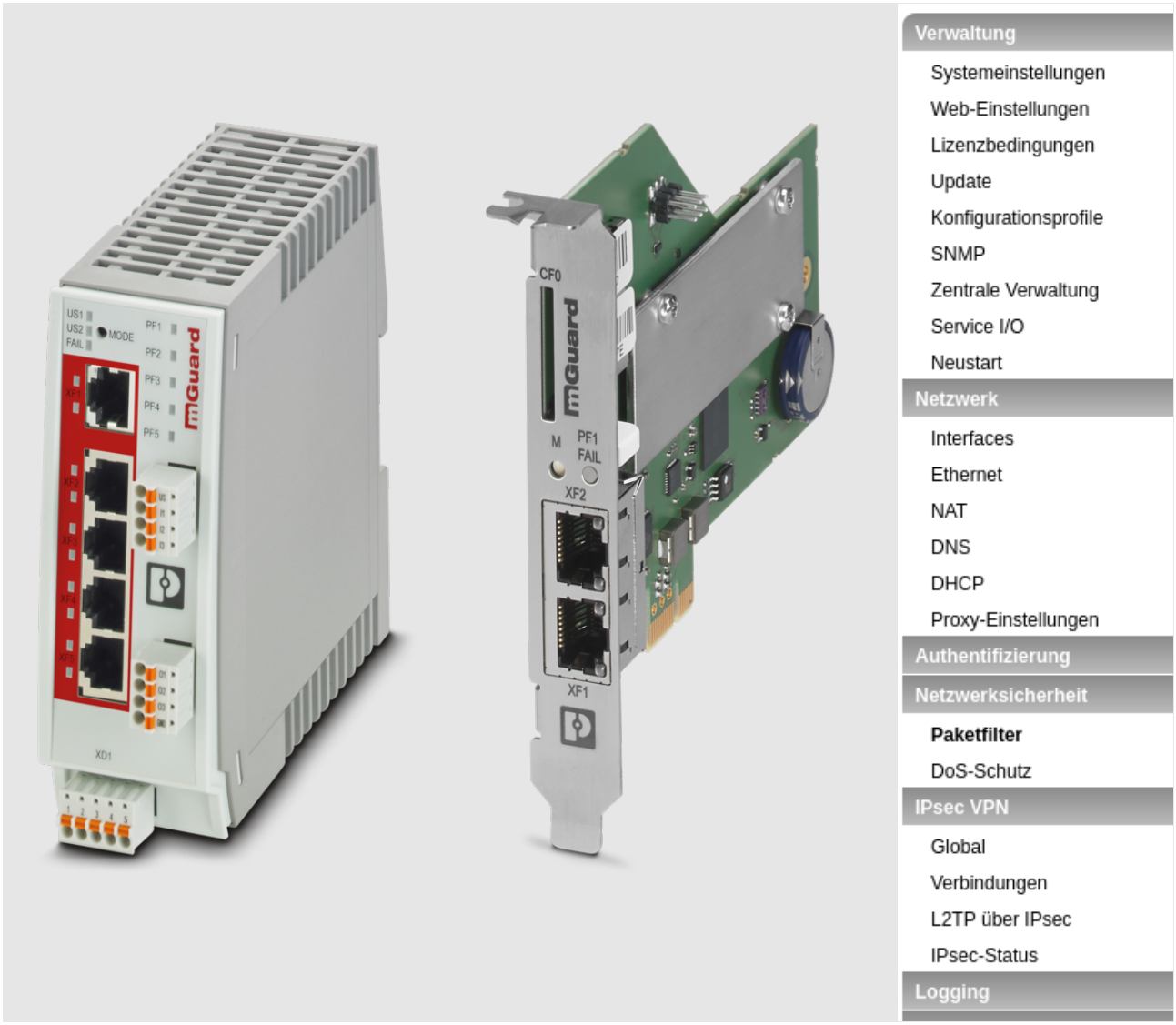


FL MGUARD 2000/4000 Web-based Management mGuard 10.5.x

Anwenderhandbuch

Anwenderhandbuch

FL MGUARD 2000/4000 - Web-based Management mGuard 10.5.x

UM DE FW MGUARD10 , Revision 09 2025-01-30

Dieses Handbuch ist gültig für:

Bezeichnung	Artikel-Nr.
FL MGUARD 2102	1357828
FL MGUARD 4302	1357840
FL MGUARD 4302/KX	1696708
FL MGUARD 2105	1357850
FL MGUARD 4305	1357875
FL MGUARD 4305/KX	1696779
FL MGUARD 4102 PCI	1441187
FL MGUARD 4102 PCIE	1357842

Firmware-Version: mGuard 10.5.x

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

Release Notes

mGuard 10.5.x Firmware – Release Notes

Benutzerhandbuch „Installation und Inbetriebnahme“

UM DE HW FL MGUARD 2000/4000 – 110192_de_xx

Benutzerhandbuch „Generic Administration Interface - gaiconfig User Guide“:

UM DE GAICONFIG MGUARD10 – 110193_de_xx

Benutzerhandbuch „Installation, Konfiguration und Benutzung des mGuard device manager (mdm)“:

UM DE MDM 1.17 – 111024_de_xx

Benutzerhandbuch „IEC 62443-4-2-konforme Konfiguration der FL MGUARD-Produktfamilie“:

UM DE MGUARD 62443-4-2 – 109049_de_xx

110191_de_09

Inhaltsverzeichnis

1 Zu Ihrer Sicherheit

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

1.1 Kennzeichnung der Warnhinweise

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

Hier finden Sie zusätzliche Informationen oder weiterführende Informationsquellen.

1.2 Über dieses Handbuch

Folgende Elemente werden in diesem Handbuch verwendet:

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

1.3 Qualifikation der Benutzer

Der in diesem Handbuch beschriebene Produktgebrauch richtet sich ausschließlich an

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

1.4 Bestimmungsgemäße Verwendung

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

1.5 Veränderung des Produkts

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

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

1.6 Sicherheitshinweise

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

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

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

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

ACHTUNG: Anforderung an den Schaltschrank/Schaltkasten
Tragschienengeräte werden innerhalb eines Schaltschranks oder -kastens auf eine Norm-Tragschiene aufgerastet. Dieser Schaltschrank/-kasten muss den Anforderungen der IEC/EN 62368-1 bez. der Brandschutzumhüllung genügen.

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

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

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

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

ACHTUNG: Beachten Sie beim Einsatz des Geräts folgende Sicherheitshinweise.

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

1.6.1 Sicherheitshinweise zur Installation in Zone 2 (nur Geräte mit Ex-Zulassung)

– Das Gerät der Kategorie 3 ist zur Installation im explosionsgefährdeten Bereich der Zone 2 geeignet. Es erfüllt die Anforderungen der EN 60079-0 und EN 60079-7.
– Das Gerät ist nicht für den Einsatz in staubexplosionsgefährdeten Atmosphären ausgelegt.
– Das Konfigurieren des Geräts mittels DIP-Schalter, Taster oder weiterer zugänglicher Schalter am Gerät ist nur außerhalb des explosionsgefährdeten Bereichs erlaubt.
– Halten Sie die festgelegten Bedingungen für den Einsatz in explosionsgefährdeten Bereichen ein. Setzen Sie bei der Installation ein geeignetes, zugelassenes Gehäuse der Mindestschutzart IP54 ein, das die Anforderungen der IEC/EN 60079-7 und GB/T 3836.1-2010 erfüllt. Beachten Sie auch die Anforderungen der IEC/EN 60079-14.
– An Stromkreise der Zone 2 dürfen nur Geräte angeschlossen werden, die für den Betrieb in der Ex-Zone 2 und die am Einsatzort vorliegenden Bedingungen geeignet sind.
– Das Trennen und Verbindungen von Leitungen, SFP-Modulen und SD-Karten im explosionsgefährdeten Bereich ist nur im spannungslosen Zustand zulässig.
– Verwenden Sie nur einwandfreie Ethernet-Leitungen mit funktionierender Verrastung.
– Steckbare Verbindungen (z. B. Stecker, SD-Karte) müssen eine funktionsfähige Verriegelung aufweisen (z. B. Rasthaken, Verschraubung). Setzen Sie die Verriegelung ein und setzen Sie beschädigte Verriegelungen unverzüglich instand. Stellen Sie sicher, dass alle steckbaren Verbindungen vollständig eingesteckt sind.
– Das Gerät ist außer Betrieb zu nehmen und unverzüglich aus dem Ex-Bereich zu entfernen, wenn es beschädigt ist, unsachgemäß belastet oder gelagert wurde bzw. Fehlfunktionen aufweist.
– Die Umgebungstemperatur innerhalb des Endverbrauchergehäuses muss innerhalb von 25 mm zum Gerät gemessen und eingehalten werden.
– Schließen Sie nur eine Leitung pro Klemmpunkt an.
– Der Luftdruck im Betrieb ist begrenzt auf 108 kPa.
– Galvanische Isolierung, 500 V AC nach EN/IEC 60079-7. Beachten Sie die Einschränkungen in den besonderen Verwendungsbedingungen.

– Zwischen den Spannungsversorgungsanschlüssen und FE leiten Überspannungsableiter Störungen <500 V_{eff} ab. Ziehen Sie deshalb vor der Isolationsmessung den Spannungsversorgungsstecker ab. Andernfalls sind Isolationsfehlmessungen möglich. Setzen Sie den Stecker nach der Isolationsmessung wieder in die vorgesehene Buchse ein.

1.7 IT-Sicherheit

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

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

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

Weiterführende Informationen zu den im Folgenden genannten Maßnahmen erhalten Sie auf den folgenden Webseiten (letzter Zugriff am 15.01.2025):

– bsi.bund.de/it-sik.html

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

Verwenden Sie die jeweils aktuelle Firmware-Version

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

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

Verwenden Sie die jeweils aktuelle Firmware-Version

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

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

Verwenden Sie die jeweils aktuelle Dokumentation

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

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

Stellen Sie die Integrität von heruntergeladenen Dateien sicher

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

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

Führen Sie regelmäßige Bedrohungsanalysen durch

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

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

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

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

Deaktivieren Sie nicht benötigte Kommunikationskanäle

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

Binden Sie Komponenten und Systeme nicht in öffentliche Netzwerke ein

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

Beschränken Sie die Zugangsberechtigung zum Gerät

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

Sichern Sie den Zugriff ab

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

Verwenden Sie bei Fernzugriff sichere Zugriffswege

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

Verwenden Sie eine Firewall

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

Aktivieren Sie eine sicherheitsrelevante Ereignisprotokollierung (Logging)

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

Schützen Sie den Zugriff auf die SD-Karte

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

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

1.8 Aktuelle Sicherheitshinweise zu Ihrem Produkt

Product Security Incident Response Team (PSIRT)

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

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

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

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

1.9 Support

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

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

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

Die Verwendung von Snapshots wird in diesem Anwenderhandbuch beschrieben.

2 Grundlagen mGuard

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

- Industrial Security Netzwerkrouter
- Modellabhängig mit eingebautem 3- oder 4-Port-Switch und DMZ-Port
- VPN-Router für sichere Datenübertragung über öffentliche Netze (AES-Verschlüsselung, IPsec- und OpenVPN-Protokoll)
- Konfigurierbare Firewall für den Schutz vor unberechtigtem Zugriff. Der dynamische Paketfilter untersucht Datenpakete anhand der Ursprungs- und Zieladresse und blockiert unerwünschten Datenverkehr.

2.1 Neue Geräteplattform FL MGUARD 2000/4000

Mit den Geräten der FL MGUARD 2000/4000-Serie werden die etablierten mGuard-Geräte der RS2000/RS4000- und PCI(E)4000-Serie nach und nach ersetzt.

Die neuen Geräte mit bewährter *mGuard Security Technology* sind mit schnellem Gigabit-Ethernet ausgestattet und werden mit der Firmware-Version mGuard 10.x betrieben.

Die Geräte sind kompatibel zu ihren Vorgängermodellen, können bestehende Konfigurationsprofile (atv-Dateien) importieren und über CGI- und GAI-Schnittstellen konfiguriert werden.

Der mGuard device manager (ab Version mdm 1.17.0) kann zur **Verwaltung** von mGuard-Geräten mit installierter Firmware-Version bis mGuard 10.5.x verwendet werden (siehe Benutzerhandbuch „UM DE MDM 1.17“ – 111024_de_xx).

Einige Gerätefunktionen der Vorgängermodelle werden auf den neuen Modellen nicht unterstützt (siehe Kapitel 2.1.1).

2.1.1 Nicht mehr unterstützte Funktionen

Auf der neuen Geräteplattform werden bestimmte Funktionen der alten Geräteplattform nicht mehr unterstützt.

Hardware

Die neuen mGuard-Modelle der FL MGUARD 2000/4000-Serie verfügen über keine serielle Schnittstelle und kein internes Modem.

Firmware (Funktionen)

Gerätefunktionen, die auf der neuen Geräteplattform nicht unterstützt werden, sind in Tabelle 2-1 aufgeführt.

Tabelle 2-1 Aktuell nicht unterstützte Gerätefunktionen

Funktionen, die in der Firmware mGuard 10.5.x aktuell nicht unterstützt werden
Netzwerk: Interfaces – PPPoE – PPTP – Sekundäres externes Interface
Netzwerk: Serielle Schnittstelle
Netzwerk: GRE-Tunnel (Generic Routing Encapsulation)
VPN-Redundanz
Quality of Service (QoS)
CIFS-Integrity-Monitoring
SEC-Stick
Update-Methode „Online-Update“ (Installation von Package-Sets)

Bei der Übertragung von älteren Gerätekonfigurationen auf die neuen Geräte muss deshalb darauf geachtet werden, dass die in Tabelle 2-1 beschriebenen Funktionen vor dem Export in der Gerätekonfiguration deaktiviert bzw. auf Werkseinstellungen zurückgesetzt wurden (siehe auch Kapitel 2.1.6).

2.1.2 Hinzugefügte Funktionen, die auf der alten Geräteplattform bereits vorhanden waren

Auf der neuen Geräteplattform wurden Variablen erneut hinzugefügt, die auf der alten Geräteplattform bereits vorhanden aber zwischenzeitlich entfernt worden waren.

Tabelle 2-2 Neu hinzugefügte Funktionen / Variablen / Variablenwerte

Neue Funktion / Variable /Werte	Neue Funktion / Auswirkung Migration	Firmware (Eingefügt mit Firmware-Version)
[Deep Packet Inspection / Modbus TCP] **Menü:** Netzwerksicherheit >> Deep Packet Inspection >> Modbus TCP **Sektion:** Regelsätze **Variable:** diverse **GAI-Variablen:** MODBUS_RULESETS.x.FRIENDLY_NAME MODBUS_RULESETS.x.SET.y.MODBUS_FUNCTION_CODE MODBUS_RULESETS.x.SET.y.ADDRESS_RANGE MODBUS_RULESETS.x.SET.y.TARGET MODBUS_RULESETS.x.SET.y.COMMENT MODBUS_RULESETS.x.SET.y.LOG MODBUS_RULESETS.x.LOG_DEFAULT	Das mGuard-Gerät kann Pakete ein- und ausgehender Modbus-TCP-Verbindungen prüfen (*Deep Packet Inspection*) und bei Bedarf filtern. **Migration von älteren mGuard-Konfigurationen** Keine Auswirkungen. Bereits konfigurierte Variablenwerte werden übernommen.	**10.5.0**
[Deep Packet Inspection / OPC Inspector] **Menü:** Netzwerksicherheit >> Deep Packet Inspection >> OPC Inspector **Sektion:** OPC Inspector **Variable:** diverse **GAI-Variablen:** IP_CONNTRACK_OPC IP_CONNTRACK_OPC_SANITY IP_CONNTRACK_OPC_TIMEOUT	Die Nutzung des Netzwerk-Protokolls *OPC Classic* ist über Firewalls hinweg bislang nur möglich, wenn große Port-Bereiche geöffnet werden. Die Aktivierung der *OPC Classic*-Funktion erlaubt die einfache Nutzung dieses Netzwerk-Protokolls, ohne die Firewall des mGuard-Geräts unsicher konfigurieren zu müssen. **Migration von älteren mGuard-Konfigurationen** Keine Auswirkungen. Bereits konfigurierte Variablenwerte werden übernommen.	**10.5.0**
[Web-Zugriff über HTTPS / Server-Zertifikat] **Menü:** Verwaltung >> Web-Einstellungen >> Zugriff **Sektion:** Web-Zugriff über HTTPS **Variable:** HTTPS Server-Zertifikat **GAI-Variable:** HTTPS_SERVER_CERT_REF In früheren Firmware-Versionen war die Funktion offiziell **nicht verfügbar**, konnte jedoch als nicht unterstützte Expertenfunktion verwendet werden.	Anstelle des auf dem mGuard-Gerät vorinstallierten selbstsignierten Webserver-Zertifikats kann ein eigenes Maschinenzertifikat auf das Gerät hochgeladen und verwendet werden. Mit diesem Zertifikat kann sich das Gerät gegenüber anfragenden Clients authentifizieren. Die Verwendung von CA-Zertifikaten in Verbindung mit einer Zertifikatskette des Vertrauens (*chain of trust*) ist möglich.	**10.5.0**

Neue Funktion / Variable /Werte	Neue Funktion / Auswirkung Migration	Firmware (Eingefügt mit Firmware-Version)
	Migration von älteren mGuard-Konfigurationen Wenn bereits ein HTTPS Server-Zertifikat verwendet wird, muss die Verwendung **vor einer Migration und vor einem Update** deaktiviert werden. Befehl auf der Kommandozeile: `gaiconfig --set HTTPS_SERVER_CERT_REF ""` Sie können nun die Migration/das Update erneut ausführen und das Zertifikat (wenn es gültig ist) erneut verwenden. Wenn kein HTTPS Server-Zertifikat verwendet wird, gilt: Keine Auswirkungen.	

2.1.3 Neu hinzugefügte Funktionen

Auf der neuen Geräteplattform wurden Variablen hinzugefügt, die auf der alten Geräteplattform nicht vorhanden sind.

Tabelle 2-3 Neu hinzugefügte Funktionen / Variablen / Variablenwerte

Neue Funktion / Variable /Werte	Neue Funktion / Auswirkung Migration	Firmware (Eingefügt mit Firmware-Version)
[TCP-Dump] **Menü:** Support >> Erweitert >> TCP-Dump **Sektion:** TCP-Dump **Variable (Aktion):** (1) tcpdump starten (2) tcpdump stoppen und herunterladen	Mithilfe einer Paketanalyse (*tcpdump*) kann der Inhalt von Netzwerkpaketen analysiert werden, die über ein ausgewähltes Netzwerk-Interface gesendet oder empfangen werden. **Migration von älteren mGuard-Konfigurationen** Keine Auswirkungen	**10.5.0**
[Logging] **Menü:** Logging >> Einstellungen **Sektion:** Datenschutz **Variable:** Maximale Aufbewahrungsfrist für Log-Einträge **GAI-Variable:** LOGGING_MAX_DAYS	Um grundsätzliche Anforderungen an den Datenschutz zu beachten, ist es möglich, Log-Einträge nur für einen begrenzten Zeitraum auf dem Gerät zu speichern. Nach Ablauf einer konfigurierbaren Speicherfrist, werden Log-Einträge auf dem Gerät automatisch gelöscht. **Migration von älteren mGuard-Konfigurationen** Keine Auswirkungen	**10.5.0**
[Konfigurationsprofile] **Menü:** Verwaltung >> Konfigurationsprofile **Sektion:** Signierte Konfigurationsprofile **Variablen:** Signierte Konfigurationsprofile aktivieren Export-Zertifikat (Maschinenzertifikat zum Signieren von Konfigurationsprofilen) Import-Zertifikat (Zertifikat zur Prüfung signierter Konfigurationsprofile) **GAI-Variablen:** PROFILE_SECURE_ONLY PROFILE_EXPORT_CERT PROFILE_IMPORT_CERT	Konfigurationsprofile können mithilfe von Zertifikaten signiert werden. Auf entsprechend konfigurierten Geräten ist es dann nur noch möglich, Konfigurationsprofile, die mit gültigen Zertifikaten signiert wurden, auf das Gerät hochzuladen. **Migration von älteren mGuard-Konfigurationen** Keine Auswirkungen	**10.5.0**

Neue Funktion / Variable /Werte	Neue Funktion / Auswirkung Migration	Firmware (Eingefügt mit Firmware-Version)
[OpenVPN-Client] **Menü:** OpenVPN-Client > Verbindungen > Tunneleinstellungen **Sektion:** Datenverschlüsselung **Variable:** Verschlüsselungsalgorithmus **GAI-Variable:** OPENVPN_CONNECTION.x.VPN_ENCRYPTION	**Der Verschlüsselungsalgorithmus "Blowfish" wird nicht mehr unterstützt.** Insgesamt können sechs statt wie bisher drei AES-Verschlüsselungsalgorithmen ausgewählt werden: AES-128-GCM / AES-192-GCM / AES-256-GCM / AES-128-CBC / AES-192-CBC / AES-256-CBC **Migration von älteren mGuard-Konfigurationen** Nach der Migration einer Konfiguration aus einer älteren Firmware-Version mit konfiguriertem Verschlüsselungsalgorithmus „Blowfish“, wird der Wert der Variablen auf "AES-256-GCM" gesetzt. Für alle anderen Algorithmen gilt: Der Wert aus der migrierten Konfiguration wird unverändert übernommen. Der konfigurierte Verschlüsselungsalgorithmus wird nicht geändert.	**10.5.0**
[HTTPS-Zugriff] **Menü:** Verwaltung >> Web-Einstellungen >> Zugriff **Sektion:** Web-Zugriff über HTTPS **Variable:** Niedrigste unterstützte TLS-Version **GAI-Variable:** TLS_MIN_VERSION	Einige Funktionen des mGuard-Gerätes verwenden TLS-Verschlüsselung, u. a.: – Web-Server (HTTPS-Zugriff) – OpenVPN-Client Die verwendete TLS-Version wird dabei zwischen den Gegenstellen ausgehandelt. Dabei ist es möglich, dass eine nicht mehr als sicher geltende TLS-Version ausgewählt wird. Um das zu verhindern, kann festgelegt werden, welche TLS-Version als niedrigste TLS-Version vom mGuard-Gerät akzeptiert wird. Verbindungen mit niedrigeren TLS-Versionen werden vom mGuard-Gerät abgelehnt. Standard: TLS 1.2 **Migration von älteren mGuard-Konfigurationen** Die Variable wird mit dem Wert TLS 1.0/1.1 konfiguriert. Alle TLS-Versionen ab TLS 1.0 werden vom mGuard-Gerät akzeptiert.	**10.5.0**

Neue Funktion / Variable /Werte	Neue Funktion / Auswirkung Migration	Firmware (Eingefügt mit Firmware-Version)
[Web-Zugriff über HTTPS / Server-Zertifikat] **Menü:** Verwaltung >> Web-Einstellungen >> Zugriff **Sektion:** Web-Zugriff über HTTPS **Variable:** HTTPS Server-Zertifikat **GAI-Variablen:** HTTPS_SERVER_CERT_REF In früheren Firmware-Versionen war die Funktion offiziell **nicht verfügbar**, konnte jedoch als nicht unterstützte Expertenfunktion verwendet werden.	Anstelle des auf dem mGuard-Gerät vorinstallierten selbstsignierten Webserver-Zertifikats kann ein eigenes Maschinenzertifikat auf das Gerät hochgeladen und verwendet werden. Mit diesem Zertifikat kann sich das Gerät gegenüber anfragenden Clients authentifizieren. Die Verwendung von CA-Zertifikaten in Verbindung mit einer Zertifikatskette des Vertrauens (*chain of trust*) ist möglich. **Migration von älteren mGuard-Konfigurationen** Wenn bereits ein HTTPS Server-Zertifikat verwendet wird, muss die Verwendung **vor einer Migration und vor einem Update** deaktiviert werden. Befehl auf der Kommandozeile: `gaiconfig --set HTTPS_SERVER_CERT_REF ""` Sie können nun die Migration/das Update erneut ausführen und das Zertifikat (wenn es gültig ist) erneut verwenden. Wenn kein HTTPS Server-Zertifikat verwendet wird, gilt: Keine Auswirkungen.	**10.5.0**
[LINK-Modus] **Menü:** Netzwerk >> Interfaces >> Allgemein **Sektion:** Netzwerk-Status / Netzwerk-Modus **Variable:** LINK-Modus **GAI-Variable:** ROUTER_MODE_LINK	Über das bei Phoenix Contact erhältliche Gerät "CELLULINK" kann das mGuard-Gerät eine mobile Datenverbindung zu anderen Netzwerken oder dem Internet herstellen (z. B. über das 4G-Netz). Wird der LINK-Modus aktiviert, wird ein Hyperlink zum Web-based Management des Gerätes "CELLULINK" im WBM des mGuard-Gerätes angezeigt. **Migration von älteren mGuard-Konfigurationen** Keine Auswirkungen	**10.5.0**

Neue Funktion / Variable /Werte	Neue Funktion / Auswirkung Migration	Firmware (Eingefügt mit Firmware-Version)
[OpenVPN-Client] **Menü:** OpenVPN-Client > Verbindungen > Tunneleinstellungen **Sektion:** Datenverschlüsselung **Variable:** Hash-Algorithmus (HMAC-Authentication) **GAI-Variable:** OPENVPN_CONNECTION.x.VPN_AUTH_HMAC	Die Hash-Funktion, die zur Berechnung der Prüfsumme verwendet wird, kann konfiguriert werden. **Migration von älteren mGuard-Konfigurationen** Nach der Migration einer Konfiguration aus einer älteren Firmware-Version wird der Wert der neu hinzugefügten Variable auf "SHA-1" gesetzt.	**10.4.0**
[Update-Server] **Menü:** Verwaltung >> Update >> Update **Sektion:** Update-Server **Variable:** Server-Zertifikat **GAI-Variable:** PSM_REPOSITORIES.x.REMOTE_CERT_REF	Um sicherzustellen, dass eine sichere HTTPS-Verbindung zum konfigurierten Update-Server aufgebaut wird, kann ein Server-Zertifikat des Update-Servers auf dem mGuard-Gerät installiert werden. Dieses kann vom mGuard-Gerät genutzt werden, um die Authentizität des Update-Servers zu überprüfen. **Migration von älteren mGuard-Konfigurationen** Nach der Migration einer Konfiguration aus einer älteren Firmware-Version wird der Wert der neu hinzugefügten Variable auf "Ignorieren" gesetzt.	**10.3.0**
[Alarmausgang] **Menü:** Verwaltung >> Service I/O >> Alarmausgang **Sektion:** Funktions-Überwachung **Variable:** Passwörter nicht konfiguriert **GAI-Variable:** PASSWORD_CHECK	Ein konfigurierbarer Alarm "Passwörter nicht konfiguriert" für nicht geänderte Standardpasswörter (*admin*/*root*) wurde zum Gerät hinzugefügt. Der Alarm löst den Alarmausgang über I/Os sowie die entsprechende FAIL-LED aus. **Migration von älteren mGuard-Konfigurationen** Nach der Migration einer Konfiguration aus einer älteren Firmware-Version wird der Wert der neu hinzugefügten Variable auf "Überwachen" gesetzt.	**10.3.0**

2.1.4 Geänderte Werkseinstellungen

In wenigen Fällten unterscheiden sich die Werkseinstellungen vorhandener Variablen auf der alten und der neuen Geräteplattform.

Tabelle 2-4 Geänderte Werkseinstellungen

Funktion	Geänderte Werkseinstellung / Auswirkung Migration	Firmware (Eingefügt mit Firmware-Version)
[OpenVPN-Client] **Menü:** OpenVPN-Client > Verbindungen > Tunneleinstellungen **Sektion:** Datenverschlüsselung **Variable:** Verschlüsselungsalgorithmus **GAI-Variable:** OPENVPN_CONNECTION.x.VPN_ENCRYPTION	In den Werkseinstellungen wird der Verschlüsselungsalgorithmus "AES-256-GCM" statt wie bisher "AES-256-CBC" verwendet. **Migration von älteren mGuard-Konfigurationen** Nach der Migration einer Konfiguration aus einer älteren Firmware-Version mit konfiguriertem Verschlüsselungsalgorithmus „Blowfish“, wird der Wert der Variablen auf "AES-256-GCM" gesetzt. Für alle anderen Algorithmen gilt: Der Wert aus der migrierten Konfiguration wird unverändert übernommen. Der konfigurierte Verschlüsselungsalgorithmus wird nicht geändert.	**10.5.0**
[OpenVPN-Client] **Menü:** OpenVPN-Client > Verbindungen > Tunneleinstellungen **Sektion:** Datenverschlüsselung **Variable:** Hash-Algorithmus (HMAC-Authentication) **GAI-Variable:** OPENVPN_CONNECTION.x.VPN_AUTH_HMAC	In den Werkseinstellungen wird der Hash-Algorithmus "SHA-256" statt wie bisher "SHA-1" verwendet. **Migration von älteren mGuard-Konfigurationen** Der Wert aus der migrierten Konfiguration wird unverändert übernommen. Der konfigurierte Hash-Algorithmus wird nicht geändert.	**10.5.0**
[E-Mail] **Menü:** Verwaltung >> Systemeinstellungen >> E-Mail **Sektion:** E-Mail **Variable:** Verschlüsselungsmodus für den E-Mail-Server **GAI-Variable:** EMAIL_RELAY_TLS	In den Werkseinstellungen wird der Verschlüsselungsalgorithmus „TLS-Verschlüsselung“ statt wie bisher „Keine Verschlüsselung“ verwendet. **Migration von älteren mGuard-Konfigurationen** Der Wert aus der migrierten Konfiguration wird unverändert übernommen. Der konfigurierte Verschlüsselungsmodus wird nicht geändert.	**10.5.0**

Funktion	Geänderte Werkseinstellung / Auswirkung Migration	Firmware (Eingefügt mit Firmware-Version)
[Network Address Translation] **Menü:** Netzwerk >> NAT >> Maskierung **Sektion:** Network Address Translation/IP-Masquerading **Variable:** Ausgehend über Interface / Von IP	In den Werkseinstellungen wird eine Tabellenzeile/Regel mit den folgenden Variablen-Werten hinzugefügt: – Ausgehend über Interface: *Extern* – Von IP: *0.0.0.0/0* IP-Masquerading ist damit für alle Pakete aktiviert, die aus dem internen Netzwerk (LAN) in das externe Netzwerk (WAN) geroutet werden (LAN --> WAN). **Migration von älteren mGuard-Konfigurationen** Die Werte aus der migrierten Konfiguration werden unverändert übernommen. Eine neueTabellenzeile/Regel wird nicht hinzugefügt.	10.3.0
[Netzwerkeinstellungen] **Menü:** Netzwerk >> Interfaces >> Allgemein **Sektion:** Netzwerk-Modus **Variable:** Netzwerk-Modus	Alle Geräte der neuen Gerätegeneration werden im Netzwerk-Modus „Router“ ausgeliefert. Das externe WAN-Interface erhält seine IP-Konfiguration über DHCP. In der Werkseinstellung verhindert jedoch die Firewall den Fernzugang zum Gerät über das WAN-Interface. Über das interne LAN-Interface ist das Gerät unter der Netzwerkadresse 192.168.1.1/24 aus dem LAN-Netzwerk erreichbar. Mit dem LAN-Interface verbundene Geräte können ihre IP-Konfiguration über den DHCP-Server des mGuard-Geräts erhalten. **Migration von älteren mGuard-Konfigurationen** Der Wert aus der migrierten Konfiguration wird unverändert übernommen. Der konfigurierte Netzwerkmodus wird nicht geändert.	10.3.0

2.1.5 Geänderte Variablenwerte

In wenigen Fällten sind Werte von Variablen auf der neuen Geräteplattform nicht mehr verfügbar und werden durch andere Werte ersetzt.

Tabelle 2-5 Geänderte Variablenwerte

Funktion	Geänderter Variablenwert / Auswirkung Migration	Firmware (Eingefügt mit Firmware-Version)
[OpenVPN-Client] **Menü:** OpenVPN-Client > Verbindungen > Tunneleinstellungen **Sektion:** Datenverschlüsselung **Variable:** Verschlüsselungsalgorithmus **GAI-Variable:** OPENVPN_CONNECTION.x.VPN_ENCRYPTION	**Der Verschlüsselungsalgorithmus „Blowfish“ wird nicht mehr unterstützt.** Insgesamt können sechs statt bisher drei AES-Verschlüsselungsalgorithmen ausgewählt werden: AES-128-GCM / AES-192-GCM / AES-256-GCM / AES-128-CBC / AES-192-CBC / AES-256-CBC **Migration von älteren mGuard-Konfigurationen** Nach der Migration einer Konfiguration aus einer älteren Firmware-Version mit konfiguriertem Verschlüsselungsalgorithmus „Blowfish“, wird der Wert der Variablen auf "AES-256-GCM" gesetzt. Für alle anderen Algorithmen gilt: Der Wert aus der migrierten Konfiguration wird unverändert übernommen. Der konfigurierte Verschlüsselungsalgorithmus wird nicht geändert.	**10.5.0**

[Shell-Zugang]
Menü: Verwaltung >> Systemeinstellungen >> Shell-Zugang
Sektion: Maximale Anzahl gleichzeitiger Sitzungen pro Rolle
Variable: Admin / Netadmin / Audit
GAI-Variablen:
SSH_ADMIN_LOGIN_ALLOWED_MAX
SSH_NETADMIN_LOGIN_ALLOWED_MAX
SSH_AUDIT_LOGIN_ALLOWED_MAX
	Die „Maximale Anzahl gleichzeitiger Sitzungen pro Rolle“ wird auf 10 begrenzt.
	Migration von älteren mGuard-Konfigurationen
	– Für alle konfigurierten Werte **<= 10** gilt:
	  – Der Wert aus der migrierten Konfiguration wird unverändert übernommen. Die konfigurierte maximale Anzahl gleichzeitiger Sitzungen pro Rolle wird nicht geändert.
	– Für alle konfigurierten Werte **> 10** gilt:
	  – Nach der Migration wird der Wert der Variable„Maximale Anzahl gleichzeitiger Sitzungen pro Rolle“ jeweils auf 10 gesetzt.
		10.5.0

Funktion	Geänderter Variablenwert / Auswirkung Migration	Firmware (Eingefügt mit Firmware-Version)
[Multicast] **Menü:** Netzwerk >> Ethernet >> Multicast **Sektion:** Allgemeine Multicast-Konfiguration **Variable:** IGMP-Snooping	**Damit Daten in „Statischen Multicast-Gruppen“ korrekt an die konfigurierten Ports weitergeleitet werden, muss „IGMP-Snooping“ aktiviert werden** **Migration von älteren mGuard-Konfigurationen** Der Wert der Variable wird nach einer Migration wie folgt geändert: – **Aktiviert**: Wenn „Statischen Multicast-Gruppen“ konfiguriert sind. – **Aktiviert**: Wenn „IGMP-Snooping“ in der alten Konfiguration aktiviert ist. – **Deaktiviert**: Wenn keine „Statischen Multicast-Gruppen“ konfiguriert sind und IGMP-Snooping“ in der alten Konfiguration deaktiviert ist.	10.3.0

2.1.6 Migration der Gerätekonfiguration

Die Migration der Konfiguration älterer mGuard-Geräte kann über das Web-based Management (WBM) oder via SD-Karte (ECS) vorgenommen werden.

Voraussetzungen

Sind Gerätefunktionen des Geräts, dessen Konfiguration migriert werden soll, auf dem neuen Gerät nicht verfügbar, müssen die Variablen vor dem Export der Konfiguration auf dem alten Gerät auf Werkseinstellungen zurückgesetzt werden (siehe Tabelle 2-1).

Das genaue Vorgehen bei der Gerätemigration wird im Dokument 111259_de_xx (AH DE MGUARD MIGRATE 10) beschrieben, erhältlich unter phoenixcontact.com/product/1357875.

2.2 Grundlegende Eigenschaften

Die genannten Eigenschaften sind keine garantierten Eigenschaften, da sie grundsätzlich gerätespezifisch sind.

Wenn nicht anders angegeben, sind in diesem Dokument bei der Nennung der Geräte FL MGUARD 4302 und FL MGUARD 4305 die Varianten 4302/KX und 4305/KX ebenfalls mitgemeint.

Netzwerk-Features

- Stealth (Auto, Static, Multi), Router (Static, DHCP-Client)
- DMZ
- VLAN
- DHCP-Server/Relay auf den internen und externen Netzwerkschnittstellen
- DNS-Cache auf der internen Netzwerkschnittstelle
- Dynamisches Routing (OSPF)
- Administration über HTTPS und SSH
- LLDP
- MAU-Management
- SNMP

Firewall-Features

- Stateful Packet Inspection
- Anti-Spoofing
- IP-Filter
- L2-Filter (nur im Stealth-Modus)
- NAT mit FTP-, IRC-Unterstützung (nur im Netzwerkmodus „Router“)
- 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)
- Deep Packet Inspection für Modbus-TCP
- Schutzgerät für PROFIsafe-Netzwerkzellen (nach IEC 61784-3-3)

VPN-Features (IPsec)

- Protokoll: IPsec (Tunnel- und Transport-Mode, XAuth/Mode Config)
- IPsec-Verschlüsselung mit DES (56 Bit), 3DES (168 Bit), AES (128, 192, 256 Bit)
- Paket-Authentifizierung: MD5, SHA-1, SHA-265, SHA-384, SHA-512
- 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 IPsec NAT

- Standard-Route über VPN-Tunnel
- Weiterleiten von Daten zwischen VPNs (Hub and Spoke)
- Gerätetypenabhängig bis zu 250 aktive VPN-Tunnel

VPN-Features (OpenVPN)

- OpenVPN-Client
- OpenVPN-Verschlüsselung mit AES (128, 192, 256 Bit) (Block cipher modes: GCM und CBC)
- HMAC-Authentifizierung: SHA-1, SHA-256 , SHA-512
- Dead-Peer-Detection (DPD)
- Authentisierung über Benutzerkennung, Passwort oder X.509v3-Zertifikat
- Erkennen wechselnder IP-Adressen von Gegenstellen über DynDNS
- OpenVPN-Firewall und 1:1-NAT
- Routen über VPN-Tunnel statisch konfigurierbar und dynamisch erlernbar
- Weiterleiten von Daten zwischen VPNs (Hub and Spoke)
- Bis zu 250 VPN-Tunnel

Weitere Features

- Remote Logging
- Administration unter Benutzung von SNMP v1-v3 und mGuard device manager (FL MGUARD DM UNLIMITED)
- PKI-Unterstützung für HTTPS/SSH Remote Access
- Kann über die LAN-Schnittstelle als NTP- und DNS-Server agieren
- Plug-n-Protect Technologie
- Kompatibel zur *mGuard Secure Cloud* (mSC)

Support

Bei Problemen mit Ihrem mGuard wenden Sie sich bitte an Ihre Bezugsquelle.

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

2.3 Typische Anwendungsszenarien

In diesem Kapitel werden verschiedene Anwendungsszenarien für den mGuard skizziert.

- „Stealth-Modus (Plug-n-Protect)“
- „Netzwerkrouter“
- „DMZ“ (Demilitarized Zone)
- „VPN-Gateway“
- „WLAN über VPN“-Tunnel
- „Auflösen von Netzwerkkonflikten“

2.3.1 Stealth-Modus (Plug-n-Protect)

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.

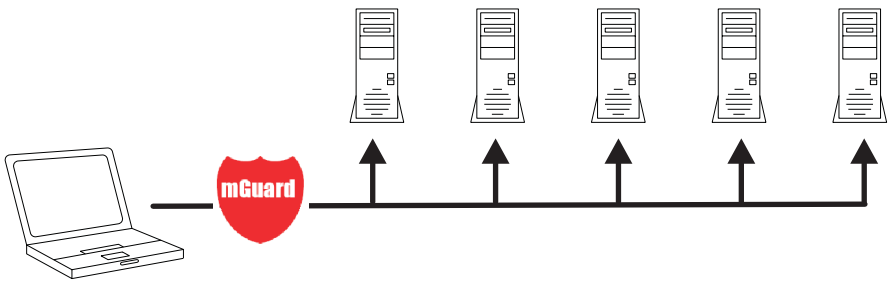


Bild 2-1 Stealth-Modus (Plug-n-Protect)

2.3.2 Netzwerkrouter

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

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

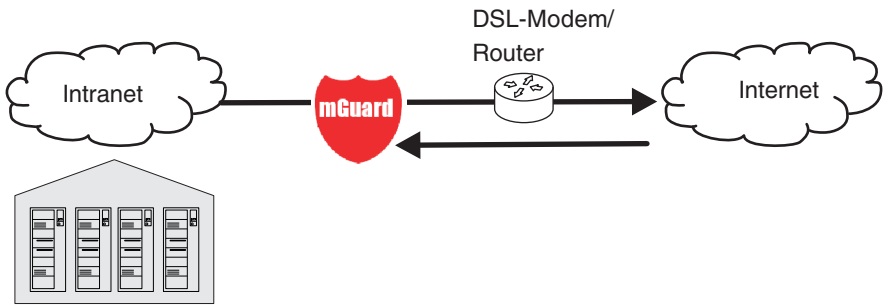


Bild 2-2 Netzwerk-Router

2.3.3 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.

Ein DMZ-Szenario lässt sich entweder durch zwei mGuards realisieren (siehe Bild 2-3), oder per dediziertem DMZ-Port einiger mGuard-Geräte, z. B. dem FL MGUARD 4305.

Der DMZ-Port wird nur im Router-Modus unterstützt und benötigt wenigstens eine IP-Adresse und eine entsprechende Netzmaske. Die DMZ unterstützt keine VLANs.

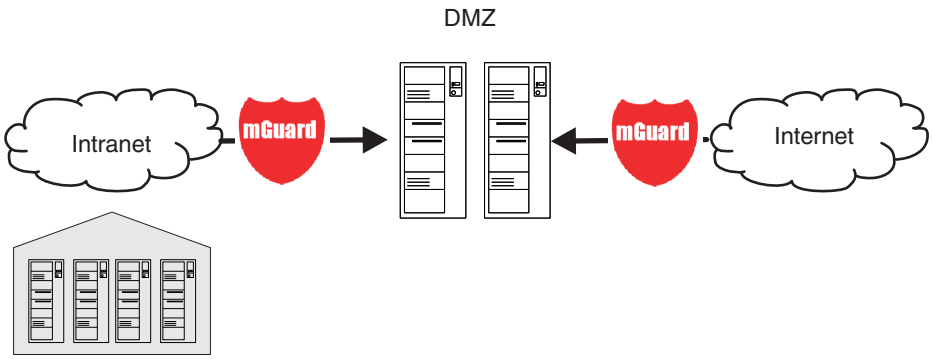


Bild 2-3 DMZ

2.3.4 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 oder der Rechner wird mit einem mGuard ausgerüstet.

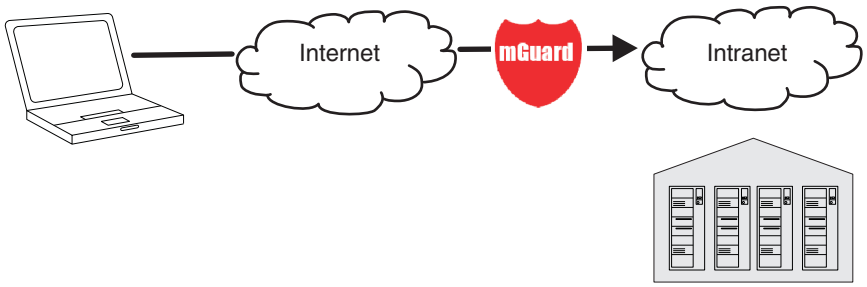


Bild 2-4 VPN-Gateway

2.3.5 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.

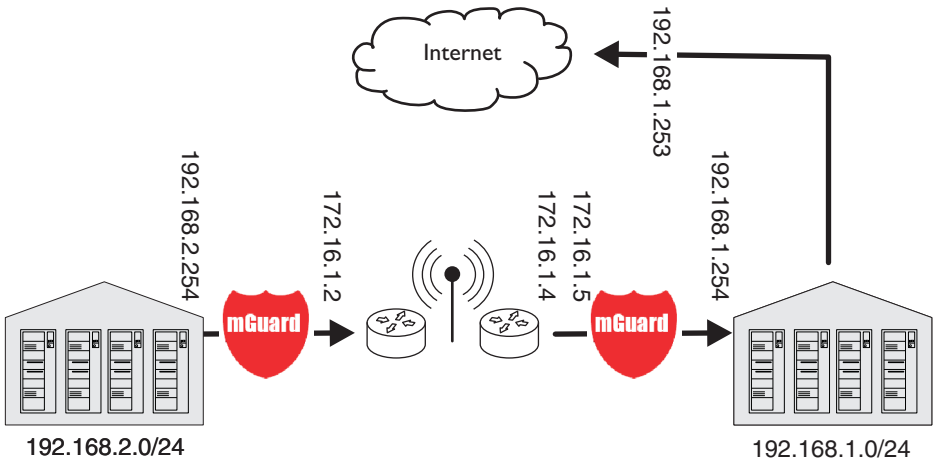


Bild 2-5 WLAN über VPN

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 Remote-Netzes	0.0.0.0/0

Im Hauptgebäude wird das entsprechende Gegenstück der Verbindung konfiguriert:

Tunnelkonfiguration im Hauptgebäude

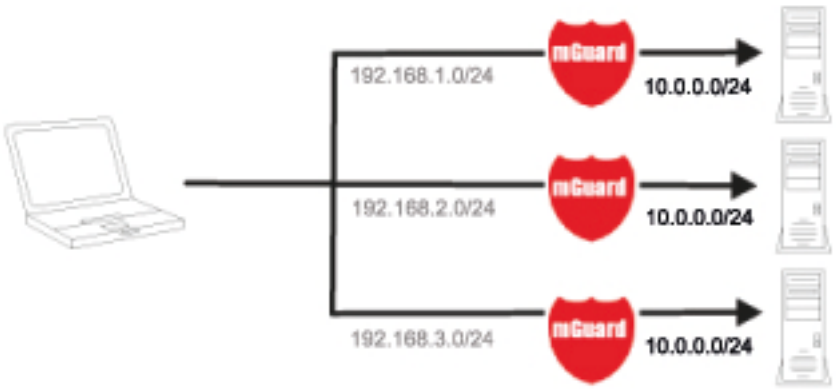
Verbindungstyp	Tunnel (Netz <-> Netz)
Lokales Netz	0.0.0.0
Adresse des Remote-Netzes	192.168.2.0/24

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

2.3.6 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 1:1-NAT-Feature können diese Netze nun auf andere Netze umgeschrieben werden, so dass der Konflikt aufgelöst wird.

(1:1-NAT kann im normalen Routing, in IPsec-Tunneln und in OpenVPN-Verbindungen genutzt werden.)

3 Hilfen zur Konfiguration

3.1 Sichere Verschlüsselung

Der mGuard bietet die Möglichkeit, unterschiedliche Verschlüsselungs- und Hash-Algorithmen zu verwenden.

Einige der zur Verfügung stehenden Algorithmen sind veraltet und werden nicht mehr als sicher angesehen. Sie sind deshalb nicht zu empfehlen. Aus Gründen der Abwärtskompatibilität können sie jedoch weiterhin ausgewählt und verwendet werden. Im WBM sind entsprechend veraltete Algorithmen oder unsichere Einstellungen mit einem Sternchen (*) markiert.

In den folgenden Bereichen des mGuards muss der Benutzer sicherstellen, dass sichere Verschlüsselungs- und Hash-Algorithmen zur Anwendung kommen:

– IPsec VPN-Verbindungen
– OpenVPN-Verbindungen
– Shell-Zugang (SSH)
– Web-Zugriff über HTTPS (TLS/SSL)
– Verbindung zu einem E-Mail-Server

Die sichere Verwendung von Verschlüsselung wird in den folgenden Kapiteln erläutert.

Weitergehende Informationen finden sich z. B. in der Technischen Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik: „BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen“.

Verwendung sicherer Verschlüsselungs- und Hash-Algorithmen

Phoenix Contact empfiehlt die Verwendung von Verschlüsselungs- und Hash-Algorithmen entsprechend der unten stehenden Tabelle.

Tabelle 3-1 Sichere Verschlüsselungs- und Hash-Algorithmen

Bereich / Protokoll	Verschlüsselung	Hash / Prüfsumme	Diffie-Hellman / PFS
VPN – IPsec VPN			
ISAKMP-SA (Schlüsselaustausch)	AES-256	SHA-256, -384, -512	2048 Bits oder höher
IPsec-SA (Datenaustausch)	AES-256	SHA-256, -384, -512	
Perfect Forward Secrecy (PFS)			2048 Bits oder höher
VPN – OpenVPN			
Datenverschlüsselung	AES-256-GCM	SHA-256, -512	
E-Mail – SMTP			
Verschlüsselungsmodus für den E-Mail-Server	TSL-Verschlüsselung, TLS-Verschlüsselung mit StartTLS		
TLS-basierte Verschlüsselung			
Niedrigste unterstützte TLS-Version	TLS 1.3, TLS 1.2		

Verwendung sicherer SSH-Clients

Der Aufbau verschlüsselter SSH-Verbindungen zum mGuard wird vom jeweils benutzten SSH-Client initiiert. Verwendet der SSH-Client veraltete und damit unsichere Verschlüsselungsalgorithmen, werden diese vom mGuard grundsätzlich akzeptiert.

