	Um sich auf der entsprechenden Stufe anzumelden, muss der Benutzer das Passwort angeben, das der jeweiligen Berechtigungsstufe (*root*, *admin*, *user*) zugeordnet ist	
Root	**Root-Passwort (Account: root)**	Bietet vollständige Rechte für alle Parameter des mGuards. Hintergrund: Nur diese Berechtigungsstufe erlaubt unbegrenzten Zugriff auf das Dateisystem des mGuards. Benutzername (nicht änderbar): **root** Voreingestelltes Root-Passwort: **root** • Wollen Sie das Root-Passwort ändern, geben Sie ins Feld *Altes Passwort* das alte Passwort ein, in die beiden Felder darunter das neue gewünschte Passwort.
Admin	**Administrator-Passwort (Account: admin)**	Bietet die Rechte für die Konfigurationsoptionen, die über die Web-basierte Administratoroberfläche zugänglich sind. Benutzername (nicht änderbar): **admin** Voreingestelltes Passwort: **mGuard**

Authentifizierung >> Administrative Benutzer >> Passwörter [...]		
User	**Deaktiviere das VPN, bis sich der Benutzer über HTTP authentifiziert**	Ist ein Nutzerpasswort festgelegt und aktiviert, dann muss der Benutzer nach jedem Neustart des mGuards bei Zugriff auf eine beliebige HTTP URL dieses Passwort angeben, **damit die VPN-Verbindungen des mGuards aktiviert werden**. Wollen Sie diese Option nutzen, legen Sie im entsprechenden Eingabefeld das Nutzerpasswort fest. Werkseitig ist dieser Schalter auf **Nein** gesetzt. Bei **Ja** können VPN-Verbindungen erst dann genutzt werden, wenn sich ein User mittels HTTP gegenüber dem mGuard ausgewiesen hat. Alle HTTP Verbindung werden auf den mGuard umgeleitet solange die Authentifizierung erforderlich ist. Die Änderung dieser Option wird erst mit dem nächsten Neustart aktiv.
	Benutzer-Passwort	Werkseitig ist kein Benutzer-Passwort voreingestellt. Um eines festzulegen, geben Sie in beide Eingabefelder übereinstimmend das gewünschte Passwort ein.

6.5.1.2 RADIUS-Filter



Hier können Sie Gruppennamen für administrative Benutzer anlegen, deren Passwort bei einem Zugriff auf den mGuard mit Hilfe eines RADIUS-Servers überprüft wird. Sie können jeder dieser Gruppen eine administrative Rolle zuweisen.

Authentifizierung >> Administrative Benutzer >> RADIUS-Filter	
Dieser Menüpunkt gehört nicht zum Funktionsumfang vom mGuard rs2000.	Der mGuard prüft Passwörter nur dann mit Hilfe von RADIUS-Servern, wenn Sie die RADIUS-Authentifizierung aktiviert haben: – für den Shell-Zugang siehe Menü: *Verwaltung >> Systemeinstellungen >> Shell-Zugang* – über den Web-Zugriff siehe Menü: *Verwaltung >> Web-Einstellungen >> Zugriff* Die RADIUS-Filter werden nacheinander durchsucht. Bei der ersten Übereinstimmung wird der Zugriff mit der entsprechenden Rolle *(admin, netadmin, audit)* gewährt.

Authentifizierung >> Administrative Benutzer >> RADIUS-Filter [...]		
	Nachdem ein RADIUS-Server das Passwort eines Benutzers positiv geprüft hat, sendet der RADIUS-Server dem mGuard in seiner Antwort eine Liste von Filter-IDs. Diese Filter-IDs sind in einer Datenbank des Servers dem Benutzer zugeordnet. Über sie weist der mGuard die Gruppe zu und damit die Autorisierung als „admin“, „netadmin“ oder „audit“. Eine erfolgreiche Authentifizierung wird im Logging des mGuards vermerkt. Weitere Aktionen des Benutzers werden dort mit seinem ursprünglichen Namen protokolliert. Die Log-Nachrichten werden an einen Syslog-Server weitergeleitet, sofern ein Syslog-Server vom mGuard freigegeben ist. Aktionen, die festgehalten werden, sind: – Login, – Logout, – Start eines Firmware-Updates, – Ändern der Konfiguration und – das Ändern des Passwortes eines der vordefinierten Benutzer *(root, admin, netadmin, audit and user)*.	
RADIUS-Filter für den administrativen Zugriff	**Gruppe / Filter-ID**	Der Gruppenname darf nur einmal verwendet werden. Zwei Zeilen dürfen nicht denselben Wert haben. Antworten vom RADIUS-Server, die eine erfolgreiche Authentifizierung melden, müssen in ihrem Filter-ID-Attribut diesen Gruppennamen enthalten. Erlaubt sind bis zu 50 Zeichen (nur druckbare UTF-8 Zeichen) ohne Leerzeichen
	Für den Zugriff autorisiert als	Jeder Gruppe wird eine administrative Rolle zugewiesen. **admin**: Administrator **netadmin**: Administrator für das Netzwerk **audit**: Auditor/Prüfer

6.5.2 Authentifizierung >> Firewall-Benutzer

Um z. B. privates Surfen im Internet zu unterbinden, wird unter *Netzwerksicherheit* >> *Paketfilter* >> *Regelsätze* jede ausgehende Verbindung unterbunden (nicht betroffen: VPN).

Unter *Netzwerksicherheit* >> *Benutzerfirewall* können für bestimmte Firewall-Benutzer anders lautende Firewall-Regeln definiert werden, z. B. dass für diese jede ausgehende Verbindung erlaubt ist. Diese Benutzerfirewall-Regel greift, sobald sich der oder die betreffende(n) Firewall-Benutzer angemeldet haben, für die diese Benutzerfirewall-Regel gilt, siehe „Netzwerksicherheit >> Benutzerfirewall“ auf Seite 6-161.

6.5.2.1 Firewall-Benutzer

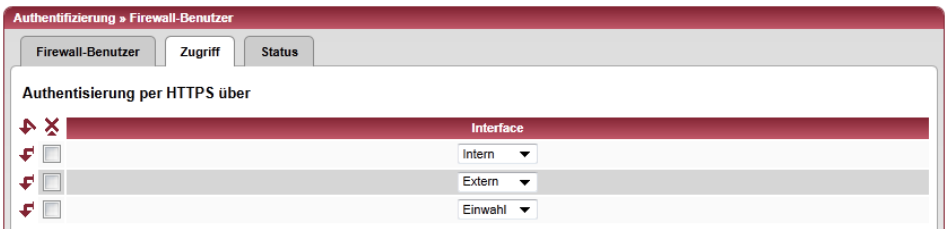
Dieses Menü steht **nicht** auf dem **mGuard rs2000** zur Verfügung.

Der **Safari-Browser** kann nicht gleichzeitig einen administrativen Zugriff über eine X.509-Authentisierung und über ein Login zur mGuard-Benutzerfirewall ermöglichen.

Authentifizierung >> Firewall-Benutzer >> Firewall-Benutzer	
Benutzer	**Listet die Firewall-Benutzer auf durch Angabe der ihnen zugeordneten Benutzernamen. Legt außerdem die Authentifizierungsmethode fest.**
	Aktiviere Benutzer-Firewall: Unter dem Menüpunkt *Netzwerksicherheit* >> *Benutzerfirewall* können Firewall-Regeln definiert werden, die dort bestimmten Firewall-Benutzern zugeordnet werden. Mit **Ja** legen Sie fest, dass die den unten aufgelisteten Benutzern zugeordneten Firewall-Regeln in Kraft gesetzt werden, sobald sich betreffende Benutzer anmelden.
	Aktiviere Gruppenauthentifizierung: Wenn aktiviert, leitet der mGuard Logins für ihn unbekannte Benutzer an den RADIUS-Server weiter. Bei Erfolg wird die Antwort des RADIUS-Servers einen Gruppennamen enthalten. Der mGuard wird dann Benutzerfirewall-Templates freischalten, die diesen Gruppennamen als Template Benutzer eingetragen haben. Der RADIUS-Server muss so konfiguriert werden, dass dieser den Gruppennamen im „Access Accept“ Paket als „Filter-ID=<gruppenname>“ Attribut mitschickt.
	Benutzername: Name, den der Benutzer bei der Anmeldung angibt.
	Authentifizierungsmethode: **Lokale DB**: Ist *Lokale DB* ausgewählt, muss in der Spalte *Benutzer-Passwort* das Passwort eingetragen werden, das dem Benutzer zugeordnet ist, und das dieser neben seinem *Benutzernamen* angeben muss, wenn er sich anmeldet. **RADIUS**: Ist RADIUS ausgewählt, kann das Passwort für den Benutzer auf dem RADIUS-Server hinterlegt werden.

Authentifizierung >> Firewall-Benutzer >> Firewall-Benutzer [...]	
Benutzer-Passwort	Nur aktiv, wenn als Authentifizierungsmethode *Lokale DB* ausgewählt ist.

6.5.2.2 Zugriff

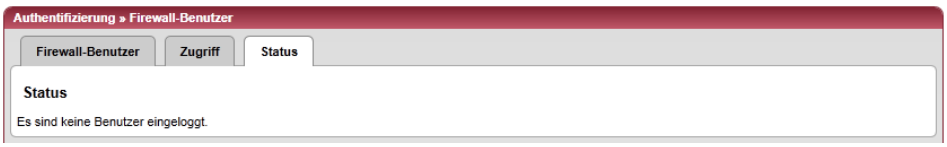


Authentifizierung >> Firewall-Benutzer >> Zugriff	
Authentifizierung über HTTPS	**ACHTUNG:** Bei Authentisierung über ein externes Interface ist Folgendes zu bedenken: Kann sich ein Firewall-Benutzer über ein „unsicheres“ Interface einloggen, könnte es passieren, dass bei einer Trennung ohne ordnungsgemäßes Ausloggen das Login bestehen bleibt und von einer anderen, nicht berechtigten Person missbraucht wird. „Unsicher“ ist das Interface z. B. dann, wenn sich ein Benutzer über das Internet einloggt von einer Stelle oder einem Rechner, der/dem die IP-Adresse vom Internet Service Provider dynamisch zugeordnet wird - wie es bei vielen Internet-Benutzern üblich ist. Kommt es während einer solchen Verbindung z. B. zu einer kurzzeitigen Zwangstrennung, weil dem eingeloggten Benutzer gerade eine andere IP-Adresse zugeordnet wird, dann muss sich dieser Benutzer neu einloggen. Das alte Login, dass er unter seiner alten IP-Adresse vollzogen hat, bleibt aber bestehen, so dass dieses Login von einem Eindringling benutzt werden könnte, der diese „alte“ IP-Adresse des rechtmäßigen Benutzers für sich verwendet und unter dieser Absender-Adresse auf den mGuard zugreift. Entsprechendes könnte auch geschehen, wenn ein (befugter) Firewall-Benutzer vergisst, sich nach der Sitzung auszuloggen. Diese Unsicherheit beim Einloggen über ein „unsicheres Interface“ wird zwar nicht grundsätzlich beseitigt, aber zeitlich eingegrenzt, indem für das verwendete Benutzerfirewall-Template das konfigurierte Timeout gesetzt ist. Siehe „Timeout-Typ“ auf Seite 6-162. **Interface** — **Extern / Intern / Extern 2 / Einwahl**[1] Gibt an, über welche mGuard-Interfaces Firewall-Benutzer sich beim mGuard anmelden können. Für das ausgewählte Interface muss Web-Zugriff über HTTPS freigeschaltet sein: Menü **Verwaltung**, **Web-Einstellungen**, Registerkarte *Zugriff* (siehe „Zugriff“ auf Seite 6-24). Im Netzwerk-Modus *Stealth* müssen sowohl das Interface **Intern** als auch das Interface **Extern** freigeschaltet werden, damit Firewall-Benutzer sich beim mGuard anmelden können. (Dazu müssen 2 Zeilen in die Tabelle aufgenommen werden.)

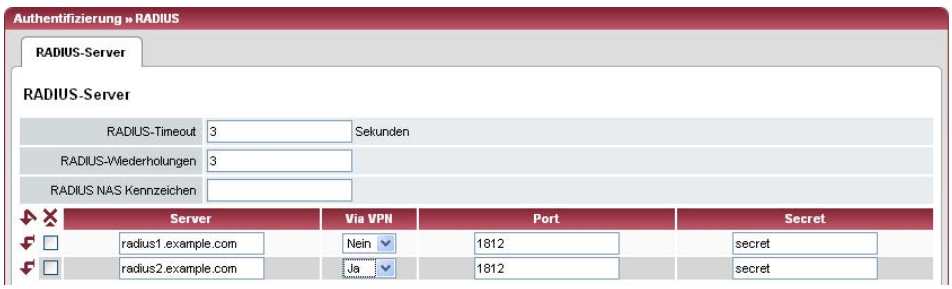
1 *Extern 2* und *Einwahl* nur bei Geräten mit serieller Schnittstelle (siehe „Netzwerk >> Interfaces“ auf Seite 6-64).

6.5.2.3 Status

Bei aktivierter Benutzerfirewall wird hier deren Status angezeigt.



6.5.3 Authentifizierung >> RADIUS-Server



Ein RADIUS-Server ist ein zentraler Authentifizierungsserver, an den sich Geräte und Dienste wenden, die die Passwörter von Benutzern prüfen lassen wollen. Diese Geräte und Dienste kennen das Passwort nicht. Das Passwort kennen nur ein oder mehrere RADIUS-Server.

Außerdem stellt der RADIUS-Server dem Gerät oder dem Dienst, auf den ein Benutzer zugreifen möchte, weitere Informationen über den Benutzer bereit, zum Beispiel seine Gruppenzugehörigkeit. Auf diese Weise lassen sich alle Einstellungen von Benutzern zentral verwalten.

Damit die RADIUS-Authentifizierung aktiv wird, müssen Sie unter *Authentifizierung* >> *Firewall-Benutzer* bei dem Unterpunkt *Aktiviere Gruppenauthentifizierung* die Auswahl **Ja** einstellen und als *Authentifizierungsmethode* den Punkt *RADIUS auswählen.*

Unter Authentifizierung >> RADIUS-Server wird eine Liste von RADIUS-Servern erstellt, die durch den mGuard verwendet wird. Diese Liste wird auch verwendet, wenn beim administrativen Zugriff (SSH/HTTPS), die RADIUS-Authentifizierung aktiviert ist.

Wenn die RADIUS-Authentifizierung aktiv ist, wird der Log-in-Versuch von einem nicht vordefinierten Benutzer (nicht: *root, admin, netadmin, audit* oder *user)* an alle hier aufgelisteten RADIUS-Server weitergeleitet. Die erste Antwort, die der mGuard von einem der RADIUS-Server erhält, entscheidet über das Gelingen des Authentifizierungsversuches.

Authentifizierung >> Radius-Server		
RADIUS-Server Dieser Menüpunkt gehört nicht zum Funktionsumfang vom mGuard rs2000.	**RADIUS-Timeout**	Legt fest (in Sekunden), wie lange der mGuard auf die Antwort des RADIUS-Servers wartet. Standard: 3 Sekunden.
	RADIUS-Wiederholungen	Legt fest, wie oft bei Überschreitung des RADIUS-Timeouts Anfragen an den RADIUS-Server wiederholt werden. Standard: 3.

Authentifizierung >> Radius-Server [...]

RADIUS NAS Kennzeichen

Mit jedem RADIUS-Request wird ein NAS-Kennzeichen (NAS-Identifier, NAS-ID) gesendet, außer wenn das Feld leer bleibt.

Sie können alle üblichen Zeichen der Tastatur als NAS-ID verwenden, mit Ausnahme der Umlaute.

Die NAS-ID ist ein RADIUS-Attribut, das der Client nutzen kann, um sich selbst beim RADIUS-Server zu identifizieren. Die NAS-ID kann anstelle einer IP-Adresse genutzt werden, um den Clienten zu identifzieren. Sie muss einzigartig im Bereich des RADIUS-Servers sein.

Server

Name des RADIUS-Servers oder dessen IP-Adresse

Wir empfehlen, wenn möglich IP-Adressen statt Namen als Server anzugeben. Sonst muss der mGuard zuerst die Namen auflösen, bevor er Authentifizierungsanfragen an den RADIUS-Server senden kann. Dies kostet beim Einloggen Zeit. Außerdem kann unter Umständen keine Authentifizierung stattfinden, wenn eine Namensauflösung fehl schlägt, weil z. B. der DNS nicht erreichbar ist oder der Name im DNS gelöscht wurde.

Via VPN

Bei **Ja** wird die Authentifizierungsanfrage des mGuards immer dann über einen verschlüsselten VPN-Tunnel gesendet, wenn ein passender verfügbar ist.

Bei **Nein** wird eine solche Anfrage immer unverschlüsselt außerhalb des VPNs gesendet.

Wenn unter **Via VPN** die Auswahl **Ja** getroffen worden ist, dann unterstützt der mGuard Anfragen von einem RADIUS-Server über seine VPN-Verbindung. Dies passiert automatisch immer dann, wenn der RADIUS-Server zum Remote-Netzwerk eines konfigurierten VPN-Tunnels gehört und der mGuard eine interne IP-Adresse hat, die zum lokalen Netzwerk desselben VPN-Tunnels gehört. Dadurch wird die Authentifizierungsanfrage abhängig von der Verfügbarkeit eines VPN-Tunnels.

Achten Sie beim Konfigurieren darauf, dass nicht der Ausfall eines einzigen VPN-Tunnels den administrativen Zugang zum mGuard unmöglich macht.

Port

Vom RADIUS-Server benutze Port-Nummer

Authentifizierung >> Radius-Server [...]

Secret

RADIUS-Server-Passwort

Dieses Passwort muss dasselbe wie beim mGuard sein. Der mGuard nutzt dieses Passwort, um Nachrichten mit dem RADIUS-Server auszutauschen und das Benutzerpasswort zu verschlüsseln. Das RADIUS-Server-Passwort wird nicht im Netzwerk übertragen.

Das Passwort ist wichtig für die Sicherheit, da der mGuard an dieser Stelle durch zu schwache Passwörter angreifbar wird. Wir empfehlen ein Passwort mit mindestens 32 Zeichen und vielen Sonderzeichen zu verwenden. Es muss regelmäßig erneuert werden.

Wenn das RADIUS-Secret aufgedeckt wird, kann der Angreifer das Benutzer-Passwort der RADIUS-Authentifizierungs-Anfragen lesen. Der Angreifer kann außerdem RADIUS-Antworten fälschen und sich Zugang zum mGuard verschaffen, wenn er die Benutzernamen kennt. Diese Benutzernamen werden als Klartext mit der RADIUS-Anfrage übertragen. Der Angreifer kann also RADIUS-Anfragen vortäuschen und auf diese Weise Benutzernamen und dazugehörige Passwörter herausfinden.

Während der Erneuerung des RADIUS-Server-Passwortes soll der administrative Zugriff auf den mGuard möglich bleiben. Damit das gewährleistet ist, gehen Sie so vor:

- Richten Sie den RADIUS-Server beim mGuard ein zweites Mal mit einem neuen Passwort ein.
- Stellen Sie dieses neue Passwort ebenfalls beim RADIUS-Server ein.
- Löschen Sie beim mGuard die Zeile mit dem alten Passwort.

6.5.4 Authentifizierung >> Zertifikate

Der Nachweis und die Prüfung der Authentizität, Authentifizierung genannt, ist grundlegendes Element einer sicheren Kommunikation. Beim X.509-Authentifizierungsverfahren wird anhand von Zertifikaten sichergestellt, dass wirklich die „richtigen“ Partner kommunizieren und kein „falscher“ dabei ist. Falsch wäre ein Kommunikationspartner dann, wenn er vorgibt, jemand zu sein, der er in Wirklichkeit gar nicht ist, siehe Glossar unter „X.509-Zertifikat“.

Zertifikat

Ein Zertifikat dient dem Zertifikatsinhaber als Bescheinigung dafür, dass er der ist, für den er sich ausgibt. Die bescheinigende, beglaubigende Instanz dafür ist die CA (Certificate Authority). Von ihr stammt die Signatur (= elektronische Unterschrift) auf dem Zertifikat, mit der die CA bescheinigt, dass der rechtmäßige Inhaber des Zertifikats einen privaten Schlüssel besitzt, der zum öffentlichen Schlüssel im Zertifikat passt.

Der Name des Ausstellers eines Zertifikats wird im Zertifikat als *Issuer* aufgeführt, der Name des Inhabers eines Zertifikats als *Subject*.

Selbst signierte Zertifikate

Ist ein Zertifikat nicht von einer CA (Certificate Authority) signiert, sondern vom Zertifikatsinhaber selber, spricht man von einem selbst signierten Zertifikat. In selbst signierten Zertifikaten wird der Name des Zertifikatsinhabers sowohl als *Issuer* als auch als *Subject* aufgeführt.

Selbst signierte Zertifikate werden benutzt, wenn die Kommunikationspartner den Vorgang der X.509-Authentifizierung verwenden wollen oder müssen, ohne ein offizielles Zertifikat zu haben oder zu benutzen. Diese Art der Authentifizierung sollte aber nur unter Kommunikationspartnern Verwendung finden, die sich „gut kennen“ und deswegen vertrauen. Sonst sind solche Zertifikate unter dem Sicherheitsaspekt genauso wertlos wie z. B. selbst erstellte Ausweispapiere, die keinen Behördenstempel tragen.

Zertifikate werden von kommunizierenden Maschinen / Menschen bei der Verbindungsaufnahme einander „vorgezeigt“, sofern zur Verbindungsaufnahme die X.509-Authentifizierung verwendet wird. Beim mGuard können das die folgenden Anwendungen sein:

– Authentifizierung der Kommunikationspartner bei der Herstellung von VPN-Verbindungen (siehe „IPsec VPN >> Verbindungen“ auf Seite 6-189, „Authentifizierung“ auf Seite 6-204).
– Verwaltung des mGuards per SSH (Shell Zugang) (siehe „Verwaltung >> Systemeinstellungen“ auf Seite 6-4, „Shell-Zugang“ auf Seite 6-12).
– Verwaltung des mGuards per HTTPS (siehe „Verwaltung >> Web-Einstellungen“ auf Seite 6-23, „Zugriff“ auf Seite 6-24)

Zertifikat, Maschinenzertifikat

Mit Zertifikaten kann man sich gegenüber anderen ausweisen (sich authentisieren). Das Zertifikat, mit dem sich der mGuard gegenüber anderen ausweist, soll hier, der Terminologie von Microsoft Windows folgend, „Maschinenzertifikat“ genannt werden.

Wird ein Zertifikat von einem Menschen benutzt, um sich gegenüber Gegenstellen zu authentisieren (z. B. von einem Menschen, der per HTTPS und Web-Browser auf den mGuard zwecks Fernkonfiguration zugreifen will), spricht man einfach von Zertifikat, personenbezogenem Zertifikat oder Benutzerzertifikat, das dieser Mensch „vorzeigt“. Ein solches personenbezogenes Zertifikat kann z. B. auch auf einer Chipkarte gespeichert sein und von dessen Inhaber bei Bedarf in den Kartenleser seines Rechners gesteckt werden, wenn der Web-Browser bei der Verbindungsherstellung dazu auffordert.

Gegenstellen-Zertifikat

Ein Zertifikat wird also von dessen Inhaber (Mensch oder Maschine) wie ein Ausweis benutzt, nämlich um zu beweisen, dass er/sie wirklich der/die ist, für den er/sie sich ausgibt. Weil es bei einer Kommunikation mindestens zwei Partner gibt, geschieht das wechselweise: Partner A zeigt sein Zertifikat seiner Gegenstelle Partner B vor. Im Gegenzug zeigt Partner B zeigt sein Zertifikat seiner Gegenstelle Partner A vor.

Damit A das ihm von B vorgezeigte Zertifikat, also das Zertifikat seiner Gegenstelle, akzeptieren und die Kommunikation mit B erlauben kann, gibt es folgende Möglichkeit: A hat zuvor von B eine Kopie des Zertifikats erhalten (z. B. per Datenträger oder E-Mail), mit dem sich B bei A ausweisen wird. Anhand eines Vergleiches mit dieser Kopie kann A dann erkennen, dass das von B vorgezeigte Zertifikat zu B gehört. Die Kopie des Zertifikats, das in diesem Beispiel Partner B an A übergeben hatte, nennt man (auf die Oberfläche des mGuards bezogen) *Gegenstellen-Zertifikat*.

Damit die wechselseitige Authentifizierung gelingen kann, müssen also zuvor beide Partner sich gegenseitig die Kopie ihres Zertifikats, mit dem sie sich ausweisen werden, einander übergeben. Dann installiert A die Kopie des Zertifikats von B bei sich als Gegenstellen-Zertifikat. Und B installiert die Kopie des Zertifikats von A bei sich als Gegenstellen-Zertifikat.

Als Kopie eines Zertifikats auf keinen Fall die PKCS#12-Datei (Dateinamen-Erweiterung *.p12) nehmen und eine Kopie davon der Gegenstelle geben, um eine spätere Kommunikation per X.509-Authentifizierung mit ihr zu ermöglichen! Denn die PKCS#12-Datei enthält auch den privaten Schlüssel, der nicht aus der Hand gegeben werden darf (siehe „Erstellung von Zertifikaten“ auf Seite 6-130).

Um eine Kopie eines in den mGuard importierten Maschinenzertifikats zu erstellen, können Sie wie folgt vorgehen:

- Auf der Registerkarte Maschinenzertifikate beim betreffenden Maschinen-zertifikat neben dem Zeilentitel *Zertifikat herunterladen* auf die Schaltfläche **Aktuelle Zertifikatsdatei** klicken (siehe „Maschinenzertifikate“ auf Seite 6-136).

CA-Zertifikate

Das von einer Gegenstelle vorgezeigte Zertifikat kann vom mGuard auch anders überprüft werden als durch Heranziehung des lokal auf dem mGuard installierten Gegenstellen-Zertifikats. Die nachfolgend beschriebene Möglichkeit wird je nach Anwendung statt dessen oder ergänzend verwendet, um gemäß X.509 die Authentizität von möglichen Gegenstellen zu überprüfen: durch das Heranziehen von CA-Zertifikaten.

CA-Zertifikate geben ein Mittel in die Hand, überprüfen zu können, ob das von einer Gegenstelle gezeigte Zertifikat wirklich von der CA signiert ist, die im Zertifikat dieser Gegenstelle angegeben ist.

Ein CA-Zertifikat kann von der betreffenden CA (Certificate Authority) in Dateiform zur Verfügung gestellt werden (Dateinamen-Erweiterung *.cer, *.pem oder *.crt), z. B. frei herunterladbar von der Webseite der betreffenden CA.

Anhand von in den mGuard geladenen CA-Zertifikaten kann der mGuard also überprüfen, ob das „vorgezeigte“ Zertifikat einer Gegenstelle vertrauenswürdig ist. Es müssen aber dem mGuard alle CA-Zertifikate verfügbar gemacht werden, um mit dem von der Gegenstelle vorgezeigten Zertifikat eine Kette zu bilden: neben dem CA-Zertifikat der CA, deren Signatur im zu überprüfenden, von der Gegenstelle vorgezeigten Zertifikat steht, auch das CA-Zertifikat der ihr übergeordneten CA usw. bis hin zum Root-Zertifikat (siehe im Glossar unter CA-Zertifikat).

Die Authentifizierung anhand von CA-Zertifikaten macht es möglich, den Kreis möglicher Gegenstellen ohne Verwaltungsaufwand zu erweitern, weil nicht für jede mögliche Gegenstelle deren Gegenstellen-Zertifikat installiert werden muss.

Erstellung von Zertifikaten

Für die Erstellung eines Zertifikats wird zunächst ein *privater Schlüssel* und der dazu gehörige *öffentliche Schlüssel* benötigt. Zum Erstellen dieser Schlüssel gibt es Programme, mit denen das jeder selbst tun kann. Ein zugehöriges Zertifikat mit dem zugehörigen *öffentlichen Schlüssel* kann man sich ebenfalls selbst erzeugen, wenn ein selbst signiertes Zertifikat entstehen soll. (Hinweise zum Selbstausstellen gibt ein Dokument, welches von der Webseite www.innominate.com aus dem Download-Bereich heruntergeladen werden kann. Es ist als Application Note unter dem Titel „How to obtain X.509 certificates“ veröffentlicht.)

Ein zugehöriges von einer CA (Certificate Authority) signiertes Zertifikat muss bei einer CA beantragt werden.

Damit der private Schlüssel zusammen mit dem zugehörigen Zertifikat in den mGuard importiert werden können, müssen diese Bestandteile in eine sogenannte PKCS#12-Datei (Dateinamen-Erweiterung *.p12) eingepackt werden.

Authentifizierungsverfahren

Bei X.509-Authentifizierungen kann der mGuard zwei prinzipiell unterschiedliche Verfahren anwenden.

– Die Authentifizierung einer Gegenstelle erfolgt auf Basis von Zertifikat und Gegenstellen-Zertifikat. In diesem Fall muss z. B. bei VPN-Verbindungen für jede einzelne Verbindung angegeben werden, welches Gegenstellen-Zertifikat herangezogen werden soll.
– Der mGuard zieht die ihm verfügbar gemachten CA-Zertifikate heran, um zu prüfen, ob das von der Gegenstelle ihm vorgezeigte Zertifikat echt ist. Dazu müssen dem mGuard alle CA-Zertifikate verfügbar gemacht werden, um mit dem von der Gegenstelle vorgezeigten Zertifikat eine Kette zu bilden, bis hin zum Root-Zertifikat.

„Verfügbar machen“ bedeutet, dass die betreffenden CA-Zertifikate im mGuard installiert sein müssen (siehe „CA-Zertifikate“ auf Seite 6-138) und zusätzlich bei der Konfiguration der betreffenden Anwendung (SSH, HTTPS, VPN) referenziert werden müssen.

Ob die beiden Verfahren alternativ oder kombiniert zu verwenden sind, wird bei VPN, SSH und HTTPS unterschiedlich gehandhabt.

Einschränkung Safari-Browser

Beachten Sie bei einem administrativer Zugriff zum mGuard mit dem **Safari Browser** über ein X.509-Zertifikat, dass alle Sub-CA-Zertifikate im Truststore des Browsers installiert seien müssen.

Authentifizierung bei SSH

Die Gegenstelle zeigt vor:	Zertifikat (personenbezogen) von **CA signiert**	Zertifikat (personenbezogen) **selbst signiert**
Der mGuard authentifiziert die Gegenstelle anhand von...		
	... allen CA-Zertifikaten, die mit dem von der Gegenstelle vorgezeigten Zertifikat die Kette bis zum Root-CA-Zertifikat bilden ggf. PLUS Gegenstellen-Zertifikaten, **wenn** sie als Filter verwendet werden.[1]	Gegenstellen-Zertifikat

1 (Siehe „Verwaltung >> Systemeinstellungen“ auf Seite 6-4, „Shell-Zugang“ auf Seite 6-12)

Authentifizierung bei HTTPS

Die Gegenstelle zeigt vor:	Zertifikat (personenbezogen) von **CA signiert**[1]	Zertifikat (personenbezogen) **selbst signiert**
Der mGuard authentifiziert die Gegenstelle anhand von...		
	...allen CA-Zertifikaten, die mit dem von der Gegenstelle vorgezeigtem Zertifikat die Kette bis zum Root-CA-Zertifikat bilden ggf. PLUS Gegenstellen-Zertifikaten, **wenn** sie als Filter verwendet werden.[2]	Gegenstellen-Zertifikat

1 Die Gegenstelle kann zusätzlich Sub-CA-Zertifikate anbieten. In diesem Fall kann der mGuard mit den angebotenen CA-Zertifikaten und den bei ihm selber konfigurierten CA-Zertifikaten die Vereinigungsmenge bilden, um die Kette zu bilden. Auf jeden Fall muss aber das zugehörige Root-CA-Zertifikat auf dem mGuard zur Verfügung stehen.

2 (Siehe „Verwaltung >> Web-Einstellungen“ auf Seite 6-23, „Zugriff“ auf Seite 6-24)

Authentifizierung bei VPN

Die Gegenstelle zeigt vor:	Maschinenzertifikat von **CA signiert**	Maschinenzertifikat **selbst signiert**
Der mGuard authentifiziert die Gegenstelle anhand von...		
	Gegenstellen-Zertifikat oder allen CA-Zertifikaten, die mit dem von der Gegenstelle vorgezeigten Zertifikat die Kette bis zum Root-CA-Zertifikat bilden	Gegenstellen-Zertifikat

ACHTUNG: Es reicht nicht aus, beim mGuard unter *Authentifizierung* >> *Zertifikate* die zu verwendenden Zertifikate zu installieren. Zusätzlich muss bei den jeweiligen Anwendungen (VPN, SSH, HTTPS) referenziert werden, welche aus dem Pool der in den mGuard importierten Zertifikate jeweils verwendet werden sollen.

Das Gegenstellen-Zertifikat für das Authentifizieren einer VPN-Verbindung (bzw. der Kanäle einer VPN-Verbindung) wird im Menü *IPsec VPN* >> *Verbindungen* installiert.

6.5.4.1 Zertifikatseinstellungen

Authentifizierung >> Zertifikate >> Zertifikatseinstellungen

Zertifikatseinstellungen

Die hier vollzogenen Einstellungen beziehen sich auf alle Zertifikate und Zertifikatsketten, die der mGuard prüfen soll.

Generell ausgenommen davon:

– Selbst signierte Zertifikate von Gegenstellen
– bei VPN alle Gegenstellen-Zertifikate

Beachte den Gültigkeitszeitraum von Zertifikaten und CRLs

Nein: Angaben in Zertifikaten und CRLs über deren Gültigkeitszeitraum werden vom mGuard ignoriert.

Warte auf Synchronisation der Systemzeit

Der in Zertifikaten und CRLs angegebene Gültigkeitszeitraum wird vom mGuard erst dann beachtet, wenn dem mGuard die aktuelle Zeit (Datum und Uhrzeit) bekannt ist, entweder

– durch die eingebaute Uhr (bei *mGuard rs4000/2000, mGuard centerport, mGuard industrial rs*, *mGuard delta* und bei *mGuard smart²*, aber nicht bei *mGuard smart*) oder
– durch Synchronisierung der Systemzeit (siehe „Zeit und Datum“ auf Seite 6-8).

Bis zu diesem Zeitpunkt werden alle zu prüfenden Zertifikate sicherheitshalber als ungültig erachtet.

Authentifizierung >> Zertifikate >> Zertifikatseinstellungen [...]

CRL-Prüfung einschalten

Bei **Ja**: Bei eingeschalteter CRL-Prüfung zieht der mGuard die CRL (Certificate Revocation Liste = Zertifikats-Sperrliste) heran und prüft, ob die dem mGuard vorliegenden Zertifikate gesperrt sind oder nicht.

CRLs werden von den CAs herausgegeben und enthalten die Seriennummern von Zertifikaten, die gesperrt sind, z. B. weil sie als gestohlen gemeldet worden sind.

Auf der Registerkarte **CRL** (siehe „CRL“ auf Seite 6-142) geben Sie an, von wo der mGuard die Sperrlisten bekommt....

Bei eingeschalteter CRL-Prüfung ist es notwendig, dass zu jedem *Issuer* von Zertifikaten im mGuard eine CRL konfiguriert sein muss. Fehlende CRLs führen dazu, dass Zertifikate als ungültig betrachtet werden.

Sperrlisten werden mit Hilfe eines entsprechenden CA-Zertifikats vom mGuard auf Echtheit geprüft. Darum müssen alle zu einer Sperrliste gehörenden CA-Zertifikate (alle Sub-CA-Zertifikate und das Root-Zertifikat) auf dem mGuard importiert sein. Ist die Echtheit einer Sperrliste nicht prüfbar, wird sie vom mGuard so behandelt, als wäre sie nicht vorhanden.

Ist die Verwendung von Sperrlisten aktiviert und zusätzlich die Beachtung ihrer Gültigkeitszeiträume aktiviert, gelten Sperrlisten als nicht vorhanden, wenn ihre Gültigkeit laut Systemzeit abgelaufen oder noch nicht eingetreten ist.

CRL-Download-Intervall

Ist *CRL-Prüfung einschalten* auf **Ja** gesetzt (s. o.), wählen Sie hier aus, nach welchen Zeitabständen die Sperrlisten heruntergeladen und in Kraft gesetzt werden sollen.

Auf der Registerkarte **CRL** (siehe „CRL“ auf Seite 6-142) geben Sie an, von wo der mGuard die Sperrlisten bekommt.

Ist die CRL-Prüfung eingeschaltet, der CRL-Download aber auf **Nie** gesetzt, muss die CRL manuell in den mGuard geladen worden sein, damit die CRL-Prüfung gelingen kann.

6.5.4.2 Maschinenzertifikate

Mit einem Maschinenzertifikat, das in den mGuard geladen ist, authentisiert sich dieser mGuard bei der Gegenstelle. Das Maschinenzertifikat ist sozusagen der Personalausweis eines mGuards, mit dem er sich bei der jeweiligen Gegenstelle ausweist.

Weitere Erläuterungen siehe „Authentifizierung >> Zertifikate“ auf Seite 6-128.

Durch das Importieren einer PKCS#12-Datei erhält der mGuard einen privaten Schlüssel und das dazu gehörige Maschinenzertifikat. Es können mehrere PKCS#12-Dateien in den mGuard geladen werden, so dass der mGuard bei unterschiedlichen Verbindungen jeweils das gewünschte selbst signierte oder von einer CA signierte Maschinenzertifikat verwenden kann, um es der Gegenstelle vorzuzeigen.

Zur Verwendung eines an dieser Stelle installierten Maschinenzertifikats muss bei der Konfiguration von Anwendungen (SSH, VPN) **zusätzlich** auf dieses Maschinenzertifikat referenziert werden, um es für die jeweilige Verbindung bzw. die jeweilige Fernzugriffsart zu benutzen.

Beispiel für importierte Maschinenzertifikate:

Authentifizierung >> Zertifikate >> Maschinenzertifikate	
Maschinenzertifikate	**Zeigt die aktuell importierten X.509-Zertifikate an, mit dem sich der mGuard gegenüber Gegenstellen, z. B. anderen VPN-Gateways, ausweist.**

Um ein (neues) Zertifikat zu importieren, gehen Sie wie folgt vor:

Neues Maschinenzertifikat importieren

Voraussetzung:

Die PKCS#12 (Dateiname = *.p12 oder *.pfx) ist auf dem angeschlossenen Rechner gespeichert.

Gehen Sie wie folgt vor:

- Klicken Sie auf **Durchsuchen...** , um die Datei zu selektieren
- Geben Sie in das Feld *Passwort* das Passwort ein, mit dem der private Schlüssel der PKCS#12-Datei geschützt ist.
- Klicken Sie auf **Importieren**.

  Nach dem Import ist unter *Zertifikat* das geladene Zertifikat zu sehen.
- Vergessen Sie nicht, das importierte Zertifikat samt der anderen Eingaben durch einen Klick auf die Schaltfläche **Übernehmen** abzuspeichern.

Kurzname

Beim Importieren eines Maschinenzertifikats wird das CN-Attribut aus dem Subject-Feld des Zertifikats hier als Kurzname vorgeschlagen, sofern das Feld *Kurzname* bis jetzt leer ist. Dieser Name kann übernommen oder frei geändert werden.

- Sie müssen einen Namen vergeben, den vorgeschlagenen oder einen anderen. Und Namen müssen eindeutig sein, dürfen also nicht doppelt vergeben werden.

Verwendung des Kurznamens:

Bei der Konfiguration

– von SSH (Menü *Verwaltung >> Systemeinstellungen , Shell-Zugang*),
– von HTTPS (Menü *Verwaltung >> Web-Einstellungen , Zugriff*) und
– von VPN-Verbindungen (Menü *IPsec VPN >> Verbindungen*)

werden die in den mGuard importierten Zertifikate per Auswahlliste angeboten.

In dieser werden die Zertifikate jeweils unter dem Kurznamen angezeigt, den Sie hier auf dieser Seite den einzelnen Zertifikaten geben.

Darum ist eine Namensvergabe zwingend erforderlich.

Zertifikats-Kopie erstellen

Aus dem importierten Maschinenzertifikat können Sie eine Kopie erzeugen (z. B. für die Gegenstelle, so dass diese den mGuard damit authentifizieren kann). Diese Kopie enthält nicht den privaten Schlüssel und ist deshalb unbedenklich.

Gehen Sie dazu wie folgt vor:

- Beim betreffenden Maschinenzertifikat neben dem Zeilentitel *Zertifikat herunterladen* auf die Schaltfläche **Aktuelle Zertifikatsdatei** klicken.
- Im sich daraufhin öffnenden Dialogfeld die gewünschten Angaben machen.

6.5.4.3 CA-Zertifikate

CA-Zertifikate sind Zertifikate von Zertifizierungsstellen (CA). CA-Zertifikate dienen dazu, die von Gegenstellen vorgezeigten Zertifikate auf Echtheit zu überprüfen.

Die Überprüfung geschieht wie folgt: Im von der Gegenstelle übertragenen Zertifikat ist der Zertifikatsaussteller (CA) als Issuer angegeben. Diese Angabe kann mit dem lokal vorliegenden CA-Zertifikat von dem selben Issuer auf Echtheit überprüft werden. Weitere Erläuterungen siehe „Authentifizierung >> Zertifikate“ auf Seite 6-128.

Beispiel für importierte CA-Zertifikate:

Authentifizierung >> Zertifikate >> CA-Zertifikate	
Vertauenswürdige CA-Zertifikate	**Zeigt die aktuell importierten CA-Zertifikate an.**

Um ein (neues) Zertifikat zu importieren, gehen Sie wie folgt vor:

CA-Zertifikat importieren

Voraussetzung:

Die Datei (Dateinamen-Erweiterung *.cer, *.pem oder *.crt) ist auf dem angeschlossenen Rechner gespeichert.

Gehen Sie wie folgt vor:

- Klicken Sie auf **Durchsuchen...** , um die Datei zu selektieren
- Klicken Sie auf **Importieren** .
  Nach dem Import ist unter *Zertifikat* das geladene Zertifikat zu sehen.
- Vergessen Sie nicht, das importierte Zertifikat samt der anderen Eingaben durch einen Klick auf die Schaltfläche **Übernehmen** abzuspeichern.

Kurzname

Beim Importieren eines CA-Zertifikats wird das CN-Attribut aus dem Subject-Feld des Zertifikats hier als Kurzname vorgeschlagen, sofern das Feld Kurzname bis jetzt leer ist. Dieser Name kann übernommen oder frei geändert werden.

- Sie müssen einen Namen vergeben, den vorgeschlagenen oder einen anderen. Und Namen müssen eindeutig sein, dürfen also nicht doppelt vergeben werden.

Verwendung des Kurznamens:

Bei der Konfiguration

– von SSH (Menü *Verwaltung >> Systemeinstellungen , Shell-Zugang*),
– von HTTPS (Menü *Verwaltung >> Web-Einstellungen , Zugriff*) und
– von VPN-Verbindungen (Menü *IPsec VPN >> Verbindungen*)

werden die in den mGuard importierten Zertifikate per Auswahlliste angeboten. In dieser werden die Zertifikate jeweils unter dem Kurznamen angezeigt, den Sie hier auf dieser Seite den einzelnen Zertifikaten geben. Eine Namensvergabe ist also zwingend erforderlich.

Zertifikats-Kopie erstellen

Aus dem importierten CA-Zertifikat können Sie eine Kopie erzeugen.

Gehen Sie dazu wie folgt vor:

- Beim betreffenden CA-Zertifikat neben dem Zeilentitel *Zertifikat herunterladen* auf die Schaltfläche **Aktuelle Zertifikatsdatei** klicken. Im sich daraufhin öffnenden Dialogfeld die gewünschten Angaben machen.

6.5.4.4 Gegenstellen-Zertifikate

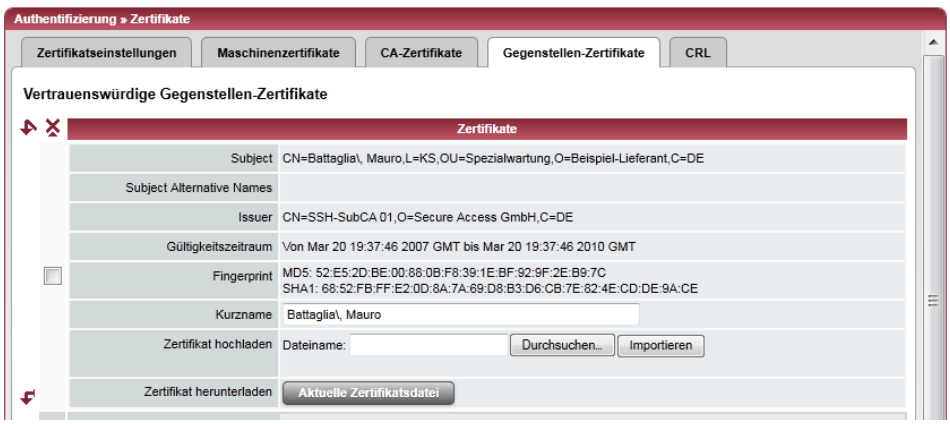
Ein Gegenstellen-Zertifikat ist die Kopie des Zertifikats, mit dem sich eine Gegenstelle beim mGuard ausweist.

Gegenstellen-Zertifikate haben Sie von Bedienern möglicher Gegenstellen auf vertrauenswürdigem Wege als Datei (Dateinamen-Erweiterung *.cer, *.pem oder *.crt) erhalten. Diese Datei laden Sie in den mGuard, damit die wechselseitige Authentifizierung gelingen kann. Es können die Gegenstellen-Zertifikate mehrerer möglicher Gegenstellen geladen werden.

Das Gegenstellen-Zertifikat für das Authentifizieren einer VPN-Verbindung (bzw. der Kanäle einer VPN-Verbindung) wird im Menü *IPsec VPN* >> *Verbindungen* installiert.

Weitere Erläuterungen siehe „Authentifizierung >> Zertifikate“ auf Seite 6-128.

Beispiel für importierte Gegenstellen-Zertifikate:



Authentifizierung >> Zertifikate >> Gegenstellen-Zertifikate

Vertauenswürdige Gegenstellen-Zertifikate	**Zeigt die aktuell importierten Gegenstellen-Zertifikate an.**

Neues Zertifikat importieren

Voraussetzung:

Die Datei (Dateinamen-Erweiterung *.cer, *.pem oder *.crt) ist auf dem angeschlossenen Rechner gespeichert.

Gehen Sie wie folgt vor:

- Klicken Sie auf **Durchsuchen...** , um die Datei zu selektieren
- Klicken Sie auf **Importieren** .
  Nach dem Import ist unter *Zertifikat* das geladene Zertifikat zu sehen.
- Vergessen Sie nicht, das importierte Zertifikat samt der anderen Eingaben durch einen Klick auf die Schaltfläche **Übernehmen** abzuspeichern.

Kurzname

Beim Importieren eines Gegenstellen-Zertifikats wird das CN-Attribut aus dem Subject-Feld des Zertifikats hier als Kurzname vorgeschlagen, sofern das Feld *Kurzname* bis jetzt leer ist. Dieser Name kann übernommen oder frei geändert werden.

- Sie müssen einen Namen vergeben, den vorgeschlagenen oder einen anderen. Und Namen müssen eindeutig sein, dürfen also nicht doppelt vergeben werden.

Verwendung des Kurznamens:

Bei der Konfiguration

– von SSH (Menü *Verwaltung >> Systemeinstellungen , Shell-Zugang*) und
– von HTTPS (Menü *Verwaltung >> Web-Einstellungen , Zugriff*)

werden die in den mGuard importierten Zertifikate per Auswahlliste angeboten. In dieser werden die Zertifikate jeweils unter dem Kurznamen angezeigt, den Sie hier auf dieser Seite den einzelnen Zertifikaten geben.

Eine Namensvergabe ist also zwingend erforderlich.

Zertifikats-Kopie erstellen

Aus dem importierten Gegenstellen-Zertifikat können Sie eine Kopie erzeugen.

Gehen Sie dazu wie folgt vor:

- Beim betreffenden Gegenstellen-Zertifikat neben dem Zeilentitel *Zertifikat herunterladen* auf die Schaltfläche **Aktuelle Zertifikatsdatei** klicken. Im sich daraufhin öffnenden Dialogfeld die gewünschten Angaben machen.

6.5.4.5 CRL

Authentifizierung >> Zertifikate >> CRL

CRL

CRL - Certificate Revocation List = Zertifikats-Sperrliste.

Die CRL ist eine Liste mit den Seriennummern gesperrter Zertifikate. Diese Seite dient zur Konfiguration der Stellen, von denen der mGuard CRLs herunterladen soll, um sie verwenden zu können.

Zertifikate werden nur dann auf Sperrung geprüft, wenn auch der Schalter **CRL-Prüfung einschalten** auf **Ja** gesetzt ist (siehe „Zertifikatseinstellungen“ auf Seite 6-134).

Zu jedem Issuer-Namen, der in zu prüfenden Zertifikaten angegeben wird, muss eine CRL mit dem selben Issuer-Namen vorhanden sein. Fehlt eine solche CRL, dann wird bei eingeschalteter CRL-Prüfung das zu prüfende Zertifikat als ungültig betrachtet.

Issuer

Information, die der mGuard direkt aus der CRL liest:

Zeigt den Aussteller der betreffenden Zertifikats-Sperrliste (Certificate Revocation Liste - CRL).

Letztes Update

Information, die der mGuard direkt aus der CRL liest:

Zeit und Datum der Ausstellung der aktuell auf dem mGuard vorhandenen CRL.

Nächstes Update

Information, die der mGuard direkt aus der CRL liest:

Zeit und Datum des Zeitpunktes, zu dem die CA voraussichtlich eine neue CRL veröffentlichen wird.

Diese Angabe wird weder vom CRL-Download-Intervall beeinflusst noch berücksichtigt.

URL

Wenn auf der Registerkarte *Zertifikatseinstellungen* (siehe „Zertifikatseinstellungen“ auf Seite 6-134) unter **CRL-Download-Intervall** festgelegt ist, dass die CRL regelmäßig neu heruntergeladen werden soll, dann geben Sie hier die URL der CA an, von der der Download von deren CRL stattfinden kann.

Herunterladen durch VPN wenn möglich

Bei **Ja** greift der mGuard durch einen VPN-Tunnel auf die URL zu, die die CRL zum Download bereitstellt. Dazu muss ein passender VPN-Tunnel konfiguriert und aktiv sein und den Zugang erlauben. Sonst werden die CRL-Downloads dieser URL nicht durch einen VPN-Tunnel weitergeleitet.

Authentifizierung >> Zertifikate >> CRL

Hochladen

Falls die CRL als Datei vorliegt, kann sie auch manuell in den mGuard geladen werden.

- Dazu auf die Schaltfläche **Durchsuchen...** klicken, die Datei selektieren und dann auf **Importieren** klicken.
- Vergessen Sie nicht, das die importierte CRL samt der anderen Eingaben durch einen Klick auf die Schaltfläche Übernehmen abzuspeichern.

Es muss immer eine aktuelle CRL-Datei verwendet werden. Deshalb gehört sie nicht zur mGuard-Konfiguration.

Wenn Sie eine mGuard-Konfiguration exportieren und anschießend auf einem anderen mGuard importieren, müssen Sie die zugehörige CRL-Datei erneut laden.

Während eines Firmware-Upgrades können vorhandene CRL-Dateien gelöscht werden. In diesem Fall werden die CRL-Dateien vom mGuard von der angegebenen URL erneut heruntergeladen. Alternativ kann diese auch manuell hochgeladen werden.

6.6 Menü Netzwerksicherheit

Dieses Menü steht **nicht** auf dem **mGuard blade-Controller** zur Verfügung.
Auf dem **mGuard rs2000** steht das Menü in reduzierter Form zur Verfügung.

6.6.1 Netzwerksicherheit >> Paketfilter

Der mGuard beinhaltet eine *Stateful Packet Inspection Firewall*. Die Verbindungsdaten einer aktiven Verbindung werden in einer Datenbank erfasst (connection tracking). Dadurch sind Regeln nur für eine Richtung zu definieren. Dann werden die Daten aus der anderen Richtung der jeweiligen Verbindung, und nur diese, automatisch durchgelassen.

Ein Nebeneffekt ist, dass bestehende Verbindungen bei einer Umkonfiguration nicht abgebrochen werden, selbst wenn eine entsprechende neue Verbindung nicht mehr aufgebaut werden dürfte.

Werkseitige Voreinstellung der Firewall:

- Alle eingehenden Verbindungen werden abgewiesen (außer VPN).
- Die Datenpakete aller ausgehenden Verbindungen werden durchgelassen.

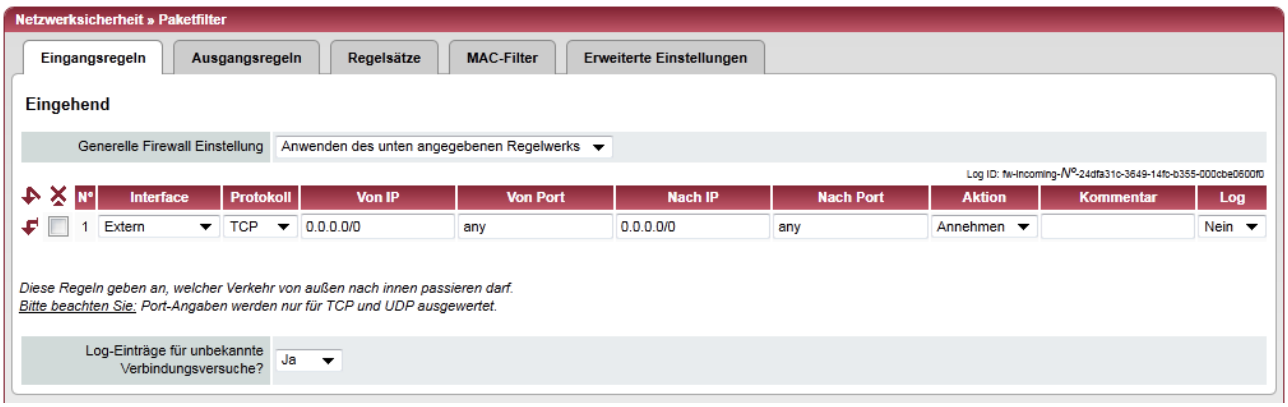
Firewall-Regeln an dieser Stelle wirken sich aus auf die Firewall, die immer aktiv ist, mit folgenden Ausnahmen:

- **VPN-Verbindungen**. Für VPN-Verbindungen werden eigene Firewall-Regeln definiert (siehe „IPsec VPN >> Verbindungen“ auf Seite 6-189, „Firewall“ auf Seite 6-210).
- **Benutzer-Firewall**. Wenn sich Benutzer anmelden, für die Benutzer-Firewall-Regeln definiert sind, werden vorrangig diese Regeln angewandt (siehe „Netzwerksicherheit >> Benutzerfirewall“ auf Seite 6-161), sekundär die immer aktiven Firewall-Regeln.

Sind mehrere Firewall-Regeln gesetzt, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt.

Sollten nachfolgend in der Regelliste weitere Regeln vorhanden sein, die auch passen würden, werden diese ignoriert.

6.6.1.1 Eingangsregeln



Netzwerksicherheit >> Paketfilter >> Eingangsregeln

Eingehend

Listet die eingerichteten Firewall-Regeln auf. Sie gelten für eingehende Datenverbindungen, die von extern initiiert wurden.

Wenn keine Regel gesetzt ist, werden die Datenpakete aller eingehenden Verbindungen (außer VPN) verworfen (= Werkseinstellung).

Generelle Firewall Einstellung

Alle eingehenden Verbindungen annehmen, die Datenpakete aller eingehenden Verbindungen werden angenommen.

Alle eingehenden Verbindungen verwerfen, die Datenpakete aller eingehenden Verbindungen werden verworfen.

Anwenden des unten angegebenen Regelwerks, blendet weitere Einstellmöglichkeiten ein. (Dieser Menüpunkt gehört nicht zum Funktionsumfang vom mGuard rs2000).

Die folgenden Einstellungen sind nur sichtbar, wenn „**Anwenden des unten angegebenen Regelwerks**“ eingestellt ist.

Interface

Extern / Extern 2 / Alle Externen[1]

Gibt an, über welches Interface die Datenpakete eingehen, damit sich die Regel auf sie bezieht. Mit **Alle Externen** sind die Interfaces **Extern** und **Extern 2** gemeint. Diese Interfaces stehen nur bei mGuard-Modellen mit von außen zugänglicher serieller Schnittstelle zur Verfügung.

Protokoll

TCP, UDP, ICMP, GRE, Alle

Von IP / Nach IP

0.0.0.0/0 bedeutet alle IP-Adressen. Um einen Adressenbereich anzugeben, benutzen Sie die CIDR-Schreibweise (siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 6-261).

Von Port / Nach Port

(wird nur ausgewertet bei den Protokollen TCP und UDP)

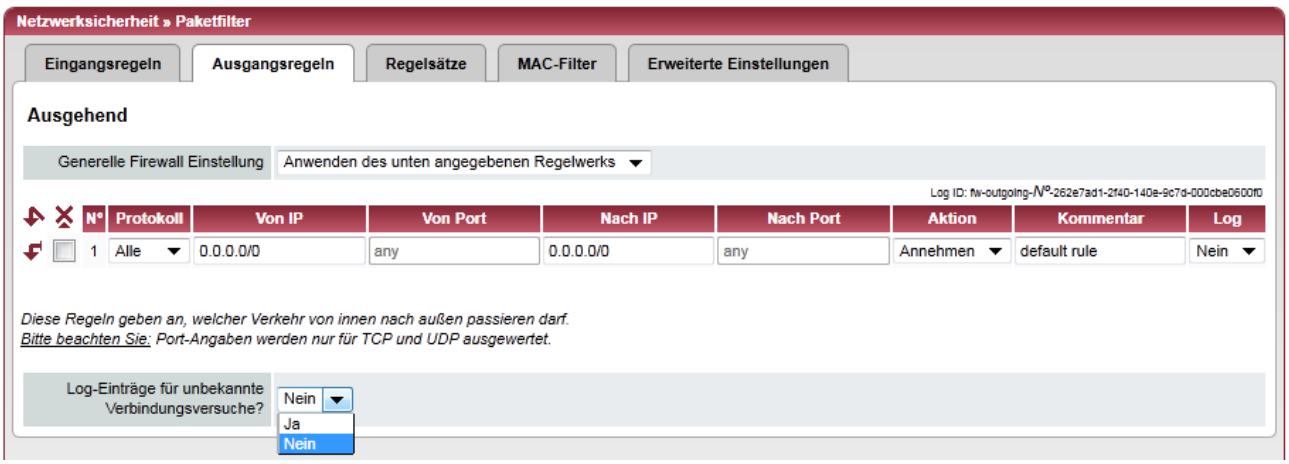
- **any** bezeichnet jeden beliebigen Port.
- **startport:endport** (z. B. 110:120) bezeichnet einen Portbereich.

Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben: (z. B. 110 für pop3 oder pop3 für 110).

Netzwerksicherheit >> Paketfilter >> Eingangsregeln [...]		
	Aktion	**Annehmen** bedeutet, die Datenpakete dürfen passieren. **Abweisen** bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. . Im Stealth-Modus entspricht **Abweisen** der Aktion **Verwerfen**. **Verwerfen** bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information über deren Verbleib erhält. **Namen von Regelsätzen**, sofern definiert. Bei Angabe eines Namens für Regelsätze treten die Firewall-Regeln in Kraft, die unter diesem Namen gespeichert sind (siehe Registerkarte *Regelsätze*).
	Kommentar	Ein frei wählbarer Kommentar für diese Regel.
	Log	Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel – das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen – oder nicht - *Log* auf **Nein** setzen (werkseitige Voreinstellung).
	Log-Einträge für unbekannte Verbindungsversuche	Bei **Ja** werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden. (Werkseitige Voreinstellung: **Nein**)

[1] *Extern 2* und *Alle Externen* nur bei Geräten mit serieller Schnittstelle (siehe „Netzwerk >> Interfaces“ auf Seite 6-64).

6.6.1.2 Ausgangsregeln



Netzwerksicherheit >> Paketfilter >> Ausgangsregeln

Ausgehend

Listet die eingerichteten Firewall-Regeln auf. Sie gelten für ausgehende Datenverbindungen, die von intern initiiert wurden, um mit einer entfernten Gegenstelle zu kommunizieren.

Werkseinstellung: Per Werkseinstellung ist eine Regel gesetzt, die alle ausgehenden Verbindungen zulässt.

Ist keine Regel gesetzt, sind alle ausgehenden Verbindungen verboten (außer VPN).

Generelle Firewall Einstellung

Alle ausgehenden Verbindungen annehmen, die Datenpakete aller ausgehenden Verbindungen werden angenommen.

Alle ausgehenden Verbindungen verwerfen, die Datenpakete aller ausgehenden Verbindungen werden verworfen.

Anwenden des unten angegebenen Regelwerks, blendet weitere Einstellmöglichkeiten ein. (Dieser Menüpunkt gehört nicht zum Funktionsumfang vom mGuard rs2000).

Die folgenden Einstellungen sind nur sichtbar, wenn „**Anwenden des unten angegebenen Regelwerks**“ eingestellt ist.

Protokoll

TCP, UDP, ICMP, GRE, Alle

Von IP / Nach IP

0.0.0.0/0 bedeutet alle IP-Adressen. Um einen Adressenbereich anzugeben, benutzen Sie die CIDR-Schreibweise (siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 6-261).

Von Port / Nach Port

(wird nur ausgewertet bei den Protokollen TCP und UDP)

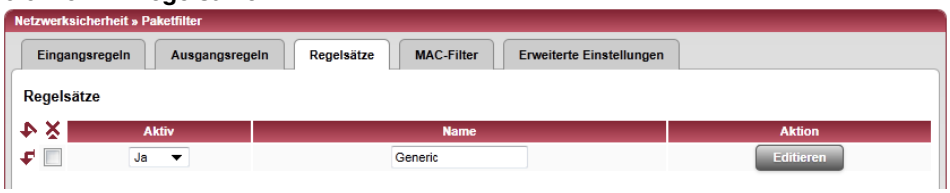
- **any** bezeichnet jeden beliebigen Port.
- **startport:endport** (z. B. 110:120) bezeichnet einen Portbereich.

Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben: (z. B. 110 für pop3 oder pop3 für 110).

Netzwerksicherheit >> Paketfilter >> Ausgangsregeln [...]

Aktion	**Annehmen** bedeutet, die Datenpakete dürfen passieren. **Abweisen** bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. . Im Stealth-Modus entspricht **Abweisen** der Aktion **Verwerfen**. **Verwerfen** bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information über deren Verbleib erhält. **Namen von Regelsätzen**, sofern definiert. Bei Angabe eines Namens für Regelsätze treten die Firewall-Regeln in Kraft, die unter diesem Namen gespeichert sind (siehe Registerkarte *Regelsätze*).
Kommentar	Ein frei wählbarer Kommentar für diese Regel.
Log	Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel – das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen – oder nicht - *Log* auf **Nein** setzen (werkseitige Voreinstellung).
Log-Einträge für unbekannte Verbindungsversuche	Bei **Ja** werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden. (Werkseitige Voreinstellung: **Nein**)

6.6.1.3 Regelsätze



Zwecks Strukturierung der Eingangs- und Ausgangsregeln können Sätze von Regeln definiert und jeweils unter einem Namen als Regelsatz abgelegt werden. Dann kann in einer Eingangs- bzw. Ausgangsregel ein Regelsatz referenziert werden, mit dem Effekt, dass die im Regelsatz enthaltenen Regeln dort eingesetzt werden.

Auch ist es möglich, in der Definition eines Regelsatzes selber einen anderen, bereits definierten Regelsatz zu referenzieren, also diesen als Baustein im aktuellen Regelsatz einzusetzen.

Regelsatz neu definieren

- In der Tabelle der Regelsätze rechts im Eintrag mit dem Namen „(unnamed)“ auf die Schaltfläche **Editieren** klicken.
- Sollte der Eintrag „(unnamed)“ nicht sichtbar sein, in der Tabelle der Regelsätze eine weitere Zeile öffnen.

Regelsatz bearbeiten

- Rechts im betreffenden Eintrag auf die Schaltfläche **Editieren** klicken.
- Besteht ein Firewall-Regelsatz aus mehreren Firewall-Regeln, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Sollten nachfolgend in der Regelliste weitere Regeln vorhanden sein, die auch passen würden, werden diese ignoriert.

Netzwerksicherheit >> Paketfilter >> Regelsätze

Regelsätze

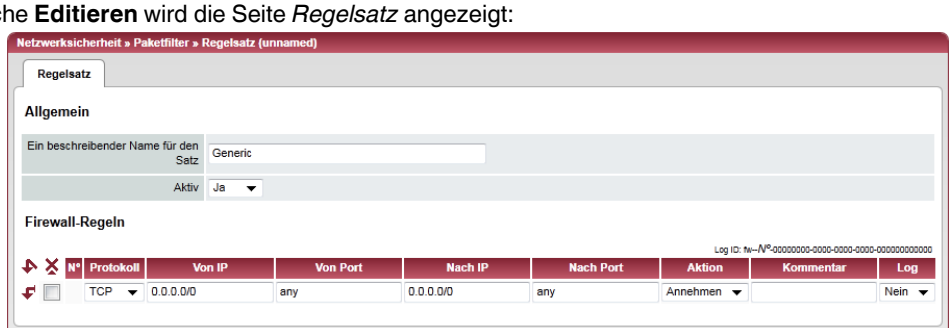
Listet alle Firewall-Regelsätze auf, die definiert worden sind.

Regelsätze werden nur angewendet, wenn sie auf der Registerkarte *Eingangsregeln* bzw. *Ausgangsregeln* referenziert sind.

Nur wenn alle Kriterien einer Firewall-Regel erfüllt werden, wird ein Regelsatz, der in dieser Firewall-Regel referenziert wird, angewendet.

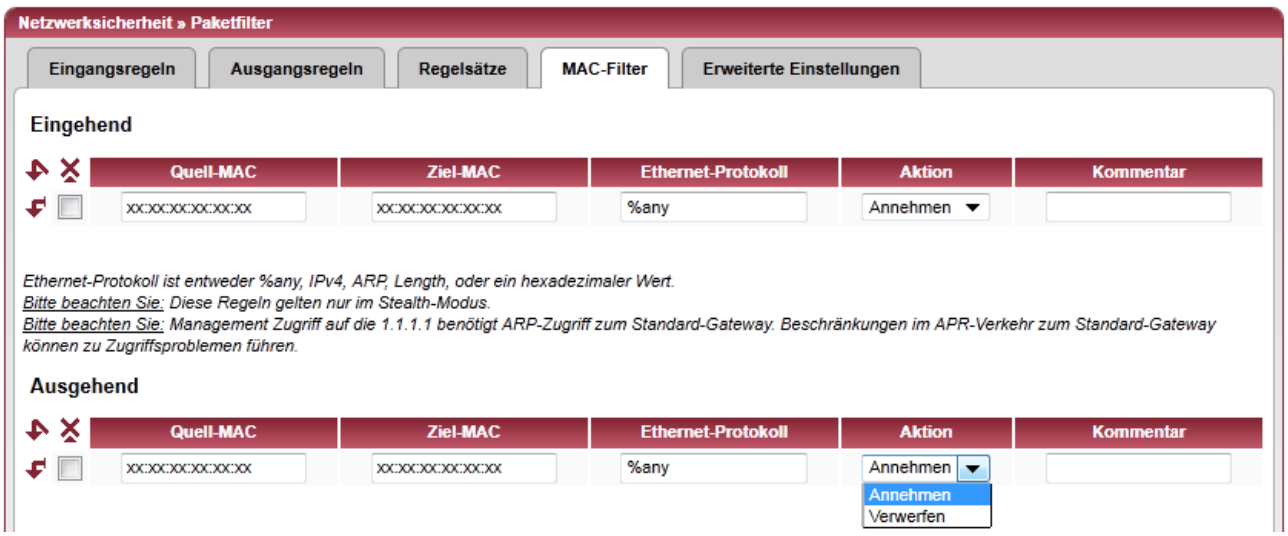
Aktiv	Aktiviert / deaktiviert den betreffenden Regelsatz.
Name	Name des Regelsatzes. Der Name ist beim Erstellen des Regelsatzes festgelegt worden.