Benutzen Sie immer **aktuelle SSH-Clients** (z. B. *PuTTY*), um die Verwendung schwacher Verschlüsselungsalgorithmen zu vermeiden.

Verwendung sicherer Web-Browser

Der Aufbau verschlüsselter HTTPS-Verbindungen (TLS/SSL) zum mGuard wird vom jeweils benutzten Web-Browser initiiert. Verwendet der Web-Browser veraltete und damit unsichere Verschlüsselungsalgorithmen, werden diese vom mGuard nur dann akzeptiert, wenn diese als „Niedrigste unterstützte TLS-Version“ konfiguriert wurden.

Benutzen Sie immer **aktuelle Web-Browser** bzw. **HTTPS-Clients**, um die Verwendung schwacher Verschlüsselungsalgorithmen zu vermeiden.

Wählen Sie die Version TLS 1.2 oder TLS 1.3 als „Niedrigste unterstützte TLS-Version“ auf dem mGuard-Gerät.

Erstellung sicherer X.509-Zertifikate

X.509-Zertifikate werden mithilfe unterschiedlicher Software-Tools erstellt.

Benutzen Sie immer **aktuelle Programm-Versionen** der Software-Tools (z. B. *XCA*), um die Verwendung schwacher Verschlüsselungsalgorithmen bei der Erstellung von X.509-Zertifikaten zu vermeiden.

Verwenden Sie bei der Erstellung von X.509-Zertifikaten **Schlüssellängen von mindestens 2048 Bit** sowie sichere **Hash-Algorithmen** (siehe auch Tabelle 3-1).

Verwendung von X.509-Zertifikaten statt Pre-Shared Keys (PSK)

Die Authentisierung mittels Pre-Shared-Keys (PSK) in VPN-Verbindungen gilt als unsicher und sollte nicht mehr verwendet werden. Verwenden Sie aus Sicherheitsgründen zur Authentisierung X.509-Zertifikate.

Verwendung von Configuration Pull (pullconfig)

Wählen Sie die Version TLS 1.2 oder TLS 1.3 als „Niedrigste unterstützte TLS-Version“ auf dem mGuard-Gerät.

Verwendung von Automatischen Updates

Wählen Sie die Version TLS 1.2 oder TLS 1.3 als „Niedrigste unterstützte TLS-Version“ auf dem mGuard-Gerät.

Verwendung der CRL-Prüfung

Wählen Sie die Version TLS 1.2 oder TLS 1.3 als „Niedrigste unterstützte TLS-Version“ auf dem mGuard-Gerät.

3.2 Geeignete Web-Browser

Die Konfiguration des Geräts erfolgt über eine grafische Benutzeroberfläche im Web-Browser.

Benutzen Sie immer **aktuelle Web-Browser**, um die Verwendung schwacher Verschlüsselungsalgorithmen zu vermeiden.

Unterstützt werden aktuelle Versionen folgender Web-Browser:

- Mozilla Firefox
- Google Chrome
- Microsoft Edge

3.3 Anzahl gleichzeitiger Sitzungen

Die gleichzeitige Anmeldung beim Web-based Management (WBM) des Gerätes ist auf 10 Web-Sitzungen (HTTPS) begrenzt. Das Limit gilt für die Benutzer *root*, *admin*, *audit* und *netadmin.* Die Anzahl gleichzeitiger Anmeldungen von Firewall-Benutzern wird nicht limitiert.

Sind bereits 10 Benutzer über das HTTPS-Protokoll angemeldet, d. h. wurden 10 parallele Web-Sitzungen gestartet, wird die Anmeldung weiterer Benutzer vom Gerät abgelehnt.

Die Limitierung greift für die Anmeldung über das HTTPS-Protokoll, unabhängig vom verwendeten Web-Client. Das schließt sowohl Web-Browser als auch Kommandozeilen-Tools wie *cURL* ein.

Aus Sicherheitsgründen und um die Anmeldung weiterer Benutzern nicht zu blockieren, sollten über das HTTPS-Protokoll angemeldete Benutzer (Web-Browser, *cURL*, etc.) ihre Sitzung nach Abschluss ihrer Tätigkeit immer aktiv beenden und sich vom Gerät abmelden.

Die Anzahl gleichzeitiger SSH-Anmeldungen (SSH-Sitzungen) kann konfiguriert werden (siehe „Maximale Anzahl gleichzeitiger Sitzungen pro Rolle“ auf Seite 60).

Begrenzung von Login-Versuchen

Bei einem Denial of Service-Angriff werden Dienste mutwillig arbeitsunfähig gemacht. Um einen solchen Angriff zu verhindern, ist der mGuard mit einer Drossel für verschiedene Netzwerkanfragen ausgerüstet.

Dabei werden alle Verbindungen gezählt, die von einer IP-Adresse mit einem bestimmten Protokoll ausgehen. Wenn eine bestimmte Anzahl an Verbindungsversuchen gezählt wird, wird die Drossel wirksam. Die Drossel wird zurückgesetzt, wenn 30 Sekunden lang keine weiteren Verbindungsversuche stattfinden.

Die Anzahl der Verbindungsversuche, die zu einer Aktivierung der Drossel führen, ist vom verwendeten Protokoll abhängig:

- 32 bei HTTPS
- 6 bei SSH, SNMP

3.4 Benutzerrollen

root	Benutzerrolle ohne Einschränkungen
admin	Administrator
netadmin	Administrator nur für das Netzwerk
audit	Auditor/Prüfer

Die vordefinierten Benutzer (*root*, *admin*, *netadmin*, *audit*) besitzen unterschiedliche Berechtigungen.

– Der Benutzer *root* hat einen uneingeschränkten Zugriff auf den mGuard. Die Anzahl gleichzeitiger HTTPS-Sitzungen ist begrenzt.
– Der Benutzer *admin* hat einen funktional uneingeschränkten Zugriff auf den mGuard. Die Anzahl gleichzeitiger HTTPS-Sitzungen ist begrenzt. Die Anzahl der gleichzeitigen SSH-Sitzungen kann eingeschränkt werden.
– Dem Benutzer *netadmin* werden über den mGuard device manager (FL MGUARD DM UNLIMITED) die Berechtigungen explizit zugewiesen. Er kann auf die anderen Funktionen nur lesend zugreifen. Passwörter und Private Keys können von ihm nicht gelesen werden.
– Der Benutzer *audit* kann auf alle Funktionen ausschließlich lesend zugreifen. Die Benutzerrolle *audit* kann wie *netadmin* standardmäßig nur über den mGuard device manager (FL MGUARD DM UNLIMITED) eingeschaltet werden.

3.5 Eingabehilfe bei der Konfiguration (Systemnachrichten)

Geänderte oder ungültige Einträge werden in der Web-Oberfläche farblich markiert.

Zusätzlich stehen Systemnachrichten zur Verfügung, die z. B. erläutern, warum ein Eintrag ungültig ist.

Für diese Unterstützung muss die Verwendung von JavaScript im verwendeten Web-Browser erlaubt sein.

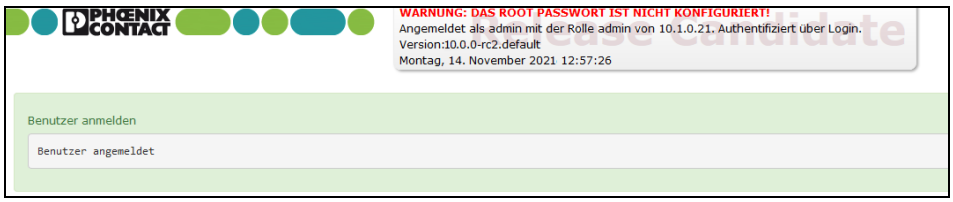


Bild 3-1 Beispiel für Systemnachricht

- **Geänderte Einträge** werden innerhalb der relevanten Seite und im zugehörigen Menüpunkt **grün** markiert, bis die Änderungen übernommen oder rückgängig gemacht werden. Bei Tabellen wird nur die Änderung bzw. Entfernung einer Tabellenzeile angezeigt, nicht aber der geänderte Wert.
- **Ungültige Einträge** werden innerhalb der relevanten Seite, des relevantenTabs und im zugehörigen Menüpunkt **rot** markiert.

Auch wenn Sie ein Menü schließen, bleiben die geänderten oder ungültigen Einträge gekennzeichnet.

Bei Bedarf werden systemrelevante Informationen und Alarmmeldungen (siehe Kapitel 4.8.2, „Alarmausgang“) im oberen Bereich des Bildschirms angezeigt.

3.6 Bedienung der Web-Oberfläche

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

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 42).
– Wenn sich unten rechts die Schaltfläche **„Zurück“** befindet, kehren Sie durch Klicken auf diese Schaltfläche auf die Seite zurück, von der Sie gekommen sind.

Änderung von Werten

Wenn Sie den Wert einer Variablen in der Web-Oberfläche ändern, die Änderung jedoch noch nicht durch einen Klick auf das Icon **Übernehmen** übernehmen, dann erscheint der Variablen-Name der geänderten Variable in Grün.

Um das Auffinden der Änderungen zu erleichtern, wird zusätzlich der komplette Menüpfad zur geänderten Variable ebenfalls in Grün dargestellt: Menü >> Untermenü >> Registerkarte >> Sektion >> Variable.

Bei Eingabe unzulässiger Werte

Wenn Sie einen unzulässigen Wert (z. B. eine unzulässige Zahl in einer IP-Adresse) angegeben haben und auf das Icon **Übernehmen** klicken, wird die Schrift des betreffenden Variablen-Namens in Rot dargestellt und in der Regel eine Fehlermeldung angezeigt.

Um das Auffinden des Fehlers zu erleichtern, wird zusätzlich der komplette Menüpfad zur geänderten Variable ebenfalls in Rot dargestellt: Menü >> Untermenü >> Registerkarte >> Sektion >> Variable.

Eingabe eines Timeouts

Die Eingabe eines Timeouts kann auf drei Arten erfolgen:

– in Sekunden [ss]
– in Minuten und Sekunden [mm:ss]
– in Stunden, Minuten und Sekunden [hh:mm:ss]

Zur Abtrennung der drei möglichen Werte wird jeweils ein Doppelpunkt verwendet. Wird nur ein Wert eingegeben, wird dieser als Sekunden interpretiert, zwei Werte als Minuten und Sekunden, drei Werte als Stunden, Minuten und Sekunden. Die Werte für Minuten und Sekunden dürfen größer als 59 sein. Nach Übernahme der Werte werden diese unabhängig vom Eingabeformat immer als [hh:mm:ss] angezeigt (aus 90:120 wird z. B. 1:32:00).

Globale Icons

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

Abmelden

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.

Zurücksetzen

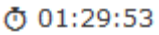
Zurücksetzen auf die alten Werte. Wenn Sie auf einer oder mehreren Konfigurationsseiten Werte eingetragen haben und diese noch nicht mit **Übernehmen** in Kraft gesetzt haben, können Sie mit **Zurücksetzen** die geänderten Werte auf die alten Werte zurücksetzen.

Übernehmen

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

Beachten Sie, dass bereits an anderer Stelle vorgenommene Änderungen (grün markiert) ebenfalls übernommen werden.

Ablauf der Sitzung



Zeigt die Zeit an, nach der der angemeldete Benutzer von der Web-Oberfläche abgemeldet wird. Durch einen Klick auf die Zeitanzeige, wird die Ablaufzeit auf den konfigurierten Ausgangswert zurückgesetzt (siehe „Verwaltung >> Web-Einstellungen >> Allgemein“ auf Seite 75).

Online-Hilfe

Verweis auf die **Online-Hilfe** zur installierten Firmware-Version.

Die Online-Hilfe ist nur bei bestehender Internetverbindung und entsprechender Firewall-Einstellung erreichbar.

Nach einem Klick auf das Icon öffnet sich das dem Inhalt der Seite entsprechende Kapitel des mGuard-Firmwarehandbuchs in einem neuen Tab/Fenster des Web-Browsers.

Das mGuard-Firmwarehandbuch als **PDF-Version** können Sie auf den entsprechenden Produktseiten unter phoenixcontact.com/products herunterladen.

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 in der Zeile, unter der eine neue Zeile eingefügt werden soll, auf das Icon ⊕ **Neue Zeile einfügen**.
2. Eine neue Zeile wird unter der ausgewählten Zeile eingefügt.
   Die eingefügte Zeile erscheint in der Farbe grün, bis die Änderung übernommen wurde.

Verschieben von Zeilen

1. Bewegen Sie den Mauszeiger über die Zeilennummer (Seq.) der Zeile, die Sie verschieben möchten.
   Der Mauszeiger verändert sich zu einem Kreuz  .
2. Klicken Sie mit der linken Maustaste in die gewünschte Zeile und halten Sie die Maustaste gedrückt.
   Die Zeile wird aus der bestehenden Reihenfolge gelöst.
3. Verschieben Sie die ausgewählte Zeile mit der Maus an die gewünschte Position.
   Ein Rahmen um die Ziel-Zeile zeigt an, an welcher Stelle die Zeile eingefügt wird.
4. Lassen Sie die Maustaste los.
5. Die Zeilen wird an die mit einen Kasten markierten Stelle verschoben.

Löschen von Zeilen

1. Klicken Sie in der Zeile, die Sie löschen möchten, auf das Icon **Zeile löschen**.
2. Klicken Sie anschließend auf das Icon **Übernehmen**, um die Änderung wirksam werden zu lassen.

3.7 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

3.8 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.

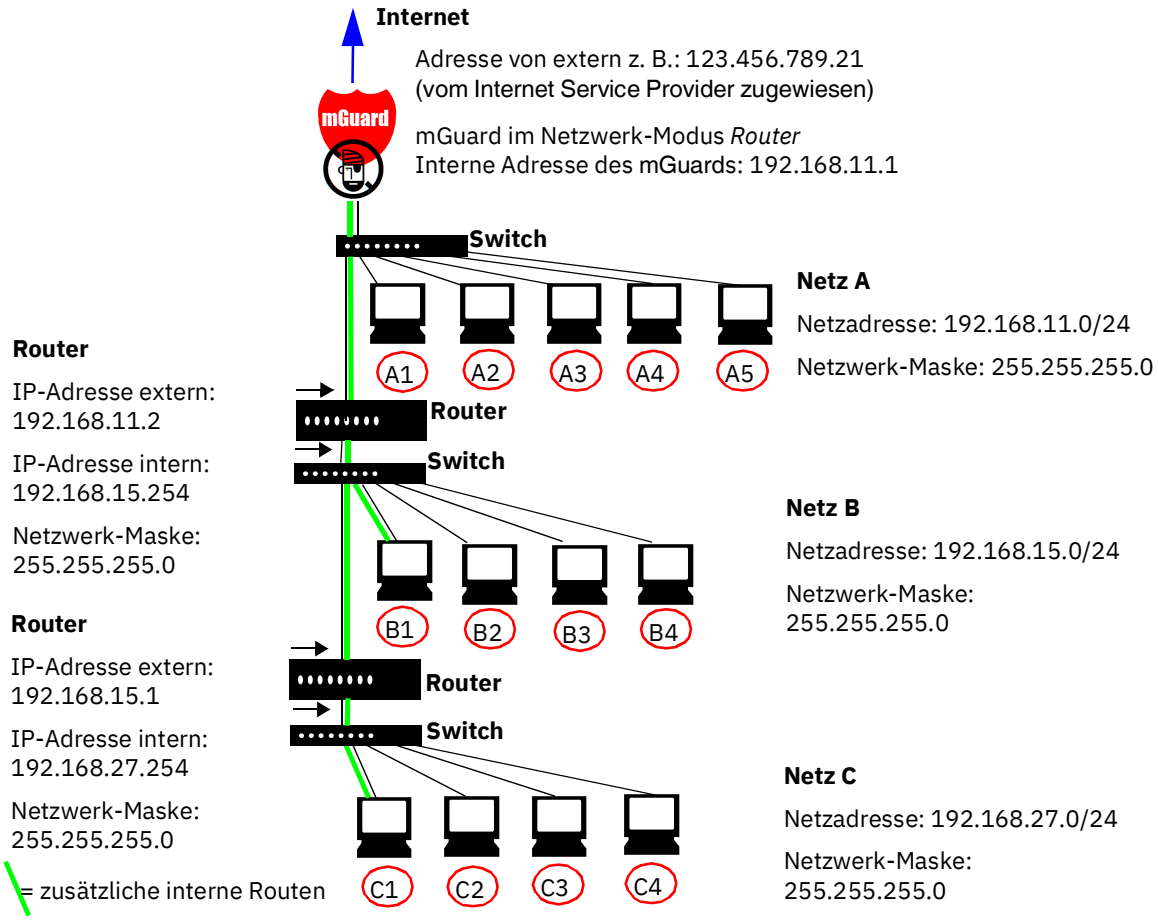


Tabelle 3-2 Netzwerk-Beispielskizze

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**

Tabelle 3-2 Netzwerk-Beispielskizze[...]

Netz B	**Rechner**	**B1**	**B2**	**B3**	**B4**	**Zusätzliche interne Routen** Netzwerk: 192.168.15.0/24 Gateway: 192.168.11.2 Netzwerk: 192.168.27.0/24 Gateway: 192.168.11.2
	IP-Adresse	192.168.15.2	192.168.15.3	192.168.15.4	192.168.15.5	
	Netzwerk-Maske	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	
Netz C	**Rechner**	**C**	**C2**	**C3**	**C4**	
	IP-Adresse	192.168.27.1	192.168.27.2	192.168.27.3	192.168.27.4	
	Netzwerk-Maske	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	

3.9 LED-Statusanzeige und Blinkverhalten

Mithilfe von eingebauten LED-Dioden zeigen mGuard-Geräte verschiedene Systemzustände an. Dabei kann es sich um Status-, Alarm- oder Fehlermeldungen handeln.

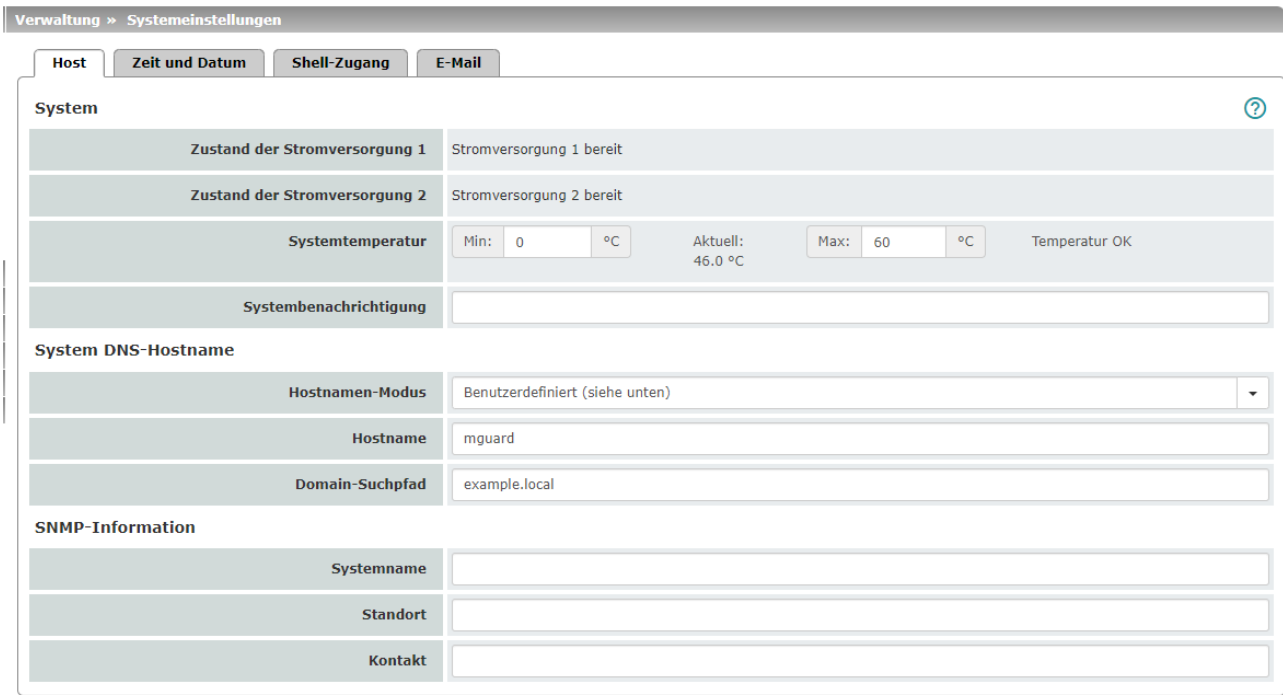
Detaillierte Informationen zu den LEDs finden Sie im Anhang (siehe „LED-Statusanzeige und Blinkverhalten“ auf Seite 375)

4 Menü Verwaltung

Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administrator-Passwort zu ändern (siehe „Authentifizierung >> Administrative Benutzer“ auf Seite 181). Solange dies noch nicht geschehen ist, erhalten Sie oben auf der Seite einen Hinweis darauf.

4.1 Verwaltung >> Systemeinstellungen

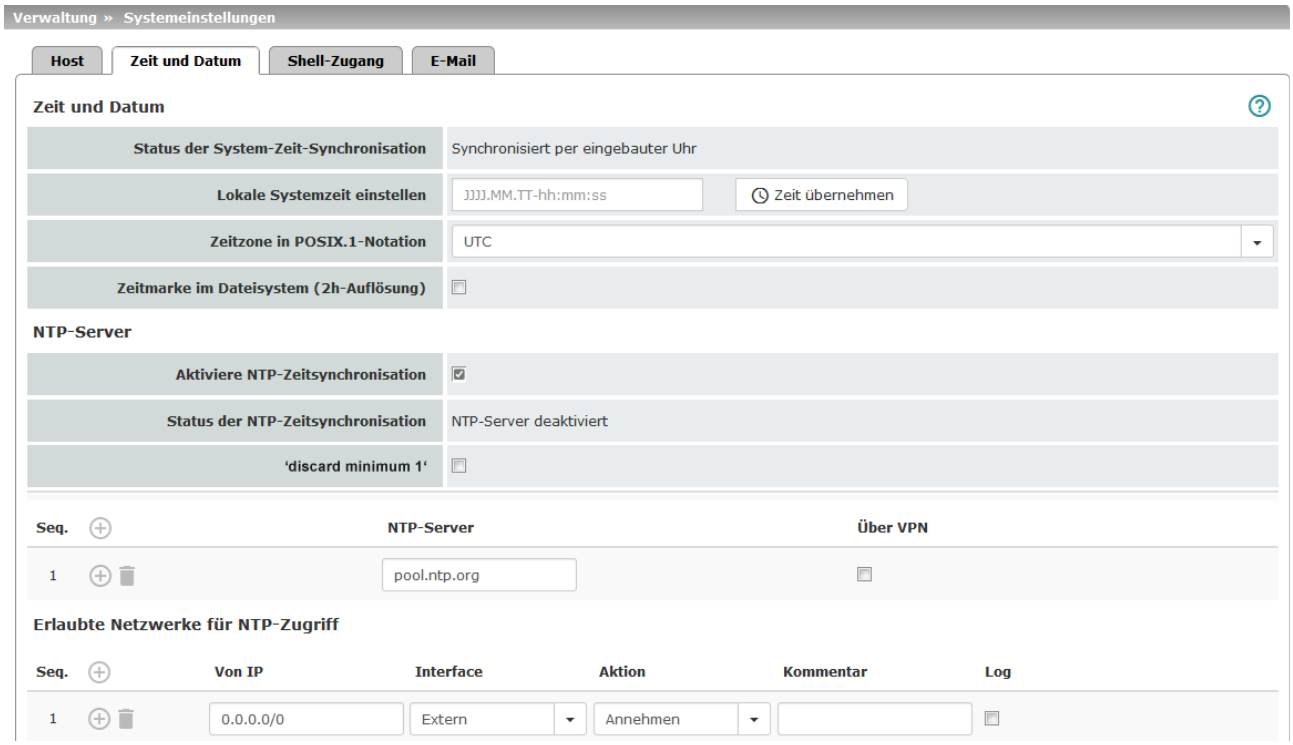
4.1.1 Host



Verwaltung >> Systemeinstellung >> Host		
System	**Zustand der Stromversorgung 1/2**	Zustand der beiden Netzteile (modellabhängig mit redundanter Stromversorgung)
	Systemtemperatur (°C)	Wenn der angegebene Temperaturbereich unter- bzw. überschritten wird, wird ein SNMP-Trap ausgelöst.

Verwaltung >> Systemeinstellung >> Host [...]		
	Systembenachrichtigung	Frei wählbarer Text für eine Systembenachrichtigung, die vor einer Anmeldung am mGuard-Gerät angezeigt wird (maximal 1024 Zeichen). Wird angezeigt bei: – Anmeldung per SSH-Login – Anmeldung über die Web-Oberfläche (Web-UI). Mithilfe eines geeigneten SSH-Clients kann das (wiederholte) Anzeigen der Benachrichtigung durch den Benutzer unterbunden werden. **Werkseitige Voreinstellung (Standard):** *The usage of this mGuard security appliance is reserved to authorized staff only. Any intrusion and its attempt without permission is illegal and strictly prohibited.*
System DNS-Hostname	**Hostnamen-Modus**	Mit *Hostnamen 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 47, „Shell-Zugang“ auf Seite 56). 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 *Hostnamen-Modus* die Option „Benutzer definiert“ ausgewählt, dann tragen Sie hier den Namen ein, den der mGuard erhalten soll.
	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)

4.1.2 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 50).

Verwaltung >> Systemeinstellung >> Zeit und Datum

Zeit und Datum

Sie können die Systemzeit des mGuards manuell einstellen und einer beliebigen Zeitzone zuordnen oder die Synchronisation der Systemzeit mittels frei wählbarer NTP-Server vornehmen.

Stellen Sie Zeit und Datum korrekt ein, da sonst der mGuard bestimmte zeitabhängige Aktivitäten nicht starten kann (siehe „Zeitabhängige Aktivitäten“ auf Seite 50).

Verbundene Geräte können den mGuard ihrerseits als NTP-Server verwenden.

Bitte beachten Sie, dass aus Sicherheitsgründen die NTP-Version *NTP v1* vom mGuard nicht unterstützt wird.

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

Zustand der Systemzeit

Zeigt an, ob die Systemzeit des mGuards zur Laufzeit des mGuards einmal mit einer gültigen Zeit synchronisiert wurde.

Solange hier angezeigt wird, dass die Systemzeit des mGuards nicht synchronisiert ist, führt der mGuard keine zeitgesteuerten Aktivitäten aus.

Geräte ohne eingebaute Uhr starten immer „Nicht synchronisiert“. Geräte, die eine eingebaute Uhr haben, starten in der Regel mit „Synchronisiert per eingebauter Uhr“.

Der Zustand der Uhr wechselt nur wieder auf „nicht synchronisiert“, wenn die Firmware neu auf das Gerät aufgebracht wird oder die eingebaute Uhr zu lange vom Strom getrennt war.

Die Stromversorgung der eingebauten Uhr wird durch einen Akku sichergestellt. Der Akku hält mindestens fünf Tage.

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 **Zeitplan** die Einstellung *Zeitgesteuert* ausgewählt ist (siehe „Verwaltung >> Konfigurationsprofile“ auf Seite 98, „Konfiguration holen“ auf Seite 118).
- **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 „Authentifizierung >> Zertifikate“ und „Zertifikatseinstellungen“ auf Seite 197).

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

Die Systemzeit kann durch verschiedene Ereignisse gestellt oder synchronisiert werden:

- **Synchronisiert per eingebauter Uhr:** Der mGuard besitzt eine eingebaute Uhr, die mindestens einmal mit der aktuellen Zeit synchronisiert wurde. 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.
- **Manuell synchronisiert:** Der Administrator hat zur Laufzeit dem mGuard die aktuelle Zeit mitgeteilt, indem er im Feld **„Lokale Systemzeit einstellen“** eine entsprechende Eingabe gemacht hat.
- **Synchronisiert per Zeitmarke im Dateisystem:** 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 einstellen“** selbst eingestellt. Dann wird der mGuard auch ohne eingebaute Uhr nach einem Neustart sofort seine Systemzeit mit Hilfe des Zeitstempels synchronisieren. Eventuell wird die Zeit später per NTP genauer eingestellt.
- **Synchronisiert durch das Network Time Protocol NTP:** 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 **„Status der NTP-Zeitsynchronisation“** wechselt eventuell erheblich später erst auf „synchronisiert“ (siehe dazu die Erklärung weiter unten zu **„Status der NTP-Zeitsynchronisation“**).

Lokale Systemzeit einstellen

Hier können Sie die Zeit des mGuards setzen, falls kein NTP-Server eingestellt wurde 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
MM	Minute
SS	Sekunde

Verwaltung >> Systemeinstellung >> Zeit und Datum [...]		
	Zeitzone in POSIX.1-Notation	Soll die *aktuelle Systemzeit* nicht die mittlere Greenwich-Zeit anzeigen, sondern Ihre aktuelle Ortszeit (abweichend von der mittleren Greenwich-Zeit), dann tragen Sie hier ein, um wie viel Stunden bei Ihnen die Zeit voraus bzw. zurück ist. Sie können Ihren Standort aus der Drop-Down-Liste auswählen (Sommer- und Winterzeit werden in der Regel automatisch berücksichtigt). Alternativ können Sie die Einstellung manuell wie folgt vornehmen: **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
	Zeitmarke im Dateisystem	Ist diese Funktion aktiviert, 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	Der mGuard kann für externe Rechner als NTP-Server fungieren (NTP = Network Time Protocol). In diesem Fall sind die Rechner so zu konfigurieren, dass als Adresse des NTP-Servers die Adresse des mGuards angegeben ist. In den Werkseinstellungen ist der NTP-Server des mGuard-Geräts deaktiviert. Nach dem Starten des NTP-Servers ist der Zugriff über das interne Interface (LAN-Interface) möglich. Über Firewall-Regeln kann der Zugriff über alle verfügbaren Interfaces freigegeben oder beschränkt werden. 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.	

Verwaltung >> Systemeinstellung >> Zeit und Datum [...]		
	Aktiviere NTP-Zeit-synchronisation	Ist diese Funktion aktiviert, 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. Nach der initialen Zeitsynchronisation vergleicht der mGuard regelmäßig die batteriegepufferte Systemzeit mit den Zeit-Servern. In der Regel erfolgen Nachjustierungen nur noch im Sekundenbereich.
	Status der NTP-Zeit-synchronisation	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.
	‘discard minimum 1‘	Die Aktivierung dieser Option kann die Zeitsynchronisation mit einigen NTP-Clients, insbesondere von SPS-Systemen, verbessern. Zusätzlich sollte das Aktualisierungsintervall auf dem SPS-System auf den maximal möglichen Wert erhöht werden (z. B. 86400 Sekunden).
	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.

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

Über VPN

Die Anfrage des NTP-Servers wird, wenn möglich, über einen VPN-Tunnel durchgeführt.

Bei aktivierter Funktion wird die Kommunikation mit dem Server immer dann über einen verschlüsselten VPN-Tunnel geführt, wenn ein passender VPN-Tunnel verfügbar ist.

Bei deaktivierter Funktion oder wenn kein passender VPN-Tunnel verfügbar ist, wird der Verkehr **unverschlüsselt über das Standard-Gateway** gesendet.

Voraussetzung für die Verwendung der Funktion ist die Verfügbarkeit eines passenden VPN-Tunnels. Das ist der Fall, wenn der angefragte 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.

Erlaubte Netzwerke für NTP-Zugriff

(Bei aktivierter Funktion „Aktiviere NTP-Zeitsynchronisation“)

Wenn die Funktion **Aktiviere NTP-Zeitsynchronisation** aktiviert ist, können externe Geräte auf den NTP-Server des mGuards zugreifen. Der Zugriff ist standardmäßig nur über das interne LAN-Interface (*Intern*) möglich.

ACHTUNG: Zugriff auf das Gerät über externe Netze möglich.
Die Server-Dienste des Geräts sind je nach Einstellung über externe Netze und möglicherweise aus dem Internet erreichbar. Stellen Sie sicher, dass der Zugriff nur erfolgen kann, wenn er erwünscht ist. Konfigurieren Sie andernfalls Ihr Netzwerk entsprechend, um einen Zugriff zu verhindern.

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

– NTP-Zugriffe über *Intern* sind erlaubt.
– NTP-Zugriffe über *Extern*, *DMZ* und *VPN* werden verwehrt.

Legen Sie die Überwachungsmöglichkeiten nach Bedarf fest.

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

Die Tabelle listet eingerichtete Firewall-Regeln auf. Sie gelten für eingehende Datenpakete eines NTP-Zugriffs. 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 >> Systemeinstellung >> Zeit und Datum [...]

Von IP

Geben Sie hier die Adresse des Rechners oder Netzes an, von dem der Zugriff 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 43).
– **0.0.0.0/0** bedeutet alle Adressen.

Interface

Intern / Extern / DMZ / VPN

Gibt an, für welches Interface die Regel gelten soll.

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

– NTP-Zugriffe über *Intern* sind erlaubt.
– NTP-Zugriffe über *Extern*, *DMZ* und *VPN* werden verwehrt.

Legen Sie die Überwachungsmöglichkeiten nach Bedarf fest.

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

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

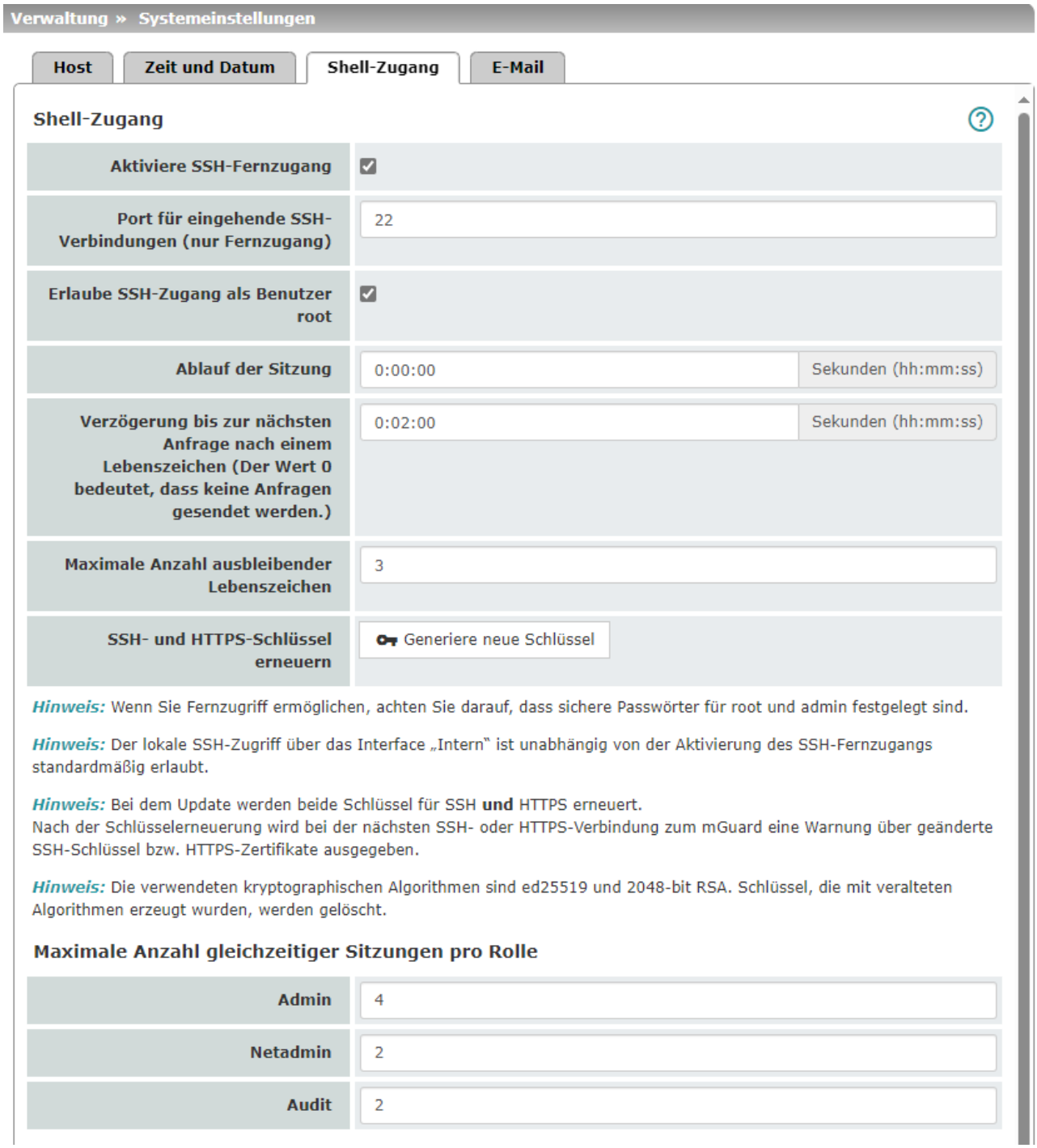
Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

– das Ereignis protokolliert werden soll – Funktion *Log* aktivieren oder
– das Ereignis nicht protokolliert werden soll – Funktion *Log* deaktivieren (Standard).

Log-Meldung (Beispiel):

2024-11-25_10:09:51.83909 firewall: fw-ntp-access-1-12e7d62f-6be7-1c6e-b8a6-000cbe00105c act=REJECT IN=eth0 MAC=d4:aa:62:b2:6d:62 SRC=192.168.1.55 DST=192.168.1.55 LEN=52 TOS=0x00 PREC=0x00 TTL=128 ID=47714 DF PROTO=TCP SPT=53379 DPT=22 SEQ=506303301 ACK=0 WINDOW=64240 SYN URGP=0 CTMARK=100030

4.1.3 Shell-Zugang



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

Sie können den mGuard über die Web-Oberfläche oder über die Kommandozeile (Shell) konfigurieren. Der Zugriff auf die Kommandozeile erfolgt über SSH.

Benutzen Sie immer **aktuelle SSH-Clients** (z. B. *PuTTY*), um die Verwendung schwacher Verschlüsselungsalgorithmen zu vermeiden.

Wenn Sie Änderungen am Authentifizierungsverfahren vornehmen, sollten Sie den mGuard anschließend neu starten, um bestehende Sitzungen mit nicht mehr gültigen Zertifikaten oder Passwörtern sicher zu beenden.

Bei aktiviertem **SSH-Fernzugang** kann der mGuard **von entfernten Rechnern aus** über die Kommandozeile konfiguriert werden. Der **SSH-Fernzugang** ist standardmäßig deaktiviert. Er kann aktiviert und auf ausgewählte Netzwerke beschränkt werden.

ACHTUNG: Zugriff auf das Gerät über externe Netze möglich.
Die Server-Dienste des Geräts sind je nach Einstellung über externe Netze und möglicherweise aus dem Internet erreichbar. Stellen Sie sicher, dass der Zugriff nur erfolgen kann, wenn er erwünscht ist. Konfigurieren Sie andernfalls Ihr Netzwerk entsprechend, um einen Zugriff zu verhindern.

ACHTUNG: Der lokale SSH-Zugriff über das Interface „Intern“ ist unabhängig von der Aktivierung des SSH-Fernzugangs standardmäßig erlaubt.
Um Zugriffsmöglichkeiten auf den mGuard differenziert festzulegen, müssen Sie Firewall-Regeln für das interne Interface entsprechend definieren (siehe „Erlaubte Netzwerke“ auf Seite 61)

ACHTUNG: Wenn Sie den Fernzugang ermöglichen, achten Sie darauf, dass sichere Passwörter für die Benutzer *root* und *admin* festgelegt sind.
Wenn Sie das Passwort für *root* oder *admin* ändern, sollten Sie den mGuard anschließend neu starten, um bestehende Sitzungen mit nicht mehr gültigen Passwörtern sicher zu beenden.

Aktiviere SSH-Fernzugang

Aktivieren Sie die Funktion, um SSH-Fernzugriff zu ermöglichen.

SSH-Zugriff über das Interface *Intern* (d. h. aus dem direkt angeschlossenen LAN oder vom direkt angeschlossenen Rechner aus) ist unabhängig von der Aktivierung der Funktion möglich.
Nach Aktivierung des Fernzugangs ist der Zugriff über die Interfaces *Intern* und *VPN* möglich.

Um Zugriffsmöglichkeiten auf den mGuard differenziert festzulegen, müssen Sie die Firewall-Regeln für die verfügbaren Interfaces entsprechend definieren (siehe „Erlaubte Netzwerke“ auf Seite 61).

Erlaube SSH-Zugang als Benutzer root

Standard: aktiviert

Bei aktivierter Funktion kann sich der Benutzer „*root*“ via SSH-Zugang auf dem Gerät anmelden.

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

Port für eingehende SSH-Verbindungen (nur Fernzugang) (Nur wenn SSH-Fernzugang aktiviert ist)	**Standard: 22** Wird diese Port-Nummer geändert, gilt die geänderte Port-Nummer nur für Zugriffe über das Interface *Extern, DMZ* und *VPN*. Im Stealth-Modus wird eingehender Verkehr auf dem angegebenen Port nicht mehr zum Client weitergeleitet. Im Router-Modus mit NAT bzw. Port-Weiterleitung hat die hier eingestellte Portnummer Priorität gegenüber Regeln zur Port-Weiterleitung. Für internen Zugriff gilt weiterhin Port 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
Ablauf der Sitzung	Gibt an, nach wie viel Zeit (in hh:mm:ss) 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. 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 nächsten Anfrage nach einem Lebenszeichen“ auf Seite 59.

Verwaltung >> Systemeinstellungen >> Shell-Zugang [...]		
	Verzögerung bis zur nächsten Anfrage nach einem Lebenszeichen	**Standard: 120 Sekunden (0:02:00)** Einstellbar sind Werte von 0 Sekunden bis 1 Stunde. 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 Wert 0 bedeutet, dass keine Anfragen nach einem Lebenszeichen gesendet werden. Da die Anzahl der gleichzeitiger Sitzungen begrenzt ist, ist es wichtig, abgelaufene Sitzungen zu beenden (siehe *„Maximale Anzahl gleichzeitiger Sitzungen pro Rolle“ auf Seite 60*). 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. Deshalb wird die Anfrage nach einem Lebenszeichen auf 120 Sekunden voreingestellt. Bei maximal drei Anfragen nach einem Lebenszeichen, wird eine abgelaufene Sitzung nach sechs Minuten entdeckt und entfernt. In vorherigen Versionen war die Voreinstellung „0“. 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. Die Eingabe kann aus Sekunden [ss], Minuten und Sekunden [mm:ss] oder Stunden, Minuten und Sekunden [hh:mm:ss] bestehen.
	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.

Verwaltung >> Systemeinstellungen >> Shell-Zugang [...]		
	SSH und HTTPS Schlüssel erneuern	**Generiere neue Schlüssel** Schlüssel, die mit einer älteren Firmware-Version erstellt worden sind (insbesondere < 10.5), 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 Web-Browser zur Verfügung gestellt werden. Die erzeugten Schlüssel werden bei einem Update auf eine neue Firmware-Version nicht neu generiert, sondern beibehalten.
Maximale Anzahl gleichzeitiger Sitzungen pro Rolle	Sie können die Anzahl der Benutzer (SSH-Sessions), die gleichzeitig auf die Kommandozeile des mGuards zugreifen dürfen begrenzen. Der Benutzer „*root*“ hat immer uneingeschränkten Zugang. Die Anzahl der Zugänge (SSH-Sessions) für administrative Benutzerrollen (*admin, netadmin, audit*) können jeweils einzeln begrenzt werden. Die Berechtigungsstufen *netadmin* und *audit* beziehen sich auf Zugriffsrechte bei Zugriffen mit dem mGuard device manager (FL MGUARD DM UNLIMITED). Die Einschränkung hat keine Auswirkung auf bereits bestehende Sitzungen, sondern nur auf neu aufgebaute Zugriffe. Pro Sitzung werden ca. 0,5 MB Speicherplatz benötigt.	
	Admin	2 bis 10 (Standard: 4) Für die Rolle „*admin*“ sind mindestens 2 gleichzeitig erlaubte Sitzungen erforderlich, damit sich „*admin*“ nicht selbst aussperrt.
	Netadmin	0 bis 10 (Standard: 2) Bei „0“ ist keine Sitzung erlaubt. Es kann sein, dass der Benutzer „*netadmin*“ nicht verwendet wird.
	Audit	0 bis 10 (Standard: 2) Bei „0“ ist keine Sitzung erlaubt. Es kann sein, dass der Benutzer „*audit*“ nicht verwendet wird.

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

Erlaubte Netzwerke

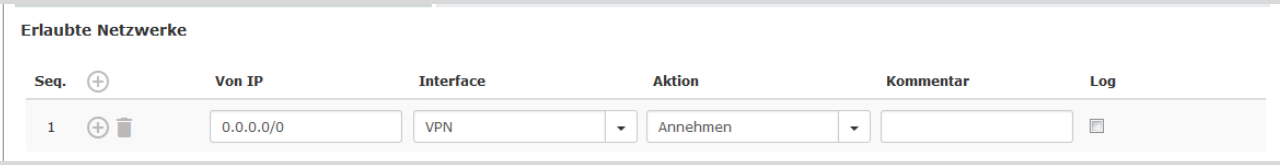
Sie können den SSH-Zugriff auf die Kommandozeile des mGuards mittels Firewall-Regeln auf ausgewählte Interfaces und Netzwerke beschränken.

Die Regeln gelten für eingehende Datenpakete und können geräteabhängig für alle Interfaces konfiguriert werden.

1. Für den SSH-Fernzugang (*Extern* und *DMZ*) gilt:
   a) Der Zugang über die Interfaces *Extern* und *DMZ* ist grundsätzlich deaktiviert, wenn die Funktion **Aktiviere SSH-Fernzugang** deaktiviert ist.
   b) Der Zugang über die Interfaces *Extern* und *DMZ* ist auch deaktiviert, wenn keine Firewall-Regel besteht, die den Zugriff explizit erlaubt (Aktion = Annehmen).
   c) Um den Zugriff zu erlauben, müssen Sie sowohl die Funktion **Aktiviere SSH-Fernzugang** aktivieren als auch eine entsprechende Firewall-Regel für die Interfaces *Extern* und *DMZ* konfigurieren (Aktion = Annehmen).
2. Für den internen LAN-Zugang (*Intern*) und den VPN-Zugang (*VPN*) gilt abweichend:
   a) Der Zugang über das Interface *Intern* (LAN) ist immer erlaubt, wenn er nicht durch eine explizite Firewall-Regel in dieser Tabelle verboten wird (Aktion = Verwerfen oder Abweisen).
   a) Der Zugang über über das Interface *VPN* ist erlaubt, wenn die Funktion **Aktiviere SSH-Fernzugang** aktiviert wurde und wenn er nicht durch eine explizite Firewall-Regel in dieser Tabelle verboten wird (Aktion = Verwerfen oder Abweisen).

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:



Von IP

Geben Sie hier die Adresse des Rechners oder Netzes an, von dem der Zugang 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 43.

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

	Interface	**Intern / Extern / DMZ / VPN** Gibt an, für welches Interface die Regel gelten soll. Sind keine Regeln gesetzt oder greift keine Regel, gelten folgende Standardeinstellungen: – SSH-Zugriffe über *Intern* und *VPN* sind erlaubt. – SSH-Zugriffe über *Extern* und *DMZ* werden verwehrt. Legen Sie die Zugriffsmöglichkeiten nach Bedarf fest. **ACHTUNG:** Wenn Sie Zugriffe über *Intern* oder *VPN* verwehren wollen, müssen Sie das explizit durch entsprechende Firewall-Regeln bewirken, in denen 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	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 – Funktion *Log* aktivieren – oder das Ereignis nicht protokolliert werden soll – Funktion *Log* deaktivieren (Standard). Log-Meldung (Beispiel): 2024-11-25_10:09:51.83909 firewall: fw-ssh-access-1-12e7d62f-6be7-1c6e-b8a6-000cbe00105c act=REJECT IN=eth0 MAC=d4:aa:62:b2:6d:62 SRC=192.168.1.55 DST=192.168.1.55 LEN=52 TOS=0x00 PREC=0x00 TTL=128 ID=47714 DF PROTO=TCP SPT=53379 DPT=22 SEQ=506303301 ACK=0 WINDOW=64240 SYN URGP=0 CTMARK=100030
RADIUS-Authentifizierung	Benutzer können bei ihrer Anmeldung über einen RADIUS-Server authentifiziert werden. Dies gilt für Anwender, die über den Shell-Zugang mit Hilfe von SSH auf den mGuard zugreifen wollen. Bei den vordefinierten Benutzern *(root, admin, netadmin* und *audit)* wird das Passwort lokal geprüft.	

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

Nutze RADIUS-Authentifizierung für den Shell-Zugang

Ja / Nein / Als einzige Methode zur Passwortprüfung

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 auf den mGuard zugreifen wollen. Nur bei den vordefinierten Benutzern *(root, admin, netadmin, audit)* wird das Passwort lokal geprüft.

Die Berechtigungsstufen *netadmin* und *audit* beziehen sich auf Zugriffsrechte bei Zugriffen mit dem mGuard device manager (FL MGUARD DM UNLIMITED).