Nach Klicken auf die Schaltfläche **Editieren** wird die Seite *Regelsatz* angezeigt:



Netzwerksicherheit >> Paketfilter >> Regelsätze [...]		
Allgemein	**Ein beschreibender Name für den Satz**	Frei zu vergebender Name. Er ist frei wählbar, muss aber einen Regelsatz eindeutig definieren. Über diesen Namen kann ein Regelsatz aus der Liste der Eingangs- und Ausgangsregeln referenziert werden. Dazu wird der betreffende Regelsatz-Name dort in der Spalte *Aktion* ausgewählt.
	Aktiv	Aktiviert / deaktiviert den betreffenden Regelsatz.
Firewall-Regeln	**Protokoll**	TCP, UDP, ICMP, GRE, Alle
	Von IP / Nach IP	**0.0.0.0/0** bedeutet alle IP-Adressen. Um einen Adressenbereich anzugeben, benutzen Sie die CIDR-Schreibweise (siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 6-261).
	Von Port / Nach Port	(wird nur ausgewertet bei den Protokollen TCP und UDP) – **any** bezeichnet jeden beliebigen Port. – **startport:endport** (z. B. 110:120) bezeichnet einen Portbereich. Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben: (z. B. 110 für pop3 oder pop3 für 110).
	Aktion	**Annehmen** bedeutet, die Datenpakete dürfen passieren. **Abweisen** bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. Im Stealth-Modus entspricht **Abweisen** der Aktion **Verwerfen**. **Verwerfen** bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information über deren Verbleib erhält. **Namen von Regelsätzen**, sofern definiert. Neben „Annehmen“, „Abweisen“ und „Verwerfen“ führt die Auswahlliste auch die Namen bereits definierter Regelsätze auf. Wird ein Name ausgewählt (referenziert), wird dieser, d. h. die Regeln dieses Regelsatzes, an dieser Stelle eingesetzt. Falls die Regeln des eingesetzten Regelsatzes nicht angewendet und mit „Annehmen“, „Abweisen“ oder „Verwerfen“ durchgesetzt werden können, wird mit der Abarbeitung der Regel fortgefahren, die auf die folgt, aus der der Regelsatz referenziert wurde.
	Kommentar	Ein frei wählbarer Kommentar für diese Regel.
	Log	Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel – das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen – oder nicht - *Log* auf **Nein** setzen (werkseitige Voreinstellung).

6.6.1.4 MAC-Filter



Der MAC-Filter „Eingehend“ wird auf Frames angewendet, die der mGuard an der WAN-Schnittstelle empfängt. Der MAC-Filter „Ausgehend“ wird auf Frames angewendet, die der mGuard an der LAN-Schnittstelle empfängt. Datenpakete, die bei mGuard-Modellen mit serieller Schnittstelle[1] per Modemverbindung ein- bzw. ausgehen, werden vom MAC-Filter nicht erfasst, weil hier kein Ethernet-Protokoll angewendet wird.

Im *Stealth*-Modus können neben dem Paketfilter (Layer 3/4), der den Datenverkehr z. B. nach ICMP-Nachrichten oder TCP/UDP-Verbindungen filtert, zusätzlich MAC-Filter (Layer 2) gesetzt werden. Ein MAC-Filter (Layer 2) filtert nach MAC-Adressen und Ethernet-Protokollen.

Im Gegensatz zum Paketfilter ist der MAC-Filter stateless. Das heißt, werden Regeln eingeführt, müssen gegebenenfalls entsprechende Regeln für die Gegenrichtung ebenfalls erstellt werden.

Ist keine Regel gesetzt, sind alle ARP- und IP-Pakete erlaubt.

Achten Sie auf die Hinweise auf dem Bildschirm, wenn Sie MAC-Filterregeln setzen.

Die hier angegebenen Regeln haben Vorrang gegenüber den Packet-Filterregeln.

Der MAC-Filter unterstützt keine Logging Funktionalität.

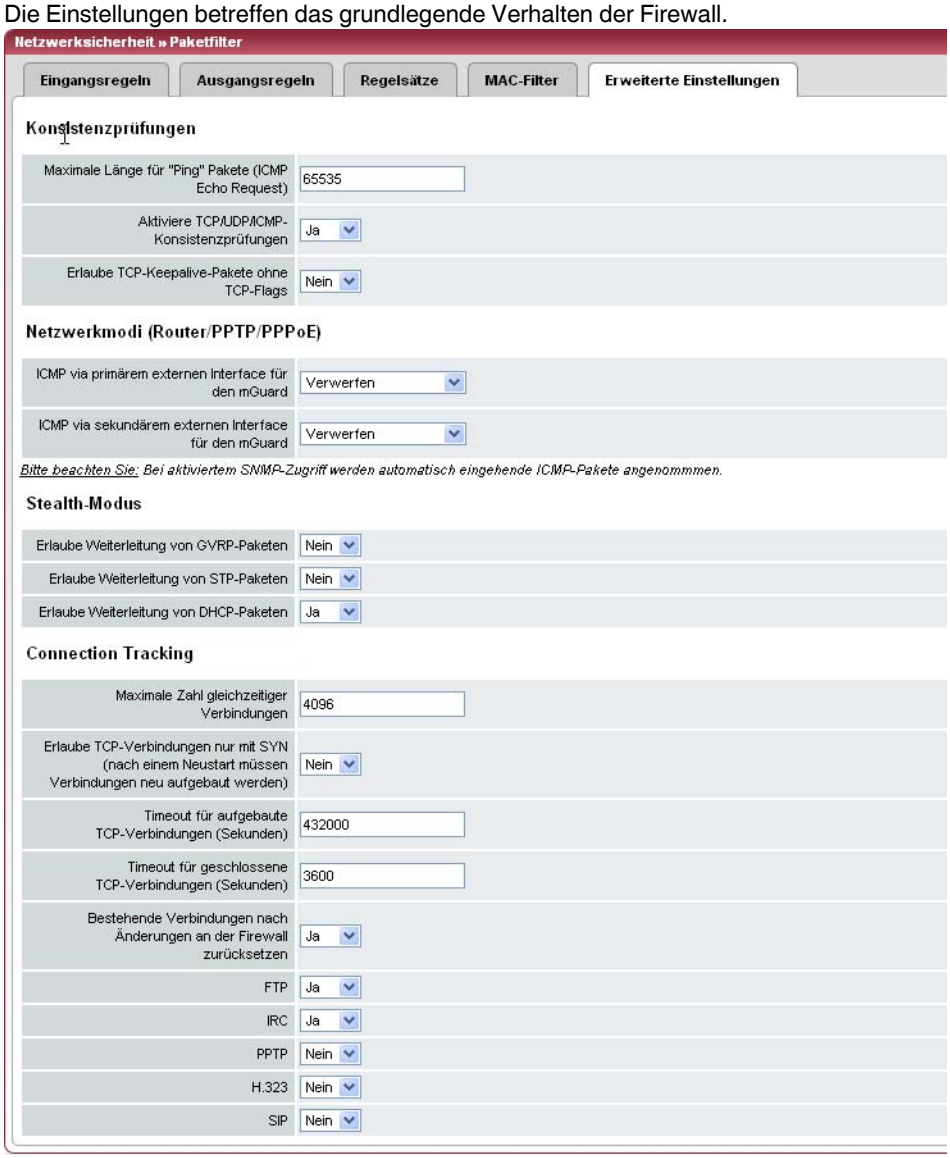
Netzwerksicherheit >> Paketfilter >> MAC-Filter		
Eingehend	**Quell-MAC**	Angabe der Quell-MAC-Adresse: xx:xx:xx:xx:xx:xx steht für alle MAC-Adressen.
	Ziel-MAC	Angabe der Ziel-MAC-Adresse: xx:xx:xx:xx:xx:xx steht für alle MAC-Adressen. Der Wert ff:ff:ff:ff:ff:ff ist die Broadcast MAC-Adresse, an die z. B. alle ARP-Anfragen geschickt werden.

[1] mGuard rs4000/2000, mGuard centerport, mGuard industrial rs, mGuard blade, EAGLE mGuard, mGuard delta

Netzwerksicherheit >> Paketfilter >> MAC-Filter[...]		
	Ethernet-Protokoll	**%any** steht für alle Ethernet-Protokolle. Weitere Protokolle können mit dem Namen oder in HEX angegeben werden, zum Beispiel: – IPv4 oder 0800 – ARP oder 0806
	Aktion	**Annehmen** bedeutet, die Datenpakete dürfen passieren **Verwerfen** bedeutet, die Datenpakete werden verworfen
	Kommentar	Ein frei wählbarer Kommentar für diese Regel.
Ausgehend	Die Erklärung unter „Eingehend“ gilt auch für „Ausgehend“.	

6.6.1.5 Erweiterte Einstellungen

Die Einstellungen betreffen das grundlegende Verhalten der Firewall.



Netzwerksicherheit >> Paketfilter >> Erweiterte Einstellungen

Konsistenzprüfungen

Dieser Menüpunkt gehört nicht zum Funktionsumfang vom mGuard rs2000.

Maximale Länge für „Ping“ Pakete (ICMP-Echo-Request)

Bezieht sich auf die Länge des gesamten Paketes inklusive Header. Normalerweise beträgt die Paketlänge 64 Byte, kann aber auch größer sein. Sollen übergroße Pakete verhindert werden, um „Verstopfungen“ zu vermeiden, kann ein maximaler Wert angegeben werden. Dieser sollte auf jeden Fall über 64 liegen, damit normale ICMP-Echo-Requests nicht blockiert werden.

Netzwerksicherheit >> Paketfilter >> Erweiterte Einstellungen[...]		
	Aktiviere TCP/UDP/ICMP-Konsistenzprüfungen	Wenn auf **Ja** gesetzt, führt der mGuard eine Reihe von Tests auf falsche Prüfsummen, Paketgrößen, usw. durch und verwirft Pakete, die die Tests nicht bestehen. Werkseitig ist dieser Schalter auf **Ja** gesetzt.
	Erlaube TCP-Keepalive-Pakete ohne TCP-Flags	Normalerweise werden TCP-Pakete ohne gesetzte Flags in deren TCP-Header von Firewalls verworfen. Mindestens ein Typ von Steuerungen von Siemens mit älterer Firmware versendet TCP-Keepalive-Pakete ohne gesetzte TCP-Flags, welche vom mGuard deshalb als ungültig verworfen werden. Die Einstellung **Ja** erlaubt das Weiterleiten von TCP-Paketen, bei denen keine TCP-Flags im Header gesetzt sind. Dies gilt ausschließlich, wenn solche TCP-Pakete innerhalb einer schon existierenden, regulär aufgebauten TCP-Verbindungen versendet werden. TCP-Pakete ohne TCP-Flags führen nicht zu einem neuen Eintrag in der Verbindungstabelle (siehe „Connection Tracking“ auf Seite 6-155). Besteht die Verbindung, wenn der mGuard neu gestartet wird, werden entsprechende Pakete weiterhin verworfen und Verbindungsstörungen werden beobachtet, solange keine zu der Verbindung gehörenden Pakete mit Flags gesendet werden. Diese Einstellung wirkt auf alle TCP-Pakete ohne Flags. Die Einstellung **Ja** ist also eine Abschwächung der Sicherheitsfunktion, die der mGuard bietet.
Netzwerk-Modi (Router / PPTP / PPPoE)	**ICMP via primärem externen Interface für den mGuard** **ICMP via sekundärem externen Interface für den mGuard**	Mit dieser Option können Sie das Verhalten beim Empfang von ICMP-Nachrichten beeinflussen, die aus dem externen Netz über das primäre / sekundäre externe Interface an den mGuard gesendet werden. Unabhängig von der hier festgelegten Einstellung werden bei aktiviertem SNMP-Zugriff eingehende ICMP-Pakete immer angenommen. **Verwerfen**: Alle ICMP-Nachrichten zum mGuard werden verworfen. **Annehmen von Ping**: Nur Ping-Nachrichten (ICMP Typ 8) zum mGuard werden akzeptiert. **Alle ICMPs annehmen**: Alle Typen von ICMP-Nachrichten zum mGuard werden akzeptiert.
Stealth-Modus	**Erlaube Weiterleitung von GVRP-Paketen:**	**Ja / Nein** Das GARP VLAN Registration Protocol (GVRP) wird von GVRP-fähigen Switches verwendet, um Konfigurationsinformationen miteinander auszutauschen. Ist dieser Schalter auf **Ja** gesetzt, dann können GVRP-Pakete den mGuard im *Stealth*-Modus passieren.

Netzwerksicherheit >> Paketfilter >> Erweiterte Einstellungen[...]		
	Erlaube Weiterleitung von STP-Paketen	**Ja / Nein** Das Spanning-Tree Protocol (STP) (802.1d) wird von Bridges und Switches verwendet, um Schleifen in der Verkabelung zu entdecken und zu berücksichtigen. Ist dieser Schalter auf **Ja** gesetzt, dann können STP-Pakete den mGuard im *Stealth*-Modus passieren.
	Erlaube Weiterleitung von DHCP-Paketen:	**Ja / Nein** Bei **Ja** wird dem Client erlaubt, über DHCP eine IP-Adresse zu beziehen - unabhängig von den Firewall-Regeln für ausgehenden Datenverkehr. Die Voreinstellung für diesen Schalter ist **Ja**.
Connection Tracking	**Maximale Zahl gleichzeitiger Verbindungen**	Dieser Eintrag legt eine Obergrenze fest. Diese ist so gewählt, dass sie bei normalem praktischen Einsatz nie erreicht wird. Bei Angriffen kann sie dagegen leicht erreicht werden, so dass durch die Begrenzung ein zusätzlicher Schutz eingebaut ist. Sollten in Ihrer Betriebsumgebung besondere Anforderungen vorliegen, dann können Sie den Wert erhöhen. Auch vom mGuard aus aufgebaute Verbindungen werden mitgezählt. Deshalb dürfen Sie diesen Wert nicht zu klein wählen, da es sonst zu Fehlfunktionen kommt.
	Erlaube TCP-Verbindungen nur mit SYN	**Ja / Nein, Standard: Nein.** SYN ist ein spezielles Datenpaket im TCP/IP-Verbindungsaufbau, das den Anfang des Verbindungsaufbaus markiert. **Nein** (Standard): Der mGuard erlaubt auch Verbindungen, deren Anfang er nicht registriert hat. D. h. der mGuard kann bei Bestehen einer Verbindung einen Neustart durchführen, ohne dass die Verbindung abreißt. **Ja**: Der mGuard muss das SYN-Paket einer bestehenden Verbindung registriert haben. Sonst baut er die Verbindung ab. Falls der mGuard während des Bestehens einer Verbindung einen Neustart durchführt, wird diese Verbindung getrennt. Damit werden Angriffe auf bestehende Verbindungen und das Entführen bestehender Verbindungen erschwert.
	Timeout für aufgebaute TCP-Verbindungen	Wird eine TCP-Verbindung über den hier angegebenen Zeitraum hinaus nicht verwendet, so werden ihre Verbindungsdaten gelöscht. Eine durch NAT umgeschriebene Verbindung (nicht 1:1-NAT), muss danach erneut aufgebaut werden. Wenn unter „Erlaube TCP-Verbindungen nur mit SYN“ die Auswahl **Ja** eingestellt ist, dann müssen alle abgelaufen Verbindungen neu aufgebaut werden. Die Voreinstellung sind 432000 Sekunden (5 Tage).

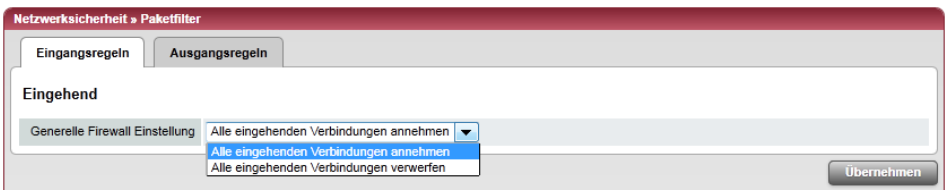
Netzwerksicherheit >> Paketfilter >> Erweiterte Einstellungen[...]	
Timeout für geschlossene TCP-Verbindungen	Der Timeout sperrt eine TCP-Port-zu-Port-Verbindung für längere Zeit nach dem Schließen. Das ist notwendig, da nach dem Schließen der Verbindung in einem paketorientierten Netzwerk noch Pakete ankommen können, die zur bereits geschlossenen TCP-Verbindung gehören. Ohne die zeitgesteuerte Sperre könnten die alten Pakete versehentlich einer neuen Verbindung zugeordnet werden. Die Voreinstellung sind 3600 Sekunden (1 Stunde).
Bestehende Verbindungen nach Änderungen an der Firewall zurücksetzen	**Ja / Nein, Standard: Ja** Bei **Ja** werden die bestehenden Verbindungen zurückgesetzt, – wenn „Erlaube TCP-Verbindungen nur mit SYN“ auf **Ja** steht und – wenn die Firewall-Regeln angepasst wurden oder – wenn der Wert von **Nein** auf **Ja** geändert wird (auch ohne Änderung der Firewall-Regeln.) Nach einer Änderung der Firewall-Regeln verhält sich der mGuard wie nach einem Neustart, allerdings gilt dies nur für die weitergeleiteten Verbindungen. Bestehende TCP-Verbindungen werden unterbrochen, auch wenn sie nach den neuen Firewall-Regeln erlaubt sind. Verbindungen zum Gerät sind davon nicht betroffen, selbst wenn die Firewall-Regeln für den Remote-Zugriff geändert wurden. Bei **Nein** bleiben die Verbindungen bestehen, auch wenn die geänderten Firewall-Regeln diese nicht erlauben oder beenden würden.
FT	**Ja / Nein** Wird beim FTP-Protokoll eine ausgehende Verbindung hergestellt, um Daten abzurufen, gibt es zwei Varianten der Datenübertragung: Beim „aktiven FTP“ stellt der angerufene Server im Gegenzug eine zusätzliche Verbindung zum Anrufer her, um auf dieser Verbindung die Daten zu übertragen. Beim „passiven FTP“ baut der Client diese zusätzliche Verbindung zum Server zur Datenübertragung auf. Damit die zusätzlichen Verbindungen von der Firewall durchgelassen werden, muss FTP auf **Ja** stehen (Standard).
IRC	**Ja / Nein** Ähnlich wie bei FTP: Beim Chatten im Internet per IRC müssen nach aktivem Verbindungsaufbau auch eingehende Verbindungen zugelassen werden, soll das Chatten reibungslos funktionieren. Damit diese von der Firewall durchgelassen werden, muss IRC auf **Ja** stehen (Standard).

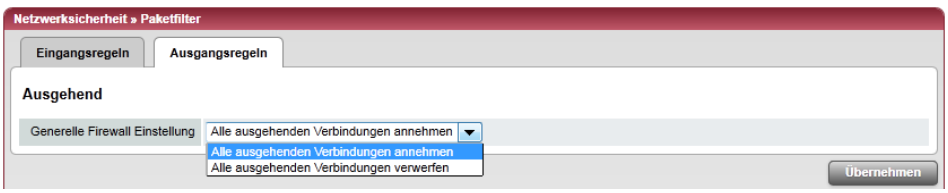
Netzwerksicherheit >> Paketfilter >> Erweiterte Einstellungen[...]		
	PPTP	**Ja / Nein, Standard: Nein** Muss auf **Ja** gesetzt werden, wenn von lokalen Rechnern ohne Zuhilfenahme des mGuards VPN-Verbindungen mittels PPTP zu externen Rechner aufgebaut werden können sollen. Muss auf **Ja** gesetzt werden, wenn GRE-Pakete von intern nach extern weiter geleitet werden müssen.
	H.323	**Ja / Nein, Standard: Nein** Protokoll, das zum Aufbau von Kommunikationssitzungen mit zwei oder mehr Teilnehmern dient. Wird für audio-visuelle Übertragungen verwendet. Dieses Protokoll ist älter als SIP.
	SIP	**Ja / Nein, Standard: Nein.** Das SIP (Session Initiation Protocol) dient zum Aufbau von Kommunikationssitzungen mit zwei oder mehr Teilnehmern. Wird häufig bei der IP-Telefonie verwendet. Mit **Ja** ist es dem mGuard möglich, das SIP zu verfolgen und dynamisch notwendige Firewall-Regeln einzufügen, wenn weitere Kommunikationskanäle zu derselben Sitzung aufgebaut werden. Wenn zusätzlich NAT aktiviert ist, können einer oder mehrere lokal angeschlossene Rechner über den mGuard mit extern erreichbaren Rechnern per SIP kommunizieren.

6.6.1.6 Firewall beim mGuard rs2000

Der mGuard rs2000 besitzt eine einfache „2-Click-Firewall“. Diese lässt alle eingehenden und ausgehenden Verbindungen entweder komplett zu oder lehnt alle Verbindungen komplett ab. Weitere Einstellmöglichkeiten sind nicht vorgesehen. Außerdem werden Zugriffe über diese Firewall nicht mitgeloggt (siehe Kapitel 6.12.2, *Logging >> Logs ansehen*).

Folgende Firewall-Funktionalität steht Ihnen bei der Nutzung des **mGuard rs2000** zur Verfügung:



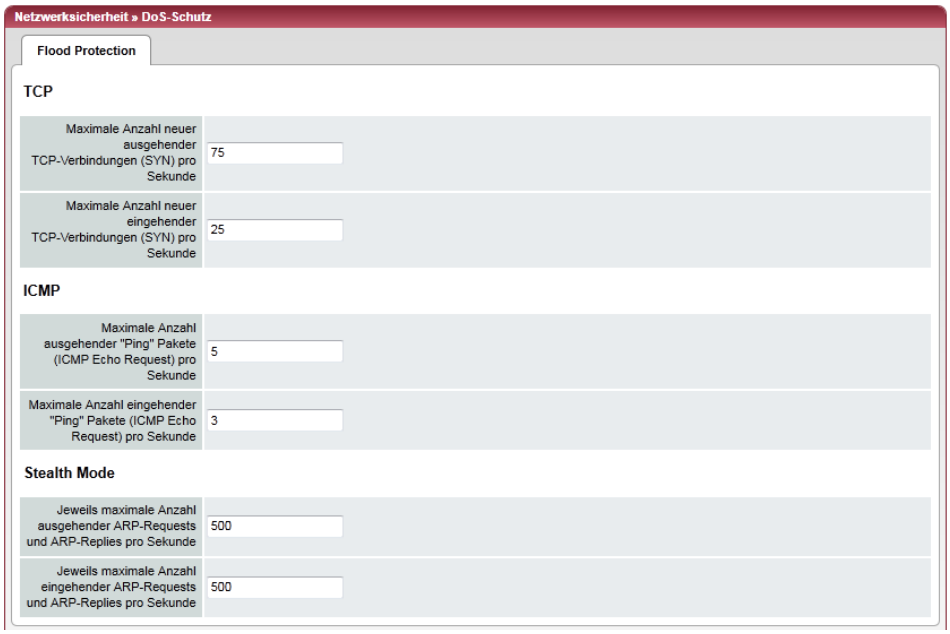


Diese Variablen stehen auch bei anderen Geräten zur Verfügung. Aber für andere Geräte gibt es weitere Einstellmöglichkeiten (siehe „Eingangsregeln“ auf Seite 6-145 und „Ausgangsregeln“ auf Seite 6-147).

6.6.2 Netzwerksicherheit >> DoS-Schutz

6.6.2.1 Flood Protection

Dieses Menü steht **nicht** auf dem **mGuard rs2000** zur Verfügung.



Netzwerksicherheit >> DoS-Schutz >> Flood Protection		
TCP	**Maximale Anzahl neuer ein- bzw. ausgehender TCP-Verbindungen (SYN) pro Sekunde**	Ausgehend: Werkseinstellung: 75 Eingehend: Werkseinstellung: 25 Maximalwerte für die zugelassenen ein- und ausgehenden TCP-Verbindungen pro Sekunde. Sie sind so gewählt, dass sie bei normalem praktischen Einsatz nie erreicht werden. Bei Angriffen können sie dagegen leicht erreicht werden, so dass durch die Begrenzung ein zusätzlicher Schutz eingebaut ist. Sollten in Ihrer Betriebsumgebung besondere Anforderungen vorliegen, dann können Sie die Werte erhöhen.

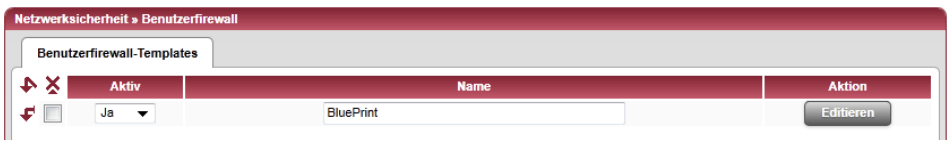
Netzwerksicherheit >> DoS-Schutz >> Flood Protection[...]		
ICMP	**Maximale Anzahl ein- bzw. ausgehender „Ping“ Pakete (ICMP-Echo-Request) pro Sekunde**	Ausgehend: Werkseinstellung: 5 Eingehend: Werkseinstellung: 3 Maximalwerte für die zugelassenen ein- und ausgehenden „Ping“-Pakete pro Sekunde. Sie sind so gewählt, dass sie bei normalem praktischen Einsatz nie erreicht werden. Bei Angriffen können sie dagegen leicht erreicht werden, so dass durch die Begrenzung ein zusätzlicher Schutz eingebaut ist. Sollten in Ihrer Betriebsumgebung besondere Anforderungen vorliegen, dann können Sie die Werte erhöhen. Der Wert **0** bewirkt, dass kein „Ping“ Paket durchgelassen bzw. eingelassen wird.
Stealth-Mode	**Jeweils maximale Anzahl ein- bzw. ausgehender ARP-Requests und ARP-Replies pro Sekunde**	Werkseinstellung: 500 Maximalwerte für die zugelassenen ein- und ausgehenden ARP-Requests pro Sekunde. Sie sind so gewählt, dass sie bei normalem praktischen Einsatz nie erreicht werden. Bei Angriffen können sie dagegen leicht erreicht werden, so dass durch die Begrenzung ein zusätzlicher Schutz eingebaut ist. Sollten in Ihrer Betriebsumgebung besondere Anforderungen vorliegen, dann können Sie die Werte erhöhen.

6.6.3 Netzwerksicherheit >> Benutzerfirewall

Die Benutzerfirewall ist ausschließlich bei Firewall-Benutzern in Kraft, also bei Benutzern, die sich als Firewall-Benutzer angemeldet haben (siehe „Authentifizierung >> Firewall-Benutzer“ auf Seite 6-124).

Jedem Firewall-Benutzer kann ein Satz von Firewall-Regeln, ein sogenanntes Template, zugeordnet werden.

6.6.3.1 Benutzerfirewall-Templates



Hier werden alle definierten Benutzerfirewall-Templates aufgelistet. Ein Template kann aus mehreren Firewall-Regeln bestehen. Ein Template kann mehreren Nutzern zugeordnet sein.

Template neu definieren:

- In der Tabelle der Templates rechts im Eintrag mit dem Namen „(unnamed)“ auf die Schaltfläche **Editieren** klicken.
- Sollte der Eintrag „(unnamed)“ nicht sichtbar sein, in der Tabelle der Regelsätze eine weitere Zeile öffnen.

Regelsatz bearbeiten:

- Rechts im betreffenden Eintrag auf die Schaltfläche **Editieren** klicken.

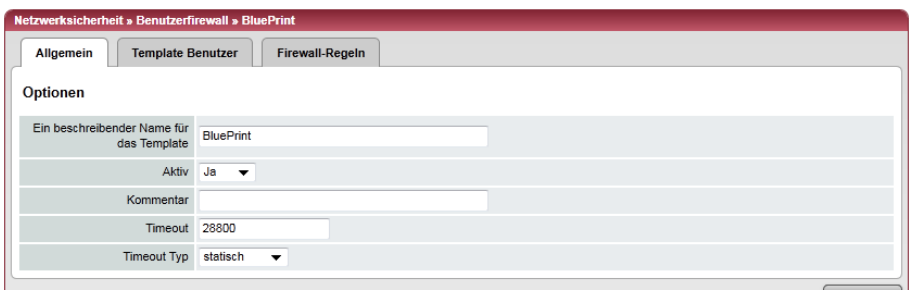
Netzwerksicherheit >> Benutzerfirewall >> Benutzerfirewall-Templates

Allgemein

Aktiv — Aktiviert / deaktiviert das betreffende Template.

Name — Name des Templates. Der Name ist beim Erstellen des Templates festgelegt worden.

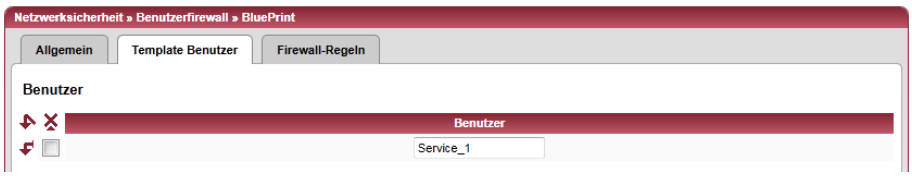
Nach Klicken auf **Editieren** erscheint folgende Registerkarte:



Netzwerksicherheit >> Benutzerfirewall >> Benutzerfirewall-Templates [...]		
Optionen	**Ein beschreibender Name für das Template**	Sie können das Benutzerfirewall-Template frei benennen bzw. umbenennen.
	Aktiv	**Ja / Nein** Bei **Ja** ist das Benutzerfirewall-Template aktiv, sobald sich Firewall-Benutzer beim mGuard anmelden, die auf der Registerkarte *Template Benutzer* (s. u.) erfasst sind und denen dieses Template zugeordnet ist. Es spielt keine Rolle, von welchem Rechner und unter welcher IP-Adresse sich ein Benutzer anmeldet. Die Zuordnung Benutzer - Firewall-Regeln erfolgt über die Authentifizierungsdaten, die der Benutzer bei seiner Anmeldung angibt (Benutzername, Passwort).
	Kommentar	Optional: erläuternder Text
	Timeout	Standard: 28800. Gibt in Sekunden an, wann die Firewall-Regeln außer Kraft gesetzt werden. Dauert die Sitzung des betreffenden Benutzers länger als die hier festgelegte Timeout-Zeit, muss er sich neu anmelden.
	Timeout-Typ	statisch / dynamisch Bei *statischem* Timeout werden Benutzer automatisch abgemeldet, sobald die eingestellte Timeout-Zeit verstrichen ist. Bei *dynamischem* Timeout werden Benutzer automatisch abgemeldet, nachdem die Verbindungen durch den Benutzers geschlossen wurden oder aber auf dem mGuard abgelaufen sind und anschließend die hier eingestellte Timeout-Zeit verstrichen ist. Eine Verbindung gilt auf dem mGuard dann als abgelaufen, wenn über die folgenden Zeiträume hinaus keine Daten mehr für diese Verbindung vorlagen.
	Ablaufzeitraum der Verbindung nach Nichtbenutzung – TCP 5 Tage (Dieser Wert ist einstellbar, siehe 6-155.) Hinzukommen zusätzlich 120 s nach Schließen der Verbindung. (Diese 120s gelten auch nach dem Schließen durch den Benutzer.) – UDP 30s nach Datenverkehr in einer Richtung; 180 s nach Datenverkehr in beide Richtungen – ICMP 30s – Andere 10min	

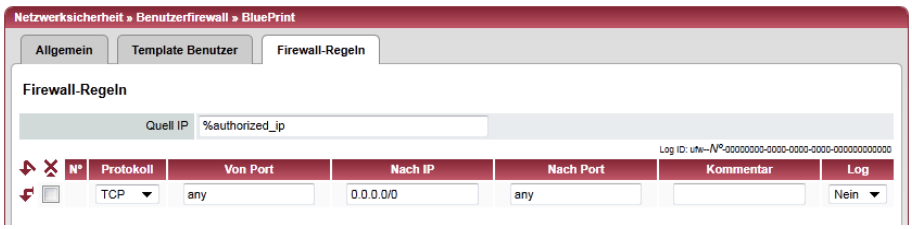
Netzwerksicherheit >> Benutzerfirewall >> Benutzerfirewall-Templates >> Editieren > ...

Template Benutzer



Geben Sie die Namen von Benutzern an. Die Namen müssen denen entsprechen, die unter Menü Authentifizierung >> Firewall-Benutzer festgelegt sind (siehe Seite 6-124).

Firewall-Regeln



Quell IP — IP-Adresse, von der aus Verbindungsaufbauten zugelassen werden. Soll es die Adresse sein, von der sich der Benutzer beim mGuard angemeldet hat, sollte der Platzhalter „%authorized_ip“ verwendet werden.

> Wenn mehrere Firewall-Regeln gesetzt sind, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Falls in der Regelliste weitere passende Regeln vorhanden sind, werden diese ignoriert.

Protokoll — **Alle** bedeutet: TCP, UDP, ICMP, GRE und andere IP-Protokolle.

Von Port/Nach Port — (wird nur ausgewertet bei den Protokollen TCP und UDP)

- **any** bezeichnet jeden beliebigen Port.
- **startport:endport** (z. B. 110:120) > Portbereich.

Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben: (z. B. 110 für pop3 oder pop3 für 110).

Nach IP — **0.0.0.0/0** bedeutet alle IP-Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise (siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 6-261)

Kommentar — Ein frei wählbarer Kommentar für diese Regel.

Log — Für jede Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

- das Ereignis protokolliert werden soll – *Log* auf **Ja** setzen
- oder nicht – *Log* auf **Nein** setzen (werkseitig voreingestellt).

6.7 Menü CIFS-Integrity-Monitoring

Das CIFS-Integrity-Monitoring steht **nicht** für den **mGuard rs2000** zur Verfügung.
Es darf **nicht** auf dem **mGuard blade Controller** verwendet werden.

Im Netzwerk-Modus Stealth ist ohne Management-IP keine CIFS-Integritätsprüfung möglich und der CIFS-Server für den Anti-Virus-Scan wird nicht unterstützt.

Beim CIFS-Integrity-Monitoring gibt es zwei Möglichkeiten, Netzlaufwerke auf Viren zu prüfen.

- CIFS-Integritätsprüfung
- CIFS-Anti-Virus-Scan-Connector

CIFS-Integritätsprüfung

Bei der **CIFS-Integritätsprüfung** werden Windows-Netzlaufwerke daraufhin geprüft, ob sich bestimmte Dateien (z. B. *.exe, *.dll) verändert haben. Eine Veränderung dieser Dateien deutet auf einen Virus oder unbefugtes Eingreifen hin.

CIFS-Anti-Virus-Scan-Connector

Beim **CIFS-Anti-Virus-Scan-Connector** ermöglicht der mGuard einen Viren-Scan auf Laufwerke, die sonst von außen nicht erreichbar sind (z. B. Produktionszellen). Dabei spiegelt der mGuard ein Laufwerk nach außen, um dort den Viren-Scan durchführen zu lassen. Bei diesem Verfahren ist zusätzlich eine Anti-Virus-Software notwendig. Stellen Sie den für Ihre Anti-Virus-Software notwendigen Lese-Zugriff ein.

Einstellmöglichkeiten für die CIFS-Integritätsprüfung

- Welche Netzlaufwerke dem mGuard bekannt sind (siehe „CIFS-Integrity-Monitoring >> Netzlaufwerke“ auf Seite 6-165).
- Welche Art von Zugriff erlaubt ist (siehe „CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Einstellungen“ auf Seite 6-167)
- In welchem Abstand die Laufwerke geprüft werden sollen (siehe „CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Einstellungen >> Editieren“ auf Seite 6-168).
- Welche Dateitypen geprüft werden sollen (siehe „CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Muster für Dateinamen“ auf Seite 6-170).
- Form, in der gewarnt werden soll, wenn eine Veränderung festgestellt wird (z. B. per E-Mail, siehe „CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Einstellungen“ auf Seite 6-167, oder per SNMP, siehe „CIFS-Integritäts-Traps“ auf Seite 6-52).

Einstellmöglichkeiten für den CIFS-Anti-Virus-Scan-Connector

- Welche Netzlaufwerke dem mGuard bekannt sind (siehe „CIFS-Integrity-Monitoring >> Netzlaufwerke“ auf Seite 6-165).
- Welche Art von Zugriff erlaubt ist (Lese- oder Lese/Schreib-Zugriff, siehe „CIFS-Integrity-Monitoring >> CIFS-Anti-Virus-Scan-Connector“ auf Seite 6-175).

6.7.1 CIFS-Integrity-Monitoring >> Netzlaufwerke

Voraussetzungen:

Sie können hier die Netzlaufwerke angeben, die der mGuard regelmäßig prüfen soll.

Damit diese Netzlaufwerke tatsächlich geprüft werden können, müssen Sie zusätzlich unter einem der beiden möglichen Verfahren (CIFS-Integritätsprüfung/CIFS-Anti-Virus-Scan-Connector) auf diese Netzlaufwerke verweisen.

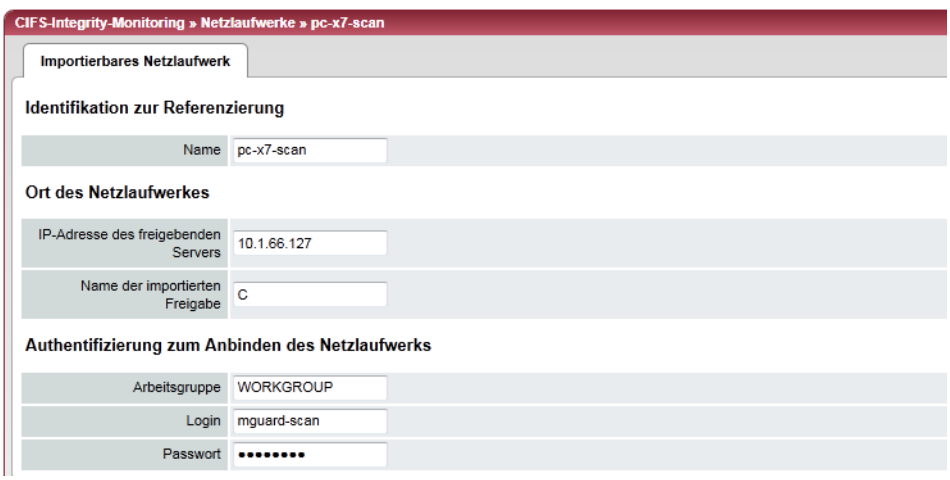
Die Verweise auf die Netzlaufwerke können Sie an folgenden Stellen einstellen:

– bei der CIFS-Integritätsprüfung, siehe „Überprüftes Netzlaufwerk“ auf Seite 6-168.

– beim CIFS-Anti-Virus-Scan, siehe „CIFS-Anti-Virus-Scan-Connector“ auf Seite 6-175

6.7.1.1 Netzlaufwerke

CIFS-Integrity-Monitoring >> Netzlaufwerke		
Importierbare Netzlaufwerke	**Name**	Name des Netzlaufwerkes, das geprüft werden soll. (Interner Name, der in der Konfiguration verwendet wird.)
	Server	IP-Adresse des freigebenden Servers.
	Netzlaufwerk	Name des Laufwerkes, unter dem es vom freigebenden Server bereitgestellt wird. Klicken Sie auf die Schaltfläche **Editieren**, um Einstellungen vorzunehmen.



CIFS-Integrity-Monitoring >> Netzlaufwerke >> Editieren		
Identifikation zur Referenzierung	**Name**	Name des Netzlaufwerkes, das geprüft werden soll. (Interner Name, der in der Konfiguration verwendet wird.)
Ort des Netzlaufwerkes	**IP-Adresse des freigebenden Servers**	IP-Adresse des Servers, dessen Netzlaufwerk geprüft werden soll.

CIFS-Integrity-Monitoring >> Netzlaufwerke >> Editieren [...]		
Authentifizierung zum Anbinden des Netzlaufwerkes	**Name der importierten Freigabe**	Verzeichnis auf dem oben freigegebenen Server, das geprüft werden soll.
	Arbeitsgruppe	Name der Arbeitsgruppe, zu der das Netzlaufwerk gehört.
	Login	Login für den Server.
	Passwort	Passwort für den Login.

6.7.2 CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung

Bei der **CIFS-Integritätsprüfung** werden Windows-Netzlaufwerke daraufhin geprüft, ob sich bestimmte Dateien (z. B. *.exe, *.dll) verändert haben. Eine Veränderung dieser Dateien deutet auf einen Virus oder unbefugtes Eingreifen hin.

Integritätsdatenbank

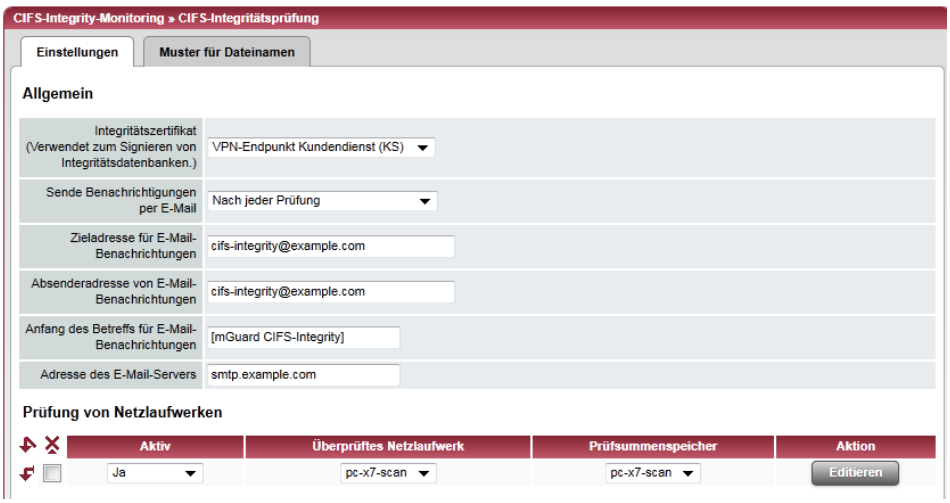
Wenn ein zu prüfenden Netzlaufwerk neu konfiguriert wird, muss eine Integritätsdatenbank angelegt werden.

Diese Integritätsdatenbank dient als Vergleichsgrundlage für die regelmäßige Prüfung des Netzlaufwerkes. Darin sind die Prüfsummen aller zu überwachenden Dateien aufgezeichnet. Die Integritätsdatenbank selbst ist gegen Manipulation gesichert.

Sie wird entweder auf explizite Veranlassung erstellt (siehe „CIFS-Integrity-Monitoring >> CIFS-Integritätsstatus >> Anzeigen >> Aktionen“ auf Seite 6-173) oder zum Zeitpunkt der ersten regulären Prüfung des Laufwerkes.

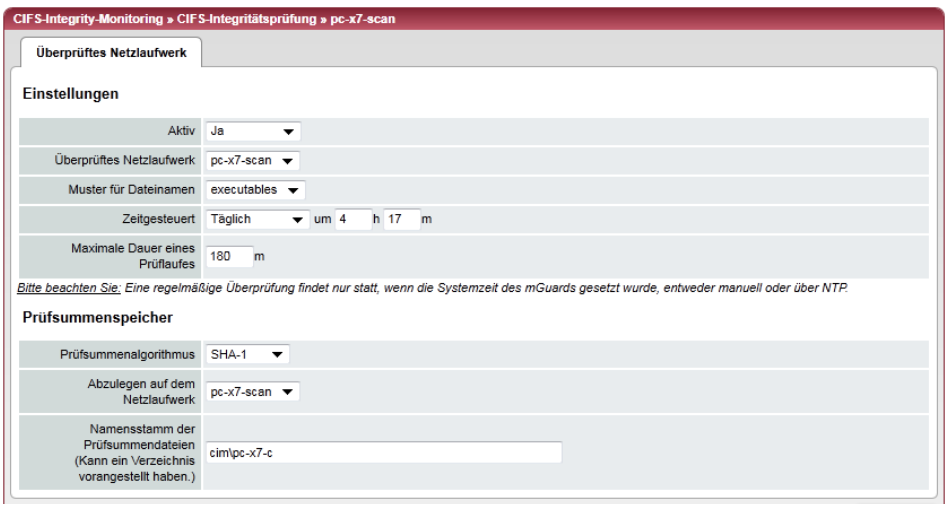
Nach einer gewollten Manipulation der relevanten Dateien des Netzlaufwerkes muss die Integritätsdatenbank neu erstellt werden. Solange keine (gültige) Integritätsdatenbank besteht, kann eine unerlaubte Manipulation der relevanten Dateien nicht entdeckt werden.

6.7.2.1 Einstellungen



CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Einstellungen		
Allgemein	**Integritätszertifikat (Verwendet zum Signieren von Integritätsdatenbanken)**	Dient zum Signieren und Prüfen der Integritätsdatenbank, damit diese nicht unbemerkt durch einen Angreifer ausgetauscht oder manipuliert werden kann. Informationen zu Zertifikaten finden Sie unter „Maschinenzertifikate“ auf Seite 6-136.
	Sende Benachrichtigung per E-Mail	**Nach jeder Prüfung**: An die unten angegebene Adresse wird nach jeder Prüfung eine E-Mail verschickt. **Nein:** An die unten angegebene Adresse wird keine E-Mail verschickt. **Nur bei Fehlern und Abweichungen**: An die unten angegebene Adresse wird eine E-Mail verschickt, wenn bei der CIFS-Integritätsprüfung eine Abweichung entdeckt worden ist, oder wenn die Prüfung auf Grund eines Zugriffsfehlers nicht stattfindet.
	Zieladresse für E-Mail-Benachrichtigungen	An diese Adresse wird eine E-Mail verschickt, entweder nach jeder Prüfung oder nur, wenn bei der CIFS-Integritätsprüfung eine Abweichung entdeckt worden ist, oder die Prüfung auf Grund eines Zugriffsfehlers nicht stattfinden konnte.
	Absenderadresse von E-Mail-Benachrichtigungen	Diese Adresse wird in der E-Mail als Absender eingetragen.
	Adresse des E-Mail-Servers	IP-Adresse oder Hostname des E-Mail-Servers, über den die E-Mail verschickt wird.
	Anfang des Betreffs für E-Mail-Benachrichtigung	Text für die Betreffzeile der E-Mail-Nachricht.

CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Einstellungen[...]		
Prüfung von Netzlaufwerken	**Aktiv**	**Nein**: Es wird keine Prüfung für dieses Netzlaufwerk ausgelöst. Der mGuard hat dieses Laufwerk nicht verbunden. Ein Status kann nicht eingesehen werden. **Ja**: Die Prüfung für dieses Netzlaufwerk wird regelmäßig ausgelöst. **Ausgesetzt**: Die Prüfung wird bis auf Weiteres ausgesetzt. Ein Status kann eingesehen werden.
	Überprüftes Netzlaufwerk	Name des zu prüfenden Netzlaufwerkes (wird unter *CIFS-Integrity-Monitoring >> Netzlaufwerke >> Editieren* angelegt).
	Prüfsummenspeicher	Um die Prüfung durchführen zu können, muss der mGuard ein Netzlaufwerk zum Auslagern der Dateien zur Verfügung gestellt bekommen. Der Prüfsummenspeicher darf über die externe Netzwerkschnittstelle erreichbar sein.
	Klicken Sie auf die Schaltfläche **Editieren**, um für die Prüfung der Netzlaufwerke weitere Einstellungen vorzunehmen.	

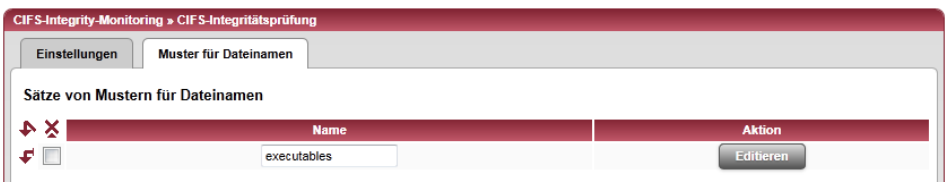


CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Einstellungen >> Editieren		
Einstellungen	**Aktiv**	**Nein**: Es wird keine Prüfung für dieses Netzlaufwerk ausgelöst. Der mGuard hat dieses Laufwerk nicht verbunden. Ein Status kann nicht eingesehen werden. **Ja**: Die Prüfung für dieses Netzlaufwerk wird regelmäßig ausgelöst. **Ausgesetzt**: Die Prüfung wird bis auf Weiteres ausgesetzt. Ein Status kann eingesehen werden.
	Überprüftes Netzlaufwerk	Name des zu prüfenden Netzlaufwerkes (wird unter *CIFS-Integrity-Monitoring >> Netzlaufwerke >> Editieren* angelegt).

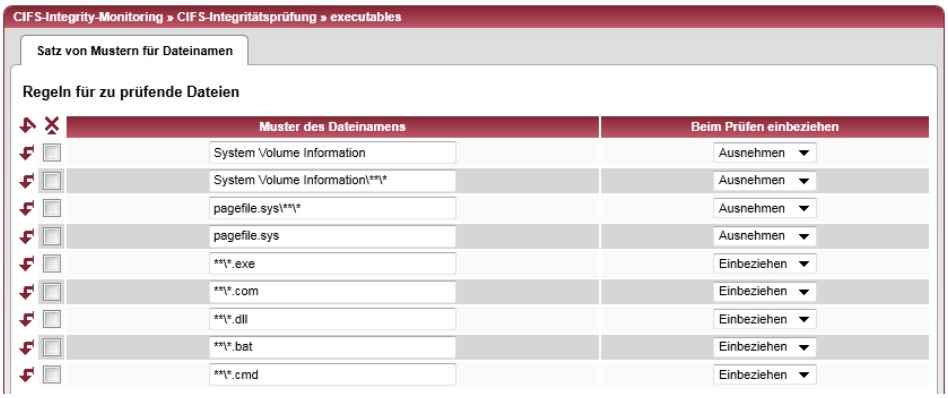
CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Einstellungen >> Editieren [...]		
	Muster für Dateinamen	Es werden bestimmte Datei-Typen geprüft (z. B. nur ausführbare Dateien wie *.exe, *.dll). Sie können die Regeln dafür unter *CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Muster für Dateinamen* einstellen. Lassen Sie keine Dateien prüfen, die im Regelbetrieb verändert werden, da sonst Fehlalarme ausgelöst werden. Lassen Sie keine Dateien prüfen, die gleichzeitig **exklusiv** von anderen Programmen geöffnet werden müssen, da dies zu Zugriffskonflikten führen kann.
	Zeitgesteuert	Täglich, Montags, Dienstags... um x h, x m Sie können täglich oder an einem bestimmte Wochentag die Prüfung um eine bestimmte Uhrzeit starten (Stunde, Minute). Damit die Zeitsteuerung funktioniert, muss die Systemzeit des mGuards gesetzt sein. Solange die Systemzeit nicht synchronisiert ist werden keine Integritätsprüfungen durchgeführt. Dies kann manuell oder über NTP geschehen (siehe „Zeit und Datum“ auf Seite 6-8). Eine Überprüfung wird nur gestartet, wenn der mGuard zum eingestellten Zeitpunkt in Betrieb ist. Ist er außer Betrieb, wird eine Prüfung nicht nachgeholt, wenn der mGuard später in Betrieb genommen wird. Sie können die Prüfung auch manuell starten („CIFS-Integrity-Monitoring >> CIFS-Integritätsstatus >> Anzeigen >> Aktionen“ auf Seite 6-173).
	Maximale Dauer eines Prüfablaufes	Maximale Dauer des Prüfablaufes in Minuten. So können Sie sicherstellen, dass die Prüfung rechtzeitig (z. B. vor Beginn des Schichtbetriebes) abgeschlossen sein wird.
Prüfsummenspeicher	**Prüfsummenalgorithmus**	**SHA-1** **MD5** **SHA-256** Prüfsummenalgorithmen wie MD5, SHA-1 oder SHA-256 helfen zu überprüfen, ob eine Datei verändert wurde. SHA-256 gilt als sicherer als SHA-1, benötigt aber länger in der Verarbeitung.

CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Einstellungen >> Editieren [...]		
	Abzulegen auf dem Netzlaufwerk	Um die Prüfung durchführen zu können, muss der mGuard ein Netzlaufwerk zum Auslagern der Dateien zur Verfügung gestellt bekommen. Der Prüfsummenspeicher darf über die externe Netzwerkschnittstelle erreichbar sein. Dasselbe Netzlaufwerk kann für verschiedene zu prüfende Netzlaufwerke als Prüfsummenspeicher verwendet werden. Der Namensstamm für die Prüfsummendateien muss dann allerdings eindeutig gewählt werden. Der mGuard merkt sich, welchen Versionstand die Prüfsummendateien auf dem Netzlaufwerk haben müssen. Wenn es zum Beispiel notwendig ist, nach einem Defekt des Netzlaufwerkes dessen Inhalt von einem Backup wieder herzustellen, dann werden zu alte Prüfsummendateien bereitgestellt werden, und der mGuard würde Abweichungen erkennen. In diesem Fall muss die Integritätsdatenbank neu erstellt werden (siehe „CIFS-Integrity-Monitoring >> CIFS-Integritätsstatus >> Anzeigen >> Aktionen“ auf Seite 6-173).
	Namensstamm der Prüfsummendateien (Kann ein Verzeichnis vorangestellt haben.)	Die Prüfsummendateien werden auf dem oben genannten Netzlaufwerk abgelegt. Sie können Sie auch in einem eigenen Verzeichnis ablegen. Der Verzeichnisname darf nicht mit einem Backslash (\) beginnen. Beispiel: Prüfsummenverzeichnis\integrity-checksum Es gibt ein Verzeichnis „Prüfsummenverzeichnis“ in dem Dateien liegen, die mit „integrity-checksum“ beginnen.

6.7.2.2 Muster für Dateinamen



CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Muster für Dateinamen		
Sätze von Mustern für Dateinamen	**Name**	Frei definierbarer Name für einen Satz von Regeln für die zu prüfenden Dateien. Dieser Name muss unter **CIFS-Integrity-Monitoring >>CIFS-Integritätsprüfung >> Einstellungen >> Editieren** ausgewählt sein, damit das Muster aktiv wird. Klicken Sie auf die Schaltfläche **Editieren**, um einen Satz von Regeln für die zu prüfenden Dateien festzulegen und unter dem definierten Namen zu speichern.



CIFS-Integrity-Monitoring >>CIFS-Integritätsprüfung >> Muster für Dateinamen >> Editieren

Regeln für zu prüfende Dateien

Muster des Dateinamens

Dabei gibt es folgende Regeln:

****.exe* bedeutet, dass Dateien einbezogen (oder ausgenommen) werden, die in einem beliebigen Verzeichnis liegen und die Dateiendung **.exe* haben.

Nur ein Platzhalter (*) ist pro Verzeichnis oder Dateiname erlaubt.

Platzhalter stehen für beliebige Zeichen, z. B. findet *win***.exe* Dateien mit der Endung *.exe*, die in einem Verzeichnis liegen, dass mit *win*... beginnt.

**** am Anfang bedeutet, dass in einem beliebigen Verzeichnis gesucht wird, auch in der obersten Ebene, wenn diese leer ist. Es kann nicht mit Zeichen kombiniert werden (z. B. *c*** ist nicht erlaubt).

Beispiel: *Name****.exe* bezieht alle Dateien mit der Endung .exe ein, die in dem Verzeichnis „*Name*“ und beliebigen Unterverzeichnissen liegen.

Fehlende Dateien führen zu einem Alarm. Fehlende Dateien sind Dateien, die beim Initialisieren vorhanden waren.

Ebenso gibt es einen Alarm, wenn zusätzliche Dateien vorhanden sind.

Beim Prüfen einbeziehen

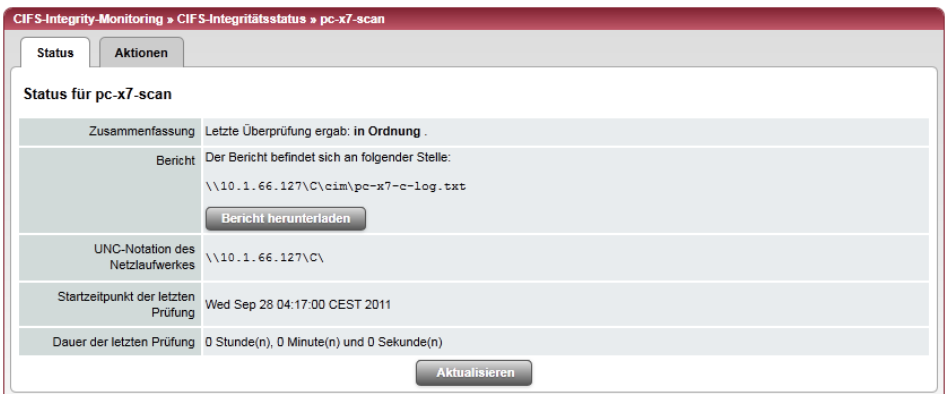
Einbeziehen: Die Dateien werden in die Prüfung einbezogen.

(Jeder Dateiname wird mit den Mustern der Reihe nach verglichen. Der erste Treffer entscheidet, ob die Datei in die Integritätsprüfung einbezogen wird. Ohne einen Treffer wird die Datei nicht einbezogen.)

Ausnehmen: Die Dateien werden aus der Prüfung ausgenommen.

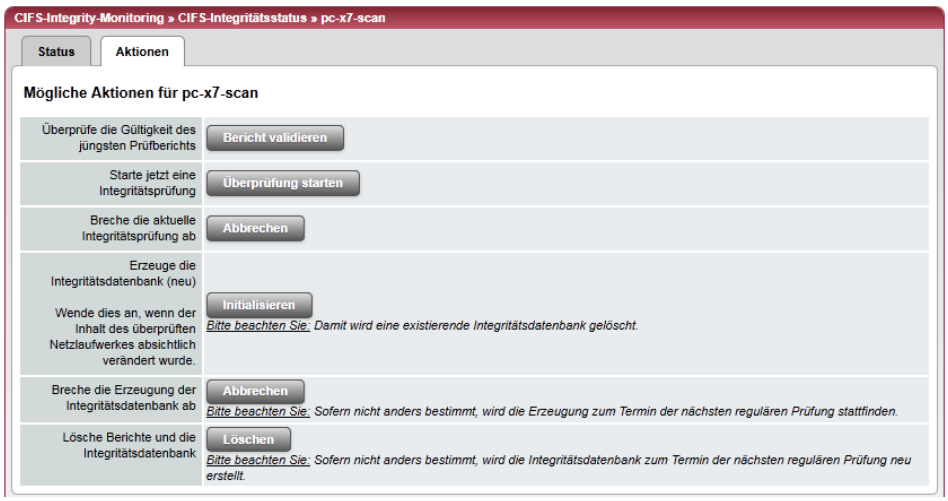
6.7.3 CIFS-Integrity-Monitoring >> CIFS-Integritätsstatus

CIFS-Integrity-Monitoring >> CIFS-Integritätsstatus		
	Liste mit Schaltflächen für jedes Netzlaufwerk einzeln	
Überprüftes Netzlaufwerk		Klicken Sie auf die Schaltfläche **Anzeigen**, um das Ergebnis der Prüfung zu sehen oder Aktionen auszuführen (wie Prüfung zu starten, abzubrechen oder eine Integritätsdatenbank zu aktualisieren, wenn die zu überprüfenden Netzlaufwerke absichtlich geändert worden sind). Klicken Sie auf die Schaltfläche **Editieren**, um die Einstellungen für die Prüfung zu überarbeiten (identisch mit „CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Einstellungen >> Editieren“ auf Seite 6-168).
Statuszusammenfassung		Ergebnis und Alter der letzten Prüfungen.
	Klicken Sie auf die Schaltfläche **Aktualisieren**, um eine Zusammenfassung der Ergebnisse der letzten Prüfungen zu sehen. Die Schaltfläche **Aktualisieren** bezieht sich auf alle Netzlaufwerke.	



CIFS-Integrity-Monitoring >> CIFS-Integritätsstatus >> Anzeigen >> Status		
Status für [Name des Netzlaufwerkes laut Konfiguration]	**Zusammenfassung**	**Letzte Prüfung ergab: in Ordnung:** keine Abweichungen gefunden **Letzte Prüfung fand x Abweichungen(n)**: Die genauen Abweichungen finden Sie im Prüfbericht.
	Bericht	Hier finden Sie den Prüfbericht. Er kann über die Schaltfläche **Bericht herunterladen** heruntergeladen werden.
	UNC-Notation des Netzlaufwerkes	\\Servername\Netzlaufwerk\

CIFS-Integrity-Monitoring >> CIFS-Integritätsstatus >> Anzeigen >> Status[...]		
	Startzeitpunkt der letzten Prüfung	Wochentag, Monat, Tag, HH:MM:SS koordinierte Weltzeit (UTC, Coordinated Universal Time). Die Landeszeit kann von dieser Zeit abweichen. **Beispiel**: Die Standardzeit in Deutschland ist die mitteleuropäische Zeit (MEZ), die gleich der UTC plus einer Stunde ist. Während der Sommerzeit gilt die mitteleuropäische Sommerzeit, die der UTC plus zwei Stunden entspricht.
	Dauer der letzten Prüfung	Dauer der Prüfung in Stunden und Minuten. (Wird nur angezeigt, wenn eine Prüfung stattgefunden hat.)
	Startzeitpunkt der aktuellen Prüfung	Siehe „Startzeitpunkt der letzten Prüfung“ auf Seite 6-173. (Wird nur angezeigt, wenn eine Prüfung stattgefunden hat.)
	Fortschritt der aktuellen Prüfung	Wird nur angezeigt, wenn eine Prüfung aktiv ist.



CIFS-Integrity-Monitoring >> CIFS-Integritätsstatus >> Anzeigen >> Aktionen		
Mögliche Aktionen für ...	**Überprüfe die Gültigkeit des jüngsten Prüfberichts**	Durch einen Klick auf die Schaltfläche **Bericht validieren,** wird geprüft, ob der Bericht in der vom mGuard erstellten Form unverändert vorliegt (Prüfung mit Hilfe von Signatur und Zertifikat).
	Starte jetzt eine Integritätsprüfung	Durch einen Klick auf die Schaltfläche **Überprüfung starten**, wird mit der Integritätsprüfung begonnen. Wird nur angezeigt, wenn keine Prüfung aktiv ist.
	Breche die aktuelle Integritätsprüfung ab	Durch einen Klick auf die Schaltfläche **Abbrechen**, wird die Integritätsprüfung gestoppt. Wird nur angezeigt, wenn eine Prüfung aktiv ist.

CIFS-Integrity-Monitoring >> CIFS-Integritätsstatus >> Anzeigen >> Aktionen [...]

Erzeuge die Integritätsdatenbank (neu)	Der mGuard legt eine Datenbank mit Prüfsummen an, um festzustellen ob sich Dateien verändert haben. Eine Veränderung von ausführbaren Dateien deutet auf einen Virenbefall hin. Wenn jedoch diese Dateien absichtlich verändert worden sind, muss durch einen Klick auf die Schaltfläche **Initialisieren** eine neue Datenbank erzeugt werden, um Fehlalarme zu verhindern. Das Erzeugen einer Integritätsdatenbank ist auch sinnvoll, wenn Netzlaufwerke neu eingerichtet worden sind. Sonst wird statt der Prüfung beim ersten Prüftermin eine Integritätsdatenbank eingerichtet.
Breche die Erzeugung der Integritätsdatenbank ab **Wird nur angezeigt, wenn eine erzeugt wird.**	Durch einen Klick auf die Schaltfläche **Abbrechen** bricht die Erzeugung der Integritätsdatenbank ab. Die alte Datenbank wird nicht weiter verwendet. Es muss dann entweder manuell eine neue Datenbank angelegt werden, oder sie wird automatisch zum Zeitpunkt der nächsten regulären Überprüfung des Laufwerkes neu erstellt. In der Zeit, in der keine Integritätsdatenbank besteht, kann der Inhalt des Laufwerkes unbemerkt manipuliert (z. B. infiziert) werden.
Lösche die Berichte und die Integritätsdatenbank	Durch einen Klick auf die Schaltfläche **Löschen** werden die vorhandenen Berichte/Datenbanken gelöscht. Für eine weitere Integritätsprüfung muss eine neue Integritätsdatenbank angelegt werden. Sie können dies über die Schaltfläche **Initialisieren** anstoßen**.** Ansonsten wird eine neue Integritätsdatenbank zum nächsten Prüftermin automatisch angelegt. Dieser Vorgang ist nicht sichtbar.

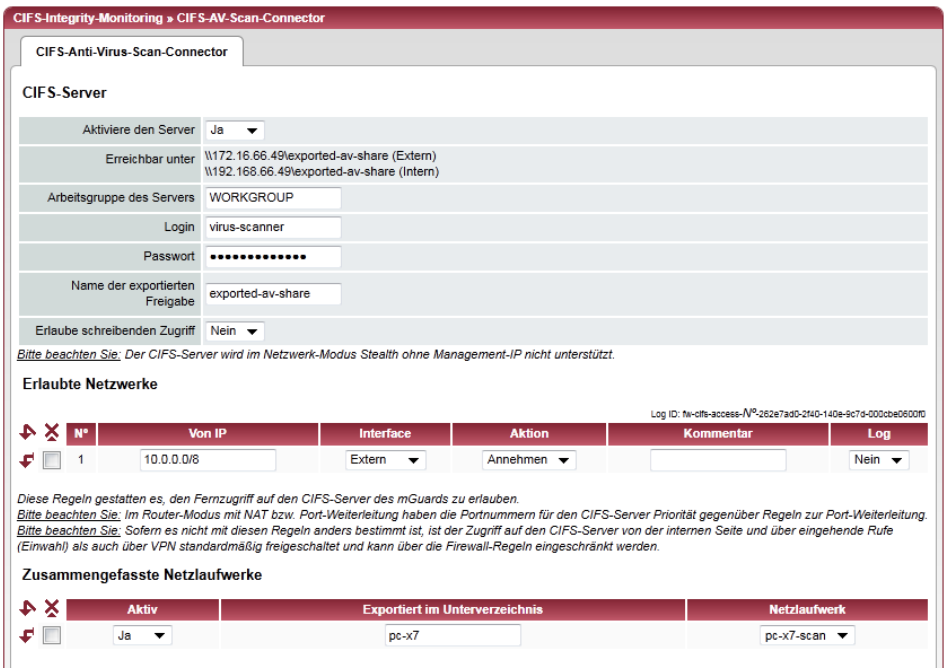
6.7.4 CIFS-Integrity-Monitoring >> CIFS-AV-Scan-Connector

Im Netzwerk-Modus Stealth ohne Management-IP wird der CIFS-Server für den Anti-Virus-Scan nicht unterstützt.

CIFS-Anti-Virus-Scan-Connector

Beim **CIFS-Anti-Virus-Scan-Connector** ermöglicht der mGuard einen Viren-Scan auf Laufwerke, die sonst von außen nicht erreichbar sind (z. B. Produktionszellen). Dabei spiegelt der mGuard ein Laufwerk nach außen, um dort den Viren-Scan durchführen zu lassen. Bei diesem Verfahren ist zusätzlich eine Anti-Virus-Software notwendig. Stellen Sie den für Ihre Anti-Virus-Software notwendigen Lese-Zugriff ein.

6.7.4.1 CIFS-Anti-Virus-Scan-Connector



CIFS-Integrity-Monitoring >> CIFS-Anti-Virus-Scan-Connector		
CIFS-Server	**Aktiviere den Server**	**Nein:** CIFS-Server ist nicht verfügbar **Ja:** CIFS-Server ist verfügbar

CIFS-Integrity-Monitoring >> CIFS-Anti-Virus-Scan-Connector [...]		
	Erreichbar unter	Anzeige des virtuellen Netzlaufwerkes, welches der mGuard für die Funktion CIFS-Anti-Virus-Scan-Connector bereitstellt. Dieser Pfad ist in UNC-Notation dargestellt. Sie können ihn durch Kopieren und Einfügen direkt auf dem PC verwenden, der das virtuelle Netzlaufwerk verwenden soll (siehe „Zugriff auf das virtuelle Netzlaufwerk (CIFS-Anti-Virus-Scan-Connector)“ auf Seite 6-178). Im Netzwerk-Modus „Router“ werden zwei (für das interne und externe Interface) und beim Netzwerk-Modus „Stealth“ eine UNC-Adresse angezeigt. Der Zugriff auf das virtuelle Netzlaufwerk kann wegen der Einstellungen im Abschnitt „Erlaubte Netzwerke“ verhindert werden. Tragen Sie eine entsprechende Regel ein, besonders wenn der Zugriff über das externe Interface gewünscht ist. Weitere Zugriffsmöglichkeiten können je nach Konfiguration des mGuards über andere IP-Adressen bestehen, zum Beispiel über VPN-Kanäle oder über eingehende Rufe (die Einwahl, siehe „Eingehender Ruf“ auf Seite 6-97.)
	Arbeitsgruppe des Servers	Name der Arbeitsgruppe des CIFS-Servers.
	Login	Login für den Server.
	Passwort	Passwort für den Login.
	Name der exportieren Freigabe	Name, der für Rechner einzustellen ist, die den CIFS-Server verwenden wollen, um auf die zusammengefassten Laufwerke zuzugreifen. (Unter diesem Namen die Laufwerke verbinden.)
	Erlaube schreibenden Zugriff	**Nein:** Nur Lese-Zugriff **Ja:** Schreib- und Lese-Zugriff
Erlaubte Netzwerke	Diese Regeln erlauben es, von außen auf den CIFS-Server des mGuards zuzugreifen.	
	Im Router-Modus mit NAT- bzw. Port-Weiterleitung haben die Portnummern für den CIFS-Server Priorität gegenüber den Regeln zur Port-Weiterleitung. (Port-Weiterleitungen werden unter „Netzwerk >> NAT“ eingestellt.)	
	Standardmäßig ist der Zugriff auf den CIFS-Server von der internen Seite sowohl über eingehende Rufe (Einwahl) als auch über VPN freigeschaltet und kann über die Firewall-Regeln eingeschränkt und erweitert werden. Die Standardeinstellung kann mit diesen Regeln anders bestimmt werden.	
	Von IP	Geben Sie hier die Adresse des Rechners/Netzes an, von dem der Fernzugriff erlaubt beziehungsweise verboten ist. IP-Adresse: **0.0.0.0/0** bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise (siehe 6-261).

CIFS-Integrity-Monitoring >> CIFS-Anti-Virus-Scan-Connector [...]		
	Interface	**Extern / Intern / Extern 2 / VPN / Einwahl**[1] Gibt an, für welches Interface die Regel gelten soll. Sind keine Regeln gesetzt oder es greift keine Regel, gelten folgende Standardeinstellungen: – Der Fernzugang ist erlaubt über *Intern, VPN* und *Einwahl*. – Zugriffe über *Extern* und *Extern 2* werden verwehrt. Legen Sie die Zugriffsmöglichkeiten nach Bedarf fest. Wenn Sie Zugriffe über *Intern, VPN* oder *Einwahl* verwehren wollen, müssen Sie das explizit durch entsprechende Firewall-Regeln bewirken, in der Sie als Aktion z. B. *Verwerfen* festlegen.
	Aktion	**Annehmen** bedeutet, die Datenpakete dürfen passieren. **Abweisen** bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat Abweisen dieselbe Wirkung wie Verwerfen.) **Verwerfen** bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information über deren Verbleib erhält.
	Kommentar	Ein frei wählbarer Kommentar für diese Regel.
	Log	Für jede einzelne Regel können Sie festlegen, ob beim Greifen der Regel – das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen – oder nicht - *Log* auf **Nein** setzen (werkseitige Voreinstellung).
Zusammengefasste Netzlaufwerke	**Aktiv**	**Nein:** Dieses Netzlaufwerk wird nicht gespiegelt. **Ja:** Dieses Netzlaufwerk wird gespiegelt und zur Verfügung gestellt.
	Exportiert im Unterverzeichnis	In diesem Verzeichnis können mehrere Laufwerke zu einem zusammengefasst werden.
	Netzlaufwerk	Name des zu importierenden Netzlaufwerkes (wird unter *CIFS-Integrity-Monitoring* >> *Netzlaufwerke* >> *Editieren* angelegt)

1 *Extern 2* und *Einwahl* nur bei Geräten mit serieller Schnittstelle (siehe „Netzwerk >> Interfaces“ auf Seite 6-64).

Zugriff auf das virtuelle Netzlaufwerk (CIFS-Anti-Virus-Scan-Connector)

Sie können das virtuelle Netzlaufwerk das der mGuard für den CIFS-Anti-Virus-Scan-Connector bereitstellt, im Windows Explorer einbinden. Dazu im Explorer das Menü "Extras, Netzlaufwerk verbinden..." öffnen und den Pfad in UNC-Notation angeben.

Dieser Pfad wird Ihnen unter „CIFS-Integrity-Monitoring >> CIFS-Anti-Virus-Scan-Connector >> Erreichbar unter“ angezeigt.

\\<Externe IP mGuard>\<Name der exportierten Freigabe> bzw.
\\<Interne IP mGuard>\<Name der exportierten Freigabe>

Beispiel

\\10.1.66.49\exported-av-share

\\192.168.66.49\exported-av-share

Alternativ können Sie den Befehl „net use“ in die Befehlszeile eingeben. Nähere Informationen dazu finden sie in der Produktfinformation von Mircosoft.

Hinweise

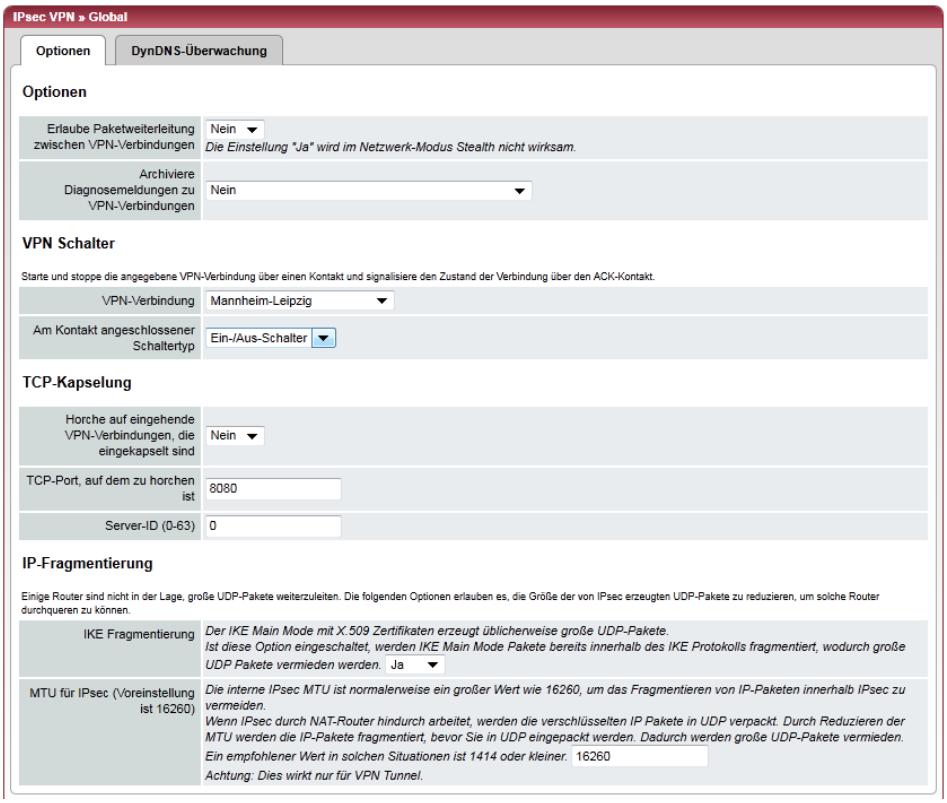
- Anstelle der IP-Adresse können Sie auch einen DNS-Namen verwenden.
- Das freigegebene Netzlaufwerk kann nicht über browsen oder die Suchfunktionen gefunden werden.
- Der „Name der exportieren Freigabe“ muss immer hinzugefügt werden.
- Windows zeigt das freigegebene Netzlaufwerk nicht automatisch an, wenn der mGuard angeschlossen wird.

6.8 Menü IPsec VPN

Dieses Menü steht **nicht** auf dem **mGuard blade-Controller** zur Verfügung.

6.8.1 IPsec VPN >> Global

6.8.1.1 Optionen



IPsec VPN >> Global >> Optionen

Optionen

Erlaube Paketweiterleitung zwischen VPN-Verbindungen

Die Einstellung **Ja** wird nur auf dem mGuard benötigt, der zwischen zwei verschiedenen VPN-Gegenstellen vermitteln soll.

Damit die Vermittlung zwischen zwei VPN-Gegenstellen funktioniert, muss auf dem vermittelnden mGuard das lokale Netzwerk so konfiguriert werden, dass die Remote-Netze, in denen sich die VPN-Gegenstellen befinden, enthalten sind. Natürlich muss das umgekehrt (lokales und entferntes Netz vertauscht) auch bei den VPN-Gegenstellen so eingerichtet sein (siehe „Remote“ auf Seite 6-195).

Die Einstellung **Ja** wird im Netzwerk-Modus *Stealth* nicht unterstützt.

Bei **Nein** (Standard): VPN-Verbindungen existieren für sich separat.

Bei **Ja**: Hub and Spoke Feature eingeschaltet: Eine Zentrale unterhält VPN-Verbindungen zu mehreren Zweigstellen, die auch untereinander kommunizieren können.

Bei Aufbau solch einer sternförmigen Topologie von VPN-Verbindungen können Gegenstellen des mGuards auch untereinander Daten austauschen. In diesem Fall ist zu empfehlen, dass der lokale mGuard für die Authentifizierung möglicher Gegenstellen CA-Zertifikate heranzieht (siehe „Authentifizierung“ auf Seite 6-204).

Archiviere Diagnosemeldungen zu VPN-Verbindungen: Nein / Nur beim Start mittels nph-vpn.cgi (oder CMD-Kontakt)

Der CMD-Kontakt steht nur beim mGuard rs4000/2000 und beim mGuard industrial rs zur Verfügung

Falls beim Aufbau von VPN-Verbindungen Fehler auftreten, kann das Logging des mGuards herangezogen und anhand entsprechender Einträge die Fehlerquelle ausfindig gemacht werden (Siehe Menüpunk *Logging >> Logs ansehen*). Diese Möglichkeit zur Fehlerdiagnose ist standardmäßig gegeben, und wenn sie ausreichend ist, setzen Sie diesen Schalter auf **Nein** (Standard).

Option **Nur beim Start mittels nph-vpn.cgi (oder CMD-Kontakt):**

Wird die Möglichkeit zur Diagnose von VPN-Verbindungsproblemen anhand des Loggings des mGuards als zu unpraktisch oder unzureichend empfunden, wählen Sie diese Option. Das ist möglicherweise der Fall, wenn folgende Bedingungen vorliegen:

IPsec VPN >> Global >> Optionen [...]

- In bestimmten Anwendungsumgebungen, z. B. wenn der mGuard per Maschinensteuerung über den CMD-Kontakt „bedient“ wird (nur bei *mGuard rs4000/2000* und beim *mGuard industrial rs*), steht die Möglichkeit, dass ein Anwender über die Webbasierte Bedienoberfläche des mGuards die Logdatei des mGuards einsieht, vielleicht gar nicht zur Verfügung.
- Bei dezentralem Einsatz kann es vorkommen, dass eine Diagnose eines VPN-Verbindungsfehlers erst möglich ist, nachdem der mGuard vorübergehend von seiner Stromquelle getrennt worden ist - was zum Löschen aller Logeinträge führt.
- Die relevanten Logeinträge des mGuards, die Aufschluss geben könnten, sind eventuell gelöscht, weil der mGuard aufgrund seines endlichen Speicherplatzes ältere Logeinträge regelmäßig löscht.
- Wird ein mGuard als zentrale VPN-Gegenstelle eingesetzt, z. B. in einer Fernwartungszentrale als Gateway für die VPN-Verbindungen vieler Maschinen, werden die Meldungen zu Aktivitäten der verschiedenen VPN-Verbindungen im selben Datenstrom protokolliert. Das dadurch entstehende Volumen des Logging macht es zeitaufwendig, die für einen Fehler relevanten Informationen zu finden.

Nach Einschalten der Archivierung werden relevante Logeinträge über die Vorgänge beim Aufbau von VPN-Verbindungen im nicht flüchtigen Speicher des mGuards archiviert, wenn die Verbindungsaufbauten wie folgt veranlasst werden:

- über den CMD-Kontakt, oder
- über das CGI-Interface nph-vpn.cgi per Kommando „synup“ (siehe *Application Note: Diagnosis of VPN connections*). (Application Notes stehen im Download-Bereich von www.innominate.com bereit.)

Archivierte Logeinträge überleben einen Neustart. Sie können als Bestandteil des Support-Snapshots (Menüpunkt *Support >> Erweitert* , Registerkarte *Snapshot*) heruntergeladen werden. Der Support Ihres Händlers erhält durch solch einen Snapshot erweiterte Möglichkeiten, effizienter nach Problemursachen zu suchen und diese zu finden, als ohne die Archivierung möglich wäre.

Archiviere Diagnosemeldungen nur bei Fehlern: Ja / Nein	Nur sichtbar, wenn Archivierung eingeschaltet ist. Sollen nach Einschalten der Archivierung nur solche Logeinträge archiviert werden, die bei fehlgeschlagenen Verbindungsaufbauversuchen erzeugt werden, setzen Sie diesen Schalter auf **Ja**. Bei **Nein** werden alle Logeinträge archiviert.

IPsec VPN >> Global >> Optionen [...]

VPN-Schalter

Nur bei mGuard rs4000/rs2000 und mGuard industrial rs

VPN-Verbindung

Der mGuard rs4000/rs2000 und der mGuard industrial rs verfügen über Anschlüsse, an die ein externer Taster oder Ein/Aus-Schalter und eine Signal-LED angeschlossen werden können. Über den Taster bzw. Ein/Aus-Schalter kann eine der konfigurierten VPN-Verbindungen aufgebaut und wieder abgebaut werden. Welche VPN-Verbindung das ist, wird hier festgelegt:

Sind unter dem Menüpunkt *IPsec VPN >> Verbindungen* (siehe Seite 6-189) VPN-Verbindungen konfiguriert und aufgelistet, werden diese in der Auswahlliste angezeigt. Soll eine davon manuell auf Tastendruck bzw. durch Schalterbetätigung aufgebaut und wieder abgebaut werden können, wählen Sie diese hier aus.

Ist das Starten und Stoppen der VPN-Verbindung über den CMD-Kontakt eingeschaltet, hat ausschließlich der CMD-Kontakt das Recht dazu.

D. h. die Einstellung des Schalters Aktiv für die gesamte VPN-Verbindung hat keine Wirkung.

Ist am CMD-Kontakt ein Taster (statt eines Schalters - siehe unten) angeschlossen, kann der Verbindungsaufbau und -abbau aber auch gleichberechtigt und konkurrierend über die Kommandos des CGI-Skriptes nph-vpn.cgi erfolgen.

Bei **Aus** ist diese Funktion ausgeschaltet. Ist an den Service Kontakten des mGuards ein Taster oder Ein/Aus-Schalter angeschlossen, dann hat dessen Betätigung keine Wirkung.

Wenn eine VPN-Verbindung über einen VPN-Schalter gesteuert wird, dann kann die VPN-Redundanz nicht aktiviert werden.

IPsec VPN >> Global >> Optionen [...]

Nur bei mGuard rs4000/rs2000 und mGuard industrial rs

Am Kontakt angeschlossener Schaltertyp:

Taster / Ein-/Aus-Schalter

Der mGuard rs4000/rs2000 und der mGuard industrial rs verfügen über Anschlüsse, an die ein externer Taster/Schalter und eine Signal-LED angeschlossen werden können. Wählen Sie den Schaltertyp aus, der an den entsprechenden Service-Kontakten des mGuards angeschlossen ist.

Mehr dazu siehe

– „mGuard rs4000/rs2000 installieren“ auf Seite 4-4 unter **Service-Kontakte**.
– „mGuard industrial rs installieren“ auf Seite 4-12 unter **Service-Kontakte**.

Dort wird auch die unterschiedliche Bedienung der Schaltertypen beschrieben.

Ist durch entsprechende Betätigung des Tasters oder Schalters eine VPN-Verbindung aufgebaut, so bleibt diese bestehen, bis sie durch Taster- bzw. Schalterbetätigung wieder abgebaut wird.

Wird ein Ein/Aus-Schalter (statt Taster) verwendet und ist durch dessen Betätigung eine VPN-Verbindung aufgebaut worden, wird diese nach einem Neustart des mGuards automatisch wieder aufgebaut.

TCP-Kapselung

Die Funktion dient dazu, die über eine VPN-Verbindung zu übertragenden Datenpakete in TCP-Pakete einzukapseln. Ohne diese Einkapselung kann es bei VPN-Verbindungen unter Umständen passieren, dass z. B. durch zwischengeschaltete NAT-Router, Firewalls oder Proxy-Server wichtige Datenpakete, die zu einer VPN-Verbindung gehören, nicht ordnungsgemäß übertragen werden.

Zum Beispiel können Firewalls so eingestellt sein, dass keine Datenpakete des UDP-Protokolls durchgelassen werden oder (mangelhaft implementierte) NAT-Router könnten bei UDP-Paketen die Port-Nummern nicht korrekt verwalten.

Durch die TCP-Kapselung werden diese Probleme vermieden, weil die zur betreffenden VPN-Verbindung gehörenden Pakete in TCP-Pakete eingekapselt, d. h. verborgen sind, so dass für die Netz-Infrastruktur nur TCP-Pakete in Erscheinung treten

Der mGuard kann in TCP gekapselte VPN-Verbindungen annehmen, selbst wenn er im Netzwerk hinter einem NAT-Gateway angeordnet ist und deshalb von der VPN-Gegenstelle nicht unter seiner primären externen IP-Adresse erreicht werden kann. Das NAT-Gateway muss dafür den entsprechenden TCP-Port zum mGuard weiterreichen (siehe „Horche auf eingehende VPN-Verbindungen, die eingekapselt sind“ auf Seite 6-185).

TCP-Kapselung kann nur eingesetzt werden, wenn auf beiden Seiten des VPN-Tunnels ein mGuard (ab Version 6.1) eingesetzt wird.

TCP-Kapselung sollte nur eingesetzt werden, wenn es erforderlich ist. Denn durch die beträchtliche Vergrößerung des Datenpaket-Overheads und durch entsprechend verlängerte Verarbeitungszeiten werden Verbindungen langsamer.

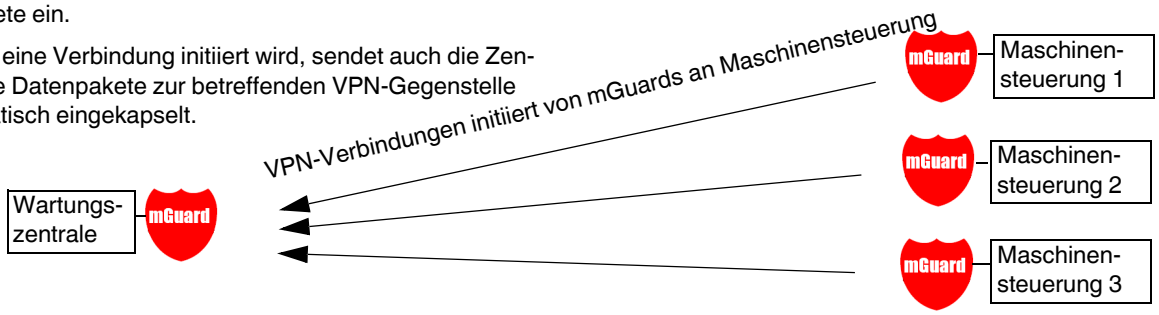
Ist beim mGuard unter Menüpunkt „Netzwerk >> Proxy-Einstellungen“ festgelegt, dass ein Proxy für HTTP und HTTPS benutzt wird, dann wird dieser auch für VPN-Verbindungen verwendet, bei denen TCP-Kapselung eingesetzt wird.

TCP-Kapselung unterstützt die Authentifizierungsverfahren *Basic Authentification* und *NTLM* gegenüber dem Proxy.

Damit die TCP-Kapselung durch einen HTTP-Proxy hindurch funktioniert, muss einerseits der Proxy explizit in den Proxy-Einstellungen (Menüpunkt „Netzwerk >> Proxy-Einstellungen“) benannt werden (darf also kein transparenter Proxy sein) und andererseits muss dieser Proxy die HTTP-Methode CONNECT verstehen und erlauben.

Als Teilnehmer der TCP-Kapselung initiieren die mGuards der Maschinensteuererungen den VPN-Datenverkehr zur Wartungszentrale und kapseln die zu ihr gesendeten Datenpakete ein.

Sobald eine Verbindung initiiert wird, sendet auch die Zentrale die Datenpakete zur betreffenden VPN-Gegenstelle automatisch eingekapselt.



mGuard der Wartungszentrale

Erforderliche Grundeinstellungen

– Menüpunkt **IPsec VPN,** *Global*, Register *Optionen*:
  Horche auf eingehende VPN-Verbindungen, die eingekapselt sind: **JA**
– Untermenü *Verbindungen,*
  Register *Allgemein*:
  Adresse des VPN-Gateways der Gegenstelle: **%any**
  Verbindungsinitiierung: **Warte**

mGuards an Maschinensteuererungen

Erforderliche Grundeinstellungen

– Menüpunkt **IPsec VPN**, *Global, Register Optionen*:
  Horche auf eingehende VPN-Verbindungen, die eingekapselt sind: **NEIN**
– Untermenü *Verbindungen,* Register *Allgemein*:
  Adresse des VPN-Gateways der Gegenstelle: Feste IP-Adresse oder Hostname
  Verbindungsinitiierung: **Initiiere** oder **Initiiere bei Datenverkehr**
  Kapsele den VPN-Datenverkehr in TCP ein: **JA**

Bild 6-2 TCP-Kapselung bei einem Anwendungsszenario mit Wartungszentrale und ferngewarteten Maschinen über VPN-Verbindungen

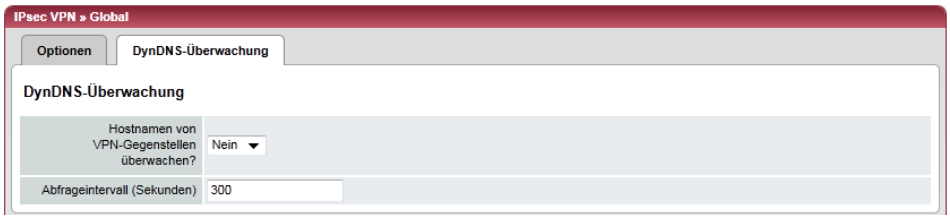
IPsec VPN >> Global >> Optionen

TCP-Kapselung	**Horche auf eingehende VPN-Verbindungen, die eingekapselt sind**	Standardeinstellung: **Nein**. Nur bei Einsatz der Funktion TCP-Kapselung diesen Schalter auf **Ja** setzen. Nur dann kann der mGuard Verbindungsaufbauten mit eingekapselten Paketen annehmen. Aus technischen Gründen erhöht sich der Bedarf an Hauptspeicher (RAM) mit jeder Schnittstelle, an welcher auf in TCP gekapselte VPN-Verbindungen gehorcht werden muss. Wenn auf mehreren Schnittstellen gehorcht werden muss, muss das Gerät mindestens 64 MB RAM haben. Auf welchen Schnittstellen gehorcht werden muss, ermittelt der mGuard aus den Einstellungen der aktiven VPN-Verbindungen, die „%any“ als Gegenstelle konfiguriert haben. Die Einstellung unter „Interface, welches bei der Einstellung %any für das Gateway benutzt wird“ ist ausschlaggebend.

IPsec VPN >> Global >> Optionen [...]		
	TCP-Port, auf dem zu horchen ist	Nummer des TCP-Ports, über den die zu empfangenen eingekapselten Datenpakete eingehen. Die hier angegebene Portnummer muss mit der Portnummer übereinstimmen, die beim mGuard der Gegenstelle als **TCP-Port des Servers, welche die gekapselte Verbindung annimmt** festgelegt ist (Menüpunkt *IPsec VPN >> Verbindungen* , Editieren, Registerkarte *Allgemein*). Es gelten folgende Einschränkung: – Der Port, auf dem zu horchen ist, darf nicht identisch sein mit einem Port, der für Fernzugriff benutzt wird (SSH, HTTPS oder SEC-Stick).
	Server ID (0-63)	Der Standardwert **0** muss normalerweise nicht geändert werden. Die Nummern dienen zur Unterscheidung unterschiedlicher Zentralen. Eine andere Nummer muss nur in folgendem Fall verwendet werden: Ein mGuard, vorgeschaltet einer Maschine, muss zu zwei oder mehreren verschiedenen Wartungszentralen und deren mGuards Verbindungen mit eingeschalteter TCP-Kapselung aufnehmen.
IP-Fragmentierung	**IKE-Fragmentierung:**	UDP-Pakete können insbesondere dann übergroß werden, wenn bei Aufbau einer IPsec-Verbindung die Verbindung zwischen den beteiligten Geräten per IKE ausgehandelt wird und dabei Zertifikate ausgetauscht werden. Es gibt Router, die nicht in der Lage sind, große UDP-Pakete weiterzuleiten, wenn diese auf dem Übertragungsweg (z. B. per DSL in 1500 Bytes große Stücke) fragmentiert worden sind. Manches defekte Gerät leitet dann nur das erste Fragment weiter, so dass dann die Verbindung fehlschlägt. Wenn zwei mGuards miteinander kommunizieren, kann von vornherein dafür gesorgt werden, dass nur kleine UDP-Pakete ausgesandt werden. Damit wird verhindert, dass die Pakete unterwegs fragmentiert und damit möglicherweise von einigen Routern nicht korrekt weitergeleitet werden. Wenn Sie diese Option nutzen wollen, setzen Sie diesen Schalter auf **Ja**.  Wird der Schalter auf **Ja** gesetzt, ist diese Einstellung nur wirksam, wenn die Gegenstelle ein mGuard ist, auf dem die Firmware ab Version 5.1.0 installiert ist. In allen anderen Fällen bleibt die Einstellung unwirksam, schadet aber nicht.

IPsec VPN >> Global >> Optionen [...]		
	MTU für IPsec (Voreinstellung ist 16260)	Die Option zur Vermeidung übergroßer IKE-Datenpakete, die von defekten Routern auf dem Übertragungsweg nicht korrekt weitergeleitet werden könnten, gibt es auch für IPsec-Datenpakete. Um unter der oft durch DSL gesetzten Obergrenze von 1500 Bytes zu bleiben, wird ein Wert von 1414 (Bytes) empfohlen, so dass auch für zusätzliche Header genügend Platz bleibt. Wenn Sie diese Option nutzen wollen, legen Sie einen niedrigeren Wert als die Voreinstellung fest.

6.8.1.2 DynDNS-Überwachung



Erläuterung zu DynDNS siehe „DynDNS“ auf Seite 6-115.

IPsec VPN >> Global >> Optionen		
DynDNS-Überwachung	**Hostnamen von VPN-Gegenstellen überwachen?**	**Ja / Nein** Ist dem mGuard die Adresse einer VPN-Gegenstelle als Hostname angegeben (siehe „VPN-Verbindung / VPN-Verbindungskanäle definieren“ auf Seite 6-190), und ist dieser Hostname bei einem DynDNS-Service registriert, dann kann der mGuard regelmäßig überprüfen, ob beim betreffenden DynDNS eine Änderung erfolgt ist. Falls ja, wird die VPN-Verbindung zu der neuen IP-Adresse aufgebaut.
	Abfrageintervall (Sekunden)	Standard: 300

6.8.2 IPsec VPN >> Verbindungen

Voraussetzungen für eine VPN-Verbindung

Generelle Voraussetzung für eine VPN-Verbindung ist, dass die IP-Adressen der VPN-Partner bekannt und zugänglich sind.

- Die mGuards, die im Netzwerk-Modus Stealth ausgeliefert werden, sind auf die Stealth-Konfiguration „mehrere Clients“ voreingestellt. In diesem Modus müssen Sie, wenn Sie VPN-Verbindungen nutzen wollen, eine Management IP-Adresse und ein Standard-Gateway konfigurieren (siehe Seite 6-74). Alternativ können Sie eine andere Stealth-Konfiguration als „mehrere Clients“ wählen oder einen anderen Netzwerk-Modus verwenden.
- Damit eine IPsec-Verbindung erfolgreich aufgebaut werden kann, muss die VPN-Gegenstelle IPsec mit folgender Konfiguration unterstützen:
  - Authentifizierung über Pre-Shared Key (PSK) oder X.509-Zertifikate
  - ESP
  - Diffie-Hellman Gruppe 2 oder 5
  - DES, 3DES oder AES encryption
  - MD5, SHA-1 oder SHA-2 Hash Algorithmen
  - Tunnel oder Transport Modus
  - Quick Mode
  - Main Mode
  - SA Lifetime (1 Sekunde bis 24 Stunden)

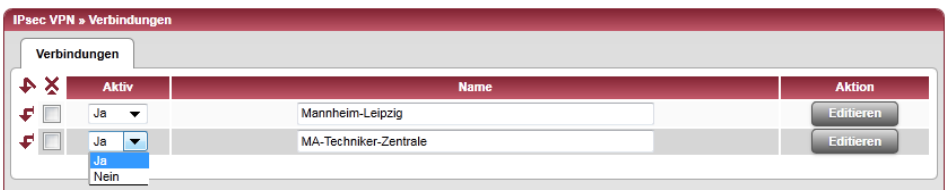
  Ist die Gegenstelle ein Rechner unter Windows 2000, muss dazu das *Microsoft Windows 2000 High Encryption Pack* oder mindestens das *Service Pack 2* installiert sein.
- Befindet sich die Gegenstelle hinter einem NAT-Router, so muss die Gegenstelle NAT-T unterstützen. Oder aber der NAT-Router muss das IPsec-Protokoll kennen (IPsec/VPN Passthrough). In beiden Fällen sind aus technischen Gründen nur IPsec Tunnel-Verbindungen möglich.

6.8.2.1 Verbindungen

Liste aller VPN-Verbindungen, die definiert worden sind.

Jeder hier aufgeführte Verbindungsname kann eine einzige VPN-Verbindung oder eine Gruppe von VPN-Verbindungskanälen bezeichnen. Denn es gibt die Möglichkeit, unter den Transport- und/oder Tunneleinstellungen des betreffenden Eintrags mehrere Tunnel zu definieren.

Sie haben die Möglichkeit, neue VPN-Verbindungen zu definieren, VPN-Verbindungen zu aktivieren / deaktivieren, die Eigenschaften einer VPN-Verbindung oder -Verbindungsgruppe zu ändern (editieren) und Verbindungen zu löschen.



VPN-Verbindung / VPN-Verbindungskanäle neu definieren:

- In der Tabelle der Verbindungen beim Eintrag mit dem Namen „(unnamed)“ auf die Schaltfläche **Editieren** klicken.
- Falls „(unnamed)“ nicht sichtbar ist, in der Tabelle eine weitere Zeile öffnen.

VPN-Verbindung / VPN-Verbindungskanäle bearbeiten:

- Rechts im betreffenden Eintrag auf die Schaltfläche **Editieren** klicken.

URL für Starten, Stoppen, Statusabfrage einer VPN-Verbindung

Die folgende URL kann verwendet werden, um VPN-Verbindungen unabhängig von ihrer **Aktiv** Einstellung zu starten, zu stoppen oder den Verbindungsstatus abzufragen:

https://server/nph-vpn.cgi?name=verbindung&cmd=(up|down|status)

Beispiel

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

Die Option ***--no-check-certificate*** sorgt dafür, dass das HTTPS-Zertifikat des mGuards nicht weiter geprüft wird.

Es kann ebenfalls für die URL notwendig sein, das Passwort zu codieren, wenn es Sonderzeichen enthält.

Ein solches Kommando bezieht sich auf alle Verbindungskanäle, die unter dem betreffenden Namen, in diesem Beispiel *Athen*, zusammengefasst sind. Das ist der Name, der auf der Registerkarte *Allgemein* als „Ein beschreibender Name für die VPN-Verbindung“ aufgeführt ist. Sofern Mehrdeutigkeit besteht, wirkt der Aufruf des URL nur auf den ersten Eintrag in der Liste der Verbindungen.

Ein Ansprechen einzelner Kanäle einer VPN-Verbindung ist nicht möglich. Sind einzelne Kanäle deaktiviert (**Aktiv**: Nein), werden diese nicht gestartet. Damit hat das Starten und Stoppen auf diesem Wege keine Auswirkung auf die Einstellungen zu den einzelnen Kanälen (= die Liste unter *Transport- und Tunneleinstellungen*).

Das Starten und Stoppen einer Verbindung per URL macht nur Sinn, wenn in der Konfiguration die Verbindung deaktiviert ist (**Aktiv**: Nein) oder wenn die **Verbindungsinitiierung** auf „Warte“ eingestellt ist. Ansonsten wird die Verbindung vom mGuard selbständig (wieder) aufgebaut.

Wenn durch Verwendung der oben angegeben URL der Status einer VPN-Verbindung abgefragt wird, können folgende Antworten erwartet werden:

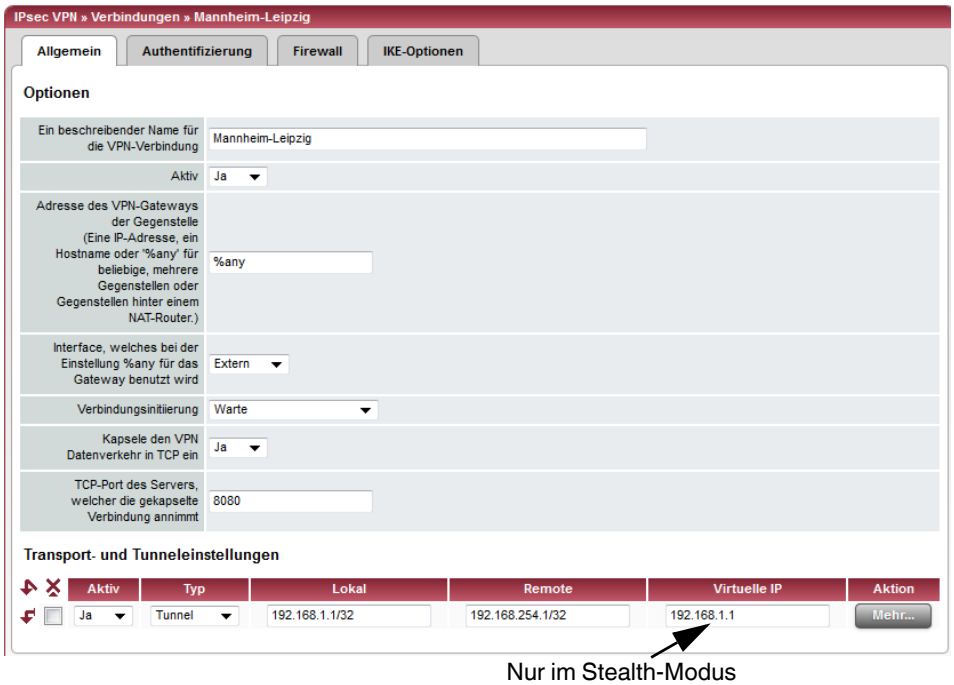
Tabelle 6-1 Status einer VPN-Verbindung

Antwort	Bedeutung
unknown	Eine VPN-Verbindung mit dem Namen existiert nicht.
void	Die Verbindung 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). Die Antwort "void" wird von der CGI-Schnittstelle auch herausgegeben, ohne dass ein Fehler vorliegt. Zum Beispiel, wenn die VPN-Verbindung entsprechend der Konfiguration deaktiviert ist (Spalte auf **Nein**) und nicht vorübergehend mit Hilfe der CGI-Schnittstelle oder des CMD-Kontaktes freigeschaltet worden ist.
ready	Die Verbindung ist bereit, selbst Kanäle aufzubauen oder hereinkommende Anfragen zum Kanalaufbau zu erlauben.
active	Zu der Verbindung ist mindestens ein Kanal auch wirklich aufgebaut.

VPN-Verbindung / VPN-Verbindungskanäle definieren

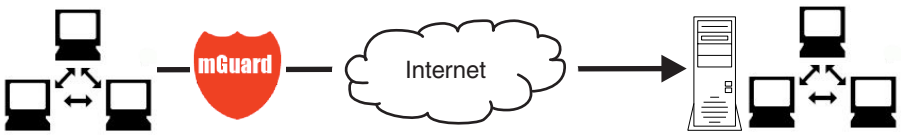
Nach Klicken auf **Editieren** erscheint je nach Netzwerk-Modus des mGuards folgende Seite.

6.8.2.2 Allgemein



IPsec VPN >> Verbindungen >> Editieren >> Allgemein		
Optionen	**Ein beschreibender Name für die VPN-Verbindung**	Sie können die Verbindung frei benennen bzw. umbenennen. Werden weiter unten unter *Transport und Tunneleinstellungen* mehrere Verbindungskanäle definiert, benennt dieser Name das gesamte Set der VPN-Verbindungskanäle, die unter diesem Namen zusammengefasst sind. Gemeinsamkeiten bei VPN-Verbindungskanälen: – gleiches Authentifizierungsverfahren, festgelegt auf der Registerkarte *Authentifizierung* (siehe „Authentifizierung“ auf Seite 6-204) – gleiche Firewall-Einstellungen – gleiche Einstellung der IKE-Optionen.
	Aktiv	**Ja / Nein** Legt fest, ob die unten definierten VPN-Verbindungskanäle insgesamt aktiv (= Ja) sein soll oder nicht (= Nein).
	Adresse des VPN-Gateways der Gegenstelle	(Eine IP-Adresse, ein Hostname oder **%any** für beliebige, mehrere Gegenstellen oder Gegenstellen hinter einem NAT-Router)

Adresse des VPN-Gateways der Gegenstelle



VPN-Gateway
der Gegenstelle

Bild 6-3 Die Adresse des Übergangs zum privaten Netz, in dem sich der entfernte Kommunikationspartner befindet.

– Falls der mGuard aktiv die Verbindung zur entfernten Gegenstelle initiieren und aufbauen soll, dann geben Sie hier die IP-Adresse oder den Hostnamen der Gegenstellen an.
– Falls das VPN-Gateway der Gegenstelle keine feste und bekannte IP-Adresse hat, kann über die Inanspruchname des DynDNS-Service (siehe Glossar) dennoch eine feste und bekannte Adresse simuliert werden.
– Falls der mGuard bereit sein soll, die Verbindung anzunehmen, die eine entfernte Gegenstelle mit beliebiger IP-Adresse aktiv zum lokalen mGuard initiiert und aufbaut, dann geben Sie an: **%any**

  Diese Einstellung ist auch bei einer VPN-Sternkonfiguration zu wählen, wenn der mGuard an der Zentrale angeschlossen ist.

  So kann eine entfernte Gegenstelle den mGuard „anrufen“, wenn diese Gegenstelle ihre eigene IP-Adresse (vom Internet Service Provider) dynamisch zugewiesen erhält, d. h. eine wechselnde IP-Adresse hat. Nur wenn in diesem Szenario die entfernte „anrufende“ Gegenstelle auch eine feste und bekannte IP-Adresse hat, können Sie diese IP-Adresse angeben.

%any kann nur zusammen mit dem Authentisierungsverfahren über X.509-Zertifikate verwendet werden.

Wenn die Gegenstelle mit Hilfe von lokal hinterlegten CA-Zertifikaten authentifiziert werden soll, kann die Adresse des VPN-Gateway der Gegenstelle konkret (durch IP-Adresse oder Hostname) oder durch **%any** angegeben werden. Wird sie durch eine konkrete Adresse angegeben (und nicht durch „%any“), dann muss ein VPN-Identifier (siehe „VPN-Identifier“ auf Seite 6-207) spezifiziert werden.

Wenn sich die Gegenstelle hinter einem NAT-Gateway befindet, muss **%any** gewählt werden. Ansonsten wird das Aushandeln weiterer Verbindungsschlüssel nach der ersten Kontaktaufnahme fehlschlagen.

Bei Einsatz von **TCP-Kapselung** (siehe „TCP-Kapselung“ auf Seite 6-184): Es muss eine feste IP-Adresse oder ein Hostname angegeben werden, wenn dieser mGuard die VPN-Verbindung initiieren und den VPN-Datenverkehr einkapseln soll.

Ist dieser mGuard einer Wartungszentrale vorgeschaltet, zu der mehrere entfernte mGuards VPN-Verbindungen herstellen und eingekapselte Datenpakete senden, muss das VPN-Gateway der Gegenstelle mit **%any** angegeben werden.

IPsec VPN >> Verbindungen >> Editieren >> Allgemein		
Optionen	**Interface, welches bei der Einstellung %any für das Gateway benutzt wird**	**Intern, Extern, Extern 2, Einwahl** *Extern 2* und *Einwahl* nur bei Geräten mit serieller Schnittstelle, siehe „Netzwerk >> Interfaces“ auf Seite 6-64. Die Auswahl *von Intern* ist im Stealth-Modus nicht erlaubt. Die Einstellung des Interfaces wird nur beachtet, wenn als Adresse des VPN-Gateways der Gegenstelle „%any“ eingetragen ist. In diesem Fall wird hier das Interface des mGuards eingestellt, über das er Anfragen zum Aufbau dieser VPN-Verbindung beantwortet und erlaubt. Bei allen Stealth-Modi gilt, wenn **Extern** ausgewählt ist, kann die VPN-Verbindung sowohl über den LAN- als auch den WAN-Port aufgebaut werden. Die Einstellung des Interfaces ermöglicht es für VPN-Gegenstellen ohne bekannte IP-Adresse die verschlüsselte Kommunikation über ein konkretes Interface zu führen. Falls eine IP-Adresse oder ein Hostname für die Gegenstelle angegeben sind, wird die Zuordnung zu einem Interface implizit daraus ermittelt. Über Auswahl von **Intern** kann der mGuard im Router-Modus als "Einbein-Router" eingesetzt werden, weil dann der entschlüsselte wie auch der verschlüsselte VPN-Verkehr dieser VPN-Verbindung über das interne Interface geführt wird. IKE- und IPsec-Datenverkehr ist immer nur über die primäre IP-Adresse der jeweils zugeordneten Schnittstelle möglich. Dies gilt auch für VPN-Verbindungen mit konkreter Gegenstelle.
	Verbindungsinitiierung: Initiiere / Initiiere bei Datenverkehr / Warte	**Initiiere** In diesem Fall initiiert der mGuard die Verbindung zur Gegenstelle. Im Feld *Adresse des VPN-Gateways der Gegenstelle* (s. o.) muss die feste IP-Adresse der Gegenstelle oder deren Name eingetragen sein. **Initiiere bei Datenverkehr** Die Verbindung wird automatisch initiiert, wenn der mGuard bemerkt, dass die Verbindung genutzt werden soll. (Ist bei jeder Betriebsart des mGuards (*Stealth, Router* usw.) wählbar.) **Warte** In diesem Fall ist der mGuard bereit, die Verbindung anzunehmen, die eine entfernte Gegenstelle aktiv zum mGuard initiiert und aufbaut. Wenn Sie unter *Adresse des VPN-Gateways der Gegenstelle* **%any** eingetragen haben, müssen Sie **Warte** auswählen.

IPsec VPN >> Verbindungen >> Editieren >> Allgemein[...]

Kapsele den VPN-Datenverkehr in TCP ein

Nein / Ja (Standard: Nein)

Bei Anwendung der Funktion **TCP-Kapselung** (siehe „TCP-Kapselung“ auf Seite 6-184) diesen Schalter nur dann auf **Ja** setzen, wenn der mGuard bei der von ihm initiierten VPN-Verbindung den von ihm ausgehenden Datenverkehr einkapseln soll. In diesem Fall muss auch die Nummer des Ports angegeben werden, über den die Gegenstelle die eingekapselten Datenpakete empfängt.

Bei **Ja** wird der mGuard nicht versuchen, die VPN-Verbindung über die Standard IKE-Verschlüsselung (UDP-Port 500 und 4500) herzustellen, sondern sie immer mit TCP verkapseln.

TCP-Port des Servers, welcher die gekapselte Verbindung annimmt

(Nur sichtbar, wenn „Kapsele den VPN-Datenverkehr in TCP ein“ auf **Ja** steht.)

Standard: **8080**. Nummer des Ports, über den die Gegenstelle die eingekapselten Datenpakete empfängt. Die hier angegebene Portnummer muss mit der Portnummer übereinstimmen, die beim mGuard der Gegenstelle als **TCP-Port, auf dem zu horchen ist** festgelegt ist (Menüpunkt *IPsec VPN >> Global >> Optionen*).

Bei Einsatz von TCP-Kapselung (siehe Seite 6-184):

– Wenn der mGuard eine VPN-Verbindung zu einer Wartungszentrale aufbauen und den Datenverkehr dorthin einkapseln soll:

– Es muss **Initiiere** oder **Initiiere bei Datenverkehr** festgelegt werden.

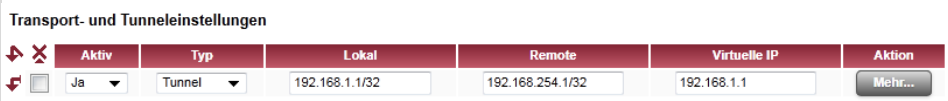
– Wenn der mGuard bei einer Wartungszentrale installiert ist, zu der mGuards eine VPN-Verbindung aufbauen:

– Es muss **Warte** festgelegt werden.

Transport und Tunneleinstellungen

Hier klicken, wenn weitere Tunnel bzw. Transportwege festgelegt werden sollen.

Stealth-Modus:



Router-Modus:

VPN-Verbindungskanäle

Eine unter einem beschreibenden Namen definierte VPN-Verbindung kann aus mehreren VPN-Verbindungskanälen bestehen. Also können Sie hier mehrere VPN-Verbindungskanäle definieren.

Für jeden einzelnen VPN-Verbindungskanal

Nach Klicken auf die Schaltfläche **Mehr...** wird eine weitere Seite zur Festlegung der Verbindungsparameter des betreffenden Transportweges oder Tunnels angezeigt, zum Teil überschneidend.

Aktiv

Ja / Nein

Legen Sie fest, ob der Verbindungskanal aktiv (= Ja) sein soll oder nicht (= Nein).

IPsec VPN >> Verbindungen >> Editieren >> Allgemein[...]

Kommentar

Frei einzugebender kommentierender Text. Kann leer bleiben.

Typ

Es stehen zur Auswahl:

– Tunnel (Netz ↔ Netz)
– Transport (Host ↔ Host)

Tunnel (Netz ↔ Netz)

Dieser Verbindungstyp eignet sich in jedem Fall und ist der sicherste. In diesem Modus werden die zu übertragenen IP-Datagramme vollkommen verschlüsselt und mit einem neuen Header versehen zum VPN-Gateway der Gegenstelle, dem „Tunnelende“, gesendet. Dort werden die übertragenen Datagramme entschlüsselt und aus ihnen die ursprünglichen Datagramme wiederhergestellt. Diese werden dann zum Zielrechner weitergeleitet.

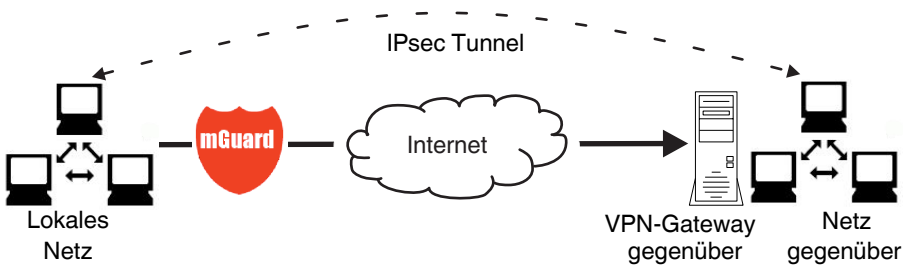
Transport (Host ↔ Host)

Bei diesem Verbindungstyp werden nur die Daten der IP-Pakete verschlüsselt. Die IP-Header-Informationen bleiben unverschlüsselt.

Bei Wechsel auf *Transport* werden die nachfolgenden Felder (bis auf Protokoll) ausgeblendet, weil diese Parameter entfallen.

Lokal / Remote - bei Verbindungstyp *Tunnel* **(Netz ↔ Netz)**

Unter **Lokal** und **Remote** definieren Sie die Netzwerkbereiche für beide Tunnelenden.



Lokal

Hier geben Sie die Adresse des Netzes oder Computers an, das oder der lokal am mGuard angeschlossen ist.

Remote

Hier geben Sie die Adresse des Netzes oder Computers an, das/der sich hinter dem gegenüberliegenden VPN-Gateway befindet.

Ist oben unter Adresse des *VPN-Gateways der Gegenstelle* (siehe „Adresse des VPN-Gateways der Gegenstelle“ auf Seite 6-191) diese mit **%any** angegeben, ist es möglich, dass mehrere verschiedene Gegenstellen zum mGuard Verbindung aufnehmen.

Einstellung für Tunneleinstellung IPsec/L2TP

Wenn sich Clients per IPsec/L2TP über den mGuard verbinden sollen, dann aktivieren Sie den L2TP-Server und machen in den nachfolgend aufgelisteten Feldern die jeweils dahinter stehenden Angaben:

- **Typ**: Transport
- **Protokoll**: UDP
- **Lokaler Port:** %all
- **Remote-Port:** %all

Festlegung einer Standard-Route über das VPN:

Die Adresse 0.0.0.0/0 gibt eine *Standard-Route über das VPN* an.

Bei dieser wird sämtlicher Datenverkehr, für den keine anderen Tunnel oder Routen existieren, durch diesen VPN-Tunnel geleitet.

Eine Standard-Route über das VPN sollte nur für einen einzigen Tunnel angegeben werden.

Im *Stealth*-Modus kann eine *Standard-Route über das VPN* nicht verwendet werden.

Option nach Installation einer VPN-Tunnel Group-Lizenz

Wird als Adresse des *VPN-Gateway der Gegenstelle* **%any** angegeben, können sich auf der entfernten Seite viele mGuards bzw. viele Netzwerke befinden.

Dann wird beim lokalen mGuard im Feld **Remote** ein sehr großer Adressenbereich festgelegt, und bei den entfernten mGuards wird jeweils für das bei ihnen unter **Lokal** angegebene Netz ein Teil dieses Adressenbereichs verwendet.

Um das zu illustrieren: Die Angaben in den Feldern *Lokal* und *Remote* beim lokalen und bei entfernten mGuards könnten zum Beispiel wie folgt lauten:

Lokaler mGuard			Entfernter mGuard **A**	
Lokal	Remote		Lokal	Remote
10.0.0.0/8	10.0.0.0/8	>	10.1.7.0/24	10.0.0.0/8
			Entfernter mGuard **B**	
			Lokal	Remote
		>	10.3.9.0/24	10.0.0.0/8
			usw.	

Auf diese Weise kann durch die Konfiguration eines einzigen Tunnels der Verbindungsaufbau durch viele Stellen gewährt werden.

Zur Nutzung dieser Möglichkeiten muss vorher die *VPN-Tunnel Group-Lizenz* installiert werden, es sei denn, das Gerät wurde bereits entsprechend ausgeliefert. Wird eine solche Lizenz installiert, muss das Gerät erst neu gestartet werden, um sie nutzen zu können.

Virtuelle IP-Adresse *(nur Stealth-Modus)*

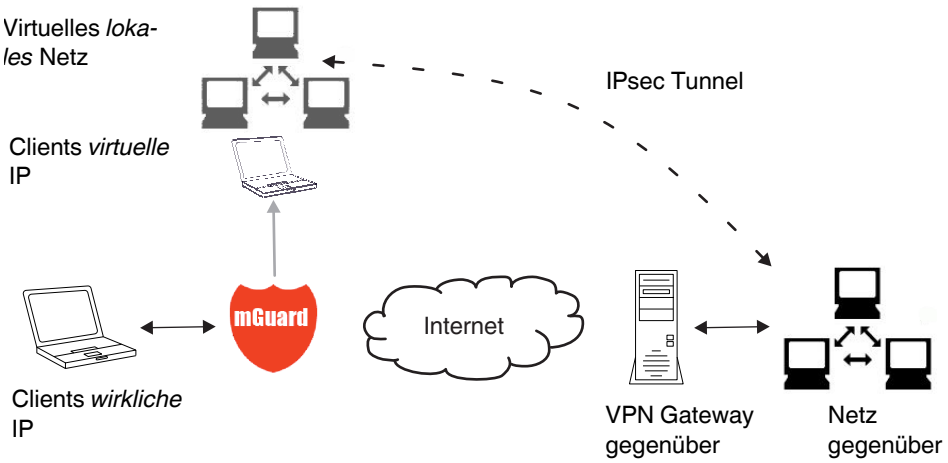


Bild 6-4 Virtuelle IP

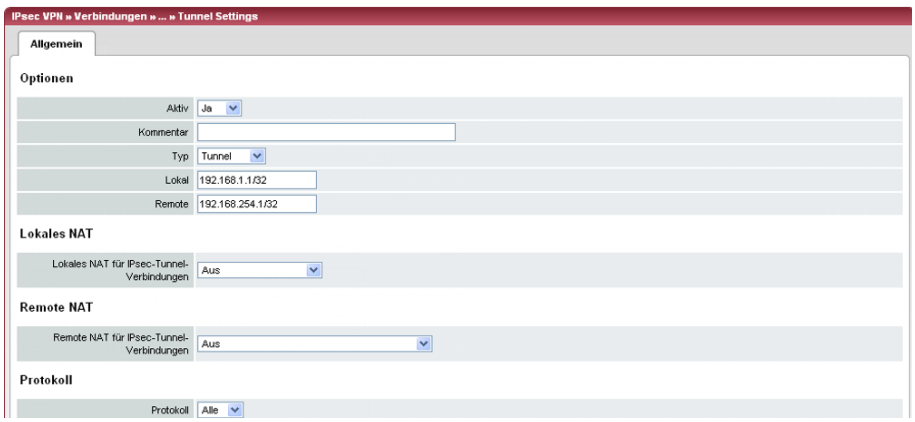
Im *Stealth*-Modus wird das lokale Netz des VPNs durch den mGuard simuliert. Innerhalb dieses *virtuellen* Netzes ist der Client unter der hier einzutragenden *virtuellen* IP-Adresse bekannt und ansprechbar.

IPsec VPN >> Verbindungen >> Editieren >> Allgemein

Weitere Einstellungen nach Klicken auf **Mehr...**

Optionen

Verbindungstyp *Tunnel*



Aktiv	**Ja / Nein** Wie oben.
Kommentar	Frei einzugebender kommentierender Text. Kann leer bleiben.
Typ	**Tunnel / Transport** Wie oben. Bei Wechsel auf *Transport* werden die nachfolgenden Felder (bis auf *Protokoll*) ausgeblendet, weil diese Parameter entfallen.
Lokal	Siehe „Lokal“ auf Seite 6-195
Remote	Siehe „Remote“ auf Seite 6-195
Die virtuelle IP für den Client	Siehe „Die virtuelle IP für den Client“ auf Seite 6-198

Lokales NAT

NAT

Beim NAT (**N**etwork **A**ddress **T**ranslation) werden Adressen in Datenpaketen durch andere Adressen ersetzt.

Es können die IP-Adressen von Geräten umgeschrieben werden, die sich am lokalen Ende des VPN-Tunnels befinden (Lokales NAT) oder es werden die Adressen von Geräten umgeschrieben, die sich am entfernten Ende befinden (Remote NAT).

IPsec VPN >> Verbindungen >> Editieren >> Allgemein[...]

Weitere Einstellungen nach Klicken auf **Mehr...**

Lokales NAT für IPsec-Tunnel-Verbindungen

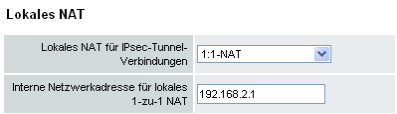
Aus / 1-zu-1-NAT / Lokales Masquerading

Default: **Aus**

Hier wird definiert, welche Art von Adress-Umschreibung für die Zieladresse der ankommenden und die Quelladresse der gesendeten Pakete vorgenommen wird.

Aus: Es wird kein NAT vorgenommen.

1-zu-1-NAT



Bei 1-zu-1-NAT werden die IP-Adressen von Geräten am lokalen Ende des Tunnels so ausgetauscht, dass jede einzelne gegen eine bestimmte andere umgeschrieben wird, und nicht wie beim IP-Masquerading gegen eine für alle Geräte identische IP-Adresse.

Wenn lokale Geräte Datenpakete senden, kommen nur solche in Betracht,

- die der mGuard tatsächlich verschlüsselt (vom mGuard werden nur Pakete durch den VPN-Tunnel weitergeleitet, wenn sie aus einer vertrauenswürdigen Quelle stammen).
- die ihren Ursprung in einer Quelladresse innerhalb des Netzwerkes haben, das unter **Interne Netzwerkadresse für lokales 1-zu-1 NAT** in Kombination mit der Netzwerkmaske unter *Lokal* definiert wird.
- deren Zieladresse im Netzwerk *Remote* (siehe „Remote“ auf Seite 6-195) liegt, wenn kein 1-zu-1-NAT für das Remote-NAT eingestellt ist.
- deren Zieladresse im Bereich der *Netzwerkadresse für gegebenüberliegendes 1-zu-1-NAT* liegt, wenn 1-zu-1-NAT für das Remote-NAT eingestellt ist.

Die Datenpakete von lokalen Geräten bekommen eine Quelladresse entsprechend der eingestellten Adresse unter *Lokal* (siehe „Lokal“ auf Seite 6-195) zugewiesen und werden durch den VPN-Tunnel gesendet.

Interne Netzwerkadresse für lokales 1-zu-1 NAT

Datenpakete, die durch den VPN-Tunnel empfangen werden, werden umgekehrt zugeordnet. Zieladressen, die zum Netzwerk *Lokal* gehören, werden auf die entsprechende Adresse unter **Interne Netzwerkadresse für lokales 1-zu-1 NAT** umgeschrieben.

IPsec VPN >> Verbindungen >> Editieren >> Allgemein[...]

Weitere Einstellungen nach Klicken auf **Mehr...**

	Lokales NAT für IPsec-Tunnel-Verbindungen	**Lokales Masquerading** Lokales NAT Lokales NAT für IPsec-Tunnel-Verbindungen: Lokales Masquerading Interne Netzwerkadresse für lokales Masquerading: 192.168.1.0/24 Wenn lokale Geräte Datenpakete senden, kommen nur solche in Betracht, – die der mGuard tatsächlich verschlüsselt (vom mGuard werden nur Pakete durch den VPN-Tunnel weitergeleitet, wenn sie aus einer vertrauenswürdigen Quelle stammen). – die ihren Ursprung in einer Quelladresse innerhalb des Netzwerkes haben, das unter **Interne Netzwerkadresse für lokales Masquerading** definiert wird. – deren Zieladresse im Netzwerk *Remote* (siehe „Remote“ auf Seite 6-195) liegt, wenn kein 1-zu-1-NAT für das Remote-NAT eingestellt ist. – deren Zieladresse im Bereich der *Netzwerkadresse für gegebenüberliegendes 1-zu-1-NAT* liegt, wenn 1-zu-1 NAT für das Remote-NAT eingestellt ist. Die Quelladresse solcher Datenpakete wird mit der niedrigsten IP-Adresse des Netzwerkes unter *Lokal* maskiert. Danach werden die Datenpakete durch den VPN-Tunnel gesendet. Das Maskieren ändert die Quelladresse (und den Quell-Port). Die ursprünglichen Adressen werden in einem Eintrag der Conntrack-Tabelle aufgezeichnet. Antwort-Pakete, die durch den VPN-Tunnel empfangen werden und zu einem Eintrag der Conntrack-Tabelle passen, bekommen ihre Zieladresse (und ihren Ziel-Port) zurückgeschrieben.
Remote NAT	**Remote NAT für IPsec-Tunnel-Verbindungen**	**Aus / 1-zu-1-NAT / Masquerading des gegenüberliegenden Netzes** Hier wird definiert, welche Art von Adress-Umschreibung für die Quelladresse der ankommenden und die Zieladresse der gesendeten Pakete vorgenommen wird. Default: **Aus** **Aus**: Es wird kein NAT vorgenommen.

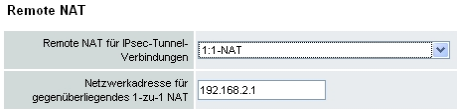
IPsec VPN >> Verbindungen >> Editieren >> Allgemein[...]

Weitere Einstellungen nach Klicken auf **Mehr...**

Remote NAT

Remote NAT für IPsec-Tunnel-Verbindungen

1-zu-1-NAT



Bei 1-zu-1-NAT werden die IP-Adressen der entfernten Geräte so ausgetauscht, dass jede einzelne gegen eine bestimmte andere ausgetauscht wird, und nicht wie beim IP-Masquerading gegen eine für alle Geräte identische IP-Adresse.

Wenn lokale Geräte Datenpakete senden, kommen nur solche in Betracht,

– die der mGuard tatsächlich verschlüsselt (vom mGuard werden nur Pakete durch den VPN-Tunnel weitergeleitet, wenn sie aus einer vertrauenswürdigen Quelle stammen).
– deren Quelladresse innerhalb des Netzwerkes liegt, das unter *Local NAT* definiert wird (unter „Lokal“ auf Seite 6-195*,* unter *1-zu-1-NAT* oder unter *Lokales Masquerading)*,

  oder deren Quelladresse innerhalb des Netzes Lokal liegt, wenn kein *Local NAT* definiert ist.
– deren Zieladresse zu der **Netzwerkadresse für gegebenüberliegendes 1-zu-1-NAT** gehört, wenn auf sie die Netzwerkmaske vom Netzwerk „Remote“ angewendet wird.

Die Datenpakete bekommen eine entsprechende Zieladresse aus dem Netzwerk, das unter **Remote** (siehe „Remote“ auf Seite 6-195) eingestellt ist. Wenn nötig wird auch die Quelladresse ersetzt (siehe *Local NAT*). Danach werden die Datenpakete durch den VPN-Tunnel gesendet.

Netzwerkadresse für gegebenüberliegendes 1-zu-1-NAT

Die Quell-Adressen der Pakete, die der mGuard durch den VPN-Tunnel empfängt, werden umgekehrt umgeschrieben. Solche Pakete kommen mit einer Quelladresse aus dem Netzwerk an, das unter *Remote* definiert ist. Diese Adresse wird mit Hilfe der **Netzwerkadresse für gegebenüberliegendes 1-zu-1-NAT** umgeschrieben.

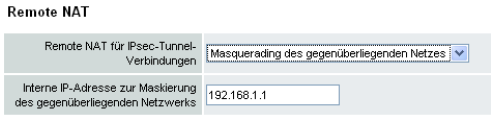
IPsec VPN >> Verbindungen >> Editieren >> Allgemein[...]

Weitere Einstellungen nach Klicken auf **Mehr...**

Remote NAT

Remote NAT für IPsec-Tunnel-Verbindungen

Masquerading des gegenüberliegenden Netzes



Die Quell-Adressen von Datenpaketen, die der mGuard durch den VPN-Tunnel empfängt, werden mit der IP-Adresse maskiert, die unter **Interne IP-Adresse zur Maskierung des genüberliegenden Netzwerkes** definiert ist.

Die ursprüngliche und die übersetzte Quelladresse (und der Quell-Port) werden aufgezeichnet. Antworten, zu denen eine passende Aufzeichnung gefunden wird, bekommen so ihre ursprüngliche Zieladresse zurück. Wenn nötig, wird auch die Zieladresse umgeschrieben (siehe *Local NAT*).

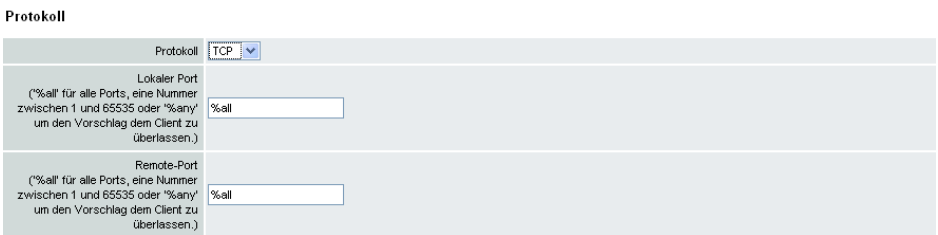
Protokoll

Protokoll

Alle / TCP / UDP / ICMP

Sie können auswählen, ob das VPN auf ein bestimmtes Protokoll eingeschränkt werden soll oder aber für den gesamten Datenverkehr gilt.

Bei Auswahl von TCP oder UDP:



Lokaler Port

Mit **%all** (Standard) wird festgelegt, dass alle Ports benutzt werden können. Soll ein bestimmer Port verwendet werden, geben Sie dessen Nummer an. Mit **%any** legen Sie fest, dass die Auswahl des Ports dem Client überlassen ist.

Remote-Port

Mit **%all** (Standard) wird festgelegt, dass alle Ports benutzt werden können. Soll ein bestimmer Port verwendet werden, geben Sie dessen Nummer an.

Lokales Masquerading

Kann nur für VPN-Typ *Tunnel* verwendet werden.

Beispiel

Eine Zentrale unterhält zu sehr vielen Zweigstellen jeweils einen VPN-Tunnel. In den Zweigstellen ist jeweils ein lokales Netzwerk mit zahlreichen Rechnern installiert, die über den jeweiligen VPN-Tunnel mit der Zentrale verbunden sind. In diesem Fall könnte der Adressraum zu klein sein, um die Rechner an den verschiedenen VPN-Tunnelenden insgesamt darin unterzubringen.

Lokales Masquerading schafft hier Abhilfe:

Die im Netzwerk einer Zweigstelle angeschlossenen Rechner treten durch das lokale Masquerading für das VPN-Gateway der Zentrale unter einer einzigen IP-Adresse in Erscheinung. Außerdem wird ermöglicht, dass die lokalen Netzwerke in den unterschiedlichen Zweigstellen lokal jeweils die selben Netzwerkadresse benutzen. Nur die Zweigstelle kann VPN-Verbindungen zur Zentrale aufbauen.

Interne Netzwerkadresse für lokales Masquerading

Gibt das Netz, d. h. den IP-Adressenbereich an, für den das lokale Masquerading angewendet wird.

Nur wenn ein Rechner eine IP-Adresse aus diesem Bereich hat, wird in den Datenpaketen, die dieser Rechner über die VPN-Verbindung aussendet, die Absenderadresse gegen die ausgetauscht, die im Feld **Lokal** angegeben ist (siehe oben).

Die im Feld **Lokal** angegebene Adresse muss die Netzmaske /32 haben, damit es sich um genau eine IP-Adresse handelt.

Lokales Masquerading kann in folgenden Netzwerk-Modi verwendet werden: Router, PPPoE, PPTP, Modem, Eingebautes Modem und Stealth (nur Stealth-Modus „mehrere Clients“).