Wenn Sie unter **„X.509-Authentifizierung“** den Punkt **„Unterstütze 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 Änderungen am Authentifizierungsverfahren vornehmen, sollten Sie den mGuard anschließend neu starten, um bestehende Sitzungen mit nicht mehr gültigen Zertifikaten oder Passwörtern sicher zu beenden.

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 beim mGuard anmelden.

Verwaltung >> Systemeinstellungen >> Shell-Zugang

X.509-Authentifizierung

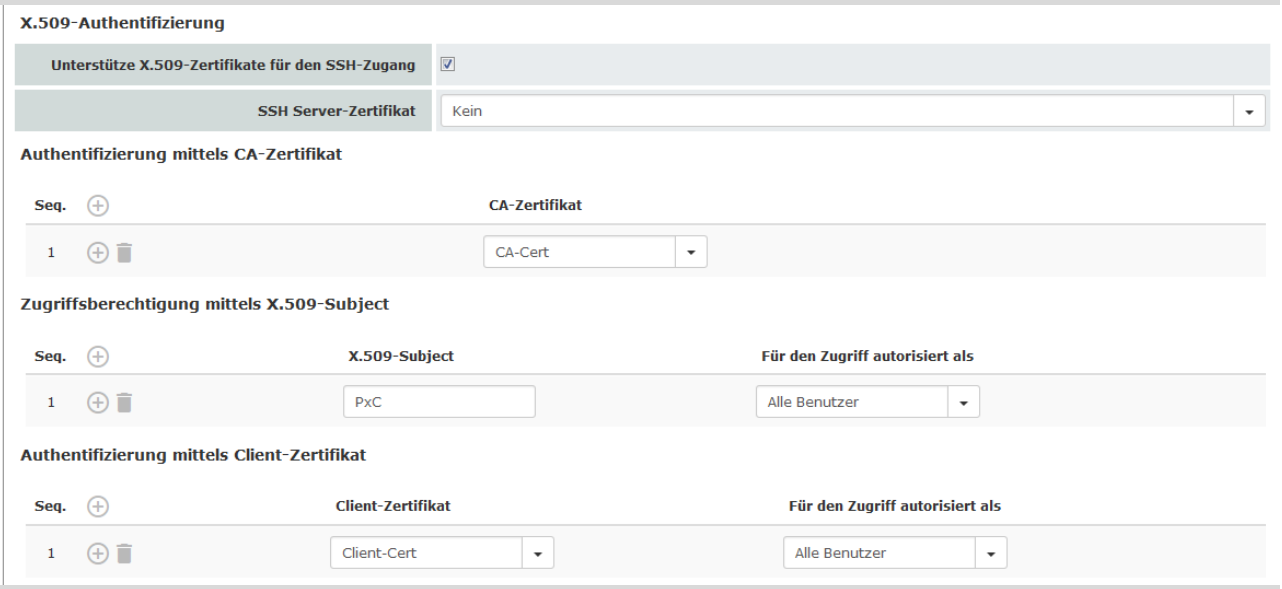
X.509-Zertifikate für den SSH-Clienten

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 56).

Wenn der Gültigkeitszeitraum des Client-Zertifikats vom mGuard geprüft wird (siehe „Zertifikatseinstellungen“ auf Seite 197), dann müssen irgendwann 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.

Wenn Sie Änderungen am Authentifizierungsverfahren vornehmen, sollten Sie den mGuard anschließend neu starten, um bestehende Sitzungen mit nicht mehr gültigen Zertifikaten oder Passwörtern sicher zu beenden.



Verwaltung >> Systemeinstellungen >> Shell-Zugang [...]	
Unterstütze X.509-Zertifikate für den SSH-Zugang	**Ist die Funktion deaktiviert**, werden zur Authentifizierung nur die herkömmlichen Authentifizierungsverfahren (Benutzername und Passwort bzw. privater und öffentlicher Schlüssel) erlaubt, nicht das X.509-Authentifizierungsverfahren. **Ist die Funktion aktiviert**, kann zur Authentifizierung zusätzlich zum herkömmlichen Authentifizierungsverfahren (wie es auch bei deaktivierter Funktion verwendet wird) das X.509-Authentifizierungsverfahren verwendet werden. Bei aktivierter Funktion 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 192).
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 selbstsigniertes Zertifikat Zum Verständnis der nachfolgenden Tabelle siehe Kapitel „Authentifizierung >> Zertifikate“ .

Authentifizierung bei SSH

Die Gegenstelle zeigt vor:	Zertifikat (personenbezogen) von **CA signiert**	Zertifikat (personenbezogen) **selbstsigniert**
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 Client-Zertifikaten (Gegenstellen-Zertifikaten), **wenn** sie als Filter verwendet werden	Client-Zertifikat (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 *„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

Authentifizierung mittels 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.

Wenn Sie Änderungen am Authentifizierungsverfahren vornehmen, sollten Sie den mGuard anschließend neu starten, um bestehende Sitzungen mit nicht mehr gültigen Zertifikaten oder Passwörtern sicher zu beenden.

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

Zugriffsberechtigung mittels 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 367*).

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

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 mGuard device manager (FL MGUARD DM UNLIMITED).

Authentifizierung mittels Client-Zertifikat

Die Konfiguration ist in den folgenden Fällen erforderlich:

– SSH-Clients zeigen jeweils ein selbstsigniertes 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 Client-Zertifikat (Gegenstellen-Zertifikat) der mGuard heranziehen soll, um die Gegenstelle, den SSH-Client, zu authentifizieren.

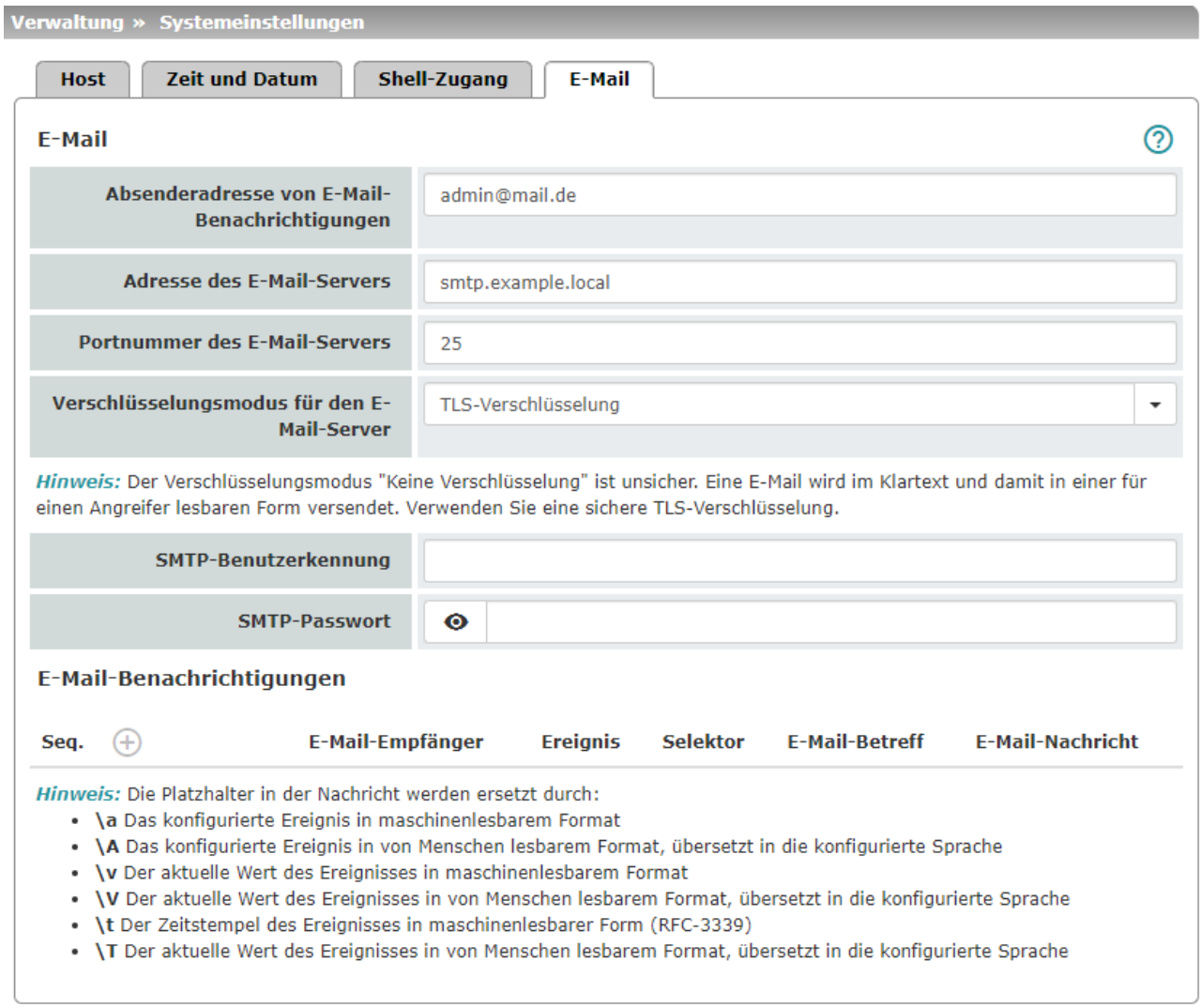
Dazu in der Auswahlliste eines der Client-Zertifikate auswählen. Die Auswahlliste stellt die Client-Zertifikate zur Wahl, die in den mGuard unter Menüpunkt *„Authentifizierung >> Zertifikate“* geladen worden sind.

Wenn Sie Änderungen am Authentifizierungsverfahren vornehmen, sollten Sie den mGuard anschließend neu starten, um bestehende Sitzungen mit nicht mehr gültigen Zertifikaten oder Passwörtern sicher zu beenden.

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 mGuard device manager (FL MGUARD DM UNLIMITED).

4.1.4 E-Mail



Verwaltung >> Systemeinstellungen >> E-Mail

E-Mail (Achten Sie auf die korrekte Konfiguration der E-Mail-Einstellungen des mGuards)	Sie können den mGuard für die Versendung von E-Mails über einen E-Mail-Server konfigurieren. Bestimmte Ereignisse können damit im Falle ihres Eintretens an frei wählbare Empfänger im Klartext oder in maschinenlesbarer Form versendet werden.
Absenderadresse von E-Mail-Benachrichtigungen	E-Mail-Adresse, die als Absender vom mGuard angezeigt wird.
Adresse des E-Mail-Servers	Adresse des E-Mail-Servers
Port-Nummer des E-Mail-Servers	Port-Nummer des E-Mail-Servers

Verwaltung >> Systemeinstellungen >> E-Mail [...]		
	Verschlüsselungsmodus für den E-Mail-Server	**Keine Verschlüsselung* / TLS-Verschlüsselung (Standard) / TLS-Verschlüsselung mit StartTLS** Verschlüsselungsmodus für den E-Mail-Server **Verwenden Sie sicherer Algorithmen** Einige der zur Verfügung stehenden Algorithmen sind veraltet und werden nicht mehr als sicher angesehen. Sie sind deshalb nicht zu empfehlen. Aus Gründen der Abwärtskompatibilität können sie jedoch weiterhin ausgewählt und verwendet werden. Im WBM sind entsprechend veraltete Algorithmen oder unsichere Einstellungen mit einem Sternchen (*) markiert. Siehe „Verwendung sicherer Verschlüsselungs- und Hash-Algorithmen“ .
	SMTP-Benutzerkennung	Benutzerkennung (Login)
	SMTP-Passwort	Passwort für den E-Mail-Server
E-Mail-Benachrichtigungen	Es können beliebige E-Mail-Empfänger mit vordefinierten Ereignissen und einer frei definierbaren Nachricht verknüpft werden. Die Liste wird von oben nach unten abgearbeitet.	
	E-Mail-Empfänger	Legt eine E-Mail-Adresse an.
	Ereignis	Wenn das ausgewählte Ereignis eintritt oder das Ereignis das erste Mal konfiguriert wird, wird die damit verknüpfte Empfängeradresse angewählt und an diese wird das Ereignis als E-Mail geschickt. Zusätzlich kann eine E-Mail-Nachricht hinterlegt und gesendet werden. Manche der aufgelisteten Ereignisse sind abhängig von der verwendeten Hardware. Eine vollständige Liste aller Ereignisse finden Sie unter „Ereignistabelle“ auf Seite 72.
	Selektor	Hier können konfigurierte VPN-Verbindungen (IPsec-VPN / OpenVPN) oder Firewall-Regelsätze ausgewählt werden, die per E-Mail überwacht werden sollen.
	E-Mail-Betreff	Text erscheint in der Betreff-Zeile der E-Mail Der Text ist frei definierbar. Sie können Bausteine aus der Ereignistabelle verwenden, die als Platzhalter in Klartext (\A und \V) oder in maschinenlesbarer Form (\a und \v) eingefügt werden können. Zeitstempel in Form eines Platzhalters (\T bzw. \t (maschinenlesbar)) können ebenfalls eingefügt werden.

Verwaltung >> Systemeinstellungen >> E-Mail [...]		
	E-Mail-Nachricht	Sie können hier den Text eingeben, der als E-Mail verschickt wird. Der Text ist frei definierbar. Sie können Bausteine aus der Ereignistabelle verwenden, die als Platzhalter in Klartext (\A und \V) oder in maschinenlesbarer Form (\a und \v) eingefügt werden können. Zeitstempel in Form eines Platzhalters in Klartext (\T) oder maschinenlesbar (\t) können ebenfalls eingefügt werden.

Zeitstempel

Tabelle 4-1 Beispiele für Zeitstempel

Klartext \T	Maschinenlesbar \t (nach RFC-3339)
Montag, April 22 2016 13:22:36	2016-04-22T11:22:36+0200

Ereignistabelle

Tabelle 4-2 Ereignistabelle

Klartext		Maschinenlesbar	
\A = Ereignis	**\V = Wert**	**\a = Ereignis**	**\v = Wert**
Zustand des ECS	Nicht vorhanden	/ecs/status	1
	Entfernt		2
	Vorhanden und synchronisiert		3
	Nicht synchronisiert		4
	Allgemeiner Fehler		8
Ergebnis der Konnektivitätsprüfung des internen Interface	Konnektivitätsprüfung erfolgreich	/redundancy/cc/int/ok	yes
	Konnektivitätsprüfung fehlgeschlagen		no
Ergebnis der Konnektivitätsprüfung des externen Interface	Konnektivitätsprüfung erfolgreich	/redundancy/cc/ext/ok	yes
	Konnektivitätsprüfung fehlgeschlagen		no
Zustand des Alarmausgangs	Alarmausgang geschlossen / high [OK]	/ihal/contact	close
	Alarmausgang ist offen / low [FEHLER]		open

Tabelle 4-2 Ereignistabelle

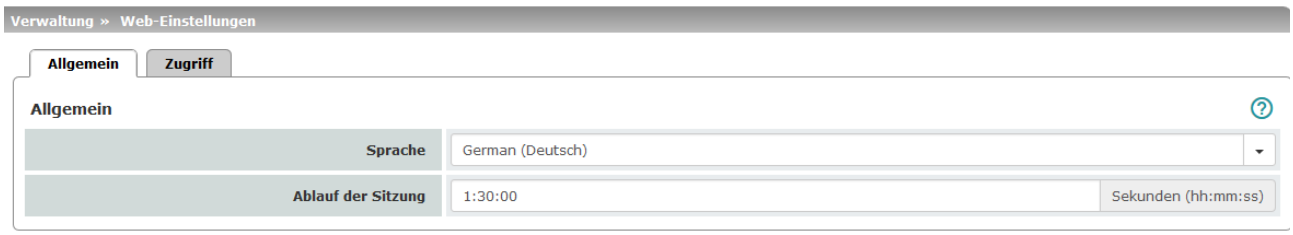
Klartext		Maschinenlesbar	
\A = Ereignis	**\V = Wert**	**\a = Ereignis**	**\v = Wert**
Aktivierungsgrund des Alarmausgangs	Kein Alarm	/ihal/contactreason	
	Keine Verbindung am externen Interface		link_ext
	Keine Verbindung am internen Interface		link_int
	Stromversorgung 1 defekt		psu1
	Stromversorgung 2 defekt		psu2
	Boardtemperatur außerhalb des konfigurierten Bereichs		temp
	Redundanz-Konnektivitätsprüfung fehlgeschlagen		ccheck
	Keine Verbindung am XF2-Interface		link_swp0
	Keine Verbindung am XF3-Interface		link_swp1
	Keine Verbindung am XF4-Interface		link_swp2
	Keine Verbindung am XF5-Interface		link_swp3
	Keine Verbindung am DMZ-Interface		link_dmz
	Passwörter nicht konfiguriert		password
Zustand der Stromversorgung 1	Stromversorgung 1 bereit	/ihal/power/psu1	ok
	Stromversorgung 1 defekt		fail
Zustand der Stromversorgung 2	Stromversorgung 2 bereit	/ihal/power/psu2	ok
	Stromversorgung 2 defekt		fail
Zustand des Eingangs/ CMD 1 (I1)	Service Eingang/CMD1 (I1) aktiviert	/ihal/service/cmd1	on
	Service Eingang/CMD1 (I1) deaktiviert		off
Zustand des Eingangs/ CMD 2 (I2)	Service Eingang/CMD2 (I2) aktiviert	/ihal/service/cmd2	on
	Service Eingang/CMD2 (I2) deaktiviert		off
Zustand des Eingangs/ CMD 3 (I3)	Service Eingang/CMD3 (I3) aktiviert	/ihal/service/cmd3	on
	Service Eingang/CMD3 (I3) deaktiviert		off
Temperaturzustand des Gerätes	Temperatur OK	/ihal/temperature/board_alarm	ok
	Temperatur zu heiß		hot
	Temperatur zu kalt		cold

Tabelle 4-2 Ereignistabelle

Klartext		Maschinenlesbar	
\A = Ereignis	**\V = Wert**	**\a = Ereignis**	**\v = Wert**
Zustand der Redundanz	Die Redundanzsteuerung startet	/redundancy/status	booting
	Keine hinreichende Netzwerkanbindung		faulty
	Keine hinreichende Netzwerkanbindung und wartet auf eine Komponente		faulty_waiting
	Synchronisiert sich mit aktivem Gerät		outdated
	Synchronisiert sich mit aktivem Gerät und wartet auf eine Komponente		outdated_waiting
	In Bereitschaft		on_standby
	In Bereitschaft und wartet auf eine Komponente		on_standby_waiting
	Wird aktiv		becomes_active
	Leitet Netzwerkverkehr weiter		active
	Leitet Netzwerkverkehr weiter und wartet auf eine Komponente		active_waiting
Aktivierungszustand der IPsec VPN-Verbindung	Gestoppt	/vpn/con/*/armed	no
	Gestartet		yes
IPsec-SA-Status der VPN-Verbindung	Keine IPsec-SAs aufgebaut	/vpn/con/*/ipsec	down
	Nicht alle IPsec-SAs aufgebaut		some
	Alle IPsec-SAs aufgebaut		up
Aktivierungszustand des Firewall-Regelsatzes	Der Zustand der Firewall-Regelsätze hat sich geändert.	/fwrules/*/state	inactive
			active
Aktivierungszustand der OpenVPN-Verbindung	Gestoppt	/openvpn/con/*/armed	no
	Gestartet		yes
Status der OpenVPN-Verbindung	Getrennt	/openvpn/con/*/state	down
	Aufgebaut		up

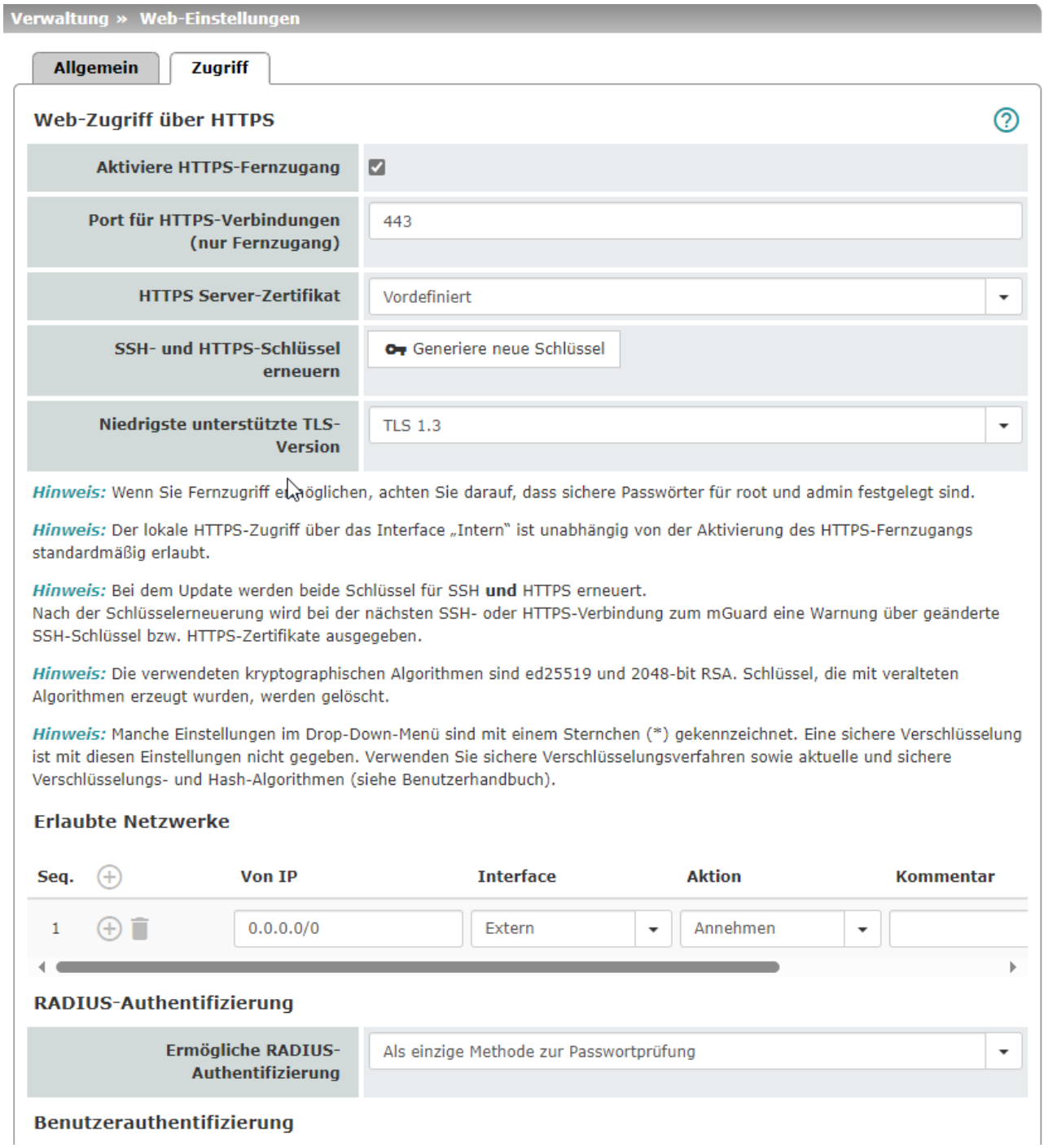
4.2 Verwaltung >> Web-Einstellungen

4.2.1 Allgemein



Verwaltung >> Web-Einstellungen >> Allgemein		
Allgemein	**Sprache**	Ist in der Sprachauswahlliste **Automatisch** ausgewählt, übernimmt das Gerät die Spracheinstellung aus dem Web-Browser des Rechners.
	Ablauf der Sitzung	Zeit der Inaktivität, nach denen der Benutzer von der Web-Schnittstelle des mGuards automatisch abgemeldet wird. Mögliche Werte: 15 bis 86400 Sekunden (= 24 Stunden) Die Eingabe kann aus Sekunden [ss], Minuten und Sekunden [mm:ss] oder Stunden, Minuten und Sekunden [hh:mm:ss] bestehen.

4.2.2 Zugriff



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 >> Web-Einstellungen >> Zugriff

Web-Zugriff über HTTPS

Bei aktiviertem HTTPS-Fernzugang kann der mGuard über seine Web-Oberfläche **von entfernten Rechnern aus** konfiguriert werden. Der Zugang erfolgt mittels Web-Browser (z. B. Mozilla Firefox, Google Chrome, Microsoft Edge).

Benutzen Sie immer **aktuelle Web-Browser**, um die Verwendung schwacher Verschlüsselungsalgorithmen zu vermeiden.

Wenn Sie Änderungen am Authentifizierungsverfahren vornehmen, sollten Sie den mGuard anschließend neu starten, um bestehende Sitzungen mit nicht mehr gültigen Zertifikaten oder Passwörtern sicher zu beenden.

Der **HTTPS-Fernzugang** ist standardmäßig deaktiviert. Nach einer Aktivierung kann er auf ausgewählte Interfaces und Netzwerke beschränkt werden.

ACHTUNG: Zugriff auf das Gerät über externe Netze möglich.
Die Server-Dienste des Geräts sind je nach Einstellung über externe Netze und möglicherweise aus dem Internet erreichbar. Stellen Sie sicher, dass der Zugriff nur erfolgen kann, wenn er erwünscht ist. Konfigurieren Sie andernfalls Ihr Netzwerk entsprechend, um einen Zugriff zu verhindern.

ACHTUNG: Der lokale HTTPS-Zugriff über das Interface „Intern“ ist unabhängig von der Aktivierung des SSH-Fernzugangs standardmäßig erlaubt.

Um Zugriffsmöglichkeiten auf den mGuard differenziert festzulegen, müssen Sie entsprechende Firewall-Regeln definieren (siehe „Erlaubte Netzwerke“ auf Seite 82).

ACHTUNG: Wenn Sie den Fernzugang ermöglichen, achten Sie darauf, dass sichere Passwörter für die Benutzer *root* und *admin* festgelegt sind.

Wenn Sie das Passwort für *root* oder *admin* ändern, sollten Sie den mGuard anschließend neu starten, um bestehende Sitzungen mit nicht mehr gültigen Passwörtern sicher zu beenden.

Aktiviere HTTPS-Fernzugang

Aktivieren Sie die Funktion, um den HTTPS-Fernzugriff zu ermöglichen.

HTTPS-Zugriff über das Interface *Intern* (d. h. aus dem direkt angeschlossenen LAN oder vom direkt angeschlossenen Rechner aus) ist unabhängig von der Aktivierung der Funktion möglich.

Nach Aktivierung des Fernzugangs ist der Zugriff über die Interfaces *Intern* und *VPN* möglich.

Um Zugriffsmöglichkeiten auf den mGuard differenziert festzulegen, müssen Sie die Firewall-Regeln für die verfügbaren Interfaces entsprechend definieren (siehe „Erlaubte Netzwerke“ auf Seite 82).

Zusätzlich müssen gegebenenfalls unter **Benutzerauthentifizierung** die Authentifizierungsregeln gesetzt werden.

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

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, DMZ* und *VPN*. Für internen Zugriff gilt weiterhin 443.

Im Stealth-Modus wird eingehender Verkehr auf dem angegebenen Port nicht mehr zum Client weitergeleitet.

Im Router-Modus mit NAT bzw. Port-Weiterleitung hat die hier eingestellte Portnummer Priorität gegenüber Regeln zur Port-Weiterleitung.

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: Wenn dieser mGuard über die Adresse 123.124.125.21 über das Internet zu erreichen ist und für den Fernzugang die Port-Nummer 443 festgelegt ist, 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/

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

HTTPS Server-Zertifikat	**Vordefiniert / <Maschinenzertifikat>**

Vordefiniertes Zertifikat

In der Werkseinstellung zeigt das mGuard-Gerät ein vorinstalliertes, selbstsigniertes Webserver-Zertifikat vor, wenn ein Client (z. B. ein Web-Browser) den Webserver des Gerätes kontaktiert.

Damit ist es dem Client grundsätzlich möglich, die Authentizität des mGuard-Gerätes zu verifizieren.

Individuelles Maschinenzertifikat (selbstsigniert)

Anstelle des vorinstallierten Zertifikats kann zur Authentifizierung des Webservers ein eigenes, selbst erstelltes Maschinenzertifikat verwendet werden.

Dieses Zertifikat muss zunächst auf das mGuard-Gerät hochgeladen werden, damit es in der Drop-Down-Liste ausgewählt werde kann (siehe Kapitel 6.4.2).

Beachten Sie Folgendes:

– Enthält das Zertifikat Attribute des Typs "*key usage*“, müssen diese den Wert "*digital signature*", "*key encipherment*" oder "*key agreement*" beinhalten.
– Enthält das Zertifikat Attribute des Typs "*extended key usage*", müssen diese den Wert "*TLS web server authentication*" enthalten.
– Enthält das Zertifikat Attribute des Typs "*netscape certificate*" (nicht empfohlen), müssen diese den Wert "*SSL server*" enthalten.

Individuelles Maschinenzertifikat (CA signiert)

Wurde das eigene Maschinenzertifikat von einer CA ausgestellt, muss die gesamte Zertifikatskette, einschließlich des Root-CA-Zertifikats und aller CA-Zwischenzertifikate, auf das Gerät hochgeladen werden (Authentifizierung >> Zertifikate >> CA-Zertifikate), damit eine Kette des Vertrauens (*chain of trust*) gebildet werden kann (siehe Kapitel 6.4.3 und „CA-Zertifikat“).

Das Maschinenzertifikat muss ebenfalls auf dem Gerät gespeichert werden (Authentifizierung >> Zertifikate >> Maschinenzertifikate).

Um das Gerät zu authentifizieren, verwendet der Client (z. B. Web-Browser) die gesamte Zertifikatskette. Der Client muss dem Root-CA-Zertifikat vertrauen.

Verwaltung >> Web-Einstellungen >> Zugriff [...]		
	SSH- und HTTPS-Schlüssel erneuern	**Generiere neue Schlüssel** Schlüssel, die mit einer älteren Firmware-Version erstellt worden sind (insbesondere < mGuard 10.5), 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 Web-Browser zur Verfügung gestellt werden. Die erzeugten Schlüssel werden bei einem Update auf eine neue Firmware-Version nicht neu generiert, sondern beibehalten.

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

Niedrigste unterstützte TLS-Version

TLS 1.0/1.1*, TLS 1.2 (Standard), TLS 1.3

Wählen Sie aus Sicherheitsgründen die Version TLS 1.2 oder TLS 1.3 als „Niedrigste unterstützte TLS-Version“, um sichere TLS-verschlüsselte Verbindungen (z. B. HTTPS-Verbindungen zum Gerät) zu gewährleisten.

Im WBM sind entsprechend veraltete Algorithmen oder unsichere Einstellungen mit einem Sternchen (*) markiert.

Siehe auch Kapitel 3.1, „Sichere Verschlüsselung“.

Das mGuard-Gerät unterstützt TLS-verschlüsselte Verbindungen zu anderen Gegenstellen. Dabei kann die Verbindung vom mGuard-Gerät selbst (mGuard = Client) oder von der Gegenstelle (mGuard = Server) aufgebaut werden.

Für TLS-verschlüsselte Verbindungen gilt, dass beide Gegenstellen die gleiche und mindestens die hier ausgewählte „Niedrigste unterstützte TLS-Version“ verwenden müssen.

Verwendet ein Client (z. B. ein Web-Browser, der den Web-Server des mGuard-Gerätes kontaktiert) eine veraltete und damit unsichere TLS-Version, wird die Verbindungsanfrage vom mGuard-Gerät nur dann akzeptiert, wenn sie als „Niedrigste unterstützte TLS-Version“ ausgewählt wurde.

Ist die verwendete TLS-Version des Clients niedriger als die hier konfigurierte , wird die Verbindung abgelehnt.

ACHTUNG: Diese Einschränkung gilt nicht für TSL-verschlüsselte Verbindungen, die TCP-Kapselung/„Path Finder“ verwenden (siehe „TCP-Kapselung“ auf Seite 253).

Aus Gründen der Abwärtskompatibilität können in diesen Verbindungen grundsätzlich immer (und unabhängig von der hier festgelegten niedrigsten unterstützten TLS-Version) die TLS-Versionen TLS 1.0/1.1 verwenden werden.

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

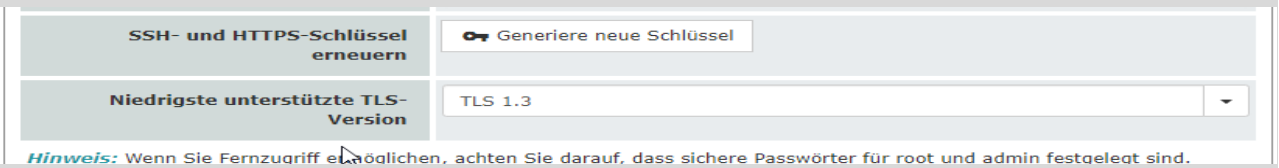
Erlaubte Netzwerke

Sie können den HTTPS-Zugriff auf den mGuard mittels Firewall-Regeln auf ausgewählte Interfaces und Netzwerke beschränken.

1. Für den HTTPS-Fernzugang (*Extern* und *DMZ*) gilt:
   a) Der Zugang über die Interfaces *Extern* und *DMZ* ist grundsätzlich deaktiviert, wenn die Funktion **Aktiviere SSH-Fernzugang** deaktiviert ist.
   b) Der Zugang über die Interfaces *Extern* und *DMZ* ist auch deaktiviert, wenn keine Firewall-Regel besteht, die den Zugriff explizit erlaubt (Aktion = Annehmen).
   c) Um den Zugriff zu erlauben, müssen Sie sowohl die Funktion **Aktiviere HTTPS-Fernzugang** aktivieren als auch eine entsprechende Firewall-Regel für die Interfaces *Extern* und *DMZ* konfigurieren (Aktion = Annehmen).
2. Für den internen LAN-Zugang (*Intern*) und den VPN-Zugang (*VPN*) gilt abweichend:
   a) Der Zugang über das Interface *Intern* (LAN) ist immer erlaubt, wenn er nicht durch eine explizite Firewall-Regel in dieser Tabelle verboten wird (Aktion = Verwerfen oder Abweisen).
   a) Der Zugang über über das Interface *VPN* ist erlaubt, wenn die Funktion **Aktiviere HTTPS-Fernzugang** aktiviert wurde und wenn er nicht durch eine explizite Firewall-Regel in dieser Tabelle verboten wird (Aktion = Verwerfen oder Abweisen).

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:



Von IP

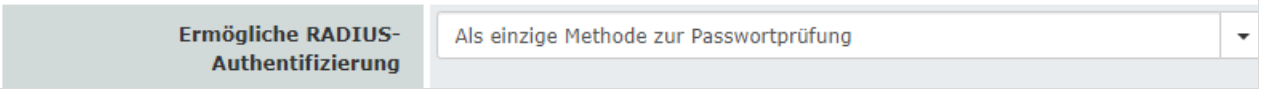
Geben Sie hier die Adresse des Rechners oder Netzes an, von dem der Zugang erlaubt beziehungsweise verboten ist.

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 43.

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

	Interface	**Intern / Extern / DMZ / VPN** Gibt an, für welches Interface die Regel gelten soll. Sind keine Regeln gesetzt oder greift keine Regel, gelten folgende **Standardeinstellungen**: – HTTPS-Zugriffe über *Intern* und *VPN* sind erlaubt. – HTTPS-Zugriffe über *Extern* und *DMZ* werden verwehrt. Legen Sie die Zugriffsmöglichkeiten nach Bedarf fest. Wenn Sie Zugriffe über *Intern* oder *VPN* verwehren wollen, müssen Sie das explizit durch entsprechende Firewall-Regeln bewirken, in denen 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, 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 – Funktion *Log* aktivieren – oder das Ereignis nicht protokolliert werden soll – Funktion *Log* deaktivieren (Standard). Log-Meldung (Beispiel): 2024-11-25_10:09:51.83909 firewall: fw-https-access-1-12e7d62f-6be7-1c6e-b8a6-000cbe00105c act=REJECT IN=eth0 MAC=d4:aa:62:b2:6d:62 SRC=192.168.1.55 DST=192.168.1.55 LEN=52 TOS=0x00 PREC=0x00 TTL=128 ID=47714 DF PROTO=TCP SPT=53379 DPT=22 SEQ=506303301 ACK=0 WINDOW=64240 SYN URGP=0 CTMARK=100030
RADIUS-Authentifizierung	Benutzer können bei ihrer Anmeldung über einen RADIUS-Server authentifiziert werden. Nur bei den vordefinierten Benutzern *(root, admin, netadmin, audit* und *user)* wird das Passwort lokal geprüft.	

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



Ermögliche RADIUS-Authentifizierung

Ja / Nein / Als einzige Methode zur Passwortprüfung

Bei aktivierter Funktion 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.

Wenn Sie Änderungen am Authentifizierungsverfahren vornehmen, sollten Sie den mGuard anschließend neu starten, um bestehende Sitzungen mit nicht mehr gültigen Zertifikaten oder Passwörtern sicher zu beenden.

Die Berechtigungsstufen *netadmin* und *audit* beziehen sich auf Zugriffsrechte bei Zugriffen mit dem mGuard device manager (FL MGUARD DM UNLIMITED).

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.

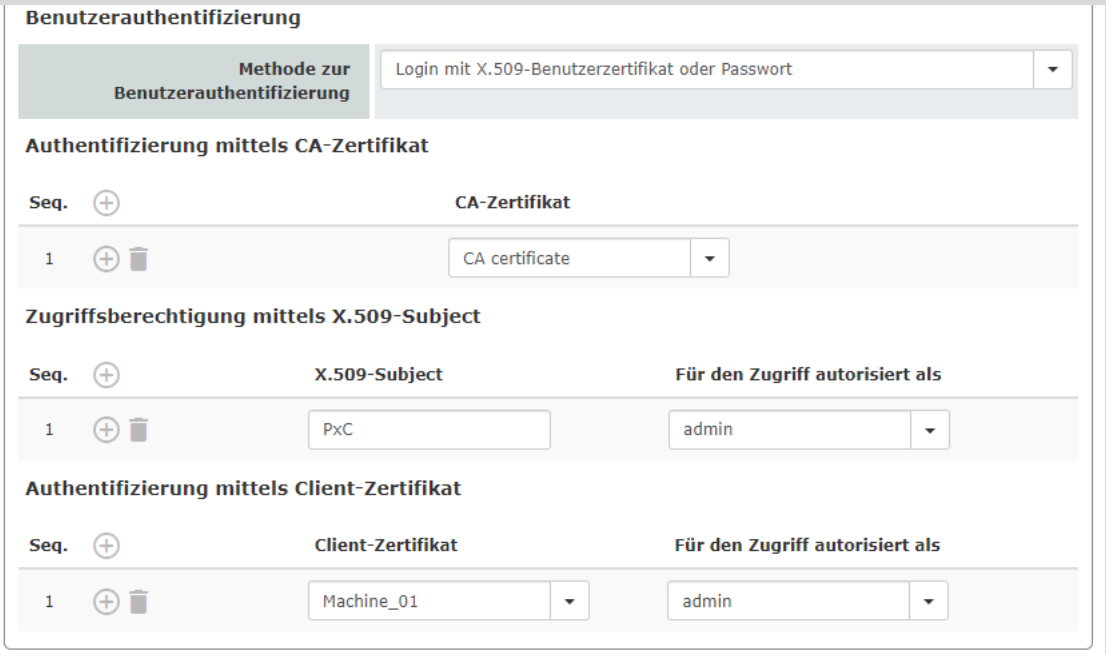
Wenn Sie die RADIUS-Authentifizierung **als einzige Methode zur Passwortprüfung** ausgewählt haben, dann ist der Zugang zum mGuard unter Umständen nicht mehr möglich. Dies gilt z. B. wenn Sie einen falschen RADIUS-Server einrichten oder den mGuard umsetzen. Die vordefinierten Benutzer (*root*, *admin*, *netadmin*, *audit* und *user)* werden dann nicht mehr akzeptiert.

Verwaltung >> Web-Einstellung >> Zugriff

Benutzerauthentifizierung

Sie können festlegen, ob sich ein Benutzer des mGuards bei seiner Anmeldung mit einem Passwort, einem X.509-Benutzerzertifikat oder einer Kombination daraus authentifiziert.

Wenn Sie Änderungen am Authentifizierungsverfahren vornehmen, sollten Sie den mGuard anschließend neu starten, um bestehende Sitzungen mit nicht mehr gültigen Zertifikaten oder Passwörtern sicher zu beenden.



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

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 181). Außerdem gibt es die Möglichkeit der RADIUS-Authentifizierung (siehe Seite 188). Wenn Sie Passwörter ändern oder Änderungen am Authentifizierungsverfahren vornehmen, sollten Sie den mGuard anschließend neu starten, um bestehende Sitzungen mit nicht mehr gültigen Zertifikaten oder Passwörtern sicher zu beenden. 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 Web-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 Web-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. **Es könnte sonst 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,

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 Web-Browser bei Verbindungsaufnahme eines der folgenden Zertifikatstypen vorzeigt:

– ein von einer CA signiertes Zertifikat
– ein selbstsigniertes Zertifikat.

Zum Verständnis der nachfolgenden Tabelle siehe „Authentifizierung >> Zertifikate“ auf Seite 192.

X.509-Authentifizierung bei HTTPS

Die Gegenstelle zeigt vor:	Zertifikat (personenbezogen) von **CA signiert**[1]	Zertifikat (personenbezogen) **selbstsigniert**
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 Client-Zertifikaten (Gegenstellen-Zertifikaten), **wenn** sie als Filter verwendet werden.	Client-Zertifikat (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 Web-Browser zu authentifizieren.

Die nachfolgenden Anleitungen gehen davon aus, dass die Zertifikate bereits ordnungsgemäß im mGuard installiert sind (siehe „Authentifizierung >> Zertifikate“ auf Seite 192).

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

Authentifizierung mittels CA-Zertifikat

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

Wenn Sie Änderungen am Authentifizierungsverfahren vornehmen, sollten Sie den mGuard anschließend neu starten, um bestehende Sitzungen mit nicht mehr gültigen Zertifikaten oder Passwörtern sicher zu beenden.

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 Web-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 [...]

Zugriffsberechtigung mittels X.509-Subject

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

Dadurch ist es möglich, den Zugriff von Web-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 367).

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

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

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

Mit * (Sternchen) im Feld *X.509-Subject* legen Sie fest, dass im vom Web-Browser/HTTPS-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) 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 Web-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 Web-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 als“).

Das hat folgende Konsequenz: Gibt es mehrere Filter, die einen bestimmten Benutzer „durchlassen“, tritt der erste Filter in Kraft.

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

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 Client-Zertifikate als Authentifizierungsmethode ausgewählt, dann haben diese Vorrang gegenüber den Filtersetzungen hier.

Für den Zugriff autorisiert als

root / admin / netadmin / audit / user

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 181.

Die Berechtigungsstufen *netadmin* und *audit* beziehen sich auf Zugriffsrechte bei Zugriffen mit dem mGuard device manager (FL MGUARD DM UNLIMITED).

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

Authentifizierung mittels Client-Zertifikat

Die Konfiguration ist in den folgenden Fällen erforderlich:

– Von entfernt zugreifende Benutzer zeigen jeweils ein selbstsigniertes 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 *Client-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 Web-Browser des von entfernt zugreifenden Benutzers, zu authentifizieren.

Dazu in der Auswahlliste eines der Client-Zertifikate auswählen.

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

Wenn Sie Änderungen am Authentifizierungsverfahren vornehmen, sollten Sie den mGuard anschließend neu starten, um bestehende Sitzungen mit nicht mehr gültigen Zertifikaten oder Passwörtern sicher zu beenden.

Der Client muss exakt dieses Zertifikat verwenden, um sich zu authentifizieren.

Weitere Informationen aus dem Zertifikat (Gültigkeitszeitraum, Aussteller und Verwendungszweck) werden bei der Prüfung nicht betrachtet.

Für den Zugriff autorisiert als

root / admin / netadmin / audit / user

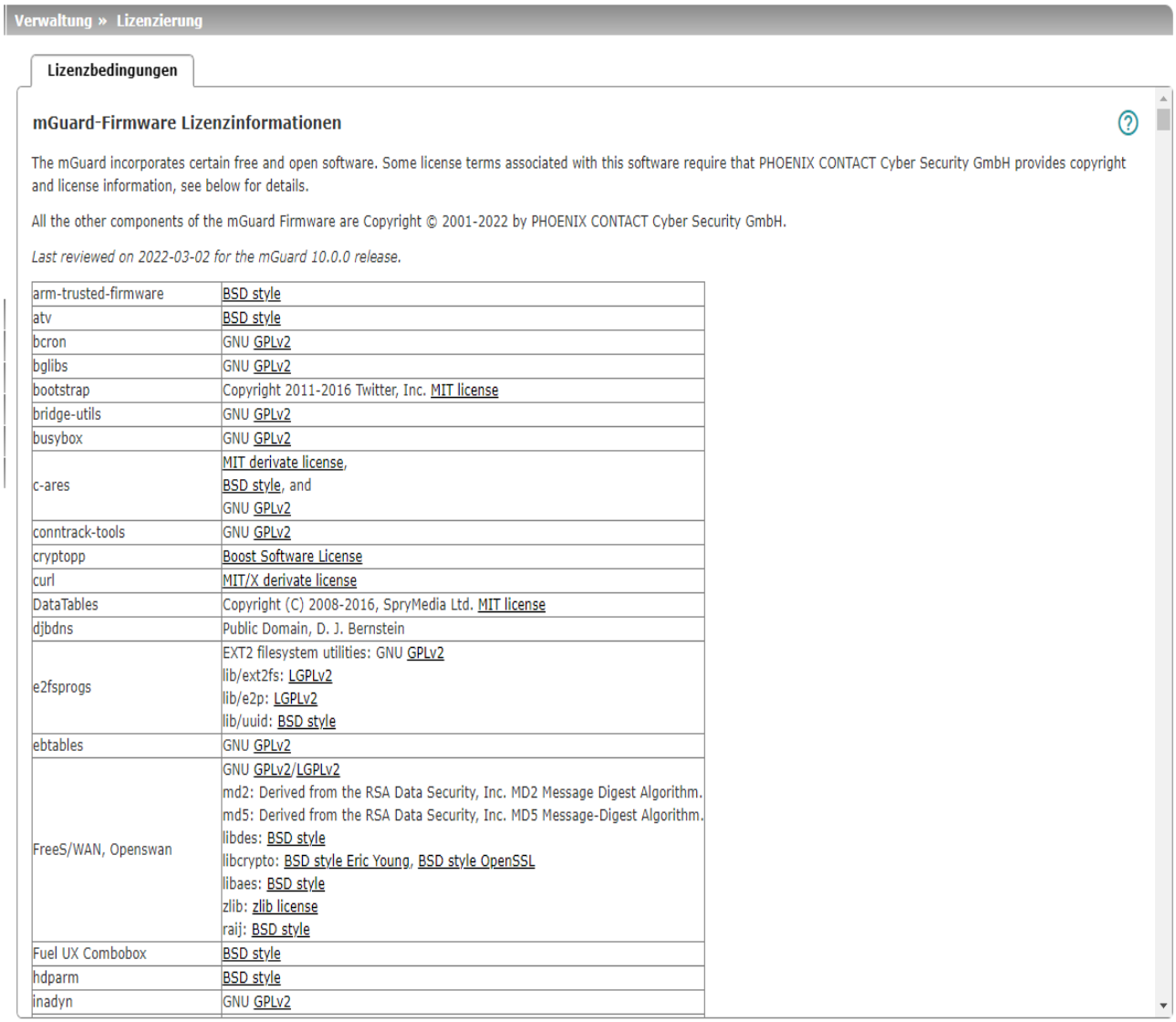
Legt fest, welche Nutzer- bzw. Administratorrechte dem aus der Ferne zugreifenden Bediener eingeräumt werden.

Für eine Beschreibung der Berechtigungsstufen *root, admin* und *user* siehe „Authentifizierung >> Administrative Benutzer“ auf Seite 181.

Die Berechtigungsstufen *netadmin* und *audit* beziehen sich auf Zugriffsrechte bei Zugriffen mit dem mGuard device manager (FL MGUARD DM UNLIMITED).

4.3 Verwaltung >> Lizenzbedingungen

Listet die Lizenzen der Fremd-Software auf, die im mGuard verwendet wird. Es handelt sich meistens um Open-Source-Software (für die jeweils aktuelle Liste siehe auch Anwenderhinweis AH DE MGUARD3 MG10 LICENSES „Lizenzinformationen - Freie und Open-Source-Software“ (verfügbar im PHOENIX CONTACT Web Shop z. B. unter phoenixcontact.com/product/1357828)).



arm-trusted-firmware	BSD style
atv	BSD style
bcron	GNU GPLv2
bglibs	GNU GPLv2
bootstrap	Copyright 2011-2016 Twitter, Inc. MIT license
bridge-utils	GNU GPLv2
busybox	GNU GPLv2
c-ares	MIT derivate license, BSD style, and GNU GPLv2
conntrack-tools	GNU GPLv2
cryptopp	Boost Software License
curl	MIT/X derivate license
DataTables	Copyright (C) 2008-2016, SpryMedia Ltd. MIT license
djbdns	Public Domain, D. J. Bernstein
e2fsprogs	EXT2 filesystem utilities: GNU GPLv2 lib/ext2fs: LGPLv2 lib/e2p: LGPLv2 lib/uuid: BSD style
ebtables	GNU GPLv2
FreeS/WAN, Openswan	GNU GPLv2/LGPLv2 md2: Derived from the RSA Data Security, Inc. MD2 Message Digest Algorithm. md5: Derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm. libdes: BSD style libcrypto: BSD style Eric Young, BSD style OpenSSL libaes: BSD style zlib: zlib license raij: BSD style
Fuel UX Combobox	BSD style
hdparm	BSD style
inadyn	GNU GPLv2

4.4 Verwaltung >> Update

Verwenden Sie die jeweils aktuelle Firmware-Version
Da mit jeder neuen Firmware-Version sicherheitsrelevante Verbesserungen in das Produkt eingefügt werden, sollte grundsätzlich immer auf die neueste Firmware-Version aktualisiert werden.
Phoenix Contact stellt regelmäßig Firmware-Updates zur Verfügung. Diese finden Sie auf der Produktseite des jeweiligen Geräts (z. B. phoenixcontact.com/product/1357840).