Modem / Eingebautes Modem: Steht nicht bei allen mGuard-Modellen zur Verfügung (siehe „Netzwerk >> Interfaces“ auf Seite 6-64).

Für IP-Verbindungen, die durch eine VPN-Verbindung mit aktiviertem lokalem Masquerading vermittelt werden, werden die Firewall-Regeln für ausgehende Daten in der VPN-Verbindung auf die originale Quelladresse der Verbindung angewendet.

1-zu-1-NAT

Nur im Router-Modus.

Mit Hilfe von 1-zu-1-NAT im VPN können weiterhin die tatsächlich genutzten Netzwerkadressen - lokal und/oder entfernt - zur Angabe des Tunnelanfangs bzw. -endes angegeben werden, unabhängig von den mit der Gegenseite vereinbarten Tunnelparametern:

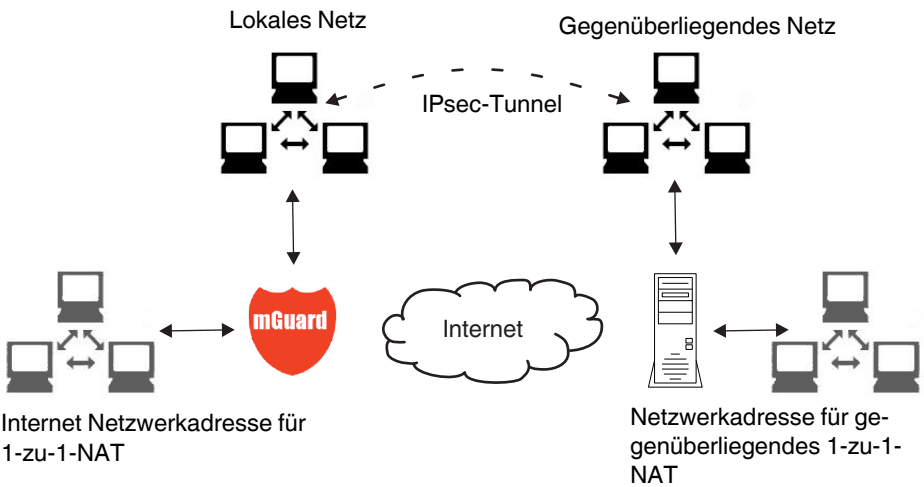
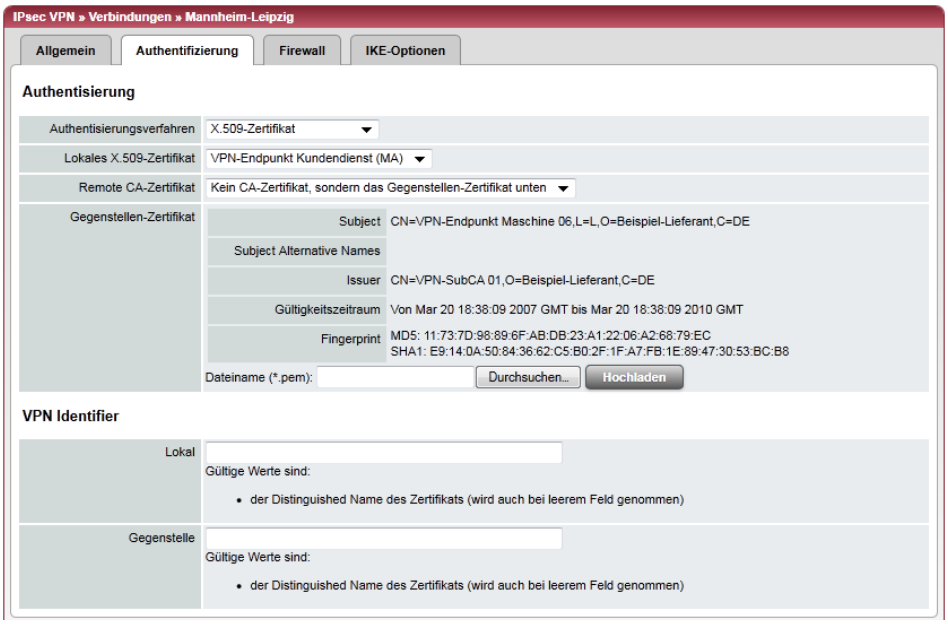


Bild 6-5 1-zu1-NAT

6.8.2.3 Authentifizierung



IPsec VPN >> Verbindungen >> Editieren >> Authentifizierung

Authentisierung

Authentisierungsverfahren

Es gibt 2 Möglichkeiten:

– X.509-Zertifikat (Standard)

– Pre-Shared Key

Je nach dem, welches Verfahren Sie auswählen, zeigt die Seite unterschiedliche Einstellmöglichkeiten.

Bei Authentisierungsverfahren X.509-Zertifikat

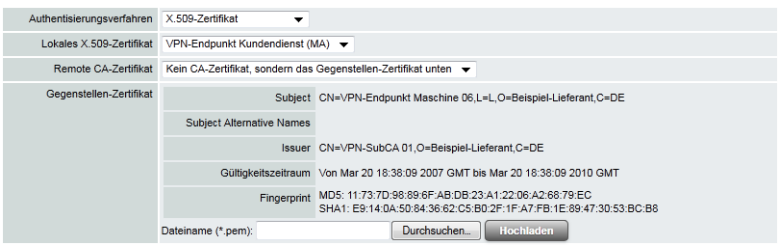
Dieses Verfahren wird von den meisten neueren IPsec-Implementierungen unterstützt. (Dabei besitzt jeder VPN-Teilnehmer einen privaten geheimen Schlüssel sowie einen öffentlichen Schlüssel in Form eines X.509-Zertifikats, welches weitere Informationen über seinen Eigentümer und einer Beglaubigungsstelle (Certification Autority, CA) enthält.)

Es muss Folgendes festgelegt werden:

– Wie sich der mGuard bei der Gegenstelle authentisiert.

– Wie der mGuard die entfernte Gegenstelle authentifiziert

....wie sich der mGuard bei der Gegenstelle authentisiert.



IPsec VPN >> Verbindungen >> Editieren >> Authentifizierung

Lokales X.509-Zertifikat

Legt fest, mit welchem Maschinenzertifikat sich der mGuard bei der VPN-Gegenstelle ausweist.

In der Auswahlliste eines der Maschinenzertifikate auswählen.

Die Auswahlliste stellt die Maschinenzertifikate zur Wahl, die in den mGuard unter Menüpunkt *Authentifizierung >> Zertifikate* geladen worden sind (siehe Seite 6-128).

Falls nur der Eintrag *Keines* zu sehen ist, muss erst ein Zertifikat installiert werden. Der Eintrag *Keines* darf nicht belassen werden, weil sonst keine X.509-Authentifizierung möglich ist.

....wie der mGuard die entfernte Gegenstelle authentifiziert

Nachfolgend wird festgelegt, wie der mGuard die Authentizität der entfernten VPN-Gegenstelle prüft.

Die Tabelle unten zeigt, welche Zertifikate dem mGuard zur Authentifizierung der VPN-Gegenstelle zur Verfügung stehen müssen, wenn die VPN-Gegenstelle bei Verbindungsaufnahme eines der folgenden Zertifikatstypen vorzeigt:

– ein von einer CA signiertes Maschinenzertifikat
– ein selbst signiertes Maschinenzertifikat

Zum Verständnis der nachfolgenden Tabelle siehe Kapitel „Authentifizierung >> Zertifikate“ auf Seite 6-128.

Authentifizierung bei VPN

Die Gegenstelle zeigt vor:	Maschinenzertifikat von **CA signiert**	Maschinenzertifikat **selbst signiert**
Der mGuard authentifiziert die Gegenstelle anhand von...	⇕	⇕
	Gegenstellen-Zertifikat oder, allen CA-Zertifikaten, die mit dem von der Gegenstelle vorgezeigten Zertifikat die Kette bis zum Root-CA-Zertifikat bilden	Gegenstellen-Zertifikat

Nach dieser Tabelle sind dem mGuard die Zertifikate zur Verfügung zu stellen, die er zur Authentifizierung der jeweiligen VPN-Gegenstelle heranziehen muss.

Voraussetzung

Die nachfolgenden Anleitungen gehen davon aus, dass die Zertifikate bereits ordnungsgemäß im mGuard installiert sind (siehe „Authentifizierung >> Zertifikate“ auf Seite 6-128; abgesehen vom Gegenstellen-Zertifikat).

Ist unter Menüpunkt *Authentifizierung >> Zertifikate , Zertifikatseinstellungen* die Verwendung von Sperrlisten (= CRL-Prüfung) aktiviert, wird jedes von einer CA signierte Zertifikat, das VPN-Gegenstellen „vorzeigen“, auf Sperrung geprüft. Ausgenommen sind lokal konfigurierte (hier importierte) Gegenstellen-Zertifikate.

Remote CA-Zertifikat

Selbst signiertes Maschinenzertifikat

Wenn sich die VPN-Gegenstelle mit einem **selbst signierten** Maschinenzertifikat authentisiert:

- Wählen Sie aus der Auswahlliste folgenden Eintrag:
  „Kein CA-Zertifikat, sondern das Gegenstellen-Zertifikat unten“
- Installieren Sie unter *Gegenstellen-Zertifikat* das Gegenstellen-Zertifikat (siehe „Gegenstellen-Zertifikat installieren“ auf Seite 6-206).

Es ist nicht möglich, ein Gegenstellen-Zertifikat zu referenzieren, das unter Menüpunkt *Authentifizierung* >> *Zertifikate* geladen ist.

CA-signiertes Maschinenzertifikat

Wenn sich die VPN-Gegenstelle mit einem **von einer CA signierten** Maschinenzertifikat authentisiert:

Es gibt die Möglichkeit, das von der Gegenstelle vorgezeigte Maschinenzertifikat wie folgt zu authentifizieren;

– durch CA-Zertifikate
– durch das entsprechende Gegenstellen-Zertifikat

Authentifizierung durch CA-Zertifikate:

An dieser Stelle ist ausschließlich das CA-Zertifikat von der CA zu referenzieren (in der Auswahlliste auszuwählen), welche das von der VPN-Gegenstelle vorgezeigte Zertifikat signiert hat. Die weiteren CA-Zertifikate, die mit dem von der Gegenstelle vorgezeigten Zertifikat die Kette bis zum Root-CA-Zertifikat bilden, müssen aber im mGuard installiert sein - unter Menüpunkt *Authentifizierung* >> *Zertifikate* .

Die Auswahlliste stellt alle CA-Zertifikate zur Wahl, die in den mGuard unter Menüpunkt *Authentifizierung* >> *Zertifikate* geladen worden sind.

Weitere Auswahlmöglichkeit ist *„Alle bekannten CAs“.*

Mit dieser Einstellung werden alle VPN-Gegenstellen akzeptiert, wenn sie sich mit einem von einer CA signierten Zertifikat anmelden, das von einer bekannten CA (Certification Authority) ausgestellt ist. Bekannt dadurch, weil in den mGuard das jeweils entsprechende CA-Zertifikat und außerdem alle weiteren CA-Zertifikate geladen worden sind, so dass sie zusammen mit den vorgezeigten Zertifikaten jeweils die Kette bilden bis zum Root-Zertifikat.

Authentifizierung durch das entsprechende Gegenstellen-Zertifikat:

- Wählen Sie aus der Auswahlliste folgenden Eintrag:
  „Kein CA-Zertifikat, sondern das Gegenstellen-Zertifikat unten“
- Installieren Sie unter *Gegenstellen-Zertifikat* das Gegenstellen-Zertifikat siehe „Gegenstellen-Zertifikat installieren“ auf Seite 6-206).

Es ist nicht möglich, ein Gegenstellen-Zertifikat zu referenzieren, das unter Menüpunkt *Authentifizierung* >> *Zertifikate* geladen ist.

Gegenstellen-Zertifikat installieren

Das Gegenstellen-Zertifikat muss konfiguriert werden, wenn die VPN-Gegenstelle per Gegenstellen-Zertifikat authentifiziert werden soll.

Um ein Zertifikat zu importieren, gehen Sie wie folgt vor:

Voraussetzung: Die Zertifikatsdatei (Dateiname = *.pem, *.cer oder *.crt) ist auf dem angeschlossenen Rechner gespeichert.

- **Durchsuchen...** klicken, um die Datei zu selektieren
- **Hochladen** klicken.
  Danach wird der Inhalt der Zertifikatsdatei angezeigt.

IPsec VPN >> Verbindungen >> Editieren >> Authentisierung

VPN-Identifier

Bei Authentisierungsverfahren CA-Zertifikat

Die nachfolgende Erklärung gilt, wenn die Authentifizierung der VPN-Gegenstelle anhand von CA-Zertifikaten erfolgt.

Über VPN-Identifier erkennen die VPN-Gateways, welche Konfigurationen zu der gleichen VPN-Verbindung gehören.

Wenn der mGuard CA-Zertifikate heranzieht, um eine VPN-Gegenstellen zu authentifizieren, ist es möglich den VPN-Identifier als Filter zu benutzen.

- Machen Sie dazu ist im Feld *Gegenstelle* den entsprechenden Eintrag.

Lokal

Standard: leeres Feld

Mit dem lokalen VPN-Identifier können Sie den Namen festlegen, mit dem sich der mGuard bei der Gegenstelle meldet (identifiziert). Er muss mit den Angaben aus dem Maschinenzertifikat des mGuards übereinstimmen.

Gültige Werte sind:

- Leer, also kein Eintrag (Voreinstellung). Dann wird der Subject-Eintrag (früher *Distinguished Name*) des Maschinenzertifikats verwendet.
- Der Subject-Eintrag im Maschinenzertifikat
- Einen der *Subject Alternative Name*s, wenn die im Zertifikat aufgelistet sind. Wenn das Zertifikat *Subject Alternative Name*s enthält, werden diese unter „Gültige Werte sind:“ mit angegeben. Es können IP-Adressen, Hostnamen mit vorangestelltem @-Zeichen oder E-Mail-Adressen sein.

Gegenstelle

Legt fest, was im Maschinenzertifikat der VPN-Gegenstelle als Subject eingetragen sein muss, damit der mGuard diese VPN-Gegenstelle als Kommunikationspartner akzeptiert.

Durch eine entsprechende Festlegung ist es möglich, VPN-Gegenstellen, die der mGuard auf Grundlage von Zertifikatsprüfungen im Prinzip akzeptieren würde, wie folgt zu beschränken bzw. freizugeben:

- Beschränkung auf bestimmte *Subjects* (d. h. Maschinen) und/oder auf *Subjects*, die bestimmte Merkmale (Attribute) haben, oder
- Freigabe für alle *Subjects*

(Siehe „Subject, Zertifikat“ auf Seite 9-5.)

Statt „Subject“ wurde früher die Bezeichnung „Distinguished Name“ verwendet.

IPsec VPN >> Verbindungen >> Editieren >> Authentisierung [...]

Freigabe für alle Subjects:

Wenn Sie das Feld *Gegenstelle* leer lassen, legen Sie fest, dass im Maschinenzertifikat, das die VPN-Gegenstelle vorzeigt, beliebige Subject-Einträge erlaubt sind. Dann ist es überflüssig, das im Zertifikat jeweils angegebene Subject zu kennen oder festzulegen.

Beschränkung auf bestimmte Subjects:

Im Zertifikat wird der Zertifikatsinhaber im Feld *Subject* angegeben, das sich aus mehreren Attributen zusammensetzt. Diese Attribute werden entweder als Object Identifier ausgedrückt (z. B.: 132.3.7.32.1) oder, geläufiger, als Buchstabenkürzel mit einem entsprechenden Wert.

Beispiel: CN=VPN-Endpunkt-01, O=Beispiel GmbH, C=DE

Sollen bestimmte Attribute des Subjects ganz bestimmte Werte haben, damit der mGuard die VPN-Gegenstelle akzeptiert, muss dies entsprechend spezifiziert werden. Die Werte der anderen Attribute, die beliebig sein können, werden dann durch das Wildcard * (Sternchen) angegeben.

Beispiel: CN=*, O=Beispiel GmbH, C=DE (mit oder ohne Leerzeichen zwischen Attributen)

Bei diesem Beispiel müsste im vorgezeigten Zertifikat im Subject das Attribut „O=Beispiel GmbH“ und das Attribut „C=DE“ stehen. Nur dann würde der mGuard den Zertifikatsinhaber (= Subject) als Kommunikationspartner akzeptieren. Die anderen Attribute könnten in den zu filternden Zertifikaten beliebige Werte haben.

Beachten Sie folgendes, wenn Sie einen Subject-Filter setzen.

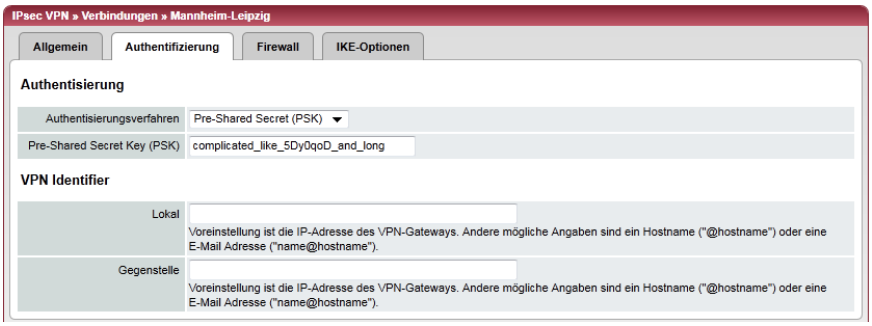
Bei den Attributen müssen Anzahl und Reihenfolge mit denen in den Zertifikaten übereinstimmen, auf die der Filter angewendet wird.

Achten Sie auf Groß- und Kleinschreibung.

IPsec VPN >> Verbindungen >> Editieren >> Authentisierung [...]

VPN Identifier

Bei Authentisierungsverfahren Pre-Shared Secret (PSK)



Dieses Verfahren wird vor allem durch ältere IPsec Implementierungen unterstützt. Dabei authentifizieren sich beide Seiten des VPNs über den gleichen PSK.

Um den verabredeten Schlüssel dem mGuard zur Verfügung zu stellen, gehen Sie wie folgt vor:

- Tragen Sie ins Eingabefeld **Pre-Shared Secret Key (PSK)** die verabredete Zeichenfolge ein.

Um eine mit 3DES vergleichbare Sicherheit zu erzielen, sollte die Zeichenfolge aus ca. 30 nach dem Zufallsprinzip ausgewählten Klein- und Großbuchstaben sowie Ziffern bestehen.

Pre-Shared Secret Key kann nicht mit dynamischen (%any) IP-Adressen verwendet werden, nur feste IP-Adressen oder Hostnamen auf beiden Seiten werden unterstützt. Hinter dem Hostnamen dürften sich aber wechselnde IP-Adressen verbergen (DynDNS).

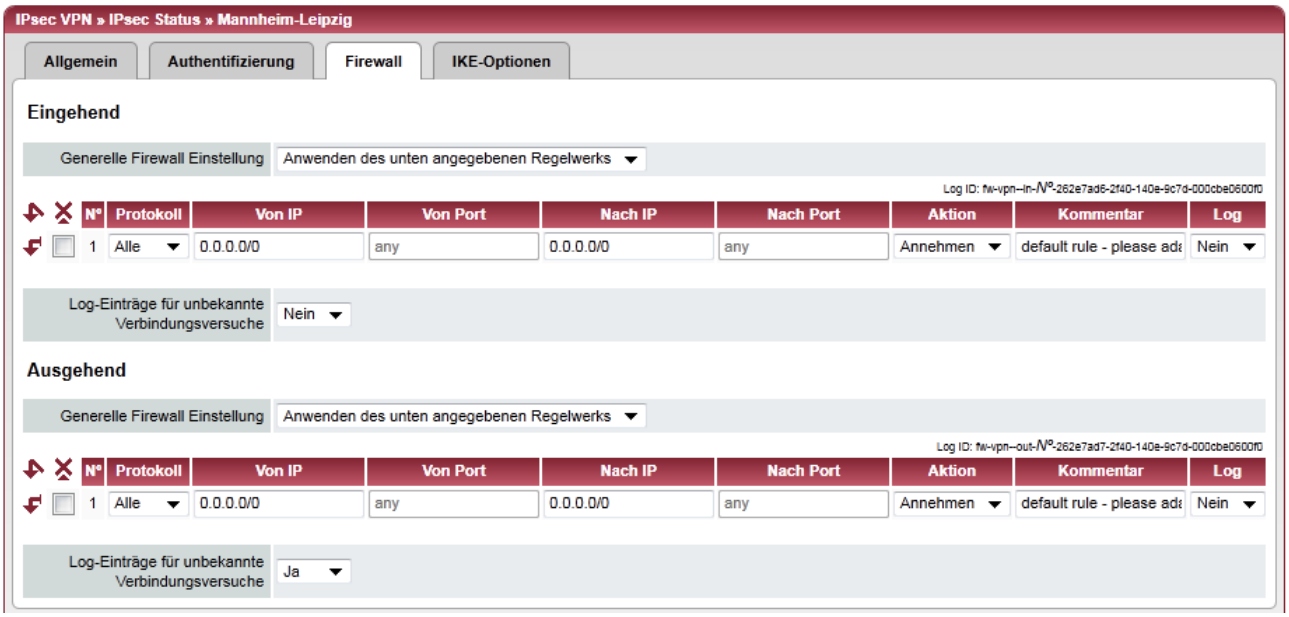
Pre-shared Secret Key kann nicht verwendet werden, wenn sich mindestens einer der Kommunikationspartner (oder beide) hinter einem NAT-Gateway befinden.

Über *VPN Identifier* erkennen die VPN-Gateways, welche Konfigurationen zu der gleichen VPN-Verbindung gehören.

Bei PSK sind folgende Einträge gültig:

– leer (die IP-Adresse wird verwendet, dies ist die Voreinstellung)
– eine IP-Adresse
– ein Hostname mit voran gestelltem ’@’ Zeichen (z. B. „@vpn1138.example.com“)
– eine E-Mail Adresse (z. B. „piepiorra@example.com“)

6.8.2.4 Firewall



Firewall eingehend, Firewall ausgehend

Während die unter dem Menüpunkt *Netzwerk Sicherheit* vorgenommenen Einstellungen sich nur auf Nicht-VPN-Verbindungen beziehen (siehe oben unter „Menü Netzwerksicherheit“ auf Seite 6-144), beziehen sich die Einstellungen hier ausschließlich auf die VPN-Verbindung, die auf diesem Registerkarten-Set definiert ist.

Wenn Sie mehrere VPN-Verbindungen definiert haben, können Sie für jede einzelne den Zugriff von außen oder von innen beschränken. Versuche, die Beschränkungen zu übergehen, können Sie ins Log protokollieren lassen.

Die VPN-Firewall ist werkseitig so voreingestellt, dass für diese VPN-Verbindung alles zugelassen ist.

Für jede einzelne VPN-Verbindung gelten aber unabhängig voneinander gleichwohl die erweiterten Firewall-Einstellungen, die weiter oben definiert und erläutert sind (siehe „Menü Netzwerksicherheit“ auf Seite 6-144, „Netzwerksicherheit >> Paketfilter“ auf Seite 6-144, „Erweiterte Einstellungen“ auf Seite 6-153).

Wenn mehrere Firewall-Regeln gesetzt sind, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Falls in der Regelliste weitere passende Regeln vorhanden sind, werden diese ignoriert.

Im *Stealth*-Modus ist in den Firewall-Regeln die vom Client wirklich verwendete IP-Adresse zu verwenden oder aber auf 0.0.0.0/0 zu belassen, da nur ein Client durch den Tunnel angesprochen werden kann.

Ist auf der Registerkarte *Global* der Schalter *Erlaube Paketweiterleitung zwischen VPN-Verbindungen* auf **Ja** gesetzt, werden für die in den mGuard eingehende Datenpakete die Regeln unter **Firewall eingehend** angewendet und für die ausgehende Datenpakete die Regeln unter **Firewall ausgehend**.

Fallen die ausgehenden Datenpakete unter die selbe Verbindungsdefinition (bei einer definierten VPN-Verbindungsgruppe), werden die Firewall-Regeln für **Eingehend** und **Ausgehend** der selben Verbindungsdefinition angewendet.

Gilt für die ausgehenden Datenpakete eine andere VPN-Verbindungsdefinition, werden die Firewall-Regeln für **Ausgehend** dieser anderen Verbindungsdefinition angewendet.

Wenn der mGuard so konfiguriert wurde, dass er Pakete einer SSH-Verbindung weiterleitet (z. B. durch das Erlauben einer SEC-Stick Hub & Spoke-Verbindung), dann werden vorhandene VPN-Firewall-Regeln nicht angewendet. Das bedeutet, dass zum Beispiel die Pakete einer SSH-Verbindung durch einen VPN-Tunnel geschickt werden, obwohl dessen Firewall-Regel dies verbietet.

IPsec VPN >> Verbindungen >> Editieren >> Firewall

Eingehend

Generelle Firewall Einstellung

Alle eingehenden Verbindungen annehmen, die Datenpakete aller eingehenden Verbindungen werden angenommen.

Alle eingehenden Verbindungen verwerfen, die Datenpakete aller eingehenden Verbindungen werden verworfen.

Anwenden des unten angegebenen Regelwerks, blendet weitere Einstellmöglichkeiten ein. (Dieser Menüpunkt gehört nicht zum Funktionsumfang vom mGuard rs2000).

Die folgenden Einstellungen sind nur sichtbar, wenn „**Anwenden des unten angegebenen Regelwerks**“ eingestellt ist.

Protokoll

Alle bedeutet: TCP, UDP, ICMP, GRE und andere IP-Protokolle.

Von IP/Nach IP

0.0.0.0/0 bedeutet alle IP-Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise (siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 6-261).

Eingehend:

- Von IP: die IP-Adresse im VPN-Tunnel
- Nach IP die 1-zu-1-NAT Adresse bzw. die reale Adresse

Ausgehend:

- Von IP: die 1-zu-1-NAT Adresse bzw. die reale Adresse
- Nach IP: die IP-Adresse im VPN-Tunnel

Von Port/Nach Port

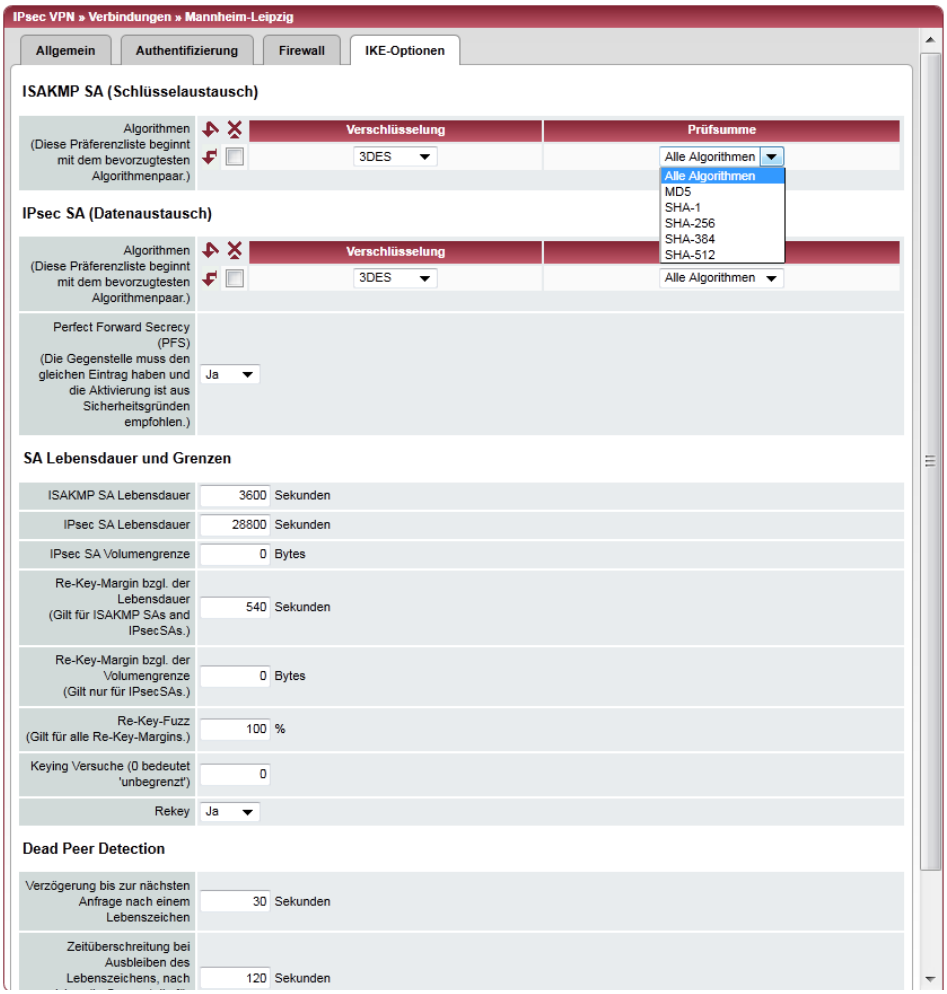
(wird nur ausgewertet bei den Protokollen TCP und UDP)

- **any** bezeichnet jeden beliebigen Port.
- **startport:endport** (z. B. 110:120) bezeichnet einen Portbereich.

Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben: (z. B. 110 für pop3 oder pop3 für 110).

IPsec VPN >> Verbindungen >> Editieren >> Firewall		
	Aktion	**Annehmen** bedeutet, die Datenpakete dürfen passieren. **Abweisen** bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat Abweisen dieselbe Wirkung wie Verwerfen.) **Verwerfen** bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information über deren Verbleib erhält.
	Kommentar	Ein frei wählbarer Kommentar für diese Regel.
	Log	Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel – das Ereignis protokolliert werden soll – *Log* auf **Ja** setzen – oder nicht – *Log* auf **Nein** setzen (werkseitige Voreinstellung).
	Log-Einträge für unbekannte Verbindungsversuche	Bei **Ja** werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden.
Ausgehend	Die Erklärung unter „Eingehend“ gilt auch für „Ausgehend“.	

6.8.2.5 IKE-Optionen



IPsec VPN >> Verbindungen >> Editieren >> IKE-Optionen		
ISAKMP SA (Schlüsselaustausch)	**Algorithmen**	Vereinbaren Sie mit dem Administrator der Gegenstelle, welches Verschlüsselungsverfahren verwendet werden soll. **Verschlüsselung** 3DES-168 ist das am häufigsten benutzte Verfahren und ist deshalb als Standard voreingestellt. Grundsätzlich gilt Folgendes: Je mehr Bits ein Verschlüsselungsalgorithmus hat (angegeben durch die angefügte Zahl), desto sicherer ist er. Das relativ neue Verfahren AES-256 gilt daher als am sichersten, ist aber noch nicht so verbreitet. Der Verschlüsselungsvorgang ist um so zeitaufwendiger, je länger der Schlüssel ist. Dieser Gesichtspunkt spielt für den mGuard keine Rolle, weil er mit Hardware-basierter Verschlüsselungstechnik arbeitet. Jedoch könnte dieser Aspekt für die Gegenstelle eine Rolle spielen. Der zur Auswahl stehende mit „Null“ bezeichnete Algorithmus beinhaltet keinerlei Verschlüsselung. **Prüfsumme** Lassen Sie die Einstellung auf *Alle Algorithmen* stehen. Dann spielt es keine Rolle, ob die Gegenstelle mit MD5, SHA-1, SHA-256, SHA-384 oder SHA-512 arbeitet. Die Verschlüsselungs-Algorithmen SHA-256 und SHA-512 werden von allen mGuards unterstützt. Aber nicht alle mGuards beschleunigen die Algorithmen per Hardware. Der mGuard centerport unterstützt und benötigt keine Hardware-Beschleunigung. Bei den anderen mGuards werden MD5 und SHA1 mit Hardware beschleunigt. Nur der mGuard smart^2 beschleunigt zusätzlich SHA-256 per Hardware.
IPsec SA (Datenaustausch)	Im Unterschied zu *ISAKMP SA (Schlüsselaustausch)* (s. o.) wird hier das Verfahren für den Datenaustausch festgelegt. Es kann sich von denen des Schlüsselaustausches unterscheiden, muss aber nicht.	
	Algorithmen	Siehe oben.

IPsec VPN >> Verbindungen >> Editieren >> IKE-Optionen		
	Perfect Forward Secrecy (PFS)	Verfahren zur zusätzlichen Steigerung der Sicherheit bei der Datenübertragung. Bei IPsec werden in bestimmten Intervallen die Schlüssel für den Datenaustausch erneuert. Mit PFS werden dabei mit der Gegenstelle neue Zufallszahlen ausgehandelt, anstatt sie aus zuvor verabredeten Zufallszahlen abzuleiten. Die Gegenstelle muss den gleichen Eintrag haben. Wir empfehlen aus Sicherheitsgründen die Aktivierung. Wenn die Gegenstelle PFS unterstützt, wählen Sie **Ja**. Ist die Gegenstelle ein IPsec/L2TP-Client, dann setzen Sie *Perfect Forward Secrecy (PFS)* auf **Nein**.
SA-Lebensdauer und Grenzen	**Die Schlüssel einer IPsec-Verbindung werden in bestimmten Abständen erneuert, um die Kosten eines Angriffs auf eine IPsec-Verbindung zu erhöhen.**	
	ISAKMP SA-Lebensdauer	Lebensdauer der für die ISAKMP SA vereinbarten Schlüssel in Sekunden. Werkseinstellung: 3600 Sekunden (1 Stunde). Das erlaubte Maximum sind 86400 Sekunden (24 Stunden).
	IPsec SA-Lebensdauer	Lebensdauer der für die IPsec SA vereinbarten Schlüssel in Sekunden. Werkseinstellung: 28800 Sekunden (8 Stunden). Das erlaubte Maximum sind 86400 Sekunden (24 Stunden).
	IPsec SA-Volumengrenze	0 bis 2147483647 Bytes Der Wert 0 bedeutet, dass es keine Volumengrenze für die IPsec SAs dieser VPN-Verbindung gibt. Alle anderen Werte geben die Anzahl an Bytes an, die maximal von IPsec SA für diese VPN-Verbindung verschlüsselt werden (Hard Limit).
	Re-Key-Margin bzgl. der Lebensdauer	Gilt für ISAKMP SAs und IPsec SAs Minimale Zeitspanne vor Ablauf der alten Schlüssel, innerhalb der ein neuer Schlüssel erzeugt werden soll. Werkseinstellung: 540 Sekunden (9 Minuten).

IPsec VPN >> Verbindungen >> Editieren >> IKE-Optionen		
	Re-Key-Margin bzgl. der Volumengrenze	Gilt nur für IPsec SAs Der Wert 0 bedeutet, dass die Volumengrenze nicht angewendet wird. Sie müssen 0 einstellen, wenn der unter *IPsec SA-Volumengrenze* eingestellte Wert 0 ist. Wenn ein Wert über 0 eintragen wird, dann wird eine neue Grenze aus zwei Werten errechnet. Und zwar wird von dem unter *IPsec SA-Volumengrenze* angegebenen Wert (dem *Hard Limit*) die hier angegebene Byteanzahl abgezogen. Der so errechnete Wert wird als *Soft Limit* bezeichnet. Er gibt die Anzahl an Bytes an, die verschlüsselt worden sein müssen, damit ein neuer Schlüssel für die IPsec SA ausgehandelt wird. Wenn außerdem ein Re-Key-Fuzz (s. u.) über 0 eingetragen ist, wird ein zusätzlicher Betrag abgezogen. Dieser Betrag ist ein Prozentsatz des Re-Key-Margins. Die Höhe dieses Prozentsatzes wird unter Re-Key-Fuzz angegeben. Der Re-Key-Margin-Wert muss unter dem des *Hard Limits* liegen. Er muss sogar deutlich darunter liegen, wenn zusätzlich ein *Re-Key-Fuzz* addiert wird. Wenn die *IPsec SA-Lebensdauer* vorher erreicht wird, dann wird das *Soft Limit* ignoriert.
	Re-Key-Fuzz	Maximum in Prozent, um das *Re-Key-Margin* zufällig vergrößert werden soll. Dies dient dazu, den Schlüsselaustausch auf Maschinen mit vielen VPN-Verbindungen zeitversetzt stattfinden zu lassen. Werkseinstellung: 100 Prozent.
	Keying-Versuche	Anzahl der Versuche, die unternommen werden sollen, neue Schlüssel mit der Gegenstelle zu vereinbaren. Der Wert 0 bedeutet bei Verbindungen, die der mGuard initiieren soll, unendlich viele Versuche, ansonsten 5 Versuche.
	Rekey	**Ja / Nein** Bei **Ja** wird der mGuard versuchen, einen neuen Schlüssel zu vereinbaren, wenn die Gültigkeit des alten abläuft.
Dead Peer Detection	**Wenn die Gegenstelle das Dead Peer Detection (DPD) Protokoll unterstützt, können die jeweiligen Partner erkennen, ob die IPsec-Verbindung noch gültig ist oder nicht und evtl. neu aufgebaut werden muss.**	
	Verzögerung bis zur nächsten Anfrage nach einem Lebenszeichen	Zeitspanne in Sekunden, nach welcher *DPD Keep Alive* Anfragen gesendet werden sollen. Diese Anfragen testen, ob die Gegenstelle noch verfügbar ist. Werkseinstellung: 30 Sekunden.

IPsec VPN >> Verbindungen >> Editieren >> IKE-Optionen		
	Zeitüberschreitung bei Ausbleiben des Lebenszeichens, nach welcher die Gegenstelle für tot befunden wird	Zeitspanne in Sekunden, nach der die Verbindung zur Gegenstelle für tot erklärt werden soll, wenn auf die *Keep Alive* Anfragen keine Antwort erfolgte. Werkseinstellung: 120 Sekunden. Wenn der mGuard eine Verbindung für tot befindet, handelt er entsprechend der Einstellung, die unter **Verbindungsinitiierung** festgelegt ist (siehe Definition dieser VPN-Verbindung, Registerkarte *Allgemein,* **Verbindungsinitiierung**).

6.8.3 IPsec VPN >> L2TP über IPsec

Diese Einstellungen gelten nicht im Stealth-Modus.

Ermöglicht den Aufbau von VPN-Verbindungen durch das IPsec/L2TP-Protokoll zum mGuard.

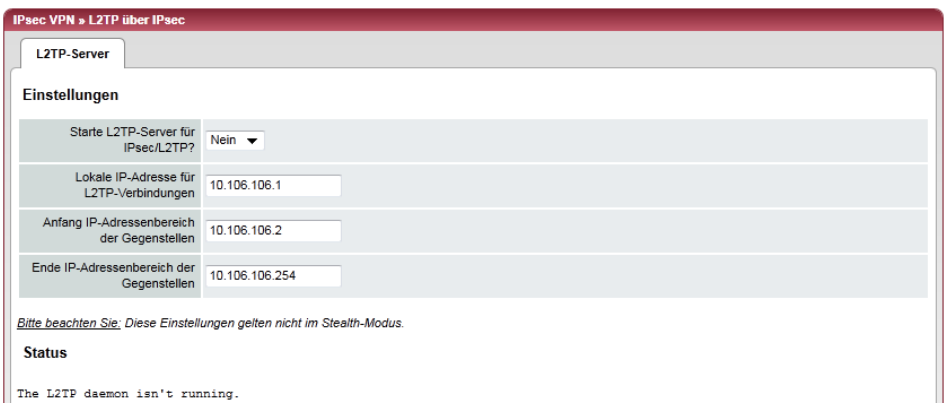
Dabei wird über eine IPsec Transportverbindung das L2TP-Protokoll gefahren um darin wiederum eine Tunnelverbindung mit dem Point-to-Point-Protokoll (PPP) aufzubauen. Durch das PPP werden den Clients automatisch IP-Adressen zugewiesen.

Um IPsec/L2TP zu nutzen muss der L2TP-Server aktiviert werden sowie eine oder mehrere IPsec-Verbindungen mit den folgenden Eigenschaften eingerichtet werden:

- **Typ**: Transport
- **Protokoll**: UDP
- **Lokaler Port**: %all
- **Remote Port**: %all
- **PFS**: Nein

(Siehe auch „Weitere Einstellungen nach Klicken auf **Mehr...**“ auf Seite 6-198 sowie „IKE-Optionen“ auf Seite 6-213.)

6.8.3.1 L2TP-Server



IPsec VPN >> L2TP über IPsec >> L2TP-Server		
Einstellungen	**Starte L2TP-Server für IPsec/L2TP?**	Wollen Sie IPsec/L2TP-Verbindungen ermöglichen, setzen Sie diesen Schalter auf **Ja**. Über IPsec können dann zum mGuard L2TP-Verbindungen aufgebaut werden, über welche den Clients dynamisch IP-Adressen innerhalb des VPNs zugeteilt werden.
	Lokale IP-Adresse für L2TP-Verbindungen	Nach dem obigen Screenshot teilt der mGuard der Gegenstelle mit, er habe die Adresse 10.106.106.1.
	Anfang / Ende IP-Adressbereich der Gegenstellen	Nach dem obigen Screenshot teilt der mGuard der Gegenstelle eine IP-Adresse zwischen 10.106.106.2 und 10.106.106.254 mit.
	Status	Informiert über den L2TP-Status, wenn dieser als Verbindungstyp gewählt ist.

6.8.4 IPsec VPN >> IPsec Status

Informiert über den Status der IPsec-Verbindungen.

Links sind die Namen der VPN-Verbindungen aufgelistet, rechts daneben wird jeweils deren aktueller Status angezeigt.

Schaltflächen

Aktualisieren — Um gegebenenfalls die angezeigten Daten auf den aktuellen Stand zu bringen, auf die Schaltfläche **Aktualisieren** klicken.

Neustart — Wollen Sie eine Verbindung trennen und dann neu starten, auf die entsprechende **Neustart**-Schaltfläche klicken.

Editieren — Wollen Sie eine Verbindung neu konfigurieren, auf die entsprechende **Editieren**-Schaltfläche klicken.

Verbindung, ISAKMP Status, IPsec Status

GATEWAY — *GATEWAY* zeigt die IP-Adressen der miteinander kommunizierenden VPN-Gateways.

TRAFFIC — *TRAFFIC* bezeichnet Rechner bzw. Netze, die über die VPN-Gateways kommunizieren.

ID — bezeichnet das Subject eines X.509-Zertifikats.

ISAKMP-Status — *ISAKMP-Status* (Internet security association and key management protocol) ist mit „established“ angegeben, wenn die beiden beteiligten VPN-Gateways einen Kanal zum Schlüsselaustausch aufgebaut haben. In diesem Fall konnten sie einander kontaktieren, und alle Einträge bis einschließlich „ISAKMP SA“ auf der Konfigurationsseite der Verbindung sind korrekt.

IPsec-Status — *IPsec-Status* ist mit „established“ angegeben, wenn die IPsec-Verschlüsselung bei der Kommunikation aktiviert ist. In diesem Fall sind auch die Angaben unter „IPsec SA“ und „Tunneleinstellungen“ korrekt.

Bei Problemen empfiehlt es sich, in die VPN-Logs der Gegenstelle zu schauen, zu der die Verbindung aufgebaut wurde. Denn der initiierende Rechner bekommt aus Sicherheitsgründen keine ausführlichen Fehlermeldungen zugesandt.

Falls angezeigt wird:	**Bedeutet das:**
ISAKMP SA established, IPsec State: WAITING	Die Authentifizierung war erfolgreich, jedoch stimmten die anderen Parameter nicht: Stimmt der Verbindungstyp (Tunnel, Transport) überein? Wenn Tunnel gewählt ist, stimmen die Netzbereiche auf beiden Seiten überein?
IPsec State: IPsec SA established	Die VPN-Verbindung ist erfolgreich aufgebaut und kann genutzt werden. Sollte dies dennoch nicht möglich sein, dann macht das VPN-Gateway der Gegenstelle Probleme. In diesem Fall die Verbindung deaktivieren und wieder aktivieren, um die Verbindung erneut aufzubauen.

6.9 Menü SEC-Stick

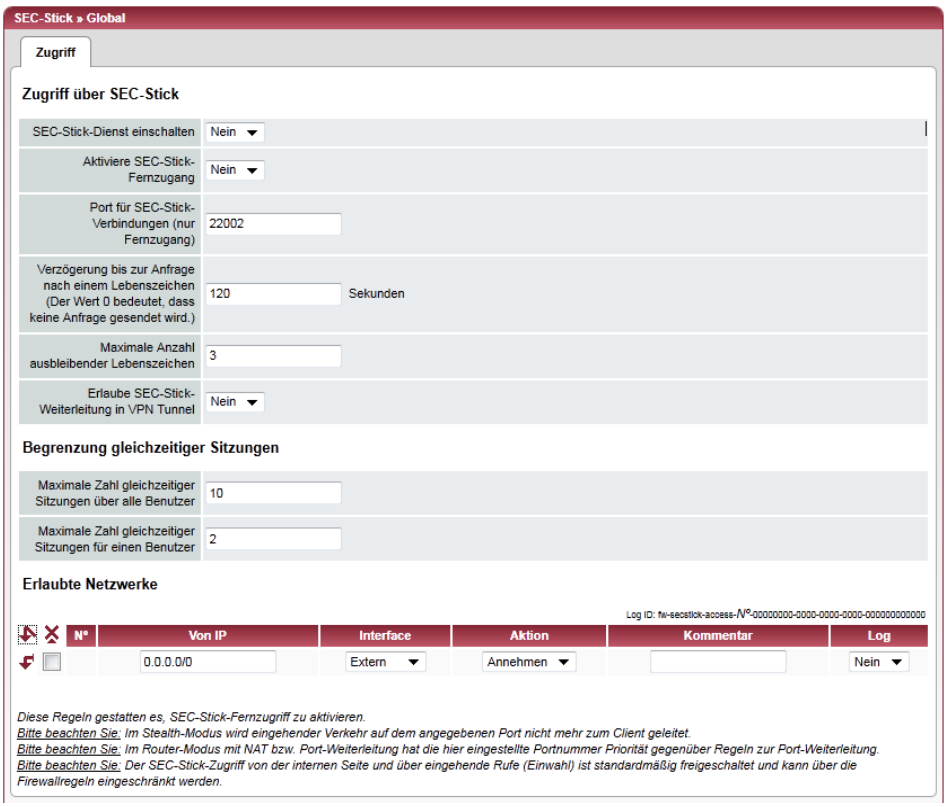
Der mGuard unterstützt die Nutzung eines SEC-Sticks, ein Zugriffsschutz für IT-Systeme. Der SEC-Stick ist ein Produkt der Firma team2work: www.team2work.de.

Der SEC-Stick ist praktisch ein Schlüssel. Der Benutzer steckt ihn in den USB-Port eines Rechners mit Internetanbindung, und kann dann eine verschlüsselte Verbindung zum mGuard aufbauen, um sicher auf definierte Dienste im Netzwerk des Büros oder daheim zuzugreifen. Zum Beispiel kann das Remote Desktop Protokoll innerhalb der verschlüsselten und sicheren SEC-Stick-Verbindung benutzt werden, um den PC im Büro oder zu Hause fernzusteuern als säße man direkt davor.

Damit das funktioniert, ist der Zugang zum Geschäfts-PC durch den mGuard geschützt, und der mGuard muss für den SEC-Stick konfiguriert sein, damit dieser den Zugang öffnen kann. Denn der Benutzer des entfernten Rechners, in den der SEC-Stick eingesteckt ist, authentisiert sich beim mGuard mit den Daten und der Software, die auf seinem SEC-Stick gespeichert sind.

Der SEC-Stick stellt eine SSH-Verbindung zum mGuard her. In diese können weitere Kanäle eingebettet sein, z. B. TCP/IP-Verbindungen.

6.9.1 Global



SEC-Stick >> Global >> Zugriff

Zugriff über SEC-Stick

Dieser Menüpunkt gehört nicht zum Funktionsumfang vom mGuard rs2000.

Der Zugriff über SEC-Stick ist eine lizenzpflichtige Funktion. Sie kann nur benutzt werden, wenn die entsprechende Lizenz erworben und installiert ist.

SEC-Stick-Dienst einschalten: Mit **Ja** legen Sie fest, dass der an einem entfernten Standort eingesetzte SEC-Stick bzw. dessen Besitzer sich einloggen kann. In diesem Fall muss zusätzlich der SEC-Stick-Fernzugang aktiviert werden (nächster Schalter).

Aktiviere SEC-Stick-Fernzugang Mit **Ja** wird der SEC-Stick-Fernzugang aktiviert.

Port für SEC-Stick-Verbindungen (nur Fernzugang) Standard: 22002

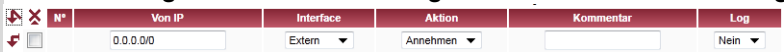
Wird diese Port-Nummer geändert, gilt die geänderte Port-Nummer nur für Zugriffe über das Interface *Extern, Extern 2* oder *VPN*. Für internen Zugriff gilt weiterhin 22002

SEC-Stick >> Global >> Zugriff [...]		
	Verzögerung bis zur Anfrage nach einem Lebenszeichen	Default: 120 Sekunden Einstellbar sind Werte von 0 bis 3600 Sekunden. Positive Werte bedeuten, dass der mGuard innerhalb der verschlüsselten SSH-Verbindung eine Anfrage an die Gegenstelle sendet, ob sie noch erreichbar ist. Die Anfrage wird gesendet, wenn für die angegebene Anzahl von Sekunden keine Aktivität von der Gegenstelle bemerkt wurde (zum Beispiel durch Netzwerkverkehr innerhalb der verschlüsselten Verbindung). Der hier eingetragene Wert bezieht sich auf die Funktionsfähigkeit der verschlüsselten SSH-Verbindung. Solange diese gegeben ist, wird die SSH-Verbindung vom mGuard wegen dieser Einstellungen nicht beendet, selbst wenn der Benutzer während dieser Zeit keine Aktion ausführt. Da die Anzahl der gleichzeitig geöffneten Sitzungen begrenzt ist (siehe *Maximale Zahl gleichzeitiger Sitzungen für alle Benutzer*), ist es wichtig, abgelaufene Sitzungen zu beenden. Deshalb wird ab Version 7.4.0 die Anfrage nach einem Lebenszeichen auf 120 Sekunden voreingestellt. Bei maximal drei Anfragen nach einem Lebenszeichen, wird eine abgelaufende Sitzung nach sechs Minuten entdeckt und entfernt. In vorherigen Versionen war die Voreinstellung „0“. Das bedeutet, dass keine Anfragen nach einem Lebenszeichen gesendet werden. Beachten Sie, dass durch die Lebenszeichen-Anfragen zusätzlicher Traffic erzeugt wird.
	Maximale Anzahl ausbleibender Lebenszeichen	Gibt an, wie oft Antworten auf Anfragen nach Lebenszeichen der Gegenstelle ausbleiben dürfen. Wenn z. B. alle 15 Sekunden nach einem Lebenszeichen gefragt werden soll und dieser Wert auf 3 eingestellt ist, dann wird die Verbindung des SEC-Stick-Clients gelöscht, wenn nach circa 45 Sekunden immer noch kein Lebenszeichen gegeben wurde.
Begrenzung gleichzeitiger Störungen	Für SEC-Stick-Verbindungen gibt eine Begrenzung der Anzahl von gleichzeitigen Sitzungen. Pro Sitzung wird etwa 0,5 MB Speicherplatz benötigt, um das maximale Sicherheitslevel zu gewährleisten. Die Einschränkung hat keine Auswirkung auf bereits bestehende Sitzungen, sondern nur auf neu aufgebaute Verbindungen.	
	Maximale Zahl gleichzeitiger Sitzungen für alle Benutzer	0 bis 2147483647 Gibt die Anzahl der Verbindungen an, die von allen Benutzern gleichzeitig erlaubt sind. Bei "0" ist keine Sitzung erlaubt.
	Maximale Zahl gleichzeitiger Sitzungen für einen Benutzer	0 bis 2147483647 Gibt die Anzahl der Verbindungen an, die von einem Benutzer gleichzeitig erlaubt sind. Bei "0" ist keine Sitzung erlaubt.

SEC-Stick >> Global >> Zugriff [...]

Erlaubte Netzwerke

Listet die eingerichteten Firewall-Regeln für den SEC-Stick-Fernzugriff auf



Wenn mehrere Firewall-Regeln gesetzt sind, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Falls in der Regelliste weitere passende Regeln vorhanden sind, werden diese ignoriert.

Die hier angegebenen Regeln treten nur in Kraft, wenn der Schalter **Aktiviere SEC-Stick-Fernzugang** auf **Ja** steht. Weil Zugriffe von *Intern* auch möglich sind, wenn dieser Schalter auf *Nein* steht, tritt für diesen Fall eine Firewall-Regel, die den Zugriff von *Intern* verwehren würde, nicht in Kraft.

Sie können mehrere Regeln festlegen.

Von IP

Geben Sie hier die Adresse des Rechners/Netzes an, von dem der Fernzugriff erlaubt beziehungsweise verboten ist.

IP-Adresse: **0.0.0.0/0** bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise (siehe 6-261).

Interface

Extern / Intern / Extern 2 / VPN / Einwahl[1]

Gibt an, für welches Interface die Regel gelten soll.

Wenn keine Regeln gesetzt sind oder keine Regel greift, gelten folgende Standardeinstellungen:

- SEC-Stick-Fernzugang ist erlaubt über *Intern, VPN* und *Einwahl*.
- Zugriffe über *Extern* und *Extern 2* werden verwehrt.

Legen Sie die Zugriffsmöglichkeiten nach Bedarf fest.

> Wenn Sie Zugriffe über *Intern, VPN* oder *Einwahl* verwehren wollen, müssen Sie das explizit durch entsprechende Firewall-Regeln bewirken, in der Sie als Aktion z. B. *Verwerfen* festlegen.

Aktion

Annehmen bedeutet, die Datenpakete dürfen passieren.

Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat *Abweisen* dieselbe Wirkung wie *Verwerfen*.)

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information über deren Verbleib erhält.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

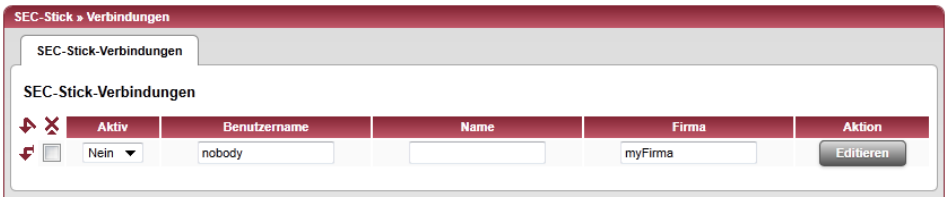
Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob beim Greifen der Regel

- das Ereignis protokolliert werden soll – *Log* auf **Ja** setzen
- oder das Ereignis nicht protokolliert werden soll – *Log* auf **Nein** setzen (werkseitige Voreinstellung).

[1] *Extern 2* und *Einwahl* nur bei Geräten mit serieller Schnittstelle (siehe „Netzwerk >> Interfaces“ auf Seite 6-64).

6.9.2 Verbindungen



SEC-Stick >> Verbindungen >> SEC-Stick-Verbindungen

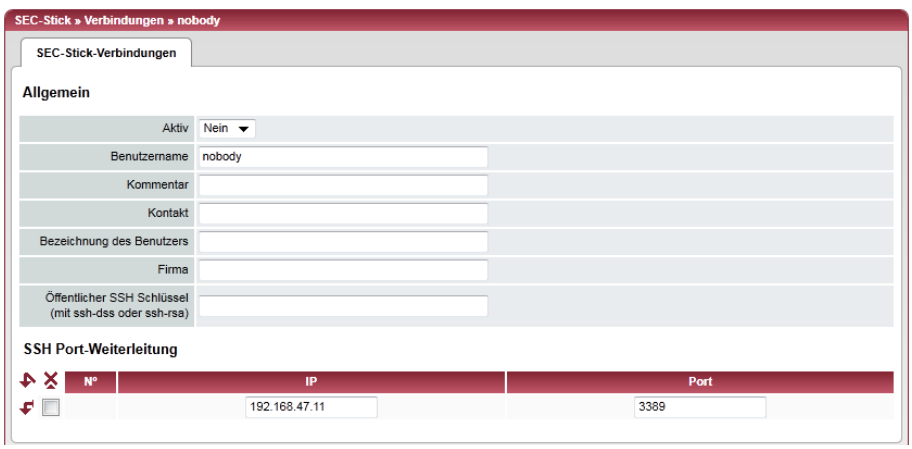
SEC-Stick-Verbindungen

Liste der definierten SEC-Stick-Verbindungen. Wollen Sie eine neue Verbindung hinzufügen klicken sie links oben auf den Pfeil nach unten. Eine bereits bestehende Verbindung können Sie bearbeiten, indem Sie auf die Schaltfläche Editieren klicken.

Nicht alle Funktionen des SEC-Sticks können über die Web-Benutzeroberfläche des mGuards konfiguriert werden.

Aktiv	Um eine definierte SEC-Stick-Verbindung nutzen zu können, muss der Schalter **Aktiv** auf **Ja** gesetzt werden.
Benutzername	Für jeden zugriffsberechtigten Inhaber eines SEC-Sticks, muss eine SEC-Stick-Verbindung mit einem eindeutig zugeordneten Benutzernamen definiert werden. Anhand dieses Benutzernamens werden die definierten Verbindungen eindeutig identifiziert.
Name	Name der Person.
Firma	Angabe der Firma.

Nach Klicken auf **Editieren** erscheint folgende Seite:



Allgemein

Aktiv	Wie oben
Benutzername	Wie oben
Kommentar	Optional: kommentierender Text.
Kontakt	Optional: kommentierender Text.
Bezeichnung des Benutzers	Optional: Name der Person. (Wiederholt)

SEC-Stick >> Verbindungen >> SEC-Stick-Verbindungen [...]		
	Firma	Optional: Wie oben
	Öffentlicher SSH-Schlüssel (mit ssh-dss oder ssh-rsa)	Hier muss der öffentliche SSH-Schlüssel, der zum SEC-Stick gehört, im ASCII-Format eingetragen werden. Das geheime Gegenstück ist auf dem SEC-Stick gespeichert.
SSH Port-Weiterleitung	**Liste der erlaubten Zugriffe und SSH-Port-Weiterleitungen bezogen auf den SEC-Stick des entsprechenden Benutzers.**	
	IP	IP-Adresse des Rechners, auf den der Zugriff ermöglicht wird.
	Port	Port-Nummer, die beim Zugriff auf den Rechner benutzt werden soll.

6.10 Menü QoS

Dieses Menü steht **nicht** auf dem **mGuard rs2000** zur Verfügung.

QoS (Quality of Service) bezeichnet die Dienstgüte einzelner Übertragungskanäle in IP-Netzwerken. Dabei geht es um die Zuteilung bestimmter Ressourcen an bestimmte Dienste (Services) bzw. Kommunikationsarten, damit diese reibungslos funktionieren. So muss z. B. für die Übertragung von Audio- oder Videodaten in Realzeit die notwendige Bandbreite bereitgestellt werden, um eine zufriedenstellende Kommunikation zu erreichen, während ein eventuell langsamerer Datentransfer per FTP oder E-Mail unkritisch für den gewünschten Gesamterfolg (Übertragung der gewünschten Datei oder E-Mail) ist.

6.10.1 Ingress Filter

Ein Ingress Filter bewirkt, dass bestimmte Datenpakete vor Eintreten in den Verarbeitungsmechanismus des mGuards ausgefiltert und verworfen werden, so dass eine Verarbeitung nicht stattfindet. Der mGuard kann Ingress-Filter benutzen, um die vorhandene Verarbeitungsleistung nach Möglichkeit nicht mit solchen Datenpaketen zu belasten, die im Netzwerk nicht gebraucht werden. Das hat den Effekt, dass die anderen, d. h. die gebrauchten Datenpakete schneller verarbeitet werden.

Durch geeignete Filterregeln kann z. B. sichergestellt werden, dass der administrative Zugang zum mGuard immer mit hoher Wahrscheinlichkeit erfolgen kann.

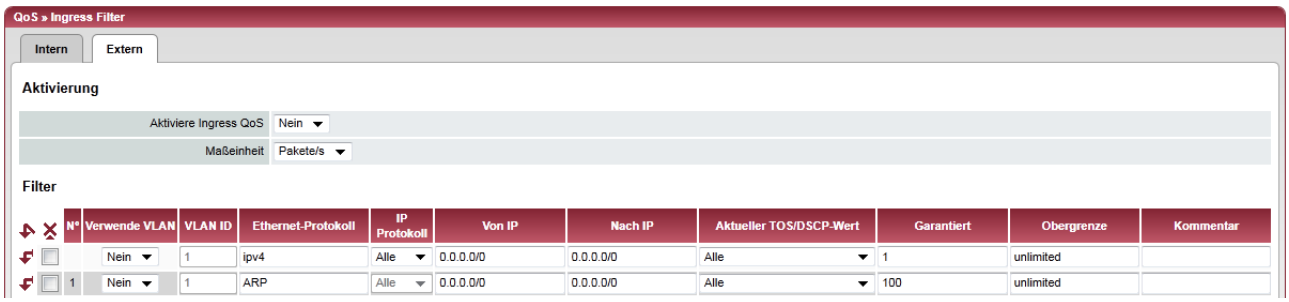
Die Paketverarbeitung auf dem mGuard ist im Wesentlichen durch das Handling des einzelnen Datenpakets geprägt, so dass die Verarbeitungsleistung nicht von der Bandbreite sondern von der Zahl der zu verarbeitenden Pakete abhängt.

Gefiltert wird ausschließlich nach Merkmalen, die jedes einzelne Datenpaket aufweist oder aufweisen kann: die im Header angegebene IP-Adresse von Sender und Absender, das angegebene Ethernet-Protokoll, das angegebene IP-Protokoll, der angegebene TOS/DSCP-Wert und/oder die VLAN-ID, wenn VLANs eingerichtet sind. Da durch die gesetzten Filterregeln bei jedem einzelnen Datenpaket geprüft wird, ob es unter die Filterregeln fällt, sollte die Liste der Filterregeln kurz sein. Sonst könnte die Zeit, die zum Ausfiltern gebraucht wird, länger sein, als der durch das Ausfiltern erzielte Zeitgewinn.

Es ist zu beachten, dass nicht alle angebbaren Filterkriterien sinnvoll kombiniert werden können. Zum Beispiel macht es keinen Sinn, bei Angabe des Ethernet-Protokolls ARP im selben Regelsatz zusätzlich ein IP-Protokoll anzugeben. Oder bei Angabe des Ethernet-Protokolls IPX (hexadezimal anzugeben) die IP-Adressen von Sender oder Absender vorzugeben.

6.10.1.1 Intern / Extern

Intern: Einstellung für Ingress Filter an der LAN-Schnittstelle



Extern: Einstellung für Ingress Filter an der WAN-Schnittstelle

Menü QoS >> Ingress Filter >> Intern/Extern		
Aktivierung	**Aktiviere Ingress QoS**	**Nein** (Standard): Das Feature ist ausgeschaltet. Falls Filterregeln definiert sind, werden sie ignoriert. **Ja**: Das Feature ist eingeschaltet. Datenpakete dürfen nur dann passieren und werden der Weitervermittlung und -verarbeitung des mGuards zugeführt, wenn sie den nachfolgend festgelegten Filterregeln entsprechen. Filter können für den LAN-Port (Registerkarte **Intern**) und den WAN-Port (Registerkarte **Extern**) gesetzt werden.
	Maßeinheit	**kbit/s / Pakete/s** Legt fest, in welcher Maßeinheit die weiter unten unter **Garantiert** und **Obergrenze** anzugebenden Zahlenwerte zu verstehen sind.
Filter	**Verwende VLAN**	Ist ein VLAN eingerichtet, kann die betreffende VLAN-ID angegeben werden, damit die betreffenden Datenpakete passieren dürfen. Dazu muss dieser Schalter auf **Ja** stehen.
	VLAN-ID	Legt fest, dass die Datenpakete des VLANs, das diese VLAN-ID hat, passieren dürfen. (Dazu muss der Schalter **Verwende VLAN** auf **Ja** stehen.)
	Ethernet-Protokoll	Legt fest, dass nur Datenpakete des angegebenen Ethernet-Protokolls passieren dürfen. Mögliche Einträge: **ARP**, **IPV4**, **%any**. Anderer Angaben müssen hexadezimal (bis zu 4 Ziffern) eingetragen werden. (Bei den Angaben handelt es sich um die Kennung des betreffenden Protokolls, die im Ethernet-Header steht. Kann in den Veröffentlichungen des betreffenden Standards nachgeschlagen werden.)
	IP-Protokoll	**Alle / TCP / UDP / ICMP / ESP** Legt fest, dass nur Datenpakete des ausgewählten IP-Protokolls passieren dürfen. Mit **Alle** findet keine Filterung nach IP-Protokoll statt.

Menü QoS >> Ingress Filter >> Intern/Extern [...]		
	Von IP	Legt fest, dass nur Datenpakete passieren dürfen, die von der angegebenen IP-Adresse kommen. Die Angabe **0.0.0.0/0** steht für alle Adressen, d. h. in diesem Fall findet keine Filterung nach IP-Adresse des Absenders statt. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise (siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 6-261).
	Nach IP	Legt fest, dass nur solche Datenpakete passieren dürfen, die zur angegebenen IP-Adresse weitergeleitet werden sollen. Angabe entsprechend wie oben unter *Von IP*. Die Angabe **0.0.0.0/0** steht für alle Adressen, d. h. in diesem Fall findet keine Filterung nach IP-Adresse des Absenders statt.
	Aktueller TOS/DSCP-Wert	Jedes Datenpaket enthält ein TOS bzw. DSCP-Feld. (TOS steht für Type Of Service, DSCP für Differentiated Services Code Point.) Hier wird angegeben, zu welcher Art von Traffic das Datenpaket gehört. So wird z. B. ein IP-Telefon in dieses Feld der von ihm ausgehenden Datenpakete etwas anderes hineinschreiben als ein FTP-Programm. Wenn Sie hier einen Wert auswählen, dürfen nur die Datenpakete passieren, die in ihrem TOS-bzw. DSCP-Feld diesen Wert haben. Mit **Alle** findet keine Filterung nach TOS/DSCP Wert statt.
	Garantiert	Die anzugebende Zahl legt fest, wie viele Datenpakete/s bzw. kbit/s - je nach eingestellter **Maßeinheit** (s. o.) - auf jeden Fall passieren dürfen. Das gilt für den Datenstrom, der den links angegebenen Kriterien dieses Regelsatzes entspricht, also passieren darf. Liefert dieser Datenstrom mehr Datenpakete pro Sekunde, dann **darf** der mGuard bei Kapazitätsengpässen die überzählige Anzahl an Datenpaketen verwerfen.
	Obergrenze	Die anzugebende Zahl legt fest, wie viele Datenpakete/s bzw. kbit/s - je nach eingestellter **Maßeinheit** (s. o.) - maximal passieren dürfen. Das gilt für den Datenstrom, der den links angegebenen Kriterien dieses Regelsatzes entspricht, also passieren darf. Liefert dieser Datenstrom mehr Datenpakete pro Sekunde, dann verwirft der mGuard die überzählige Anzahl an Datenpaketen.
	Kommentar	Optional: kommentierender Text.

6.10.2 Egress-Queues

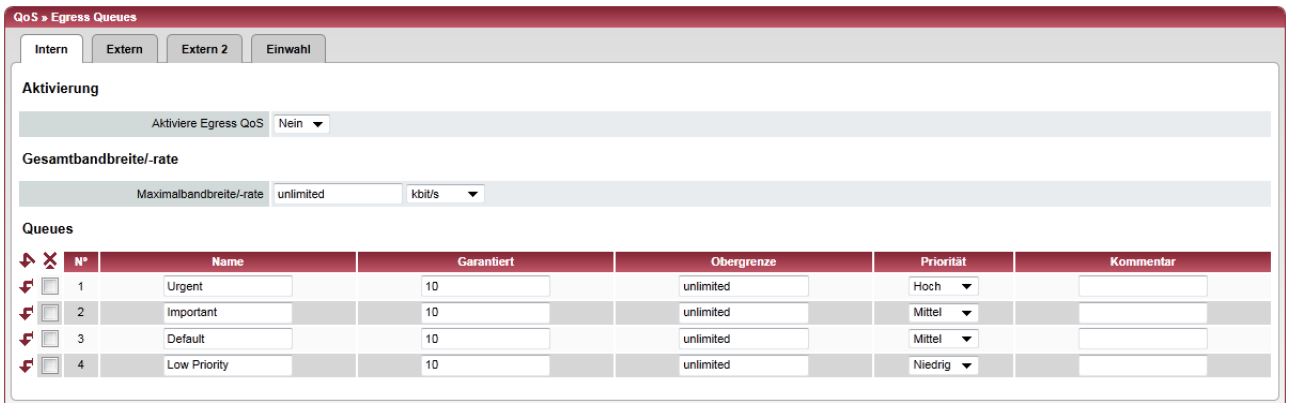
Den Diensten werden entsprechende Prioritätsstufen zugeordnet. Bei Verbindungsengpässen werden dann je nach zugeordneter Prioritätsstufe die ausgehenden Datenpakete in Egress-Queues (= Warteschlangen für anstehende Pakete) gestellt, die mit entsprechender Priorität abgearbeitet werden. Die Zuordnung von Prioritätsstufe und Bandbreite sollte im Idealfall so erfolgen, dass für Datenpakete von in Realzeit zu vollziehenden Übertragungen immer genügend Bandbreite zur Verfügung steht, während Pakete von anderen wie z. B. FTP-Downloads im Ernstfall vorübergehend auf Warten gesetzt werden.

Die Hauptanwendung von Egress-QoS ist die optimale Ausnutzung der zur Verfügung stehenden Bandbreite am jeweiligen Anschluss. In einigen Fällen kann auch eine Begrenzung der Paketrate nützlich sein, z. B. um einen langsamen Rechner im geschützten Netz vor Überlast zu schützen.

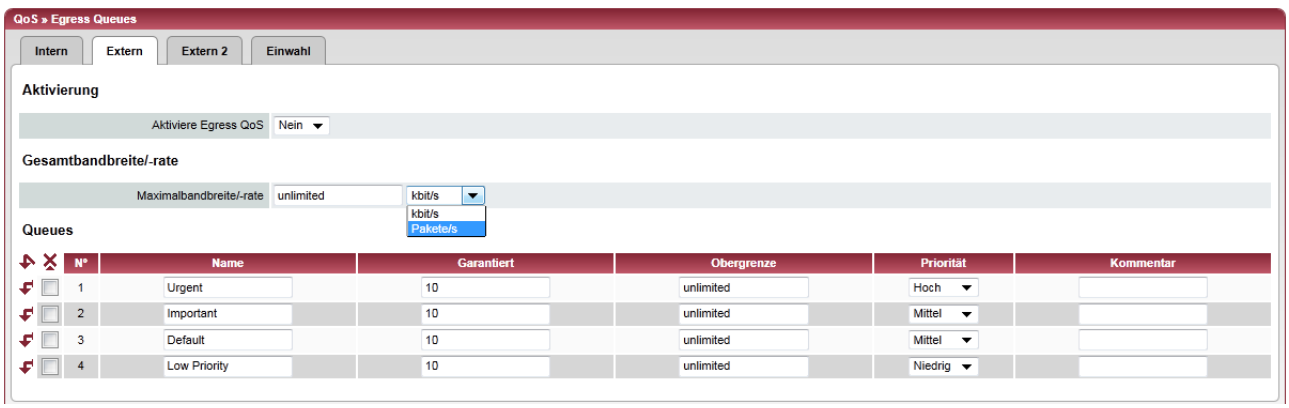
Das Feature *Egress-Queues* kann für alle Schnittstellen eingesetzt werden und für VPN-Verbindungen.

6.10.2.1 Intern / Extern / Extern 2 / Einwahl

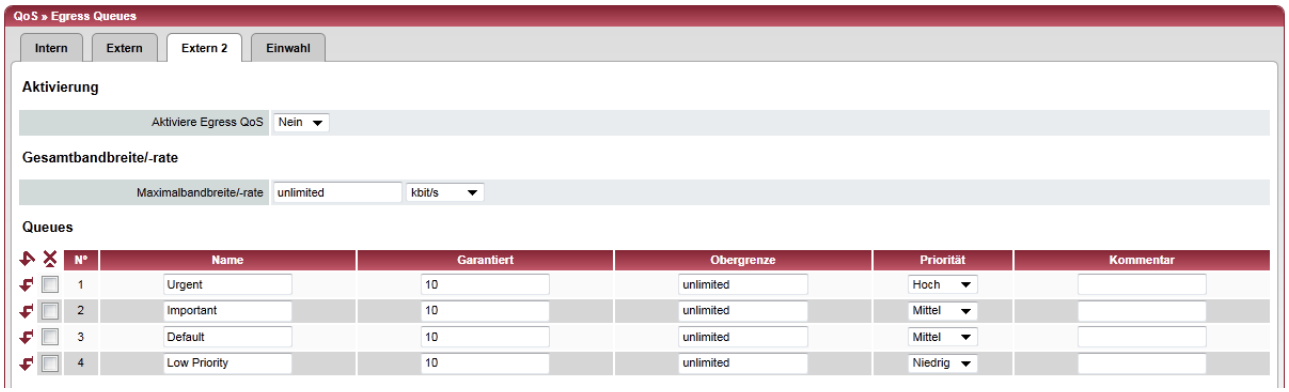
Intern: Einstellung für Egress-Queues an der LAN-Schnittstelle



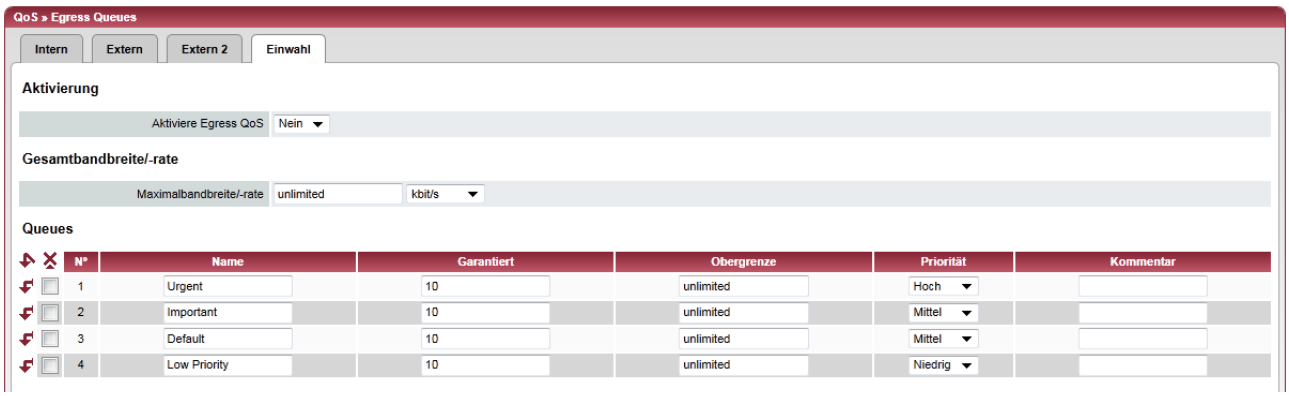
Extern: Einstellung für Egress-Queues an der WAN-Schnittstelle Extern



Extern 2: Einstellung für Egress-Queues bei der sekundären externen Schnittstelle.



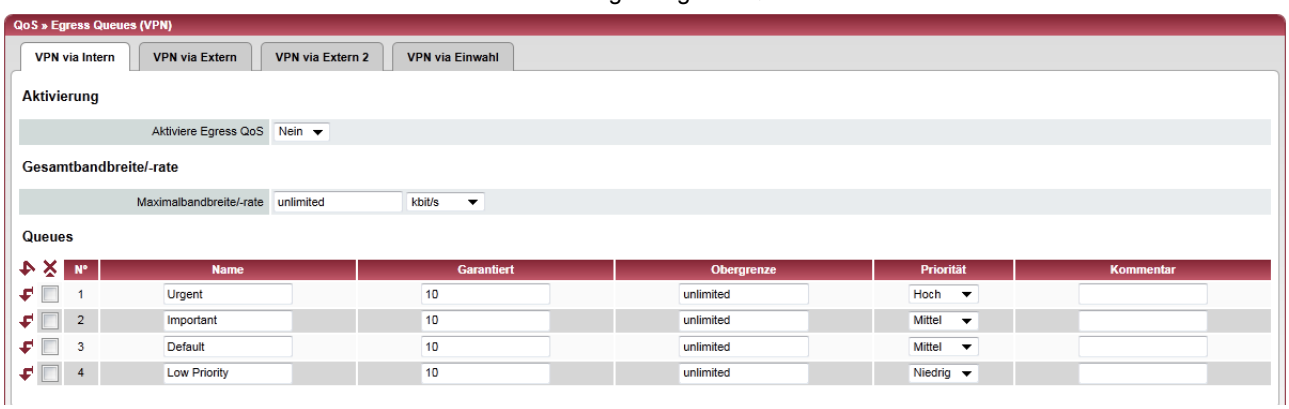
Einwahl: Einstellung für Egress-Queues für Pakete für ppp-Wählverbindung (Einwahl)



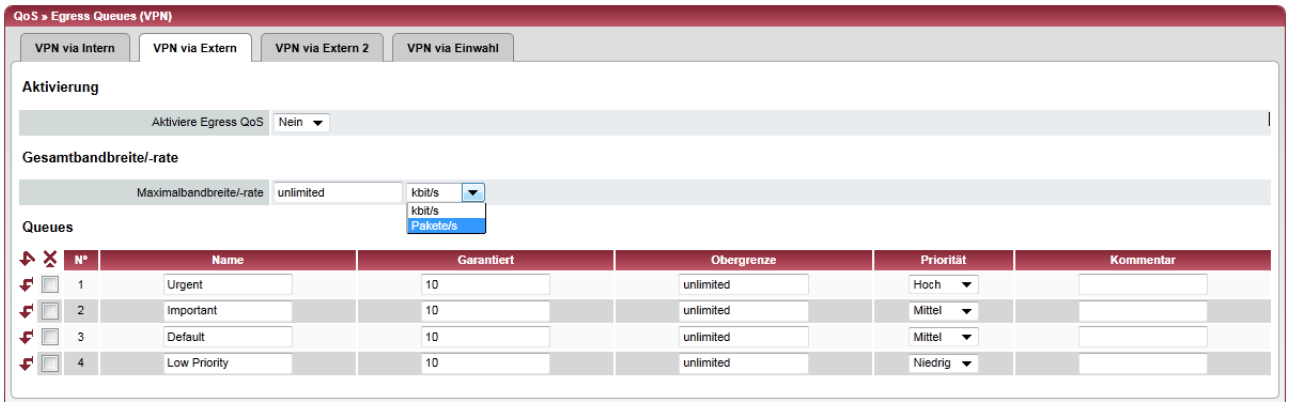
6.10.3 Egress-Queues (VPN)

6.10.3.1 VPN via Intern / VPN via Extern / VPN via Extern 2 / VPN via Einwahl

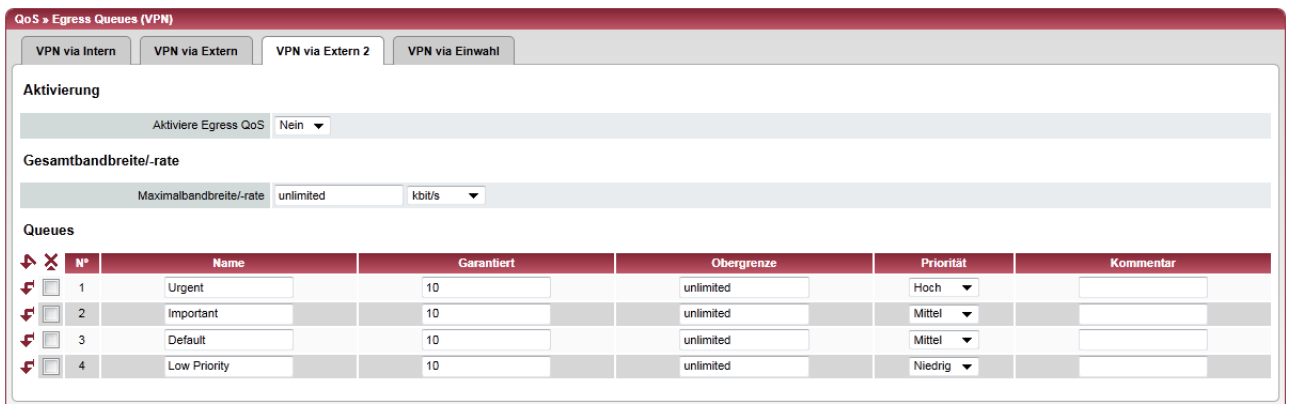
VPN via Intern: Einstellung für Egress-Queues



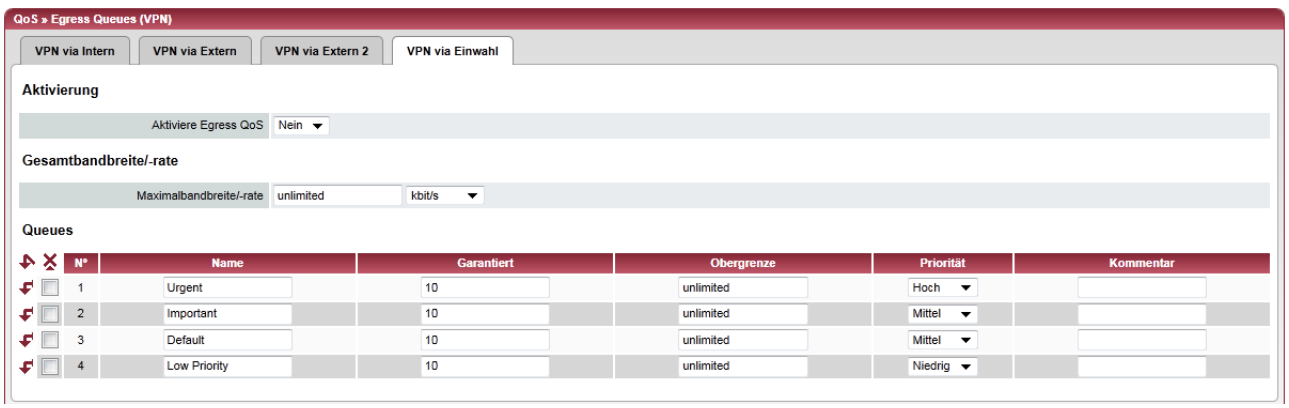
VPN via Extern: Einstellung für Egress-Queues



VPN via Extern 2: Einstellung für Egress-Queues



VPN via Einwahl: Einstellung für Egress-Queues



Alle oben aufgeführten Registerkarten für *Egress-Queues* bei den Interfaces *Intern, Extern, Extern 2, Einwahl* sowie für VPN-Verbindungen, die über dieses Interfaces geführt werden, bieten die gleichen Einstellmöglichkeiten.

In allen Fällen beziehen sich die Einstellungen auf die Daten, die von der jeweiligen Schnittstelle gesehen vom mGuard nach außen ins Netz gehen.

Menü QoS >> Egress-Queues >> Intern / Extern / Extern 2 / Einwahl Menü QoS >> Egress-Queues (VPN) >> PN via Intern / VPN via Extern / VPN via Extern 2 / VPN via Einwahl		
Aktivierung	**Aktiviere Egress QoS**	**Nein** (Standard): Das Feature ist ausgeschaltet. **Ja**: Das Feature ist eingeschaltet. Empfiehlt sich dann, wenn die Schnittstelle an ein Netz mit geringer Bandbreite angeschlossen ist, so dass eine Beeinflussung der Bandbreitenzuordnung zugunsten besonders wichtiger Daten gewünscht wird.
Gesamtbandbreite/-rate	**Maximalbandbreite/-rate**	**kBit/s / Pakete/s** Bandbreite, die insgesamt maximal physikalisch zur Verfügung steht - anzugeben in kBit/s oder Pakete/s. Die hier angegebene Gesamtbandbreite sollte etwas geringer angegeben werden als tatsächlich vorhanden, damit die Priorisierung optimal arbeitet. Damit wird verhindert, dass Puffer von weitervermittelnden Geräten überlaufen können und dadurch einen unerwünschten Effekt erzeugen.
Queues	**Name**	Sie können die voreingestellten Namen für die Egress-Queues übernehmen oder andere vergeben. Die Namen legen nicht die Prioritätsstufe fest.
	Garantiert	Bandbreite, die der betreffenden Queue auf jeden Fall zur Verfügung stehen soll. Je nach dem, ob oben unter **Maximalbandbreite/-rate** diese in **kbit/s** ODER in **Pakete/s** angegeben ist, verwenden Sie auch hier die selbe Maßeinheit, ohne diese explizit anzugeben. Die Summe aller garantierten Bandbreiten muss in Bezug zur Gesamtbandbreite kleiner oder gleich sein.
	Obergrenze	Bandbreite, die der betreffenden Queue vom System maximal zur Verfügung gestellt werden darf. Je nach dem, ob oben unter **Maximalbandbreite/-rate** diese in **kbit/s** ODER in **Pakete/s** angegeben ist, verwenden Sie auch hier die selbe Maßeinheit, ohne diese explizit anzugeben. Der Wert muss größer sein als die garantierte Bandbreite oder dieser gleich sein. Es kann auch der Wert **unlimited** angegeben werden, der keine weitere Beschränkung bewirkt.
	Priorität	**Niedrig / Mittel / Hoch** Legt fest, mit welcher Priorität die betreffende Warteschlange, sofern vorhanden, abgearbeitet werden muss, falls die zur Verfügung stehende Gesamtbandbreite aktuell nicht ausgeschöpft ist.
	Kommentar	Optional: kommentierender Text.

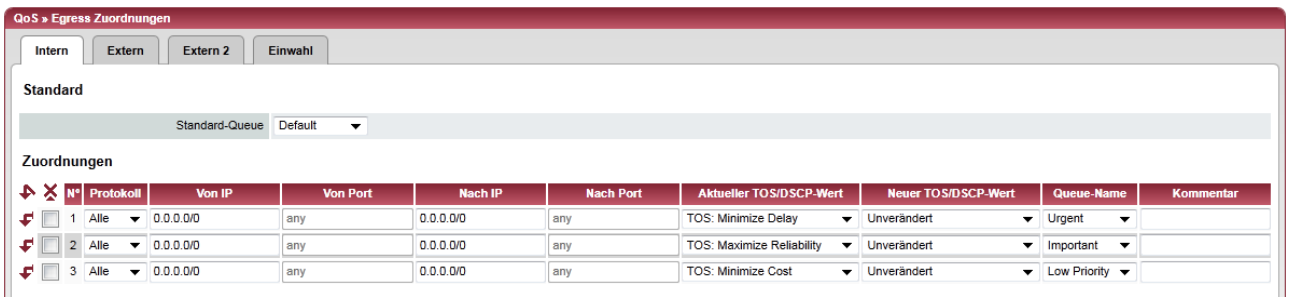
6.10.4 Egress-Zuordnungen

Welche Daten werden den definierten Egress-Queues (= Warteschlangen) (s. o.) zugeordnet, damit sie mit der Priorität übertragen werden, die der jeweiligen Queue zugeteilt ist?

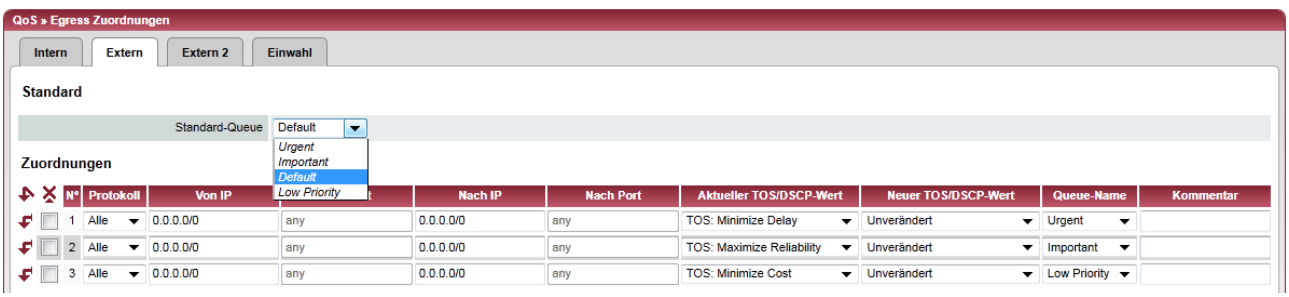
Die Zuordnungen können bezüglich aller Schnittstellen sowie für VPN-Verbindungen separat festgelegt werden.

6.10.4.1 Intern / Extern / Extern2 / Einwahl

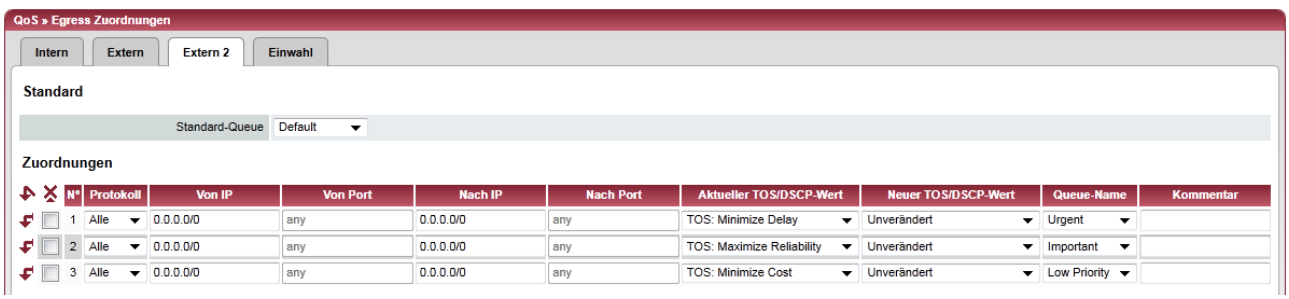
Intern: Einstellung für Egress-Queue-Zuordnungen



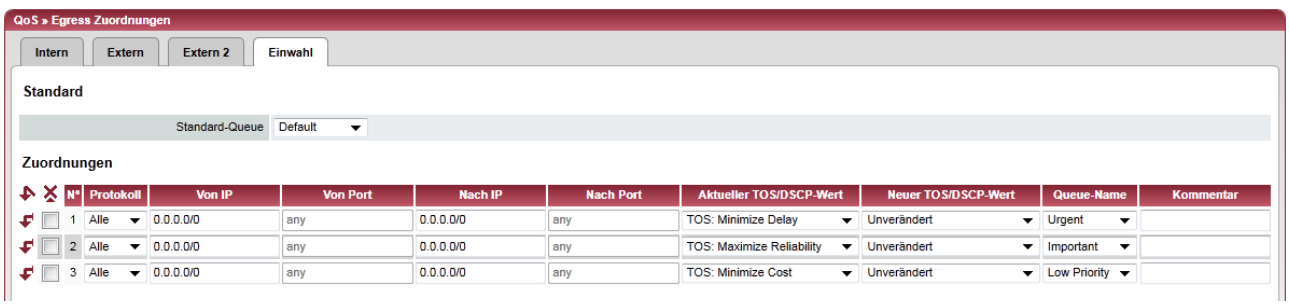
Extern: Einstellung für Egress-Queue-Zuordnungen



Extern 2: Einstellung für Egress-Queue-Zuordnungen



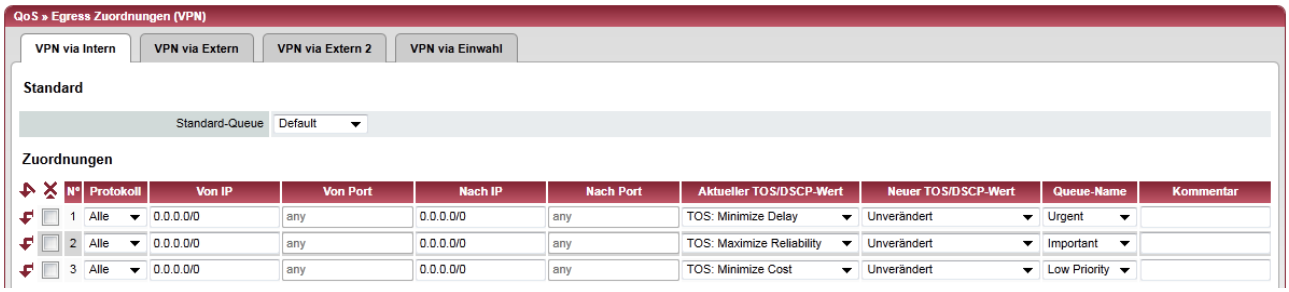
Einwahl: Einstellung für Egress-Queue-Zuordnungen



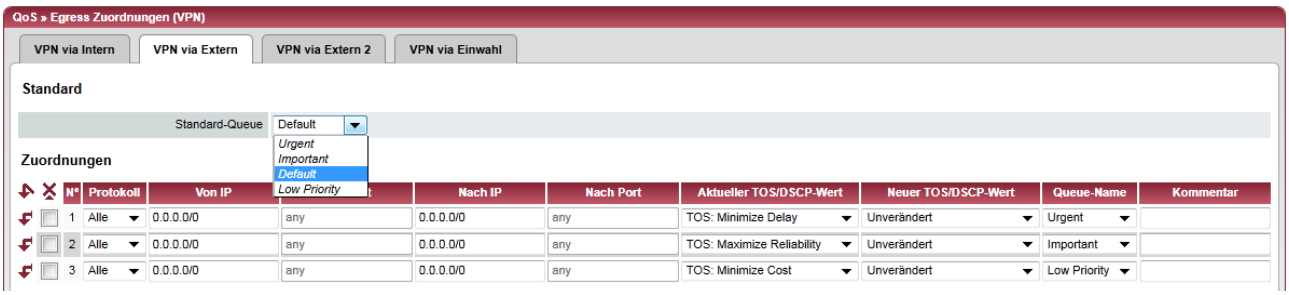
6.10.4.2 Egress-Zuordnungen VPN

VPN via Intern / VPN via Extern / VPN via Extern2 / VPN via Einwahl

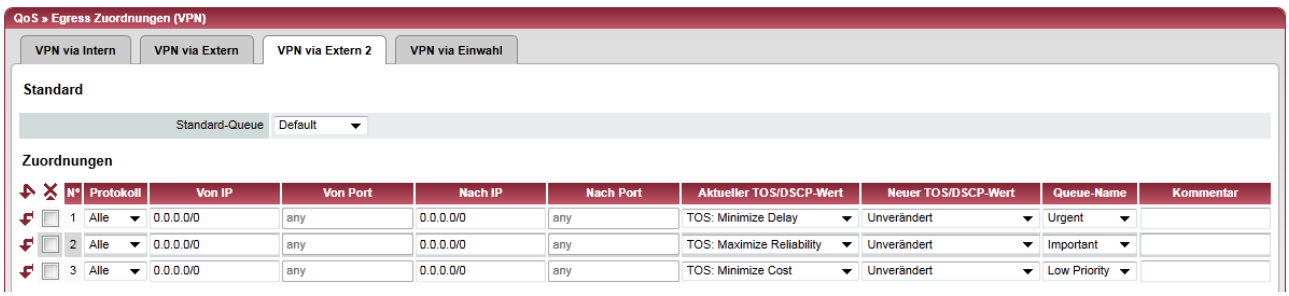
VPN via Intern: Einstellung für Egress-Queue-Zuordnungen



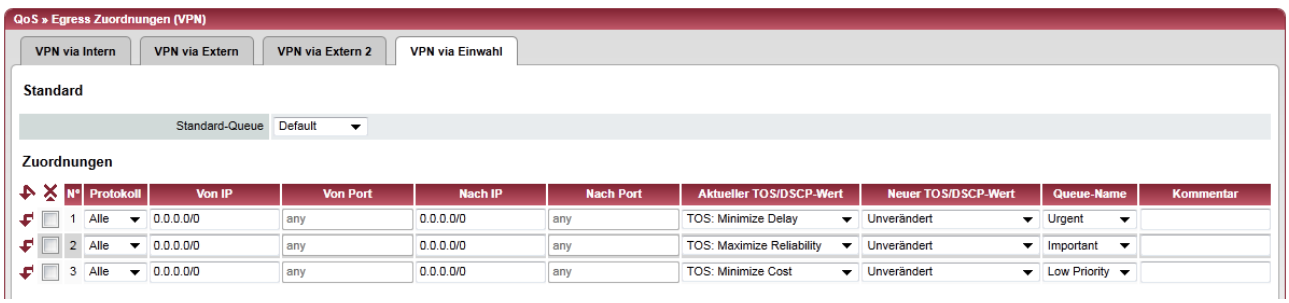
VPN via Extern: Einstellung für Egress-Queue-Zuordnungen



VPN via Extern 2: Einstellung für Egress-Queue-Zuordnungen



VPN via Einwahl: Einstellung für Egress-Queue-Zuordnungen



Alle oben aufgeführten Registerkarten für *Egress-Zuordnungen* in Bezug auf die Interfaces *Intern, Extern, Extern 2, Einwahl* sowie für VPN-Verbindungen, die über diese Interfaces geführt werden, bieten die gleichen Einstellmöglichkeiten.

In allen Fällen beziehen sich die Einstellungen auf die Daten, die von der jeweiligen Schnittstelle gesehen vom mGuard nach außen ins Netz gehen.

Menü QoS >> Egress-Zuordnungen >> Intern / Extern / Extern 2 / Einwahl Menü QoS >> Egress-Zuordnungen (VPN) >> PN via Intern/VPN via Extern/VPN via Extern 2/VPN via Einwahl		
Standard	**Standard -Queue**	*Name der Egress-Queues* (benutzerdefiniert) Angezeigt werden die Namen der Queues, wie sie unter *Egress-Queues* auf den Registerkarten *Intern* / *Extern* / *VPN via Extern* angezeigt oder festgelegt sind. Standardmäßig sind das folgende Namen: Default / Urgent / Important / Low Priority Traffic, der **nicht** nachfolgend unter *Zuordnungen* einer bestimmten Egress-Queue zugeordnet wird, bleibt der *Standard-Queue* zugeordnet. Über diese Auswahlliste legen Sie fest, welche Egress-Queue als *Standard-Queue* gelten soll.
	Zuordnungen	Die Zuordnung bestimmten Daten-Traffics zu einer Egress-Queue erfolgt über eine Liste von Kriterien. Treffen die Kriterien einer Zeile auf ein Datenpaket zu, wird es in die dort benannte Egress-Queue eingeordnet. **Beispiel**: Sie haben für zu übertragende Audio-Daten unter Egress-Queues (siehe Seite 6-229) unter dem Namen *Urgent* eine Queue mit garantierter Bandbreite und Priorität definiert. Dann legen Sie hier fest, nach welchen Regeln Audio-Daten erkannt werden, und dass diese Daten zur Queue *Urgent* gehören sollen.
	Protokoll	**Alle / TCP / UDP / ICMP /ESP** Protokoll(e), auf das/die sich die Zuordnung bezieht.
	Von IP	IP-Adresse des Netzes/Geräts, von wo die Daten kommen. **0.0.0.0/0** bedeutet alle IP-Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise (siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 6-261). Den Traffic von dieser Quelle ordnen Sie weiter hinten in dieser Zeile der Queue zu, die Sie unter *Queue-Name* auswählen.
	Von Port	Benutzter Port bei der Quelle, von wo die Daten kommen (wird nur ausgewertet bei den Protokollen TCP und UDP). – **any** bezeichnet jeden beliebigen Port. – **startport:endport** (z. B. 110:120) bezeichnet einen Portbereich. Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben: (z. B. 110 für pop3 oder pop3 für 110).
	Nach IP	IP-Adresse des Netzes/Geräts, wohin die Daten gehen. Angabe entsprechend wie oben unter *Von IP*.
	Nach Port	Benutzter Port bei der Quelle, wohin die Daten gehen. Angabe entsprechend wie oben unter *Von Port.*

Menü QoS >> Egress-Zuordnungen >> Intern / Extern / Extern 2 / Einwahl Menü QoS >> Egress-Zuordnungen (VPN) >> PN via Intern/VPN via Extern/VPN via Extern 2/VPN via		
	Aktueller TOS/DSCP-Wert	Jedes Datenpaket enthält ein TOS bzw. DSCP Feld. (TOS steht für Type Of Service, DSCP für Differentiated Services Code Point.) Hier wird angegeben, zu welcher Art von Traffic das Datenpaket gehört. So wird z. B. ein IP-Telefon in dieses Feld der von ihm ausgehenden Datenpakete etwas anderes hineinschreiben als ein FTP-Programm, das Datenpakete auf einen Server hochlädt. Wenn Sie hier einen Wert auswählen, werden nur die Datenpakete genommen, die in ihrem TOS-bzw. DSCP-Feld diesen Wert haben, um sie - je nach Eintrag im Feld **Neuer TOS/DSCP-Wert** - auf einen anderen Wert zu setzen.
	Neuer TOS/DSCP-Wert	Wenn Sie den TOS/DSCP-Wert der Datenpakete ändern wollen, die anhand der gegebenen Regeln selektiert sind, wählen Sie hier aus, was ins TOS- bzw. DSCP-Feld geschrieben werden soll. Weitere Erläuterungen zu **Aktueller TOS/DSCP-Wert** und **Neuer TOS/DSCP-Wert** finden Sie in folgenden RFC-Dokumenten – RFC3260 „New Terminology and Clarifications for Diffserv“ – RFC3168 „The Addition of Explicit Congestion Notification (ECN) to IP“ – RFC2474 „Definition of the Differentiated Services Field (DS Field)“ – RFC1349 „Type of Service in the Internet Protocol Suite“
	Queue-Name	Name der Egress-Queue, welcher der Traffic zugeordnet werden soll.
	Kommentar	Optional: kommentierender Text.

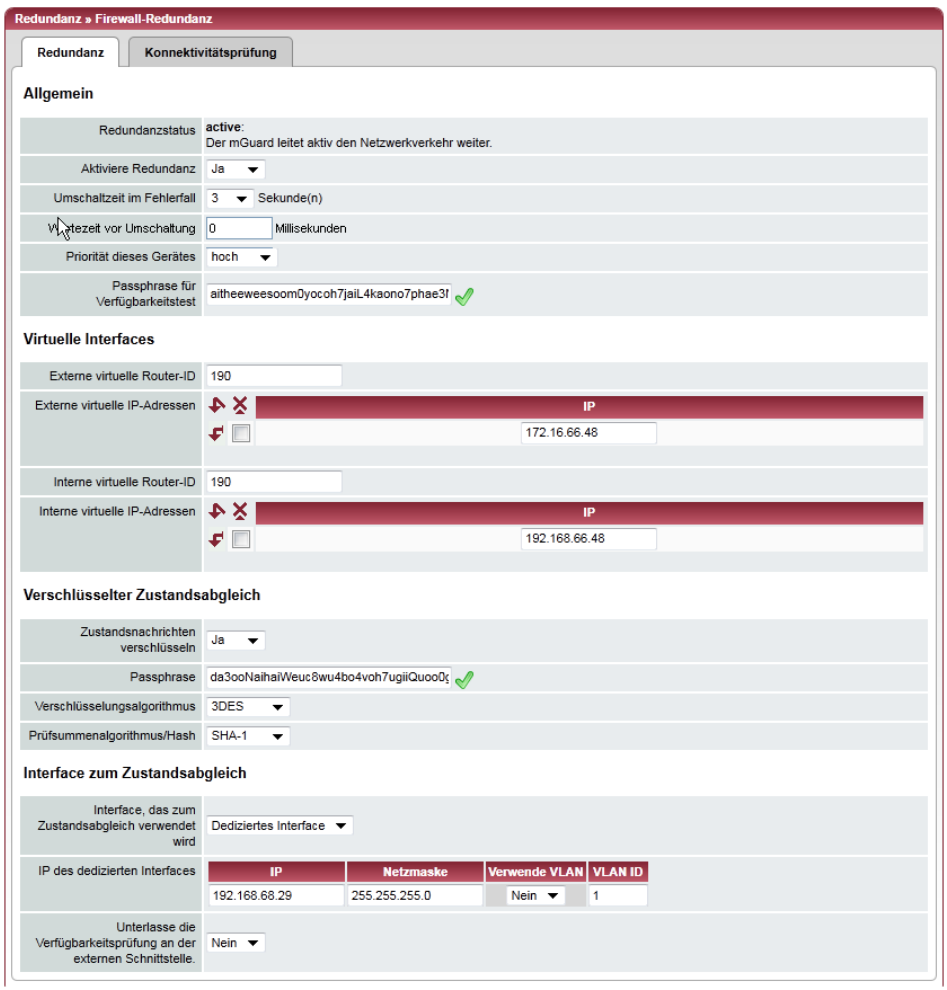
6.11 Redundanz

Eine ausführliche Darstellung zum Thema Redundanz finden Sie in Kapitel 7, „Redundanz“.

6.11.1 Redundanz >> Firewall-Redundanz

Dieses Menü steht **nicht** auf dem **mGuard rs2000** zur Verfügung.

6.11.1.1 Redundanz



Redundanz >> Firewall-Redundanz >> Redundanz		
Allgemein	**Redundanzstatus**	Zeigt den aktuellen Status an.
	Aktiviere Redundanz	**Nein** (Standard): Die Firewall-Redundanz ist ausgeschaltet. **Ja**: Die Firewall-Redundanz ist aktiviert. Sie können diese Funktion nur aktivieren, wenn ein passender Lizenzschlüssel installiert ist. Wenn Sie gleichzeitig die VPN-Redundanz aktivieren wollen, gelten weitere Bedingungen, siehe „VPN-Redundanz“ auf Seite 7-15.
	Umschaltzeit im Fehlerfall	Zeit, die im Fehlerfall maximal verstreichen darf, bevor auf den anderen mGuard gewechselt wird.
	Wartezeit vor Umschaltung	**0 ... 10 000 Millisekunden, Standard: 0** Zeitdauer, in der ein Fehler vom Redundanz-System ignoriert wird. Ein Fehler wird von der Konnektivitäts- und der Verfügbarkeitsprüfung ignoriert, bis er länger als die hier eingestellte Zeit andauert.
	Priorität dieses Gerätes	**hoch/niedrig** Definiert die Priorität, die mit den Anwesenheitsnachrichten (CARP) verbunden ist. Setzen Sie bei dem mGuard, der aktiv sein soll, die Priorität **hoch**. Der mGuard in Bereitschaft bekommt die Priorität **niedrig**. Beide mGuards eines Redundanzpaares dürfen entweder eine unterschiedliche Priorität oder die Priorität **hoch** haben. . Setzen Sie niemals **beide** mGuards eines Redundanzpaares auf die Priorität **niedrig**.

Redundanz >> Firewall-Redundanz >> Redundanz

Passphrase für Verfügbarkeitstest

Bei einem mGuard, der Teil eines Redundanzpaares ist, wird kontinuierlich geprüft, ob ein aktiver mGuard vorhanden ist und ob dieser aktiv bleiben soll. Dafür wird eine Variante des CARP (Common Address Redundancy Protocol) verwendet.

CARP nutzt die SHA-1 HMAC-Verschlüsselung in Verbindung mit einem Passwort. Dieses Passwort muss für beide mGuards gleich eingestellt sein. Er wird niemals im Klartext übertragen, sondern zur Verschlüsselung genutzt.

Das Passwort ist wichtig für die Sicherheit, da der mGuard an dieser Stelle angreifbar ist. Wir empfehlen, ein Passwort mit mindestens 20 Zeichen und vielen Sonderzeichen zu verwenden (druckbare UTF-8-Zeichen). Es muss regelmäßig erneuert werden.

Gehen Sie so vor, um das Passwort zu ändern:

Prüfen Sie, welchen Status das eingestellte Passwort hat, bevor Sie ein neues eintragen.

Nur wenn Sie einen **grünen Haken** rechts neben dem Eingabefeld sehen, ist ein gültiges Passwort vorhanden und Sie dürfen ein neues Passwort eintragen.

Stellen Sie das neue Passwort an beiden mGuards ein. Die Reihenfolge ist egal, aber das Passwort muss bei beiden gleich sein. Wenn Sie versehentlich ein abweichendes Passwort eingetragen haben, folgen Sie den Anweisungen unter „Vorgehensweise bei einem falschem Passwort“ auf Seite 6-240.

Sobald ein Redundanzpaar ein neues Passwort erhalten hat, handelt es selbst aus, wann es unterbrechungsfrei zum neuen Passwort wechseln kann.

Der Status wird über Symbole angezeigt. Wir empfehlen, diesen Status aus Sicherheitsgründen zu beobachten.

Ein **rotes Kreuz** zeigt an, dass der mGuard ein neues Passwort hat, dass er nutzen möchte. Aber das alte Passwort ist weiterhin in Gebrauch.

Ein **gelber Haken** zeigt, dass bereits das neue Passwort genutzt, aber das alte noch akzeptiert wird, für den Fall, dass der andere mGuard es noch verwendet.

Wenn **kein Symbol** vorhanden ist, wird kein Passwort genutzt. Zum Beispiel, weil die Redundanz nicht aktiviert ist oder die Firmware bootet.

Wenn ein mGuard während des Passwort-Wechsels ausfällt, gibt es diese Fälle:

– Die Passwort-Erneuerung wurde an allen mGuards gestartet und dann unterbrochen, z. B. durch einen Netzwerk-Fehler. Dieser Fall wird automatisch behoben.

– Die Passwort-Erneuerung wurde an allen mGuards gestartet. Aber dann fällt ein mGuard aus und muss ausgetauscht werden.

  Stellen Sie am verbleibenden mGuard fest, ob der Passwort-Wechsel schon vollzogen worden ist. Wenn Sie ein grünes Häkchen sehen, müssen Sie am zu ersetzenden mGuard das neue Passwort direkt einstellen.

  Wenn Sie kein grünes Häkchen sehen, dann hat noch kein Passwort-Wechsel am verbleibenden mGuard stattgefunden. Dann müssen Sie auf dem mGuard, der noch in Betrieb ist, das Passwort noch einmal ändern. Warten Sie bis, das grüne Häkchen erscheint. Ersetzen Sie erst dann den ausgefallenen mGuard. Konfigurieren Sie den Ersatz-mGuard sofort beim Einrichten der Redundanz mit dem neuen Passwort.

– Die Passwort-Erneuerung wurde gestartet, aber nicht an allen mGuards, weil diese ausgefallen sind. Sobald ein fehlerhafter mGuard wieder online ist, muss die Passwort-Erneuerung gestartet werden. Bei einem ausgetauschten mGuard muss dieser zunächst mit dem alten Passwort konfiguriert werden, bevor er angeschlossen wird.

Vorgehensweise bei einem falschem Passwort

Wenn Sie versehentlich bei einem mGuard ein falsches Passwort eingegeben haben, dann dürfen Sie es nicht einfach noch einmal korrekt eingeben. Unter ungünstigen Umständen sind ansonsten danach beide mGuards aktiv.

Wenn Sie das alte Passwort noch kennen, gehen Sie so vor:

- Rekonfigurieren Sie den mGuard, bei dem das falsche Passwort eingetragen wurde, noch einmal mit dem alten Passwort.
- Warten Sie bis der mGuard anzeigt, dass das alte Passwort benutzt wird.
- Tragen Sie dann das richtige Passwort ein.

Wenn Sie das alte Passwort nicht mehr kennen, gehen Sie so vor:

- Prüfen Sie, ob Sie das alte Passwort beim anderen mGuard auslesen können.
- Wenn der andere mGuard ausgeschaltet ist oder fehlt, dann können Sie bei dem aktiven mGuard, dem sie versehentlich das falsche Passwort eingestellt haben, einfach das korrekte neue Passwort eintragen. Sorgen Sie dafür, dass der andere mGuard das gleiche Passwort erhält, bevor er wieder in Betrieb geht.
- Wenn der andere mGuard das neue Passwort bereits verwendet, dann müssen Sie sicherstellen, dass der mGuard mit dem falschen Passwort nicht aktiv ist oder wird, z. B. durch das Herausziehen des Kabels an der LAN- oder WAN-Schnittstelle.

  Bei einem Fernzugriff können Sie für die Konnektivitätsprüfung ein Ziel eintragen, das nicht reagieren wird. Bevor Sie einen solchen Fehler provozieren, prüfen Sie, dass bei keinem der mGuards ein Fehler bei der Redundanz vorliegt. Ein mGuard muss aktiv und der andere in Bereitschaft sein. Gegebenenfalls müssen Sie angezeigte Fehler beheben und dann erst die Methode verwenden. Dann führen Sie die folgenden Schritte aus:
  – Ersetzen Sie das falsche Passwort durch ein anderes.
  – Geben Sie dieses Passwort auch beim aktiven mGuard ein.
  – Nehmen Sie den nicht aktiven mGuard wieder in Betrieb. Stecken Sie zum Beispiel das Ethernet-Kabel wieder ein oder stellen Sie die alten Einstellungen für die Konnektivitätsprüfung wieder her.

Redundanz >> Firewall-Redundanz >> Redundanz		
Virtuelle Interfaces	**Externe virtuelle Router-ID**	**1, 2, 3, ... 255 (Default: 51)** Nur im Netzwerk-Modus Router Diese ID wird vom Redundanzpaar bei jeder Anwesenheitsnachricht (CARP) über das externe Interface mitgesendet und dient der Identifizierung des Redundanzpaares. Diese ID muss für beide mGuards gleich sein. Sie ist notwendig, um das Redundanzpaar von anderen Redundanzpaaren zu unterscheiden, die über ihr externes Interface mit demselben Ethernet-Segment verbunden sind. Beachten Sie dabei, dass CARP dasselbe Protokoll und denselben Port wie VRRR (Virtuell Router Redundancy Protokoll) nutzt. Die hier eingestellte ID muss sich unterscheiden von den IDs der Geräte, die VRRR oder CARP nutzen und sich im selben Ethernet-Segment befinden.
	Externe virtuelle IP-Adressen	Default: 10.0.0.100 Nur im Netzwerk-Modus Router IP-Adressen, die von beiden mGuards als virtuelle IP-Adresse des externen Interfaces geteilt wird. Diese IP-Adressen müssen für beide mGuards gleich sein. Diese Adressen werden als Gateway für explizite statische Routen von Geräten genutzt, die sich im selben Ethernet-Segment wie das externe Netzwerk-Interface des mGuards befinden. Der aktive mGuard kann auf dieser IP-Adresse ICMP-Anfragen erhalten. Er reagiert auf diese ICMP-Anfragen wie es im Menü unter *Netzwerksicherheit >> Paketfilter >> Erweiterte Einstellungen* eingestellt ist. Für die virtuelle IP-Adressen werden keine Netzwerkmaske oder VLAN ID eingerichtet, da diese Attribute von der realen externen IP-Adresse bestimmt werden. Zu jeder virtuellen IP-Adresse muss eine reale IP-Adresse konfiguriert sein, in deren IP-Netz die virtuelle Adresse passt. Der mGuard überträgt die Netzwerkmaske und die VLAN-Einstellung von der realen externen IP-Adresse auf die entsprechende virtuelle IP-Adresse. Die übernommenen VLAN-Einstellungen bestimmen, ob Standard-MTU-Einstellungen oder VLAN-MTU-Einstellungen für die virtuelle IP-Adresse genutzt werden.  Wenn keine reale IP-Adresse und Netzwerkmaske vorhanden sind, kann die Firewall-Redundanz nicht richtig arbeiten.

Redundanz >> Firewall-Redundanz >> Redundanz		
	Interne virtuelle Router-ID	**1, 2, 3, ... 255 (Default: 51)** Nur im Netzwerk-Modus Router Diese ID wird vom Redundanzpaar bei jeder Anwesenheitsnachricht (CARP) über das externe und interne Interface mitgesendet und dient der Identifizierung des Redundanzpaares. Diese ID muss für beide mGuards gleich eingestellt sein. Sie ist notwendig, um das Redundanzpaares von anderen Ethernet-Teilnehmern zu unterscheiden, die über ihr externes/internes Interface mit demselben Ethernet-Segment verbunden sind. Beachten Sie dabei, dass CARP dasselbe Protokoll und denselben Port wie VRRR (Virtuell Router Redundancy Protokoll) nutzt. Die hier eingestellte ID muss sich unterscheiden von den IDs der Geräte, die VRRR oder CARP nutzen und sich im selben Ethernet-Segment befinden.
	Interne virtuelle IP-Adressen	Wie unter *Externe virtuelle IP-Adressen* beschrieben, aber mit zwei Ausnahmen Unter **Interne virtuelle IP-Adresse** werden IP-Adressen definiert für Geräte, die zum internen Ethernet-Segment gehören. Diese Geräte müssen die IP-Adresse als ihr Standard-Gateway nutzen. Sie können diese Adresse als DNS- oder NTP-Server nutzen, wenn der mGuard als Server für die Protokolle konfiguiert ist. Zu jeder virtuellen IP-Adresse muss eine reale IP-Adresse konfiguriert sein, in deren IP-Netz die virtuelle Adresse passt. Die Reaktion auf ICMP-Anfragen bei internen virtuellen IP-Adressen ist unabhängig von den Einstellungen unter *Netzwerksicherheit >> Paketfilter >> Erweiterte Einstellungen .*
Verschlüsselter Zustandsabgleich	**Zustandsnachrichten verschlüsseln**	**Ja/Nein** Bei **Ja** wird der Zustandsabgleich verschlüsselt.
	Passphrase	Das Passwort wird so gewechselt, wie es unter „Passphrase für Verfügbarkeitstest“ auf Seite 6-239 beschrieben ist. Nur wenn versehentlich ein falsches Passwort eingegeben wurde, gibt es ein Abweichung von der verschriebenen Vorgehensweise.

Redundanz >> Firewall-Redundanz >> Redundanz

Vorgehensweise bei einem falschen Passwort

Wenn Sie versehentlich bei einem mGuard ein falsches Passwort eingegeben haben, dann dürfen Sie es nicht einfach noch einmal korrekt eingeben. Unter ungünstigen Umständen sind ansonsten danach beide mGuards aktiv.

Fall 1: Nur ein mGuard hat ein falsches Passwort. Beim anderen mGuard wurde mit dem Passworttausch noch gar nicht begonnen.

- Rekonfigurieren Sie den mGuard, bei dem das falsche Passwort eingetragen wurde, noch einmal mit dem alten Passwort.
- Warten Sie bis der mGuard anzeigt, dass das alte Passwort benutzt wird.
- Tragen Sie dann das richtige Passwort ein.

Fall 2: Der andere mGuard nutzt bereits das neue Passwort.

- Beide mGuards müssen in dem Status sein, dass sie ein altes Passwort nutzen aber ein neues erwarten (rotes Kreuz). Damit es dazu kommt, tragen Sie nacheinander zufällige Passwörter ein.
- Zum Schluss generieren Sie ein sicheres Passwort und tragen es in beiden mGuards ein. Dieses Passwort wird sofort ohne Abstimmung genutzt.

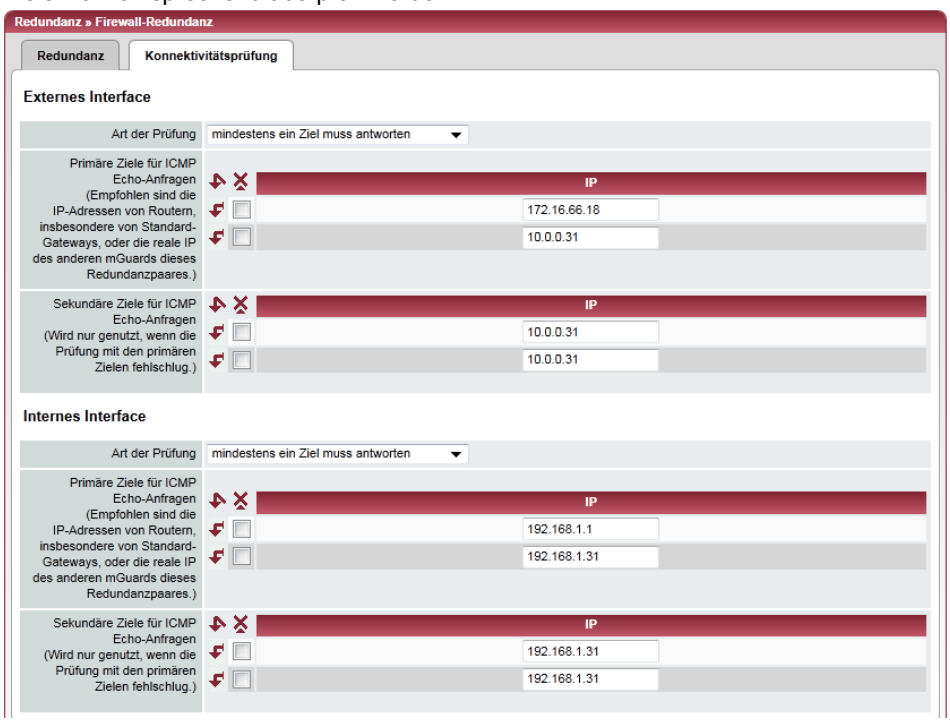
Der mGuard in Bereitschaft kann bei diesem Vorgang für kurze Zeit im Zustand „outdated“ sein, aber das behebt sich automatisch wieder.

	Verschlüsselungsalgorithmus	**DES, 3DES, AES-128, AES-192, AES-256** Siehe „Algorithmen“ auf Seite 6-214.
	Prüfsummenalgorithmus/Hash	**MD5, SH1, SHA-256, SHA-512** Siehe „Algorithmen“ auf Seite 6-214.
Interface zum Zustandsabgleich	**Interface, das zum Zustandsabgleich verwendet wird**	**Internes Interface/Dediziertes Interface** Der **mGuard centerport** unterstützt ein **dediziertes Interface**. Das ist eine reservierte direkte Ethernet-Schnittstelle oder ein dediziertes LAN-Segment, über das der Zustandsabgleich gesendet wird. Das Redundanzpaar kann über ein zusätzliches dediziertes Ethernet-Interface verbunden sein oder über einen dazwischen geschalteten Switch. Bei **Dediziertes Interface** wird an dem dritten Ethernet-Interface ebenfalls auf Anwesenheitsnachrichten (CARP) gelauscht. Wenn der mGuard aktiv ist, werden auch Anwesenheitsnachrichten (CARP) gesendet. Für dieses Interface wird aber kein zusätzliches Routing unterstützt. Aus Sicherheitsgründen werden Frames, die an dieser Schnittstelle empfangen werden, nicht weitergeleitet. Über das SNMP kann der Verbindungsstatus des dritten Ethernet-Interface abgefragt werden.

Redundanz >> Firewall-Redundanz >> Redundanz		
	IP des dedizierten Interfaces	Nur wenn **Dediziertes Interface** ausgewählt ist. **IP** IP-Adresse, die der mGuard centerport an seinem dritten Netzwerk-Interface für den Zustandsabgleich mit dem anderen mGuard nutzt. Default: 192.168.68.29 **Netzmaske** Netzwerkmaske, die der mGuard centerport an seinem dritten Netzwerk-Interface für den Zustandsabgleich mit dem anderen mGuard nutzt. Default: 255.255.255.0 **Verwendete VLAN** Bei **Ja** wird eine VLAN-ID für das dritte Netzwerk-Interface genutzt. **VLAN ID** 1, 2, 3, ... 4094 (Default: 1) VLAN-ID, wenn diese Einstellung aktiviert ist.
	Unterlasse die Verfügbarkeitsprüfung der externen Schnittstelle	Nur wenn **Dediziertes Interface** ausgewählt ist. Bei **Ja** werden an dem externen Interface keine Anwesenheitsnachrichten (CARP) gesendet und empfangen. Das macht für einige Szenarien Sinn, um Angreifer von außen abzuwehren.

6.11.1.2 Konnektivitätsprüfung

Bei der Konnektivitätsprüfung können Ziele für das interne und externe Interface konfiguriert werden. Es ist wichtig, dass diese Ziele tatsächlich an dem angegebenen Interface angeschlossen sind. Ein ICMP-Echo-Reply kann nicht von einem externen Interface empfangen werden, wenn das zugehörige Ziel am internen Interface angeschlossen ist (und umgekehrt). Bei einem Wechsel der statischen Routen kann es leicht passieren, dass die Ziele nicht entsprechend überprüft werden.

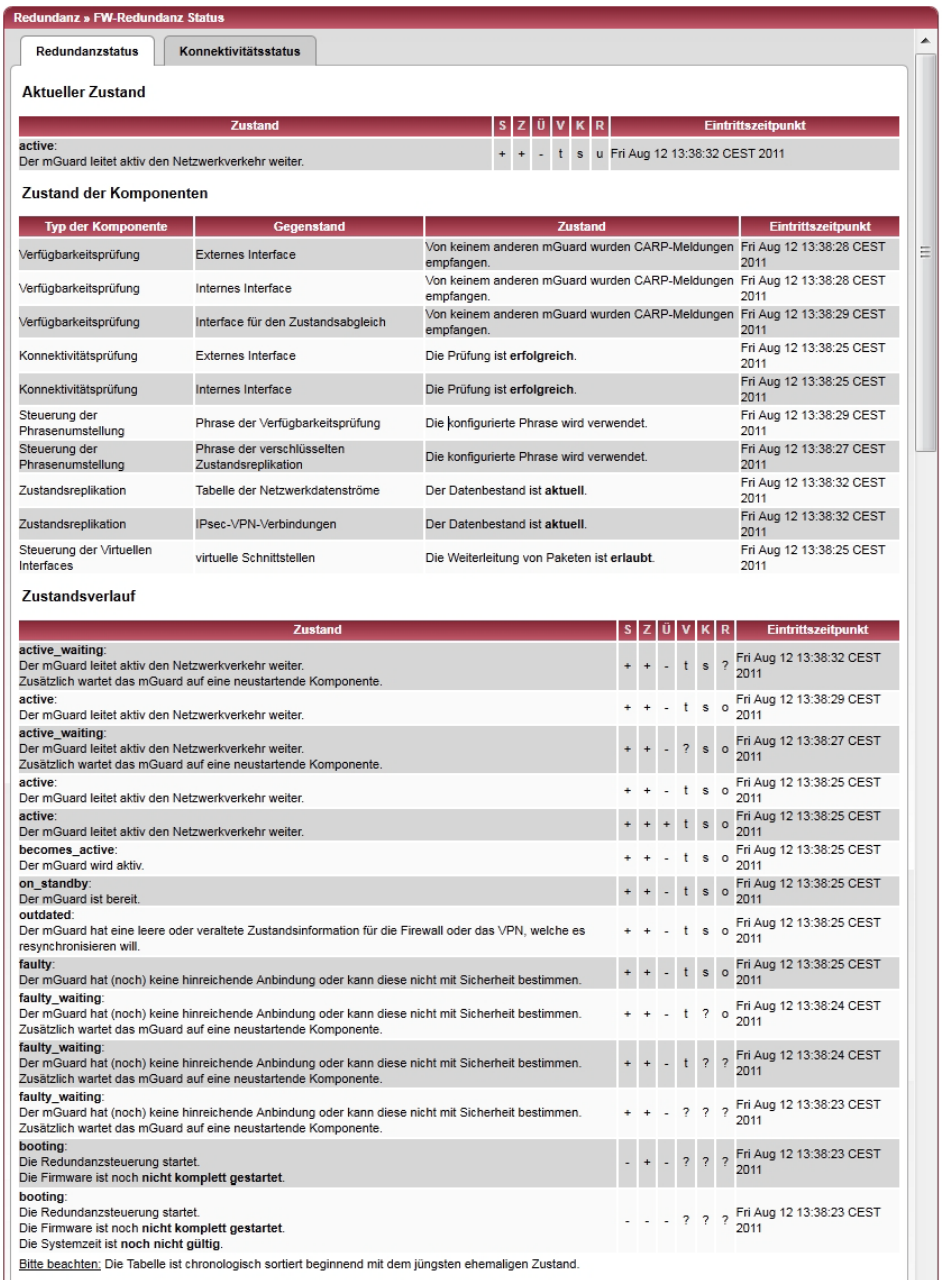


Redundanz >> Firewall-Redundanz >> Konnektivitätsprüfung		
Externes Interface	**Art der Prüfung**	Legt fest, ob und wie bei dem externen Interface eine Konnektivitätsprüfung durchgeführt wird. Wenn **Mindestens ein Ziel muss antworten** ausgewählt ist, dann ist es egal, ob der ICMP-Echo-Request von dem primären oder sekundären Ziel beantwortet wird. Die Anfrage wird nur an das sekundäre Ziel geschickt, wenn das primäre nicht zufriedenstellend geantwortet hat. Auf diese Weise können Konfigurationen unterstützt werden, bei denen die Geräte nur bei Bedarf mit ICMP-Echo-Requests ausgestattet sind. Bei **Alle Ziele einer Menge müssen antworten** müssen beide Ziele antworten. Wenn kein sekundäres Ziel angegeben ist, muss nur das primäre antworten. Bei **Nur Prüfung des Ethernet-Links** wird nur der Verbindungsstatus der Ethernet-Verbindung geprüft.

Redundanz >> Firewall-Redundanz >> Konnektivitätsprüfung		
	Primäre Ziele für ICMP Echo-Anfragen	Unsortierte Liste von IP-Adressen, die als Ziele für die ICMP-Echo-Requests genutzt werden. Wir empfehlen, die IP-Adressen von Routern zu verwenden, insbesondere die IP-Adressen von Standard-Gateways oder die reale IP-Adresse des anderen mGuards. Default: 10.0.0.30, 10.0.0.31 (für neue Adressen) Jeder Satz von Zielen für den Zustandsabgleich kann maximal zehn Ziele beinhalten.
	Sekundäre Ziele für ICMP Echo-Anfragen	siehe oben Wir nur genutzt, wenn die Prüfung der primären Ziele fehlgeschlagen ist. Ein Ausfall eines sekundären Ziels wird im normalen Betrieb nicht entdeckt. Default: 10.0.0.30, für neue Adressen 10.0.0.31 Jeder Satz von Zielen für den Zustandsabgleich kann maximal zehn Ziele beinhalten.
Internes Interface	**Art der Prüfung**	Legt fest, ob und wie bei dem internen Interface eine Konnektivitätsprüfung durchgeführt wird. Die Einstellungen sind gleichbedeutend mit dem des externen Interfaces.
	Primäre Ziele für ICMP Echo-Anfragen	siehe oben Voreingestellt: 192.168.1.30, für neue Adressen 192.168.1.31
	Sekundäre Ziele für ICMP Echo-Anfragen	siehe oben Voreingestellt: 192.168.1.30, für neue Adressen 192.168.1.31

6.11.2 Redundanz >> Firewall-Redundanz Status

6.11.2.1 Redundanzstatus



Redundanz » FW-Redundanz Status

Redundanzstatus | Konnektivitätsstatus

Aktueller Zustand

Zustand	S	Z	Ü	V	K	R	Eintrittszeitpunkt
active: Der mGuard leitet aktiv den Netzwerkverkehr weiter.	+	+	-	t	s	u	Fri Aug 12 13:38:32 CEST 2011

Zustand der Komponenten

Typ der Komponente	Gegenstand	Zustand	Eintrittszeitpunkt
Verfügbarkeitsprüfung	Externes Interface	Von keinem anderen mGuard wurden CARP-Meldungen empfangen.	Fri Aug 12 13:38:28 CEST 2011
Verfügbarkeitsprüfung	Internes Interface	Von keinem anderen mGuard wurden CARP-Meldungen empfangen.	Fri Aug 12 13:38:28 CEST 2011
Verfügbarkeitsprüfung	Interface für den Zustandsabgleich	Von keinem anderen mGuard wurden CARP-Meldungen empfangen.	Fri Aug 12 13:38:29 CEST 2011
Konnektivitätsprüfung	Externes Interface	Die Prüfung ist **erfolgreich**.	Fri Aug 12 13:38:25 CEST 2011
Konnektivitätsprüfung	Internes Interface	Die Prüfung ist **erfolgreich**.	Fri Aug 12 13:38:25 CEST 2011
Steuerung der Phrasenumstellung	Phrase der Verfügbarkeitsprüfung	Die konfigurierte Phrase wird verwendet.	Fri Aug 12 13:38:29 CEST 2011
Steuerung der Phrasenumstellung	Phrase der verschlüsselten Zustandsreplikation	Die konfigurierte Phrase wird verwendet.	Fri Aug 12 13:38:27 CEST 2011
Zustandsreplikation	Tabelle der Netzwerkdatenströme	Der Datenbestand ist **aktuell**.	Fri Aug 12 13:38:32 CEST 2011
Zustandsreplikation	IPsec-VPN-Verbindungen	Der Datenbestand ist **aktuell**.	Fri Aug 12 13:38:32 CEST 2011
Steuerung der Virtuellen Interfaces	virtuelle Schnittstellen	Die Weiterleitung von Paketen ist **erlaubt**.	Fri Aug 12 13:38:25 CEST 2011

Zustandsverlauf

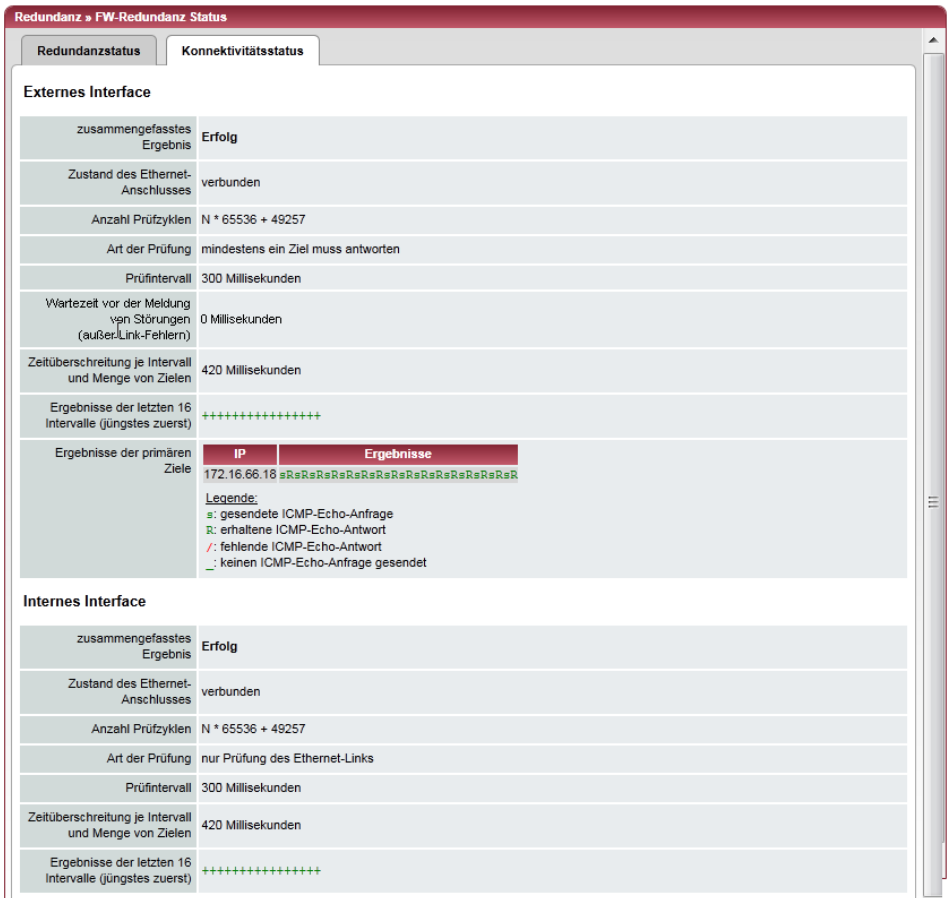
Zustand	S	Z	Ü	V	K	R	Eintrittszeitpunkt
active_waiting: Der mGuard leitet aktiv den Netzwerkverkehr weiter. Zusätzlich wartet das mGuard auf eine neustartende Komponente.	+	+	-	t	s	?	Fri Aug 12 13:38:32 CEST 2011
active: Der mGuard leitet aktiv den Netzwerkverkehr weiter.	+	+	-	t	s	o	Fri Aug 12 13:38:29 CEST 2011
active_waiting: Der mGuard leitet aktiv den Netzwerkverkehr weiter. Zusätzlich wartet das mGuard auf eine neustartende Komponente.	+	+	-	?	s	o	Fri Aug 12 13:38:27 CEST 2011
active: Der mGuard leitet aktiv den Netzwerkverkehr weiter.	+	+	-	t	s	o	Fri Aug 12 13:38:25 CEST 2011
active: Der mGuard leitet aktiv den Netzwerkverkehr weiter.	+	+	+	t	s	o	Fri Aug 12 13:38:25 CEST 2011
becomes_active: Der mGuard wird aktiv.	+	+	-	t	s	o	Fri Aug 12 13:38:25 CEST 2011
on_standby: Der mGuard ist bereit.	+	+	-	t	s	o	Fri Aug 12 13:38:25 CEST 2011
outdated: Der mGuard hat eine leere oder veraltete Zustandsinformation für die Firewall oder das VPN, welche es resynchronisieren will.	+	+	-	t	s	o	Fri Aug 12 13:38:25 CEST 2011
faulty: Der mGuard hat (noch) keine hinreichende Anbindung oder kann diese nicht mit Sicherheit bestimmen.	+	+	-	t	s	o	Fri Aug 12 13:38:25 CEST 2011
faulty_waiting: Der mGuard hat (noch) keine hinreichende Anbindung oder kann diese nicht mit Sicherheit bestimmen. Zusätzlich wartet das mGuard auf eine neustartende Komponente.	+	+	-	t	?	o	Fri Aug 12 13:38:24 CEST 2011
faulty_waiting: Der mGuard hat (noch) keine hinreichende Anbindung oder kann diese nicht mit Sicherheit bestimmen. Zusätzlich wartet das mGuard auf eine neustartende Komponente.	+	+	-	t	?	?	Fri Aug 12 13:38:24 CEST 2011
faulty_waiting: Der mGuard hat (noch) keine hinreichende Anbindung oder kann diese nicht mit Sicherheit bestimmen. Zusätzlich wartet das mGuard auf eine neustartende Komponente.	+	+	-	?	?	?	Fri Aug 12 13:38:23 CEST 2011
booting: Die Redundanzsteuerung startet. Die Firmware ist noch **nicht komplett gestartet**.	-	+	-	?	?	?	Fri Aug 12 13:38:23 CEST 2011
booting: Die Redundanzsteuerung startet. Die Firmware ist noch **nicht komplett gestartet**. Die Systemzeit ist **noch nicht gültig**.	-	-	-	?	?	?	Fri Aug 12 13:38:23 CEST 2011

Bitte beachten: Die Tabelle ist chronologisch sortiert beginnend mit dem jüngsten ehemaligen Zustand.