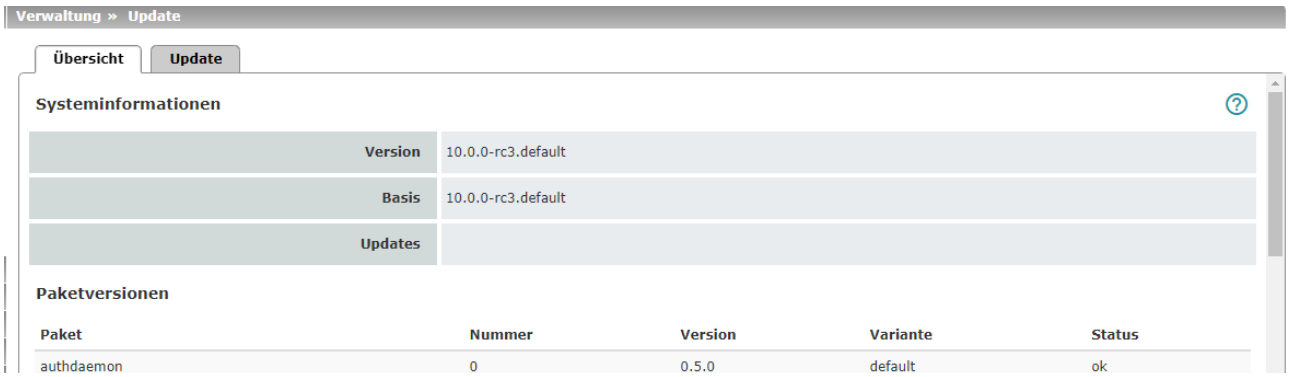
- Beachten Sie die Change Notes / Release Notes zur jeweiligen Firmware-Version.
- Beachten Sie die Webseite des Product Security Incident Response Teams (PSIRT) von Phoenix Contact für Sicherheitshinweise zu veröffentlichten Sicherheitslücken.

Um sicherzustellen, dass die heruntergeladene Firmware- oder Update-Datei während des Downloads nicht von Dritten verändert wurde, können Sie die SHA256-Prüfsumme der Datei mit der auf der entsprechenden Produktseite angegebenen Prüfsumme vergleichen (phoenixcontact.com/product/<Bestellnummer>).

Ein Update auf die aktuelle Firmware-Version ist von allen Firmware-Versionen ab mGuard 10.0.0 möglich. Ein Downgrade auf eine niedrigere Firmware-Version ist grundsätzlich nicht möglich.

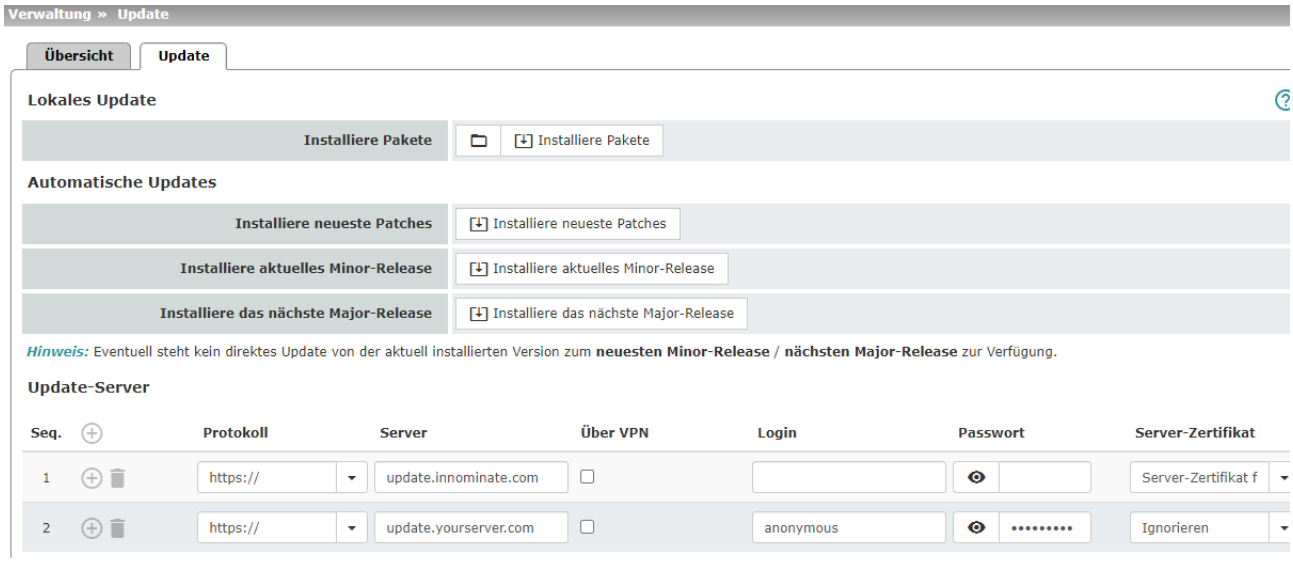
ACHTUNG: Eine Unterbrechung des Updates kann das Gerät beschädigen.
Schalten Sie das Gerät während des Update-Vorgangs nicht aus und unterbrechen Sie nicht die Stromversorgung des Geräts.

4.4.1 Übersicht



Verwaltung >> Update >> Übersicht		
Systeminformationen	Listet Informationen zur Firmware-Version des mGuards auf.	
	Version	Die aktuelle Software-Version des mGuard-Geräts.
	Basis	Die Version, mit der dieses Gerät ursprünglich geflasht wurde.
	Updates	Liste der Updates, die zur Basis hinzu installiert worden sind.
Paketversionen	Listet die einzelnen Software-Module des mGuards auf. Diese Informationen werden gegebenenfalls im Support-Fall benötigt.	

4.4.2 Update



Firmware-Updates bei eingeschalteter Firewall-Redundanz

ACHTUNG: Nur das jeweils inaktive Gerät eines Redundanzpaares kann upgedatet werden.

Vorgehen

- Updaten Sie immer zuerst das inaktive Gerät des Redundanzpaares.
  Dieses wird nach einem erfolgreichen Update automatisch zum aktiven Gerät.
- Starten Sie nun das Update für das andere, nun inaktive, Gerät.
- Prüfen Sie, ob beide Geräte erfolgreich upgedatet wurden.

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.

Verwaltung >> Update

Lokales Update

Installiere Pakete

Zur Installation von Paketen gehen Sie wie folgt vor:

- Das Icon **Keine Datei ausgewählt** klicken, die Datei selektieren und öffnen.

  Der Dateiname der Update-Datei ist abhängig von der Geräteplattform und der aktuell installierten Firmware-Version (siehe auch **Anwenderhinweis** AH DE MGUARD UPDATE „Update und Flash mGuard 8.9.3 und 10.5.0“).
- **Beispiel**: *update-10.{0-4}-10.5.0.default.aarch64.tar.gz*
- Klicken Sie dann die Schaltfläche **Installiere Pakete**.

Automatische Updates

Bei einem automatischen Update ermittelt das Gerät das benötigte Package-Set eigenständig.

Ein automatisches Update kann über die konfigurierten Update-Server auch auf der Kommandozeile gestartet werden (siehe „Kommandozeilen-Tool „mg““ auf Seite 374).

– Berechtigte Benutzer: *root* und *admin*

– Befehl: *mg update*, Parameter: *major* | *minor* | *patches* .

Die erfolgreiche Durchführung oder auftretende Fehler werden im Logfile dokumentiert: */var/log/psm-sanitize* .

Installiere neueste Patches

Patch-Releases beheben Fehler der vorherigen Versionen und haben eine Versionsnummer, welche sich nur in der dritten Stelle ändern. Die Version 10.0.**1** ist z. B. ein Patch-Release zur Version 10.0.**0**.

Installiere aktuelles Minor-Release

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. Die Version 10.**1.0** ist z. B. ein Minor-Release zur Version 10.**0.1**.

Installiere das nächste Major-Release

Die Version **11**.0.0 ist z. B. ein Major-Release zur Version **10**.1.0.

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.

Die Login-Informationen (Login + Passwort) müssen nicht angegeben werden, wenn der werkseitig voreingestellte Update-Server (https://update.innominate.com) verwendet wird.

Bei den Angaben haben Sie folgende Möglichkeiten:

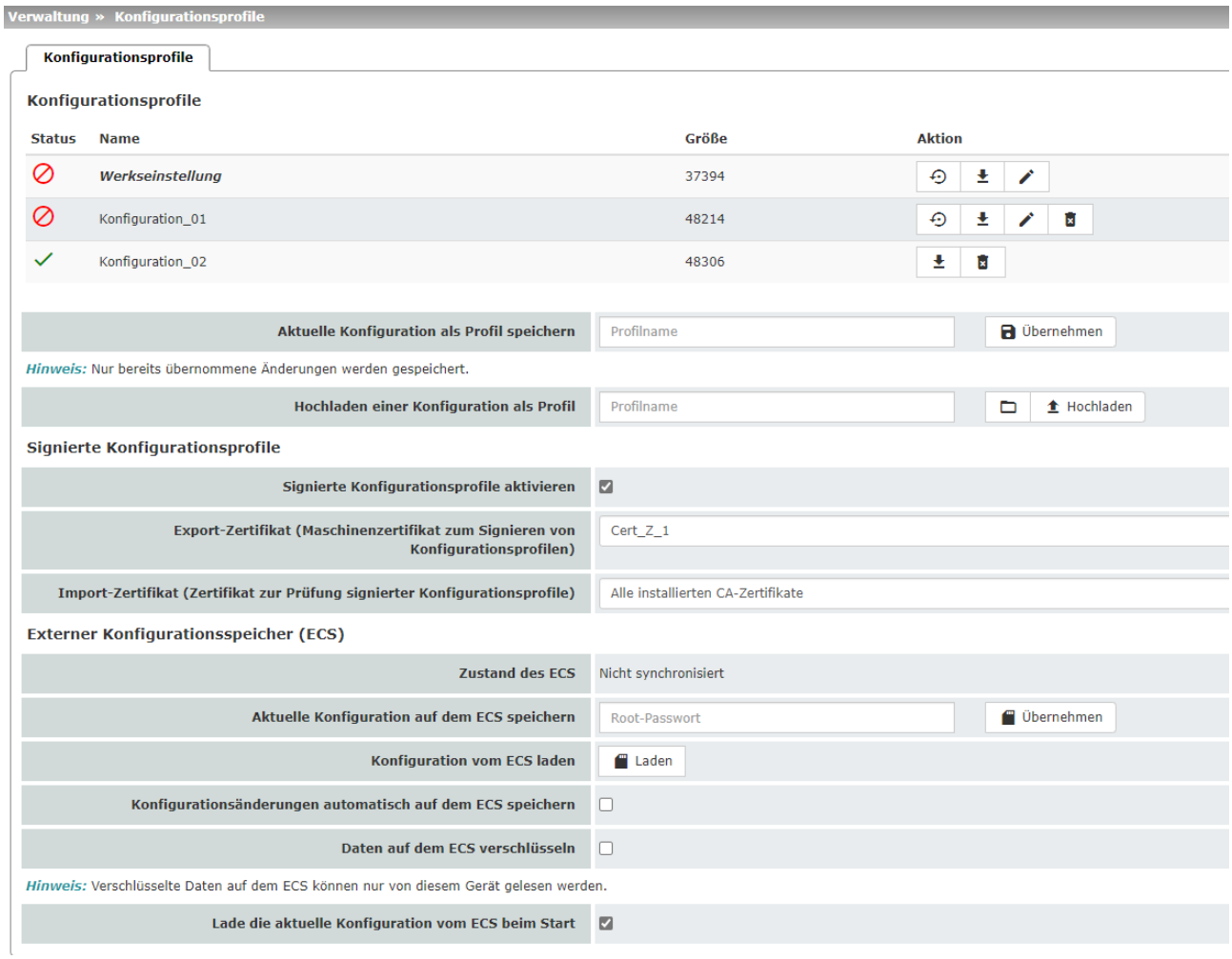
Protokoll

Das Update kann per HTTPS, HTTP, FTP oder TFTP erfolgen.

Verwaltung >> Update [...]	
Server	Hostname oder IP-Adresse des Servers, der die Update-Dateien bereitstellt.
Über VPN	Die Anfrage des Update-Servers wird, wenn möglich, über einen VPN-Tunnel durchgeführt. Bei aktivierter Funktion wird die Kommunikation mit dem Server immer dann über einen verschlüsselten VPN-Tunnel geführt, wenn ein passender VPN-Tunnel verfügbar ist. Bei deaktivierter Funktion oder wenn kein passender VPN-Tunnel verfügbar ist, wird der Verkehr **unverschlüsselt über das Standard-Gateway** gesendet. Voraussetzung für die Verwendung der Funktion ist die Verfügbarkeit eines passenden VPN-Tunnels. Das ist der Fall, wenn der angefragte 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.
Login	Login für den Server.
Passwort	Passwort für den Login.
Server-Zertifikat	Um sicherzustellen, dass eine sichere HTTPS-Verbindung zum konfigurierten Update-Server aufgebaut wird, muss das entsprechende Server-Zertifikat des Update-Servers vom mGuard-Gerät geprüft werden. Die Authentifizierung des Update-Servers erfolgt dabei entweder über ein entsprechendes Gegenstellen-Zertifikat oder über ein CA-Zertifikat. Das Zertifikat muss auf das mGuard-Gerät hochgeladen werden, damit es zur Prüfung des Server-Zertifikats in der Drop-Down-Liste ausgewählt werde kann (siehe Kapitel 6.4.4, „Gegenstellen-Zertifikate“ und Kapitel 6.4.3, „CA-Zertifikate“). Wird die Option „Ignorieren“ ausgewählt. findet keine Prüfung statt.

4.5 Verwaltung >> Konfigurationsprofile

4.5.1 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.

Konfigurationsprofile können mithilfe von Zertifikaten digital signiert werden. Auf entsprechend konfigurierten Geräten ist es dann nur noch möglich, Konfigurationsprofile, die mit entsprechenden Zertifikaten signiert wurden, auf das Gerät hochzuladen.

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

Konfigurationsprofile können auf einer SD-Karte als externem Konfigurationsspeicher (ECS) abgelegt werden.

Beim Abspeichern eines Konfigurationsprofils werden die Passwörter, die zur Authentifizierung des administrativen Zugriffs auf den mGuard dienen (Root-Passwort, Admin-Passwort, SNMPv3-Passwort), 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 und wird zurückgewiesen.

Verschlüsselte Konfigurationsspeicher (ECS)

Konfigurationsprofile, die auf einem ECS abgespeichert werden, können verschlüsselt und damit für jedes Gerät individuell zuordenbar gemacht werden. Damit wird der Rollout erleichtert.

Sie können mehrere mGuard-Konfigurationen auf einer SD-Karte abspeichern und anschließend zur Inbetriebnahme aller mGuards verwenden. Beim Startvorgang findet der mGuard die für ihn gültige Konfiguration auf der SD-Karte. Diese wird geladen, entschlüsselt und als gültige Konfiguration verwendet (siehe „Daten auf dem ECS verschlüsseln“ auf Seite 105.)

Recovery-Prozedur

Vor der Durchführung einer Recovery-Prozedur wird die aktuelle Konfiguration des Geräts in einem neuen Konfigurationsprofil gespeichert („Recovery-DATUM“). Das Gerät startet nach der Recovery-Prozedur mit den werkseitigen Voreinstellungen.

Das Konfigurationsprofil mit der Bezeichnung „Recovery-DATUM“) erscheint nach der Recovery-Prozedur in der Liste der Konfigurationsprofile und kann mit oder ohne Änderungen wiederhergestellt 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.

Beachten Sie, dass es sich bei den Konfigurationsprofilen sowohl um unsignierte als auch signierte Profile handeln kann (siehe „Signierte Konfigurationsprofile“).

Aktives Konfigurationsprofil: Das Konfigurationsprofil, das zurzeit in Kraft ist, hat vorne im Eintrag das *Active*-Symbol. Wird eine Konfiguration so geändert, dass sie einem gespeicherten Konfigurationsprofil entspricht, erhält dieses das *Active*-Symbol, nachdem die Änderungen übernommen wurden.

Sie können Konfigurationsprofile, die im mGuard gespeichert sind:

– in Kraft setzen (Profil wiederherstellen)
– als atv-Datei auf dem angeschlossenen Konfigurationsrechner herunterladen
– ansehen und bearbeiten (Profil bearbeiten)
– löschen

Konfigurationsprofil als atv-Datei herunterladen

- In der Liste den Namen des Konfigurationsprofils anklicken.
  Das Konfigurationsprofil wird als atv-Datei heruntergeladen und kann mit einem Text-Editor analysiert werden.

Beachten Sie, dass es sich bei den Konfigurationsprofilen sowohl um unsignierte als auch signierte Profile handeln kann (siehe „Signierte Konfigurationsprofile“).

Verwaltung >> Konfigurationsprofile [...]

Konfigurationsprofil vor der Wiederherstellung ansehen und bearbeiten (Profil bearbeiten)

- Rechts neben dem Namen des betreffenden Konfigurationsprofils auf das Icon **Profil bearbeiten** klicken.

  Das Konfigurationsprofil wird geladen aber noch nicht aktiviert. Alle Einträge, die Änderungen zur aktuell verwendeten Konfiguration aufweisen, werden innerhalb der relevanten Seite und im zugehörigen Menüpfad grün markiert. Die angezeigten Änderungen können unverändert oder mit weiteren Änderungen übernommen oder verworfen werden:
  - Um die Einträge des geladenen Profils (gegebenenfalls mit weiteren Änderungen) zu übernehmen, klicken Sie auf das Icon **Übernehmen**.
  - Um alle Änderungen zu verwerfen, klicken Sie auf das Icon **Zurücksetzen**.

Die Werkseinstellung oder ein vom Benutzer im mGuard gespeichertes Konfigurationsprofil in Kraft setzen (Profil wiederherstellen)

- Rechts neben dem Namen des betreffenden Konfigurationsprofils auf das Icon **Profil wiederherstellen** klicken.

  Das betreffende Konfigurationsprofil wird ohne Rückfrage wiederhergestellt und sofort aktiviert.

Konfigurationsprofil als Datei auf dem Konfigurationsrechner speichern

- Rechts neben dem Namen des betreffenden Konfigurationsprofils auf das Icon **Profil herunterladen** klicken.
- Legen Sie gegebenenfalls im angezeigten Dialogfeld den Dateinamen und Speicherort fest, unter dem das Konfigurationsprofil als Datei gespeichert werden soll. (Sie können die Datei beliebig benennen.)

Beachten Sie, dass es sich bei den Konfigurationsprofilen sowohl um unsignierte als auch signierte Profile handeln kann (siehe „Signierte Konfigurationsprofile“).

Konfigurationsprofil löschen

- Rechts neben dem Namen des betreffenden Konfigurationsprofils auf das Icon **Profil löschen** klicken.

Das Profil wird ohne Rückfrage unwiderruflich gelöscht.

Das Profil *Werkseinstellung* kann nicht gelöscht werden.

Aktuelle Konfiguration als Profil speichern

Aktuelle Konfiguration als Profil im mGuard speichern

- Hinter „Aktuelle Konfiguration als Profil speichern“ in das Feld *Profilname* den gewünschten Profilnamen eintragen.
- Auf die Schaltfläche **Übernehmen** klicken.

Das Konfigurationsprofil wird im mGuard gespeichert. Der Name des Profils wird in der Liste der im mGuard gespeicherten Konfigurationsprofile angezeigt.

Beachten Sie, dass es sich bei den Konfigurationsprofilen sowohl um unsignierte als auch signierte Profile handeln kann (siehe „Signierte Konfigurationsprofile“).

Verwaltung >> Konfigurationsprofile [...]

Hochladen einer Konfiguration als Profil

Hochladen eines Konfigurationsprofils, das auf dem Konfigurationsrechner in einer Datei gespeichert ist

Voraussetzung: Sie haben nach dem oben beschriebenem Verfahren ein Konfigurationsprofil als Datei auf dem Konfigurationsrechners gespeichert.

- Hinter „**Hochladen einer Konfiguration als Profil**“ in das Feld *Profilname* den gewünschten Profilnamen eintragen, der angezeigt werden soll.
- Auf das Icon **Keine Datei ausgewählt** 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 gespeicherten Profile angezeigt.

Beachten Sie, dass es sich bei den Konfigurationsprofilen sowohl um unsignierte als auch signierte Profile handeln kann (siehe „Signierte Konfigurationsprofile“).

Wenn die Funktion „Signierte Konfigurationsprofile aktivieren“ aktiviert ist, können nur signierte Konfigurationsprofile auf das Gerät hochgeladen werden. Zusätzlich müssen ein oder mehrere geeignete Zertifikate vorhanden sein, um die Signatur des Konfigurationsprofils zu verifizieren.

Konfigurationsprofile mit eigentlich identischen Einstellungen können sich aus technischen Gründen geringfügig in ihrer Größe (Bytes) unterscheiden.

Das Verhalten tritt auf, wenn bestimmte Einträge, z. B. Datumsangaben, Kommentare, Berechtigungen oder Firmware-Versionen bei der Erstellung/Anwendung des Profils, voneinander abweichen.

Signierte Konfigurationsprofile

Konfigurationsprofile können mithilfe von Zertifikaten signiert werden. Auf entsprechend konfigurierten Geräten ist es dann nur noch möglich, Konfigurationsprofile, die mit gültigen Zertifikaten signiert wurden, auf das Gerät hochzuladen.

Es wird nicht geprüft, ob das Ablaufdatum eines Zertifikats überschritten oder ein verwendetes Zertifikat zurückgezogen wurde („CRL“-Prüfung).

Wenn kein selbstsigniertes Zertifikat für die Signatur des Profils verwendet wird, müssen auf dem mGuard-Gerät neben dem entsprechenden Root-CA-Zertifikat auch alle Zwischenzertifikate als „CA-Zertifikate“ installiert sein (siehe Kapitel 6.4.3). Es müssen also alle notwendigen CA-Zrtifikate verfügbar gemacht werden, um mit dem vorgezeigten Zertifikat eine Kette des Vertrauens (*chain of trust*) zu bilden.

Um Konfigurationsprofile manuell zu signieren, siehe Dokument 111259_de_xx (AH DE MGUARD MIGRATE 10) , erhältlich unter phoenixcontact.com/product/1357875.

Verwaltung >> Konfigurationsprofile [...]

Signierte Konfigurationsprofile aktivieren	Ist diese Funktion aktiviert, – werden Konfigurationen, die als Konfigurationsprofil (**atv-Datei**) oder auf einem externen Konfigurationsspeicher (**ECS**) gespeichert werden, mittels X.509-Zertifikat signiert, – können nur signierte Konfigurationen auf das Gerät hochgeladen werden. Die entsprechenden Zertifikate müssen vor der Verwendung der Funktion auf das mGuard-Gerät hochgeladen werden (siehe Kapitel 6.4). Zum Signieren einer Konfiguration muss ein Maschinenzertifikat verwendet werden (siehe Kapitel 6.4.2). Zum Prüfen einer hochgeladenen Konfiguration kann entweder das gleiche Maschinenzertifikat oder ein oder mehrere CA-Zertifikate verwendet werden. Werden CA-Zertifikat verwendet, muss das Maschinenzertifikat, mit dem die Konfiguration signiert wurde, mit dem CA-Zertifikat signiert worden sein und somit mit diesem eine Kette des Vertrauens bilden (siehe Kapitel 6.4.3 und „CA-Zertifikat“). Bei deaktivierter Funktion ist es möglich, unsignierte und signierte Konfigurationen hochzuladen, ohne dass deren Signatur überprüft wird. Damit ist es weiterhin möglich, unsignierte Konfigurationsprofile auf dem Gerät zu verwenden.
Export-Zertifikat (Maschinenzertifikat zum Signieren von Konfigurationsprofilen)	**Kein / <Maschinenzertifikat>** Die Konfiguration wird mittels Maschinenzertifikat signiert. Das oder die Zertifikate müssen zunächst auf das mGuard-Gerät hochgeladen werden, damit sie in der Drop-Down-Liste ausgewählt werde können (siehe Kapitel 6.4.2).
Import-Zertifikat (Zertifikat zur Prüfung signierter Konfigurationsprofile)	**Kein / Alle installierten CA-Zertifikate / <Maschinenzertifikat> / <CA-Zertifikat>** Die Authentizität der hochgeladenen Konfiguration wird mittels Maschinenzertifikat oder CA-Zertifikat geprüft. **Maschinenzertifikat**: Zur Prüfung muss das gleiche Maschinenzertifikat ausgewählt werden, mit dem die Konfiguration signiert wurde. **CA-Zertifikat**: Zur Prüfung muss mindestens ein CA-Zertifikat ausgewählt werden, das mit dem signierenden Maschinenzertifikat eine Kette des Vertrauens bildet. Es können auch alle installierten CA-Zertifikate ausgewählt werden. Das oder die Zertifikate müssen zunächst auf das mGuard-Gerät hochgeladen werden, damit sie in der Drop-Down-Liste ausgewählt werde können (siehe Kapitel 6.4.2 und Kapitel 6.4.3).

Verwaltung >> Konfigurationsprofile [...]

Externer Konfigurations-speicher (ECS)

Auf dem mGuard abgespeicherte Konfigurationsprofile können auf eine SD-Karte als externem Konfigurationsspeicher (ECS) exportiert und von dieser erneut in mGuard-Geräte importiert werden.

Name der exportierten Datei: *ECS.tgz*

Technische Voraussetzung von SD-Karten:

– FAT-kompatibles Dateisystem auf der ersten Partition.

Zertifizierte und freigegebene SD-Karten durch Phoenix Contact: siehe Bereich „Zubehör“ auf den Produktseiten unter: phoenixcontact.com/products

Um die Datei in ein mGuard-Gerät zu importieren, muss die SD-Karte in den mGuard eingelegt werden.

Die Konfiguration kann

– beim Starten des Geräts automatisch geladen, entschlüsselt und als aktive Konfiguration verwendet oder
– über die Web-Oberfläche geladen und aktiviert werden.

Die Konfiguration auf dem externen Speichermedium enthält auch die verschlüsselten Passwörter (gehasht) für die Benutzer *root*, *admin*, *netadmin*, *audit* und *user* sowie für den SNMPv3-Benutzer. Diese werden beim Laden vom externen Speichermedium ebenfalls übernommen.

Zustand des ECS

Der aktuelle Zustand wird dynamisch aktualisiert. (Siehe „Zustand des ECS“ in „Ereignistabelle“ auf Seite 72).

Aktuelle Konfiguration auf dem ECS speichern

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 **„Root-Passwort“** eingegeben werden. Übernehmen Sie die Eingabe mit einem Klick auf die Schaltfläche **Übernehmen**.

Komplexe Konfigurationen z. B. mit einer großen Anzahl konfigurierter Firewall-Regeln und/oder VPN-Verbindungen können zu großen Konfigurationsprofilen führen.

Ist die Funktion „Signierte Konfigurationsprofile aktivieren“ aktiviert, wird die Konfiguration auf dem ECS mit dem ausgewählten Maschinenzertifikat signiert.

Verwaltung >> Konfigurationsprofile [...]

Konfiguration vom ECS laden

Befindet sich ein Konfigurationsprofil auf einem eingelegten bzw. angeschlossenen ECS-Speichermedium, wird dieses nach einem Klick auf die Schaltfläche **Laden** in den mGuard importiert und dort als aktives Profil in Kraft gesetzt.

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

Ist die Funktion „Signierte Konfigurationsprofile aktivieren“ aktiviert, können nur solche Konfigurationen vom ECS geladen werden, die mit einem gültigen Zertifikat signiert wurden.

Konfigurationsänderungen automatisch auf dem ECS speichern

Bei aktivierter Funktion werden die Konfigurationsänderungen automatisch auf einem ECS gespeichert, so dass auf dem ECS stets das aktuell verwendete Profil gespeichert ist.

ACHTUNG: Speichern Sie keine weiteren Konfigurationsänderungen, wenn das Abspeichern der letzten Konfigurationsänderung auf dem ECS noch nicht erfolgreich beendet wurde.

Weitere Konfigurationsänderungen, die während eines laufenden Schreibvorgangs durchgeführt und übernommen werden, werden dann nicht automatisch auf dem ECS gespeichert.

Sie könnten verloren gehen, wenn eine „alte“ Konfiguration bei einem Neustart des Geräts vom ECS geladen wird.

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.

Ist die Funktion „Signierte Konfigurationsprofile aktivieren“ aktiviert, wird die Konfiguration auf dem ECS mit dem ausgewählten Maschinenzertifikat automatisch signiert.

Es können dann nur solche Konfigurationen vom ECS geladen werden, die mit einem gültigen Zertifikat signiert wurden.

Auch wenn der ECS nicht angeschlossen, voll oder defekt ist, werden Konfigurationsänderungen ausgeführt. Entsprechende Fehlermeldungen erscheinen im Logging (siehe „Logging >> Logs ansehen“ auf Seite 338).

Die Aktivierung der neuen Einstellung verlängert die Reaktionszeit der Bedienoberfläche, wenn Einstellungen geändert werden.

Verwaltung >> Konfigurationsprofile [...]

Daten auf dem ECS verschlüsseln	Bei aktivierter Funktion werden die Konfigurationsänderungen verschlüsselt auf einem ECS abgespeichert. Damit wird der Rollout von mGuards erleichtert. Sie können mehrere mGuard-Konfigurationen auf einer SD-Karte abspeichern und anschließend zur Inbetriebnahme aller mGuards verwenden. Beim Startvorgang findet der mGuard die für ihn gültige Konfiguration auf dem Konfigurationsspeicher. Diese wird geladen, entschlüsselt und als gültige Konfiguration verwendet.
Lade die aktuelle Konfiguration vom ECS beim Start	Bei aktivierter Funktion wird beim Booten des mGuards auf den ECS zugegriffen. Das Konfigurationsprofil wird vom ECS in den mGuard geladen, gegebenenfalls entschlüsselt und als gültige Konfiguration verwendet. Ist die Funktion „Signierte Konfigurationsprofile aktivieren“ aktiviert, können nur solche Konfigurationen vom ECS geladen werden, die mit einem gültigen Zertifikat signiert wurden. Das geladene Konfigurationsprofil erscheint nicht automatisch in der Liste der im mGuard gespeicherten Konfigurationsprofile.

4.6 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.

Im Gegensatz zum Protokoll SNMPv3 unterstützen die älteren Versionen SNMPv1/SNMPv2 keine Authentifizierung und keine Verschlüsselung und gelten daher als nicht sicher. Das SNMPv1/2-Protokoll sollte nur in einer sicheren Netzwerkumgebung verwendet werden, die gänzlich unter Kontrolle des Betreibers steht.

SNMPv3 wird allerdings nicht von allen Management-Konsolen unterstützt.

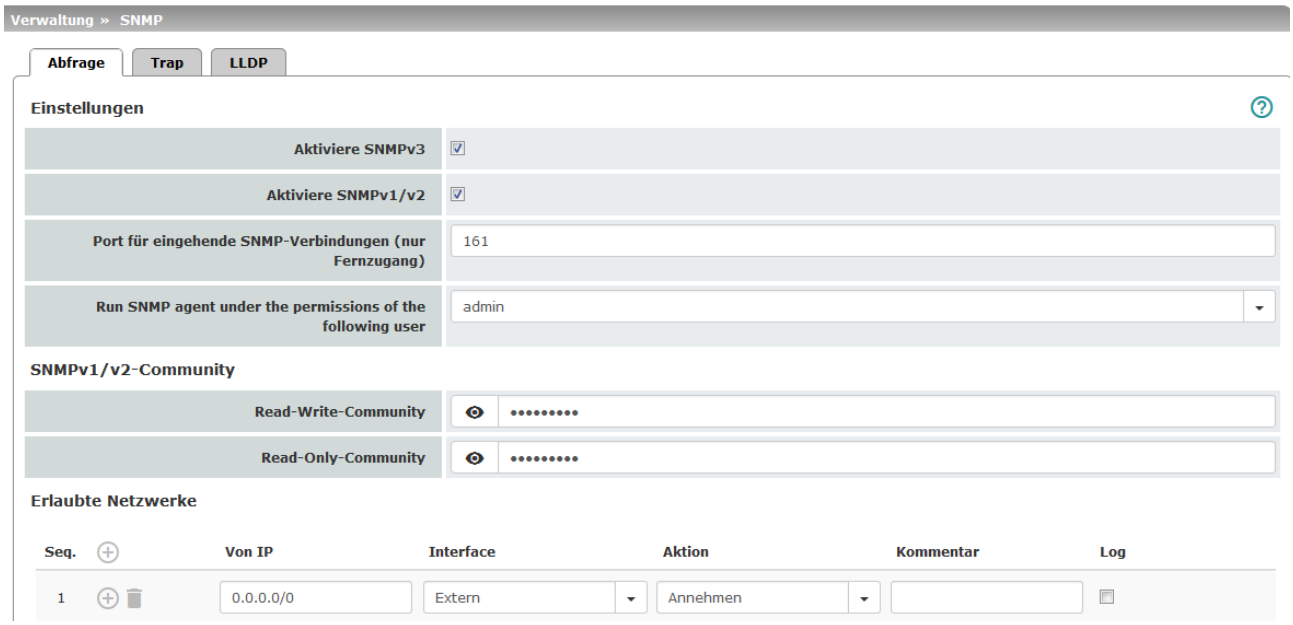
Das SNMP (Simple Network Management Protocol) wird vorzugsweise in komplexeren Netzwerken benutzt, um den Zustand und den Betrieb von Geräten zu überwachen oder zu konfigurieren.

Es ist ebenfalls möglich, auf dem mGuard Aktionen (*Actions*) über das SNMP-Protokoll auszuführen. Eine Dokumentation der ausführbaren Aktionen ist über die entsprechende MIB-Datei verfügbar.

MIB-Datei

Um den mGuard per SNMP-Client über das SNMP-Protokoll zu konfigurieren, zu überwachen oder zu steuern, muss die entsprechende MIB-Datei in den SNMP-Client importiert werden. MIB-Dateien werden in einer verpackten ZIP-Datei zusammen mit der Firmware bzw. Firmware-Updates zur Verfügung gestellt. Sie können auf der Webseite des Herstellers über die entsprechenden Produktseiten heruntergeladen werden: phoenixcontact.com/products.

4.6.1 Abfrage



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

Aktivieren Sie die Funktion, wenn Sie zulassen wollen, dass der mGuard per SNMPv3 überwacht werden kann.

Nach Aktivierung der Funktion ist der Zugriff über *Intern* und *VPN* möglich.

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 Benutzername und Passwort notwendig. Die werkseitige Voreinstellung für die Zugangsdaten lautet:

Benutzername: admin

Passwort: SnmpAdmin

(Bitte beachten Sie die Groß-/Kleinschreibung!)

Die SNMPv3-Zugangsdaten **Benutzername** und **Passwort** können über die Web-Oberfläche, eine ECS-Konfiguration oder ein Rollout-Script geändert werden.

Das Verwalten von SNMPv3-Benutzern über SNMPv3 USM ist nicht möglich.

Der geänderte Benutzername und das geänderte Passwort können auf einem **ECS** gespeichert und von dort wiederhergestellt werden.

Wird die aktuelle Konfiguration in einem **ATV-Konfigurationsprofil** gespeichert, wird nur der SNMPv3-Benutzername und **nicht** das Passwort in das Konfigurationsprofil übernommen.

Eine Aktivierung des Profils ändert das aktuell auf dem mGuard bestehende SNMPv3-Passwort nicht.

Das Hinzufügen zusätzlicher SNMPv3-Benutzer wird aktuell nicht unterstützt.

Für die Authentifizierung wird MD5 verwendet, für die Verschlüsselung DES.

Verwaltung >> SNMP >> Abfrage [...]		
	Aktiviere SNMPv1/v2	Aktivieren Sie die Funktion, wenn Sie zulassen wollen, dass der mGuard per SNMPv1/v2 überwacht werden kann. Zusätzlich müssen Sie unter **SNMPv1/v2-Community** die Login-Daten angeben. Nach Aktivierung der Funktion ist der Zugriff über *Intern* und *VPN* möglich. 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, DMZ* und *VPN*. Für internen Zugriff gilt weiterhin 161. Im Stealth-Modus wird eingehender Verkehr auf dem angegebenen Port nicht mehr zum Client weitergeleitet. Im Router-Modus mit NAT bzw. Port-Weiterleitung hat die hier eingestellte Portnummer Priorität gegenüber Regeln zur Port-Weiterleitung. Die entfernte Gegenstelle, die den Fernzugriff ausübt, muss bei der Adressenangabe gegebenenfalls die Port-Nummer angeben, die hier festgelegt ist.
	Führe den SNMP-Agent mit den Rechten des folgenden Benutzers aus	**admin / netadmin** Legt fest, mit welchen Rechten der SNMP-Agent ausgeführt wird.
SNMPv3-Zugangsdaten	**Benutzername**	Ändert den aktuell vergebenen SNMPv3-Benutzernamen.
	Passwort	Ändert das aktuell vergebene SNMPv3-Passwort. Das Passwort kann nur geschrieben und nicht ausgelesen werden (*write-only*). Der geänderte Benutzername und das geänderte Passwort können in einer **ECS-Datei** gespeichert und von dort wiederhergestellt werden. Wird die aktuelle Konfiguration in einem **ATV-Konfigurationsprofil** gespeichert, wird nur der SNMPv3-Benutzername und **nicht** das Passwort in das Konfigurationsprofil übernommen. Eine Aktivierung des Profils ändert das aktuell auf dem mGuard bestehende SNMPv3-Passwort nicht.

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

SNMPv1/v2-Community

Read-Write-Community Geben Sie in diese Felder die erforderlichen Login-Daten ein.

Read-Only-Community 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.

ACHTUNG: Zugriff auf das Gerät über externe Netze möglich.
Die Server-Dienste des Geräts sind je nach Einstellung über externe Netze und möglicherweise aus dem Internet erreichbar. Stellen Sie sicher, dass der Zugriff nur erfolgen kann, wenn er erwünscht ist. Konfigurieren Sie andernfalls Ihr Netzwerk entsprechend, um einen Zugriff zu verhindern.

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

– SNMP-Zugriffe über *Intern* und *VPN* sind erlaubt.
– SNMP-Zugriffe über *Extern* und *DMZ* werden verwehrt.

Legen Sie die Überwachungsmöglichkeiten nach Bedarf fest.

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

Die hier angegebenen Regeln treten nur in Kraft, wenn die Funktion **Aktiviere SNMPv3** oder **Aktiviere SNMPv1/v2** aktiviert ist.

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.

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

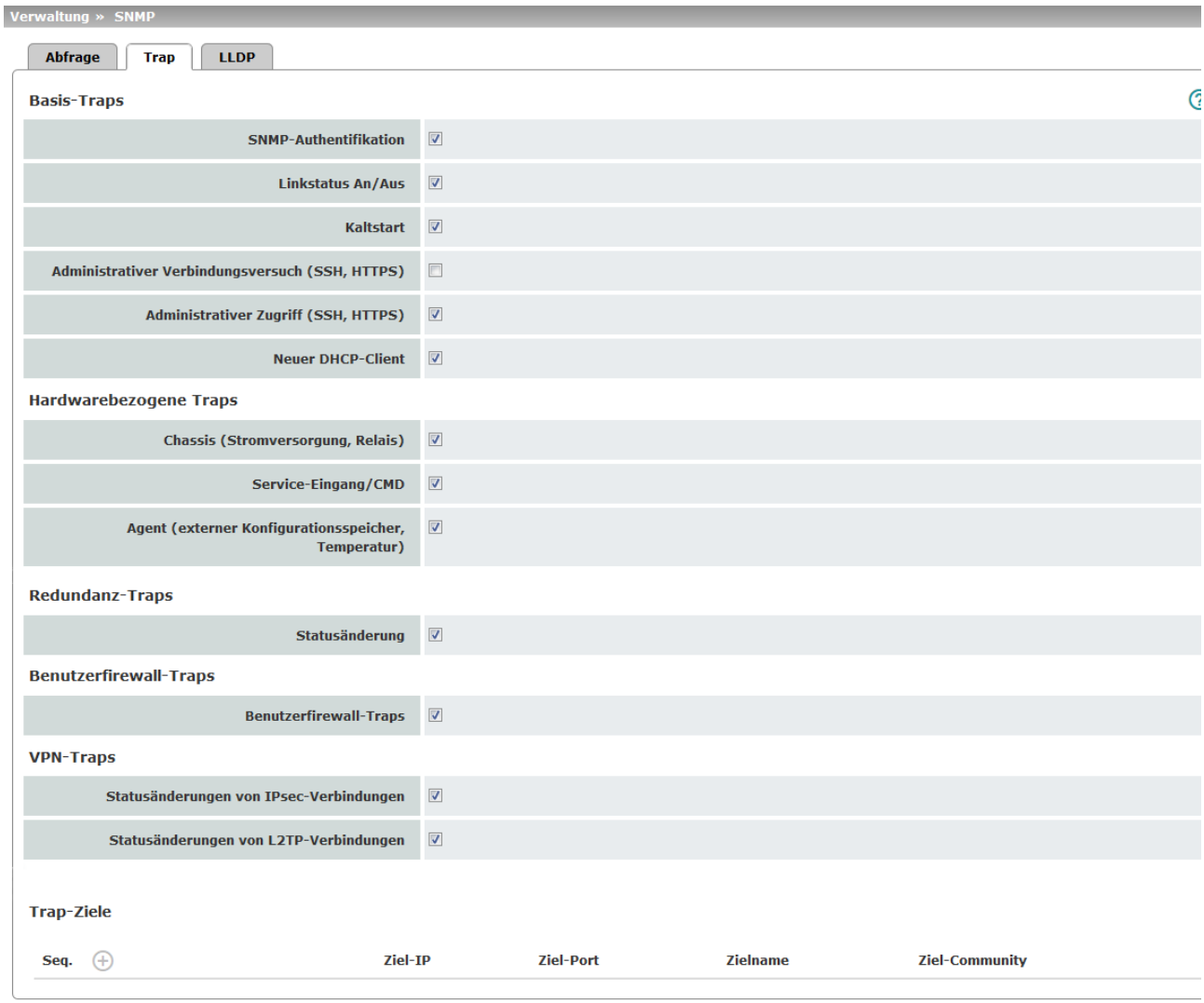
Bei den Angaben haben Sie folgende Möglichkeiten:

– Eine IP-Adresse.
– Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise (siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 43).
– **0.0.0.0/0** bedeutet alle Adressen.

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

Interface	**Intern / Extern / DMZ / VPN** Gibt an, für welches Interface die Regel gelten soll. Sind keine Regeln gesetzt oder greift keine Regel, gelten folgende Standardeinstellungen: – SNMP-Zugriffe über *Intern* und *VPN* sind erlaubt. – SNMP-Zugriffe über *Extern* und *DMZ* werden verwehrt. Legen Sie die Überwachungsmöglichkeiten nach Bedarf fest. **ACHTUNG:** Wenn Sie Zugriffe über *Intern* oder *VPN* verwehren wollen, müssen Sie das explizit durch entsprechende Firewall-Regeln bewirken, in denen Sie als Aktion z. B. *Verwerfen* festlegen.
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 – Funktion *Log* aktivieren oder – das Ereignis nicht protokolliert werden soll – Funktion *Log* deaktivieren (Standard). Log-Meldung (Beispiel): 2024-11-25_10:09:51.83909 firewall: fw-snpm-access-1-12e7d62f-6be7-1c6e-b8a6-000cbe00105c act=REJECT IN=eth0 MAC=d4:aa:62:b2:6d:62 SRC=192.168.1.55 DST=192.168.1.55 LEN=52 TOS=0x00 PREC=0x00 TTL=128 ID=47714 DF PROTO=TCP SPT=53379 DPT=22 SEQ=506303301 ACK=0 WINDOW=64240 SYN URGP=0 CTMARK=100030

4.6.2 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-Tunnel zur Gegenstelle gesendet, dann muss sich die IP-Adresse der Gegenstelle in dem Netzwerk befinden, das in der Definition der VPN-Verbindung als **Gegenstelle**n-Netzwerk angegeben ist.

Und die interne IP-Adresse muss sich in dem Netzwerk befinden, das in der Definition der VPN-Verbindung als **Lokal** angegeben ist (siehe „IPsec VPN >> Verbindungen >> Editieren >> Allgemein“).

– Wenn dabei die Option „IPsec VPN >> Verbindungen >> Editieren >> Allgemein“, **Lokal** auf **1:1-NAT** gestellt (siehe Seite 277), gilt Folgendes:

  Die interne IP-Adresse muss sich in dem angegebenen lokalen Netzwerk befinden.

– Wenn dabei die Option „IPsec VPN >> Verbindungen >> Editieren >> Allgemein“, **Gegenstelle** auf **1:1-NAT** gestellt (siehe Seite 278), gilt Folgendes:

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

Verwaltung >> SNMP >> Trap		
Basis-Traps	**SNMP-Authentifikation**	**Trap-Beschreibung** – enterprise-oid : mGuardInfo – generic-trap : authenticationFailure – specific-trap : 0 Wird gesendet, falls eine Station versucht, unberechtigt auf den SNMP-Agenten des mGuards zuzugreifen.
	Linkstatus An/Aus	**Trap-Beschreibung** – 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	**Trap-Beschreibung** – enterprise-oid : mGuardInfo – generic-trap : coldStart – specific-trap : 0 Wird gesendet nach Kalt- oder Warmstart.
	Administrativer Verbindungsversuch (SSH, HTTPS)	Trap-Beschreibung – enterprise-oid : mGuard – generic-trap : enterpriseSpecific – specific-trap : mGuardHTTPSLoginTrap (1) – additional : mGuardHTTPSLastAccessIP 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 Wird gesendet, wenn jemand die Shell per SSH öffnet. Der Trap enthält die IP-Adresse der Login-Anfrage.

Verwaltung >> SNMP >> Trap [...]		
	Administrativer Zugriff (SSH, HTTPS)	Trap-Beschreibung – enterprise-oid : mGuard – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapSSHLogin – additional : mGuardTResSSHUsername mGuardTResSSHRemoteIP Wird gesendet, wenn jemand per SSH auf den mGuard zugreift. – enterprise-oid : mGuard – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapSSHLogout – additional : mGuardTResSSHUsername mGuardTResSSHRemoteIP Wird gesendet, wenn ein Zugriff per SSH auf den mGuard beendet wird.
	Neuer DHCP-Client	Trap-Beschreibung – enterprise-oid : mGuard – generic-trap : enterpriseSpecific – specific-trap : 3 – additional : mGuardDHCPLastAccessMAC Wird gesendet, wenn eine DHCP-Anfrage von einem unbekannten Client eingegangen ist.
Hardwarebezogene Traps	**Chassis (Stromversorgung, Relais)**	Trap-Beschreibung – 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 [...]		
	Service-Eingang/CMD (Alternative Bezeichnung für den Service-Eingang: „**I**“.)	Trap-Beschreibung – enterprise-oid : mGuardTrapCMD – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapCMDStateChange (1) – additional : mGuardCMDState Wird gesendet, wenn ein Service-Eingang/CMD durch einen Schalter oder Taster geschaltet wird. Bei jedem Schaltvorgang (Ein/Aus) wird ein Trap gesendet.
	Agent (externer Konfigurationsspeicher, Temperatur)	Trap-Beschreibung – enterprise-oid : mGuardTrapIndustrial – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapIndustrialTemperature (1) – additional : mGuardSystemTemperature, mGuardTrapIndustrialTempHiLimit, mGuardTrapIndustrialLowLimit Wird gesendet bei Überschreitung der festgelegten Grenzwerte und gibt die Temperatur an. – enterprise-oid : mGuardTrapIndustrial – genericTrap : enterpriseSpecific – specific-trap : mGuardTrapAutoConfigAdapterState (4) – additional : mGuardTrapAutoConfigAdapter Change Wird gesendet nach Zugriff auf den ECS.
Benutzerfirewall-Traps (Nicht bei Geräten der FL MGUARD 2000-Serie.)	**Benutzerfirewall-Traps**	**Trap-Beschreibung**. – enterprise-oid : mGuardTrapUserFirewall – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapUserFirewallLogin (1) – additional : mGuardTResUserFirewallUsername, mGuardTResUserFirewallSrcIP, mGuardTResUserFirewallAuthenticationMethod Wird gesendet beim Einloggen eines Benutzers der Benutzer-Firewall. – enterprise-oid : mGuardTrapUserFirewall – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapUserFirewallLogout (2) – additional : mGuardTResUserFirewallUsername, mGuardTResUserFirewallSrcIP, mGuardTResUserFirewallLogoutReason Wird gesendet beim Ausloggen eines Benutzers der Benutzer-Firewall

Verwaltung >> SNMP >> Trap [...]		
		– enterprise-oid : mGuardTrapUserFirewall – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapUserFirewallAuthError TRAP-TYPE (3) – additional : mGuardTResUserFirewallUsername, mGuardTResUserFirewallSrcIP, mGuardTResUserFirewallAuthenticationMethod Wird gesendet bei einem Authentifizierungs-Fehler.
Redundanz-Traps (Nicht auf Geräten der FL MGUARD 2000-Serie)	**Statusänderung**	**Trap-Beschreibung** – enterprise-oid : mGuardTrapRouterRedundancy – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapRouterRedBackupDown – additional : mGuardTResRedundacyBackup-Down Dieser Trap wird gesendet, wenn das Backup-Gerät (sekundärer mGuard) nicht durch das Master-Gerät (primärer mGuard) erreicht werden kann. (Der Trap wird nur dann gesendet, wenn ICMP-Prüfungen aktiviert sind.) – enterprise-oid : mGuardTrapRouterRedundancy – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapRRedundancyStatusChange – additional : mGuardRRedStateSSV, mGuardRRedStateACSummary, mGuardRRedStateCCSummary, mGuardRRedStateStateRepSummary Wird gesendet, wenn sich der Zustand des HA-Clusters geändert hat.
VPN-Traps	**Statusänderungen von IPsec-Verbindungen**	Trap-Beschreibung – enterprise-oid : mGuardTrapVPN – genericTrap : enterpriseSpecific – specific-trap : mGuardTrapVPNIKEServerStatus (1) – additional : mGuardTResVPNStatus Wird gesendet beim Starten und Stoppen des IPsec-IKE-Servers.