Redundanz >> Firewall-Redundanz Status >> Redundanzstatus		
Aktueller Zustand		Mögliche Zustände sind: *booting*: Der mGuard startet. *faulty*: Der mGuard hat (noch) keine ausreichende Verbindung. *outdated*: Der Zustandsabgleich der Datenbanken ist (noch) nicht aktuell. *on_standby*: Der mGuard ist bereit, aktiv zu werden, wenn der andere mGuard ausfällt. *becomes_active*: Der mGuard ist dabei aktiv zu werden, da der andere mGuard augefallen ist. *active*: Der mGuard ist aktiv. *becomes_standby*: Der mGuard wechselt aus dem aktiven Zustand in den Bereitschaftszustand. (Der Wechsel erfolgt zum Zustand *outdated*, da die Status-Datenbank zuerst aktualisiert wird.)
Zustand der Komponenten	**Verfügbarkeitsprüfung**	Bezieht sich auf den Status der Verfügbarkeitsprüfung für das interne bzw. externe Interface. Es gibt drei Ergebnisse der Verfügbarkeitsprüfung. – Von keinem anderen mGuard wurden Anwesenheitsnachrichten (CARP) empfangen. – Es gibt einen anderen mGuard, der aktiv werden oder bleiben soll. – Es gibt einen anderen mGuard, der aktiv ist aber on_standby werden soll.
	Konnektivitätsprüfung	Stellt dar, ob das Ergebnis der Prüfung erfolgreich war. Jedes Interface wird getrennt geprüft.
	Zustandsrepliken	Beim Zustandsabgleich werden verschiedene Datenbestände geprüft, ob sie aktuell ist. Bei einem Redundanzpaar ist nur ein Datenbestand aktiv, der andere ist in Bereitschaft. Ein Wechsel dieses Zustandes wird ebenfalls angezeigt. – **Tabelle der Netzwerkdatenströme** meint die Firewall-Status-Datenbank – **IPsec-VPN-Verbindungen** (bei aktivierter VPN-Redundanz)
	Steuerung der Virtuellen Interfaces	Alle virtuellen Schnittstellen werden gemeinsam darauf hin kontrolliert, ob die Weiterleitung von Paketen erlaubt ist.

Redundanz >> Firewall-Redundanz Status >> Redundanzstatus				
Zustandsverlauf			Die Tabelle beginnt mit dem jüngsten Zustand.	
			Die Abkürzungen bedeuten:	
	S	**Status der Firmware**	**+**	Firmware vollständig gestartet.
			-	Firmware noch nicht vollständig gestartet.
	Z	**Systemzeit**	**+**	Gültige Systemzeit
			-	Keine gültige Systemzeit
	Ü	**Timeout des vorherigen Zustandes**	**+**	Timeout
			-	Kein Timeout
	V	**Verfügbarkeitsprüfung**	**?**	Zustand unbekannt
			s	Es ist ein anderer mGuard vorhanden. Dieser mGuard ist aktiv (oder wird es gerade).
			f	Es ist ein anderer mGuard vorhanden. Dieser mGuard ist in Bereitschaft (oder wechselt dorthin).
			t	Kein anderer mGuard vorhanden.
	K	**Konnektivitätsprüfung**	**?**	Zustand unbekannt
			s	Prüfung aller Komponenten war erfolgreich
			f	Prüfung mindestens einer Komponente ist fehlgeschlagen
	R	**Zustandsabgleich**	**?**	Zustand unbekannt
			u	Datenbestand ist aktuell
			o	Datenbestand ist veraltet
			-	Datenbestand wechselt in den Zustand „in Bereitschaft“
			+	Datenbestand wechselt in den Zustand „aktiv“

6.11.2.2 Konnektivitätsstatus



Redundanz >> Firewall-Redundanz Status >> Konnektivitätsstatus		
Externes Interface	**Zusammengefasstes Ergebnis**	**Erfolg/Fehler** Ergebnis der Konnektivitätsprüfung für das externe Interface Der Ergebnis **Fehler** wird auch angezeigt, solange die Konnektivitätsprüfung noch kein bestimmtes Ergebnis hat. Für das zusammengefasste Ergebnis werden die letzten beiden Intervalle der Konnektivitätsprüfung berücksichtigt. Nur wenn beide erfolgreich waren, wird **Erfolg** angezeigt. **Erfolg (wg. Wartezeit verlängert)** wird angezeigt, wenn ein Fehler kürzer bestanden hat, als unter *„Wartezeit vor Umschaltung“* im Menü *Redundanz >> Firewall-Redundanz >> Redundanz* eingestellt worden ist.
	Zustand des Ethernet-Anschlusses	Zeigt, ob der Ethernet-Anschluss verbunden ist.
	Anzahl Prüfzyklen	Anzahl der abgeschlossenen Prüfintervalle. Wenn der Zähler überläuft, wird vor die Anzahl eine Meldung gestellt.
	Art der Prüfung	Wiederholt die Einstellung für die Konnektivitätsprüfung (siehe *Art der Prüfung* auf Seite 6-245).

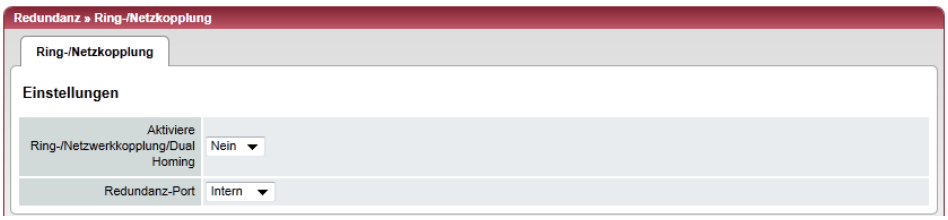
Redundanz >> Firewall-Redundanz Status >> Konnektivitätsstatus		
	Prüfintervall	Zeigt die Zeit in Millisekunden an, die zwischen den Starts der Prüfungen liegt. Dieser Wert wird aus der eingestellten Failover-Umschaltzeit berechnet.
	Zeitüberschreitung je Intervall und Menge von Zielen	Zeigt die Zeit in Millisekunden an, nach denen ein Ziel als unbeantwortet eingestuft wird, wenn es auf dem ICMP-Echo-Request nicht geantwortet hat. Dieser Wert wird aus der eingestellten Failover-Umschaltzeit berechnet.
	Wartezeit vor der Meldung von Störungen (außer Link-Fehlern)	Zeitdauer, in der ein Fehler vom Redundanz-System ignoriert wird. Ein Fehler wird von der Konnektivitäts- und der Verfügbarkeitsprüfung ignoriert, bis er länger als die hier eingestellte Zeit andauert. Dieser Wert wird unter *„Wartezeit vor Umschaltung“* im Menü *Redundanz >> Firewall-Redundanz >> Redundanz* eingestellt.
	Ergebnisse der letzten 16 Intervalle (jüngstes zuerst)	Ein grünes Plus steht für jede erfolgreiche Prüfung. Wenn eine Prüfung fehlgeschlagen ist, steht ein rotes Minus.
	Ergebnisse der primären Ziele	Nur sichtbar, wenn ein primäres Ziel eingestellt ist (siehe *Primäre Ziele für ICMP Echo-Anfragen* auf Seite 6-245). Zeigt in zeitlicher Reihenfolge die Ergebnisse der ICMP-Echo-Requests. Das letzte Ergebnis steht vorne. „sR“ steht für einen Zyklus mit korrekt gesendeten und erhaltenen ICMP-Echo-Requests. Bei fehlenden Antworten steht ein „/“ und bei nicht gesendeten Anfragen ein „_“.
	Ergebnisse der sekundären Ziele	Nur sichtbar, wenn ein sekundäres Ziel eingestellt ist (siehe *Sekundäre Ziele für ICMP Echo-Anfragen* auf Seite 6-245).
Internes Interface	**Zusammengefasstes Ergebnis**	Siehe *Externes Interface*
	Zustand des Ethernet-Anschlusses	Siehe *Externes Interface*
	Anzahl Prüfzyklen	Siehe *Externes Interface*
	Prüfintervall	Siehe *Externes Interface*
	Zeitüberschreitung je Intervall und Menge von Zielen	Siehe *Externes Interface*
	Ergebnisse der letzten 16 Intervalle (jüngstes zuerst)	Siehe *Externes Interface*

6.11.3 Ring-/Netzkopplung

Die Funktion Ring-/Netzkopplung wird **nicht** unterstützt von:
- mGuard centerport

Ring-/Netzkopplung mit Einschränkung:
- mGuard delta: hier lässt sich die interne Seite (Switch-Ports) nicht abschalten
- mGuard pci: hier lässt sich im Treibermodus die interne Netzwerkschnittstelle nicht abschalten (wohl aber im Power-over-PCI-Modus).

6.11.3.1 Ring-/Netzkopplung



Redundanz >> Firewall-Redundanz >> Ring-/Netzkopplung		
Settings	**Aktiviere Ring-/Netzkopplung/Dual Homing**	**Ja / Nein** Bei Aktivierung wird im Stealth-Modus der Status der Ethernetverbindung von einen Port auf den anderen übertragen, wodurch sich Unterbrechungen im Netzwerk leicht zurückverfolgen lassen.
	Redundanzport	**Intern / Extern** **Intern**: Wenn die Verbindung am LAN-Port wegfällt/kommt, wird auch der WAN-Port ausgeschaltet/eingeschaltet. **Extern**: Wenn die Verbindung am WAN-Port wegfällt/kommt, wird auch der LAN-Port ausgeschaltet/eingeschaltet.

6.12 Menü Logging

Unter Logging versteht man die Protokollierung von Ereignismeldungen z. B. über vorgenommene Einstellungen, über Greifen von Firewall-Regeln, über Fehler usw.

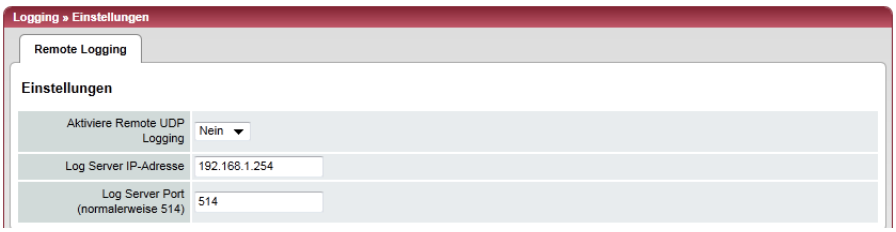
Log-Einträge werden unter verschiedenen Kategorien erfasst und können nach Kategorie sortiert angezeigt werden (siehe „Logging >> Logs ansehen“ auf Seite 6-254).

6.12.1 Logging >> Einstellungen

6.12.1.1 Remote Logging

Alle Log-Einträge finden standardmäßig im Arbeitsspeicher des mGuards statt. Ist der maximale Speicherplatz für diese Protokollierungen erschöpft, werden automatisch die ältesten Log-Einträge durch neue überschrieben. Zudem werden beim Ausschalten des mGuards alle Log-Einträge gelöscht.

Um das zu verhindern, ist es möglich, die Log-Einträge (SysLog-Meldungen) auf einen externen Rechner (SysLog-Server) zu übertragen. Das liegt auch dann nahe, sollte eine zentrale Verwaltung der Protokollierungen mehrerer mGuards erfolgen.



Logging >> Remote Logging		
Einstellungen	**Aktiviere Remote UDP Logging**	**Ja / Nein** Sollen alle Log-Einträge zum externen (unten angegebenen) Log Server übertragen werden, wählen Sie **Ja**.
	Log-Server-IP-Adresse	Geben Sie die IP-Adresse des Log-Servers an, zu dem die Log-Einträge per UDP übertragen werden sollen. Sie müssen eine IP-Adresse angeben, keinen Hostnamen! Hier wird eine Namensauflösung nicht unterstützt, weil sonst bei Ausfall eines DNS-Servers unter Umständen nicht protokolliert werden könnte.
	Log-Server-Port (normalerweise 514)	Geben Sie den Port des Log-Servers an, zu dem die Log-Einträge per UDP übertragen werden sollen. Standard: 514

Wenn SysLog-Meldungen über einen VPN-Kanal auf einen SysLog-Server übertragen werden sollen, dann muss sich die IP-Adresse des SysLog-Servers in dem Netzwerk befinden, das in der Definition der VPN-Verbindung als **Remote**-Netzwerk angegeben ist.

Und die interne IP-Adresse (im Stealth-Modus die **Stealth Management IP-Adresse** bzw. **Virtuelle IP**) muss sich in dem Netzwerk befinden, das in der Definition der VPN-Verbindung als **Lokal** angegeben ist (siehe „VPN-Verbindung / VPN-Verbindungskanäle definieren“ auf Seite 6-190).

Logging >> Remote Logging [...]

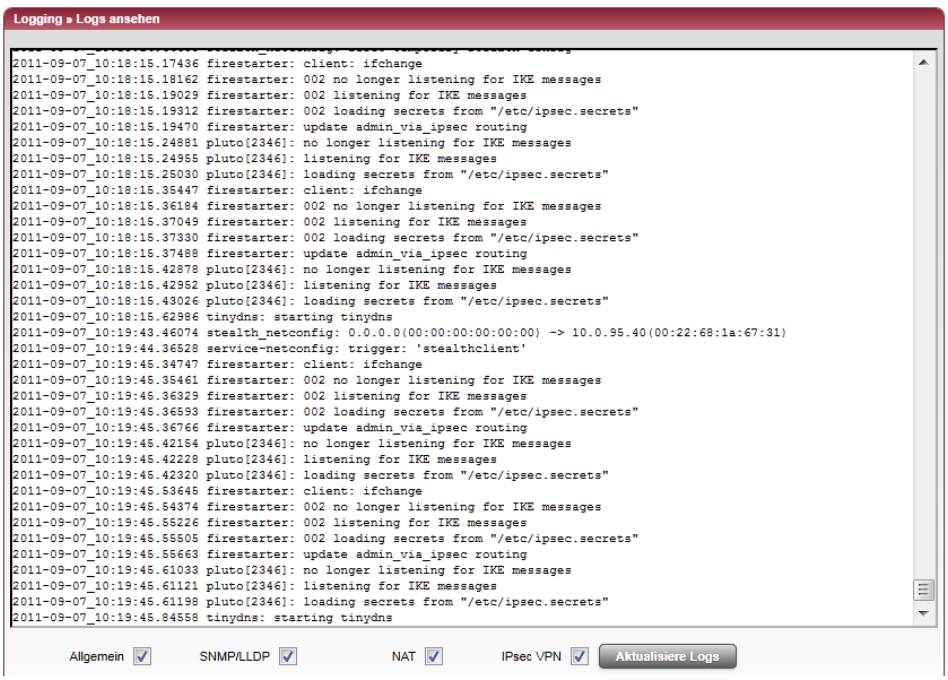
– Ist dabei die Option **Aktiviere 1-zu-1-NAT des lokalen Netzwerkes in ein internes Netz** auf **Ja** gestellt (siehe „1-zu-1-NAT“ auf Seite 6-203), gilt Folgendes:

  Die interne IP-Adresse (im Stealth-Modus die **Stealth Management IP-Adresse** bzw. **Virtuelle IP**) muss sich in dem Netzwerk befinden, das mit **Interne Netzwerkadresse für lokales 1-zu-1-NAT** angegeben ist.

– Ist dabei die Option **Aktiviere 1-zu-1-NAT des gegenüberliegenden Netzwerkes auf ein anders Netz** auf **Ja** gestellt (siehe „1-zu-1-NAT“ auf Seite 6-203), gilt Folgendes:

  Die IP-Adresse des SysLog-Servers muss sich in dem Netzwerk befinden, das in der Definition der VPN-Verbindung als **Remote** angegeben ist.

6.12.2 Logging >> Logs ansehen



Je nachdem, welche Funktionen des mGuards aktiv gewesen sind, werden unterhalb der Log-Einträge entsprechende Kontrollkästchen zum Filtern der Einträge nach Kategorien angezeigt.

Damit eine oder mehrerer Kategorien angezeigt werden, aktivieren Sie das/die Kontrollkästchen der gewünschten Kategorie(n) und klicken dann auf die Schaltfläche **Aktualisiere Logs**.

6.12.2.1 Kategorien der Log-Einträge

Allgemein

Log-Einträge, die den anderen Kategorien nicht zugeordnet werden können.

Netzwerksicherheit

Zugriffe über seine Firewall werden beim **mGuard rs2000 nicht** mitgeloggt.

Ist bei Festlegung von Firewall-Regeln das Protokollieren von Ereignissen festgelegt (Log = Ja), dann können Sie hier das Log aller protokollierten Ereignisse einsehen.

Log-ID und Nummer zum Auffinden von Fehlerquellen

Log-Einträge, die sich auf die nachfolgend aufgelisteten Firewall-Regeln beziehen, haben eine Log-D und eine Nummer. Anhand dieser Log-ID und Nr. ist es möglich, die Firewall-Regel ausfindig zu machen, auf die sich der betreffende Log-Eintrag bezieht und die zum entsprechenden Ereignis geführt hat.

Firewall-Regeln und ihre Log-ID

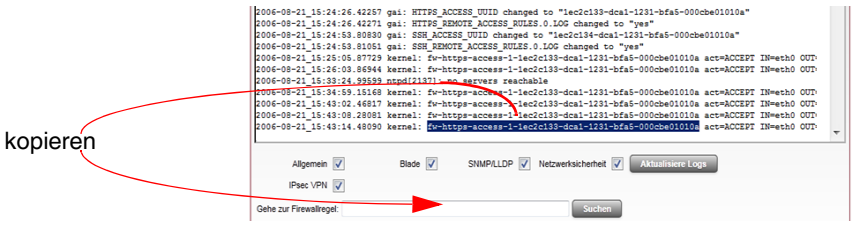
- Paketfilter:
  Menü Netzwerksicherheit >> Paketfilter >> Eingangsregeln
  Menü Netzwerksicherheit >> Paketfilter >> Ausgangsregeln
  Log-ID: ***fw-incoming*** bzw. ***fw-outgoing***
- Firewall-Regeln bei VPN-Verbindungen:
  Menü IPsec VPN >> Verbindungen >> Editieren >> Firewall , eingehend / ausgehend
  Log-ID: ***vpn-fw-in*** bzw. ***vpn-fw-out***
- Firewall-Regeln bei Web-Zugriff auf den mGuard über HTTPS:
  Menü Verwaltung >> Web-Einstellungen >> Zugriff
  Log-ID: ***fw-https-access***
- Firewall-Regeln bei Zugriff auf den mGuard über SNMP:
  Menü Verwaltung >> SNMP >> Abfrage
  Log-ID: ***fw-snmp-access***
- Firewall-Regeln bei SSH-Fernzugriff auf den mGuard:
  Menü Verwaltung >> Systemeinstellungen >> Shell-Zugang
  Log-ID: ***fw-ssh-access***
- Firewall-Regeln der Benutzerfirewall:
  Menü Netzwerksicherheit >> Benutzerfirewall , Firewall-Regeln
  Log-ID: ***ufw-***
- Regeln für NAT, Port-Weiterleitung
  Menü Netzwerk >> NAT >> IP und Port-Weiterleitung
  Log-ID: ***fw-portforwarding***
- Firewall-Regeln für serielle Schnittstelle:
  Menü Netzwerk >> Interfaces >> Eingehender Ruf
  Eingangsregeln
  Log-ID: ***fw-serial-incoming***
  Ausgangsregeln
  Log-ID: ***fw-serial-outgoing***

Suche nach Firewall-Regel auf Grundlage eines Netzwerksicherheits-Logs

Ist das Kontrollkästchen **Netzwerksicherheit** aktiviert, sodass die betreffenden Log-Einträge angezeigt werden, wird unterhalb der Schaltfläche *Aktualisiere Logs* das Suchfeld **Gehe zur Firewall-Regel** angezeigt.

Gehen Sie wie folgt vor, wenn Sie die Firewall-Regel ausfindig machen wollen, auf die sich ein Log-Eintrag der Kategorie *Netzwerksicherheit* bezieht und die zum entsprechenden Ereignis geführt hat:

1. Beim betreffenden Log-Eintrag die Passage markieren, die die Log-ID und Nummer enthält, z. B.: fw-https-access-1-1ec2c133-dca1-1231-bfa5-000cbe01010a



2. Diese Passage über die Zwischenablage ins Feld **Gehe zur Firewall-Regel** kopieren.
3. Auf die Schaltfläche **Suchen** klicken.

   Es wird die Konfigurationsseite mit der Firewall-Regel angezeigt, auf die sich der Log-Eintrag bezieht.

Blade

Auf dem mGuard blade-Controller werden, neben Fehlermeldungen, die folgenden Meldungen ausgegeben:

(Die mit < und > umklammerten Bereiche sind in den Log-Einträgen durch die jeweiligen Daten ersetzt.)

Allgemeine Meldungen:

blade daemon "<version>" starting ...
Blade[<bladenr>] online
Blade[<bladenr>] is mute
Blade[<bladenr>] not running
Reading timestamp from blade[<bladenr>]

Beim Aktivieren eines Konfigurationsprofils auf einem Blade:

Push configuration to blade[<bladenr>]
reconfiguration of blade[<bladenr>] returned <returncode>
blade[<bladenr>] # <text>

Beim Holen eines Konfigurationsprofils vom Blade:

Pull configuration from blade[<bladenr>]
Pull configuration from blade[<bladenr>] returned <returncode>

CIFS-AV-Scan-Connector

In diesem Log werden Meldungen des CIFS-Servers angezeigt, welchen der mGuard selbst zum Freigeben betreibt.

Zusätzlich sind Meldungen sichtbar, die beim Anbinden der Netzlaufwerke entstehen und die durch den CIFS-Server gesammelt in einer Freigabe bereitgestellt werden.

CIFS-Integritätsprüfung

In diesem Log werden Meldungen über die Integritätsprüfung von Netzwerklaufwerken angezeigt.

Zusätzlich sind Meldungen sichtbar, die beim Anbinden der Netzlaufwerke entstehen und die für die Integritätsprüfung benötigt werden.

DHCP-Server/Relay

Meldungen der unter Netzwerk -> DHCP konfigurierbaren Dienste.

SNMP/LLDP

Meldungen der unter Verwaltung -> SNMP konfigurierbaren Dienste.

IPsec VPN

Listet alle VPN-Ereignisse auf.

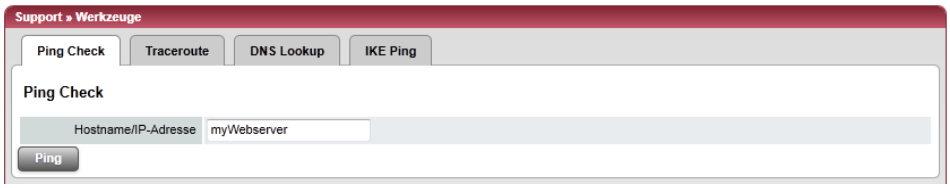
Das Format entspricht dem unter Linux gebräuchlichen Format.

Es gibt spezielle Auswertungsprogramme, die Ihnen die Informationen aus den protokollierten Daten in einem besser lesbaren Format präsentieren.

6.13 Menü Support

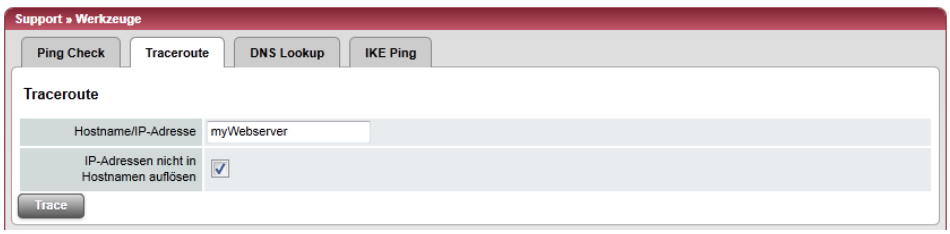
6.13.1 Support >> Werkzeuge

6.13.1.1 Ping-Check



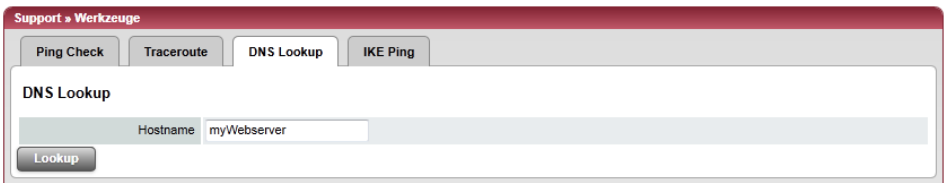
Support >> Werkzeuge >> Ping-Check	
Ping-Check	**Ziel**: Sie wollen überprüfen, ob eine Gegenstelle über ein Netzwerk erreichbar ist. **Vorgehen**: • In das Feld **Hostname/IP-Adresse** die IP-Adresse oder den Hostnamen der Gegenstelle eingeben. Dann auf die Schaltfläche **Ping** klicken. Sie erhalten daraufhin eine entsprechende Meldung.

6.13.1.2 Traceroute



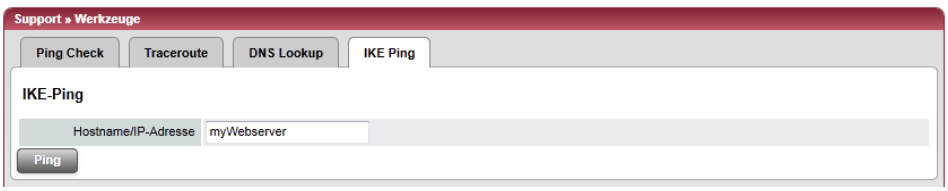
Support >> Werkzeuge >> Traceroute	
Traceroute	**Ziel**: Sie wollen wissen, welche Zwischenstellen oder Router sich auf dem Verbindungsweg zu einer Gegenstelle befinden. **Vorgehen**: • In das Feld **Hostname/IP-Adresse** den Hostnamen oder IP-Adresse der Gegenstelle eintragen, zu der die Route ermittelt werden soll. • Falls die auf der Route gelegenen Stellen mit IP-Adresse statt mit Hostnamen (falls vorhanden) ausgegeben werden sollen, aktivieren Sie das Kontrollkästchen **Do not resolve IP addresses to hostnames** (= Häkchen setzen). • Dann auf die Schaltfläche **Trace** klicken. Sie erhalten daraufhin eine entsprechende Meldung.

6.13.1.3 DNS-Lookup



Support >> Werkzeuge >> DNS-Lookup	
DNS-Lookup	**Ziel**: Sie wollen wissen, welcher Hostname zu einer bestimmten IP-Adresse gehört oder welche IP-Adresse zu einem bestimmten Hostnamen gehört. **Vorgehen**: • In das Feld **Hostname** die IP-Adresse bzw. den Hostnamen eingeben. • Auf die Schaltfläche **Lookup** klicken. Sie erhalten daraufhin die Antwort, wie sie der mGuard aufgrund seiner DNS-Konfiguration ermittelt.

6.13.1.4 IKE-Ping

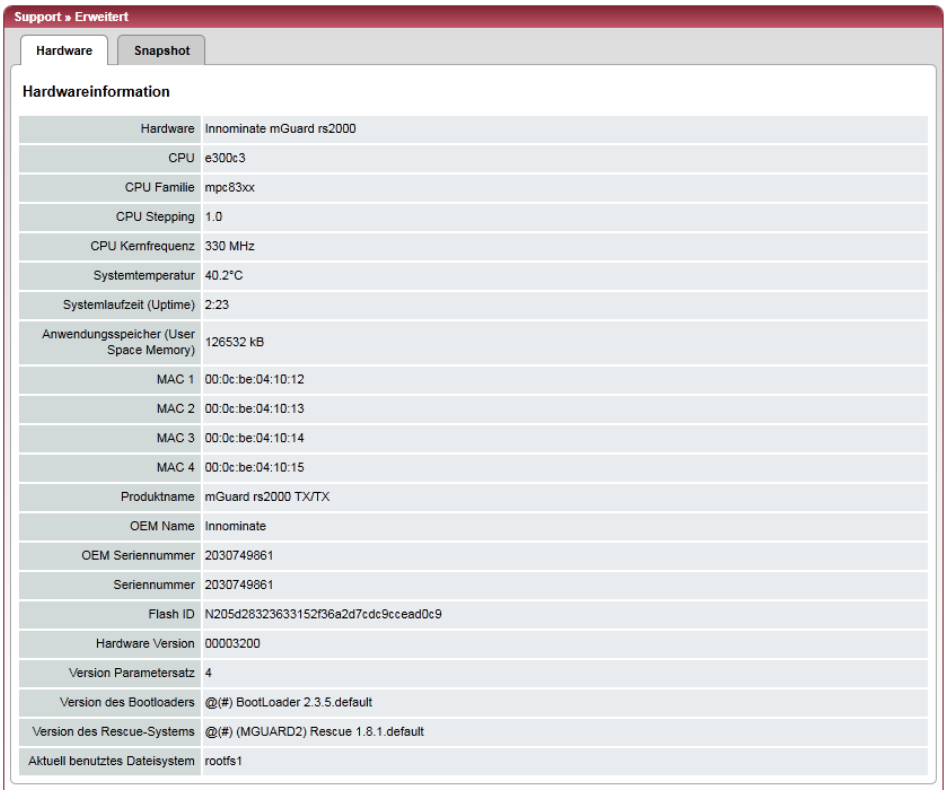


Support >> Werkzeuge >> IKE-Ping	
IKE-Ping	**Ziel**: Sie wollen ermitteln, ob die VPN-Software eines VPN-Gateways in der Lage ist, eine VPN-Verbindung aufzubauen, oder ob z. B. eine Firewall das verhindert. **Vorgehen**: • In das Feld **Hostname/IP-Adresse** den Namen bzw. die IP-Adresse des VPN-Gateways eingeben. • Auf die Schaltfläche **Ping** klicken. • Sie erhalten eine entsprechende Meldung.

6.13.2 Support >> Erweitert

6.13.2.1 Hardware

Diese Seite listet verschiedene Hardware-Eigenschaften des mGuards auf.



6.13.2.2 Snapshot

Diese Funktion dient für Support-Zwecke.

Erstellt eine komprimierte Datei (im tar.gz-Format), in der alle aktuellen Konfigurations-Einstellungen und Log-Einträge erfasst sind, die zur Fehlerdiagnose relevant sein könnten.

Diese Datei enthält keine privaten Informationen wie z. B. private Maschinenzertifikate oder Passwörter. Eventuell benutzte Pre-Shared Keys von VPN-Verbindungen sind jedoch in Snapshots enthalten.

Um einen Snapshot zu erstellen, gehen Sie wie folgt vor:

- Die Schaltfläche **Herunterladen** klicken.
- Die Datei speichern (unter dem Namen snapshot.tar.gz)

Stellen Sie die Datei dem Support Ihres Händlers zur Verfügung, wenn dies erforderlich ist.

6.14 CIDR (Classless Inter-Domain Routing)

IP-Netzmasken und CIDR sind Notationen, die mehrere IP-Adressen zu einem Adressraum zusammenfassen. Dabei wird ein Bereich von aufeinander folgenden Adressen als ein Netzwerk behandelt.

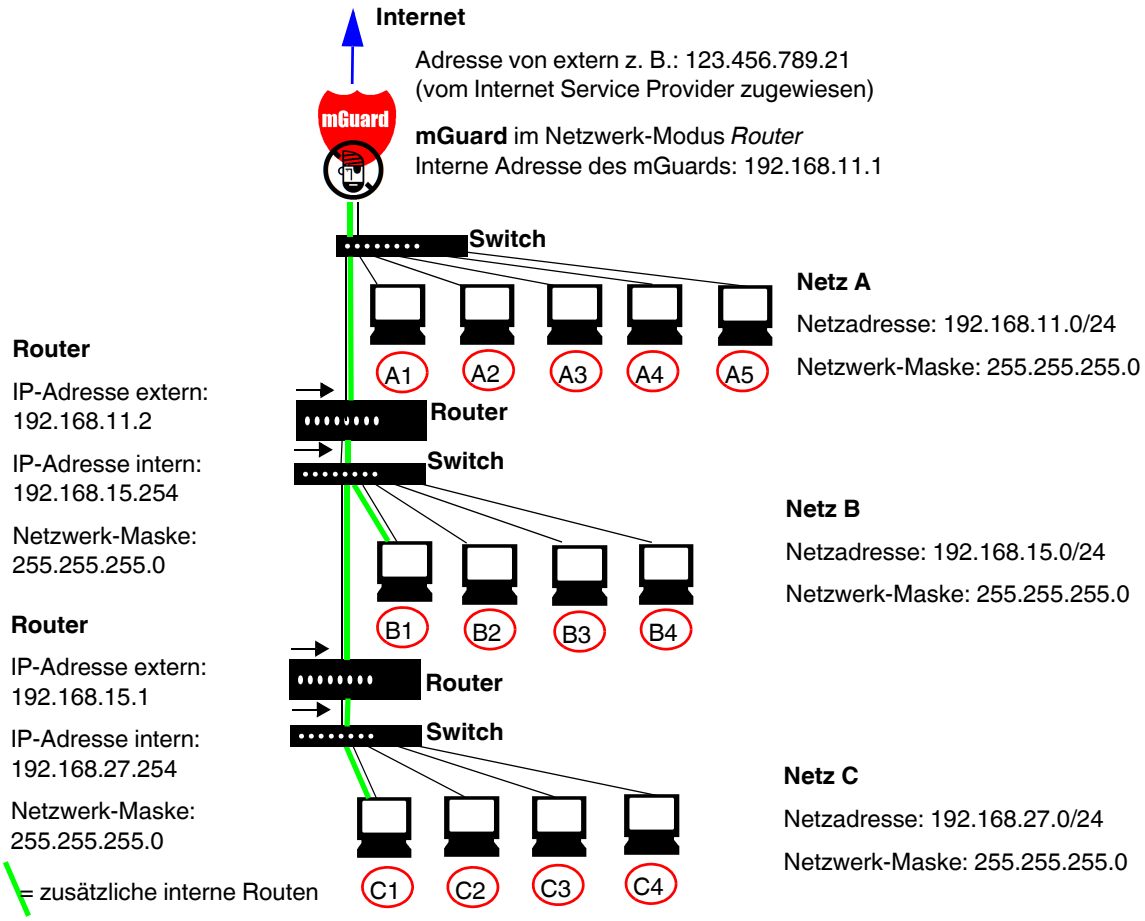
Um dem mGuard einen Bereich von IP-Adressen anzugeben, z. B. bei der Konfiguration der Firewall, kann es erforderlich sein, den Adressraum in der CIDR-Schreibweise anzugeben. Die nachfolgende Tabelle zeigt links die IP-Netzmaske, ganz rechts die entsprechende CIDR-Schreibweise.

IP-Netzmaske	binär	CIDR
255.255.255.255	11111111 11111111 11111111 11111111	32
255.255.255.254	11111111 11111111 11111111 11111110	31
255.255.255.252	11111111 11111111 11111111 11111100	30
255.255.255.248	11111111 11111111 11111111 11111000	29
255.255.255.240	11111111 11111111 11111111 11110000	28
255.255.255.224	11111111 11111111 11111111 11100000	27
255.255.255.192	11111111 11111111 11111111 11000000	26
255.255.255.128	11111111 11111111 11111111 10000000	25
255.255.255.0	11111111 11111111 11111111 00000000	24
255.255.254.0	11111111 11111111 11111110 00000000	23
255.255.252.0	11111111 11111111 11111100 00000000	22
255.255.248.0	11111111 11111111 11111000 00000000	21
255.255.240.0	11111111 11111111 11110000 00000000	20
255.255.224.0	11111111 11111111 11100000 00000000	19
255.255.192.0	11111111 11111111 11000000 00000000	18
255.255.128.0	11111111 11111111 10000000 00000000	17
255.255.0.0	11111111 11111111 00000000 00000000	16
255.254.0.0	11111111 11111110 00000000 00000000	15
255.252.0.0	11111111 11111100 00000000 00000000	14
255.248.0.0	11111111 11111000 00000000 00000000	13
255.240.0.0	11111111 11110000 00000000 00000000	12
255.224.0.0	11111111 11100000 00000000 00000000	11
255.192.0.0	11111111 11000000 00000000 00000000	10
255.128.0.0	11111111 10000000 00000000 00000000	9
255.0.0.0	11111111 00000000 00000000 00000000	8
254.0.0.0	11111110 00000000 00000000 00000000	7
252.0.0.0	11111100 00000000 00000000 00000000	6
248.0.0.0	11111000 00000000 00000000 00000000	5
240.0.0.0	11110000 00000000 00000000 00000000	4
224.0.0.0	11100000 00000000 00000000 00000000	3
192.0.0.0	11000000 00000000 00000000 00000000	2
128.0.0.0	10000000 00000000 00000000 00000000	1

Beispiel: 192.168.1.0 / 255.255.255.0 entspricht im CIDR: 192.168.1.0/24

6.15 Netzwerk-Beispielskizze

Die nachfolgende Skizze zeigt, wie in einem lokalen Netzwerk mit Subnetzen die IP-Adressen verteilt sein könnten, welche Netzwerk-Adressen daraus resultieren und wie beim mGuard die Angaben zusätzlicher interner Route lauten könnten.



Netz A	**Rechner**	**A1**	**A2**	**A3**	**A4**	**A5**
	IP-Adresse	192.168.11.3	**192.168.11.4**	**192.168.11.5**	**192.168.11.6**	**192.168.11.7**
	Netzwerk-Maske	255.255.255.0	**255.255.255.0**	**255.255.255.0**	**255.255.255.0**	**255.255.255.0**
Netz B	**Rechner**	**B1**	**B2**	**B3**	**B4**	Zusätzliche interne Routen:
	IP-Adresse	192.168.15.2	**192.168.15.3**	**192.168.15.4**	**192.168.15.5**	Netzwerk: 192.168.15.0/24
	Netzwerk-Maske	255.255.255.0	**255.255.255.0**	**255.255.255.0**	**255.255.255.0**	Gateway: 192.168.11.2
Netz C	**Rechner**	**C1**	**C2**	**C3**	**C4**	Netzwerk: 192.168.27.0/24
	IP-Adresse	192.168.27.1	**192.168.27.2**	**192.168.27.3**	**192.168.27.4**	Gateway: 192.168.11.2
	Netzwerk-Maske	255.255.255.0	**255.255.255.0**	**255.255.255.0**	**255.255.255.0**	

7 Redundanz

Die Firewall- und die VPN-Redundanz stehen **nicht** auf dem **mGuard rs2000** zur Verfügung.

Es gibt verschiedene Möglichkeiten mit dem mGuard Fehler so zu kompensieren, dass eine bestehende Verbindung nicht unterbrochen wird.

- **Firewall-Redundanz:** Sie können zwei baugleiche mGuards zu einem Redundanzpaar zusammenzufassen, bei dem im Fehlerfall der eine die Funktion des anderen übernimmt.
- **VPN-Redundanz**: Basis hierfür ist eine bestehende Firewall-Redundanz. Zusätzlich dazu werden die VPN-Verbindungen so ausgelegt, das mindestens ein mGuard eines Redunanzpaares die VPN-Verbindungen betreibt.
- **Ring-/Netzkopplung:** Bei der Ring-/Netzkopplung wird ein anderer Ansatz gewählt. Hier werden Teile eines Netzes redundant ausgelegt. Im Fehlerfall wird dann der alternative Weg gewählt.

7.1 Firewall-Redundanz

Mit Hilfe der Firewall-Redundanz ist es möglich, zwei baugleiche mGuards zu einem Redundanzpaar (einem virtuellen Router) zusammenzufassen. Dabei übernimmt ein mGuard in einem Fehlerfall die Funktion des anderen. Beide mGuards laufen synchron, so dass bei einem Wechsel die bestehende Verbindung nicht unterbrochen wird.

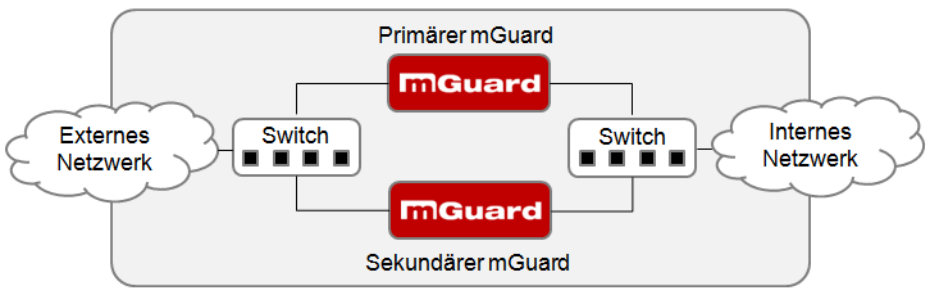


Bild 7-1 Firewall-Redundanz (Beispiel)

Grundbedingungen für die Firewall-Redundanz

Die Firewall-Redundanz ist eine lizenzpflichtige Funktion. Sie kann nur benutzt werden, wenn die entsprechende Lizenz erworben wurde und installiert ist.

- Nur baugleiche mGuards können ein Redundanzpaar bilden.
- Im Netzwerk-Modus Router wird die Firewall-Redundanz nur mit dem Router-Modus „statisch“ unterstützt.
- Der Netzwerk-Modus Stealth wird derzeit noch nicht unterstützt.
- Weitere Einschränkungen siehe „Voraussetzungen für die Firewall-Redundanz“ auf Seite 7-4 und „Grenzen der Firewall-Redundanz“ auf Seite 7-14.

7.1.1 Komponenten der Firewall-Redundanz

Die Firewall-Redundanz besteht aus mehreren Komponenten:

- **Konnektivitätsprüfung**
  Prüft, ob die erforderlichen Netzwerkverbindungen bestehen.
- **Verfügbarkeitsprüfung**
  Prüft, ob ein aktiver mGuard vorhanden ist und ob dieser aktiv bleiben soll.
- **Zustandsabgleich der Firewall**
  Der mGuard in Bereitschaft erhält eine Kopie des aktuellen Zustands der Firewall-Datenbank.
- **Virtuelles Netzwerk-Interface**
  Stellt virtuelle IP-Adressen und MAC-Adressen bereit, die von anderen Geräten als Routen und Standard-Gateways genutzt werden können.
- **Statusüberwachung**
  Koordiniert alle Komponenten.
- **Statusanzeige**
  Zeigt dem Benutzer den Zustand des mGuards an.

Konnektivitätsprüfung

Bei jedem mGuard eines Redundanzpaares wird kontinuierlich geprüft, ob eine Verbindung besteht, über die Netzwerkpakete weitergleitet werden können.

Jeder mGuard prüft seine interne und externe Netzwerk-Schnittstelle unabhängig voneinander. Beide Schnittstellen werden auf eine durchgehende Verbindung getestet. Diese Verbindung muss bestehen, sonst wird die Konnektivitätsprüfung nicht bestanden.

Optional können ICMP-Echo-Requests gesendet werden. Sie können die ICMP-Echo-Requests über das Menü *Redundanz >> Firewall-Redundanz >> Konnektivitätsprüfung* einstellen.

Verfügbarkeitsprüfung

Bei jedem mGuard eines Redundanzpaares wird außerdem kontinuierlich geprüft, ob ein aktiver mGuard vorhanden ist und ob dieser aktiv bleiben soll. Dafür wird eine Variante des CARP (Common Address Redundancy Protocol) verwendet.

Der aktive mGuard sendet ständig Anwesenheitsnachrichten über sein internes und externes Netzwerk-Interface, während beide mGuards zuhören. Wenn ein dedizierter Ethernet-Link für den Zustandsabgleich der Firewall vorhanden ist, wird die Anwesenheitsnachricht auch über diesen gesendet. In diesem Fall kann die Anwesenheitsnachricht für die externe Netzwerk-Schnittstelle auch unterdrückt werden.

Die Verfügbarkeitsprüfung wird nicht bestanden, wenn ein mGuard in einer bestimmten Zeit keine Anwesenheitsnachricht erhält. Außerdem wird die Prüfung nicht bestanden, wenn ein mGuard Anwesenheitsnachrichten von niedrigerer Priorität erhält als die eigene.

Die Daten werden immer über das physikalische Netzwerk-Interface übertragen und niemals über das virtuelle Netzwerk-Interface.

Zustandsabgleich

Der mGuard, der sich im Zustand der Bereitschaft befindet, erhält eine Kopie des Zustandes des aktuell aktiven mGuards.

Dazu gehört eine Datenbank mit den weitergeleiteten Netzwerkverbindungen. Diese Datenbank wird laufend durch die weitergeleiteten Netzwerkpakete aufgebaut und erneuert. Sie ist gegen einen unberechtigen Zugriff geschützt. Die Daten werden über die physikalische LAN-Schnittstelle übertragen und niemals über das virtuelle Netzwerk-Interface gesendet.

Um den internen Datenverkehr gering zu halten, kann ein VLAN so konfiguiert werden, dass es die Abgleichsdaten in eine separate Multicast- und Broadcast-Domain verlagert.

Virtuelle IP-Adressen

Jeder mGuard wird mit virtuellen IP-Adressen konfiguriert. Deren Anzahl hängt von dem verwendeten Netzwerk-Modus ab. Bei einem Redundanzpaar müssen Sie beiden mGuards die gleichen virtuellen IP-Adressen zuweisen. Die virtuellen IP-Adressen werden vom mGuard benötigt, um virtuelle Netzwerk-Interfaces aufzubauen.

Für den Netzwerk-Modus Router sind zwei virtuelle IP-Adressen notwendig, weitere können angelegt werden. Eine virtuelle IP-Adresse wird für das externe Netzwerk-Interface und die andere für das interne Netzwerk-Interface benötigt.

Diese IP-Adressen werden als Gateway für das Routen von Geräten benutzt, die sich im externen oder internen LAN befinden. Auf diese Weise können die Geräte von der hohen Verfügbarkeit profitieren, die durch die beiden redundanten mGuards entsteht.

Das Redundanzpaar bestimmt automatisch MAC-Adressen für das virtuelle Netzwerk-Interface. Diese MAC-Adressen sind identisch für das Redundanzpaar. Im Netzwerk-Modus Router teilen sich beide mGuards je eine MAC-Adresse für das virtuelle Netzwerk-Interface, das mit dem externen und dem internen Ethernet-Segment verbunden ist.

Im Netzwerk-Modus Router unterstützen die mGuards eine Weiterleitung von speziellen UDP/TCP-Ports von einer virtuellen IP-Adresse zu anderen IP-Adressen, sofern letztere vom mGuard erreicht werden können. Zusätzlich maskiert der mGuard Daten mit virtuellen IP-Adressen, wenn Masquerading-Regeln eingerichtet sind.

Statusüberwachung

Die Statusüberwachung entscheidet darüber, ob der mGuard im Zustand aktiv, in Bereitschaft oder im Fehlerzustand ist. Jeder mGuard entscheidet autonom über seinen Zustand, basierend auf den Informationen, die von anderen Komponenten bereitgestellt werden. Die Statusüberwachung sorgt dafür, dass nicht zwei mGuards gleichzeitig aktiv sind.

Statusanzeige

Die Statusanzeige enthält detaillierte Informationen über den Status der Firewall-Redundanz. Eine Zusammenfassung des Status kann über das Menü *Redundanz* >> *Firewall-Redundanz* >> *Redundanz* oder *Redundanz* >> *Firewall-Redundanz* >> *Konnektivitätsprüfung* abgerufen werden.

7.1.2 Zusammenarbeit der Firewall-Redundanz-Komponenten

Während des Betriebes interagieren die Komponenten folgendermaßen: Beide mGuards führen fortlaufend für ihre beiden Netzwerk-Schnittstellen (internes und externes Interface) eine Konnektivitätsprüfung durch. Außerdem wird fortlaufend eine Verfügbarkeitsprüfung gemacht. Dazu lauscht jeder mGuard kontinuierlich auf Anwesenheitsnachrichten (CARP) und der aktive mGuard sendet diese zusätzlich.

Auf Grundlage der Informationen aus der Konnektivitäts- und - Verfügbarkeitsprüfung weiß die Statusüberwachung, in welchem Zustand sich die mGuards befinden. Die Statusüberwachung sorgt dafür, dass der aktive mGuard seine Daten auf den anderen mGuard spiegelt (Zustandsabgleich).

7.1.3 Firewall-Redundanz-Einstellungen aus vorherigen Versionen

Vorhandene Konfigurationsprofile der Firmware-Version 6.1.x (und davor) können mit bestimmten Einschränkungen importiert werden. Bitte nehmen Sie hierzu Kontakt zu Innominate auf.

7.1.4 Voraussetzungen für die Firewall-Redundanz

- Die Firewall-Redundanz kann nur aktiviert werden, wenn ein gültiger Lizenzschlüssel installiert ist.
  (unter: *Redundanz >> Firewall-Redundanz >> Redundanz >> Aktiviere Redundanz)*
- *Redundanz >> Firewall-Redundanz >> Redundanz >> Interface, das zum Zustandsabgleich verwendet wird*
  Der Wert **Dediziertes Interface** wird nur auf mGuards akzeptiert, die mehr als zwei physikalische und getrennte Ethernet-Interfaces haben. Zur Zeit ist das der mGuard centerport.
- Jeder Satz von Zielen für die Konnektivitätsprüfung kann mehr als zehn Ziele beinhalten. (Ohne eine Obergrenze kann eine Failover-Zeit nicht garantiert werden.)
  Redundanz >> Firewall-Redundanz >> Redundanz
  - *>> Externes Interface >> Primäre Ziele für ICMP Echo-Anfragen*
  - *>> Externes Interface >> Sekundäre Ziele für ICMP Echo-Anfragen*
  - *>> Internes Interface >> Primäre Ziele für ICMP Echo-Anfragen*
  - *>> Internes Interface >> Sekundäre Ziele für ICMP Echo-Anfragen*

  Wenn unter *Externes Interface >> Art der Prüfung* „**mindestens ein Ziel muss antworten**“ oder „**alle Ziele einer Menge müssen antworten**“ ausgewählt ist, darf *Externes Interface >> Primäre Ziele für ICMP Echo-Anfragen* nicht leer sein. Das Gleiche gilt für das Interne Interface.
- Im **Netzwerk-Modus Router** müssen mindestens eine externe und eine interne virtuelle IP-Adresse eingestellt werden. Keine virtuelle IP-Adresse darf doppelt aufgelistet werden.

7.1.5 Umschaltzeit im Fehlerfall

Von der Variablen **Umschaltzeit im Fehlerfall** errechnet der mGuard automatisch die Zeitabstände für die Konnektivitäts- und Verfügbarkeitsprüfung.

Konnektivitätsprüfung

In der Tabelle 7-1 auf Seite 7-5 werden die Faktoren angegeben, die die Zeitabstände für die Konnektivitätsprüfung bestimmen.

Für die Konnektivitätsprüfung werden ICMP-Echo-Requests verschickt, die 64 kByte groß sind. Sie werden auf Layer 3 des Internet-Protokolls gesendet. Mit dem Ethernet auf Layer 2 kommen 18 Bytes für den MAC-Header und die Prüfsumme dazu, wenn kein VLAN verwendet wird. Der IMCP-Echo-Reply hat die gleiche Größe.

In Tabelle 7-1 wird außerdem die Bandbreite gezeigt. Sie berücksichtigt die genannten Werte für ein einzelnes Ziel und summiert die Bytes für ICMP-Echo-Request und Reply.

Der Timeout am mGuard nach dem Senden enthält Folgendes:

– Die Zeit, die der mGuard braucht, um den ICMP-Echo-Reply zu übertragen. Der Halb-Duplex-Modus ist hierfür nicht geeignet, wenn anderer Datenverkehr dazu kommt.
– Die Zeit, die für die Übertragung des ICMP-Echo-Requests zu einem Ziel erforderlich ist. Beachten Sie dabei die Latenzzeit bei einer hohen Auslastung. Die gilt besonders, wenn Router die Anfrage weiterleiten.
– Die Zeit, die pro Ziel benötigt wird, um den Request zu bearbeiten und das Reply zum Ethernet-Layer zu übertragen. Beachten Sie, dass hier ebenfalls der Voll-Duplex-Modus gebraucht wird.
– Die Zeit für die Übertragung des ICMP-Echo-Replies zum mGuard.

Tabelle 7-1 Frequenz der ICMP-Echo-Requests

Failover-Umschaltzeit	ICMP-Echo-Requests pro Ziel	Timeout am mGuard nach dem Senden	Bandbreite pro Ziel
1 s	10 pro Sekunde	100 ms	6560 Bit/s
3 s	$3,\overline{3}$ pro Sekunde	300 ms	2187 Bit/s
10 s	1 pro Sekunde	1 s	656 Bit/s

Wenn sekundäre Ziele konfiguriert sind, kann es gelegentlich passieren, dass zusätzliche ICMP-Echo-Requests zu diesen Zielen gesendet werden. Dies muss bei der Berechnung für die ICMP-Echo-Request-Rate berücksichtigt werden.

In der Tabelle 7-1 wird der Timeout für einen einzelnen ICMP-Echo-Request gezeigt. Das sagt noch nichts darüber aus, wie viele der Responses vermisst werden dürfen, bevor die Konnektivitätsprüfung ausfällt. Diese Prüfung toleriert, wenn von zwei aufeinander folgenden Intervallen eines negativ ist.

Verfügbarkeitsprüfung

Die Größe der Anwesenheitsnachrichten (CARP) beträgt bis zu 76 Bytes am Layer 3 des Internet-Protokolls. Mit dem Ethernet auf Layer 2 kommen 18 Bytes für den MAC-Header und die Prüfsumme dazu, wenn kein VLAN verwendet wird. Der IMCP-Echo-Reply hat die gleiche Größe.

Die Tabelle 7-2 zeigt die maximale Frequenz, mit der Anwesenheitsnachrichten (CARP) vom aktiven mGuard gesendet werden. Sie zeigt außerdem die Bandbreite, die dabei verbraucht wird. Die Frequenz hängt von der Priorität des mGuards und der *Umschaltzeit im Fehlerfall* ab.

Die Tabelle 7-2 zeigt außerdem die maximale Latenzzeit, die der mGuard für das Netzwerk toleriert, das die Anwesenheitsnachrichten (CARP) überträgt. Wenn diese Latenzzeit überschritten wird, kann das Redundanzpaar ein undefiniertes Verhalten zeigen.

Tabelle 7-2 Frequenz der Anwesenheitsnachrichten (CARP)

Failover-Umschaltzeit	Anwesenheitsnachrichten (CARP) pro Sekunde		Maximale Latenzzeit	Bandbreite am Layer 2 für die hohe Priorität
	Hohe Priorität	Niedrige Priorität		
1 s	50 pro Sekunde	25 pro Sekunde	20 ms	37,600 Bit/s
3 s	16,6 pro Sekunde	8,3 pro Sekunde	60 ms	12,533 Bit/s
10 s	5 pro Sekunde	2,5 pro Sekunde	200 ms	3,760 Bit/s

7.1.6 Fehlerkompensation durch die Firewall-Redundanz

Die Firewall-Redundanz dient dazu, den Ausfall von Hardware auszugleichen.

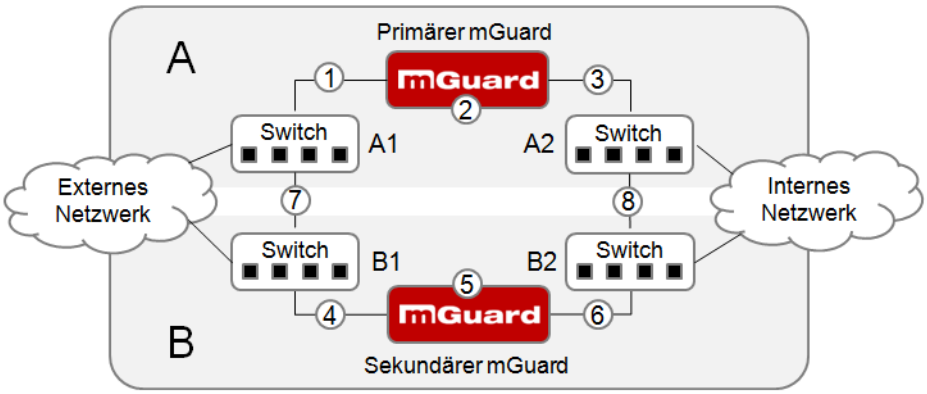


Bild 7-2 Mögliche Fehlerorte (1 ... 8)

In Bild 7-2 wird ein Aufbau gezeigt, der verschiedene Fehlerorte zeigt (unabhängig vom Netzwerk-Modus).

Jeder der beiden mGuards eines Redundanzpaares sitzt in einem unterschiedlichen Bereich (A und B). Der mGuard in Bereich A ist mit seinem externen Ethernet-Interface an Switch A1 und mit seinem internen Ethernet-Interface an Switch A2 angeschlossen. Der mGuard B ist entsprechend mit den Switchen B1 und B2 gekoppelt. Auf diese Weise verbinden die Switche und die mGuards ein externes mit einem internen Ethernet-Netzwerk. Sie stellen die Verbindung her, indem sie Netzwerk-Pakete (im Netzwerk-Modus Router) weiterleiten.

Die Firewall-Redundanz kompensiert die Fehler, die in Bild 7-2 gezeigt werden, wenn nur einer davon zur gleichen Zeit auftritt. Wenn zwei der Fehler gleichzeitig auftreten, werden sie nur kompensiert, wenn sie im selben Bereich (A oder B) auftreten.

Wenn zum Beispiel einer der mGuards aufgrund eines Stromausfalls komplett ausfällt, dann wird das aufgefangen. Ein Ausfall einer Verbindung wird wett gemacht, wenn diese komplett oder nur teilweise ausfällt. Bei einer korrekt eingestellten Konnektivitätsprüfung wird auch eine fehlerhafte Verbindung entdeckt und kompensiert, die durch den Verlust von Datenpaketen oder einer zu hohen Latenzzeit entsteht. Ohne die Konnektivitätsprüfung kann der mGuard nicht entscheiden, welcher Bereich die Fehler verursacht hat.

Ein Ausfall der Verbindung zwischen den Switchen einer Netzwerk-Seite (intern/extern) wird nicht ausgeglichen (7 und 8 in Bild 7-2).

7.1.7 Umgang der Firewall-Redundanz mit extremen Situationen

Die hier beschriebenen Situationen treten nur selten auf.

Wiederherstellung bei einer Netzwerk-Lobotomie

Eine Netzwerk-Lobotomie bezeichnet den Zustand, dass ein Redundanzpaar in zwei unabhängig von einander agierende mGuards aufgesplittet wird. Jeder mGuard kümmert sich in diesem Fall um seine eigenen Tracking-Informationen, da die beiden mGuards nicht mehr über den Layer 2 kommunizieren können. Eine Netzwerk-Lobotomie kann durch eine unglückliche, seltene Kombinationen von Netzwerk-Einstellungen, Netzwerk-Ausfällen und Einstellungen in der Firewall-Redundanz ausgelöst werden.

Bei einer Netzwerk-Lobotomie wird jeder mGuard aktiv. Nachdem die Netzwerk-Lobotomie wieder behoben worden ist, passiert Folgendes: Wenn die mGuards unterschiedliche Prioritäten haben, wird der mit der höheren aktiv und der andere geht in den Bereitschaftszustand. Wenn beide mGuards die gleiche Priorität haben, entscheidet ein Identifier, der mit den Anwesenheitsnachrichten (CARP) mitgeschickt wird, darüber, welcher mGuard aktiv wird.

Während die Netzwerk-Lobotomie besteht, haben beide mGuards ihren Firewall-Zustand selbst verwaltet. Der mGuard, der aktiv wird, behält seinen Zustand. Die Verbindungen des anderen mGuards, die während der Lobotomie bestanden haben, werden fallengelassen.

Failover beim Aufbau von komplexen Verbindungen

Komplexe Verbindungen sind Netzwerk-Protokolle, die auf verschiedenen IP-Verbindungen basieren. Ein Beispiel dafür ist das FTP-Protokoll. Beim FPT-Protokoll baut der Client bei einer TCP-Verbindung einen Kontroll-Kanal auf. Er erwartet, dass der Server eine andere TCP-Verbindung öffnet, über die der Client dann Daten übertragen kann. Während der Kontroll-Kanal am Port 21 des Servers aufgebaut wird, wird der Datenkanal am Port 20 des Servers eingerichtet.

Wenn beim mGuard die entsprechende Verfolgung der Verbindung (Connection Tracking) aktiviert ist (siehe „Erweiterte Einstellungen“ auf Seite 6-153), dann werden solche komplexen Verbindung verfolgt. In diesem Fall braucht der Administrator nur eine Firewall-Regel am mGuard zu erstellen, die es dem Clienten erlaubt, einen Kontroll-Kanal zum FTP-Server aufzubauen. Der mGuard wird automatisch den Aufbau eines Datenkanals durch den Server erlauben, unabhängig davon, ob die Firewall-Regeln das vorsehen.

Das Verfolgen von komplexen Verbindungen ist Bestandteil des Firewall-Zustandsabgleiches. Aber um eine kurze Latenzzeit zu erreichen, leitet der mGuard Netzwerk-Pakete unabhängig vom Update des Firewall-Zustandsabgleichs weiter, das sie selbst verursacht haben.

So kann es für eine ganz kurze Zeit so sein, dass eine Statusänderung für die komplexe Verbindung nicht an den mGuard in Bereitschaft weitergeleitet worden ist, wenn der aktive mGuard ausfällt. In diesem Fall wird die Verfolgung der Verbindung vom mGuard, der nach dem Failover aktiv ist, nicht korrekt fortgeführt. Das kann durch den mGuard nicht korrigiert werden. Dann wird die Datenverbindung zurückgesetzt oder unterbrochen.

Failover beim Aufbau von semi-unidirektionalen Verbindungen

Eine semi-unidirektionale Verbindung bezieht sich auf eine einzelne IP-Verbindung (wie UDP-Verbindungen), bei denen die Daten nur in eine Richtung fließen, nachdem die Verbindung mit einem bidirektionalen Handshake zustande gekommen ist.

Die Daten fließen vom Responder zum Initiator. Der Initiator sendet nur ganz am Anfang Datenpakete.

Das folgende gilt nur für ganz bestimmt Protokolle, die auf UDP basieren. Bei TCP-Verbindungen fließen die Daten immer in beide Richtungen.

Wenn die Firewall des mGuards so gestaltet ist, dass sie nur Datenpakete akzeptiert, die vom Initiator kommen, wird die Firewall alle Antworten darauf per se zulassen. Das ist unabhängig davon, ob dafür eine Firewall-Regel vorhanden ist.

Es ist ein Fall denkbar, dass der mGuard das initierende Datenpaket hat passieren lassen und ausfällt, bevor es den entsprechenden Verbindungs-Eintrag im anderen mGuard gibt. Dann kann es sein, dass der andere mGuard die Antworten zurückweist, sobald er der aktive mGuard geworden ist.

Durch die einseitige Verbindung kann der mGuard diese Situation nicht korrigieren. Als Gegenmaßnahme kann die Firewall so konfiguriert werden, dass sie den Verbindungsaufbau in beide Richtungen zulässt. Normalerweise wird dies bereits über die Protokoll-Layer geregelt und muss nicht extra zugewiesen werden.

Datenpaket-Verlust beim Zustandsabgleich

Wenn beim Zustandsabgleich Datenpakete verloren gehen, dann entdeckt der mGuard dies automatisch und bittet den aktiven mGuard, die Daten erneut zu senden.

Diese Anfrage muss in einer bestimmten Zeit beantwortet werden, sonst erhält der mGuard in Bereitschaft den Status „outdated“ und fragt den aktiven mGuard nach einer kompletten Kopie aller Zustandsinformationen.

Die Antwortzeit wird automatisch aus der Failover-Umschaltzeit berechnet. Sie ist länger als die Zeit für die Anwesenheitsnachrichten (CARP), aber kürzer als die obere Grenze der Failover-Umschaltzeit.

Verlust von Anwesenheitsnachrichten (CARP) bei der Übertragung

Ein einzelner Verlust von Anwesenheitsnachrichten (CARP) wird vom mGuard toleriert, aber nicht für die nachfolgenden Anwesenheitsnachrichten (CARP). Dies gilt für die Verfügbarkeitsprüfung jedes einzelnen Netzwerk-Interfaces, selbst wenn diese gleichzeitig geprüft werden. Daher ist es sehr unwahrscheinlich, dass eine sehr kurze Netzwerk-Unterbrechung die Verfügbarkeitsprüfung scheitern lässt.

Verlust von ICMP-Echo-Requests/Replies bei der Übertragung

ICMP-Echo-Requests oder -Replies sind wichtig für die Konnektivitätsprüfung. Ein Verlust wird grundsätzlich beachtet, aber unter bestimmten Bedingungen wird er toleriert.

Folgende Maßnahmen tragen dazu bei, die Toleranz bei ICMP-Echo-Requests zu erhöhen.