Verwaltung >> SNMP >> Trap [...]		
		– enterprise-oid : mGuardTrapVPN – genericTrap : enterpriseSpecific – specific-trap : mGuardTrapVPNIPsecConnStatus (2) – additional : mGuardTResVPNName, mGuardTResVPNIndex, mGuardTResVPNPeer, mGuardTResVPNStatus, mGuardTResVPNType, mGuardTResVPNLocal, mGuardTResVPNRemote Wird gesendet bei einer Zustandsänderung einer IPsec-Verbindung. – enterprise-oid : mGuard – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapVPNIPsecConnStatus 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.
	Statusänderungen von L2TP-Verbindungen	Trap-Beschreibung – enterprise-oid : mGuardTrapVPN – genericTrap : enterpriseSpecific – specific-trap : mGuardTrapVPNL2TPConnStatus (3) – additional : mGuardTResVPNName, mGuardTResVPNIndex, mGuardTResVPNPeer, mGuardTResVPNStatus, mGuardTResVPNLocal, mGuardTResVPNRemote Wird gesendet bei einer Zustandsänderung einer L2TP-Verbindung.
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.

4.6.3 LLDP

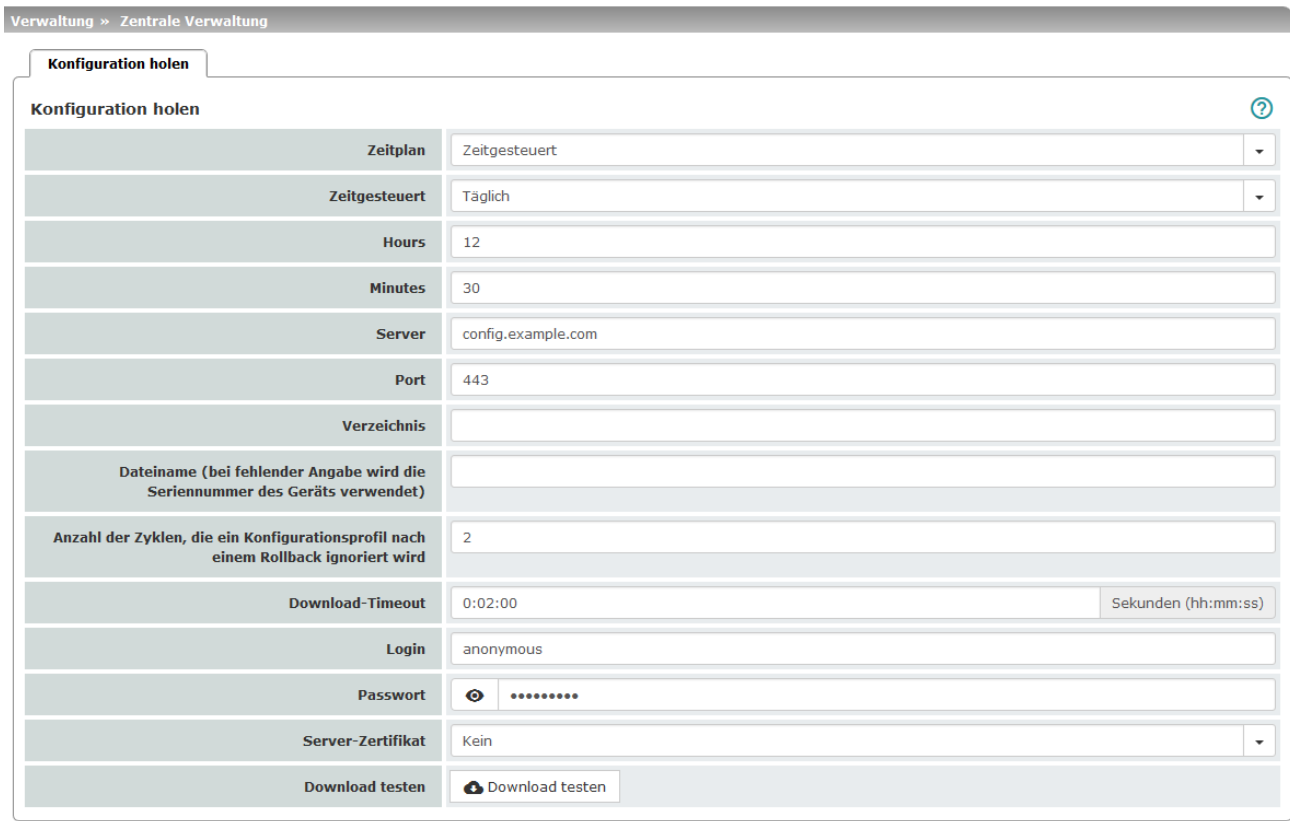
Mit LLDP (Link Layer Discovery Protocol, IEEE 802.1AB/D13) können mit geeigneten Abfragemethoden Informationen über die Netzwerk-Infrastruktur automatisch ermittelt werden. Ein System, das LLDP benutzt, kann so konfiguriert werden, dass es auf LLDP-Informationen lauscht oder LLDP-Informationen versendet. Eine Anforderung oder Beantwortung von LLDP-Informationen erfolgt grundsätzlich nicht.

Als Sender versendet der mGuard auf Ethernet-Ebene (Layer 2) dazu unaufgefordert periodisch Multicasts in konfigurierten Zeitintervallen (typischerweise ~30 s).

Verwaltung >> SNMP >> LLDP		
LLDP	**LLDP aktivieren**	Der LLDP-Service bzw. -Agent kann hier global aktiviert bzw. deaktiviert werden.
	LLDP auf externen Netzwerken	Sie können auswählen, ob der mGuard LLDP-Informationen aus externen und/oder internen Netzwerken nur **empfängt** oder ebenfalls **sendet und empfängt**.
	LLDP auf internen Netzwerken	(siehe oben)
Geräte	**Über LLDP gefundene Geräte**	**Lokales Interface** Lokales Interface, über das das Gerät gefunden wurde. **Geräte-ID-Subtyp** Eindeutiger Geräte-ID-Subtyp des gefundenen Rechners. **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. **Port-Beschreibung** Ein Text, welcher die Netzwerkschnittstelle beschreibt, über welche der Rechner gefunden wurde. **Systemname** Hostname des gefundenen Rechners.

4.7 Verwaltung >> Zentrale Verwaltung

4.7.1 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	**Zeitplan**	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. Für alle zeitbasierten Steuerungen gilt zusätzlich: Nach jedem Neustart wird der mGuard ebenfalls versuchen, eine neue Konfiguration vom Server herunterzuladen. Bei der Auswahl **Nie** wird der mGuard keinen Versuch unternehmen, eine Konfiguration vom Server herunterzuladen. Bei der Auswahl **Nach dem Einschalten** wird der mGuard nach jedem Neustart versuchen, eine Konfiguration vom Server herunterzuladen. Bei Auswahl **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 47, „Zeit und Datum“ auf Seite 49). Die Zeitsteuerung setzt die ausgewählte Zeit in Bezug auf die eventuell konfigurierte Zeitzone. Bei der Auswahl **Alle xx min/h** wird der mGuard in den ausgewählten zeitlichen Abständen versuchen, eine Konfiguration vom Server herunterzuladen.
	Server	IP-Adresse oder Hostname des Servers, welcher die Konfigurationen bereitstellt.
	Port	Port, unter dem der Server erreichbar ist.
	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: 2** 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:

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

Vorgangsbeschreibung

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 **Zeitplan** (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.

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.

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

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 **Zeitplan** = 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.

Download-Timeout

Standard: 2 Minuten (0:02:00)

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 Zeitplan (s. o.).

Die Eingabe kann aus Sekunden [ss], Minuten und Sekunden [mm:ss] oder Stunden, Minuten und Sekunden [hh:mm:ss] bestehen.

Login

Login (Benutzername), den der HTTPS Server abfragt.

Passwort

Passwort, das der HTTPS Server abfragt.

Folgende Sonderzeichen dürfen im Passwort **nicht** verwendet werden: ' ` \ " $ [ ] ? * ; < > | & !

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.

Hier darf entweder

- ein selbstsigniertes 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 selbstsigniertes)

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

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 als Meldung am oberen Bildschirmrand angezeigt.

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

4.8 Verwaltung >> Service I/O

Die Verwendung von Firewall-Regelsätzen ist auf Geräten der FL MGUARD 2000-Serie nicht möglich.

An einige mGuard-Geräte können Servicekontakte (Service I/Os) angeschlossen werden.

Der Anschluss der Servicekontakte wird im Anwenderhandbuch zu den Geräten beschrieben (siehe UM DE HW FL MGUARD 2000/4000 z. B. unter phoenixcontact.com/product/1357828).

Eingang (I1–3 bzw. CMD1–3) (COMBICON XG1)

Sie können auswählen, ob an die Eingänge ein Taster oder ein Ein-/Aus-Schalter angeschlossen wurde.

Es können ein oder mehrere frei wählbare VPN-Verbindungen oder Firewall-Regelsätze über den entsprechenden Schalter/Taster geschaltet werden:

– Der Taster oder Ein-/Aus-Schalter dient zum Auf- und Abbau von zuvor definierten VPN-Verbindungen oder zum Aktivieren/Deaktivieren von definierten Firewall-Regelsätzen.
– Die gleichzeitige Steuerung von VPN-Verbindungen und Firewall-Regelsätzen ist ebenfalls möglich.
– Über die Web-Oberfläche wird angezeigt, welche VPN-Verbindungen und Firewall-Regelsätze mit den Eingängen verknüpft sind.

Schaltung via Taster

- Zum Einschalten der gewählten VPN-Verbindungen/Firewall-Regelsätze den Taster einige Sekunden gedrückt halten und dann den Taster loslassen.
- Zum Ausschalten der gewählten VPN-Verbindungen/Firewall-Regelsätze den Taster einige Sekunden gedrückt halten und dann den Taster loslassen.

Schaltung via Ein-/Aus-Schalter

- Zum Einschalten der gewählten VPN-Verbindungen/Firewall-Regelsätze den Schalter auf EIN stellen.
- Zum Ausschalten der gewählten VPN-Verbindungen/Firewall-Regelsätze den Schalter auf AUS stellen.

Meldeausgang (O1–2 bzw. ACK1–2) (COMBICON XG2)

Sie können einstellen, ob bestimmte VPN-Verbindungen oder Firewall-Regelsätze überwacht werden sollen.

Die LEDs PF3 (für O1) bzw. PF4 (für O2) zeigen an, ob die entsprechenden VPN-Verbindungen aufgebaut oder die entsprechenden Firewall-Regelsätze aktiviert wurden.

Alarmausgang (O3 bzw. FAULT) (COMBICON XG2)

Der Alarmausgang O3 überwacht die Funktion des Geräts und ermöglicht damit eine Ferndiagnose.

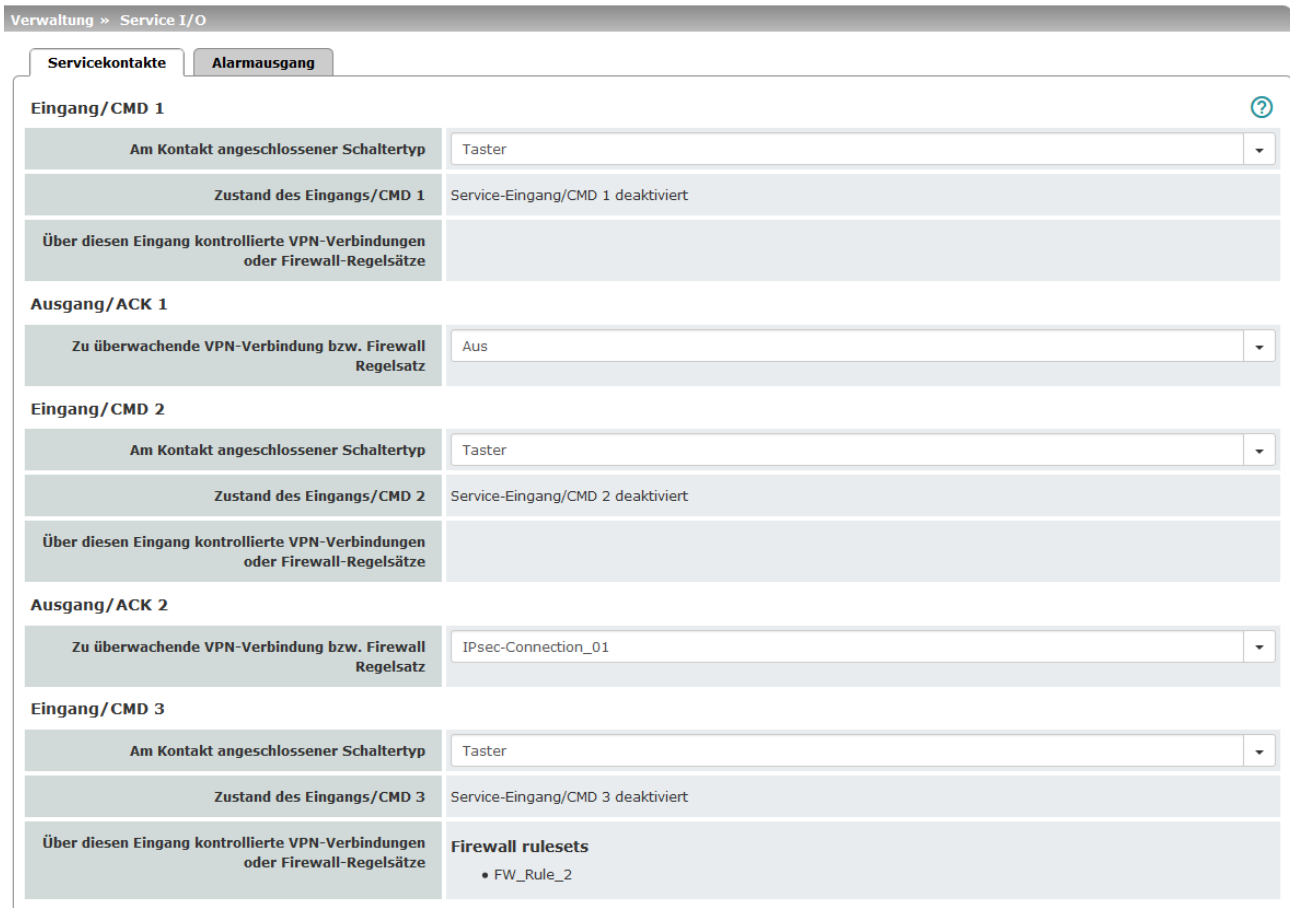
Bei Hutschienengeräten (jedoch nicht bei PCI-Karten) leuchtet die LED **FAIL** rot, wenn der Alarmausgang aufgrund eines Fehlers Low-Pegel einnimmt (invertierte Logik). Zusätzlich wird im WBM eine Meldung am oberen Bildschirmrand angezeigt.

Durch den Alarmausgang O3 können folgende Ereignisse gemeldet werden:

– Der Ausfall der redundanten Versorgungsspannung
– Nicht geänderte Administrator-Passwörter (*admin*/*root*)
– Überwachung des Link-Status der Ethernet-Anschlüsse

– Überwachung des Temperaturzustandes
– Überwachung der Redundanz

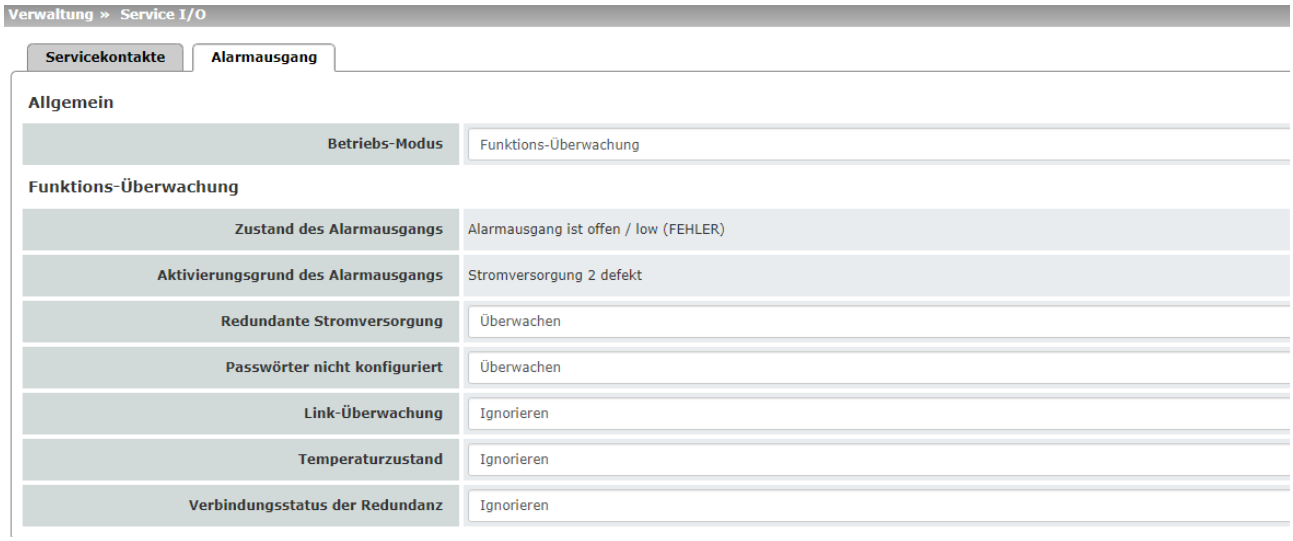
4.8.1 Servicekontakte



Verwaltung >> Service I/O>> Servicekontakte		
Eingang/CMD 1-3 (I1-3)	**Am Kontakt angeschlossener Schaltertyp**	**Taster / Ein-/Aus-Schalter** Auswahl des Typs des angeschlossen Schalters.
	Zustand des Eingangs/CMD 1-3 (I1-3)	Anzeige des Zustandes des angeschlossen Schalters. Der Schalter muss beim Editieren der VPN-Verbindung unter „Schaltender Service Eingang/CMD“ auswählt werden (unter *„IPsec VPN >> Verbindungen >> Editieren >> Allgemein“* oder *„OpenVPN-Client >> Verbindungen >> Editieren >> Allgemein“*).

Verwaltung >> Service I/O>> Servicekontakte[...]		
	Über diesen Eingang kontrollierte VPN-Verbindungen oder Firewall-Regelsätze	Der mGuard verfügt über Anschlüsse, an die externe Taster oder Ein-/Aus-Schalter und Aktoren (z. B. eine Signallampe) angeschlossen werden können. Über den Taster bzw. Ein/Aus-Schalter können – konfigurierten VPN-Verbindungen gestartet oder gestoppt werden, – konfigurierte Firewall-Regelsätze aktiviert oder deaktiviert werden. Welche Ereignisse durch den Eingang gesteuert werden, kann an folgenden Stellen konfiguriert werden: 1. **IPsec-VPN:** *„IPsec VPN >> Verbindungen >> Editieren >> Allgemein“*. 2. **OpenVPN:** *„OpenVPN-Client >> Verbindungen >> Editieren >> Allgemein“* 3. **Firewall-Regelsatz:** *„Netzwerksicherheit >> Paketfilter >> Regelsätze“*
Ausgang/ACK 1-2 (O1-2)	**Zu überwachende VPN-Verbindung bzw. Firewall-Regelsatz**	**Aus / VPN-Verbindung/Firewall-Regelsatz** Der Zustand der ausgewählten VPN-Verbindung oder des ausgewählten Firewall-Regelsatzes wird über den zugehörigen Meldekontakt (ACK-Ausgang / O1-2) signalisiert.

4.8.2 Alarmausgang



Verwaltung >> Service I/O >> Alarmausgang		
Allgemein	**Betriebsmodus**	**Funktions-Überwachung / Manuelle Einstellung** Der Alarmausgang kann automatisch durch die **Funktions-Überwachung** geschaltet werden (Standard) oder durch **Manuelle Einstellung**.
	Manuelle Einstellung	**Geschlossen / Offen (Alarm)** Hier kann der gewünschte Zustand des Alarmausgangs gewählt werden (zur Funktionskontrolle): Wird der Zustand manuell auf **Offen (Alarm)** gestellt, leuchtet die LED FAIL nicht rot (kein Alarm).
Funktions-Überwachung (Bei FL MGUARD 4102 PCI(E) wird der Zustand des Alarmausgangs nicht über die LED FAIL signalisiert.)	**Zustand des Alarmausgangs**	Anzeige des Zustandes des Alarmausgangs. Zusätzlich wird eine Meldung im WBM am oberen Bildschirmrand angezeigt. Bei Hutschienengeräten (jedoch nicht bei PCI-Karten) wird der Zustand des Alarmausgangs auch über die LED FAIL signalisiert.
	Aktivierungsgrund des Alarmausgangs	Der Grund für die Aktivierung des Alarmausgangs wird angezeigt.
	Redundante Stromversorgung (Nur bei FL MGUARD 4000)	Bei **Ignorieren** hat der Zustand der Stromversorgung keinen Einfluss auf den Alarmausgang. Bei **Überwachen** wird der Alarmausgang geöffnet, wenn eine der zwei Versorgungsspannungen ausfällt.
	Passwörter nicht konfiguriert	Überwacht, ob die voreingestellten Administrator-Passwörter für die Benutzer *root* und *admin* geändert wurden. Bei **Ignorieren** haben die nicht geänderten Passwörter keinen Einfluss auf den Alarmausgang. Bei **Überwachen** wird der Alarmausgang geöffnet, wenn die voreingestellten Passwörter nicht geändert wurden.

Verwaltung >> Service I/O >> Alarmausgang [...]		
	Link-Überwachung	Überwachung des Link-Status der Ethernet-Anschlüsse. Bei **Ignorieren** hat der Link-Status der Ethernet-Anschlüsse keinen Einfluss auf den Alarmausgang. Bei **Überwachen** wird der Alarmausgang geöffnet, wenn einLink keine Konnektivität aufweist. Stellen Sie dazu unter *„Netzwerk >> Ethernet >> MAU-Einstellungen“* unter „Link-Überwachung“ die Links ein, die überwacht werden sollen.
	Temperaturzustand	Der Alarmausgang 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 Alarmausgang geöffnet, wenn die Temperatur den zulässigen Bereich verlässt.
	Verbindungsstatus der Redundanz	Nur wenn die Funktion Redundanz genutzt wird (siehe Kapitel 13). Bei **Ignorieren** hat die Konnektivitätsprüfung keinen Einfluss auf den Alarmausgang. Bei **Überwachen** wird der Alarmausgang geöffnet, wenn die Konnektivitätsprüfung fehlschlägt. Das ist unabhängig davon, ob der mGuard aktiv oder im Bereitschaftszustand ist.

4.9 Verwaltung >> Neustart

4.9.1 Neustart

Verwaltung >> Neustart >> Neustart		
Neustart	**Neustart**	Ein Klick auf die Schaltfläche „**Neustart**“ startet den mGuard neu (Reboot). Das Gerät benötigt ca. 30 Sekunden für den Neustart. Ein Neustart hat den selben Effekt wie die vorübergehende Unterbrechung der Stromzufuhr. Der mGuard wird aus- und wieder eingeschaltet. Ein Neustart ist erforderlich im Fehlerfall. Außerdem kann ein Neustart nach einem Software-Update erforderlich sein.

5 Menü Netzwerk

5.1 Netzwerk >> Interfaces

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

Gerät	**Ethernet:** – Intern: LAN (Ports: XF2-4 bzw. XF2-5) – Extern: WAN (Port: XF1) – DMZ: DMZ (Port: XF5)
FL MGUARD 2102	**LAN: 1** **WAN: 1**
FL MGUARD 4302 (KX)	**LAN: 1** **WAN: 1**
FL MGUARD 2105	**LAN: 4** **WAN: 1**
FL MGUARD 4305 (KX)	**LAN: 3** **WAN: 1** **DMZ: 1**
FL MGUARD 4102 PCI(E)	**LAN: 1** **WAN: 1**

Der LAN-Port wird an einen Einzelrechner oder das lokale Netzwerk (= intern) angeschlossen. Der WAN-Port ist für den Anschluss an das externe Netz.

Netzwerkports (Migration mGuard 8 --> mGuard 10)

Tabelle 5-1 Mapping-Tabelle (Netzwerkports nach der Migration)

mGuard 8	**mGuard 10**	**mGuard 8** (Intern mit eingebautem Switch)	**mGuard 10** (Intern mit eingebautem Switch)
FL MGUARD 2000/4000			
WAN	XF1	(n/a)	(n/a)
LAN1	XF2	swp2	swp0
FL MGUARD 2105/4305			
LAN2	XF3	swp0	swp1
LAN3	XF4	swp1	swp2
FL MGUARD 2105			
LAN4	XF5	swp3	swp3
FL MGUARD 4305			
DMZ	XF5	swp4	dmz0
Nicht bei FL MGUARD 2105/FL MGUARD 4305			
LAN5	(n/a)	swp4	(n/a)

Anschließen der Netzwerk-Schnittstelle

Die mGuard-Plattformen haben DTE-Schnittstellen. Schließen Sie mGuards mit DTE-Schnittstelle 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.

MAC-Adressen

Die vom Hersteller festgelegte MAC-Adresse des WAN-Interface ist auf dem Typenschild des Geräts angegeben. Die weiteren MAC-Adressen (LAN/DMZ [optional]) lassen sich wie folgt berechnen:

- **WAN-Interface:** siehe Typenschild.
- **LAN-Interface:** Die MAC-Adresse des WAN-Interface um 1 erhöht (**WAN + 1**). Geräte mit integriertem Switch: Alle Switch-Ports verwenden die gleiche MAC-Adresse.
- **DMZ-Interface:** Die MAC-Adresse des WAN-Interface um 4 erhöht (**WAN + 4**).

Beispiel:

- WAN: 00:a0:45:eb:28:9d
- LAN: 00:a0:45:eb:28:9e
- DMZ: 00:a0:45:eb:28:a1

5.1.1 Überblick: Netzwerk-Modus „Router“

Bei den Geräten der neuen Gerätegeneration ist die Werkseinstellung wie folgt: **Netzwerk-Modus „Router“, Router-Modus „DHCP“**.

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.

LAN-Port

Über seinen LAN-Port ist der mGuard an ein lokales Netzwerk oder an einen Einzelrechner angeschlossen.

Wie auch in den anderen Modi stehen die Sicherheitsfunktionen Firewall und VPN (geräteabhängig) 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 153).
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.

Es gibt zwei Router-Modi:

– Statisch
– DHCP

Router-Modus: Statisch

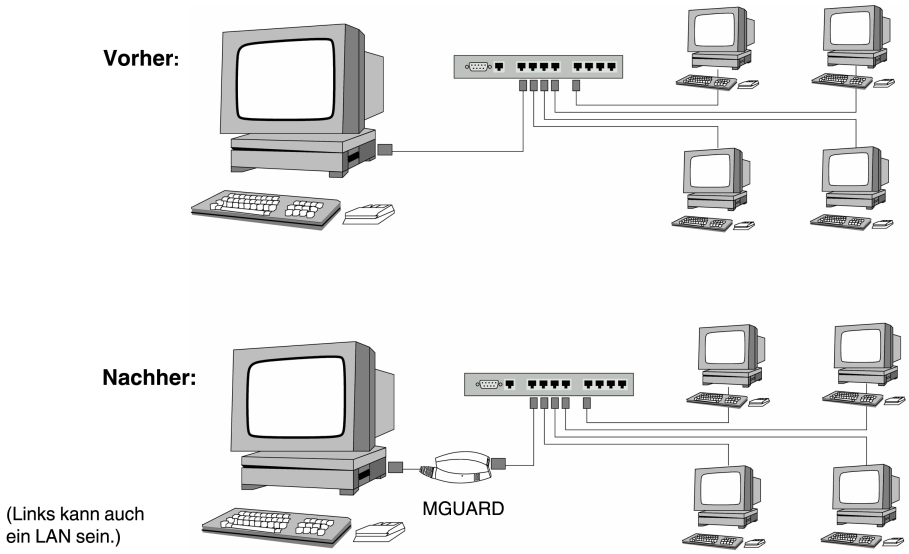
Die externen IP-Einstellungen sind fest eingestellt.

Router-Modus: DHCP

Die externen IP-Einstellungen werden vom mGuard angefragt und von einem externen DHCP-Server vergeben.

5.1.2 Überblick: Netzwerk-Modus „Stealth“

Der *Stealth*-Modus (Plug-n-Protect) 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.



Der mGuard analysiert den laufenden Netzwerkverkehr und konfiguriert dementsprechend seine Netzwerkanbindung eigenständig. Er arbeitet transparent und ist somit innerhalb des Netzes ohne konfigurierte Management-IP-Adresse nicht detektierbar. Angeschlossene Rechner behalten ihre Netzwerkkonfiguration und müssen nicht umkonfiguriert werden.

Wie auch in den anderen Modi stehen die Sicherheitsfunktionen Firewall und VPN (geräteabhängig) zur Verfügung.

Von extern gelieferte DHCP-Daten werden an den angeschlossenen Rechner durchgelassen.

Im *Single-Stealth*-Modus muss eine auf dem Rechner installierte Firewall ICMP-Echo-Requests (Ping) zulassen, wenn der mGuard Dienste wie VPN, DNS, NTP etc. bereitstellen 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.

In den *Stealth*-Konfigurationen **„Automatisch“** und **„Statisch“** ist der Aufbau einer vom internen Client ausgehenden VPN-Verbindung durch den mGuard hindurch nicht möglich.

Stealth-Konfigurationen

Automatisch

Der mGuard analysiert den ausgehenden Netzwerkverkehr, der über ihn läuft, und konfiguriert dementsprechend seine Netzwerkanbindung eigenständig. Er arbeitet transparent.

Für die Nutzung bestimmter Funktionen (z. B. automatische Updates oder Aufbau von VPN-Verbindungen) ist es erforderlich, dass der mGuard auch im Stealth-Modus eigene Anfragen an externe Server stellt.

Diese Anfragen sind nur möglich, wenn der lokal angeschlossenen Rechner Ping-Anfragen zulässt. Konfigurieren Sie dessen Sicherheitseinstellungen entsprechend.

Statisch

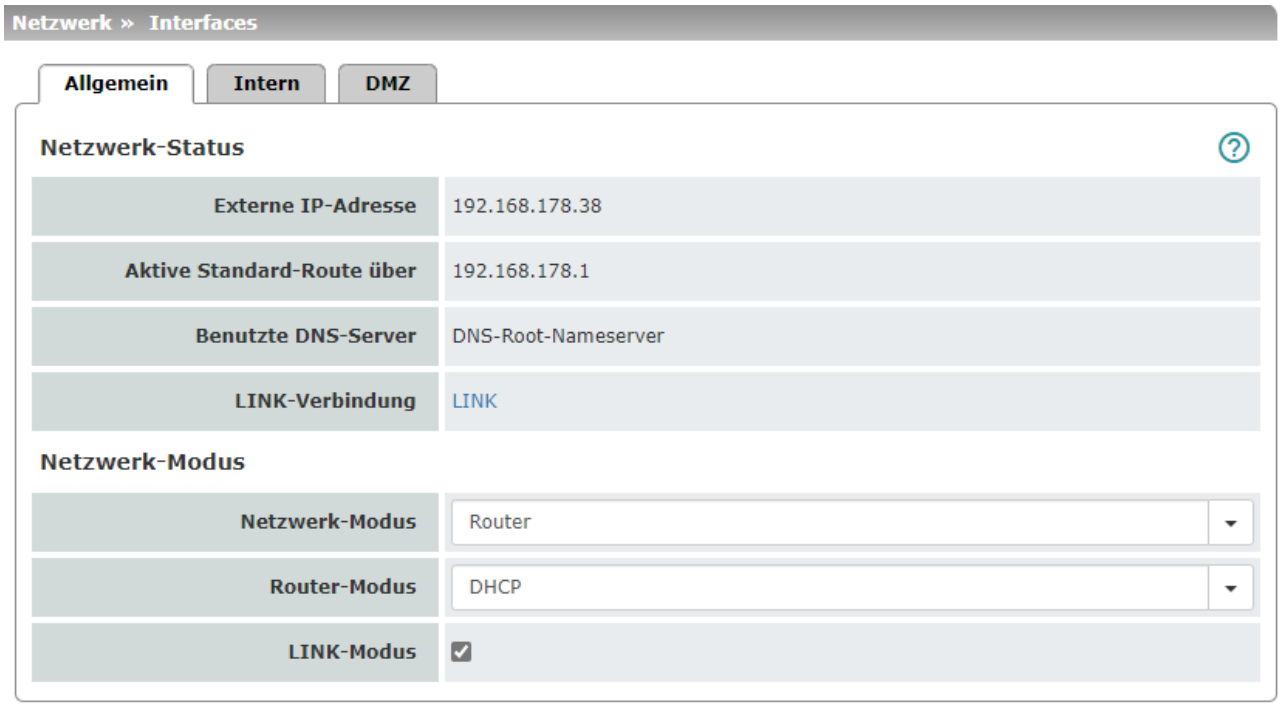
Wenn der mGuard keinen über ihn laufenden Netzwerkverkehr analysieren kann, z. B. weil zum lokal angeschlossenen Rechner nur Daten ein-, aber nicht ausgehen, dann muss die *Stealth-Konfiguration* auf **Statisch** gesetzt werden. In diesem Fall stehen weitere Eingabefelder zur statischen Stealth-Konfiguration zur Verfügung.

Mehrere Clients

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.

Für die weitere Konfiguration des Netzwerk-Modus *Stealth* siehe „Stealth“ auf Seite 144.

5.1.3 Allgemein



Netzwerk >> Interfaces >> Allgemein		
Netzwerk-Status	**Externe IP-Adresse**	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.
	Aktive Standard-Route über	Nur Anzeige: Hier wird die IP-Adresse angezeigt, über die der mGuard versucht, ihm unbekannte Netze zu erreichen. Wurde keine Standard-Route festgelegt, bleibt das Feld leer.
	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 [...]		
	LINK-Verbindung	Wird das mGuard-Gerät über ein Interface, in der Regel über sein externes WAN-Interface (XF1), mit dem Gerät "CELLULINK" verbunden und der LINK-Modus aktiviert (siehe unten), wird an dieser Stelle ein Hyperlink zum Web-based Management des Gerätes "CELLULINK" angezeigt. Ein Klick auf den Hyperlink öffnet das Web-based Management des Gerätes "CELLULINK", das damit weiter konfiguriert werden kann. Um eine Verbindung zum "CELLULINK" aus dem LAN-Netzwerk zu ermöglichen, müssen die Firewall- und NAT-Regeln des mGuard-Gerätes gegebenenfalls angepasst werden.
Netzwerk-Modus	**Netzwerk-Modus**	**Router / Stealth** Der mGuard muss auf den Netzwerk-Modus gestellt werden, der seiner Einbindung in das Netzwerk entspricht. Je nachdem, auf welchen Netzwerk-Modus der mGuard gestellt ist, ändert sich auch die Seite mit den auf ihr angebotenen Konfigurationsparametern. Siehe auch: „Überblick: Netzwerk-Modus „Router““ auf Seite 131 und „Überblick: Netzwerk-Modus „Stealth““ auf Seite 132.
	Abhängig von der Auswahl des Netzwerkmodus und je nach mGuard-Gerät stehen unterschiedliche Einstellungsmöglichkeiten auf der Web-Oberfläche zur Verfügung:	
	Router-Modus (Nur wenn Netzwerk-Modus „**Router**“ ausgewählt wurde)	**Statisch / DHCP** Für eine umfassende Beschreibung siehe: – „Router-Modus: Statisch“ auf Seite 131 – „Router-Modus: DHCP“ auf Seite 131

Netzwerk >> Interfaces >> Allgemein [...]

LINK-Modus

(Nur wenn Netzwerk-Modus „**Router**“ und Router-Modus „**DHCP**“ ausgewählt wurden)

Über das bei Phoenix Contact erhältliche Gerät "CELLULINK" kann das mGuard-Gerät eine mobile Datenverbindung zu anderen Netzwerken oder dem Internet herstellen (z. B. über das 4G-Netz).

Das mGuard-Gerät wird dazu in der Regel über sein externes WAN-Interface (XF1) mit dem Gerät "CELLULINK" verbunden, das damit als Standard-Gateway für das mGuard-Gerät fungiert.

Wird der LINK-Modus aktiviert, wird ein Hyperlink zum Web-based Management des Gerätes "CELLULINK" im Bereich Netzwerk-Status als "LINK-Verbindung" (siehe oben) angezeigt.

Ein Klick auf den Hyperlink öffnet das Web-based Management des Gerätes "CELLULINK", das damit weiter konfiguriert werden kann.

Um eine Verbindung zum "CELLULINK" aus dem LAN-Netzwerk zu ermöglichen, müssen die Firewall- und NAT-Regeln des mGuard-Gerätes gegebenenfalls angepasst werden.

Netzwerk >> Interfaces >> Allgemein [...]

Stealth-Konfiguration

(Nur wenn Netzwerk-Modus „**Stealth**“ ausgewählt wurde)

Automatisch / Statisch / Mehrere Clients

Automatisch

Der mGuard analysiert den Netzwerkverkehr, der über ihn läuft, und konfiguriert dementsprechend seine Netzwerkanbindung eigenständig. Er arbeitet transparent.

Für die Nutzung bestimmter Funktionen (z. B. automatische Updates oder Aufbau von VPN-Verbindungen) ist es erforderlich, dass der mGuard auch im Stealth-Modus eigene Anfragen an externe Server stellt.

Diese Anfragen sind nur möglich, wenn der lokal angeschlossenen Rechner Ping-Anfragen zulässt. Konfigurieren Sie dessen Sicherheitseinstellungen entsprechend.

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 (Werkseinstellung)

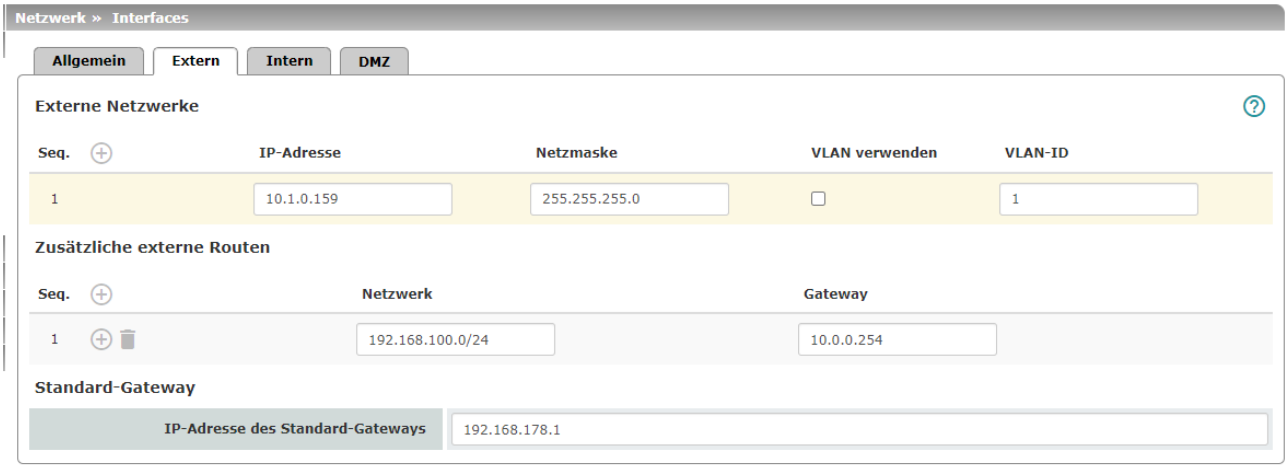
Wie bei **Automatisch**, es können jedoch mehr als nur ein Rechner am LAN-Port (gesicherter Port) des mGuards angeschlossen sein und somit mehrere IP-Adressen am LAN-Port (gesicherter Port) des mGuards verwendet werden.

Automatische Konfiguration: Ignoriere NetBIOS über TCP auf TCP-Port 139

(Nur bei Stealth-Konfiguration **Automatisch**)

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, aktivieren Sie die Funktion, sofern Sie den mGuard an einem Rechner angeschlossen haben, der diese Eigenarten aufweist.

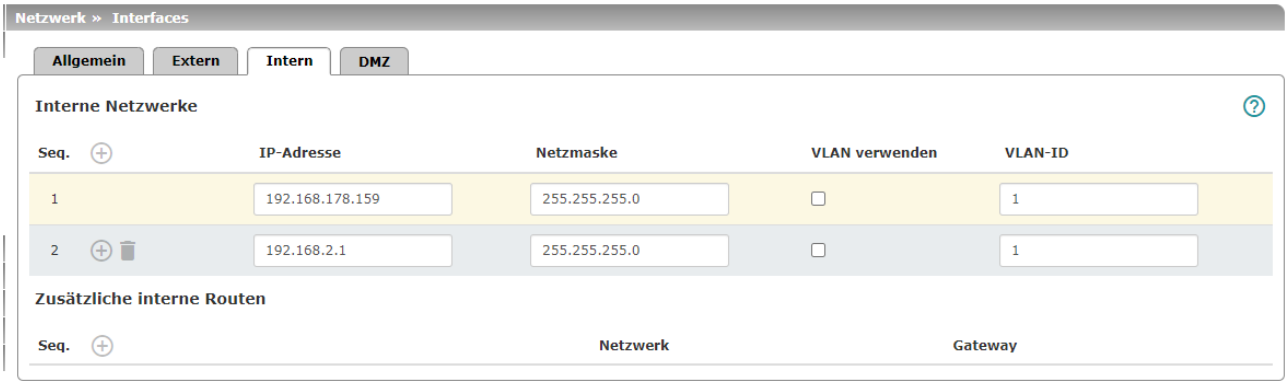
5.1.4 Extern



Netzwerk >> Interfaces >> Extern (Netzwerk-Modus = „Router“, Router-Modus = „Statisch“)		
Externe Netzwerke	Die Adressen, unter denen der mGuard von externen Geräten erreichbar ist, die sich hinter dem WAN-Port befinden. Findet hier der Übergang zum Internet statt, wird die externe IP-Adresse des mGuards vom Internet Service Provider (ISP) vorgegeben.	
	IP-Adresse	IP-Adresse, unter welcher der mGuard über seinen WAN-Port erreichbar sein soll.
	Netzmaske	Die Netzmaske des am WAN-Port angeschlossenen Netzes.
	Verwende VLAN	Wenn die IP-Adresse innerhalb eines VLANs liegen soll, aktivieren Sie die Funktion.
	VLAN-ID	– Eine VLAN-ID zwischen 1 und 4095. – Eine Erläuterung des Begriffes „VLAN“ befindet sich im Glossar auf Seite 371. – Falls Sie Einträge aus der Liste löschen wollen: Der erste Eintrag kann nicht gelöscht werden.
	OSPF-Area (Nur wenn **OSPF** aktiviert ist)	Verknüpft statisch konfigurierte oder über DHCP zugewiesene Adressen/Routen der externen Netzwerkschnittstelle mit einer OSPF-Area (siehe „Netzwerk >> Dynamisches Routing“ auf Seite 175).
Zusätzliche externe Routen	Zusätzlich zur Standard-Route über das unten angegebene Standard-Gateway können Sie weitere externe Routen festlegen.	
	Netzwerk	Das Netzwerk in CIDR-Schreibweise angeben (siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 43).
	Gateway	Das Gateway, über welches dieses Netzwerk erreicht werden kann. Siehe auch „Netzwerk-Beispielskizze“ auf Seite 44.

Netzwerk >> Interfaces >> Extern (Netzwerk-Modus = „Router“, Router-Modus = „Statisch“) [...]		
Standard-Gateway	**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. 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 unter „Netzwerk >> NAT“ Ihr lokales Netz angeben (siehe Seite 153).

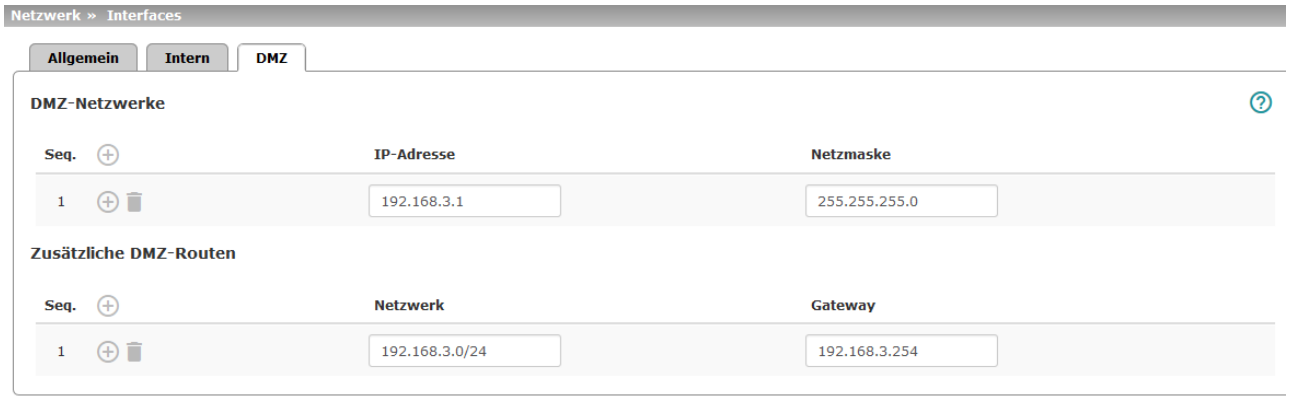
5.1.5 Intern



Netzwerk >> Interfaces >> Intern (Netzwerk-Modus = „Router“)		
Interne Netzwerke	**IP-Adresse**	IP-Adresse, unter der das mGuard-Gerät über seinen LAN-Port aus dem lokal angeschlossenen Netzwerk erreichbar sein soll. Im **Router-Modus** ist werkseitig voreingestellt: – IP-Adresse: **192.168.1.1** – Netzmaske: **255.255.255.0** Sie können weitere Adressen festlegen, unter denen 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.
	Netzmaske	Die Netzmaske des am LAN-Port angeschlossenen Netzes.
	Verwende VLAN	Wenn die IP-Adresse innerhalb eines VLANs liegen soll, aktivieren Sie die Funktion.
	VLAN-ID	– Eine VLAN-ID zwischen 1 und 4095. – Eine Erläuterung des Begriffes „VLAN“ befindet sich im Glossar auf 371. – Falls Sie Einträge aus der Liste löschen wollen: Der erste Eintrag kann nicht gelöscht werden.
	OSPF-Area (Nur wenn **OSPF** aktiviert ist)	Verknüpft die statischen Adressen/Routen der internen Netzwerkschnittstelle mit einer OSPF-Area (siehe „Netzwerk >> Dynamisches Routing“ auf Seite 175).
Zusätzliche Interne Routen	Wenn am lokal angeschlossen Netz weitere Subnetze angeschlossen sind, können Sie zusätzliche Routen definieren.	
	Netzwerk	Das Netzwerk in CIDR-Schreibweise angeben (siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 43).

Netzwerk >> Interfaces >> Intern (Netzwerk-Modus = „Router“) [...]		
	Gateway	Das Gateway, über welches dieses Netzwerk erreicht werden kann. Siehe auch „Netzwerk-Beispielskizze“ auf Seite 44.