– Wählen Sie im Menü *Redundanz >> Firewall-Redundanz >> Konnektivitätsprüfung* unter dem Punkt **Art der Prüfung** die Auswahl **Mindestens ein Ziel muss antworten** aus.
– Definieren Sie zusätzlich dort eine sekundäre Menge von Zielen. Sie können die Toleranz für den Verlust von ICMP-Echo-Requests noch erhöhen, wenn die Ziele von unzuverlässigen Verbindungen unter beiden Mengen (primär und sekundär) eingetragen werden oder innerhalb einer Menge mehrfach aufgelistet werden.

Wiederherstellen des primären mGuards nach einem Ausfall

Wenn ein Redundanzpaar mit unterschiedlichen Prioritäten definiert ist, wird der sekundäre mGuard bei einem Verbindungsausfall aktiv. Nachdem der Ausfall behoben ist, wird der primäre mGuard wieder aktiv. Der sekundäre mGuard erhält eine Anwesenheitsnachricht (CARP) und geht wieder in den Bereitschaftszustand.

Zustandsabgleich

Wenn der primäre mGuard nach einem Ausfall der internen Netzwerkverbindung wieder aktiv werden soll, hat er möglicherweise eine veraltete Kopie des Datenbestandes der Firewall. Bevor die Verbindung also wieder hergestellt wird, muss dieser Datenbestand aktualisiert werden. Der primäre mGuard sorgt dafür, dass er zunächst eine aktuelle Kopie erhält, bevor er aktiv wird

7.1.8 Zusammenwirken mit anderen Geräten

Virtuelle und reale IP-Adressen

Bei der Firewall-Redundanz im Netzwerk-Modus Router nutzt der mGuard reale IP-Adressen, um mit anderen Netzwerk-Geräten zu kommunizieren.

Virtuelle IP-Adressen werden in diesen beiden Fällen eingesetzt:

– Beim Aufbauen und Betreiben von VPN-Verbindungen werden virtuelle IP-Adressen in Anspruch genommen.
– Wenn die Dienste DNS und NTP entsprechend der Konfiguration genutzt werden, dann werden diese an internen virtuellen IP-Adressen angeboten.

Das Nutzen der realen (Management) IP-Adressen ist besonders wichtig für die Konnektivitäts- und Verfügbarkeitsprüfung. Daher muss die reale (Management) IP-Adresse so konfiguriert werden, dass der mGuard die erforderlichen Verbindungen herstellen kann.

Ein mGuard kommuniziert z. B.

– mit NTP-Servern, um seine Uhrzeit zu synchronisieren
– mit DNS-Servern, um Hostnamen aufzulösen (besonders von VPN-Partnern)
– wenn er seine IP-Adresse bei einem DynDNS-Dienst registrieren will
– wenn er SNMP-Traps sendet will
– wenn er Log-Nachrichten an einen Syslog-Server weiterleiten will
– um eine CRL von einem HTTP(S)-Server herunterzuladen
– um einen Benutzer über einen RADIUS-Server zu authentifizieren
– um über einen HTTPS-Server ein Konfigurationsprofil herunterzuladen.
– um von einem HTTPS-Server ein Firmware-Update herunterzuladen.

Bei der Firewall-Redundanz im Netzwerk-Modus Router müssen Geräte, die am selben LAN-Segment wie das Redundanzpaar angeschlossen sind, ihre jeweiligen virtuellen IP-Adressen als Gateway für ihre Routen nutzen. Wenn diese Geräte dafür die reale IP-Adresse eines der beiden mGuards nutzen würden, würde es funktionieren, bis dieser mGuard ausfällt. Dann aber kann der andere mGuard nicht übernehmen.

Ziele für die Konnektivitätsprüfung

Falls bei der Konnektivitätsprüfung ein Ziel für ICMP-Echo-Requests eingestellt ist, dann müssen diese Anfragen in einer bestimmten Zeit beantwortet werden, auch wenn das Netzwerk noch mit anderen Daten belastet ist. Der Netzwerkpfad zwischen dem Redundanzpaar und diesen Zielen muss so gestaltet sein, dass er in der Lage ist, die ICMP-Antworten auch in Zeiten hoher Last weiterzuleiten. Andernfalls könnte bei einem mGuard fälschlicherweise die Konnektivitätsprüfung scheitern.

Bei der Konnektivitätsprüfung können Ziele für das interne und externe Interface konfiguriert werden (siehe „Konnektivitätsprüfung“ auf Seite 6-245). Es ist wichtig, dass diese Ziele tatsächlich an dem angegebenen Interface angeschlossen sind. Ein ICMP-Echo-Reply kann nicht von einem externen Interface empfangen werden, wenn das Ziel am internen Interface angeschlossen ist (und umgekehrt). Bei einem Wechsel der statischen Routen kann es leicht passieren, dass vergessen wird, die Konfiguration der Ziele entsprechend anzupassen.

Die Ziele für die Konnektivitätsprüfung sollten gut durchdacht sein. Ohne eine Konnektivitätsprüfung können schon zwei Fehler zu einer Netzwerk-Lobotomie führen.

Eine Netzwerk-Lobotomie wird verhindert, wenn die Ziele für beide mGuards identisch sind und alle Ziele auf die Anfrage antworten müssen. Allerdings hat dies den Nachteil, dass die Konnektivitätsprüfung häufiger fehlschlägt, wenn eines der Ziele nicht hoch verfügbar ist.

Im **Netzwerk-Modus Router** empfehlen wir ein hoch verfügbares Gerät als Ziel am externen Interface zu definieren. Das kann das Standard-Gateway für das Redundanzpaar sein, z. B. ein virtueller Router, der aus zwei unabhängigen Geräten besteht. Am internen Interface sollte dann entweder kein Ziel definiert sein oder eine Auswahl von Zielen.

Bei der Konstellation, dass Sie bei einem Redundanzpaar als Standard-Gateway einen virtuellen Router einsetzen, der aus zwei unabhängigen Geräten besteht, gibt es noch etwas zu beachten. Wenn diese Geräte VRRP nutzen, um ihre virtuelle IP zu synchronisieren, dann könnte eine Netzwerk-Lobotomie die virtuelle IP dieses Routers in zwei identische Kopien aufsplitten. Möglicherweise nutzen diese Router ein dynamisches Routing Protokoll und nur einer darf für die Datenströme des Netzwerkes ausgewählt werden, das durch die mGuards überwacht wird. Nur dieser Router sollte die virtuelle IP behalten. Andernfalls können Sie in der Konnektivitätsprüfung Ziele definieren, die über diese Route erreichbar sind. Die virtuelle IP-Adresse des Routers wäre dann kein sinnvolles Ziel.

Redundanzverbund

Sie können innerhalb eines LAN-Segmentes mehrere Redundanzpaare anschließen (Redundanzverbund). Für jede virtuelle Existenz des Redundanzpaares legen Sie einen Wert als Identifier fest (über die Router-ID). Solange diese Identifier unterschiedlich sind, stören sich die Redundanzpaare nicht untereinander.

Datenverkehr

Eine hohe **Latenzzeit** im Netzwerk, das für Updates des Zustandsabgleichs genutzt wird oder ein ernster Datenverlust in diesem Netzwerk führen dazu, dass der mGuard in Bereitschaft in den „outdated“ Zustand geht. Solange nicht mehr als zwei aufeinander folgende Updates verloren gehen, kommt es aber nicht dazu. Denn der mGuard in Bereitschaft fordert automatisch eine Wiederholung des Updates ein. Die Anforderungen an die Latenzzeit sind dieselben, wie unter „Umschaltzeit im Fehlerfall“ auf Seite 7-5 beschrieben.

Ausreichende Bandbreite

Der Datenverkehr, der durch die Konnektivitäts- und Verfügbarkeitsprüfung und den Zustandsabgleich entsteht, verbraucht Bandbreite im Netzwerk. Außerdem erzeugt die Konnektivitätsprüfung einen rechnerischen Aufwand. Es gibt mehrere Methoden, dies zu verringern oder ganz aufzuheben.

Wenn ein Einfluss auf andere Geräte nicht akzeptabel ist,

– dann muss die Konnektivitätsprüfung entweder deaktiviert werden oder sie darf sich nur auf die reale IP-Adresse des anderen mGuards beziehen.
– dann muss der Datenverkehr durch die Verfügbarkeitsprüfung und den Zustandsabgleich in ein separates VLAN verschoben werden.
– dann müssen Switche genutzt werden, die es erlauben, VLANs zu splitten.

Dediziertes Interface

Der **mGuard centerport** unterstützt ein **dediziertes Interface**. Das ist eine reservierte direkte Ethernet-Schnittstelle oder ein dediziertes LAN-Segment, über das der Zustandsabgleich gesendet wird. Auf diese Weise ist die Last sogar physikalisch vom internen LAN-Segment getrennt.

X.509-Zertifikate für den SSH-Clienten

Der mGuard unterstützt die Authentifizierung von SSH-Clienten mit Hilfe von X.509-Zertifikaten. Es reicht aus, CA-Zertifikate zu konfigurieren, die für einen Aufbau und die Gültigkeitsprüfung einer Zertifikatskette notwendig sind. Diese Zertifikatskette muss dazu zwischen dem CA-Zertifikat beim mGuard und dem X.509.Zertifikat, das beim SSH-Clienten vorgezeigt wird, bestehen (siehe „Shell-Zugang“ auf Seite 6-12).

Wenn der Gültigkeitszeitraum des Client-Zertifikats vom mGuard geprüft wird (siehe „Zertifikatseinstellungen“ auf Seite 6-134), dann müssen irgend wann neue CA-Zertifikate am mGuard konfiguriert werden. Dies muss geschehen, bevor die SSH-Clienten ihre neuen Client-Zertifikate nutzen.

Wenn die CRL-Prüfung eingeschaltet ist (unter *Authentifizierung >> Zertifikate >> Zertifikatseinstellungen),* dann muss eine URL pro CA-Zertifikat vorgehalten werden, an der die entsprechende CRL verfügbar ist. Die URL und CRL müssen veröffentlicht werden, bevor der mGuard die CA-Zertifikate nutzt, um die Gültigkeit der von den VPN-Partnern vorgezeigten Zertifikate zu bestätigen.

7.1.9 Übertragungsleistung der Firewall-Redundanz

Die Werte gelten für den Netzwerk-Modus Router, wenn der Datenverkehr für den Zustandsabgleich unverschlüsselt übertragen wird. Wenn die hier beschriebene Übertragungsleistung überschritten wird, kann im Fehlerfall eine längere Umschaltzeiten entstehen, als eingestellt ist.

Plattform		Übertragungsleistung der Firewall-Redundanz
mGuard centerport		1500 MBit/s, bidirektional[1], nicht mehr als 400000 Frames/s
mGuard industrial rs mGuard smart mGuard core mGuard pci mGuard blade mGuard delta EAGLE mGuard	mit 533 MHz	150 MBit/s[1], bidirektional, nicht mehr als 12750 Frames/s
mGuard industrial rs mGuard smart mGuard core mGuard pci mGuard blade mGuard delta EAGLE mGuard	mit 266 MHz	62 MBit/s, bidirektional[1], nicht mehr als 5250 Frames/s
mGuard rs4000 mGuard smart[2] mGuard core[2] mGuard pci[2] SD mGuard delta[2]		62 MBit/s, bidirektional[1], nicht mehr als 5250 Frames/s

1 Bidirektional umfasst den Traffic in beide Richtungen. Zum Beispiel bedeutet 1500 MBit/s, dass in jede Richtung 750 MBit/s weitergeleitet werden.

Failover-Umschaltzeit

Sie können die Umschaltzeit im Fehlerfall auf 1, 3 oder 10 Sekunden einstellen.

Die Obergrenze von 1 Sekunde wird derzeit nur vom mGuard centerport auch unter hoher Auslastung eingehalten.

7.1.10 Grenzen der Firewall-Redundanz

- Im **Netzwerk-Modus Router** wird die Firewall-Redundanz nur mit dem Modus „statisch“ unterstützt.
- Ein Zugang zum mGuard über die **Management-Protokolle** HTTPS, SNMP und SSH ist nur mit einer realen IP-Adresse eines jeden mGuards möglich. Zugriffe auf virtuelle Adressen werden zurückgewiesen.
- Die folgenden **Features** können mit der Firewall-Redundanz **nicht benutzt** werden.
  - ein sekundäres externes Ethernet-Interface,
  - ein DHCP-Server,
  - ein DHCP-Relay,
  - ein SEC-Stick-Server,
  - eine Benutzer-Firewall und
  - das CIFS-Integrity-Monitoring.
- Das **Redundanzpaar muss identisch konfiguriert** werden. Beachten Sie dies bei der Einstellung von:
  - NAT-Einstellungen (Masquerading, Port-Weiterleitung und 1:1-NAT)
  - Flood-Protection
  - Paketfilter (Firewall-Regeln, MAC-Filter, Erweiterte Einstellungen)
  - den Queues und den Regeln für die QoS
- Nach einer **Netzwerk-Lobotomie** sind möglicherweise einige Netzwerkverbindungen unterbrochen. (Siehe „Wiederherstellung bei einer Netzwerk-Lobotomie“ auf Seite 7-8).
- Nach einem Failover können s**emi-unidirektionale oder komplexe Verbindungen** unterbrochen sein, die genau in der Sekunde vor dem Failover aufgebaut worden sind. (Siehe „Failover beim Aufbau von komplexen Verbindungen“ auf Seite 7-8 und „Failover beim Aufbau von semi-unidirektionalen Verbindungen“ auf Seite 7-8.)
- Die Firewall-Redundanz unterstützt nicht den **mGuard pci im Treiber-Modus**.
- Der Zustandsabgleich repliziert keine Connection-Tracking-Einträge für **ICMP-Echo-Requests**, die vom mGuard weitergeleitet werden. Deshalb können ICMP-Echo-Replies entsprechend der Firewall-Regeln fallen gelassen werden, wenn sie den mGuard erst erreichen, wenn der Failover abgeschlossen ist. Beachten Sie, dass ICMP-Echo-Replies nicht dazu geeignet sind, die Failover-Umschaltzeit zu messen.
- **Masquerading** wird dadurch ausgeführt, dass der Sender hinter der ersten virtuellen IP-Adresse bzw. der ersten internen IP-Adresse verborgen wird. Das unterscheidet sich von dem Masquerading des mGuards ohne Firewall-Redundanz. Ohne aktivierte Firewall-Redundanz wird in einer Routing-Tabelle festgelegt, hinter welcher externen bzw. internen IP-Adresse der Sender verborgen wird.

7.2 VPN-Redundanz

Die VPN-Redundanz kann nur zusammen mit der Firewall-Redundanz genutzt werden.

Das Konzept ist genauso wie bei der Firewall-Redundanz. Um einen Fehler im Umfeld aufzufangen, wird die Aktivität von dem aktiven mGuard auf einen mGuard in Bereitschaft übertragen.

Zu jedem Zeitpunkt betreibt mindestens ein mGuard des Redundanzpaares die VPN-Verbindung, außer wenn eine Netzwerk-Lobotomie vorliegt.

Grundbedingungen für die VPN-Redundanz

Für die VPN-Redundanz gibt es keine eigenen Variablen. Es gibt gegenwärtig kein eigenes Menü in der Benutzeroberfläche, sondern sie wird mit der Firewall-Redundanz zusammen aktiviert.

Voraussetzung für die VPN-Redundanz ist eine entsprechende Lizenz, die Sie auf dem mGuard installieren müssen.

Da für die VPN-Redundanz der Aufbau von VPN-Verbindungen notwendig ist, brauchen Sie zusätzlich eine entsprechende VPN-Lizenz.

Wenn Sie nur die Lizenz für die Firewall-Redundanz haben und VPN-Verbindungen installiert sind, können Sie keine VPN-Redundanz aktivieren. Sie erhalten eine Fehlermeldung, sobald Sie die Firewall-Redundanz nutzen wollen.

Nur baugleiche mGuards können ein Redundanzpaar bilden.

7.2.1 Komponenten der VPN-Redundanz

Die Komponenten der VPN-Redundanz sind die gleichen, die bei der Firewall-Redundanz beschrieben worden sind. Zusätzlich gibt es noch eine weitere Komponente: der VPN-Zustandsabgleich. Einige wenige Komponenten sind für die VPN-Redundanz leicht erweitert. Aber die Konnektivitäts- und Verfügbarkeitsprüfung und der Zustandsabgleich von der Firewall funktionieren auf die gleiche Weise.

VPN-Zustandsabgleich

Der mGuard unterstützt die Konfiguration von Firewall-Regeln für die VPN-Verbindung.

Der VPN-Zustandsabgleich verfolgt den Zustand der verschiedenen VPN-Verbindungen am aktiven mGuard. Er sorgt dafür, dass der mGuard in Bereitschaft eine zur Zeit gültige Kopie der VPN-Zustand-Datenbank erhält.

Wie bei dem Zustandsabgleich der Firewall sendet er Updates vom aktiven mGuard zum mGuard in Bereitschaft. Auf Anfrage vom mGuard in Bereitschaft versendet der aktive mGuard einen kompletten Satz aller Zustandsinformationen.

Dediziertes Interface (mGuard centerport)

Beim mGuard centerport können Sie das dritte Ethernet-Interface für den VPN-Zustandsabgleich fest zuordnen.

Wie bei dem Zustandsabgleich der Firewall wird der Datenverkehr für den VPN-Zustandsabgleich für das dedizierte Interface übertragen, wenn eine Variable gesetzt wird. Stellen Sie unter *Redundanz >> Firewall-Redundanz >> Redundanz* das *Interface, das zum Zustandsabgleich verwendet wird* auf **Dediziertes Interface**.

Aufbau von VPN-Verbindungen

Mit der VPN-Redundanz wird das virtuelle Netzwerk-Interface für einen zusätzlichen Zweck genutzt: Es wird verwendet, um VPN-Verbindungen aufzubauen, zu akzeptieren und zu betreiben. Der mGuard lauscht nur auf der ersten virtuellen IP-Adresse.

Im Netzwerk-Modus Router hört er an der ersten externen und internen virtuellen IP-Adresse zu.

Statusüberwachung

Die Statusüberwachung überwacht den VPN-Zustandsabgleich genauso wie den der Firewall.

Statusanzeige

Die Statusanzeige hält zusätzliche detaillierte Information über den Status des VPN-Zustandsabgleichs bereit. Dieser steht direkt neben den Informationen zum Zustandsabgleich der Firewall.

Als Nebeneffekt ist die Statusanzeige der VPN-Verbindung auch auf dem mGuard in Bereitschaft zu sehen. Deshalb finden Sie den replizierte Inhalt der VPN-Zustands-Datenbank unter der normalen Statusanzeige für die VPN-Verbindung (unter *IPsec VPN* >> *IPsec Status)*.

Unter der Statusanzeige für die Firewall-Redundanz *(Redundanz* >> *Firewall-Redundanz Status* >> *Redundanzstatus)* wird nur der Status des Abgleichsvorgangs gezeigt.

7.2.2 Zusammenarbeit der VPN-Redundanz Komponenten

Die einzelnen Komponenten arbeiten auf die gleiche Weise zusammen, wie bei der Firewall-Redundanz. Der VPN-Zustandsabgleich wird ebenfalls durch die Statusüberwachung gesteuert, der Status wird festgehalten und es werden Updates gesendet.

Damit die Zustände eintreten, müssen bestimmte Bedingungen erfüllt werden. Der VPN-Zustandsabgleich wird damit mit berücksichtigt.

7.2.3 Fehlerkompensation durch die VPN-Redundanz

Die VPN-Redundanz kompensiert genau die gleichen Fehler wie die Firewall-Redundanz (siehe „Fehlerkompensation durch die Firewall-Redundanz“ auf Seite 7-7).

Allerdings kann bei einer Netzwerk-Lobotomie der VPN-Teil die anderen VPN-Gateways stören. Die von einander unabhängigen mGuards haben dann die gleiche virtuelle IP-Adresse um mit den VPN-Partnern zu kommunizieren. Das kann dazu führen, dass die VPN-Verbindungen in schneller Folge auf- und abgebaut werden.

7.2.4 Variablen für die VPN-Redundanz erstellen

Bei passenden Lizenzschlüsseln wird die VPN-Redundanz automatisch aktiviert, wenn Sie die Firewall-Redundanz aktivieren. Dies geschieht, sobald Sie im Menü *Redundanz >> Firewall-Redundanz >> Redundanz* den Punkt *Aktiviere Redundanz* auf **Ja** stellen.

Es gibt kein eigenes Menü für die VPN-Redundanz. Die vorhandenen Firewall-Redundanz-Variablen werden erweitert.

Tabelle 7-3 Erweiterte Funktionen bei aktivierter VPN-Redundanz

Redundanz >> Firewall-Redundanz >> Redundanz		
Allgemein	**Aktiviere Redundanz**	Die Firewall-Redundanz und die VPN-Redundanz werden aktiviert oder deaktiviert.
Virtuelle Interfaces	**Externe virtuelle IP-Adressen**	Nur im Netzwerk-Modus Router Der mGuard nutzt die erste externe virtuelle IP-Adresse als Adresse von der er IKE-Nachrichten sendet und erhält. Die externe virtuelle IP-Adresse wird anstelle der realen primäre IP-Adresse des externen Netzwerk-Interfaces genutzt. Der mGuard verwendet die reale IP-Adresse nicht länger, um IKE-Nachrichten zu senden oder zu beantworten. Der ESP-Datenverkehr wird ähnlich gehandhabt, allerdings wird er ebenfalls von der realen IP-Adresse akzeptiert und bearbeitet.
	Interne virtuelle IP-Adressen	Wie unter *Externe virtuelle IP-Adressen* beschrieben, aber für die internen virtuellen IP-Adressen.

7.2.5 Voraussetzungen für die VPN-Redundanz

– Die VPN-Redundanz kann nur aktiviert werden, wenn ein **Lizenzschlüssel** für die VPN-Redundanz installiert ist und eine VPN-Verbindung aktiviert ist.
– **Nur bei mGuard rs4000 und mGuard industrial rs**
  Wenn eine VPN-Verbindung über einen **VPN-Schalter** gesteuert wird, dann kann die VPN-Redundanz nicht aktiviert werden.
  (unter: *IPsec VPN* >> *Global* >> *Optionen* >> *VPN-Schalter*)

Beim VPN-Zustandsabgleich wird kontinuierlich der Zustand der VPN-Verbindung vom aktiven auf den mGuard in Bereitschaft übertragen, damit dieser im Fehlerfall eine tatsächliche Kopie hat. Die einzige Ausnahme dazu ist der Status des IPsec Replay Windows. Änderungen dort werden nur von Zeit zur Zeit übertragen.

Der Umfang des Datenverkehrs für den Zustandsabgleich hängt nicht von dem Datenverkehr ab, der über die VPN-Kanäle geleitet wird. Das Datenvolumen für den Zustandsabgleich wird durch verschiedene Parameter bestimmt, die für ISAKMP SAs und IPsec SAs vergeben werden.

7.2.6 Umgang der VPN-Redundanz mit extremen Situationen

Die Bedingungen, die unter „Umgang der Firewall-Redundanz mit extremen Situationen“ auf Seite 7-8 aufgeführt sind, gelten auch für die VPN-Redundanz. Sie gelten auch dann, wenn der mGuard ausschließlich dafür genutzt wird, VPN-Verbindungen weiterzuleiten. Der mGuard leitet die Datenströme über die VPN-Kanäle weiter und sortiert fehlerhafte Pakete aus, unabhängig davon, ob für die VPN-Verbindungen Firewall-Regeln definiert sind oder nicht.

Ein Fehler unterbricht den laufenden Datenverkehr

Wenn ein Fehler den Datenverkehr unterbricht, der über die VPN-Kanäle läuft, ist das eine extreme Situation. In diesem Fall ist der IPsec-Datenverkehr für kurze Zeit für Replay-Attacken anfällig. (Eine Replay-Attacke ist die Wiederholung bereits gesendeter verschlüsselter Datenpakete mit Hilfe von Kopien, die ein Angreifer aufbewahrt hat.) Der Datenverkehr wird mit Hilfe von Sequenznummern geschützt. Für jede Richtung eines IPsec-Kanals werden unabhängige Sequenznummern verwendet. Der mGuard lässt ESP-Pakete fallen, die die gleiche Sequenznummer haben, wie ein Paket, das der mGuard für einen bestimmten IPsec-Kanal bereits entschlüsselt hat. Dieser Mechanismus wird **IPsec-Replay-Window** genannt.

Das IPsec-Relay-Window wird beim Zustandsabgleich nur von Zeit zur Zeit repliziert, da es zu viele Ressourcen bindet. So kann es vorkommen, dass nach einem Failover der aktive mGuard ein veraltetes IPsec-Replay-Window hat. Auf diese Weise ist ein Angriff möglich, bis der echte VPN-Partner das nächste ESP-Paket für die entsprechenden IPsec SA sendet oder bis der IPsec SA erneuert wird.

Um eine zu geringe Sequenznummer bei dem ausgehenden IPsec SA zu verhindern, addiert die VPN-Redundanz zu jeder ausgehenden IPsec SA einen konstanten Wert zur Sequenznummer dazu, bevor der mGuard aktiv wird. Dieser Wert ist so berechnet, dass er zu der maximalen Anzahl an Datenpaketen passt, die durch den VPN-Kanal während der maximalen Failover-Umschaltzeit gesendet werden können. Im schlimmsten Fall (bei einem Gigabit-Ethernet und einer Umschaltzeit von 10 Sekunden) sind das 0,5 % einer IPsec Sequenz. Im besten Fall ist es nur ein Promille.

Das Addieren des konstanten Wertes zur Sequenznummer verhindert, dass eine Sequenznummer versehentlich wiederverwendet wird, die bereits vom anderen mGuard verwendet wurde, kurz bevor dieser ausgefallen ist. Ein weiterer Effekt ist, dass die ESP-Pakete, die vom vorher aktiven mGuard gesendet wurden, vom VPN-Partner fallengelassen werden, wenn neue ESP-Pakete vom nun aktiven mGuard früher ankommen. Dafür ist es aber notwendig, dass die Latenzzeit im Netzwerk sich von der Failover-Umschaltzeit unterscheidet.

Ein Fehler unterbricht den ersten Aufbau von ISAKMP SA oder IPsec SA

Wenn ein Fehler den ersten Aufbau von ISAKMP SA oder IPsec SA unterbricht, dann kann der mGuard in Bereitschaft den Aufbau nahtlos fortsetzen, da der Status der SA synchron repliziert wird. Der Response auf eine IKE-Nachricht wird nur vom aktiven mGuard gesendet, nachdem der mGuard in Bereitschaft den Empfang des entsprechenden Updates des VPN-Zustandsabgleichs bestätigt hat.

Wenn ein mGuard aktiv wird, wiederholt er sofort die letzte IKE-Nachricht, die vom vorher aktiven mGuard hätte gesendet werden müssen. Damit wird der Fall kompensiert, dass der vorher aktive mGuard zwar den Zustandabgleich noch gesendet hat, aber ausgefallen ist, bevor er die entsprechende IKE-Nachricht senden konnte.

Auf diese Weise wird während eines Failovers der Aufbau von ISAKMP SA oder IPsec SA nur um die Zeit verzögert, die für die Umschaltung benötigt wird.

Ein Fehler unterbricht die Erneuerung einer ISAKMP SA

Wenn ein Fehler die Erneuerung einer ISAKMP SA unterbricht, wird das auf die gleiche Weise ausgeglichen, wie dem ersten Aufbau einer SA. Außerdem wird die alte ISAKMP SA für die Dead Peer Detection beibehalten, bis die Erneuerung der ISAKMP SA abgeschlossen ist.

Ein Fehler unterbricht die Erneuerung einer IPsec SA

Wenn ein Fehler die Erneuerung einer IPsec SA unterbricht, wird das auf die gleiche Weise ausgeglichen, wie dem ersten Aufbau einer SA. Solange die Erneuerung der ISAKMP SA noch nicht abgeschlossen ist, werden die alten ein- und ausgehende IPsec SAs beibehalten, bis der VPN-Partner den Wechsel bemerkt hat.

Der VPN-Zustandsabgleich sorgt dafür, dass die alten IPsec SA beibehalten werden, solange der mGuard in Bereitschaft ist. Wenn er dann aktiv wird, ist sichergestellt, dass er ohne weitere Aktionen mit der Ver- und Entschlüsselung des Datenverkehrs fortfahren kann.

Datenpaket-Verlust beim VPN-Zustandsabgleich

Der Zustandsabgleich ist gegen den Verlust von einem von zwei aufeinanderfolgenden Update-Paketen resistent. Wenn mehr Datenpakete verloren gehen, kann es zu einer längeren Umschaltzeit im Fehlerfall kommen.

Der mGuard in Bereitschaft hat ein veraltetes Maschinenzertifikat

Es kann vorkommen, dass X.509-Zertifikate und private Schlüssel geändert werden müssen, die von einem Redundanzpaar genutzt werden, um sich selbst als VPN-Partner zu authentifizieren. Die Kombination aus privatem Schlüssel und Zertifikat wird im Folgenden Maschinenzertifikat genannt.

Jeder mGuard eines Redundanzpaares muss neu konfiguriert werden, um das Maschinenzertifikat zu tauschen. Und beide mGuards benötigen das gleiche Zertifikat, um aus der Sicht ihrer VPN-Partner als die selbe virtuelle VPN-Appliance zu erscheinen.

Da jeder mGuard einzeln neu konfiguriert wird, kann es für eine kurze Zeit vorkommen, dass der mGuard in Bereitschaft ein veraltetes Maschinenzertifikat besitzt.

Wenn der mGuard in Bereitschaft genau in dem Augenblick aktiv wird, in dem ISAKMP SAs aufgebaut werden, kann es das mit einem veralteten Maschinenzertifikat nicht fortsetzen,

Als Gegenmaßnahme repliziert der VPN-Zustandsabgleich das Maschinenzertifikat vom aktiven mGuards zu dem mGuard in Bereitschaft. Bei einem Failover wird der mGuard in Bereitschaft dieses nur benutzen, um den bereits begonnenen Aufbau der ISAKMP SAs abzuschließen.

Wenn der mGuard in Bereitschaft nach einem Failover neue ISAKMP SAs aufbaut, wird er das noch konfigurierte Maschinenzertifikat nutzen.

Der VPN-Zustandsabgleich sorgt also für die Replizierung der Maschinenzertifikate, die gerade benutzt werden. Aber es repliziert nicht die Konfiguration selbst.

Der mGuard in Bereitschaft hat einen veralteten Pre-Shared-Key (PSK)

Ebenso müssen Preshared-Keys (PSK) zur Authentifizierung von VPN-Partnern manchmal erneuert werden. Für eine kurze Zeit können also die redundanten mGuards einen unterschiedlichen PSK haben. In diesem Fall kann nur einer der mGuards eine VPN-Verbindung aufbauen, da die meisten VPN-Partner nur einen PSK akzeptieren. Der mGuard hat hierfür keine Gegenmaßnahme.

Wir empfehlen daher, X.509-Zertifikate anstelle von PSKs zu benutzen.

Wenn der VPN-Zustandsabgleich die PSKs längere Zeit auf den mGuard in Bereitschaft repliziert, dann verdeckt dies eine fehlerhafte Konfiguration für eine längere Zeit und ist schwer zu entdecken.

7.2.7 Zusammenwirken mit anderen Geräten

Auflösen von Hostnamen

Wenn Hostnamen als VPN-Gateways konfiguriert sind, dann müssen die mGuards eines Redundanzpaares in der Lage sein, die Hostnamen zu selben IP-Adresse aufzulösen. Dies gilt besonders, wenn *DynDNS-Überwachung* (siehe *Seite 6-188*) aktiviert ist.

Wenn die Hostnamen von dem mGuard in Bereitschaft auf eine andere IP-Adresse aufgelöst werden, dann wird nach einem Failover die VPN-Verbindung zu diesem Host abgebrochen. Die VPN-Verbindung wird an einer anderen IP-Adresse wieder aufgebaut. Dies passiert direkt nach dem Failover. Es kann aber zu einer kurzen Verzögerung kommen, die u. a. davon abhängt, was unter *DynDNS-Überwachung* als Wert für das *Abfrageintervall (Sekunden)* eingetragen ist.

Veraltetes IPsec-Replay-Window

Der IPsec-Datenverkehr ist gegen einen unauthorisierten Zugriff geschützt. Dazu wird jeder IPsec-Kanal mit einer unanhängigen Sequenznummer versehen. Der mGuard lässt ESP-Pakete fallen, die die gleiche Sequenznummer haben, wie ein Paket, das der mGuard für einen bestimmten IPsec-Kanal bereits entschlüsselt hat. Dieser Mechanismus wird **IPsec-Replay-Window** genannt. Es verhindert einen Replay-Angriff, bei dem der Angreifer zuvor aufgezeichnete Daten sendet, um etwa eine fremde Identität vorzutäuschen.

Das IPsec-Relay-Window wird beim Zustandsabgleich nur von Zeit zur Zeit repliziert, da es zu viele Ressourcen bindet. So kann es vorkommen, dass nach einem Failover der aktive mGuard ein veraltetes IPsec-Replay-Window hat. Auf diese Weise ist kurzzeitig eine Re-

play-Angriff möglich, bis der echte VPN-Partner das nächste ESP-Paket für die entsprechenden IPsec SA sendet oder bis der IPsec SA erneuert wird. Allerdings müsste ein vollständiger Traffic gekapert werden.

Dead Peer Detection

Sie müssen bei der Dead Peer Detection einen Punkt beachten.

Stellen Sie bei der Dead Peer Detection einen höheren Timeout ein als die obere Grenze der *Umschaltzeit im Fehlerfall* beim Redundanzpaar.

(unter: *IPsec VPN >> Verbindungen >> Editieren >> IKE-Optionen , Verzögerung bis zur nächsten Anfrage nach einem Lebenszeichen)*

Andernfalls könnten die VPN-Partner das Redundanzpaar für tot halten, obwohl sie nur mit dem Failover beschäftigt sind.

Datenverkehr

Eine hohe Latenzzeit im Netzwerk, das für die Updates des Zustandsabgleichs genutzt wird führt dazu, dass der mGuard in Bereitschaft in den „outdated“ Zustand geht. Das Gleiche geschieht bei einem ernsten Datenverlust in diesem Netzwerk.

Solange nicht mehr als zwei aufeinander folgende Updates verloren gehen, kommt es aber nicht dazu. Denn der mGuard in Bereitschaft fordert automatisch eine Wiederholung des Updates ein. Die Anforderungen an die Latenzzeit sind dieselben, wie unter „Umschaltzeit im Fehlerfall“ auf Seite 7-5 beschrieben.

Reale IP-Adressen

VPN-Partner dürfen keinen ESP-Traffic an die reale IP-Adresse des Redundanzpaares senden. VPN-Partner müssen immer die virtuelle IP-Adresse des Redundanzpaares nutzen, um dorthin IKE-Nachrichten oder ESP-Traffic zu senden.

7.2.8 Übertragungsleistung der VPN-Redundanz

Die Werte gelten für den Netzwerk-Modus Router, wenn der Datenverkehr für den Zustandsabgleich unverschlüsselt übertragen wird. Wenn die hier beschriebene Übertragungsleistung überschritten wird, kann im Fehlerfall eine längere Umschaltzeiten entstehen, als eingestellt ist.

Plattform		Übertragungsleistung der Firewall-Redundanz
mGuard centerport		220 MBit/s, bidirektional[1], nicht mehr als 60000 Frames/s
mGuard industrial rs mGuard smart mGuard core mGuard pci mGuard blade mGuard delta EAGLE mGuard	mit 533 MHz	50 MBit/s, bidirektional[1], nicht mehr als 5500 Frames/s
mGuard industrial rs mGuard smart mGuard core mGuard pci mGuard blade mGuard delta EAGLE mGuard	mit 266 MHz	17 MBit/s, bidirektional[1], nicht mehr als 2300 Frames/s
mGuard rs4000 mGuard smart[2] mGuard core[2] mGuard pci[2] SD mGuard delta[2]		17 MBit/s, bidirektional[1], nicht mehr als 2300 Frames/s

1 Bidirektional umfasst den Traffic in beide Richtungen. Zum Beispiel bedeutet 1500 MBit/s, dass in jede Richtung 750 MBit/s weitergeleitet werden.

Failover-Umschaltzeit

Sie können die Umschaltzeit im Fehlerfall auf 1, 3 oder 10 Sekunden einstellen.

Die Obergrenze von 1 Sekunde wird derzeit nur vom mGuard centerport auch unter hoher Auslastung eingehalten.

7.2.9 Grenzen der VPN-Redundanz

Die Grenzen die für die Firewall-Redundanz dokumentiert sind, gelten auf für die VPN-Redundanz (siehe „Grenzen der Firewall-Redundanz“ auf Seite 7-14). Es gibt zusätzlich weitere Einschränkungen.

- Das Redundanzpaar muss bei diesen Punkten **identisch konfiguriert** sein:
  - bei den allgemeinen VPN-Einstellungen und
  - jeder einzelnen VPN-Verbindung.
- Der mGuard akzeptiert VPN-Verbindungen nur an der **ersten virtuellen IP-Adresse**.
  - Für den Netzwerk-Modus Router meint dies die erste interne und die erste externe IP-Adresse.
- Die folgenden **Features** können mit der VPN-Redundanz **nicht genutzt** werden:
  - Die dynamische Aktivierung der VPN-Verbindungen mit Hilfe eines VPN-Schalters oder über die Kommandos des CGI-Skriptes nph-vpn.cgi (nur beim mGuard rs4000/rs2000 und mGuard industrial rs).
  - Das Archivieren von Diagnose-Meldungen für VPN-Verbindungen.
- VPN-Verbindungen werden nur im Tunnel-Modus unterstützt. VPN-Verbindungen im Transport-Modus werden nicht hinreichend berücksichtigt.
- Die obere Grenze der **Failover-Umschaltzeit** gilt nicht für Verbindungen, die mit **TCP gekapselt** sind. Solche Verbindungen werden bei einem Failover für eine längere Zeit unterbrochen. Nach jedem Failover müssen die gekapselten TPC-Verbindungen von der initiierenden Seite neu aufgebaut werden. Wenn der Failover auf der initiierenden Seite passiert ist, können sie sofort nach der Übernahme starten. Aber wenn der Failover auf der antwortenden Seite liegt, muss der Initiator erst die Unterbrechung entdecken und kann sie dann neu aufbauen.
- Die VPN-Redundanz unterstützt **Masquerading** auf die gleiche Weise, wie ohne VPN-Redundanz. Dies gilt, wenn ein Redundanzpaar durch ein NAT-Gateway mit einer dynamischen IP-Adresse maskiert wird.

  Zum Beispiel kann ein Redundanzpaar hinter einem DSL-Router versteckt werden, der das Redundanzpaar mit einer offiziellen IP-Adresse maskiert. Dieser DSL-Router leitet den IPsec-Datenverkehr (IKE und ESP, UDP-Ports 500 und 4500) zu den virtuellen IP-Adressen weiter. Wenn sich die dynamische IP-Adresse ändert, werden alle aktiven VPN-Verbindungen, die über das NAT-Gateway fließen, wieder aufgebaut.

  Für den Wiederaufbau sorgt die Dead Peer Detection (DPD) mit der dafür konfigurierten Zeit. Dieser Effekt liegt außerhalb des Einflussbereichs des mGuards.
- Die Redundanz-Funktion des mGuards unterstützt keine **Pfad-Redundanz**. Die Pfad-Redundanz kann über andere Maßnahmen erreicht werden, z. B. über ein Routerpaar. Dieses Routerpaar wird auf der einen virtuellen Seite von den mGuards gesehen, während auf der anderen Seite jeder der Router unterschiedliche Verbindungen hat.

  Eine Pfad-Redundanz darf keine NAT-Mechanismen wie Masquerading nutzen, um die virtuellen IP-Adressen der mGuards zu verbergen. Andernfalls wird eine Migration von einem Pfad zum anderen die IP-Adressen, mit denen das Redundanzpaar maskiert ist, ändern. Das würde dazu führen, dass alle VPN-Verbindungen (alle ISAKMP SAs und alle IPsec SAs) wieder aufgebaut werden müssen.

  Für den Wiederaufbau sorgt die Dead Peer Detection (DPD) mit der dafür konfigurierten Zeit. Dieser Effekt liegt außerhalb des Einflussbereichs des mGuards.
- Bei einer Pfad-Redundanz, die durch eine Netzwerk-Lobotomie ausgelöst wird, werden die VPN-Verbindungen nicht länger unterstützt. Eine Netzwerk-Lobotomie muss wenn möglich verhindert werden.

X.509-Zertifikate für die VPN-Authentification

Der mGuard unterstützt die Verwendung von X.509-Zertifikaten beim Aufbau von VPN-Verbindungen. Dies wird ausführlich unter „Authentifizierung“ auf Seite 6-204 beschrieben.

Es gib aber einige Besonderheiten, wenn X.509-Zertifikate zur Authentifizierung von VPN-Verbindungen in Kombination mit Firewall- und VPN-Redundanz genutzt werden.

Maschinen-Zertifikate wechseln

Ein Redundanzpaar kann so konfiguriert werden, dass es gemeinsam einen X.509-Zertifikat und einen entsprechenden privaten Schlüssel nutzt, um sich selbst als virtuelle einzelne VPN-Instanz bei einem entfernten VPN-Partner zu identifizieren.

Diese X.509-Zertifikate müssen regelmäßig erneuert werden. Wenn der VPN-Partner so eingestellt ist, dass er den Gültigkeitszeitraum der Zertifikate prüft, müssen diese erneuert werden, bevor ihre Gültigkeit erlischt (siehe „Zertifikatseinstellungen“ auf Seite 6-134).

Wenn ein Maschinenzertifikat ersetzt wird, werden alle VPN-Verbindung, die es nutzen, vom mGuard neu gestartet. Währendessen kann der mGuard für eine bestimmte Zeit über die betroffenen VPN-Verbindungen keine Daten weiterleiten. Die Zeit hängt von der Anzahl der betroffenen VPN-Verbindungen, der Leistungsfähigkeit des mGuards und der VPN-Partner und der Latenzzeit der mGuards im Netzwerk ab.

Wenn dies für die Redundanz nicht tragbar seien sollte, müssten die VPN-Partner eines Redundanzpaares so konfiguriert werden, dass sie alle Zertifikate akzeptieren, deren Gültigkeit über einen Satz von bestimmten CA-Zertifikaten bestätigt wird (siehe „CA-Zertifikate“ auf Seite 6-138 und „Authentifizierung“ auf Seite 6-204).

Wählen Sie dazu unter *IPsec VPN* >> *Verbindungen* >> *Editieren* >> *Authentifizierung* bei dem Punkt *Remote CA-Zertifikat* die Einstellung **Alle bekannten CAs**.

Wenn das neue Maschinenzertifikat von einem anderen Sub-CA-Zertifikat herausgegeben wird, dann muss der VPN-Partner dieses kennen, bevor das Redundanzpaar das neue Maschinenzertifikat nutzt.

Das Maschinenzertifikat muss an beiden mGuards eines Redundanzpaars getauscht weden. Aber manchmal ist das nicht möglich, wenn einer nicht erreichbar ist. Dies kann zum Beispiel bei einem Netzwerkausfall geschehen. So kann der mGuard in Bereitschaft ein veraltetes Maschinenzertifikat haben, wenn er aktiv wird. Das ist ein weiterer Grund dafür, dass die VPN-Partner so eingestellt seien müssen, dass sie beide Maschinenzertifikate nutzen.

Normalerweise wird von dem VPN-Zustandsabgleich auch das Maschinenzertifikat mit dem passenden Schlüssel repliziert. Bei einem Failover kann der andere mGuard übernehmen und sogar den Aufbau unvollständiger ISAKMP SAs fortsetzen.

Remote-Zertifikate für eine VPN-Verbindung wechseln

Der mGuard kann so eingestellt werden, dass er VPN-Partner direkt über die X.509-Zertifikate authentifiziert, die diese vorweisen. Dafür muss dieses X.509-Zertifikat beim mGuard eingestellt sein. Es wird *Remote CA-Zertifikat* genannt.

Wenn ein Remote-Zertifikat erneuert wird, hat kurzfristig nur einer der mGuards ein neues Zertifikat. Wir empfehlen deshalb bei der VPN-Redundanz die VPN-Partner über CA-Zertifikate statt über Remote-Zertifikate zu authentifizieren.

Neues CA-Zertifikat hinzufügen, um VPN-Partner zu identifizieren

Der mGuard kann so eingestellt werden, das er VPN-Partner über CA-Zertifikate authentifiziert (siehe „CA-Zertifikate“ auf Seite 6-138 und „Authentifizierung“ auf Seite 6-204).

Wählen Sie dazu unter *IPsec VPN* >> *Verbindungen* >> *Editieren* >> *Authentifizierung* bei dem Punkt *Remote CA-Zertifikat* die Einstellung **Alle bekannten CAs**.

Bei dieser Einstellung kann ein neues CA-Zertifikat hinzugefügt werden, ohne die aufgebauten VPN-Verbindungen zu beeinflussen. Aber die neuen CA-Zertifikate werden sofort genutzt. Das X.509-Zertifikat, das der VPN-Partner nutzt, um sich beim mGuard zu authentifizieren kann dann mit einer minimalen Unterbrechung ausgetauscht werden. Es muss nur sichergestellt werden, dass das neue CA-Zertifikat zuerst verfügbar ist.

Der mGuard kann so eingestellt werden, dass er den Gültigkeitszeitraum der Zertifikate prüft, die vom VPN-Partner bereitgestellt werden (siehe „Zertifikatseinstellungen“ auf Seite 6-134). In diesem Fall ist es notwendig, dass neue vertrauenswürdige CA-Zertifikate zur Konfiguration des mGuards hinzugefügt werden. Diese Zertifikate sollten ebenfalls einen Gültigkeitszeitraum haben.

Wenn die CRL-Prüfung eingeschaltet ist (unter *Authentifizierung* >> *Zertifikate* >> *Zertifikatseinstellungen),* dann muss eine URL pro CA-Zertifikat vorgehalten werden, an der die entsprechende CRL verfügbar ist. Die URL und CRL müssen veröffentlicht werden, bevor der mGuard die CA-Zertifikate nutzt, um die Gültigkeit der von den VPN-Partnern vorgezeigten Zertifikate zu bestätigen.

Einsatz von X.509-Zertifikaten mit einem beschränkten Gültigkeitszeitraum und CRL-Prüfung

Der Einsatz von X.509-Zertifikaten wird unter „Zertifikatseinstellungen“ auf Seite 6-134 beschrieben (Menü: *Authentifizierung* >> *Zertifikate* >> *Zertifikatseinstellungen*).

Wenn Sie X.509-Zertifikate einsetzen und dort **Beachte den Gültigkeitszeitraum von Zertifikaten und CRLs** eingestellt haben, dann muss die Systemzeit stimmen. Wir empfehlen, die Systemzeit mit einem vertauenswürdigen **NTP-Server** zu synchronsieren. Jeder mGuard eines Redundanzpaars kann den anderen als NTP-Server nutzen, aber nicht als einzigen NTP-Server.

7.3 Ring-/Netzkopplung

Die Funktion Ring-/Netzkopplung wird **nicht** unterstützt von:

– mGuard centerport

Ring-/Netzkopplung mit Einschränkung:

– mGuard delta: hier lässt sich die interne Seite (Switch-Ports) nicht abschalten

– mGuard pci: hier lässt sich im Treibermodus die interne Netzwerkschnittstelle nicht abschalten (wohl aber im Power-over-PCI-Modus).

8 Neustart, Recovery-Prozedur und Flashen der Firmware

Bei den in Bild 8-1 gezeigten Geräten wird die **Rescue-Taste** oder **Reset-Taste** benutzt, um das Gerät in einen der folgenden Zustände zu bringen:

– Neustart durchführen
– Recovery-Prozedur ausführen
– Flashen der Firmware / Rescue-Prozedur

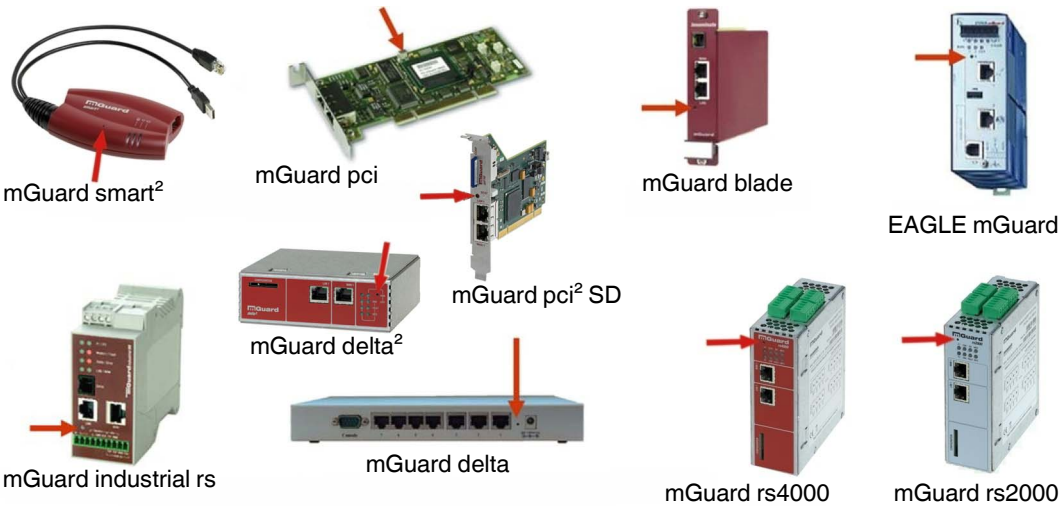


Bild 8-1 Rescue-Taste

Beim **mGuard centerport** gibt es eine **Reset-Taste**, mit der ein Neustart durchgeführt werden kann - siehe „mGuard centerport“ auf Seite 3-2. Die Rescue-Prozedur und damit das Neuladen der mGuard-Firmware wird über das Boot-Menü eingeleitet.

8.1 Neustart durchführen

Ziel

Das Gerät wird mit den konfigurierten Einstellungen neu gestartet.

Aktion

mGuard pci² SD: Die Reset-Taste drücken, bis die STAT-LED orange leuchtet.

mGuard centerport: Die Reset-Taste drücken.

Bei den anderen mGuards die Rescue-Taste für ca. 1,5 Sekunden drücken:

- **mGuard rs4000/rs2000, mGuard industrial rs,** mGuard delta²: bis die LED ERR leuchtet
- **mGuard smart²**: bis die mittlere LED in Rot aufleuchtet
- **mGuard blade, mGuard pci**: bis beide roten LEDs aufleuchten
- **mGuard EAGLE mGuard**: bis LED STATUS und die Link-LEDs aufhören zu leuchten
- **mGuard delta**: bis die LED Status aufhört zu blinken

Alternativ dazu:

- Die Stromzufuhr vorübergehend unterbrechen.
- **mGuard pci/mGuard pci² SD**: Computer, der die mGuard pci-Karte enthält, neu starten.

8.2 Recovery-Prozedur ausführen

Ziel

Die Netzwerkkonfiguration (aber nicht die restliche Konfiguration) soll in den Auslieferungszustand zurückgesetzt werden, weil auf den mGuard nicht mehr zugegriffen werden kann.

Bei der Recovery-Prozedur werden bei allen mGuard-Modellen die Werkseinstellungen gemäß der nachfolgenden Tabelle hergestellt:

Tabelle 8-1 Voreingestellte Adressen

Werkseinstellung	Netzwerk-Modus	Management-IP #1	Management-IP #2
mGuard rs4000/rs2000	Stealth	https://1.1.1.1/	https://192.168.1.1/
mGuard industrial rs	Stealth	https://1.1.1.1/	https://192.168.1.1/
mGuard smart^2	Stealth	https://1.1.1.1/	https://192.168.1.1/
mGuard pci^2 SD	Stealth	https://1.1.1.1/	https://192.168.1.1/
mGuard pci	Stealth	https://1.1.1.1/	https://192.168.1.1/
mGuard blade	Stealth	https://1.1.1.1/	https://192.168.1.1/
mGuard delta^2	Stealth	https://1.1.1.1/	https://192.168.1.1/
EAGLE mGuard	Stealth	https://1.1.1.1/	https://192.168.1.1/
mGuard centerport	Router		https://192.168.1.1/
mGuard blade-Controller	Router		https://192.168.1.1/
mGuard delta	Router		https://192.168.1.1/

– Für die mGuard-Modelle, die in den *Stealth*-Modus (mit der Werkseinstellung „mehrere Clients“) zurückgesetzt werden, gilt:
– Es wird auch das CIFS-Integrity-Monitoring abgeschaltet, weil es nur mit aktivierter Management-IP funktioniert.
– Weiterhin wird für die Ethernet-Anschlüsse das MAU-Management eingeschaltet. Der HTTPS-Zugriff wird über den lokalen Ethernet-Anschluss (LAN) freigegeben.

Die konfigurierten Einstellungen für VPN-Verbindungen und Firewall bleiben erhalten, ebenso die Passwörter.

Mögliche Gründe zum Ausführen der Recovery-Prozedur:

– Der mGuard befindet sich im Router- oder PPPoE-Modus.
– Die Geräteadresse des mGuards ist abweichend von der Standardeinstellung konfiguriert worden.
– Sie kennen die aktuelle IP-Adresse des Gerätes nicht.

Aktuelle Informationen zur Recovery- und Flash-Prozedur finden Sie in der Application Note, die für Ihre mGuard Firmware-Version relevant ist.

(Application Notes stehen im Download-Bereich von www.innominate.com bereit.)

Aktion:

mGuard centerport:

Voraussetzung: Am Gerät sind Bildschirm / Tastatur angeschlossen.

• Auf der Tastatur die folgende Tastenkombination drücken: <**Alt**>+<**S-Abf**>+<**a**>.

(Auf englischen Tastaturen ist die oben mit <S-Abf> bezeichnete Taste mit <SysRq> beschriftet. Auf manchen Tastaturen fehlt aber die Beschriftung <S-Abf> bzw. <SysRq>. Dann ist die Taste <Druck> bzw. <Print> zu verwenden.)

Nach Ausführung der Recovery-Prozedur erscheint auf dem Bildschirm eine entsprechende Meldung.

mGuard rs4000/rs2000, mGuard industrial rs, mGuard smart², mGuard pci² SD, mGuard pci, mGuard blade, mGuard delta², mGuard delta, EAGLE mGuard:

- Die **Rescue-/Reset-Taste** langsam 6-mal drücken.
  Nach ca. 2 Sekunden antwortet der mGuard:

mGuard rs4000/rs2000, mGuard pci² SD, mGuard delta²	Die LED STAT leuchtet grün
mGuard industrial rs	Die LED State leuchtet grün
mGuard smart²	Die mittlere LED leuchtet grün
mGuard pci, mGuard blade	Die LED LAN leuchtet rot
mGuard delta	Die LED Status leuchtet grün
EAGLE mGuard	Die LED STATUS leuchtet gelb

- Drücken Sie anschließend erneut die **Rescue-/Reset-Taste** langsam 6-mal.

mGuard rs4000/rs2000, mGuard delta²	Bei Erfolg leuchtet die LED STAT grün Bei Misserfolg leuchtet die LED ERR rot
mGuard industrial rs	Bei Erfolg leuchtet die LED State grün Bei Misserfolg leuchtet die Error LED rot
mGuard smart²	Bei Erfolg leuchtet die mittlere LED grün Bei Misserfolg leuchtet die mittlere LED rot
mGuard pci² SD	Bei Erfolg leuchtet die LED STAT grün Bei Misserfolg leuchtet die LED STAT rot
mGuard pci, mGuard blade	Bei Erfolg leuchtet die LED LAN rot Bei Misserfolg leuchtet die LED WAN rot
mGuard delta	Bei Erfolg leuchtet die LED Status grün Bei Misserfolg bleibt die LED Status aus
EAGLE mGuard	Bei Erfolg leuchtet die LED STATUS gelb Bei Misserfolg leuchtet die FAULT LED rot

- Bei Erfolg vollzieht das Gerät nach 2 Sekunden einen Neustart und schaltet sich dabei auf den *Stealth*- bzw. *Router*-Modus. Dann ist das Gerät wieder unter den entsprechenden Adressen zu erreichen - siehe Tabelle „Voreingestellte Adressen“ auf Seite 8-2.

8.3 Flashen der Firmware / Rescue-Prozedur

Ziel

Die gesamte Firmware des mGuards soll neu ins Gerät geladen werden.

– **Alle konfigurierten Einstellungen werden gelöscht.** Der mGuard wird in den Auslieferungszustand versetzt.
– Ab Version 5.0.0 des mGuard bleiben die im mGuard installierten Lizenzen nach Flashen der Firmware erhalten. Sie müssen also nicht erneut eingespielt werden.
– Beim mGuard industrial rs ist nur die Firmware ab Version 5.1.0 installierbar.

Mögliche Gründe:

– Das Administrator- und Root-Passwort sind verloren gegangen.

Voraussetzungen

8.3.1 Voraussetzungen für das Flashen

Voraussetzungen hinsichtlich DHCP- und TFTP-Server

ACHTUNG: Zum Flashen der Firmware muss auf dem lokal angeschlossenen Rechner ein DHCP- und TFTP-Server oder ein BootP-und TFTP-Server installiert sein.

Installieren Sie den DHCP- und TFTP-Server, falls notwendig (siehe „DHCP- und TFTP-Server installieren.“ auf Seite 8-11).

Es ist kein solcher Server für den **mGuard centerport** notwendig, wenn die Firmware von einem USB-Massenspeicher oder von CD-ROM geladen werden soll.

Es ist kein solcher Server für den **mGuard rs4000/rs2000, mGuard pci² SD und mGuard delta²** notwendig, wenn die Firmware von einer SD-Karte geladen werden soll. Beim Flashen wird die Firmware immer zuerst von einer SD-Karte geladen. Nur wenn keine SD-Karte gefunden wird, wird die Firmware von einem TFTP-Server geladen.

Voraussetzung für das Laden der Firmware von einer SD-Karte ist:

– alle notwendigen Firmware-Dateien müssen in einem gemeinsamen Verzeichnis auf der ersten Partition der SD-Karte vorhanden sein,
– diese Partition nutzt ein VFAT-Dateisystem (Standard bei SD-Karten).

ACHTUNG: Falls Sie einen zweiten DHCP-Server in einem Netzwerk installieren, könnte dadurch die Konfiguration des gesamten Netzwerks beeinflusst werden.

Weitere Voraussetzungen:

– **mGuard centerport**:
  – Am Gerät sind Bildschirm / Tastatur angeschlossen.
  – Sie haben die Firmware des mGuards vom Support Ihres Händlers oder von der Web-Site www.innominate.com bezogen und auf dem Konfigurations-Rechner gespeichert.
  – Falls die Ihnen vorliegende Firmware-Version höher ist als die beim Auslieferungszustand des Gerätes, müssen Sie eine Lizenz für die Nutzung dieses Updates erwerben. Das gilt für Major-Release Upgrades, also z. B. beim Upgrade von Version 4.x.y zu Version 5.x.y zu Version 6.x.y usw.
  – DHCP- und TFTP-Server sind unter der gleichen IP-Adresse zu erreichen.
– **mGuard rs4000/rs2000, mGuard pci² SD und mGuard delta²**:
  – Sie haben die Firmware des mGuards vom Support Ihres Händlers oder von der Web-Site www.innominate.com bezogen und auf eine kompatible SD-Karte gespeichert.
  – Diese SD-Karte ist im mGuard eingesetzt.
    Auf der Download-Seite von www.innominate.com stehen die entsprechenden Firmware-Dateien zum Herunterladen bereit. Auf der SD-Karte müssen die Dateien unter diesen Pfadnamen oder in diesen Ordnern liegen:
    Firmware/install-ubi.mpc83xx.p7s
    Firmware/ubifs.img.mpc83xx.p7s
– **mGuard pci**: Wenn der mGuard im **Power-over-PCI-Modus** betrieben wird, muss der DHCP/TFTP- Server über die LAN-Buchse des mGuards angeschlossen sein.
– **mGuard pci**: Wenn der mGuard im PCI-**Treibermodus** betrieben wird, muss der DHCP/TFTP-Server auf dem Rechner bzw. unter dem Betriebssystem ausgeführt werden, das die Schnittstelle zum mGuard bereitstellt.

Aktion

8.3.2 Flashen beim mGuard rs4000/rs2000, mGuard industrial rs, mGuard smart², mGuard pci, mGuard blade, mGuard delta², mGuard delta, EAGLE mGuard,

Gehen Sie zum Flashen der Firmware bzw. zur Durchführung der Rescue-Prozedur wie folgt vor:

ACHTUNG: Sie dürfen während der gesamten Flash-Prozedur auf keinen Fall die Stromversorgung des mGuards unterbrechen! Das Gerät könnte ansonsten beschädigt werden und nur noch durch den Hersteller reaktiviert werden.

- **Rescue-Taste** gedrückt halten, bis der *Recovery-Status* wie folgt eintritt:
  Der mGuard wird neu gestartet (nach ca. 1,5 Sekunden), nach weiteren ca. 1,5 Sekunden gelangt der mGuard in den *Recovery-Status*:
  Die Reaktion des Gerätes hängt vom Typ ab:

mGuard rs4000/rs2000, mGuard delta²	Die LEDs STAT, MOD und SIG leuchten grün
mGuard industrial rs	Die LEDs State, LAN und WAN leuchten grün
mGuard smart²	Die LEDs leuchten grün
mGuard pci, mGuard blade	Die grünen LEDs sowie die rote LAN-LED leuchten
mGuard delta	Die Status-LED wird langsam dunkel
EAGLE mGuard	Die LEDs 1, 2 und V.24 leuchten

Spätestens 1 Sekunde nach Eintritt des *Recovery-Status* **die Rescue-Taste** loslassen.
(Falls Sie die **Rescue-Taste** nicht loslassen, wird der mGuard neu gestartet.)
Der mGuard startet nun das Recovery-System: Er sucht über die LAN-Schnittstelle nach einem DHCP-Server, um von diesem eine IP-Adresse zu beziehen.
Die Reaktion des Gerätes hängt vom Typ ab:

mGuard rs4000/rs2000, mGuard delta²	Die LED STAT blinkt
mGuard industrial rs	Die LED State blinkt
mGuard smart²	Die mittlere LED („Heartbeat“) blinkt
mGuard pci, mGuard blade	Die rote LED LAN blinkt
mGuard delta	Die LED Status blinkt
EAGLE mGuard	Die LEDs 1, 2 und V.24 leuchten orange auf

Vom TFTP-Server oder von der SD-Karte wird die Datei install.p7s geladen. Diese enthält die elektronisch unterschriebene Kontrollprozedur für den Installationsvorgang. Nur von Innominate unterschriebene Dateien werden ausgeführt.
Die Kontrollprozedur löscht nun den aktuellen Inhalt des Flashspeichers und bereitet die Neuinstallation der Firmware vor.

Die Reaktion des Gerätes hängt vom Typ ab:

mGuard rs4000/rs2000, mGuard delta²	Die LEDs STAT, MOD und SIG bilden ein Lauflicht
mGuard industrial rs	Die LEDs Modem, State und LAN bilden ein Lauflicht
mGuard smart²	Die 3 grünen LEDs bilden ein Lauflicht
mGuard pci, mGuard blade	Die grünen LEDs und die rote LAN-LED bilden ein Lauflicht
mGuard delta	Die LED Status blinkt schneller
EAGLE mGuard	Die LEDs 1, 2 und V.24 bilden ein Lauflicht

Vom TFTP-Server oder von der SD-Karte wird die Firmware jffs2.img.p7s heruntergeladen und in den Flashspeicher geschrieben. Diese Datei enthält das eigentliche mGuard-Betriebssystem und ist elektronisch signiert. Nur von Innominate signierte Dateien werden akzeptiert.

Dieser Vorgang dauert ca. 3 bis 5 Minuten.

Die Reaktion des Gerätes hängt vom Typ ab:

mGuard rs4000/rs2000, mGuard delta²	Die LED STAT leuchtet kontinuierlich
mGuard industrial rs	Die LED State leuchtet kontinuierlich
mGuard smart²	Die mittlere LED („Heartbeart“) leuchtet kontinuierlich.
mGuard pci, mGuard blade	Die grünen LEDs blinken und die rote LED LAN leuchtet gleichzeitig durchgehend
mGuard delta	Die LED Status leuchtet kontinuierlich
EAGLE mGuard	Die LEDs 1, 2 und V.24 sind aus, die LEDs p1, p2 und Status leuchten kontinuierlich grün

Die neue Firmware wird entpackt und konfiguriert. Das dauert ca. 1 – 3 Minuten.

Sobald die Prozedur beendet ist, geschieht Folgendes:

mGuard rs4000/rs2000, mGuard delta²	Die LEDs STAT, MOD und SIG blinken gleichzeitig grün
mGuard industrial rs	Die LEDs Modem, State und LAN blinken gleichzeitig grün
mGuard smart²	Alle 3 LEDs blinken gleichzeitig grün
mGuard blade	Die grünen LEDs WAN und LAN und die rote WAN blinken gleichzeitig
mGuard pci	Der mGuard startet neu
mGuard delta	Die LED Status blinkt einmal pro Sekunde
EAGLE mGuard	Die LEDs 1, 2 und V.24 blinken gleichzeitig grün

- Starten Sie den mGuard neu. Dies ist beim mGuard blade und mGuard pci nicht erforderlich.
- Drücken Sie dazu kurz die **Rescue-Taste**.

  (Alternativ können Sie die Stromversorgung unterbrechen und wieder anschließen Beim mGuard smart² können Sie das USB-Kabel abziehen und aufstecken, da es ausschließlich zur Stromversorgung dient.)

Der mGuard befindet sich im Auslieferungszustand. Konfigurieren Sie ihn neu (siehe „Lokale Konfigurationsverbindung herstellen“ auf Seite 5-17).

Der **mGuard pci** erhält nach dem Neustart automatisch eine Management IP-Adresse zugewiesen. Diese Adresse bekommt er von einem im Netz erreichbaren BootP-Server, der während des Flashens verwendet wurde.

Wenn Sie den empfohlenen DHCP-Server für Windows verwenden (siehe Seite 8-11), dann arbeitet dieser auch als BootP-Server. Wenn Sie einen DHCP-Server unter Linux verwenden, dann gilt dies nicht.

8.3.3 Flashen beim mGuard pci² SD

Beim Flashen wird die Firmware immer zuerst von einer SD-Karte geladen. Nur wenn keine SD-Karte gefunden wird, wird die Firmware von einem TFTP-Server geladen.

Voraussetzung für das Laden der Firmware von einer SD-Karte ist:

– Alle notwendigen Firmware-Dateien müssen in einem gemeinsamen Verzeichnis auf der ersten Partition der SD-Karte vorhanden sein,
– Diese Partition nutzt ein VFAT-Dateisystem (Standard bei SD-Karten).
– Sie haben die Firmware des mGuards vom Support Ihres Händlers oder von der Web-Site www.innominate.com bezogen und auf eine kompatible SD-Karte gespeichert.
– Diese SD-Karte ist im mGuard eingesetzt.
– Auf der Download-Seite von www.innominate.com stehen die entsprechenden Firmware-Dateien zum Herunterladen bereit. Auf der SD-Karte müssen die Dateien unter diesen Pfadnamen oder in diesen Ordnern liegen:
  Firmware/install-ubi.mpc83xx.p7s
  Firmware/ubifs.img.mpc83xx.p7s

Aktion

• Drücken Sie die Reset-Taste an der Frontblende und halten Sie sie gedrückt.
  Die LED STAT an der Frontblende leuchtet kurz orange.
  Anschließend leuchten die LED STAT sowie die beiden oberen LEDs der Ethernet-Buchsen nacheinander grün
• Lassen Sie während der grünen Leuchtphase die Reset-Taste los.
  Die Flash-Prozedur startet.