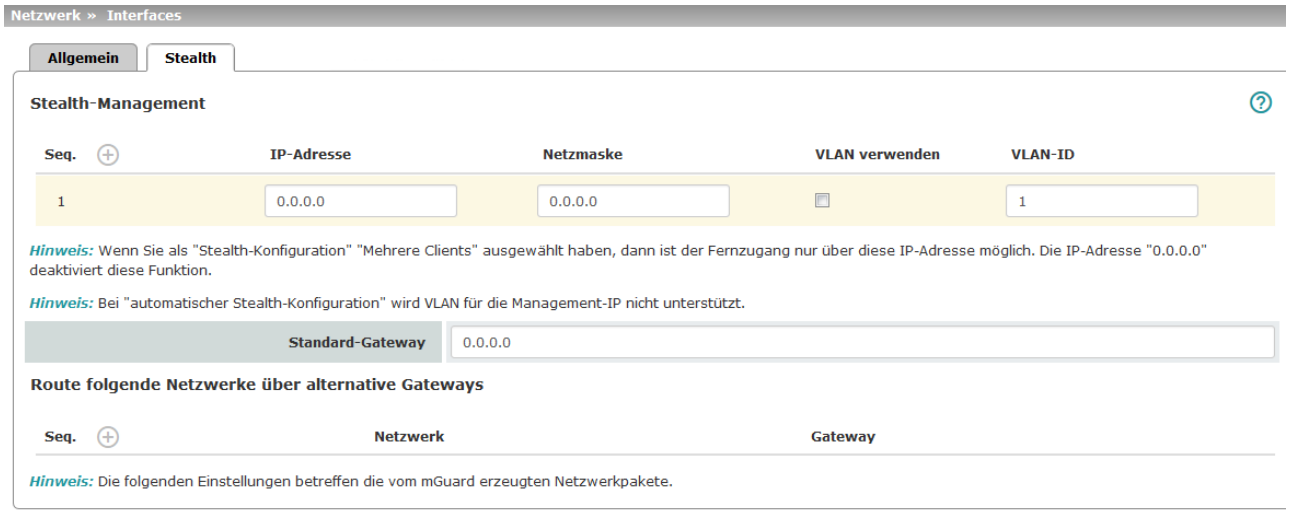
5.1.6 DMZ



Netzwerk >> Interfaces >> DMZ (Netzwerk-Modus = „Router“)		
DMZ-Netzwerke (Nur bei FL MGUARD 4305)	**IP-Adressen**	IP-Adresse, unter der der mGuard von Geräten des am DMZ-Port angeschlossenen Netzes erreichbar ist. Der DMZ-Port wird nur im Router-Modus unterstützt und benötigt wenigstens eine IP-Adresse und eine entsprechende Netzmaske. Die DMZ unterstützt keine VLANs. Im **Netzwerk-Modus „Router“** ist für jede neu hinzugefügte Tabellenzeile werkseitig voreingestellt: – IP-Adresse: **192.168.3.1** – Netzmaske: **255.255.255.0** Sie können weitere Adressen festlegen, unter der der mGuard von Geräten am DMZ-Port angeschlossenen Netzen angesprochen werden kann. Das ist zum Beispiel dann hilfreich, wenn das am DMZ-Port angeschlossenen Netze in Subnetze unterteilt wird. Dann können mehrere Geräte aus verschiedenen Subnetzen den mGuard unter unterschiedlichen Adressen erreichen.
	IP-Adresse	IP-Adresse, unter welcher der mGuard über seinen DMZ-Port erreichbar sein soll. Default: 192.168.3.1
	Netzmaske	Die Netzmaske des am DMZ-Port angeschlossenen Netzes. Default: 255.255.255.0
	OSPF-Area (Nur wenn **OSPF** aktiviert ist)	Verknüpft die statischen Adressen/Routen der DMZ-Netzwerkschnittstelle mit einer OSPF-Area (siehe „Netzwerk >> Dynamisches Routing“ auf Seite 175).
Zusätzliche DMZ-Routen	Wenn am DMZ weitere Subnetze angeschlossen sind, können Sie zusätzliche Routen definieren.	

Netzwerk >> Interfaces >> DMZ (Netzwerk-Modus = „Router“)[...]		
	Netzwerk	Das Netzwerk in CIDR-Schreibweise angeben (siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 43). Default:192.168.3.0/24
	Gateway	Das Gateway, über welches dieses Netzwerk erreicht werden kann. Siehe auch „Netzwerk-Beispielskizze“ auf Seite 44. Default: 192.168.3.254

5.1.7 Stealth



Netzwerk >> Interfaces >> Stealth (Netzwerk-Modus = „Stealth“)

Stealth-Management

Hier können Sie weitere Management-IP-Adresse angeben, über die 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.

IP-Adresse

Management-IP-Adresse, unter welcher der mGuard erreichbar und administrierbar sein soll.

Im Stealth-Modus „Automatisch“ gilt:
Wird eine Management-IP-Adresse vergeben, muss das Standard-Gateway des Netzes, in dem sich der mGuard befindet, angegeben werden.

Die IP-Adresse „0.0.0.0“ deaktiviert die Management-IP-Adresse.

Ändern Sie zuerst die Management-IP-Adresse, bevor Sie zusätzliche Adressen angeben.

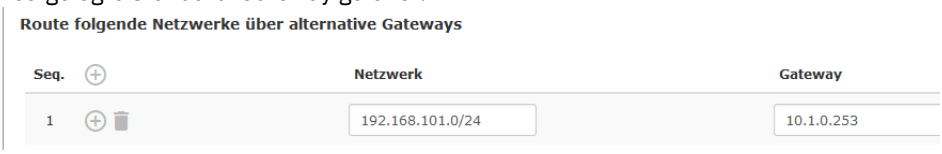
Netzmaske

Die Netzmaske zu obiger IP-Adresse.

Netzwerk >> Interfaces >> Stealth (Netzwerk-Modus = „Stealth“) [...]		
	VLAN verwenden	Diese Option ist nur gültig, wenn Sie die Option „Stealth-Konfiguration“ auf „Mehrere Clients“ gesetzt haben. IP-Adresse und Netzmaske des VLAN-Ports. Wenn die IP-Adresse innerhalb eines VLANs liegen soll, aktivieren Sie die Funktion.
	VLAN-ID	Diese Option ist nur gültig, wenn Sie die Option „Stealth-Konfiguration“ auf „Mehrere Clients“ gesetzt haben. – Eine VLAN-ID zwischen 1 und 4095. – Eine Erläuterung finden Sie unter „VLAN“ auf Seite 371. – Falls Sie Einträge aus der Liste löschen wollen: Der erste Eintrag kann nicht gelöscht werden. Im Stealth-Modus „Mehrere Clients“ 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. **Im Stealth-Modus „Automatisch“ gilt:** Wird eine Management-IP-Adresse vergeben, muss das Standard-Gateway des Netzes, in dem sich der mGuard befindet, angegeben werden.
Route folgende Netzwerke über Alternative Gateways	**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 – Log-Meldungen – das Herunterladen von Firmware-Updates – das Herunterladen von Konfigurationsprofilen von einem zentralen Server (sofern konfiguriert) – SNMP-Traps

Netzwerk >> Interfaces >> Stealth (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 43).

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 44).

Einstellungen Stealth-Modus (statisch)

(Nur bei Auswahl „statische“ Stealth-Konfiguration)

IP-Adresse des Clients

Die IP-Adresse des am LAN-Port angeschlossenen Rechners.

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:

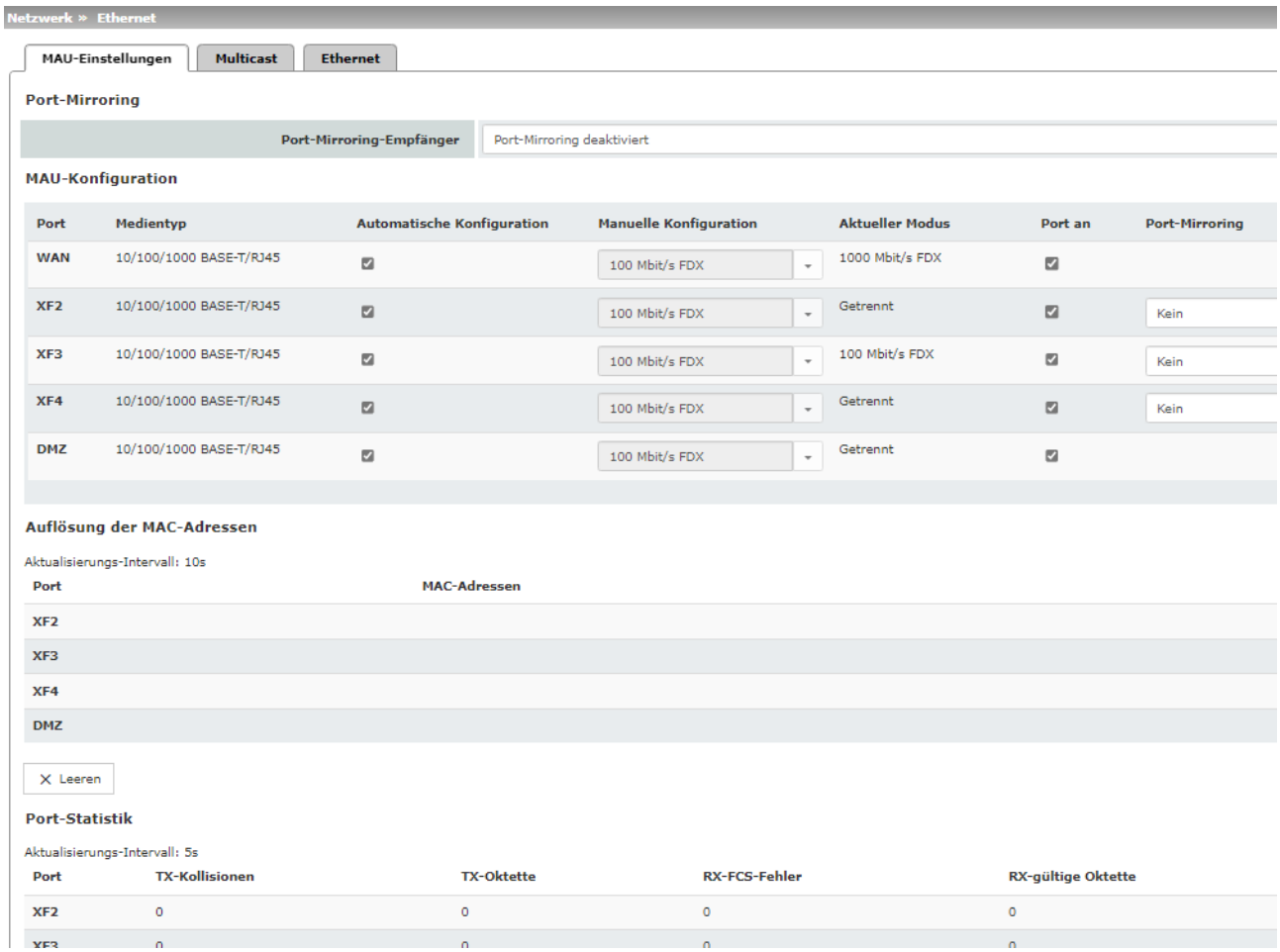
  Auf der DOS-Ebene (Menü Start, Alle Programme, Zubehör, Eingabeaufforderung) folgenden Befehl eingeben:
  ipconfig /all

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 RFC 2131 „Dynamic Host Configuration Protocol“, Abschnitt 4.4.1)

5.2 Netzwerk >> Ethernet

5.2.1 MAU-Einstellungen

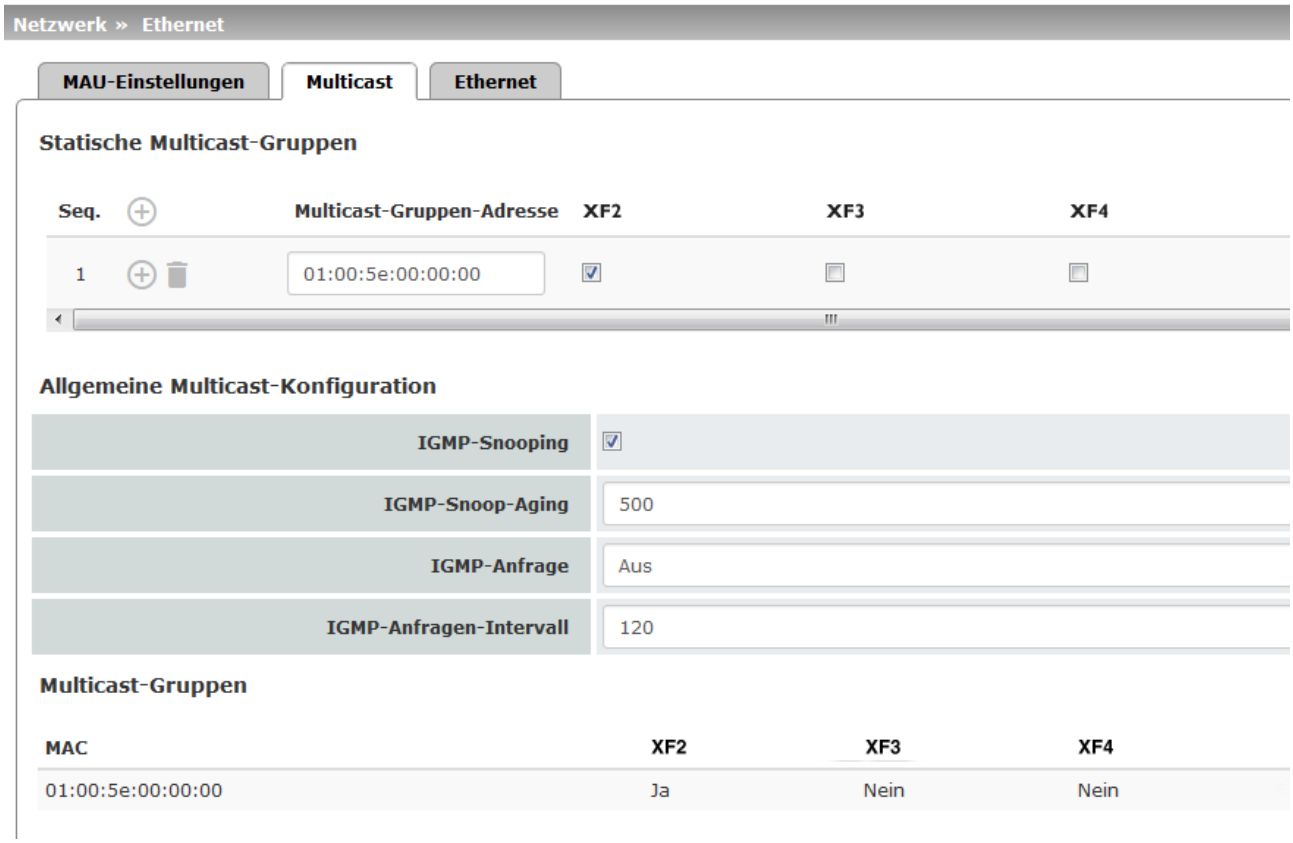


Netzwerk >> Ethernet >> MAU-Einstellungen		
Port-Mirroring (Nur bei FL MGUARD 4305)	Port-Mirroring-Empfänger	Der integrierte Switch beherrscht das Port-Mirroring, um den Netzwerkverkehr zu beobachten. Dabei können Sie entscheiden, welche Ports Sie beobachten wollen. Der Switch schickt dann Kopien von Daten-Frames der beobachteten Ports an einen dafür ausgewählten Port. Die Port-Mirroring-Funktion ermöglicht es, beliebige Frames an einen bestimmten Empfänger weiterzuleiten. Sie können den Empfänger-Port oder die Spiegelung der ein- und ausgehende Frames von jedem Switch-Port auswählen.
MAU-Konfiguration	Konfiguration und Statusanzeige der Ethernet-Anschlüsse:	
	Port	Name des Ethernet-Anschlusses, auf welchen sich die Zeile bezieht.

Netzwerk >> Ethernet >> MAU-Einstellungen [...]		
	Medientyp	Medientyp des Ethernet-Anschlusses.
	Automatische Konfiguration	**Aktiviert**: Versucht die benötigte Betriebsart automatisch zu ermitteln. **Deaktiviert**: Verwendet die vorgegebene Betriebsart aus der Spalte „Manuelle Konfiguration“
	Manuelle Konfiguration	Die gewünschte Betriebsart, wenn ***Automatische Konfiguration*** **deaktiviert** ist.
	Aktueller Modus	Die aktuelle Betriebsart des Netzwerkanschlusses.
	Port an	Schaltet den Ethernet-Anschluss auf Ein oder Aus.
	Link-Überwachung	Ist nur sichtbar, wenn unter „Verwaltung >> Service I/O >> Alarmausgang“ der Unterpunkt „Link-Überwachung“ auf „Überwachen“ steht. Bei einer Link-Überwachung wird der Alarmausgang geöffnet, wenn ein Link keine Konnektivität aufweist.
	Port-Mirroring (Nur bei FL MGUARD 4305)	Die Port-Mirroring-Funktion ermöglicht es, beliebige Frames an einen bestimmten Empfänger weiterzuleiten. Sie können den Empfänger-Port oder die Spiegelung der ein- und ausgehende Frames von jedem Switch-Port auswählen.
Auflösung der MAC-Adressen (Nur bei FL MGUARD 4305)	**Port**	Name des Ethernet-Anschlusses, auf welchen sich die Zeile bezieht.
	MAC-Adressen	Liste der MAC-Adressen der angeschlossenen ethernetfähigen Geräte. Der Switch kann MAC-Adressen lernen, die zu den Ports seines angeschlossenen ethernetfähigen Geräte gehören. Der Inhalt der Liste kann über die Schaltfläche „Leeren“ gelöscht werden.
Port-Statistik (Nur bei FL MGUARD 4305)	Für jeden physikalisch erreichbaren Port des integrierten Managed Switch wird eine Statistik angezeigt. Der Zähler kann über die Web-Oberfläche oder diesen Befehl zurückgesetzt werden: ***/Packages/mguard-api_0/mbin/action switch/reset-phy-counters***	
	Port	Name des Ethernet-Anschlusses, auf welchen sich die Zeile bezieht.
	TX-Kollisionen	Anzahl der Fehler beim Senden der Daten
	TX-Oktette	Gesendetes Datenvolumen
	RX-FCS-Fehler	Anzahl an empfangenen Frames mit ungültiger Prüfsumme
	RX-gültige Oktette	Volumen der empfangene gültigen Daten

5.2.2 Multicast

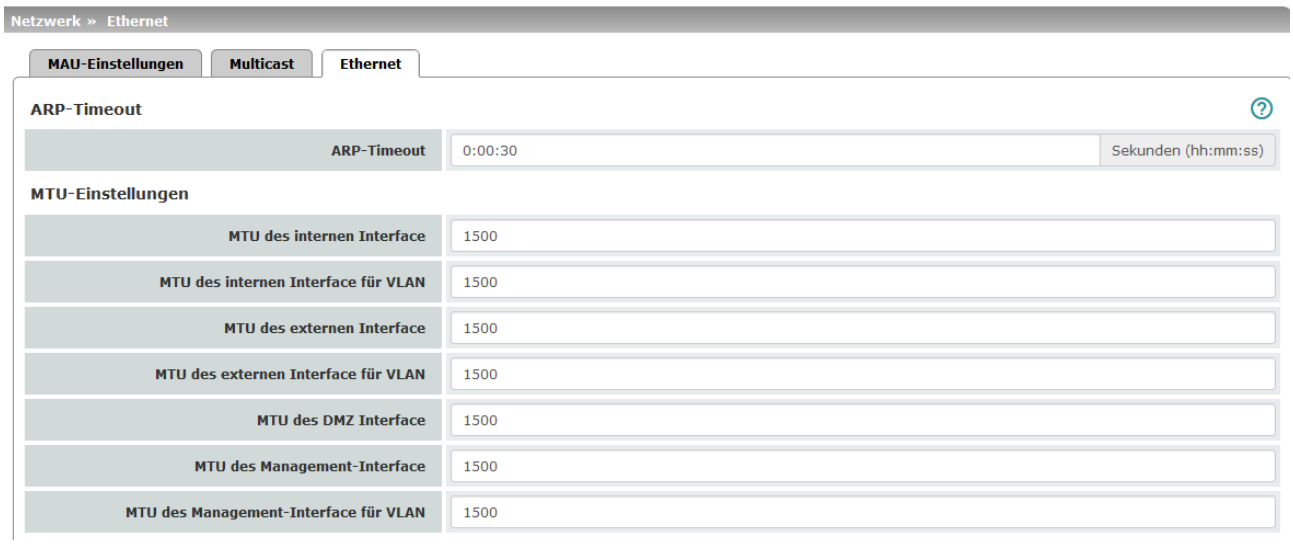
Nur verfügbar bei FL MGUARD 4305 und FL MGUARD 4305/KX.



Netzwerk >> Ethernet >> Multicast		
Statische Multicast-Gruppen	**Statische Multicast-Gruppen**	**Hinweis**: Damit Daten in Statischen Multicast-Gruppen korrekt an die konfigurierten Ports weitergeleitet werden, muss „IGMP-Snooping“ aktiviert werden (siehe unten). Multicast ist eine Technologie, die es ermöglicht, Daten an eine Gruppe von Empfängern zu versenden, ohne dass diese vom Sender mehrmals versendet werden müssen. Die Datenvervielfältigung erfolgt durch die Verteiler innerhalb des Netzes. Sie können eine Liste mit **Multicast-Gruppen-Adressen** erstellen. Die Daten werden an die konfigurierten Ports (XF2 ... XF4) weitergeleitet.
Allgemeine Multicast-Konfiguration	**IGMP-Snooping** (Nicht aktiv im Netzwerk-Modus „Stealth“)	Durch IGMP-Snooping garantiert der Switch, dass Multicast-Daten nur über Ports weitergeleitet werden, die für diese Anwendung vorgesehen sind.

Netzwerk >> Ethernet >> Multicast [...]		
	IGMP-Snoop-Aging	Zeitraum, nach dem die Zugehörigkeit zu der Multicast-Gruppe gelöscht wird in Sekunden.
	IGMP-Anfrage	Eine Multicast-Gruppe wird über IGMP an- und abgemeldet. Hier kann die Version von IGMP ausgewählt werden. Die IGMP-Version v1 (IGMPv1) wird nicht mehr unterstützt. Alle Geräte der neuen Gerätegeneration unterstützen ausschließlich die IGMP-Version v2 (IGMPv2).
	IGMP-Anfrage-Intervall	Abstand, in dem IGMP-Anfragen erzeugt werden, in Sekunden. Bei einer Änderung des Intervalls, werden neue IGMP-Anfragen erst nach Ablauf des zuvor konfigurierten Intervalls erzeugt.
Multicast-Gruppen	Anzeige der Multicast-Gruppen. Die Anzeige enthält alle statischen Einträge und die dynamischen Einträge, die durch IGMP-Snooping entdeckt werden.	

5.2.3 Ethernet



Netzwerk >> Ethernet >> Ethernet		
ARP-Timeout	**ARP-Timeout**	Lebensdauer der Einträge in der ARP-Tabelle. Die Eingabe kann aus Sekunden [ss], Minuten und Sekunden [mm:ss] oder Stunden, Minuten und Sekunden [hh:mm:ss] bestehen. In der ARP-Tabelle werden MAC- und IP-Adressen einander zugeordnet.
MTU-Einstellungen	**MTU des ... Interface**	Die Maximum Transfer Unit (MTU) beschreibt die maximale IP-Paketlänge, die beim betreffenden Interface benutzt werden darf. Erlaubte Werte: 68 - 1500 Bei VLAN-Interface gilt: 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.

5.3 Netzwerk >> NAT

5.3.1 Maskierung

Netzwerk >> NAT >> Maskierung

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 sollen.

Die Methode kann auch dazu genutzt werden, um externe Netzwerkstrukturen vor 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.

Werkseinstellungen: IP-Masquerading ist aktiv für Pakete, die aus dem internen Netzwerk (LAN) in das externe Netzwerk (WAN) geroutet werden (LAN --> WAN).

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

Intern / Extern / DMZ / Alle Externen

Gibt an, über welches Interface die Datenpakete ausgehen, damit sich die Regel auf sie bezieht.

„Alle Externen“ bezieht sich bei FL MGUARD 2000/4000-Geräten auf „Extern“.

Netzwerk >> NAT >> Maskierung [...]

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 der Einstellung „Extern“ die Ausgangsregeln (siehe „Ausgangsregeln“ auf Seite 214).

Beachten Sie bei der Einstellung „Intern“ die Eingangsregeln (siehe „Eingangsregeln“ auf Seite 211).

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 43).

Namen von IP-Gruppen, sofern definiert. Bei Angabe eines Namens einer IP-Gruppe werden die Hostnamen, IP-Adressen, IP-Bereiche oder Netzwerke berücksichtigt, die unter diesem Namen gespeichert sind (siehe „IP- und Portgruppen“ auf Seite 227).

Werden Hostnamen in IP-Gruppen verwendet, muss der mGuard so konfiguriert sein, dass der Hostname von einem DNS-Server in eine IP-Adresse aufgelöst werden kann.

Kann ein Hostname aus einer IP-Gruppe nicht aufgelöst werden, wird dieser Host bei der Regel nicht berücksichtigt. Weitere Einträge in der IP-Gruppe sind davon nicht betroffen und werden berücksichtigt.

Kommentar

Kann mit kommentierendem Text gefüllt werden.

1:1-NAT

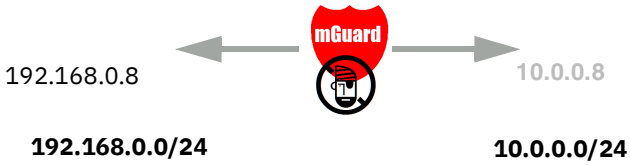
Listet die festgelegten Regeln für 1:1-NAT (Network Address Translation) auf.

Bei 1:1-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 realen Netzes in das virtuelle Netz spiegeln kann.

Netzwerk >> NAT >> Maskierung [...]

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 virtuellen Netz unter der IP-Adresse 10.0.0.8 erreichen.



Der mGuard beansprucht die für „Virtuelles Netzwerk“ angegebenen IP-Adressen für die Geräte in seinem „Realen Netzwerk“. Der mGuard antwortet stellvertretend für die Geräte aus dem „Realen Netzwerk“ mit ARP-Antworten zu allen Adressen aus dem angegebenen „Virtuellen Netzwerk“.

Die unter „Virtuelles Netzwerk“ angegebenen IP-Adressen müssen frei sein. Sie dürfen nicht für andere Geräte vergeben oder gar in Benutzung sein, weil sonst im virtuellen Netzwerk ein IP-Adressenkonflikt entsteht. Dies gilt selbst dann, wenn zu einer oder mehreren IP-Adressen aus dem angegebenen „Virtuellen Netzwerk“ gar kein Gerät im „Realen Netzwerk" existiert.

Standard: Es findet kein 1:1-NAT statt.

1:1-NAT wird nur im Netzwerk-Modus *Router* angewendet.

Reales Netzwerk

Die reale IP-Adresse des Clients, der aus einem anderen Netz über die virtuelle IP-Adresse erreichbar sein soll (je nach Szenario am LAN-, WAN- oder DMZ-Port).

Je nach Netzmaske können ein oder mehrere Clients erreichbar sein.

1:1-NAT ist zwischen allen Interfaces möglich (LAN <–> WAN, LAN <–> DMZ, DMZ <–> WAN).

Virtuelles Netzwerk

Die virtuelle IP-Adresse, über die die Clients aus dem anderen Netz erreichbar sind (je nach Szenario am LAN-, WAN- oder DMZ-Port).

Die virtuellen IP-Adressen dürfen nicht vergeben sein und von anderen Clients verwendet werden.

1:1-NAT ist zwischen allen Interfaces möglich (LAN <–> WAN, LAN <–> DMZ, DMZ <–> WAN).

Netzmaske

Die Netzmaske als Wert zwischen 1 und 32 für die lokale und externe Netzwerkadresse (siehe auch „CIDR (Classless Inter-Domain Routing)“ auf Seite 43).

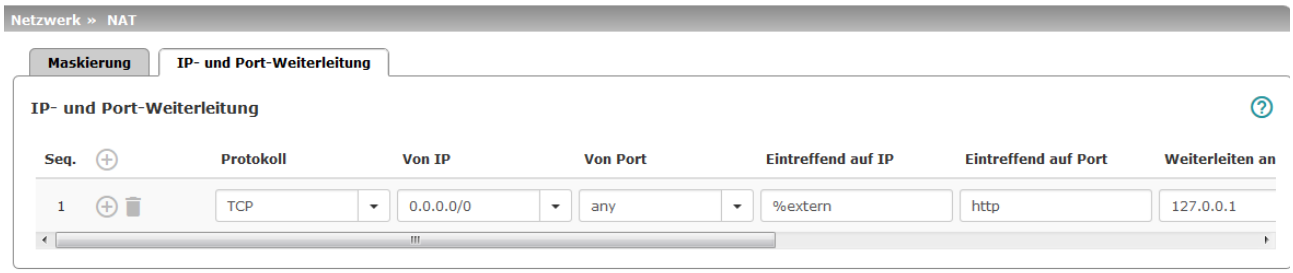
ARP aktivieren

Bei aktivierter Funktion werden ARP-Anfragen an das virtuelle Netzwerk stellvertretend vom mGuard beantwortet. Somit können Hosts, die sich im realen Netzwerk befinden, über ihre virtuelle Adresse erreicht werden.

Bei deaktivierter Funktion bleiben ARP-Anfragen an das virtuelle Netzwerk unbeantwortet. Hosts im realen Netzwerk sind dann nicht erreichbar.

Netzwerk >> NAT >> Maskierung [...]		
	Kommentar	Kann mit kommentierendem Text gefüllt werden.

5.3.2 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 IP- und 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.

Die IP- und Port-Weiterleitung aus dem internen Netz erfolgt analog zum oben beschriebenen Verhalten.

Die hier eingestellten Regeln haben gegenüber den Einstellungen unter „Netzwerksicherheit >> Paketfilter >> Eingangsregeln“ Vorrang.

IP- und Port-Weiterleitung kann im Netzwerk-Modus *Stealth* nicht verwendet werden.

Protokoll: TCP / UDP / GRE

Geben Sie hier das Protokoll an, auf das 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.

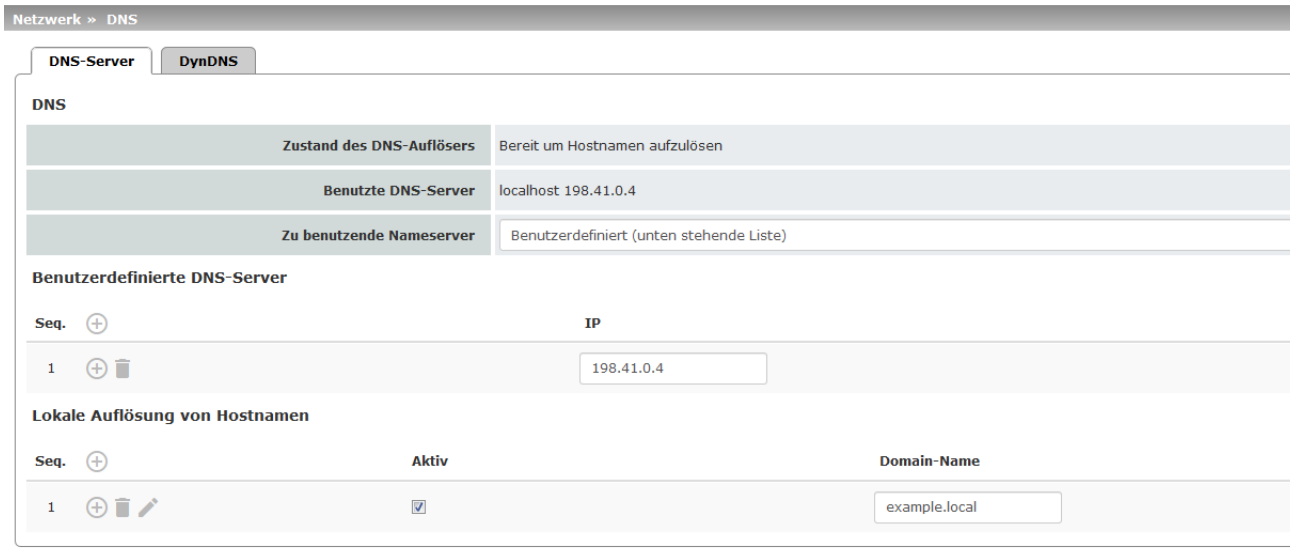
Netzwerk >> NAT >> IP- und Port-Weiterleitung [...]

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 43). **Namen von IP-Gruppen**, sofern definiert. **Bei Angabe des Namens einer IP-Gruppe werden** die Hostnamen, **IP-Adressen, IP-Bereiche oder Netzwerke berücksichtigt, die unter diesem Namen gespeichert sind (siehe „IP- und Portgruppen“ auf Seite 227).** Werden Hostnamen in IP-Gruppen verwendet, muss der mGuard so konfiguriert sein, dass der Hostname von einem DNS-Server in eine IP-Adresse aufgelöst werden kann. Kann ein Hostname aus einer IP-Gruppe nicht aufgelöst werden, wird dieser Host bei der Regel nicht berücksichtigt. Weitere Einträge in der IP-Gruppe sind davon nicht betroffen und werden berücksichtigt.
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. **Namen von Portgruppen**, sofern definiert. Bei Angabe des Namens einer Portgruppe werden die Ports oder Portbereiche berücksichtigt, die unter diesem Namen gespeichert sind (siehe „IP- und Portgruppen“ auf Seite 227).
Eintreffend auf IP	– Geben Sie hier die externe IP-Adresse (oder eine der externen IP-Adressen) des mGuards an, **oder** – geben Sie hier die interne IP-Adresse (oder eine der internen 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.

Netzwerk >> NAT >> IP- und Port-Weiterleitung [...]		
	Weiterleiten an IP	IP-Adresse, an die die Datenpakete weitergeleitet werden sollen und auf die die Original-Zieladressen umgeschrieben wird.
	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 - Funktion *Log* aktivieren – oder nicht - Funktion *Log* deaktivieren (Standard).

5.4 Netzwerk >> DNS

5.4.1 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. **Zustand des DNS-Auflösers** — Status der Auflösung des Hostnamens **Benutzte DNS-Server** — DNS-Server, bei denen die zugehörige IP-Adresse erfragt wurde.

Netzwerk >> DNS >> DNS-Server [...]		
	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 (d. h. via DHCP)** Es werden die DNS-Server des Internet Service Providers (ISP) benutzt, der den Zugang zum Internet zur Verfügung stellt. Wählen Sie diese Einstellung nur dann, wenn der mGuard im *Router*-Modus mit DHCP arbeitet. Die Einstellung kann ebenfalls verwendet werden, wenn der mGuard sich im ***Stealth*-Modus (*Automatisch*)** befindet. In diesem Fall wird der DNS-Server, den der Client verwendet, erkannt und übernommen. **Benutzerdefiniert (unten stehende Liste)** Ist diese Einstellung gewählt, nimmt der mGuard mit den DNS-Servern Verbindung auf, die in der Liste *Benutzerdefinierte DNS-Server* aufgeführt sind.
Benutzerdefinierte DNS-Server (Nur wenn als Nameserver **Benutzerdefiniert** ausgewählt wurde)	In dieser Liste können Sie die IP-Adressen von DNS- Servern erfassen. Sollen diese vom mGuard benutzt werden, muss oben unter **Zu benutzende Nameserver** die Option **„Benutzerdefiniert (unten stehende Liste)“** eingestellt sein. Ab Firmwareversion 10.3.0 gilt: Die IP-Adressen, die bereits einem Netzwerk-Interface des mGuards zugeordnet sind (Extern / Intern / DMZ), dürfen an dieser Stelle nicht verwendet werden. Updates und der Import von Profilen älterer Firmwareversionen, die entsprechend konfiguriert sind, werden abgelehnt.	
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.	

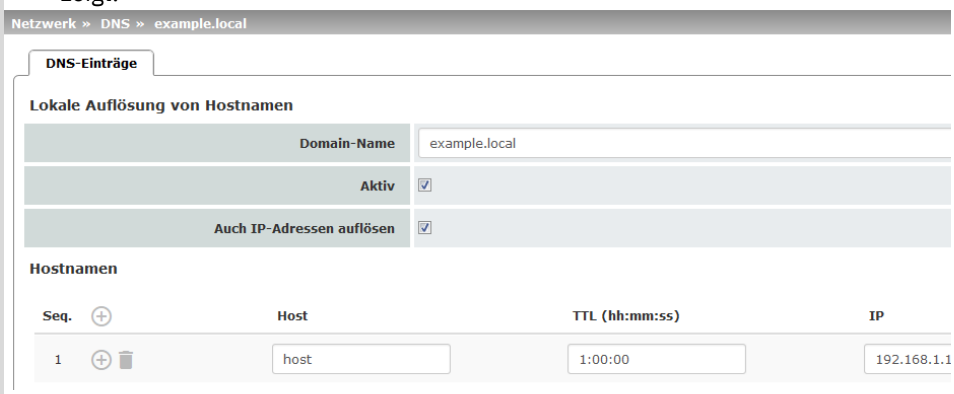
Netzwerk >> DNS >> DNS-Server [...]

Tabelle mit Zuordnungspaaren für eine Domain anlegen:

- Eine neue Zeile öffnen und in dieser auf das Icon **Zeile bearbeiten** klicken.

Zuordnungspaare, die zu einer Domain gehören, ändern oder löschen:

- In der betreffenden Tabellenzeile auf das Icon **Zeile bearbeiten** klicken.
  Nach Klicken auf **Zeile bearbeiten** wird die Registerkarte für *DNS-Einträge* angezeigt:



Domain-Name
Der Name kann frei vergeben werden, muss aber den Regeln für die Vergabe von Domain-Namen folgen. Wird jedem Hostnamen zugeordnet.

Aktiv
Aktiviert oder deaktiviert die Funktion *Lokale Auflösung von Hostnamen* für die im Feld „Domain-Name“ angegebene Domain.

Auch IP-Adressen auflösen
Deaktiviert: Der mGuard löst nur Hostnamen auf, d. h. liefert zu Hostnamen die zugeordnete IP-Adresse.

Aktiviert: Wie bei „Deaktiviert“. 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.

Host
Hostname

TTL (hh:mm:ss)
Standard: 3600 Sekunden (1:00:00)

Abkürzung für **T**ime **T**o **L**ive

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.

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.

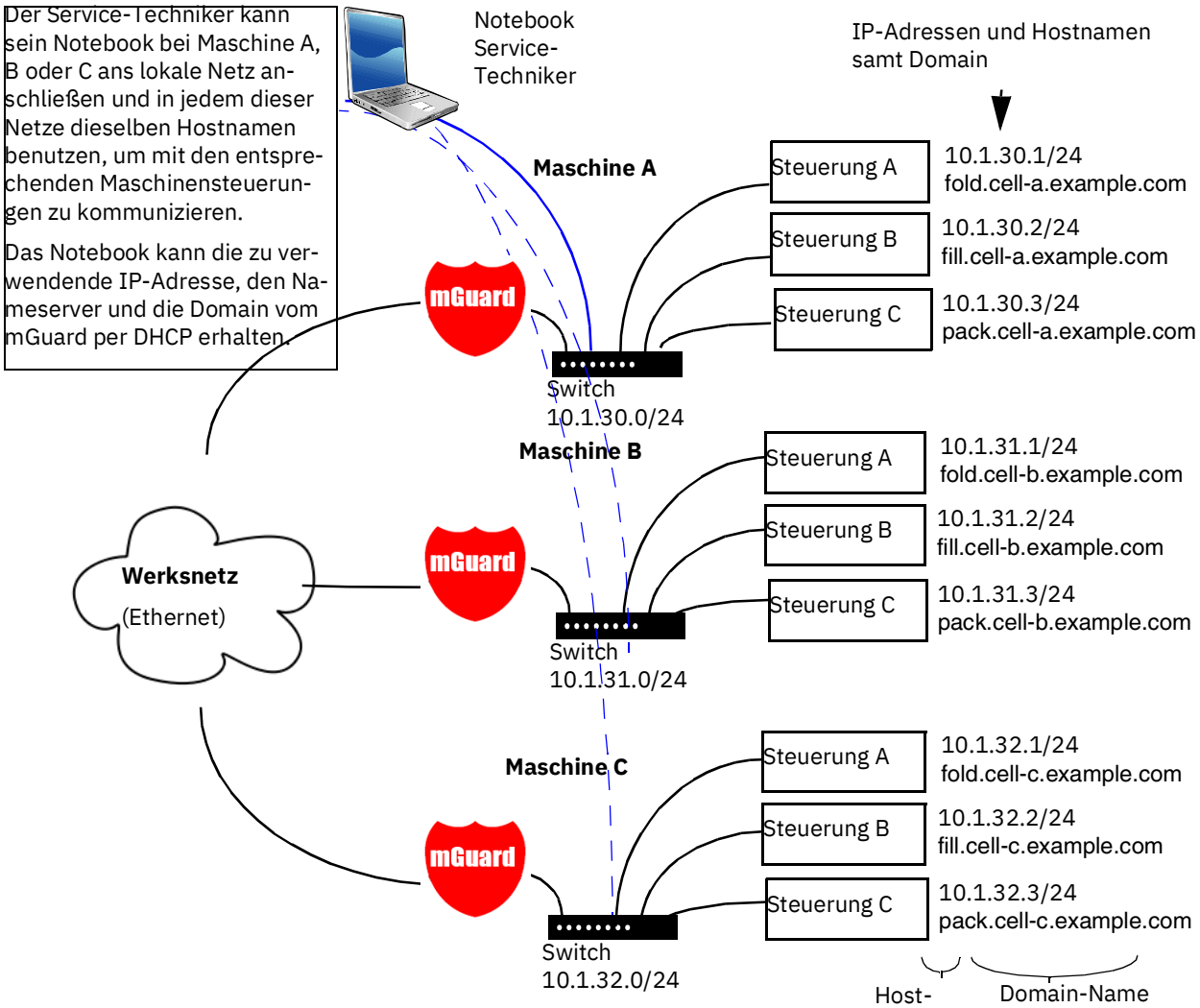
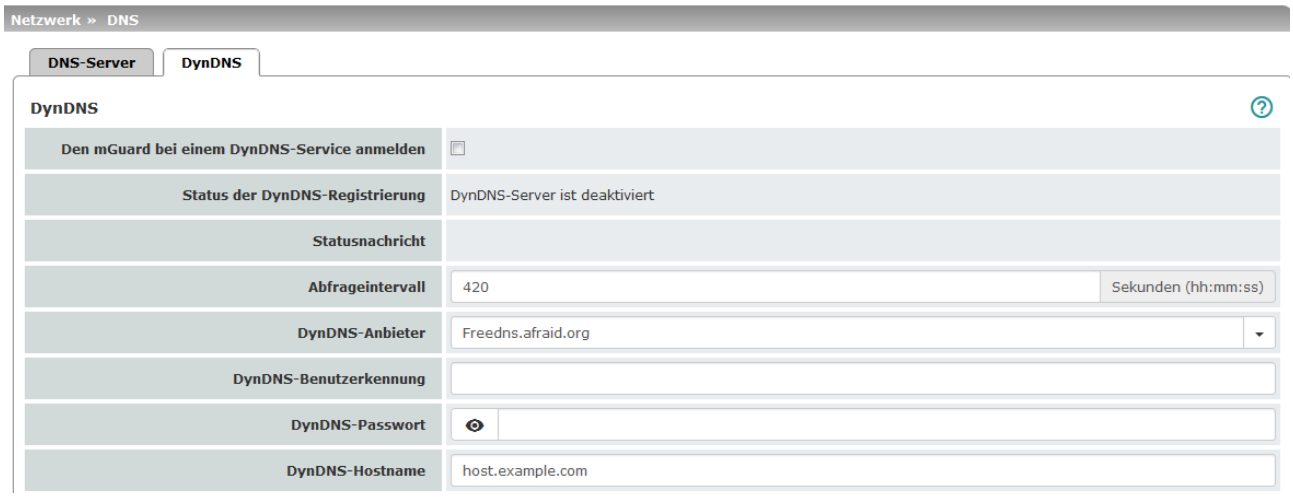


Bild 5-1 Lokale Auflösung von Hostnamen

5.4.2 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.

Wenn Sie für einen vom mGuard unterstützten DynDNS-Service registriert sind, können Sie in diesem Dialogfeld die entsprechenden Angaben machen.

Den mGuard bei einem DynDNS-Server anmelden	Aktivieren Sie die Funktion, 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.
Status der DynDNS-Registrierung	Status der DynDNS-Registrierung
Statusnachricht	Statusnachricht
Abfrageintervall	**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. Zusätzlich kann diese Meldung in dem hier festgelegten Zeitintervall erfolgen. 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.

Netzwerk >> DNS >> DynDNS [...]		
	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. Wenn Ihr Anbieter nicht in der Liste enthalten ist, wählen Sie **DynDNS-compatible** und tragen Sie Server und Port für diesen Anbieter ein.
	DynDNS-Server	Nur sichtbar, wenn unter „DynDNS-Anbieter“ **DynDNS-compatible** eingestellt ist. Name des Servers des DynDNS-Anbieters.
	DynDNS-Port	Nur sichtbar, wenn unter „DynDNS-Anbieter“ **DynDNS-compatible** eingestellt ist. Nummer des Ports des DynDNS-Anbieters.
	DynDNS-Benutzerkennung	Geben Sie hier die Benutzerkennung ein, die Ihnen vom DynDNS-Anbieter zugeteilt worden ist.
	DynDNS-Passwort	Geben Sie hier 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.

5.5 Netzwerk >> DHCP

Mit dem Dynamic Host Configuration Protocol (DHCP) kann den direkt am mGuard angeschlossenen Rechnern 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). Unter **DMZ DHCP** können DHCP-Einstellungen für das DMZ-Interface (DMZ-Port) vorgenommen werden.

In den Werkseinstellungen ist der DHCP-Server des mGuard-Geräts standardmäßig für das LAN-Interface (Port XF2-4 bzw. XF2-5) aktiviert (Internes DHCP).

Das heißt, dass über das LAN-Interface angeschlossene Netzwerk-Clients ihre Netzwerkkonfiguration automatisch vom mGuard-Gerät erhalten, wenn sie ebenfalls DHCP aktiviert haben.

Die Menüpunkte **Externes DHCP** und **DMZ DHCP** gehören nicht zum Funktionsumfang der Serie FL MGUARD 2000.

Der DHCP-Server funktioniert auch im *Stealth*-Modus.

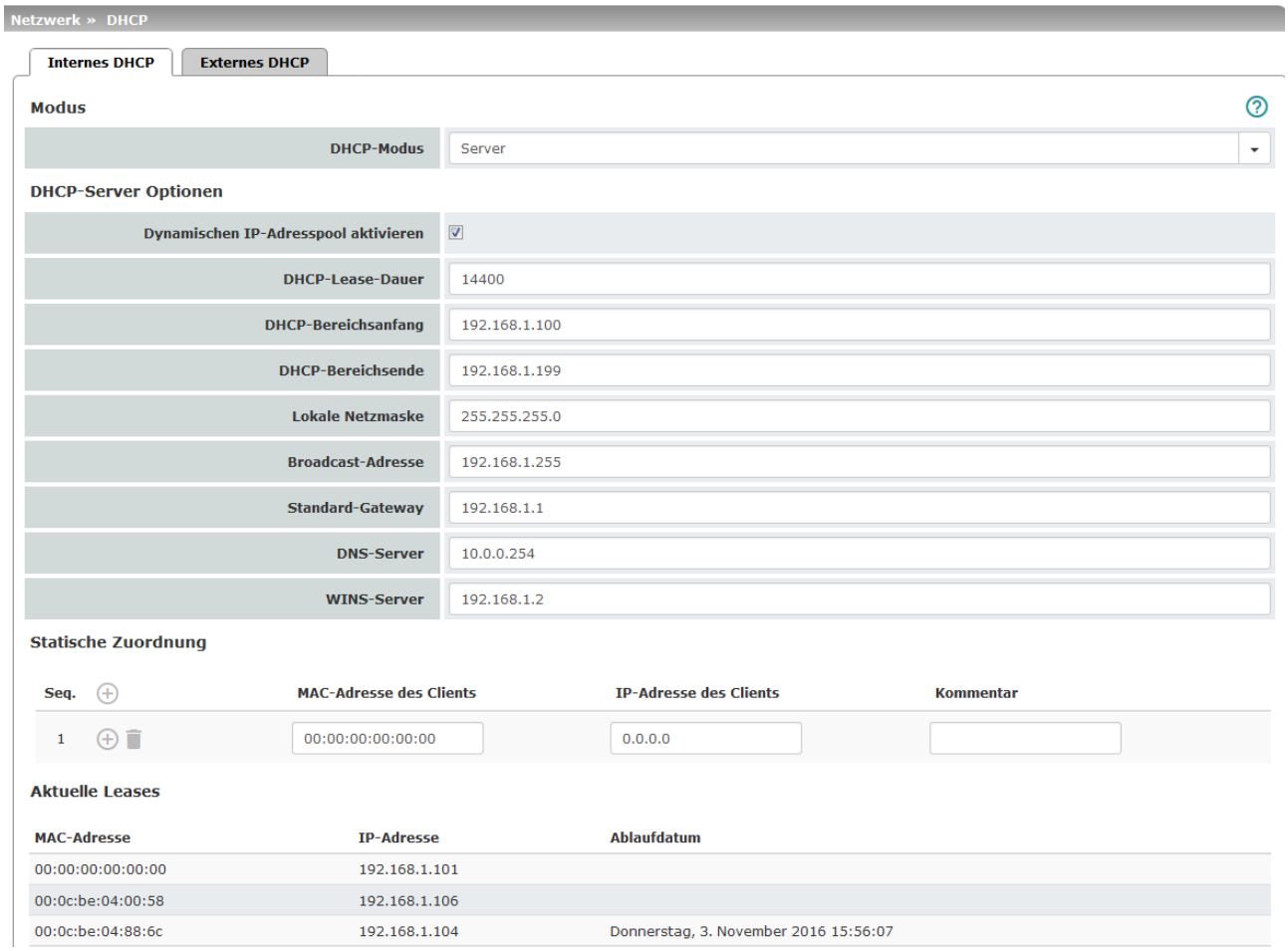
Im Multi-Stealth-Mode kann der externe DHCP-Server des mGuards nicht genutzt werden, wenn eine VLAN ID als Management IP zugewiesen ist.

IP-Konfiguration bei Windows-Rechnern: Wenn Sie den DHCP-Server des mGuards starten, können Sie die lokal angeschlossenen Rechner so konfigurieren, dass diese ihre IP-Konfiguration automatisch per DHCP vom mGuard zugeteilt bekommen.

Siehe hierzu auch das Kapitel „IP-Einstellung per DHCP beziehen (Windows)“ im Benutzerhandbuch UM DE HW FL MGUARD 2000/4000 „Installation und Inbetriebnahme“ im Phoenix Contact Web Shop z. B. unter phoenixcontact.com/product/1357828).

5.5.1 Internes / Externes DHCP

Der Menüpunkt **Externes DHCP** gehört nicht zum Funktionsumfang der Serie FL MGUARD 2000.

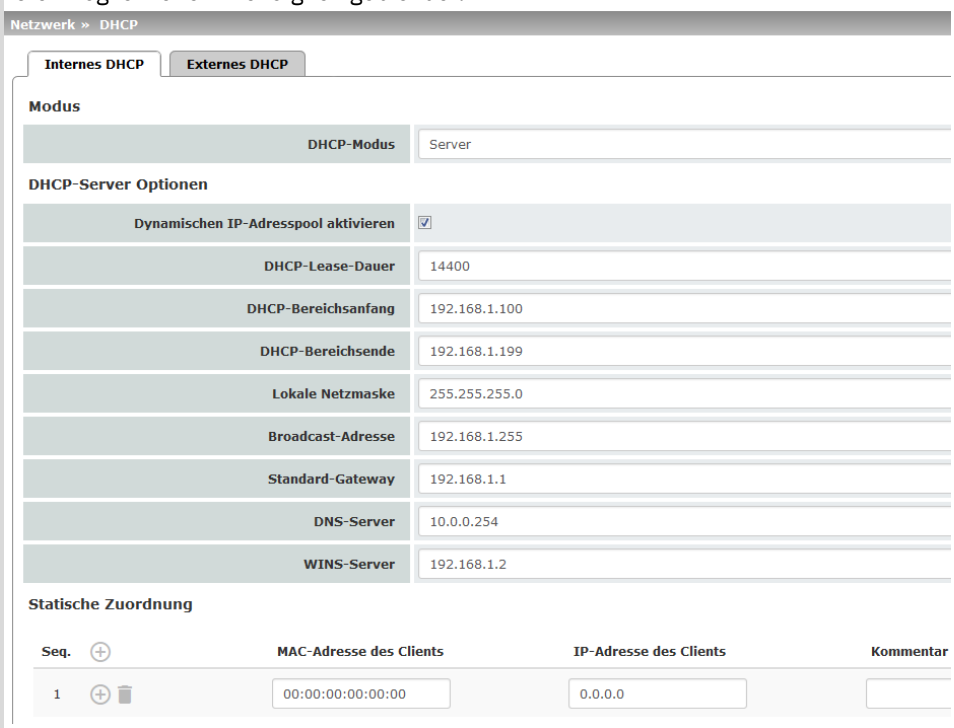


Netzwerk >> DHCP >> Internes DHCP

Die Einstellungen für **Internes DHCP** und **Externes DHCP** sind prinzipiell identisch und werden im Folgenden nicht getrennt beschrieben.

Netzwerk >> DHCP >> Internes DHCP[...]		
Modus	**DHCP-Modus**	**Deaktiviert / Server / Relay** Setzen Sie diesen Schalter auf **Server** (Werkseinstellungen: Internes DHCP), wenn der mGuard als eigenständiger DHCP-Server arbeiten soll. Dann werden unten auf der Registerkarte entsprechende Einstellmöglichkeiten eingeblendet (siehe „DHCP-Modus: **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 „DHCP-Modus: **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**	Bei aktivierter Funktion wird der durch *DHCP-Bereichsanfang* bzw. *DHCP-Bereichsende* angegebenen IP-Adresspool verwendet (siehe unten). Deaktivieren Sie die Funktion, wenn nur statische Zuweisungen anhand der MAC-Adressen vorgenommen werden sollen (siehe unten).
	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.
	DHCP-Bereichsanfang (Bei aktiviertem dynamischen IP-Adresspool)	Anfang Adressbereichs, aus dem der DHCP-Server des mGuards den lokal angeschlossenen Rechnern IP-Adressen zuweisen soll.
	DHCP-Bereichsende (Bei aktiviertem dynamischen IP-Adresspool)	Ende des Adressbereichs, aus dem der DHCP-Server des mGuards den lokal angeschlossenen Rechnern IP-Adressen zuweisen soll.
	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	**MAC-Adresse des Clients**	Die **MAC-Adresse** Ihres Rechners finden Sie wie folgt heraus: **Windows**: • 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. Bei den Angaben haben Sie folgende Möglichkeiten: – MAC-Adresse des Clients/Rechners (ohne Leerzeichen oder Bindestriche).

Netzwerk >> DHCP >> Internes DHCP[...]

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.

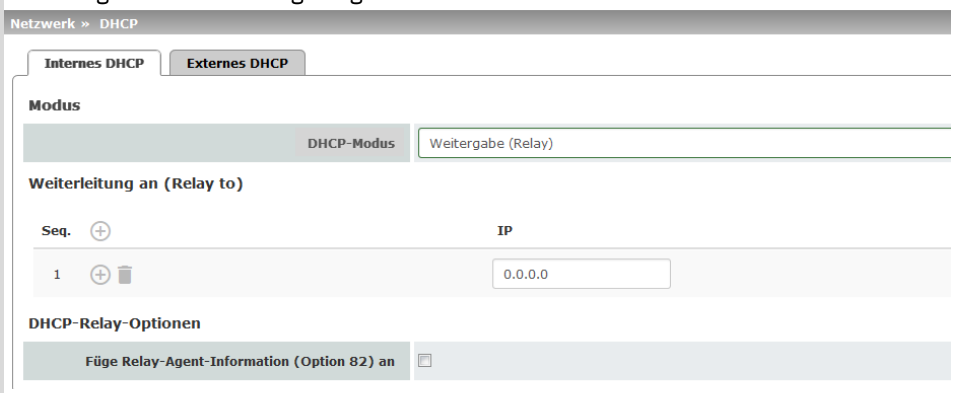
Es sollte nur ein DHCP-Server pro Subnetz verwendet werden.

Aktuelle Leases

Die aktuell vom DHCP-Server vergebenen Leases werden mit MAC-Adresse, IP-Adresse und Ablaufdatum (Timeout) angezeigt.

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

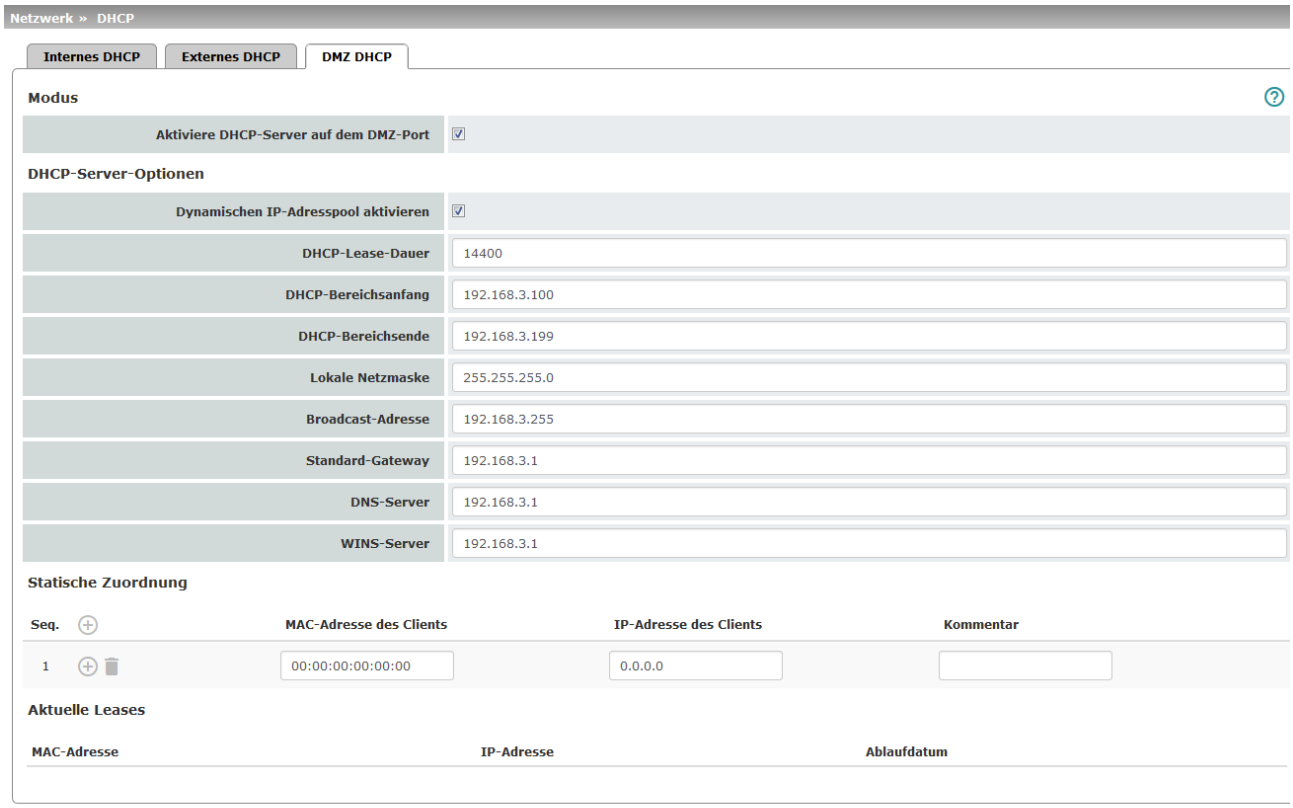
Eine Liste von einem oder mehreren DHCP-Servern, an welche DHCP-Anfragen weitergeleitet werden sollen.

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.

5.5.2 DMZ DHCP

Der Menüpunkt **DMZ DHCP** gehört nicht zum Funktionsumfang der Serie FL MGUARD 2000.



Die DHCP-Server-Funktionalität des mGuards wurde auf sein DMZ-Interface (DMZ-Port) erweitert. Der mGuard kann am DMZ-Port angeschlossenen Clients automatisch eine Netzwerkkonfiguration über das DHCP-Protokoll zuweisen.

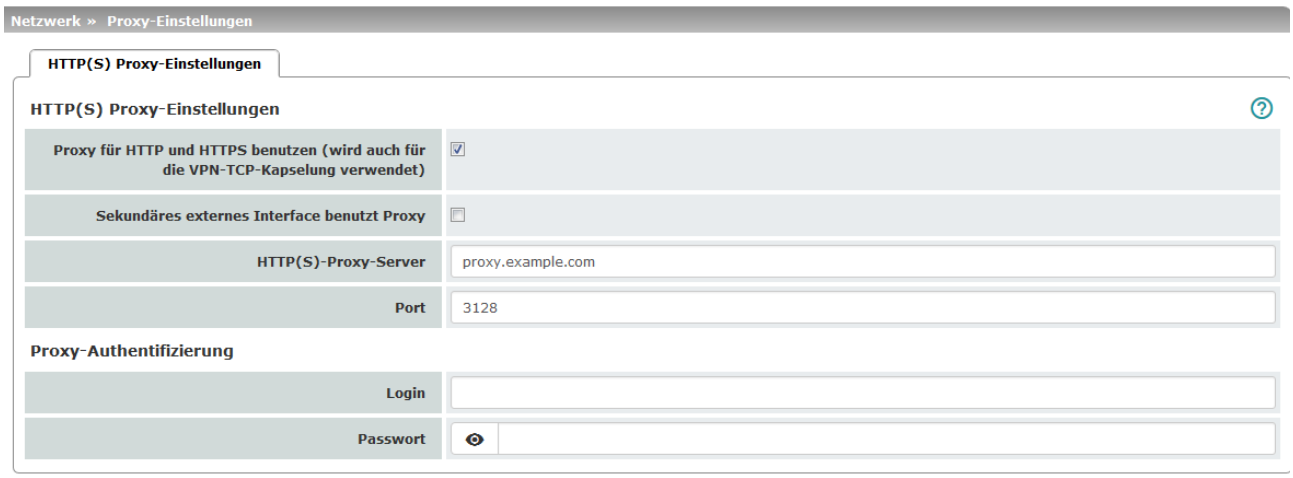
Netzwerk >> DHCP >> DMZ DHCP		
Modus	**Aktiviere DHCP-Server auf dem DMZ-Port**	Aktiviert den DHCP-Server auf dem DMZ-Interface. Bei deaktivierter Funktion beantwortet der mGuard keine DHCP-Anfragen auf dem DMZ-Interface.
DHCP-Server-Optionen	**Dynamischen IP-Adresspool aktivieren**	Bei aktivierter Funktion wird der durch *DHCP-Bereichsanfang* bzw. *DHCP-Bereichsende* angegebenen IP-Adresspool verwendet (siehe unten). Deaktivieren Sie die Funktion, wenn nur statische Zuweisungen anhand der MAC-Adressen vorgenommen werden sollen (siehe unten).

Netzwerk >> DHCP >> DMZ DHCP[...]		
	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.
	DHCP-Bereichsanfang (Bei aktiviertem dynamischen IP-Adresspool)	Anfang Adressbereichs, aus dem der DHCP-Server des mGuards den lokal angeschlossenen Rechnern IP-Adressen zuweisen soll.
	DHCP-Bereichsende (Bei aktiviertem dynamischen IP-Adresspool)	Ende des Adressbereichs, aus dem der DHCP-Server des mGuards den lokal angeschlossenen Rechnern IP-Adressen zuweisen soll.
	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	**MAC-Adresse des Clients**	Die **MAC-Adresse** Ihres Rechners finden Sie wie folgt heraus: **Windows** : • 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. Bei den Angaben haben Sie folgende Möglichkeiten: – MAC-Adresse des Clients/Rechners (ohne Leerzeichen oder Bindestriche). – IP-Adresse des Clients

Netzwerk >> DHCP >> DMZ DHCP[...]		
	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.
Aktuelle Leases	Die aktuell vom DHCP-Server vergebenen Leases werden mit MAC-Adresse, IP-Adresse und Ablaufdatum (Timeout) angezeigt.	

5.6 Netzwerk >> Proxy-Einstellungen

5.6.1 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

Netzwerk >> Proxy-Einstellungen >> HTTP(S) Proxy-Einstellungen		
HTTP(S) Proxy-Einstellungen	**Proxy für HTTP und HTTPS benutzen**	Bei aktivierter Funktion gehen Verbindungen, bei denen das Protokoll HTTP oder HTTPS verwendet wird, über einen Proxy-Server, dessen Adresse und Port ebenfalls festzulegen sind. Verbindungen, die mittels der Funktion **VPN-TCP-Kapselung** gekapselt übertragen werden, werden ebenfalls über den Proxy-Server geleitet (siehe „TCP-Kapselung“ auf Seite 253). Verwendet der Proxy-Server die Authentifizierungsmethode „Digest“, können vom mGuard-Gerät initiierte VPN-Verbindungen, die TCP-Kapselung oder „Path Finder“ verwenden, nicht aufgebaut werden. Verwenden Sie stattdessen „Basic“-Authentifizierung auf dem Proxy-Server.
	HTTP(S)-Proxy-Server	Hostname oder IP-Adresse des Proxy-Servers
	Port	Nummer des zu verwendenden Ports, z. B. 3128
Proxy-Authentifizierung	**Login**	Benutzerkennung (Login) zur Anmeldung beim Proxy-Server
	Passwort	Passwort zur Anmeldung beim Proxy-Server

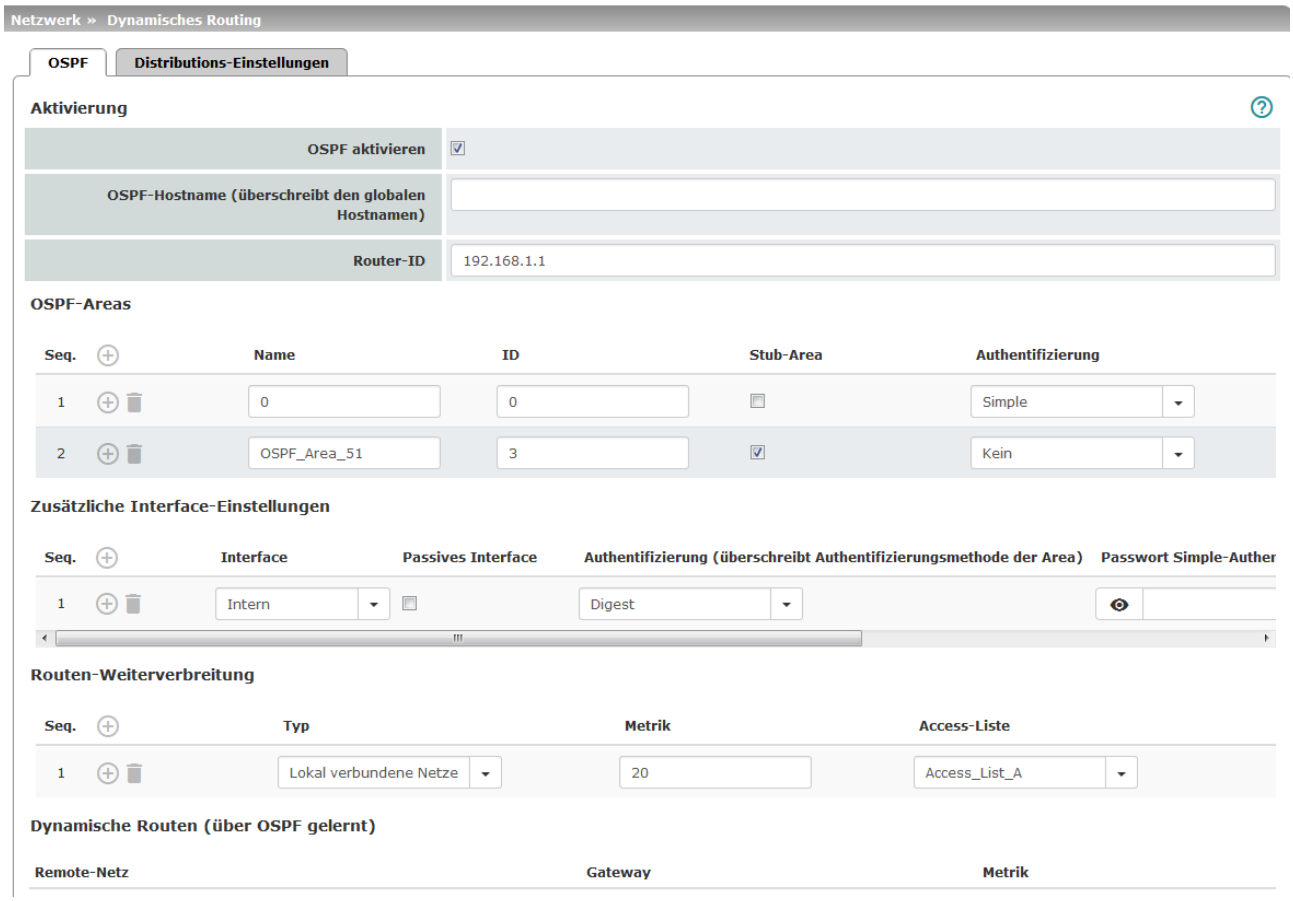
5.7 Netzwerk >> Dynamisches Routing

In größeren Firmennetzwerken kann die Verwendung von dynamischen Routing-Protokollen dem Netzwerkadministrator das Anlegen und Verwalten von Routen erleichtern bzw. abnehmen.

Das Routing-Protokoll **OSPF** (*Open Shortest Path First*) ermöglicht den teilnehmenden Routern, die Routen zur Übertragung von IP-Paketen in ihrem autonomen Netz in Echtzeit (dynamisch) untereinander auszutauschen und anzupassen. Dabei wird die jeweils beste Route zu jedem Subnetz für alle teilnehmenden Router ermittelt und in die Routingtabellen der Geräte eingetragen. Änderungen in der Netzwerktopologie werden automatisch jeweils an die benachbarten OSPF-Router gesendet und von diesen letztendlich an alle teilnehmenden OSPF-Router weiterverbreitet.

Dieses Menü steht nur zur Verfügung, wenn sich der mGuard im Netzwerkmodus „Router“ befindet.

5.7.1 OSPF



OSPF lässt sich für interne, externe und DMZ-Interfaces konfigurieren. Die Unterstützung von OSPF via IPsec und GRE ist aktuell nicht gegeben.

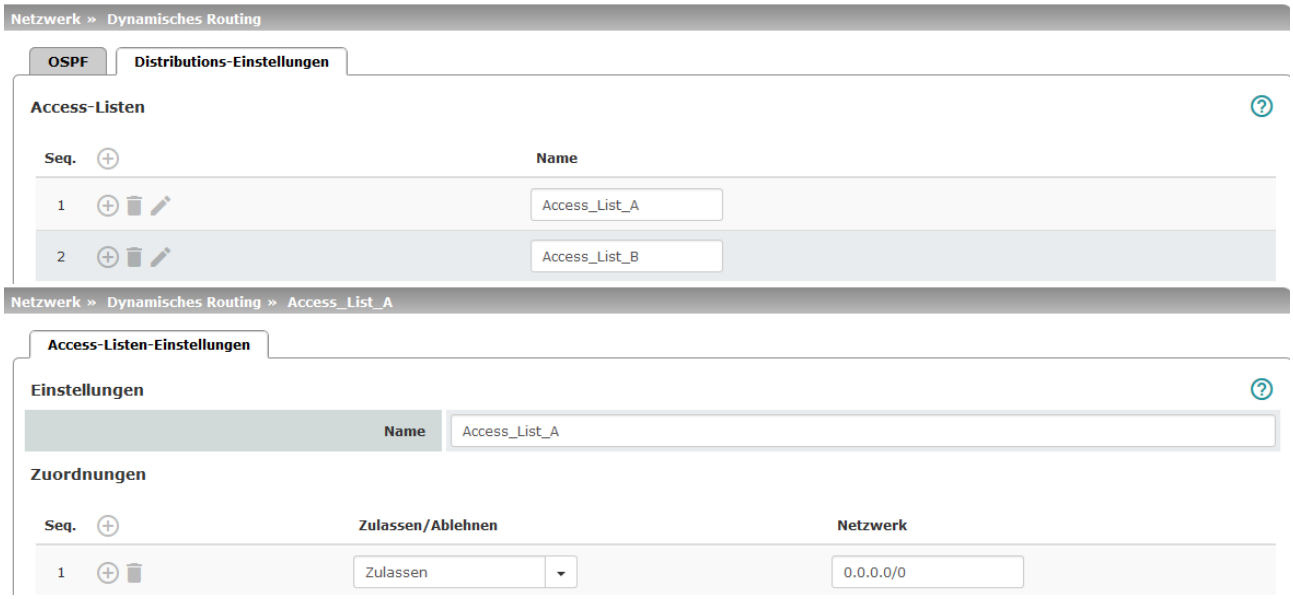
Es können mehrere OSPF-Areas konfiguriert werden, um lokale Routen weiterzuverbreiten und externe Routen zu lernen. Der Status aller gelernten Routen wird in einer Tabelle angezeigt.

Netzwerk >> Dynamisches Routing >> OSPF		
Aktivierung	**OSPF aktivieren**	Bei deaktivierter Funktion (Werkseinstellung): OSPF ist auf dem Gerät deaktiviert. Bei aktivierter Funktion: Das dynamische Routing über das OSPF-Protokoll ist auf dem Gerät aktiviert. Neue Routen können von benachbarten OSPF-Routern gelernt und weiterverbreitet werden.
	OSPF-Hostname	Wenn an dieser Stelle ein **OSPF-Hostname** vergeben wird, wird dieser den teilnehmenden OSPF-Routern anstelle des globalen Hostnamens mitgeteilt.
	Router-ID	Die **Router-ID** im Format einer IP-Adresse muss innerhalb des autonomen Systems eindeutig sein. Sie kann ansonsten frei gewählt werden und entspricht üblicherweise der IP-Adresse der WAN- oder LAN-Schnittstelle des mGuards.
OSPF-Areas	Über **OSPF-Areas** wird das autonome System segmentiert. Innerhalb einer Area werden die Routen zwischen OSPF-Routern ausgetauscht. Der mGuard kann Mitglied in einer oder mehreren OSPF-Areas sein. Eine Weiterverbreitung zwischen benachbarten Areas über die sogenannte „Transition Area“ ist ebenfalls möglich (siehe unten).	
	Name	Der **Name** ist frei wählbar (Standard: ID). Die eigentliche Identifizierung eines OSPF-Routers erfolgt anhand seiner ID.
	ID	Die **ID** ist prinzipiell frei wählbar. Wird einer OSPF-Area die ID 0 zugewiesen, wird sie damit zur „**Transition Area**“. Über diese werden Routing-Informationen zwischen zwei benachbarten Areas ausgetauscht und in diesen weiterverbreitet.
	Stub-Area	Wenn es sich bei der OSPF-Area um eine Stub-Area handelt, aktivieren Sie die Funktion.
	Authentifizierung	**Kein / Simple / Digest** Die Authentifizierung des mGuards innerhalb der OSPF-Area kann über die Methoden „Simple“ oder „Digest“ erfolgen. Die entsprechenden Passwörter bzw. Digest-Keys werden jeweils für die zugeordneten Interfaces vergeben (siehe „Zusätzliche Interface- Einstellungen“).
Zusätzliche Interface- Einstellungen	**Interface**	**Intern / Extern / DMZ** Wählt das Interface aus, für das die Einstellungen gelten. Werden an dieser Stelle keine Einstellungen vorgenommen, gelten die Standard-Einstellungen (d. h. OSPF ist für das Interface aktiv und die Passwörter sind nicht vergeben).

Netzwerk >> Dynamisches Routing >> OSPF		
	Passives Interface	**Standard: deaktiviert** Bei deaktivierter Funktion werden OSPF-Routen durch das Interface gelernt und weiterverbreitet. Bei aktivierter Funktion werden Routen weder gelernt noch weiterverbreitet.
	Authentifizierung	**Kein / Digest** Ist **Digest** ausgewählt, wird an dem ausgewählten Interface – unabhängig von der einer OSPF-Area bereits zugewiesenen Authentifizierungsmethode – immer mit „Digest“ authentifiziert. Die Authentifizierungsmethode (Kein / Simple / Digest), die bereits einer **OSPF-Area** zugewiesen wurde, wird dabei übergangen und nicht verwendet.
	Passwort Simple-Authentifizierung	Passwort zur Authentifizierung des OSPF-Routers (bei Authentifizierungsmethode „Simple“)
	Digest-Key	Digest-Key zur Authentifizierung des OSPF-Routers (bei Authentifizierungsmethode „Digest“)
	Digest-Key-ID	Digest-Key-ID zur Authentifizierung des OSPF-Routers (bei Authentifizierungsmethode „Digest“) (1–255)
Routen-Weiterverbreitung	Statisch in der Routingtabelle des Kernels eingetragene Routen können ebenfalls über OSPF weiterverbreitet werden. Es können Regeln für lokal verbundene und über Gateway erreichbare Netze angelegt werden. Die Netze, deren Routen über OSPF weiterverbreitet werden sollen, können über die „Distributions-Einstellungen“ in den sogenannten „Access-Listen“ festgelegt werden. Per Default ist für lokal verbundene und über Gateway erreichbare Netze keine Access-Liste ausgewählt. D. h., alle entsprechenden Routen in der Kernel-Routing-Tabelle werden über OSPF weiterverbreitet, wenn eine Regel und die Funktion OSPF aktiviert sind.	
	Typ	**Lokal verbundene Netze / Über Gateway erreichbare Netze** **Lokal verbundene Netze**: Alle lokalen Netze werden per OSPF weiterverbreitet, wenn OSPF aktiviert ist. Eine Einschränkung der Weiterverbreitung kann über Access-Listen erfolgen. **Über Gateway erreichbare Netze**: Alle externen Netze werden per OSPF weiterverbreitet. Zu den externen Netzen gehören z. B. statische sowie IPsec- und OpenVPN-Remote-Netze. Eine Einschränkung der Weiterverbreitung kann über Access-Listen erfolgen.
	Metrik	Metrik, mit der die Routen weiterverbreitet werden. Numerisches Maß für die Güte einer Verbindung bei Verwendung einer bestimmten Route (abhängig von Bandbreite, Hop-Anzahl, Kosten und MTU).

Netzwerk >> Dynamisches Routing >> OSPF		
	Access-Liste	Verbreitet die Routen entsprechend der ausgewählten Access-Liste weiter (siehe „Distributions-Einstellungen“). Ist **Kein** ausgewählt, werden alle Routen des ausgewählten Typs weiterverbreitet.
Dynamische Routen (über OSPF gelernt)	Der Status aller über OSPF gelernten Routen wird angezeigt.	
	Remote-Netz	Dynamisch gelerntes Remote-Netz.
	Gateway	Gateway zum Erreichen des Remote-Netzes.
	Metrik	Die Metrik der gelernten Route.

5.7.2 Distributions-Einstellungen



Dynamische Routen werden über das OSPF-Protokoll automatisch verbreitet. Für statisch in der Routingtabelle des Kernels eingetragene Routen muss jeweils festgelegt werden, ob diese ebenfalls über OSPF weiterverbreitet werden sollen.

Ist eine Regel für einen der beiden Typen „Lokal verbundene Netze“ und „Über Gateway erreichbare Netze“ ausgewählt, werden standardmäßig (Access-Liste = Kein) alle entsprechenden Routen über OSPF weiterverbreitet, wenn OSPF aktiviert ist.

Über die Distributions-Einstellungen können Regeln angelegt werden, die festlegen, welche nicht dynamisch gelernten Routen über OSPF weiterverbreitet werden. Dazu gehören:

– lokal konfigurierte Netze (siehe „Netzwerk >> Interfaces“ auf Seite 129)
– statische Routen, die als Externe, Interne oder DMZ-Netzwerke eingetragen sind (siehe „Netzwerk >> Interfaces“ auf Seite 129)
– Routen, die über OpenVPN in die Kernel-Routing-Tabelle eingetragen werden (siehe „Menü OpenVPN-Client“ auf Seite 305)

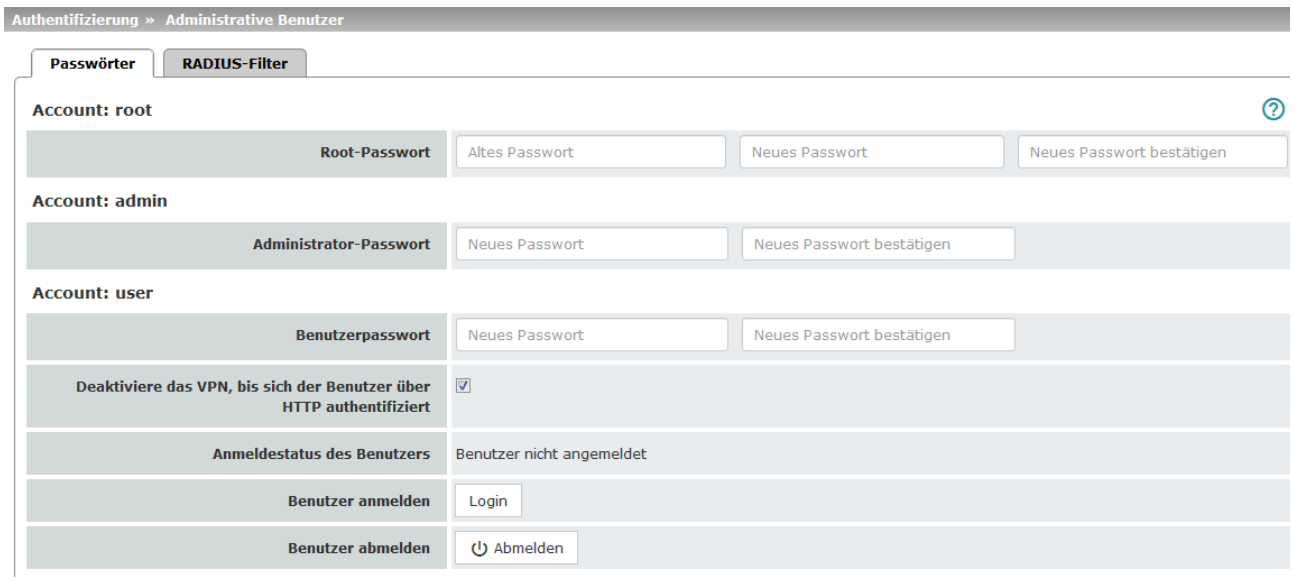
Netzwerk >> Dynamisches Routing >> Distributions-Einstellungen >> Editieren >> Access-Listen-Einstellungen		
Einstellungen	**Name**	Der **Name** muss eindeutig sein, darf also nicht doppelt vergeben werden.
Zuordnungen	**Zulassen/Ablehnen**	Listet die Access-Listen-Regeln auf. Diese gelten für nicht dynamisch über OSPF verbreitete Routen. **Zulassen** (Werkseinstellung) bedeutet, die Route zu dem eingetragenen Netzwerk wird über OSPF weiterverbreitet. **Ablehnen** bedeutet, die Route zum eingetragenen Netzwerk wird nicht über OSPF weiterverbreitet.
	Netzwerk	**Netzwerk**, dessen Weiterverbreitung per Regel zugelassen oder abgelehnt wird.

6 Menü Authentifizierung

6.1 Authentifizierung >> Administrative Benutzer

ACHTUNG: Voreingestellte Passwörter bei der Erstanmeldung ändern.
Ändern Sie bei der Erstinbetriebnahme des Geräts umgehend die voreingestellten Administrator-Passwörter für die Benutzer *root* und *admin*.

6.1.1 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

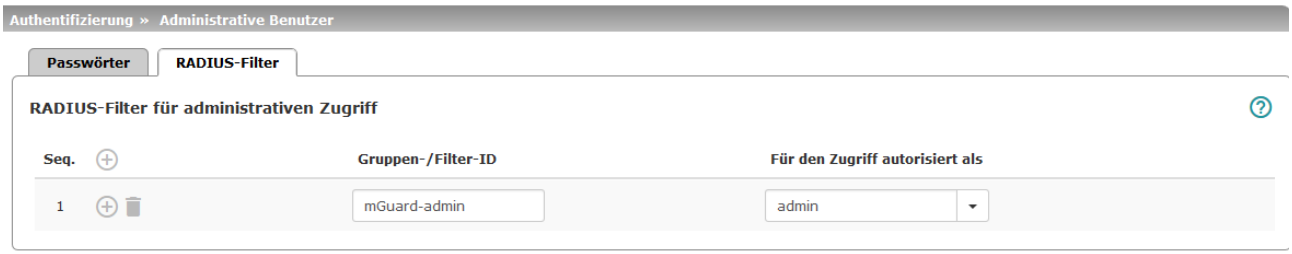
Um sich auf der entsprechenden Stufe anzumelden, muss der Benutzer das Passwort angeben, das der jeweiligen Berechtigungsstufe (*root*, *admin*, *user*) zugeordnet ist.

ACHTUNG: Verwenden Sie sichere Passwörter!
Erstellen und verwenden Sie nur sichere und komplexe Passwörter, wie vom National Institute of Standards and Technology (NIST) beschrieben (pages.nist.gov/800-63-3/sp800-63b.html)

Wenn Sie Passwörter ändern, sollten Sie den mGuard anschließend neu starten, um bestehende Sitzungen mit nicht mehr gültigen Passwörtern sicher zu beenden.

Authentifizierung >> Administrative Benutzer >> Passwörter [...]		
Account: root	**Root-Passwort**	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 folgenden Felder das neue gewünschte Passwort.
Accout: admin	**Administrator-Passwort**	Bietet die Rechte für die Konfigurationsoptionen, die über die Web-basierte Administratoroberfläche zugänglich sind. Benutzername (nicht änderbar): **admin** Voreingestelltes Passwort: **mGuard**
Account: user	**Benutzerpasswort**	Werkseitig ist kein Benutzerpasswort voreingestellt. Um eins festzulegen, geben Sie in beide Eingabefelder übereinstimmend das gewünschte Passwort ein.
	Deaktiviere das VPN, bis sich der Benutzer über HTTPS authentifiziert	Ist ein Benutzerpasswort festgelegt und aktiviert, dann muss der Benutzer nach jedem Neustart des mGuards bei Zugriff auf eine beliebige HTTPS-URL dieses Passwort angeben, **damit die VPN-Verbindungen des mGuards aktiviert werden**. Werkseitig ist die Funktion deaktiviert. Bei aktivierter Funktion können VPN-Verbindungen erst dann genutzt werden, wenn sich ein Benutzer mittels HTTPS gegenüber dem mGuard ausgewiesen hat. Alle HTTPS-Verbindungen werden auf den mGuard umgeleitet, solange die Authentifizierung erforderlich ist. Die Änderung dieser Option wird erst mit dem nächsten Neustart aktiv. Wollen Sie diese Option nutzen, legen Sie im entsprechenden Eingabefeld das Nutzerpasswort fest.
	Anmeldestatus des Benutzers	Zeigt an, ob der Benutzer an- oder abgemeldet ist.
	Benutzer anmelden	Um den Benutzer anzumelden, klicken Sie auf die Schaltfläche **Login**.
	Benutzer abmelden	Um den Benutzer anzumelden, klicken Sie auf die Schaltfläche **Abmelden**.

6.1.2 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.

Wenn Sie Passwörter ändern oder Änderungen am Authentifizierungsverfahren vornehmen, sollten Sie den mGuard anschließend neu starten, um bestehende Sitzungen mit nicht mehr gültigen Zertifikaten oder Passwörtern sicher zu beenden.

ACHTUNG: Verwenden Sie sichere Passwörter!

Erstellen und verwenden Sie nur sichere und komplexe Passwörter, wie vom National Institute of Standards and Technology (NIST) beschrieben (pages.nist.gov/800-63-3/sp800-63b.html)

Authentifizierung >> Administrative Benutzer >> RADIUS-Filter

Der mGuard prüft Passwörter nur dann mit Hilfe von RADIUS-Servern, wenn Sie die RADIUS-Authentifizierung aktiviert haben:

- für den Shell-Zugang siehe Menü: *„Shell-Zugang“*
- über den Web-Zugriff siehe Menü: *„Zugriff“*

Die RADIUS-Filter werden nacheinander durchsucht. Bei der ersten Übereinstimmung wird der Zugriff mit der entsprechenden Rolle *(admin, netadmin, audit)* gewährt.

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. Der Name des RADIUS-Benutzers und seine Rolle werden in Log-Einträgen festgehalten. Die Log-Einträge können an einen Remote-Server weitergeleitet werden. Dazu muss der Zugang zu einem Remote-Syslog-Server auf dem mGuard-Gerät eingerichtet und konfiguriert werden (siehe Kapitel 11, „Menü Logging“).

Folgende Aktionen des RADIUS-Benutzers werden in Form von Log-Einträgen (mit dem Namen und der Rolle RADIUS-Bentzers) protokolliert:

- Anmeldung/Abmeldung des RADIUS-Benutzers
- Konfigurationsänderungen durch den RADIUS-Benutzer
- Alle weiteren Aktionen, die vom RADIUS-Benutzer durchgeführt werden

Authentifizierung >> Administrative Benutzer >> RADIUS-Filter [...]		
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 Die Berechtigungsstufen *netadmin* und *audit* beziehen sich auf Zugriffsrechte bei Zugriffen mit dem mGuard device manager (FL MGUARD DM UNLIMITED)

6.2 Authentifizierung >> Firewall-Benutzer

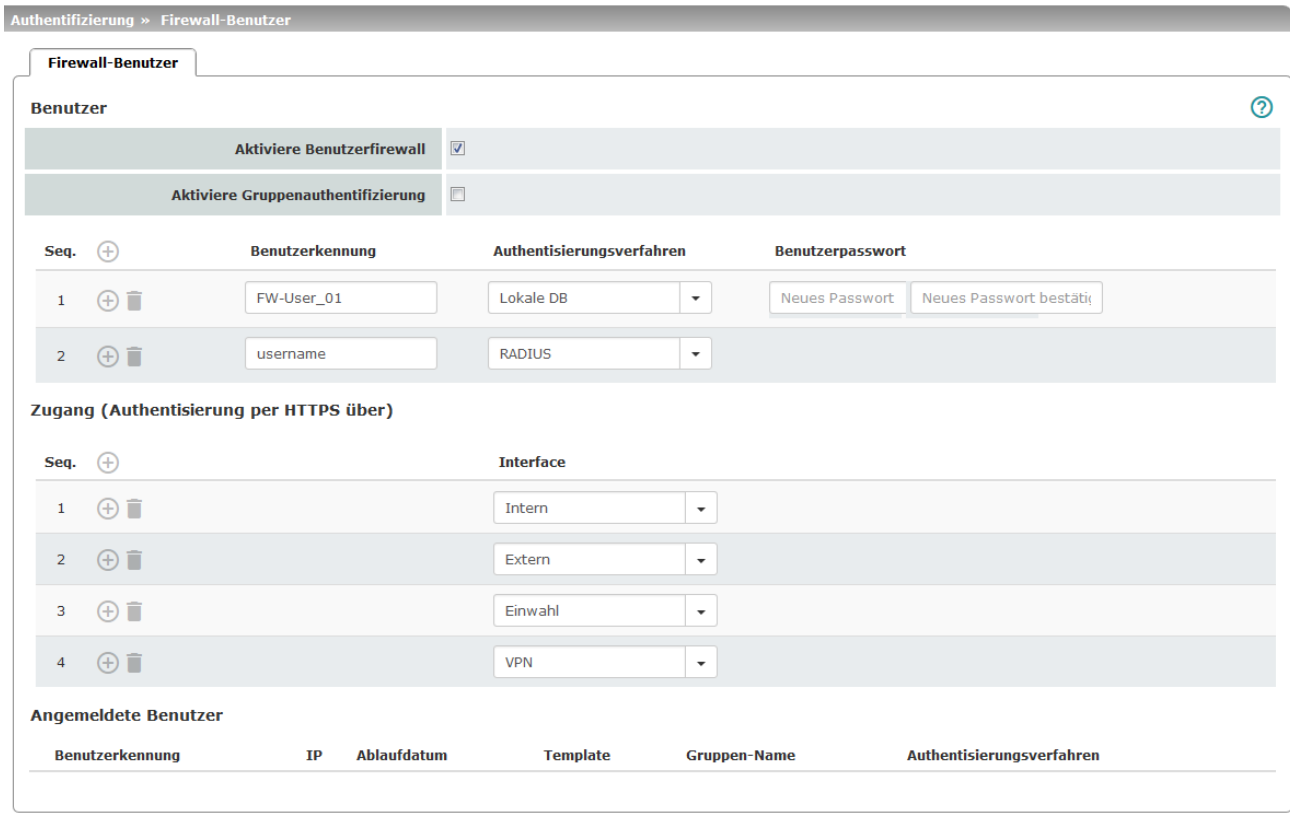
Um z. B. privates Surfen im Internet zu unterbinden, kann unter *„Netzwerksicherheit >> Paketfilter“* jede ausgehende Verbindung unterbunden werden (nicht betroffen: VPN).

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 244*.

6.2.1 Firewall-Benutzer

Dieses Menü steht **nicht** auf Geräten der FL MGUARD 2000-Serie zur Verfügung.

Der **Web-Browser „Safari“** 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 durch Angabe der ihnen zugeordneten Benutzerkennung auf. Legt außerdem die Authentifizierungsmethode fest.

Authentifizierung >> Firewall-Benutzer >> Firewall-Benutzer [...]

Aktiviere Benutzerfirewall	Unter dem Menüpunkt *„Netzwerksicherheit >> Benutzerfirewall“* können Firewall-Regeln definiert werden, die dort bestimmten Firewall-Benutzern zugeordnet werden. Bei aktivierter Benutzerfirewall werden die den unten aufgelisteten Benutzern zugeordneten Firewall-Regeln in Kraft gesetzt, 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.
Benutzerkennung	Name, den der Benutzer bei der Anmeldung angibt.
Authentifizierungsmethode	**Lokale DB**: Ist *Lokale DB* ausgewählt, muss in der Spalte *Benutzerpasswort* das Passwort eingetragen werden, das dem Benutzer zugeordnet ist, und das dieser neben seiner *Benutzerkennung* angeben muss, wenn er sich anmeldet. **RADIUS**: Ist *RADIUS* ausgewählt, kann das Passwort für den Benutzer auf dem RADIUS-Server hinterlegt werden. Wenn Sie Passwörter ändern oder Änderungen am Authentifizierungsverfahren vornehmen, sollten Sie den mGuard anschließend neu starten, um bestehende Sitzungen mit nicht mehr gültigen Zertifikaten oder Passwörtern sicher zu beenden.
Benutzerpasswort (Nur wenn als Authentifizierungsmethode **Lokale DB** ausgewählt ist)	Zugeordnetes Benutzerpasswort. **Verwenden Sie sichere Passwörter!** Erstellen und verwenden Sie nur sichere und komplexe Passwörter, wie vom National Institute of Standards and Technology (NIST) beschrieben (pages.nist.gov/800-63-3/sp800-63b.html)

Authentifizierung >> Firewall-Benutzer >> Firewall-Benutzer [...]

Zugang (Authentisierung per HTTPS über)

Gibt an, über welche mGuard-Interfaces Firewall-Benutzer sich beim mGuard anmelden können.

Der HTTPS-Fernzugriff muss im Menü "„Verwaltung >> Web-Einstellungen“" ebenfalls freigeschaltet sein, wenn der Zugang nicht über das Interface **Intern** erfolgt.

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, das 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 246.

Interface

Intern / Extern **/ VPN**

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 76**).

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.)

Angemeldete Benutzer

Bei aktivierter Benutzerfirewall wird der Status angemeldeter Firewall-Benutzer angezeigt. Ausgewählte Benutzer können mit einen Klick auf das Icon ⊖ abgemeldet werden.

6.3 Authentifizierung >> RADIUS

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.

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.

Wenn Sie Passwörter ändern oder Änderungen am Authentifizierungsverfahren vornehmen, sollten Sie den mGuard anschließend neu starten, um bestehende Sitzungen mit nicht mehr gültigen Zertifikaten oder Passwörtern sicher zu beenden.

Authentifizierung >> RADIUS		
RADIUS-Server	**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 [...]		
	RADIUS-NAS-Identifier	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. 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 identifizieren. 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.

Authentifizierung >> RADIUS [...]

Über VPN

Die Anfrage des RADIUS-Servers wird, wenn möglich, über einen VPN-Tunnel durchgeführt.

Bei aktivierter Funktion wird die Kommunikation mit dem Server immer dann über einen verschlüsselten VPN-Tunnel geführt, wenn ein passender VPN-Tunnel verfügbar ist.

Bei deaktivierter Funktion oder wenn kein passender VPN-Tunnel verfügbar ist, wird der Verkehr **unverschlüsselt über das Standard-Gateway** gesendet.

Voraussetzung für die Verwendung der Funktion ist die Verfügbarkeit eines passenden VPN-Tunnels. Das ist der Fall, wenn der angefragte 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.

Wenn die Funktion **„Über VPN“** aktiviert 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 [...]

Secret

RADIUS-Server-Passwort (Secret)

Dieses Passwort muss das selbe 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 Benutzerpasswort 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.

6.4 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“ auf Seite 369).

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 **Aussteller** aufgeführt, der Name des Inhabers eines Zertifikats als *Subject*.

Selbstsignierte Zertifikate

Ist ein Zertifikat nicht von einer CA (Certificate Authority) signiert, sondern vom Zertifikatsinhaber selber, spricht man von einem selbstsignierten Zertifikat. In selbstsignierten Zertifikaten wird der Name des Zertifikatsinhabers sowohl als **Aussteller** als auch als *Subject* aufgeführt.

Basic Constraint CA:FALSE

Ein selbstsigniertes Zertifikat, das mit dem Basic Constraint „CA:FALSE“ versehen ist, wird bei einer Validierung vom mGuard-Gerät abgelehnt.

Wenn Sie ein solches Zertifikat verwenden oder selbst erstellen möchten, müssen Sie darauf achten, dass das Basic Constraint „CA:FALSE“ nicht verwendet wird.