8.3.4 Flashen beim mGuard centerport

Gehen Sie zum Flashen der Firmware bzw. zur Durchführung der Rescue-Prozedur wie folgt vor:

ACHTUNG: Sie dürfen während der gesamten Flash-Prozedur auf keinen Fall die Stromversorgung des mGuard unterbrechen! Das Gerät könnte ansonsten beschädigt werden und nur noch durch den Hersteller reaktiviert werden.

1. mGuard centerport neu starten / booten.
2. Sobald das Boot-Menü des mGuard centerport auf dem Bildschirm erscheint, drücken Sie auf der Tastatur am besten eine der Pfeiltasten: ↑, ↓, ← oder →.
   Dann bleibt das Boot-Menü angezeigt.

Bild 8-2 Boot-Menü mGuard centerport

3. Dann mit den Pfeiltasten ↓ bzw. ↑ eine der Optionen zur Durchführung der Rescue-Prozedur auswählen:
   Start rescue procedure via DHCP / BootP+TFTP
   ODER
   Start rescue procedure from CD / DVD
   ODER
   Start rescue procedure from USB mass storage
   Zum Inkraftsetzen der Auswahl die **Enter**-Taste drücken.
   Die Optionen beinhalten:

Start rescue procedure via DHCP / BootP+TFTP

Wirkung: Der mGuard lädt alle notwendigen Dateien vom TFTP-Server. Die Namen der heruntergeladenen Dateien entsprechen denen, wie sie auch von den anderen Modellen der mGuard-Familie verwendet werden, mit folgenden Ausnahmen:

- install.p7s -> install.x86_64.p7s
- jffs2.img.p7s -> firmware.img.x86_64.p7s

Bei der Datei install.x86_64.p7s ist darauf zu achten, dass es sich um die Version dieser Datei handelt, die von Innominate zur Verwendung für die Rescue-Prozedur per TFTP ausgewiesen hat.

Start rescue procedure from CD / DVDs

Voraussetzung: Die Firmware des mGuard ist zuvor auf eine CD gebrannt worden - siehe unten unter „mGuard-Firmware auf CD-ROM brennen“ auf Seite 8-10.

Wirkung: Der mGuard lädt alle notwendigen Dateien von der eingelegten CD.

Dazu während der Anzeige des Boot-Menüs und vor Inkraftsetzten dieser Auswahl die CD mit der Firmware des mGuard ins CD-Laufwerk legen.

(Aus Sicherheitsgründen bootet der mGuard centerport nicht von CD.)

Start rescue procedure from USB mass storage

Voraussetzung: Die Firmware des mGuard ist zuvor auf ein USB-Speichermedium (USB-Stick) kopiert worden.

Das USB-Speichermedium muss als erste primäre Partition ein VFAT-Dateisystem haben, und es muss dieselben Dateien in denselben Ordnern enthalten, wie es für die CD beschrieben ist. Zusätzlich können - wie bei einer CD - im Ordner **Rescue Config** die angegebenen Dateien enthalten sein.

Wirkung: Der mGuard lädt alle notwendigen Dateien vom angeschlossenen USB-Speichermedium. Dazu spätestens während der Anzeige des Boot-Menüs und vor Inkraftsetzten dieser Auswahl das USB-Speichermedium mit der Firmware darauf an die USB-Schnittstelle anschließen. (Aus Sicherheitsgründen bootet der mGuard centerport nicht vom USB-Speichermedium.)

4. Nach der Rescue-Prozedur erscheint auf dem Bildschirm eine entsprechende Meldung. Folgen Sie möglichen weiteren Anweisungen auf dem Bildschirm.

Der mGuard befindet sich im Auslieferungszustand. Konfigurieren Sie ihn neu (siehe „Lokale Konfigurationsverbindung herstellen“ auf Seite 5-17):

mGuard-Firmware auf CD-ROM brennen

Die Firmware des mGuard kann auf CD gebrannt werden. Auf der Download-Seite von www.innominate.com steht dazu eine zip-Datei zum Herunterladen bereit.

Den Inhalt dieses zip-Archivs als Daten-CD brennen. Auf der CD müssen die folgenden Dateien in folgenden Ordnern / unter folgenden Pfadnamen liegen:

- Firmware/install.x86_64.p7s
- Firmware/firmware.img.x86_64.p7s

Bei der Datei install.x86_64.p7s ist darauf zu achten, dass es sich um die Version dieser Datei handelt, die von Innominate zur Verwendung für die Rescue-Prozedur per CD ausgewiesen hat.

Bei Bedarf können diese Dateien im Ordner **Rescue Config** auf der CD vorhanden sein:

Rescue Config/licence.lic	Lizenzdatei, die während der Rescue-Prozedur in das Gerät eingebracht werden soll.
Rescue Config/<serial>.lic	Wie oben, nur dass der Platzhalter <serial> durch die Seriennummer des Gerätes ersetzt ist. Dieselbe CD kann so für verschiedene Geräte gleichzeitig verwendet werden.
Rescue Config/preconfig.atv	Konfigurationsprofil, das während der Rescue-Prozedur in der Firmware angewendet werden soll. Die Datei muss vom Skript Rescue Config/preconfig.sh angewendet werden.
Rescue Config/<serial>.atv	Analog zu <serial>.lic
Rescue Config/preconfig.sh	Skript-Datei, die direkt nach dem Installieren der neuen Firmware ausgeführt wird. Details finden Sie in dem Dokument „Innominate mGuard - Application Note: Rollout Support“ unter www.innominate.com.

8.3.5 DHCP- und TFTP-Server installieren.

Falls Sie einen zweiten DHCP-Server in einem Netzwerk installieren, könnte dadurch die Konfiguration des gesamten Netzwerks beeinflusst werden.

Unter Windows

Installieren Sie das Programm, welches im Download-Bereich von www.innominate.com zu finden ist.

- Ist der Windows-Rechner an ein Netzwerk angeschlossen, trennen Sie ihn von diesem.
- Kopieren Sie die Firmware in einen beliebigen leeren Ordner des Windows-Rechners.
- Starten Sie das Programm TFTPD32.EXE

Die festzulegende Host-IP lautet: **192.168.10.1.** Das muss auch die Adresse für die Netzwerkkarte sein.

- Klicken Sie die Schaltfläche **Browse**, um auf den Ordner zu wechseln, wo die mGuard-Image-Dateien gespeichert sind: **install.p7s, jffs2.img.p7s**
- Falls durch das Flashen ein Major-Release-Upgrade der Firmware vorgenommen wird, muss die für das Upgrade erworbene Lizenz-Datei unter dem Namen **licence.lic** ebenfalls dort abgelegt werden.

  Stellen Sie sicher, dass es sich um die Lizenzdatei handelt, welche wirklich zum Gerät gehört (siehe „Verwaltung >> Update“ auf Seite 6-37).

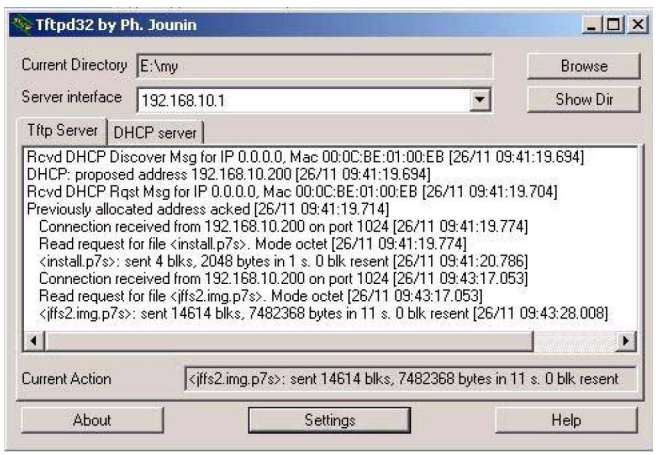
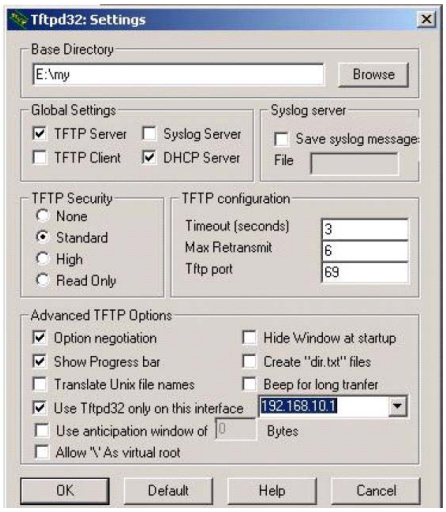


Bild 8-3 Host-IP eingeben

- Wechseln Sie auf die Registerkarte „TFTP-Server“ bzw. „DHCP-Server“ und klicken Sie dann die Schaltfläche „Settings“, um die Parameter wie folgt zu setzen:



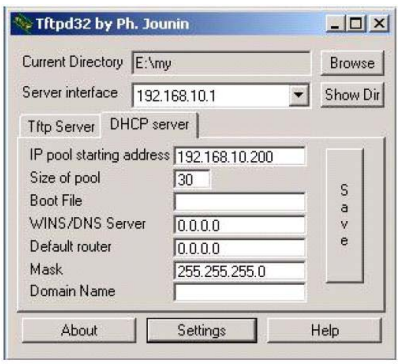


Bild 8-4 Stettings

Unter Linux

Alle aktuellen Linux-Distributionen enthalten DHCP- und TFTP-Server.

- Installieren Sie die entsprechenden Pakete gemäß der Anleitung der jeweiligen Distribution.
- Konfigurieren Sie den DHCP-Server, indem Sie in der Datei **/etc/dhcpd.conf** folgende Einstellungen vornehmen:

  subnet 192.168.134.0 netmask 255.255.255.0 {
  range 192.168.134.100 192.168.134.119;
  option routers 192.168.134.1;
  option subnet-mask 255.255.255.0;
  option broadcast-address 192.168.134.255;}

Diese Beispiel-Konfiguration stellt 20 IP-Adressen (.100 bis .119) bereit. Es wird angenommen, dass der DHCP-Server die Adresse 192.168.134.1 hat (Einstellungen für ISC DHCP 2.0).

Der benötigte TFTP-Server wird in folgender Datei konfiguriert: **/etc/inetd.conf**

- Fügen Sie in diese Datei die entsprechende Zeile ein oder setzen Sie die notwendigen Parameter für den TFTP-Service. (Verzeichnis für Daten ist: **/tftpboot)**

  tftp dgram udp wait root /usr/sbin/in.tftpd -s /tftpboot/

Im Verzeichnis **/tftpboot** müssen die mGuard-Imagedateien gespeichert sein: **install.p7s, jffs2.img.p7s**

- Falls durch das Flashen ein Major-Release-Upgrade der Firmware vorgenommen wird, muss die für das Upgrade erworbene Lizenz-Datei unter dem Namen **licence.lic** ebenfalls dort abgelegt werden.

  Stellen Sie sicher, dass es sich um die Lizenzdatei handelt, welche wirklich zum Gerät gehört (siehe „Verwaltung >> Update“ auf Seite 6-37).
- Starten Sie dann den inetd-Prozess neu, um die Konfigurationsänderungen zu übernehmen.
- Sollten Sie einen anderen Mechanismus verwenden, z. B. xinetd, dann informieren Sie sich in der entsprechenden Dokumentation.

9 Glossar

Asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung werden Daten mit einem Schlüssel verschlüsselt und mit einem zweiten Schlüssel wieder entschlüsselt. Beide Schlüssel eignen sich zum Ver- und Entschlüsseln. Einer der Schlüssel wird von seinem Eigentümer geheim gehalten (Privater Schlüssel/Private Key), der andere wird der Öffentlichkeit (Öffentlicher Schlüssel/Public Key), d. h. möglichen Kommunikationspartnern, gegeben.

Eine mit dem öffentlichen Schlüssel verschlüsselte Nachricht kann nur von dem Empfänger entschlüsselt und gelesen werden, der den zugehörigen privaten Schlüssel hat. Eine mit dem privaten Schlüssel verschlüsselte Nachricht kann von jedem Empfänger entschlüsselt werden, der den zugehörigen öffentlichen Schlüssel hat. Die Verschlüsselung mit dem privaten Schlüssel zeigt, dass die Nachricht tatsächlich vom Eigentümer des zugehörigen öffentlichen Schlüssels stammt. Daher spricht man auch von digitaler Signatur, Unterschrift.

Asymetrische Verschlüsselungsverfahren wie RSA sind jedoch langsam und anfällig für bestimmte Angriffe, weshalb sie oft mit einem symmetrischen Verfahren kombiniert werden (→„Symmetrische Verschlüsselung“ auf Seite 9-8). Andererseits sind Konzepte möglich, die die aufwendige Administrierbarkeit von symmetrischen Schlüsseln vermeiden.

DES / 3DES

Der von IBM stammende und von der NSA überprüfte symmetrische Verschlüsselungsalgorithmus (→ „Symmetrische Verschlüsselung“ auf Seite 9-8) DES wurde 1977 vom amerikanischen National Bureau of Standards, dem Vorgänger des heutigen National Institute of Standards and Technology (NIST), als Standard für amerikanische Regierungsinstitutionen festgelegt. Da es sich hierbei um den ersten standardisierten Verschlüsselungsalgorithmus überhaupt handelte, setzte er sich auch schnell in der Industrie und somit außerhalb Amerikas durch.

DES arbeitet mit einer Schlüssellänge von 56 Bit, die heute aufgrund der seit 1977 gestiegenen Rechenleistung der Computer als nicht mehr sicher gilt.

3DES ist eine Variante von DES. Es arbeitet mit drei mal größeren Schlüsseln, die also 168 Bit lang sind. Sie gilt heute noch als sicher und ist unter anderem auch Teil des IPsec-Standards.

AES

Das NIST (National Institute of Standards and Technology) entwickelt in Zusammenarbeit mit Industrie-Unternehmen seit Jahren den AES-Verschlüsselungsstandard. Diese symmetrische Verschlüsselung soll den bisherigen DES-Standard ablösen. Der AES-Standard spezifiziert drei verschiedene Schlüsselgrößen mit 128, 192 und 256 Bit.

1997 hatte die NIST die Initiative zu AES gestartet und ihre Bedingungen für den Algorithmus bekannt gegeben. Von den vorgeschlagenen Verschlüsselungsalgorithmen hat die NIST fünf Algorithmen in die engere Wahl gezogen; und zwar die Algorithmen MARS, RC6, Rijndael, Serpent und Twofish. Im Oktober 2000 hat man sich für Rijndael als Verschlüsselungsalgorithmus entschieden.

CA-Zertifikat

Wie vertrauenswürdig ist ein Zertifikat und die CA (Certificate Authority), die es ausgestellt hat? (→ „X.509 Zertifikat“ auf Seite 9-7) Ein CA-Zertifikat kann herangezogen werden, um ein Zertifikat zu überprüfen, das die Signatur dieser CA trägt. Diese Prüfung macht nur dann Sinn, wenn davon auszugehen ist, dass das CA-Zertifikat aus authentischer Quelle stammt, also selber echt ist. Wenn darüber Zweifel bestehen, kann das CA-Zertifikat selber überprüft werden. Wenn es sich um ein Sub-CA-Zertifikat handelt, also ein CA-Zertifikat ausgestellt von einer Sub-CA (Sub Certificate Authority) - was normalerweise der Fall ist -, kann das CA-Zertifikat der übergeordneten CA benutzt werden, um das CA-Zertifikat der ihr untergeordneten Instanz zu überprüfen. Und gibt es für diese übergeordnete CA eine weitere CA, die ihr wiederum übergeordnet ist, kann deren CA-Zertifikat benutzt werden, um das

CA-Zertifikat der ihr untergeordneten Instanz zu prüfen, usw. Diese Kette des Vertrauens setzt sich fort bis zur Wurzelinstanz, die Root-CA (Root Certificate Authority). Die CA-Datei der Root-CA ist zwangsläufig selbst signiert. Denn diese Instanz ist die höchste, und der „Anker des Vertrauens“ liegt letztlich bei ihr. Es ist niemand mehr da, der dieser Instanz bescheinigen kann, dass sie die Instanz ist, für die sie sich ausgibt. Eine Root-CA ist daher eine staatliche oder staatlich kontrollierte Organisation.

Der mGuard kann die in ihn importierten CA-Zertifikate benutzen, um die von Gegenstellen „vorgezeigten“ Zertifikate auf Echtheit zu überprüfen. Bei VPN-Verbindungen z. B. kann die Authentifizierung der Gegenstelle ausschließlich durch CA-Zertifikate erfolgen. Dann müssen im mGuard alle CA-Zertifikate installiert sein, um mit dem von der Gegenstelle vorgezeigten Zertifikat eine Kette zu bilden: neben dem CA-Zertifikat der CA, deren Signatur im zu überprüfenden vorgezeigten Zertifikat des VPN-Partners steht, auch das CA-Zertifikat der ihr übergeordneten CA usw. bis hin zum Root-Zertifikat. Denn je lückenloser diese „Kette des Vertrauens“ überprüft wird, um eine Gegenstelle als authentisch zu akzeptieren, desto höher ist die Sicherheitsstufe.

Client / Server

In einer Client-Server-Umgebung ist ein Server ein Programm oder Rechner, das vom Client-Programm oder Client-Rechner Anfragen entgegennimmt und beantwortet.

Bei Datenkommunikation bezeichnet man auch den Rechner als Client, der eine Verbindung zu einem Server (oder Host) herstellt. D. h. der Client ist der anrufende Rechner, der Server (oder Host) der angerufene.

Datagramm

Bei IP Übertragungsprotokollen werden Daten in Form von Datenpaketen, den sog. IP-Datagrammen, versendet. Ein IP-Datagramm hat folgenden Aufbau

IP-Header	TCP, UDP, ESP etc. Header	Daten (Payload)

Der IP-Header enthält:

– die IP-Adresse des Absenders (source IP-address)
– die IP-Adresse des Empfängers (destination IP-address)
– die Protokollnummer des Protokolls der nächst höheren Protokollschicht (nach dem OSI-Schichtenmodell)
– die IP-Header Prüfsumme (Checksum) zur Überprüfung der Integrität des Headers beim Empfang.

Der TCP-/UDP-Header enthält folgende Informationen:

– Port des Absenders (source port)
– Port des Empfängers (destination port)
– eine Prüfsumme über den TCP-Header und ein paar Informationen aus dem IP-Header (u. a. Quell- und Ziel-IP-Adresse)

Standard-Route

Ist ein Rechner an ein Netzwerk angeschlossen, erstellt das Betriebssystem intern eine Routing-Tabelle. Darin sind die IP-Adressen aufgelistet, die das Betriebssystem von den angeschlossenen Rechnern und den gerade verfügbaren Verbindungen (Routen) ermittelt hat. Die Routing-Tabelle enthält also die mögliche Routen (Ziele) für den Versand von IP-Paketen. Sind IP-Pakete zu verschicken, vergleicht das Betriebssystem des Rechners die in den IP-Paketen angegebenen IP-Adressen mit den Einträgen in der Routing-Tabelle, um die richtige Route zu ermitteln.

Ist ein Router am Rechner angeschlossen und ist dessen interne IP-Adresse (d. h. die IP-Adresse des LAN Ports des Routers) als Standard-Gateway dem Betriebssystem mitgeteilt (bei der TCP/IP-Konfiguration der Netzwerkkarte), wird diese IP-Adresse als Ziel verwendet, wenn alle anderen IP-Adressen der Routing-Tabelle nicht passen. In diesem Fall be-

zeichnet die IP-Adresse des Routers die Standard-Route, weil alle IP-Pakete zu diesem Gateway geleitet werden, deren IP-Adressen in der Routing-Tabelle sonst keine Entsprechung, d. h. keine Route finden.

DynDNS-Anbieter

Auch *Dynamic DNS-Anbieter*. Jeder Rechner, der mit dem Internet verbunden ist, hat eine IP-Adresse (IP = Internet Protocol). Ist der Rechner über die Telefonleitung per Modem, per ISDN oder auch per ADSL online, wird ihm vom Internet Service Provider dynamisch eine IP-Adresse zugeordnet, d. h. die Adresse wechselt von Sitzung zu Sitzung. Auch wenn der Rechner (z. B. bei einer Flatrate) über 24 Stunden ununterbrochen online ist, wird die IP-Adresse zwischendurch gewechselt.

Soll ein solcher Rechner über das Internet erreichbar sein, muss er eine Adresse haben, die der entfernten Gegenstelle bekannt sein muss. Nur so kann diese die Verbindung zum Rechner aufbauen. Wenn die Adresse des Rechners aber ständig wechselt, ist das nicht möglich. Es sei denn, der Betreiber des Rechners hat ein Account bei einem DynDNS-Anbieter (DNS = Domain Name Server).

Dann kann er bei diesem einen Hostnamen festlegen, unter dem der Rechner künftig erreichbar sein soll, z. B.: www.example.com. Zudem stellt der DynDNS-Anbieter ein kleines Programm zur Verfügung, das auf dem betreffenden Rechner installiert und ausgeführt werden muss. Bei jeder Internet-Sitzung des lokalen Rechners teilt dieses Tool dem DynDNS-Anbieter mit, welche IP-Adresse der Rechner zurzeit hat. Dessen Domain Name Server registriert die aktuelle Zuordnung Hostname - IP-Adresse und teilt diese anderen Domain Name Servern im Internet mit.

Wenn jetzt ein entfernter Rechner eine Verbindung herstellen will zum Rechner, der beim DynDNS-Anbieter registriert ist, benutzt der entfernte Rechner den Hostnamen des Rechners als Adresse. Dadurch wird eine Verbindung hergestellt zum zuständigen DNS (Domain Name Server), um dort die IP-Adresse nachzuschlagen, die diesem Hostnamen zurzeit zugeordnet ist. Die IP-Adresse wird zurückübertragen zum entfernten Rechner und jetzt von diesem als Zieladresse benutzt. Diese führt jetzt genau zum gewünschten Rechner.

Allen Internetadressen liegt dieses Verfahren zu Grunde: Zunächst wird eine Verbindung zum DNS hergestellt, um die diesem Hostnamen zugeteilte IP-Adresse zu ermitteln. Ist das geschehen, wird mit dieser „nachgeschlagenen" IP-Adresse die Verbindung zur gewünschten Gegenstelle, eine beliebige Internetpräsenz, aufgebaut.

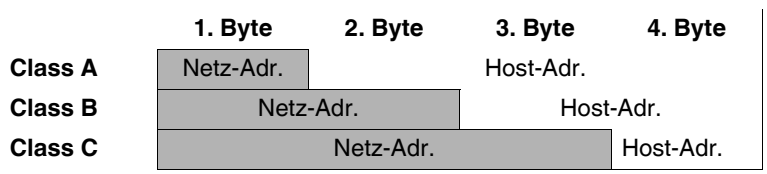
IP-Adresse

Jeder Host oder Router im Internet / Intranet hat eine eindeutige IP-Adresse (IP = Internet Protocol). Die IP-Adresse ist 32 Bit (= 4 Byte) lang und wird geschrieben als 4 Zahlen (jeweils im Bereich 0 bis 255), die durch einen Punkt voneinander getrennt sind.

Eine IP-Adresse besteht aus 2 Teilen: die Netzwerk-Adresse und die Host-Adresse.

Netzwerk-Adresse	Host-Adresse

Alle Hosts eines Netzes haben dieselbe Netzwerk-Adresse, aber unterschiedliche Host-Adressen. Je nach Größe des jeweiligen Netzes - man unterscheidet Netze der Kategorie Class A, B und C - sind die beiden Adressanteile unterschiedlich groß:



Ob eine IP-Adresse ein Gerät in einem Netz der Kategorie Class A, B oder C bezeichnet, ist am ersten Byte der IP-Adresse erkennbar. Folgendes ist festgelegt:

	Wert des 1. Byte	Bytes für die Netzadresse	Bytes für die Host-Adresse
Class A	1 - 126	1	3
Class B	128 - 191	2	2
Class C	192 - 223	3	1

Rein rechnerisch kann es nur maximal 126 Class A Netze auf der Welt geben, jedes dieser Netze kann maximal 256 x 256 x 256 Hosts umfassen (3 Bytes Adressraum). Class B Netze können 64 x 256 mal vorkommen und können jeweils bis zu 65.536 Hosts enthalten (2 Bytes Adressraum: 256 x 256). Class C Netze können 32 x 256 x 256 mal vorkommen und können jeweils bis zu 256 Hosts enthalten (1 Byte Adressraum).

Subnetzmaske

Einem Unternehmens-Netzwerk mit Zugang zum Internet wird normalerweise nur eine einzige IP-Adresse offiziell zugeteilt, z. B. 123.456.789.21. Bei dieser Beispiel-Adresse ist am 1. Byte erkennbar, dass es sich bei diesem Unternehmens-Netzwerk um ein Class B Netz handelt, d. h. die letzten 2 Byte können frei zur Host-Adressierung verwendet werden. Das ergibt rein rechnerisch einen Adressraum von 65.536 möglichen Hosts (256 x 256).

Ein so riesiges Netz macht wenig Sinn. Hier entsteht der Bedarf, Subnetze zu bilden. Dazu dient die Subnetzmaske. Diese ist wie eine IP-Adresse ein 4 Byte langes Feld. Den Bytes, die die Netz-Adresse repräsentieren, ist jeweils der Wert 255 zugewiesen. Das dient vor allem dazu, sich aus dem Host-Adressenbereich einen Teil zu „borgen“, um diesen zur Adressierung von Subnetzen zu benutzen. So kann beim Class B Netz (2 Byte für Netzwerk-Adresse, 2 Byte für Host-Adresse) mit Hilfe der Subnetzmaske 255.255.255.0 das 3. Byte, das eigentlich für Host-Adressierung vorgesehen war, jetzt für Subnetz-Adressierung verwendet werden. Rein rechnerisch können so 256 Subnetze mit jeweils 256 Hosts entstehen.

IPsec

IP Security (IPsec) ist ein Standard, der es ermöglicht, bei IP-Datagrammen (→„Datagramm“ auf Seite 9-2) die Authentizität des Absenders, die Vertraulichkeit und die Integrität der Daten durch Verschlüsselung zu wahren. Die Bestandteile von IPsec sind der Authentication Header (AH), die Encapsulating-Security-Payload (ESP), die Security Association (SA) und der Internet Key Exchange (IKE).

Zu Beginn der Kommunikation klären die an der Kommunikation beteiligten Rechner das benutzte Verfahren und dessen Implikationen wie z. B. *Transport Mode* oder *Tunnel Mode*

Im *Transport Mode* wird in jedes IP-Datagramm zwischen IP-Header und TCP- bzw. UDP-Header ein IPsec-Header eingesetzt. Da dadurch der IP-Header unverändert bleibt, ist dieser Modus nur für eine Host- zu-Host-Verbindung geeignet.

Im *Tunnel Mode* wird dem gesamten IP-Datagramm ein IPsec-Header und ein neuer IP-Header vorangestellt. D. h. das ursprüngliche Datagramm wird insgesamt verschlüsselt in der Payload des neuen Datagramms untergebracht.

Der *Tunnel Mode* findet beim VPN Anwendung: Die Geräte an den Tunnelenden sorgen für die Ver- bzw. Entschlüsselung der Datagramme, auf der Tunnelstrecke, d. h. auf dem Übertragungsweg über ein öffentliches Netz bleiben die eigentlichen Datagramme vollständig geschützt.

Subject, Zertifikat

In einem Zertifikat werden von einer Zertifizierungsstelle (CA - Certificate Authority) die Zugehörigkeit des Zertifikats zu seinem Inhaber bestätigt. Das geschieht, indem bestimmte Eigenschaften des Inhabers bestätigt werden, ferner, dass der Inhaber des Zertifikats den privaten Schlüssel besitzt, der zum öffentlichen Schlüssel im Zertifikat passt. (→ „X.509 Zertifikat“ auf Seite 9-7).

Beispiel

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1 (0x1)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=XY, ST=Austria, L=Graz, O=TrustMe Ltd, OU=Certificate Authority, CN=CA/Email=ca@trustme.dom
    Validity
      Not Before: Oct 29 17:39:10 2000 GMT
→ Subject: CN=anywhere.com,E=doctrans.de,C=DE,ST=Hamburg,L=Hamburg,O=Innominate,OU=Security
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
        Modulus (1024 bit):
          00:c4:40:4c:6e:14:1b:61:36:84:24:b2:61:c0:b5:
          d7:e4:7a:a5:4b:94:ef:d9:5e:43:7f:c1:64:80:fd:
          9f:50:41:6b:70:73:80:48:90:f3:58:bf:f0:4c:b9:
          90:32:81:59:18:16:3f:19:f4:5f:11:68:36:85:f6:
          1c:a9:af:fa:a9:a8:7b:44:85:79:b5:f1:20:d3:25:
          7d:1c:de:68:15:0c:b6:bc:59:46:0a:d8:99:4e:07:
          50:0a:5d:83:61:d4:db:c9:7d:c3:2e:eb:0a:8f:62:
          8f:7e:00:e1:37:67:3f:36:d5:04:38:44:44:77:e9:
          f0:b4:95:f5:f9:34:9f:f8:43
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Subject Alternative Name:
        email:xyz@anywhere.com
      Netscape Comment:
        mod_ssl generated test server certificate
      Netscape Cert Type:
        SSL Server
  Signature Algorithm: md5WithRSAEncryption
    12:ed:f7:b3:5e:a0:93:3f:a0:1d:60:cb:47:19:7d:15:59:9b:
    3b:2c:a8:a3:6a:03:43:d0:85:d3:86:86:2f:e3:aa:79:39:e7:
    82:20:ed:f4:11:85:a3:41:5e:5c:8d:36:a2:71:b6:6a:08:f9:
    cc:1e:da:c4:78:05:75:8f:9b:10:f0:15:f0:9e:67:a0:4e:a1:
    4d:3f:16:4c:9b:19:56:6a:f2:af:89:54:52:4a:06:34:42:0d:
    d5:40:25:6b:b0:c0:a2:03:18:cd:d1:07:20:b6:e5:c5:1e:21:
    44:e7:c5:09:d2:d5:94:9d:6c:13:07:2f:3b:7c:4c:64:90:bf:
    ff:8e
```

Der *Subject Distinguished Name*, kurz *Subject*, identifiziert den Zertifikatsinhaber eindeutig. Der Eintrag besteht aus mehreren Komponenten. Diese werden Attribute genannt (siehe das Beispiel-Zertifikat oben). Die folgende Tabelle listet die möglichen Attribute auf. In welcher Reihenfolge die Attribute in einem X.509-Zertifikat aufgeführt sind, ist unterschiedlich.

Tabelle 9-1 X.509-Zertifikat

Abkürzung	Name	Erläuterung
CN	Common Name	Identifiziert die Person oder das Objekt, zu der/dem das Zertifikat gehört. Beispiel: CN=server1
E	E-Mail-Adresse	Gibt die E-Mail-Adresse des Zertifikatsinhabers an.
OU	Organizational Unit	Gibt die Abteilung innerhalb einer Organisation oder Firma an. Beispiel: O=Entwicklung
O	Organization	Gibt die Organisation bzw. die Firma an. Beispiel: O=Innominate

Tabelle 9-1 X.509-Zertifikat

Abkürzung	Name	Erläuterung
L	Locality	Gibt den Ort an Beispiel: L=Hamburg
ST	State	Gibt den Bundesstaat bzw. das Bundesland an. Beispiel: ST=Bayern
C	Country	Code bestehend aus 2 Buchstaben, die das Land (= den Staat) angeben. (Deutschland = DE) Beispiel: C=DE

Bei VPN-Verbindungen sowie bei Fernwartungszugriffen auf den mGuard per SSH oder HTTPS kann für Subject (= Zertifikatsinhaber) ein Filter gesetzt werden. Dann werden nur solche Zertifikate von Gegenstellen akzeptiert, bei denen in der Zeile Subject bestimmte Attribute vorhanden sind.

NAT (Network Address Translation)

Bei der Network Address Translation (NAT) - oft auch als *IP-Masquerading* bezeichnet - wird hinter einem einzigen Gerät, dem sog. NAT-Router, ein ganzes Netzwerk „versteckt". Die internen Rechner im lokalen Netz bleiben mit ihren IP-Adressen verborgen, wenn Sie nach außen über die NAT-Router kommunizieren. Für die Kommunikationspartner außen erscheint nur der NAT-Router mit seiner eigenen IP-Adresse.

Damit interne Rechner dennoch direkt mit externen Rechnern (im Internet) kommunizieren können, muss der NAT-Router die IP-Datagramme verändern, die von internen Rechnern nach außen und von außen zu einem internen Rechner gehen.

Wird ein IP-Datagramm aus dem internen Netz nach außen versendet, verändert der NAT-Router den UDP- bzw. TCP-Header des Datagramms. Er tauscht die Quell-IP-Adresse und den Quell-Port aus gegen die eigene offizielle IP-Adresse und einen eigenen, bisher unbenutzen Port. Dazu führt er eine Tabelle, die die Zuordnung der ursprünglichen mit den neuen Werten herstellt.

Beim Empfang eines Antwort-Datagramms erkennt der NAT-Router anhand des angegebenen Zielports, dass das Datagramm eigentlich für einen internen Rechner bestimmt ist. Mit Hilfe der Tabelle tauscht der NAT-Router die Ziel-IP-Adresse und den Ziel-Port aus und schickt das Datagramm weiter ins interne Netz.

Port-Nummer

Bei den Protokollen UDP und TCP wird jedem Teilnehmer eine Portnummer zugeordnet. Über sie ist es möglich zwischen zwei Rechnern mehrere UDP oder TCP Verbindungen zu unterscheiden und somit gleichzeitig zu nutzen.

Bestimmte Portnummern sind für spezielle Zwecke reserviert. Zum Beispiel werden in der Regel HTTP Verbindungen zu TCP Port 80 oder POP3 Verbindungen zu TCP Port 110 aufgebaut.

Proxy

Ein Proxy (Stellvertreter) ist ein zwischengeschalteter Dienst. Ein Web-Proxy (z. B. Squid) wird gerne vor ein größeres Netzwerk geschaltet. Wenn z. B. 100 Mitarbeiter gehäuft auf eine bestimmte Webseite zugreifen und dabei über den Web-Proxy gehen, dann lädt der Proxy die entsprechenden Seiten nur einmal vom Server und teilt sie dann nach Bedarf an die anfragenden Mitarbeiter aus. Dadurch wird der Traffic nach außen reduziert, was Kosten spart.

PPPoE

Akronym für **P**oint-to-**P**oint **P**rotocol **o**ver **E**thernet. Basiert auf den Standards PPP und Ethernet. PPPoE ist eine Spezifikation, um Benutzer per Ethernet mit dem Internet zu verbinden über ein gemeinsam benutztes Breitbandmedium wie DSL, Wireless LAN oder Kabel-Modem.

PPTP

Akronym für **P**oint-to-**P**oint **T**unneling **P**rotocol. Entwickelt von Microsoft, U.S. Robotics und anderen wurde dieses Protokoll konzipiert, um zwischen zwei VPN-Knoten (→ VPN) über ein öffentliches Netz sicher Daten zu übertragen.

Router

Ein Router ist ein Gerät, das an unterschiedliche IP-Netze angeschlossen ist und zwischen diesen vermittelt. Dazu besitzt er für jedes an ihn angeschlossene Netz eine Schnittstelle (= Interface). Beim Eintreffen von Daten muss ein Router den richtigen Weg zum Ziel und damit die passende Schnittstelle bestimmen, über welche die Daten weiterzuleiten sind. Dazu bedient er sich einer lokal vorhandenen Routing-Tabelle, die angibt, über welchen Anschluss des Routers (bzw. welche Zwischenstation) welches Netzwerk erreichbar ist.

Trap

Vor allem in großen Netzwerken findet neben den anderen Protokollen zusätzlich das SNMP Protokoll (Simple Network Management Protocol) Verwendung. Dieses UDP-basierte Protokoll dient zur zentralen Administrierung von Netzwerkgeräten. Zum Beispiel kann man mit dem Befehl GET eine Konfigurationen abfragen, mit dem Befehl SET die Konfiguration eines Gerätes ändern, vorausgesetzt, das so angesprochene Netzwerkgerät ist SNMP-fähig.

Ein SNMP-fähiges Gerät kann zudem von sich aus SNMP-Nachrichten verschicken, z. B. wenn außergewöhnliche Ereignisse auftreten. Solche Nachrichten nennt man SNMP Traps.

X.509 Zertifikat

Eine Art „Siegel“, welches die Echtheit eines öffentlichen Schlüssels (→ asymmetrische Verschlüsselung) und zugehöriger Daten belegt.

Damit der Benutzer eines zum Verschlüsseln dienenden öffentlichen Schlüssels sichergehen kann, dass der ihm übermittelte öffentliche Schlüssel wirklich von seinem tatsächlichen Aussteller und damit der Instanz stammt, die die zu versendenden Daten erhalten soll, gibt es die Möglichkeit der Zertifizierung. Diese Beglaubigung der Echtheit des öffentlichen Schlüssels und die damit verbundene Verknüpfung der Identität des Ausstellers mit seinem Schlüssel übernimmt eine zertifizierende Stelle (*Certification Authority - CA*). Dies geschieht nach den Regeln der CA, indem der Aussteller des öffentlichen Schlüssels beispielsweise persönlich zu erscheinen hat. Nach erfolgreicher Überprüfung signiert die CA den öffentliche Schlüssel mit ihrer (digitalen) Unterschrift, ihrer Signatur. Es entsteht ein Zertifikat.

Ein X.509(v3) Zertifikat beinhaltet also einen öffentlichen Schlüssel, Informationen über den Schlüsseleigentümer (angegeben als Distinguised Name (DN)), erlaubte Verwendungszwecke usw. und die Signatur der CA. (→ Subject, Zertifikat).

Die Signatur entsteht wie folgt: Aus der Bitfolge des öffentlichen Schlüssels, den Daten über seinen Inhaber und aus weiteren Daten erzeugt die CA eine individuelle Bitfolge, die bis zu 160 Bit lang sein kann, den sog. HASH-Wert. Diesen verschlüsselt die CA mit ihrem privaten Schlüssel und fügt ihn dem Zertifikat hinzu. Durch die Verschlüsselung mit dem privaten Schlüssel der CA ist die Echtheit belegt, d. h. die verschlüsselte HASH-Zeichenfolge ist die digitale Unterschrift der CA, ihre Signatur. Sollten die Daten des Zertifikats missbräuchlich geändert werden, stimmt dieser HASH-Wert nicht mehr, das Zertifikat ist dann wertlos.

Der HASH-Wert wird auch als Fingerabdruck bezeichnet. Da er mit dem privaten Schlüssel der CA verschlüsselt ist, kann jeder, der den zugehörigen öffentlichen Schlüssel besitzt, die Bitfolge entschlüsseln und damit die Echtheit dieses Fingerabdrucks bzw. dieser Unterschrift überprüfen.

Durch die Heranziehung von Beglaubigungsstellen ist es möglich, dass nicht jeder Schlüsseleigentümer den anderen kennen muss, sondern nur die benutzte Beglaubigungsstelle. Die zusätzlichen Informationen zu dem Schlüssel vereinfachen zudem die Administrierbarkeit des Schlüssels.

X.509 Zertifikate kommen z. B. bei Email Verschlüsselung mittels S/MIME oder IPsec zum Einsatz.

Protokoll, Übertragungsprotokoll

Geräte, die miteinander kommunizieren, müssen dieselben Regeln dazu verwenden. Sie müssen dieselbe „Sprache sprechen". Solche Regeln und Standards bezeichnet man als Protokoll bzw. Übertragungsprotokoll. Oft benutze Protokolle sind z. B. IP, TCP, PPP, HTTP oder SMTP.

Service Provider

Anbieter, Firma, Institution, die Nutzern den Zugang zum Internet oder zu einem Online-Dienst verschafft.

Spoofing, Antispoofing

In der Internet-Terminologie bedeutet Spoofing die Angabe einer falschen Adresse. Durch die falsche Internet-Adresse täuscht jemand vor, ein autorisierter Benutzer zu sein.

Unter Anti-Spoofing versteht man Mechanismen, die Spoofing entdecken oder verhindern.

Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung werden Daten mit dem gleichen Schlüssel ver- und entschlüsselt. Beispiele für symmetrische Verschlüsselungsalgorithmen sind DES und AES. Sie sind schnell, jedoch bei steigender Nutzerzahl nur aufwendig administrierbar.

TCP/IP (Transmission Control Protocol/Internet Protocol)

Netzwerkprotokolle, die für die Verbindung zweier Rechner im Internet verwendet werden.

IP ist das Basisprotokoll.

UDP baut auf IP auf und verschickt einzelne Pakete. Diese können beim Empfänger in einer anderen Reihenfolge als der abgeschickten ankommen, oder sie können sogar verloren gehen.

TCP dient zur Sicherung der Verbindung und sorgt beispielsweise dafür, dass die Datenpakete in der richtigen Reihenfolge an die Anwendung weitergegeben werden.

UDP und TCP bringen zusätzlich zu den IP-Adressen Port-Nummern zwischen 1 und 65535 mit, über die die unterschiedlichen Dienste unterschieden werden.

Auf UDP und TCP bauen eine Reihe weiterer Protokolle auf, z. B. HTTP (Hyper Text Transfer Protokoll), HTTPS (Secure Hyper Text Transfer Protokoll), SMTP (Simple Mail Transfer Protokoll), POP3 (Post Office Protokoll, Version 3), DNS (Domain Name Service).

ICMP baut auf IP auf und enthält Kontrollnachrichten.

SMTP ist ein auf TCP basierendes E-Mail-Protokoll.

IKE ist ein auf UDP basierendes IPsec-Protokoll.

ESP ist ein auf IP basierendes IPsec-Protokoll.

Auf einem Windows-PC übernimmt die WINSOCK.DLL (oder WSOCK32.DLL) die Abwicklung der beiden Protokolle.

(→ „Datagramm" auf Seite 9-2)

VLAN

Über ein VLAN (Virtual Local Area Network) kann man ein physikalisches Netzwerk logisch in getrennte, nebeneinander existierende Netze unterteilen.

Die Geräte der unterschiedlichen VLANs können dabei nur Geräte in ihrem eigenen VLAN erreichen. Die Zuordnung zu einem VLAN wird damit nicht mehr nur allein von der Topologie des Netzes bestimmt, sondern auch durch die konfigurierte VLAN-ID.

Die VLAN Einstellung kann als optionale Einstellung zu jeder IP vorgenommen werden. Ein VLAN wird dabei durch seine VLAN-ID (1-4094) identifiziert. Alle Geräte mit der selben VLAN-ID gehören dem gleichen VLAN an und können miteinander kommunizieren.

Das Ethernet-Paket wird für VLAN nach IEEE 802.1Q um 4 Byte erweitert, davon stehen 12 Bit zur Aufnahme der VLAN-ID zur Verfügung. Die VLAN-ID „0“ und „4095“ sind reserviert und nicht zur Identifikation eines VLANs nutzbar.

VPN (Virtuelles Privates Netzwerk)

Ein **V**irtuelles **P**rivates **N**etzwerk (VPN) schließt mehrere voneinander getrennte private Netzwerke (Teilnetze) über ein öffentliches Netz, z. B. das Internet, zu einem gemeinsamen Netzwerk zusammen. Durch Verwendung kryptographischer Protokolle wird dabei die Vertraulichkeit und Authentizität gewahrt. Ein VPN bietet somit eine kostengünstige Alternative gegenüber Standleitungen, wenn es darum geht, ein überregionales Firmennetz aufzubauen.

10 Technische Daten

10.1 mGuard rs4000/rs2000

Hardware-Eigenschaften	mGuard rs4000	mGuard rs2000
Plattform	Freescale Netzwerkprozessor mit 330 MHz Taktung	Freescale Netzwerkprozessor mit 330 MHz Taktung
Netzwerk-Schnittstellen	1 LAN Port I 1 WAN Port Ethernet IEEE 802.3 10/100-BaseTX RJ 45 I Full Duplex I Auto-MDIX	1 LAN Port I 1 WAN Port Ethernet IEEE 802.3 10/100-BaseTX RJ 45 I Full Duplex I Auto-MDIX
Sonstige Schnittstellen	Seriell RS-232 9-poliger D-SUB-Stecker je 2 digitale Ein- und Ausgänge	Seriell RS-232 9-poliger D-SUB-Stecker je 2 digitale Ein- und Ausgänge
Speicher	128 MB RAM I 128 MB Flash SD-Karte wechselbarer Konfigurationsspeicher	128 MB RAM I 128 MB Flash SD-Karte wechselbarer Konfigurationsspeicher
Hochverfügbarkeit	optional: VPN I Router und Firewall	nicht verfügbar
Stromversorgung	Spannungsbereich 11 ... 36 V DC, redundant	Spannungsbereich 11 ... 36 V DC
Leistungsaufnahme	typisch 2,13 Watt	typisch 2,13 Watt
Luftfeuchtigkeitsbereich	5 % ... 95 % (Betrieb, Lagerung), nicht kondensierend	5 % ... 95 % (Betrieb, Lagerung), nicht kondensierend
Schutzart	IP20	IP20
Temperaturbereich	-20 °C ... +60 °C (Betrieb) -20 °C ... +60 °C (Lagerung)	-20 °C ... +60 °C (Betrieb) -20 °C ... +60 °C (Lagerung)
Maße (H x B x T)	130 x 45 x 114 mm (bis Auflage Tragschiene)	130 x 45 x 114 mm (bis Auflage Tragschiene)
Gewicht	725 g (TX/TX)	722 g (TX/TX)

Firmware und Leistungswerte		
Firmware-Kompatibilität	mGuard v7.4.0 oder höher; Innominate empfiehlt die Verwendung der jeweils aktuellen Firmware Version und Patch Releases Funktionsumfang siehe entsprechendes Firmware-Datenblatt	
Datendurchsatz (Router I Firewall)	99 Mbit/s bidirektional	99 Mbit/s bidirektional
Virtual Private Network (VPN)	IPsec (IETF-Standard) bis zu 250 VPN-Tunnel	IPsec (IETF-Standard) bis zu 2 VPN-Tunnel
Hardware-basierte Verschlüsselung	DES I 3DES I AES-128/192/256	DES I 3DES I AES-128/192/256
Verschlüsselter VPN-Durchsatz (AES-256)	35 Mbit/s bidirektional	35 Mbit/s bidirektional
Management Support	Web GUI (HTTPS) I Command Line Interface (SSH) I SNMP v1/2/3 I zentrale Device Management Software	
Diagnose	LEDs (Power 1 + 2, State, Error, Signal, Fault, Modem, Info) Meldekontakte I Servicekontakte I Log-File I Remote-Syslog	LEDs (Power, State, Error, Signal, Fault, Modem, Info) Meldekontakte I Servicekontakte I Log-File I Remote-Syslog

Sonstiges	mGuard rs4000	mGuard rs2000
Konformität	CE I FCC I UL 508 ANSI/ISA 12.12 Class I div. 2 (in Vorbereitung)	CE I FCC I UL 508
Besonderheiten	Echtzeituhr I Trusted Platform Module (TPM) I Temperatursensor I mGuard Remote Services Portal ready	

10.2 mGuard centerport

Hardware-Eigenschaften	
Plattform	Multi-Core x86 Prozessorarchitektur
Netzwerk Schnittstellen	1 LAN Port I 1 WAN Port Ethernet IEEE 802.3 10/100/1000 Base TX I RJ 45 I Full/Half Duplex I Auto-MDIX
Sonstige Schnittstellen	VGA-Konsole I 2 x seriell RS-232, D-Sub 9-polig, Stecker I 6 x USB
Laufwerke	1 HDD I 1 DVD-RW
Hochverfügbarkeit	abhängig von der verwendeten Firmware
Stromversorgung	2 x 100 V AC ... 240 V AC, 250 W bei 50/60 Hz, redundant
Leistungsaufnahme	abhängig von der jeweiligen Ausbaustufe
Luftfeuchtigkeitsbereich	20 % ... 90 % in Betrieb, nicht kondensierend 10 % ... 90 % außer Betrieb
Schutzart	Front IP20
Temperaturbereich	0 °C ... +50 °C (Betrieb) -20 °C ... +70 °C (Lager)
Maße (H x B x T)	88 x 482 x 472 mm (2 HE x 19“ x 18.58“)
Gewicht	10 kg

Firmware und Leistungswerte	
Firmware-Kompatibilität	mGuard v7.1 oder höher; Innominate empfiehlt den Einsatz in den jeweils aktuellen Patch Releases; Funktionsumfang siehe entsprechendes Firmware Datenblatt
Datendurchsatz (Router I Firewall)	2.000 Mbit/s bidirektional I 2.000 Mbit/s bidirektional
Hardware-basierte Verschlüsselung	DES I 3DES I AES-128/192/256
Verschlüsselter VPN Durchsatz (AES-256)	300 Mbit/s bidirektional
Management Support	Web GUI (HTTPS) I Command Line Interface (SSH) I SNMP v1/2/3 I zentrale Device Management Software
Diagnose	LEDs (1 x Power, 1 x HDD) I Boot-Menü I Log-File I Remote-Syslog

Sonstiges	
Konformität	CE, entwickelt nach UL-Anforderungen

10.3 mGuard industrial rs

Hardware-Eigenschaften	
Plattform	Intel Netzwerkprozessor mit 533 MHz Taktung
Netzwerk-Schnittstellen	1 LAN Port I 1 WAN Port Ethernet IEEE 802.3 10/100 Base TX I RJ 45 I Full Duplex I Auto-MDIX
Sonstige Schnittstellen	seriell RS-232, RJ11 Buchse I optional Analog-Modem I optional ISDN-TA
Laufwerke	–
Hochverfügbarkeit	abhängig von der verwendeten Firmware
Stromversorgung	24 V DC I 170 mA I SELV I redundant I 9-36 V Spannungsbereich
Leistungsaufnahme	typisch 4,1 Watt
Luftfeuchtigkeitsbereich	10 % ... 95 % in Betrieb, nicht kondensierend
Schutzart	IP20
Temperaturbereich	0 °C ... +55 °C (Betrieb) -20 °C ... +70 °C (Lager)
Maße (H x B x T)	100 x 45 x 112 mm
Gewicht	250 g

Firmware und Leistungswerte	
Firmware-Kompatibilität	mGuard v5.0 oder höher; Innominate empfiehlt Firmware Version 6.x oder 7.x in den jeweils aktuellen Patch Releases; Funktionsumfang siehe entsprechendes Firmware-Datenblatt
Datendurchsatz (Router I Firewall)	99 Mbit/s bidirektional I 99 Mbit/s bidirektional
Hardware-basierte Verschlüsselung	DES I 3DES I AES-128/192/256
Verschlüsselter VPN-Durchsatz (AES-256)	70 Mbit/s bidirektional
Management Support	Web GUI (HTTPS) I Command Line Interface (SSH) I SNMP v1/2/3 I zentrale Device Management Software I optional Schlüsselschalter (VPN)
Diagnose	LEDs (P1, P2, Modem, Fault, State, Error, LAN, WAN) I Meldekontakt (SELV) I Servicekontakte (⊥, CMD, ACK) I Log-File I Remote-Syslog

Sonstiges	
Konformität	CE I FCC I UL 508

10.4 mGuard smart^2

Hardware-Eigenschaften	
Plattform	Freescale Netzwerkprozessor mit 330 MHz Taktung
Netzwerk-Schnittstellen	1 LAN Port I 1 WAN Port Ethernet IEEE 802.3 10/100 Base TX I RJ 45 I Full Duplex I Auto-MDIX
Sonstige Schnittstellen	Seriell über USB-Anschluss
Laufwerke	–
Hochverfügbarkeit	abhängig von der verwendeten Firmware
Stromversorgung	über USB Schnittstelle (5 V bei 500 mA) optional: externes Netzteil (110 V ... 230 V)
Leistungsaufnahme	max. 2,5 Watt
Temperaturbereich	0 °C ... +40 °C (Betrieb) -20 °C ... +60 °C (Lager)
Luftfeuchtigkeitsbereich	20 % ... 90 % in Betrieb, nicht kondensierend
Schutzart	IP30
Maße (H x B x T)	27 x 77 x 115 mm
Gewicht	131 g

Firmware und Leistungswerte	
Firmware-Kompatibilität	mGuard v7.2 oder höher; Innominate empfiehlt Firmware Version 7.x in den jeweils aktuellen Patch Releases; Funktionsumfang siehe entsprechendes Firmware-Datenblatt
Datendurchsatz (Router I Firewall)	99 Mbit/s bidirektional
Hardware-basierte Verschlüsselung	DES I 3DES I AES-128/192/256
Verschlüsselter VPN-Durchsatz (AES-256)	35 Mbit/s (smart /256) bidirektional
Management Support	Web GUI (HTTPS) I Command Line Interface (SSH) I SNMP v1/2/3 I zentrale Device Management Software
Diagnose	3 LEDs (in Kombination für Bootvorgang, Heartbeat, Systemfehler, Ethernet-status, Recovery-Modus) I Log-File I Remote-Syslog

Sonstiges	
Konformität	CE I FCC
Besonderheiten	Echtzeituhr I Trusted Platform Module (TPM) I Temperatursensor

10.5 mGuard smart

mGuard smart /266 | mGuard smart /533

Hardware-Eigenschaften	
Plattform	Intel Netzwerkprozessor wahlweise mit 533 MHz oder 266 MHz Taktung
Netzwerk-Schnittstellen	1 LAN Port	1 WAN Port Ethernet IEEE 802.3 10/100 Base TX | RJ 45	Full Duplex	Auto-MDIX
Sonstige Schnittstellen	–
Laufwerke	–
Hochverfügbarkeit	abhängig von der verwendeten Firmware
Stromversorgung	über USB-Schnittstelle (5 V bei 500 mA) optional: externes Netzteil (110 V ... 230 V)
Leistungsaufnahme	max. 2,5 Watt
Temperaturbereich	0 °C ... +40 °C (Betrieb) -20 °C ... +70 °C (Lager)
Luftfeuchtigkeitsbereich	20 % ... 90 % in Betrieb, nicht kondensierend
Schutzart	IP30
Maße (H x B x T)	27 x 77 x 115 mm
Gewicht	158 g

Firmware und Leistungswerte	
Firmware-Kompatibilität	mGuard v5.0 oder höher; Innominate empfiehlt Firmware Version 6.x oder 7.x in den jeweils aktuellen Patch Releases; Funktionsumfang siehe entsprechendes Firmware-Datenblatt
Datendurchsatz (Router	Firewall)	99 Mbit/s bidirektional	99 Mbit/s bidirektional
Hardware-basierte Verschlüsselung	DES	3DES	AES-128/192/256
Verschlüsselter VPN-Durchsatz (AES-256)	35 Mbit/s (smart /256) bidirektional	70 Mbit/s (smart /533) bidirektional
Management Support	Web GUI (HTTPS)	Command Line Interface (SSH)	SNMP v1/2/3	zentrale Device Management Software
Diagnose	LEDs (3 Stck. in Kombination für Bootvorgang, Heartbeat, Systemfehler, Ethernetstatus, Recovery-Modus)	Log-File	Remote-Syslog

Sonstiges	
Konformität	CE	FCC

10.6 mGuard pci² SD

mGuard pci² SD | mGuard pcie² SD

Hardware-Eigenschaften		
Plattform		Freescale Netzwerkprozessor mit 330 MHz Taktung
Netzwerk-Schnittstellen		1 LAN Port | 1 WAN Port Ethernet IEEE 802.3 10/100 Base TX | RJ 45 | Full Duplex | Auto-MDIX
Sonstige Schnittstellen		seriell RS-232, interne Steckleiste
Speicher		128 MB RAM | 128 MB Flash SD-Karte, wechselbarer Konfigurationsspeicher
Laufwerke		–
Hochverfügbarkeit		optional: VPN | Router
Stromversorgung		3,3 V oder 5 V, via PCI- (mGuard pci² SD) oder PCI Express-Bus (mGuard pcie² SD)
Leistungsaufnahme		typisch 3,7 W ... 4,2 W
Luftfeuchtigkeitsbereich		5 % ... 95 % in Betrieb und Lagerung, nicht kondensierend
Schutzart		je nach Einbauart, abhängig vom Wirtssystem
Temperaturbereich	ohne Akku	0 °C ... +70 °C (Betrieb) -20 °C ... +70 °C (Lager)
	mit Akku	0 °C ... +60 °C (Betrieb) -20 °C ... +60 °C (Lager)
Maße (H x B x T)		950 mm x 18 mm x 130 mm
Gewicht		72 g

Firmware und Leistungswerte	
Firmware-Kompatibilität	mGuard v7.5.0 oder höher; Innominate empfiehlt die Verwendung der jeweils aktuellen Firmware-Version und Patch Releases Funktionsumfang siehe entsprechendes Firmware-Datenblatt
Datendurchsatz (Router | Firewall)	99 Mbit/s bidirektional
Hardware-basierte Verschlüsselung	DES | 3DES | AES-128/192/256
Verschlüsselter VPN-Durchsatz (AES-256)	35 Mbit/s bidirektional
Management Support	Web GUI (HTTPS) | Command Line Interface (SSH) | SNMP v1/2/3 | zentrale Device Management Software
Diagnose	LEDs (2 x LAN, 2 x WAN in Kombination) für Ethernet-Status und Geschwindigkeit; 1 LED für Power, Error, State, Fault, Info) | Log-File | Remote-Syslog

Sonstiges	
Konformität	CE | FCC
Besonderheiten	Echtzeituhr | Trusted Platform Module (TPM) | Temperatursensor | mGuard Remote Services Portal ready

10.7 mGuard pci

mGuard pci /266 | mGuard pci /533

Hardware-Eigenschaften	
Plattform	Intel Netzwerkprozessor wahlweise mit 266 oder 533 MHz Taktung
Netzwerk-Schnittstellen	1 LAN Port	1 WAN Port Ethernet IEEE 802.3 10/100 Base TX | RJ 45	Full Duplex	Auto-MDIX
Sonstige Schnittstellen	seriell RS-232, interne Steckleiste
Laufwerke	–
Hochverfügbarkeit	abhängig von der verwendeten Firmware
Stromversorgung	3,3 V oder 5 V, via PCI Bus
Leistungsaufnahme	typisch 3,7 W ... 4,2 W
Luftfeuchtigkeitsbereich	20 % ... 90 % in Betrieb, nicht kondensierend
Schutzart	je nach Einbauart
Temperaturbereich	0 °C ... +70 °C (Betrieb) -20 °C ... +70 °C (Lager)
Maße (H x B x T)	low profile PCI
Gewicht	72 g

Firmware und Leistungswerte	
Firmware-Kompatibilität	mGuard v5.0 oder höher; Innominate empfiehlt Firmware Version 6.x oder 7.x in den jeweils aktuellen Patch Releases; Funktionsumfang siehe entsprechendes Firmware-Datenblatt
Datendurchsatz (Router	Firewall)	99 Mbit/s bidirektional	99 Mbit/s bidirektional
Hardware-basierte Verschlüsselung	DES	3DES	AES-128/192/256
Verschlüsselter VPN-Durchsatz (AES-256)	35 Mbit/s (pci /256) bidirektional	70 Mbit/s (pci /533) bidirektional
Management Support	Web GUI (HTTPS)	Command Line Interface (SSH)	SNMP v1/2/3	zentrale Device Management Software
Diagnose	LEDs (2 x LAN, 2 x WAN in Kombination für Bootvorgang, Systemfehler, Ethernetstatus, Recovery-Modus)	Log-File	Remote-Syslog

Sonstiges	
Konformität	CE	FCC	UL 508	Betriebsmodi mit /ohne Treiber durch PoPCI

10.8 mGuard blade

mGuard blade /266 | mGuard blade /533

Hardware-Eigenschaften	
Plattform	Intel Netzwerkprozessor wahlweise mit 533 MHz oder 266 MHz Taktung
Netzwerk-Schnittstellen	1 LAN Port	1 WAN Port Ethernet IEEE 802.3 10/100 Base TX | RJ 45	Full Duplex	Auto-MDIX
Sonstige Schnittstellen	seriell RS-232, RJ11-Buchse
Laufwerke	–
Hochverfügbarkeit	abhängig von der verwendeten Firmware
Stromversorgung	über *bladebase*: 100 V AC ... 240 V AC bei 50/60 Hz
Leistungsaufnahme	*blade:* typisch 3 Watt *bladebase:* typisch 42 Watt
Luftfeuchtigkeitsbereich	10 % ... 95 % in Betrieb, nicht kondensierend
Schutzart	IP20
Temperaturbereich	+5 °C ... +40 °C (Betrieb) -20 °C... +70 °C (Lager)
Maße (H x B x T)	*blade*: 100 x 26 x 160 mm *bladebase*: 133 x 483 x 235 mm (3 HE)
Gewicht	*blade*: 245 g	*bladepack*: 7,7 kg

Firmware und Leistungswerte	
Firmware-Kompatibilität	mGuard v5.0 oder höher; Innominate empfiehlt Firmware Version 6.x oder 7.x in den jeweils aktuellen Patch Releases; Funktionsumfang siehe entsprechendes Firmware-Datenblatt
Datendurchsatz (Router	Firewall)	99 Mbit/s bidirektional	99 Mbit/s bidirektional
Hardware-basierte Verschlüsselung	DES	3DES	AES-128/192/256
Verschlüsselter VPN-Durchsatz (AES-256)	35 Mbit/s (blade /256) bidirektional	70 Mbit/s (blade /533) bidirektional
Management Support	Web GUI (HTTPS)	Command Line Interface (SSH)	SNMP v1/2/3	zentrale Device Management Software
Diagnose	LEDs (2 x LAN, 2 x WAN in Kombination für Bootvorgang, Systemfehler, Ethernetstatus, Recovery-Modus)	Log-File	Remote-Syslog

Sonstiges	
Konformität	CE	FCC

10.9 mGuard delta²

Hardware-Eigenschaften	
Plattform	Freescale Netzwerkprozessor mit 330 MHz Taktung
Netzwerk-Schnittstellen	1 LAN Port I 1 WAN Port Ethernet IEEE 802.3 10/100 Base TX I RJ 45 I Full Duplex I Auto-MDIX
Sonstige Schnittstellen	seriell RS-232, D-Sub 9-polig, Stecker
Speicher	128 MB RAM I 128 MB Flash SD-Karte, wechselbarer Konfi gurationsspeicher
Hochverfügbarkeit	optional: VPN I Router
Stromversorgung	externes Netzteil 12V / 0,85A DC I 100–240V / 0,4A AC
Leistungsaufnahme	typisch 2,13 Watt
Luftfeuchtigkeitsbereich	5 % ... 95 % in Betrieb, nicht kondensierend
Schutzart	IP20
Temperaturbereich	0 °C ... +40 °C (Betrieb) 0 °C ... +60 °C (Lager)
Maße (H x B x T)	45 x 130 x 114 mm
Gewicht	629 g

Firmware und Leistungswerte	
Firmware-Kompatibilität	mGuard v7.4.0 oder höher; Innominate empfiehlt die Verwendung der jeweils aktuellen Firmware-Version und Patch Releases Funktionsumfang siehe entsprechendes Firmware-Datenblatt
Datendurchsatz (Router I Firewall)	99 Mbit/s bidirektional I 99 Mbit/s bidirektional
Virtual Private Network (VPN)	IPsec (IETF-Standard), VPN-Modelle bis 10 Tunnel, optional bis zu 250 VPN-Tunnel
Hardware-basierte Verschlüsselung	DES I 3DES I AES-128/192/256
Verschlüsselter VPN-Durchsatz (AES-256)	35 Mbit/s bidirektional
Management Support	Web GUI (HTTPS) I Command Line Interface (SSH) I SNMP v1/2/3 I zentrale Device Management Software
Diagnose	LEDs (Power, State, Error, Fault, Info) I Log-File I Remote-Syslog

Sonstiges	
Konformität	CE I FCC
Besonderheiten	Echtzeituhr I Trusted Platform Module (TPM) I Temperatursensor I mGuard Remote Services Portal ready

10.10 mGuard delta

Hardware-Eigenschaften	
Plattform	Intel Netzwerkprozessor mit 533 MHz Taktung
Netzwerk-Schnittstellen	4 LAN Port Switch unmanaged I 1 WAN Port Ethernet IEEE 802.3 10/100 Base TX I RJ 45 I Full Duplex I Auto-MDIX
Sonstige Schnittstellen	seriell RS-232, D-Sub 9-polig, Stecker
Laufwerke	–
Hochverfügbarkeit	abhängig von der verwendeten Firmware
Stromversorgung	externes Netzteil 5 V/3 A, DC I 110 V ... 230 V, AC
Leistungsaufnahme	typisch 4,5 Watt
Luftfeuchtigkeitsbereich	5 % ... 95 % in Betrieb, nicht kondensierend
Schutzart	IP20
Temperaturbereich	0 °C ... +40 °C (Betrieb) -20 °C ... +70 °C (Lager)
Maße (H x B x T)	30 x 239 x 156 mm
Gewicht	1300 g

Firmware und Leistungswerte	
Firmware-Kompatibilität	mGuard v5.0 oder höher; Innominate empfiehlt Firmware Version 6.x oder 7.x in den jeweils aktuellen Patch Releases; Funktionsumfang siehe entsprechendes Firmware-Datenblatt
Datendurchsatz (Router I Firewall)	99 Mbit/s bidirektional I 99 Mbit/s bidirektional
Hardware-basierte Verschlüsselung	DES I 3DES I AES-128/192/256
Verschlüsselter VPN-Durchsatz (AES-256)	70 Mbit/s bidirektional
Management Support	Web GUI (HTTPS) I Command Line Interface (SSH) I SNMP v1/2/3 I zentrale Device Management Software
Diagnose	7 LEDs (Power, Status, WAN, LAN 1 – 4) I Log-File I Remote-Syslog

Sonstiges	
Konformität	CE I FCC

10.11 EAGLE mGuard

Hardware-Eigenschaften	
Plattform	Intel Netzwerkprozessor mit 533 MHz Taktung
Netzwerk-Schnittstellen	1 LAN Port I 1 WAN Port Ethernet IEEE 802.3 10/100 Base TX I RJ 45 I Full Duplex I Auto-MDIX I optional 100 Base FX (F0)
Sonstige Schnittstellen	seriell RS-232, RJ11 Buchse I USB
Laufwerke	–
Hochverfügbarkeit	abhängig von der verwendeten Firmware
Stromversorgung	24 V DC I max. 300 mA I PELV/SELV I redundant I-25 % ... +25 % Spannungsbereich
Leistungsaufnahme	max. 7,2 Watt bei 24 V
Luftfeuchtigkeitsbereich	10 % ... 95 % in Betrieb, nicht kondensierend
Schutzart	IP20
Temperaturbereich	0 °C ... +60 °C (Betrieb) -40 °C ... +80 °C (Lager)
Maße (H x B x T)	131 x 47 x 111 mm
Gewicht	340 g

Firmware und Leistungswerte	
Firmware-Kompatibilität	mGuard v5.0 oder höher; Innominate empfiehlt Firmware Version 6.x oder 7.x in den jeweils aktuellen Patch Releases; Funktionsumfang siehe entsprechendes Firmware-Datenblatt
Datendurchsatz (Router I Firewall)	99 Mbit/s bidirektional I 99 Mbit/s bidirektional
Hardware-basierte Verschlüsselung	DES I 3DES I AES-128/192/256
Verschlüsselter VPN-Durchsatz (AES-256)	70 Mbit/s bidirektional
Management Support	Web GUI (HTTPS) I Command Line Interface (SSH) I SNMP v1/2/3 I zentrale Device Management Software
Diagnose	LEDs (P1, P2, Status, Fault, LAN, WAN, V.24) I Meldekontakt (24 V, 1 A) I Log-File I Remote-Syslog
Sonstiges	EAGLE mGuard

Sonstiges	
Konformität	CE I FCC I UL 508 I GL