Selbstsignierte 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 mittels IPsec (siehe „IPsec VPN >> Verbindungen“ auf Seite 259, „Authentifizierung“ auf Seite 283).
- Authentifizierung der Kommunikationspartner bei der Herstellung von VPN-Verbindungen mittels OpenVPN (siehe „OpenVPN-Client >> Verbindungen“ auf Seite 305, „Authentifizierung“ auf Seite 283).
- Verwaltung des mGuards per SSH (Shell Zugang) (siehe „Host“ auf Seite 47, „Shell-Zugang“ auf Seite 56).
- Verwaltung des mGuards per HTTPS (siehe „Verwaltung >> Web-Einstellungen“ auf Seite 75, „Zugriff“ auf Seite 76).

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 194).

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 199).

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“ auf Seite 364).

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 jederf selbst tun kann. Ein zugehöriges Zertifikat mit dem zugehörigen *öffentlichen Schlüssel* kann man sich ebenfalls selbst erzeugen, wenn ein selbstsigniertes Zertifikat entstehen soll. (Hinweise zum Selbstausstellen gibt ein Dokument, welches von der Webseite phoenixcontact.com/products 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 201) 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.

Wenn Sie Passwörter ändern oder Änderungen am Authentifizierungsverfahren vornehmen, sollten Sie den mGuard anschließend neu starten, um bestehende Sitzungen mit nicht mehr gültigen Zertifikaten oder Passwörtern sicher zu beenden.

Einschränkung Web-Browser „Safari“

Beachten Sie bei einem administrativen Zugriff zum mGuard mit dem **Web-Browser „Safari“** über ein X.509-Zertifikat, dass alle Sub-CA-Zertifikate im Truststore des Web-Browsers installiert seien müssen.

Authentifizierung bei SSH

Die Gegenstelle zeigt vor:	Zertifikat (personenbezogen) von **CA signiert**	Zertifikat (personenbezogen) **selbstsigniert**
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 47, „Shell-Zugang“ auf Seite 56)

Authentifizierung bei HTTPS

Die Gegenstelle zeigt vor:	Zertifikat (personenbezogen) von **CA signiert**[1]	Zertifikat (personenbezogen) **selbstsigniert**
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 75, „Zugriff“ auf Seite 76)

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 Tunnel einer VPN-Verbindung) wird im Menü *„IPsec VPN >> Verbindungen“* installiert.

6.4.1 Zertifikatseinstellungen

Authentifizierung >> Zertifikate >> Zertifikatseinstellungen

Zertifikatseinstellungen

Die hier vollzogenen Einstellungen beziehen sich auf alle Zertifikate und Zertifikatsketten, die der mGuard prüfen soll.

Generell ausgenommen davon sind:

– selbstsignierte Zertifikate von Gegenstellen,
– bei VPN: alle Gegenstellen-Zertifikate

Beachte den Gültigkeitszeitraum von Zertifikaten und CRLs

Immer

Der Gültigkeitszeitraum wird immer beachtet.

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) durch Synchronisierung der Systemzeit (siehe „Zeit und Datum“ auf Seite 49) bekannt ist.

Bis zu diesem Zeitpunkt werden alle zu prüfenden Zertifikate sicherheitshalber als ungültig erachtet.

Authentifizierung >> Zertifikate >> Zertifikatseinstellungen [...]

CRL-Prüfung aktivieren

Bei **aktivierter 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 205) geben Sie an, von wo der mGuard die Sperrlisten bekommt.

Bei aktivierter CRL-Prüfung ist es notwendig, dass zu jedem **Aussteller** 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.

Nach dem Hochladen einer Sperrliste können bis zu 10 Minuten vergehen, bis VPN-Verbindungen, die Zertifikate zur Authentifizierung verwenden, aufgebaut werden.

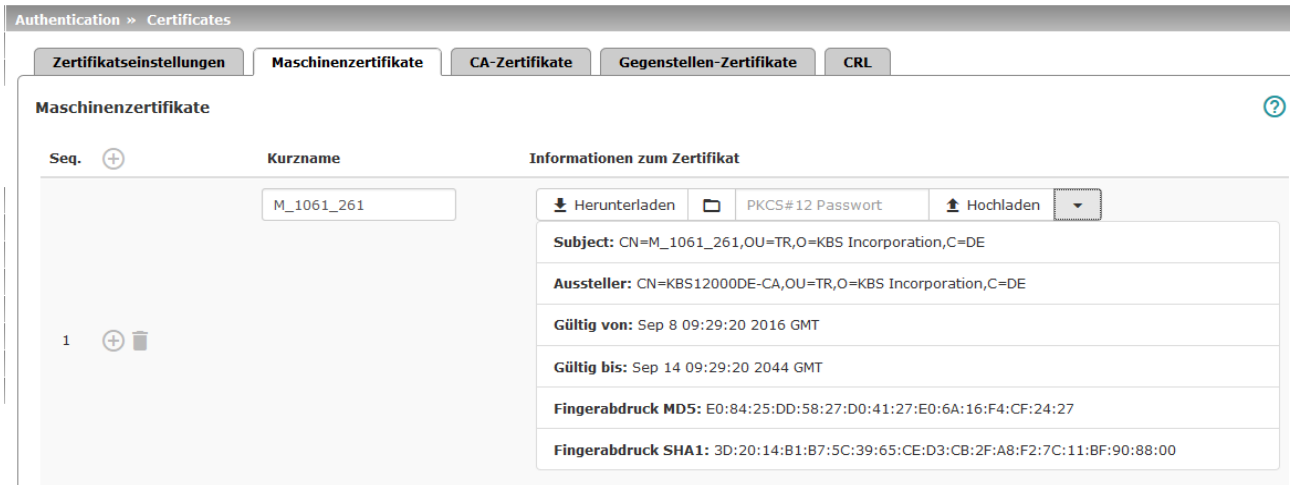
CRL-Download-Intervall

Ist die *CRL-Prüfung* aktiviert (s. o.), wählen Sie hier aus, in welchen Zeitabständen die Sperrlisten heruntergeladen und in Kraft gesetzt werden sollen.

Auf der Registerkarte **CRL** (siehe „CRL“ auf Seite 205) geben Sie an, von wo der mGuard die Sperrlisten bezieht.

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.

6.4.2 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 192.

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 selbstsignierte 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 (s. o).

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 das Icon **Keine Datei ausgewählt**, 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 das Icon **Hochladen**.
  Nach dem Import können Sie die Details des Zertifikats über einen Klick auf die Schaltfläche **Details** anzeigen.

- Speichern Sie das importierte Zertifikat durch einen Klick auf das Icon **Übernehmen**.

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 und herunterladen

Aus dem importierten Maschinenzertifikat können Sie eine Kopie erzeugen (z. B. für die Gegenstelle, so dass diese den mGuard damit authentifizieren kann) und herunterladen. Diese Kopie enthält nicht den privaten Schlüssel und ist deshalb unbedenklich.

Gehen Sie dazu wie folgt vor:

- Klicken Sie in der Zeile des betreffenden Maschinenzertifikats auf das Icon **Herunterladen**.
- Folgen Sie den Anweisungen in den folgenden Dialogfeldern.

6.4.3 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 Aussteller (Issuer) angegeben. Diese Angabe kann mit dem lokal vorliegenden CA-Zertifikat von dem selben Aussteller auf Echtheit überprüft werden. Weitere Erläuterungen siehe „Authentifizierung >> Zertifikate“ auf Seite 192.

Beispiel für importierte CA-Zertifikate (s. o).

Authentifizierung >> Zertifikate >> CA-Zertifikate

Vertrauenswürdige CA-Zertifikate — **Zeigt die aktuell importierten CA-Zertifikate an.**

Um ein (neues) Zertifikat zu importieren, gehen Sie wie folgt vor:

CA-Zertifikat importieren

Die Datei (Dateinamen-Erweiterung *.cer, *.pem oder *.crt) ist auf dem angeschlossenen Rechner gespeichert.

Gehen Sie wie folgt vor:

- Klicken Sie auf das Icon **Keine Datei ausgewählt**, um die Datei zu selektieren
- Klicken Sie auf das Icon **Hochladen**.
  Nach dem Import können Sie die Details des Zertifikats über einen Klick auf die Schaltfläche **Details** anzeigen.
- Speichern Sie das importierte Zertifikat durch einen Klick auf das Icon **Übernehmen**.

Kurzname

Beim Importieren eines CA-Zertifikats wird das CN-Attribut aus dem Subject-Feld des Zertifikats als Kurzname vorgeschlagen, sofern das Feld Kurzname bis jetzt leer ist. Dieser Name kann übernommen oder geändert werden.

- Sie müssen einen Namen vergeben. Der Name muss eindeutig ist sein.

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 Auswahlliste werden die Zertifikate jeweils unter dem Kurznamen angezeigt, den Sie hier den Zertifikaten geben. Eine Namensvergabe ist zwingend erforderlich.

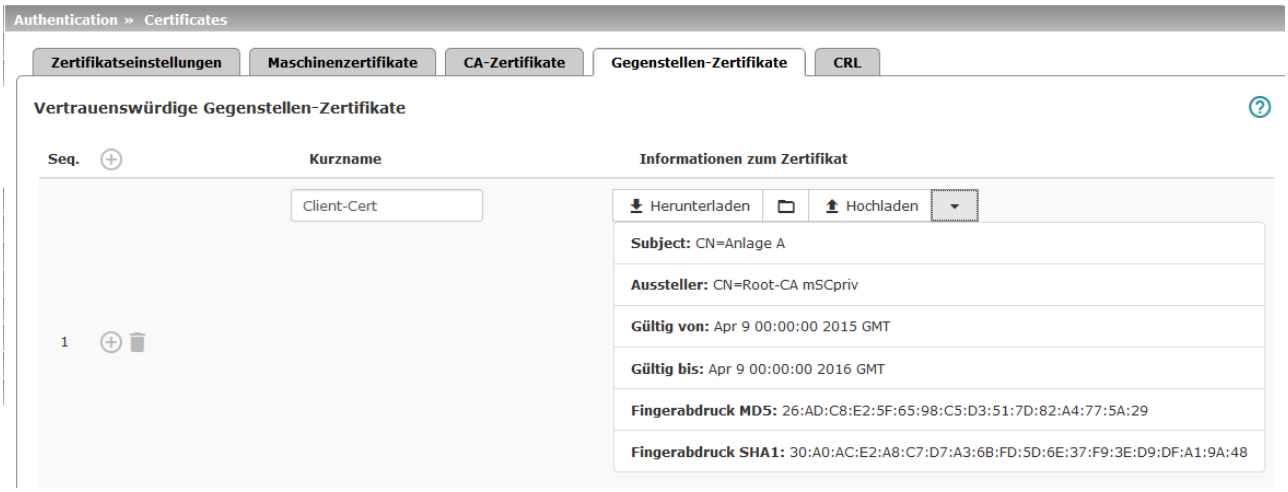
Zertifikats-Kopie erstellen und herunterladen

Aus dem importierten CA-Zertifikat können Sie eine Kopie erzeugen und herunterladen.

Gehen Sie dazu wie folgt vor:

- Klicken Sie in der Zeile des betreffenden CA-Zertifikats auf das Icon **Herunterladen**.
- Folgen Sie den Anweisungen in den folgenden Dialogfeldern.

6.4.4 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 Tunnel einer VPN-Verbindung) wird im Menü *„IPsec VPN >> Verbindungen“* installiert.

Weitere Erläuterungen siehe „Authentifizierung >> Zertifikate“ auf Seite 192.

Beispiel für importierte Gegenstellen-Zertifikate (s. o.)

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 das Icon **Keine Datei ausgewählt**, um die Datei zu selektieren • Klicken Sie auf das Icon **Hochladen**. Nach dem Import können Sie die Details des Zertifikats über einen Klick auf die Schaltfläche **Details** anzeigen. • Speichern Sie das importierte Zertifikat durch einen Klick auf das Icon **Übernehmen**.
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 Auswahlliste werden die Zertifikate jeweils unter dem Kurznamen angezeigt, den Sie hier den Zertifikaten geben. Eine Namensvergabe ist zwingend erforderlich.

Zertifikats-Kopie erstellen und herunterladen

Aus dem importierten Gegenstellen-Zertifikat können Sie eine Kopie erzeugen und herunterladen.

Gehen Sie dazu wie folgt vor:

- Klicken Sie in der Zeile des betreffenden Gegenstellen-Zertifikats auf das Icon **Herunterladen**.
- Folgen Sie den Anweisungen in den folgenden Dialogfeldern.

6.4.5 CRL

Authentifizierung >> Zertifikate >> CRL

Certificate Revocation List (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 die Funktion **CRL-Prüfung aktivieren** aktiviert wurde (siehe „Zertifikatseinstellungen“ auf Seite 197).

Zu jedem **Aussteller**-Namen, der in zu prüfenden Zertifikaten angegeben wird, muss eine CRL mit dem selben **Aussteller**-Namen vorhanden sein. Fehlt eine solche CRL, dann wird bei eingeschalteter CRL-Prüfung das zu prüfende Zertifikat als ungültig betrachtet.

Nach dem Hochladen einer Sperrliste können bis zu 10 Minuten vergehen, bis VPN-Verbindungen, die Zertifikate zur Authentifizierung verwenden, aufgebaut werden.

URL

Wenn auf der Registerkarte *Zertifikatseinstellungen* (siehe „Zertifikatseinstellungen“ auf Seite 197) 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.

Authentifizierung >> Zertifikate >> CRL

Über VPN	Die Anfrage des CRL-Download-Servers (URL) wird, wenn möglich, über einen VPN-Tunnel durchgeführt. Bei aktivierter Funktion wird die Kommunikation mit dem Server immer dann über einen verschlüsselten VPN-Tunnel geführt, wenn ein passender VPN-Tunnel verfügbar ist. Bei deaktivierter Funktion oder wenn kein passender VPN-Tunnel verfügbar ist, wird der Verkehr **unverschlüsselt über das Standard-Gateway** gesendet. Voraussetzung für die Verwendung der Funktion ist die Verfügbarkeit eines passenden VPN-Tunnels. Das ist der Fall, wenn der angefragte 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.
Nächste Aktualisierung	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.
CRL-Aussteller	Information, die der mGuard direkt aus der CRL liest: Zeigt den Aussteller der betreffenden Zertifikats-Sperrliste (Certificate Revocation Liste - CRL).

Authentifizierung >> Zertifikate >> CRL

Aktion: CRL-Datei hochladen

Falls die CRL als Datei vorliegt, kann sie auch manuell in den mGuard importiert werden.

- Klicken Sie auf das Icon **Keine Datei ausgewählt...** und selektieren Sie die gewünschte CRL-Datei. Klicken Sie anschließend auf die Schaltfläche **Öffnen**.

Falls das Icon nicht sichtbar ist, müssen Sie nach dem Einfügen einer neuen Tabellenzeile zunächst auf das Icon **Übernehmen** klicken.

- Klicken Sie anschließend auf das Icon **CRL-Datei hochladen**, um die CRL-Datei zu importieren.
- Klicken Sie auf das Icon **Übernehmen**, um die Änderungen zu übernehmen.

Es muss immer eine aktuelle CRL-Datei verwendet werden. Deshalb gehört sie nicht zur mGuard-Konfiguration.

Wenn Sie eine mGuard-Konfiguration exportieren und anschließend 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.

7 Menü Netzwerksicherheit

Auf Geräten der FL MGUARD 2000-Serie steht das Menü in reduzierter Form zur Verfügung.

7.1 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.

Die unter **Netzwerksicherheit >> Paketfilter** konfigurierbaren Firewallregeln werden nicht auf IP-Pakete angewendet, die direkt auf eine IP-Adresse des mGuards gerichtet sind. Sie gelten nur für IP-Verbindungen bzw. IP-Verkehr, der durch den mGuard hindurch geht.

Werkseitige Voreinstellung der Firewall (Standard)

- Alle eingehenden Verbindungen werden verworfen (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 259, „Firewall“ auf Seite 291).
- **Benutzer-Firewall**. Wenn sich Benutzer anmelden, für die Benutzer-Firewall-Regeln definiert sind, werden vorrangig diese Regeln angewandt (siehe „Netzwerksicherheit >> Benutzerfirewall“ auf Seite 244), 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.

Firewall-Einstellungen bei Geräten der FL MGUARD 2000-Serie

Die Geräte der FL MGUARD 2000-Serie verfügen über eine einfache Firewall-Funktionalität.

Folgende Funktionen werden nicht unterstützt:

- **Firewall-Regelsätze** können nicht konfiguriert werden.
- **MAC-Filter** können nicht konfiguriert werden.
- Eine **Benutzerfirewall** kann nicht konfiguriert werden.
- **Hostnamen in IP-Gruppen** können nicht verwendet werden.

Hinweis: Konfigurationsprofile, die entsprechende Einstellungen enthalten, können nicht importiert werden.

Verwendung von Hostnamen in IP-Gruppen (Firewall-Regeln)

In IP-Gruppen können neben IP-Adressen, IP-Bereichen und Netzwerken auch Hostnamen angegeben werden (DNS-basierte Firewall-Regeln). Die IP-Adressauflösung der Hostnamen erfolgt entsprechend den DNS-Einstellungen des mGuards. Auf diese Weise lassen sich Hostnamen über IP-Gruppen in Firewall-Regeln einsetzen (siehe „IP- und Portgruppen“ auf Seite 227).

ACHTUNG: Bei der Verwendung von Hostnamen besteht grundsätzlich die Gefahr, dass ein Angreifer DNS-Anfragen manipuliert oder blockiert (u. a. *DNS spoofing*). Konfigurieren Sie deshalb im mGuard nur vertrauenswürdige und abgesicherte DNS-Server aus Ihrem internen Firmennetzwerk, um entsprechende Angriffe zu vermeiden.

IP-Gruppen, die Hostnamen enthalten, sollten aus Sicherheitsgründen nicht in Firewall-Regeln verwendet werden, die als Aktion „Verwerfen“ oder „Abweisen“ ausführen.

Kann ein Hostname aus einer IP-Gruppe nicht aufgelöst werden, weil z. B. ein DNS-Server nicht konfiguriert wurde oder nicht erreichbar ist, wird dieser Host bei der Regel nicht berücksichtigt. Weitere Einträge in der IP-Gruppe sind davon nicht betroffen und werden berücksichtigt.

PROFINET RT

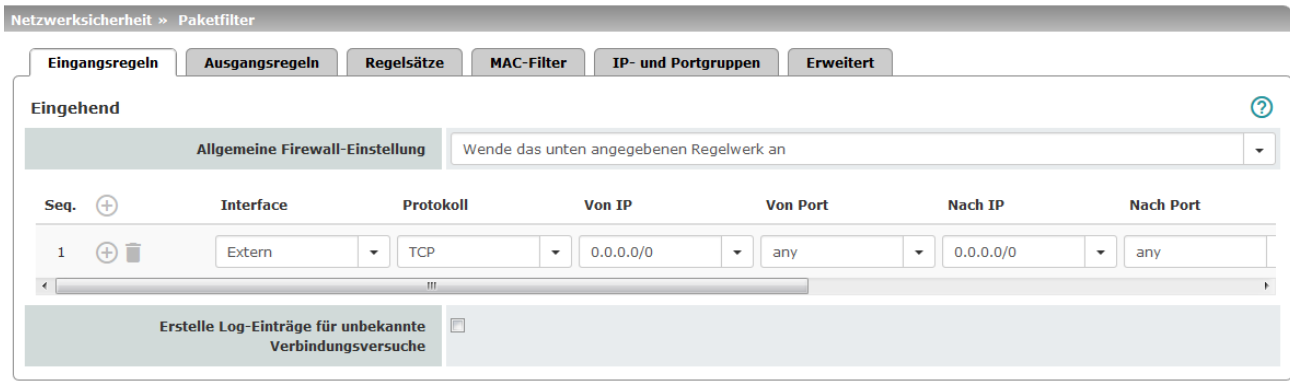
Die Geräte FL MGUARD 210X/410X/430X sind hardwaretechnisch so gestaltet, dass die WAN-Seite (Interface XF1) und die LAN-Seite (Interface XF2 bzw. XF2-XF5) über den Applikationsprozessor sicher voneinander getrennt sind.

Zudem ist die mGuard-Firmware 10.x so implementiert, dass eine Übertragung von Layer 2-Datagrammen wie z. B. PROFINET RT bei Nutzung des Netzwerk-Modus „Router“ (Werkseinstellung) ausgeschlossen ist.

mGuard-Geräte können somit als sichere Netzwerkgrenze für PROFINET verwendet werden. Sie können als Schutzgeräte für PROFIsafe-Netzwerkzellen, in Umgebungen, in denen eine Eindeutigkeit der PROFIsafe-Adressen nicht sichergestellt werden kann, verwendet werden.

Der Einsatz der Geräte erfolgt hierbei konform zur Norm IEC 61784-3-3 (5.4.2 und 8.1.2).

7.1.1 Eingangsregeln



Netzwerksicherheit >> Paketfilter >> Eingangsregeln

Eingehend

Listet die eingerichteten Firewall-Regeln auf. Sie gelten für eingehende Datenverbindungen, die von extern initiiert werden (WAN --> LAN).

Für die Geräte der FL MGUARD 2000-Serie gelten gesonderte Firewall-Einstellungen (siehe „Firewall-Einstellungen bei Geräten der FL MGUARD 2000-Serie“ auf Seite 210).

In der werkseitigen Voreinstellung werden alle eingehenden Verbindungen (außer VPN) verworfen.

Wenn bei **Allgemeine Firewall-Einstellung** „*Wende das unten angegebene Regelwerk an*“ ausgewählt ist und **keine Regel** gesetzt ist, werden die Datenpakete aller eingehenden Verbindungen (außer VPN) verworfen.

Der DoS-Schutz des Geräts steht nicht zur Verfügung, wenn bei **Allgemeine Firewall-Einstellung** „*Alle Verbindungen annehmen*“ ausgewählt ist (siehe „Flood Protection“ auf Seite 242).

Um den DoS-Schutz in diesem Fall bereitzustellen, müssen Sie die Einstellung „*Wende das unten angegebene Regelwerk an*“ auswählen und anschließend eine Firewall-Regel erstellen, mit der alle Verbindungen angenommen werden.

Allgemeine Firewall-Einstellung

Alle Verbindungen annehmen, die Datenpakete aller eingehenden Verbindungen werden angenommen.

Alle Verbindungen verwerfen, die Datenpakete aller eingehenden Verbindungen werden verworfen.

Nur Ping zulassen, die Datenpakete aller eingehenden Verbindungen werden verworfen, mit Ausnahme der Ping-Pakete (ICMP). Diese Einstellung lässt alle Ping-Pakete passieren. Der integrierte Schutz vor Brute-Force-Attacken ist hier ausnahmsweise nicht wirksam.

Wende das unten angegebene Regelwerk an, weitere Einstellmöglichkeiten werden eingeblendet.

Die folgenden Einstellungen sind nur sichtbar, wenn „**Wende das unten angegebene Regelwerk an**“ eingestellt ist.

Netzwerksicherheit >> Paketfilter >> Eingangsregeln [...]

Interface	**Extern / Alle** Gibt an, über welches Interface die Datenpakete eingehen, damit sich die Regel auf sie bezieht. Auf Geräten der FL MGUARD 2000/4000-Serie steht nur das Interface **Extern** zur Verfügung.
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 Adressenbereich anzugeben, benutzen Sie die CIDR-Schreibweise (siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 43). **Namen von IP-Gruppen**, sofern definiert. Bei Angabe des Namens einer IP-Gruppe werden die Hostnamen, IP-Adressen, IP-Bereiche oder Netzwerke berücksichtigt, die unter diesem Namen gespeichert sind (siehe Registerkarte „IP- und Portgruppen“). Werden Hostnamen in IP-Gruppen verwendet, muss der mGuard so konfiguriert sein, dass der Hostname von einem DNS-Server in eine IP-Adresse aufgelöst werden kann. Kann ein Hostname aus einer IP-Gruppe nicht aufgelöst werden, wird dieser Host bei der Regel nicht berücksichtigt. Weitere Einträge in der IP-Gruppe sind davon nicht betroffen und werden berücksichtigt. Auf Geräten der FL MGUARD 2000-Serie ist die Verwendung von Hostnamen in IP-Gruppen nicht möglich.
Von Port / Nach Port **(Nur 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). **Namen von Portgruppen**, sofern definiert. Bei Angabe des Namens einer Portgruppe werden die Ports oder Portbereiche berücksichtigt, die unter diesem Namen gespeichert sind (siehe Registerkarte „IP- und Portgruppen“).

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 der Auswahl eines Regelsatzes treten die Firewall-Regeln in Kraft, die unter diesem Regelsatz konfiguriert sind (siehe Kapitel 7.1.4). Regelsätze, die IP-Gruppen mit Hostnamen enthalten, sollten aus Sicherheitsgründen nicht in Firewall-Regeln verwendet werden, die als Aktion „Verwerfen“ oder „Abweisen“ ausführen. Auf Geräten der FL MGUARD 2000-Serie ist die Verwendung von Regelsätzen nicht möglich. **Namen von Modbus-TCP-Regelsätzen**, sofern definiert. Bei der Auswahl eines Modbus-TCP-Regelsatzes treten die Firewall-Regeln in Kraft, die unter diesem Regelsatz konfiguriert sind (siehe Kapitel 7.2.1).
	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 - Funktion *Log* aktivieren – oder nicht - Funktion *Log* deaktivieren (Standard).
	Log-Einträge für unbekannte Verbindungsversuche	Bei aktivierter Funktion werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden. (Standard: **deaktiviert**)

7.1.2 Ausgangsregeln

Netzwerksicherheit >> Paketfilter >> Ausgangsregeln

Ausgehend

Listet die eingerichteten Firewall-Regeln auf.

Sie gelten

a) für ausgehende Datenverbindungen, die von intern initiiert werden (LAN --> WAN),

b) für Datenverbindungen, die von einem VLAN-Netzwerk auf der LAN-Seite zu einem anderen VLAN-Netzwerk auf der LAN-Seite initiiert werden.

Für die Geräte der FL MGUARD 2000-Serie gelten gesonderte Firewall-Einstellungen (siehe „Firewall-Einstellungen bei Geräten der FL MGUARD 2000-Serie“ auf Seite 210).

In der werkseitigen Voreinstellung ist eine Regel gesetzt, die alle ausgehenden Verbindungen zulässt.

Wenn „**Wende das unten angegebene Regelwerk an**“ ausgewählt ist und **keine Regel** gesetzt ist, werden die Datenpakete aller ausgehenden Verbindungen (außer VPN) verworfen.

Allgemeine Firewall-Einstellung

Alle Verbindungen annehmen, die Datenpakete aller ausgehenden Verbindungen werden angenommen.

Alle Verbindungen verwerfen, die Datenpakete aller ausgehenden Verbindungen werden verworfen.

Nur Ping zulassen, die Datenpakete aller ausgehenden Verbindungen werden verworfen, mit Ausnahme der Ping-Pakete (ICMP).

Wende das unten angegebene Regelwerk an, blendet weitere Einstellmöglichkeiten ein.

Die folgenden Einstellungen sind nur sichtbar, wenn „**Wende das unten angegebene Regelwerk an**“ eingestellt ist.

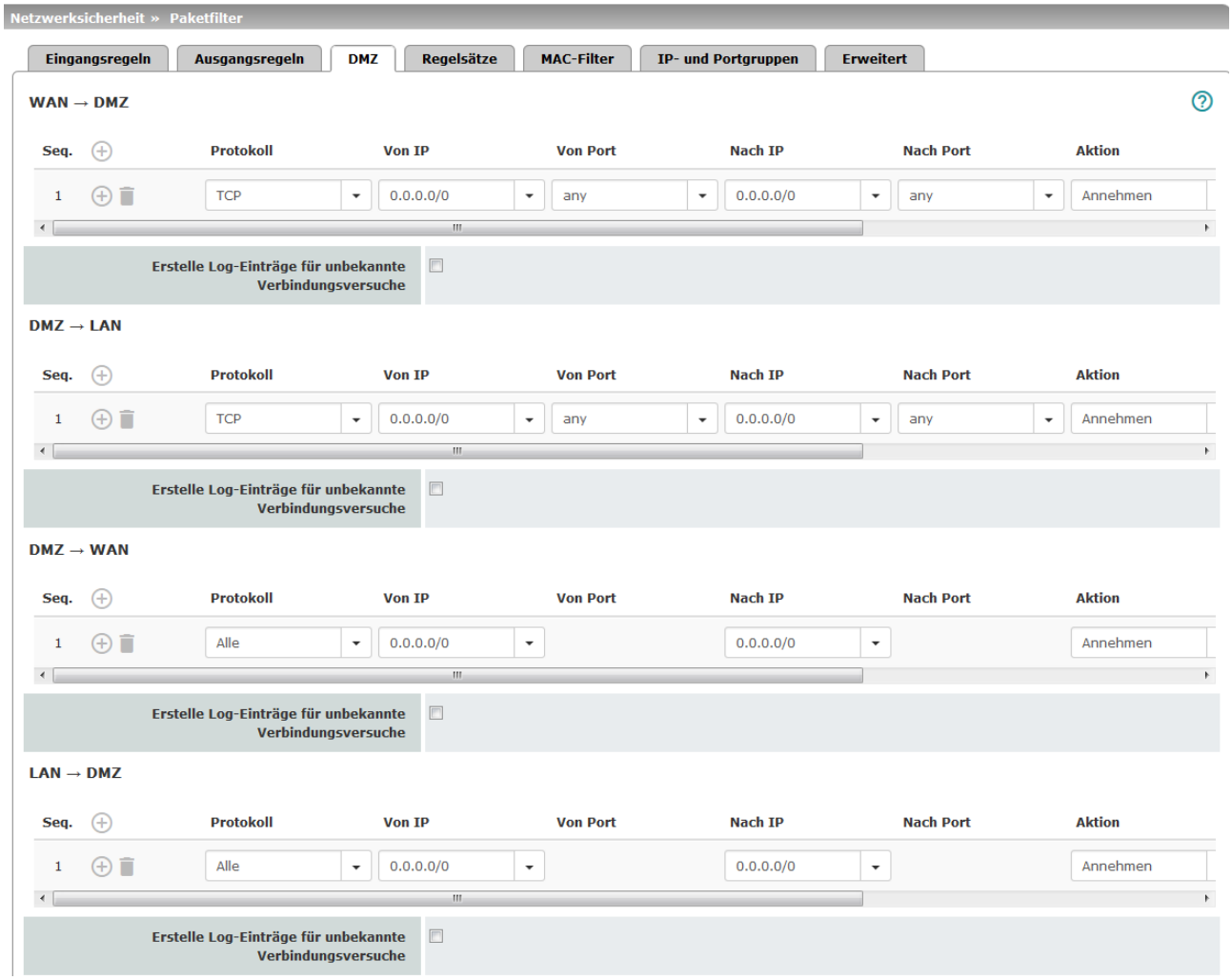
Protokoll

Alle bedeutet: TCP, UDP, ICMP, GRE und andere IP-Protokolle

Netzwerksicherheit >> Paketfilter >> Ausgangsregeln [...]		
	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 43). **Namen von IP-Gruppen**, sofern definiert. Bei Angabe des Namens einer IP-Gruppe werden die Hostnamen, IP-Adressen, IP-Bereiche oder Netzwerke berücksichtigt, die unter diesem Namen gespeichert sind (siehe Registerkarte „IP- und Portgruppen“). Werden Hostnamen in IP-Gruppen verwendet, muss der mGuard so konfiguriert sein, dass der Hostname von einem DNS-Server in eine IP-Adresse aufgelöst werden kann. Kann ein Hostname aus einer IP-Gruppe nicht aufgelöst werden, wird dieser Host bei der Regel nicht berücksichtigt. Weitere Einträge in der IP-Gruppe sind davon nicht betroffen und werden berücksichtigt. Auf Geräten der FL MGUARD 2000-Serie ist die Verwendung von Hostnamen in IP-Gruppen nicht möglich.
	Von Port / Nach Port (Nur 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). **Namen von Portgruppen**, sofern definiert. Bei Angabe des Namens einer Portgruppe werden die Ports oder Portbereiche berücksichtigt, die unter diesem Namen gespeichert sind (siehe Registerkarte „IP- und Portgruppen“).

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 der Auswahl eines Regelsatzes treten die Firewall-Regeln in Kraft, die unter diesem Regelsatz konfiguriert sind (siehe Kapitel 7.1.4). Regelsätze, die IP-Gruppen mit Hostnamen enthalten, sollten aus Sicherheitsgründen nicht in Firewall-Regeln verwendet werden, die als Aktion „Verwerfen“ oder „Abweisen“ ausführen. Auf Geräten der FL MGUARD 2000-Serie ist die Verwendung von Regelsätzen nicht möglich. **Namen von Modbus-TCP-Regelsätzen**, sofern definiert. Bei der Auswahl eines Modbus-TCP-Regelsatzes treten die Firewall-Regeln in Kraft, die unter diesem Regelsatz konfiguriert sind (siehe Kapitel 7.2.1).
	Kommentar	Ein frei wählbarer Kommentar für diese Firewall-Regel.
	Log	Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel – das Ereignis protokolliert werden soll - Aktion *Log* aktivieren – oder nicht - Aktion *Log* deaktivieren (Standard).
	Log-Einträge für unbekannte Verbindungsversuche	Bei aktivierter Funktion werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden. (Standard: **deaktiviert**)

7.1.3 DMZ



Netzwerksicherheit >> Paketfilter >> DMZ

Firewall-Regeln für die DMZ

(Nur bei FL MGUARD 4305)

Die DMZ kann über einen eigenen Satz von Firewall-Regeln gegen Zugriffe aus dem internen (LAN-Interface) und dem externen Netz (WAN-Interface) abgesichert werden. Die Einstellungen werden für die vier möglichen Richtungen des Netzwerkverkehrs getrennt vorgenommen.

WAN → DMZ

Wenn keine Regel gesetzt ist, werden die Datenpakete aller eingehenden Verbindungen (außer VPN) verworfen (= Werkseinstellung).

DMZ → LAN

Wenn keine Regel gesetzt ist, werden die Datenpakete aller ausgehenden Verbindungen (außer VPN) verworfen (= Werkseinstellung).

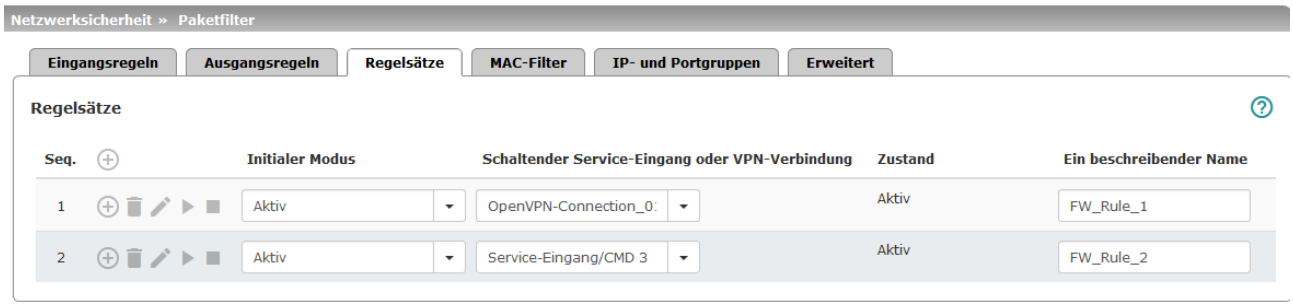
DMZ → WAN

Per Werkseinstellung ist eine Regel gesetzt, die alle ausgehenden Verbindungen zulässt.

Netzwerksicherheit >> Paketfilter >> DMZ [...]		
LAN → DMZ		Per Werkseinstellung ist eine Regel gesetzt, die alle eingehenden Verbindungen zulässt.
	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 Adressenbereich anzugeben, benutzen Sie die CIDR-Schreibweise (siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 43). **Namen von IP-Gruppen**, sofern definiert. Bei Angabe des Namens einer IP-Gruppe werden die Hostnamen, IP-Adressen, IP-Bereiche oder Netzwerke berücksichtigt, die unter diesem Namen gespeichert sind (siehe Registerkarte „IP- und Portgruppen“).  Werden Hostnamen in IP-Gruppen verwendet, muss der mGuard so konfiguriert sein, dass der Hostname von einem DNS-Server in eine IP-Adresse aufgelöst werden kann. Kann ein Hostname aus einer IP-Gruppe nicht aufgelöst werden, wird dieser Host bei der Regel nicht berücksichtigt. Weitere Einträge in der IP-Gruppe sind davon nicht betroffen und werden berücksichtigt.
	Von Port / Nach Port (Nur 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). **Namen von Portgruppen**, sofern definiert. Bei Angabe des Namens einer Portgruppe werden die Ports oder Portbereiche berücksichtigt, die unter diesem Namen gespeichert sind (siehe Registerkarte „IP- und Portgruppen“).

Netzwerksicherheit >> Paketfilter >> DMZ [...]		
	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 der Auswahl eines Regelsatzes treten die Firewall-Regeln in Kraft, die unter diesem Regelsatz konfiguriert sind (siehe Kapitel 7.1.4). Regelsätze, die IP-Gruppen mit Hostnamen enthalten, sollten aus Sicherheitsgründen nicht in Firewall-Regeln verwendet werden, die als Aktion „Verwerfen“ oder „Abweisen“ ausführen. **Namen von Modbus-TCP-Regelsätzen**, sofern definiert. Bei der Auswahl eines Modbus-TCP-Regelsatzes treten die Firewall-Regeln in Kraft, die unter diesem Regelsatz konfiguriert sind (siehe Kapitel 7.2.1).
	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 - Aktion *Log* aktivieren – oder nicht - Aktion *Log* deaktivieren (Standard).
	Log-Einträge für unbekannte Verbindungsversuche	Bei aktivierter Funktion werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden. (Standard: **deaktiviert**)

7.1.4 Regelsätze



Firewall-Regelsätze werden dazu verwendet, Firewall-Regeln in einem Regelsatz zusammenzufassen. Diese können dann über den Regelsatz gemeinsam aktiviert oder deaktiviert werden.

Ein Regelsatz – und damit alle darin konfigurierten Firewall-Regeln – könnte z. B. über einen Ein-/Aus-Schalter oder eine aufgebaute VPN-Verbindung gesteuert werden (siehe „Verwaltung >> Service I/O“ auf Seite 123).

Hinweise zur Verwendung von Regelsätzen, die nur temporär aktiviert werden

In Firewall-Regelsätzen, die nur temporär aktiviert werden (z. B. über einen Schalter gesteuert), sollten immer sogenannte „**Allow-Regeln**“ (Aktion = Annehmen) verwendet werden:

– Der Regelsatz wird aktiviert, um die konfigurierten Verbindungen zu erlauben.
– Der Regelsatz wird deaktiviert, um die konfigurierten Verbindungen zu blockieren.

„**Deny-Regeln**“ (Aktion = Abweisen/Verwerfen) sollten in temporär geltenden Regelsätzen nicht verwendet werden, da entsprechende bereits bestehende Datenverbindungen mit der Aktivierung des Regelsatzes nicht automatisch beendet würden.

Wenn eine Verbindung, die zu einem Firewall-Regelsatz passt, aufgebaut worden ist und diese Verbindung kontinuierlich Datenverkehr erzeugt, dann kann es sein, dass das Deaktivieren des Firewall-Regelsatzes diese Verbindung nicht wie erwartet unterbricht.

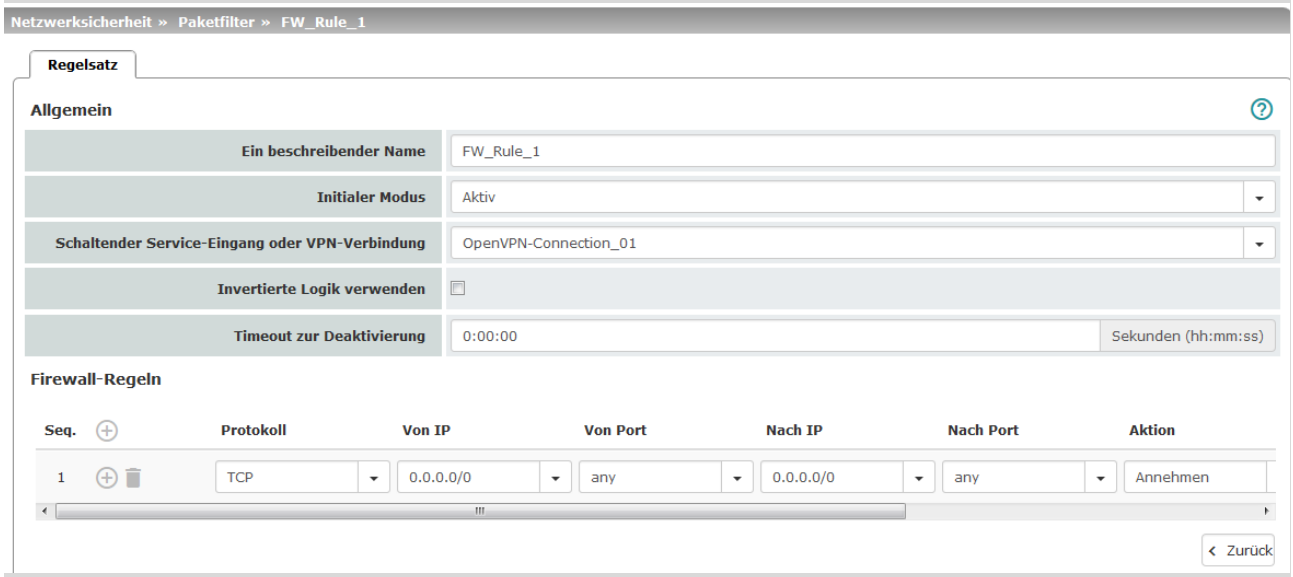
Das ist so, weil der (ausgehende) Response von einem Dienst auf der LAN-Seite einen Eintrag in der Verbindungsverfolgungs-Tabelle (Connection Tracking Table) erzeugt, der einen anderen (eingehenden) Request von einem Peer außerhalb ermöglicht. Dieser Peer passiert die Firewall mit den selben Verbindungsparametern, ist aber nicht mit dem Firewall-Regelsatz verbunden.

Es gibt zwei Wege, den mGuard so einzurichten, dass er mit dem Ausschalten eines Firewall-Regelsatzes auch die zugehörigen Verbindungen unterbricht.

– Aktivieren Sie unter „Netzwerksicherheit >> Paketfilter >> Erweitert“ die Option „Erlaube TCP-Verbindungen nur mit SYN“ .
– Blockieren Sie in der Firewall die ausgehenden Verbindungen, die über den Port laufen, den die eingehenden Verbindungen als Ziel haben.

Wenn z B. der Regelsatz an Port 22 eingehenden Datenverkehr ermöglicht, dann kann man eine Ausgangs-Regel einrichten, die jeden Datenverkehr deaktiviert, der von Port 22 kommt.

Netzwerksicherheit >> Paketfilter >> Regelsätze		
Regelsätze (Dieser Menüpunkt gehört nicht zum Funktionsumfang der Serie FL MGUARD 2000.)	**Initialer Modus**	**Deaktiviert / Aktiv / Inaktiv** Bestimmt den Ausgangszustand des Firewall-Regelsatzes nach einer Neukonfiguration oder einem Neustart. Die „Aktiv/Inaktiv“-Einstellung wirkt sich nur bei einem angeschlossenen Taster aus, Wenn die Firewall-Regelsätze über einen Schalter oder eine VPN-Verbindung gesteuert werden, haben diese Vorrang. Bei der Einstellung „Deaktiviert“ kann der Firewall-Regelsatz nicht dynamisch aktiviert werden. Der Firewall-Regelsatz bleibt bestehen, hat aber keinen Einfluss.
	Schaltender Service-Eingang oder VPN-Verbindung	**Service-Eingang CMD 1-3 (I 1-3), VPN-Verbindung** Der Firewall-Regelsatz kann über einen Taster/Schalter oder über eine VPN-Verbindung geschaltet werden. Der Taster/Schalter muss an einen der Servicekontakte (CMD 1-3 / I 1-3) angeschlossenen sein.
	Zustand	Gibt den aktuellen Status wieder.
	Ein beschreibender Name	Sie können den Firewall-Regelsatz frei benennen bzw. umbenennen.
	Regelsatz aktivieren / inaktivieren	**Aktivieren / Inaktivieren** Sie können den Regelsatz durch einen Klick auf die Icons ▶ **Aktivieren** und ■ **Inaktivieren** aktivieren oder außer Kraft setzen.
Editieren	Nach Klicken auf das Icon ✎ **Zeile bearbeiten** erscheint folgende Registerkarte:	



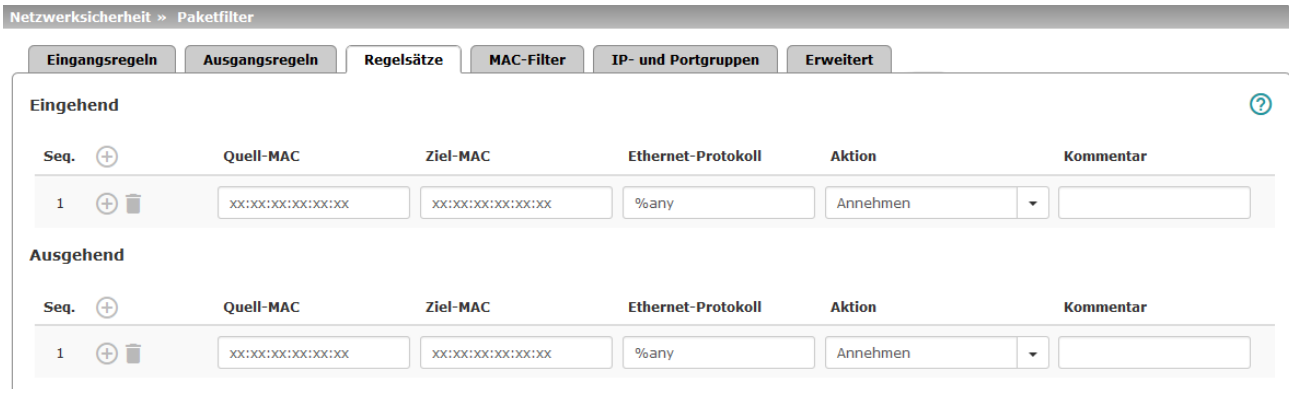
Netzwerksicherheit >> Paketfilter >> Regelsätze [...]		
Allgemein	**Ein beschreibender Name**	Sie können den Firewall-Regelsatz frei benennen bzw. umbenennen.
	Initialer Modus	**Deaktiviert / Aktiv / Inaktiv** Bestimmt den Ausgangszustand des Firewall-Regelsatzes nach einer Neukonfiguration oder einem Neustart. Die „Aktiv/Inaktiv“-Einstellung wirkt sich nur bei einem angeschlossenen Taster aus, Wenn die Firewall-Regelsätze über eine Schalter oder eine VPN-Verbindung gesteuert werden, haben diese Vorrang. Bei der Einstellung „Deaktiviert“ kann der Firewall-Regelsatz nicht dynamisch aktiviert werden. Sie bleibt bestehen, hat aber keinen Einfluss.
	Schaltender Service-Eingang oder VPN-Verbindung	**Service-Eingang CMD 1-3 (I 1-3), VPN-Verbindung** Der Firewall-Regelsatz kann über einen Taster/Schalter oder über eine VPN-Verbindung geschaltet werden. Der Taster/Schalter muss an einen der Servicekontakte (CMD 1-3 / I 1-3) angeschlossenen sein.
	Invertierte Logik verwenden	Kehrt das Verhalten des angeschlossenen Tasters/Schalters oder der schaltenden VPN-Verbindung um. Wenn der schaltende Service-Eingang als Ein-/Aus-Schalter konfiguriert ist, kann er z. B. einen Firewall-Regelsatz ein und gleichzeitig einen anderen ausschalten. Das gleich gilt für schaltende VPN-Verbindungen.
	Timeout zur Deaktivierung	Aktivierte Firewall-Regelsätze werden nach Ablauf dieser Zeit deaktiviert. Bei 0 ist diese Einstellung abgeschaltet. Zeit in hh:mm:ss (maximal 1 Tag) Die Eingabe kann aus Sekunden [ss], Minuten und Sekunden [mm:ss] oder Stunden, Minuten und Sekunden [hh:mm:ss] bestehen.
Firewall-Regeln	**Protokoll**	**Alle** bedeutet: TCP, UDP, ICMP, GRE und andere IP-Protokolle.

Netzwerksicherheit >> Paketfilter >> Regelsätze [...]		
	Von 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 43). **Namen von IP-Gruppen**, sofern definiert. Bei Angabe des Namens einer IP-Gruppe werden die Hostnamen, IP-Adressen, IP-Bereiche oder Netzwerke berücksichtigt, die unter diesem Namen gespeichert sind (siehe Registerkarte „IP- und Portgruppen“). Werden Hostnamen in IP-Gruppen verwendet, muss der mGuard so konfiguriert sein, dass der Hostname von einem DNS-Server in eine IP-Adresse aufgelöst werden kann. Kann ein Hostname aus einer IP-Gruppe nicht aufgelöst werden, wird dieser Host bei der Regel nicht berücksichtigt. Weitere Einträge in der IP-Gruppe sind davon nicht betroffen und werden berücksichtigt.
	Von Port / Nach Port (Nur 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). **Namen von Portgruppen,** sofern definiert. Bei Angabe des Namens einer Portgruppe werden die Ports oder Portbereiche berücksichtigt, die unter diesem Namen gespeichert sind (siehe Registerkarte „IP- und Portgruppen“).

Netzwerksicherheit >> Paketfilter >> Regelsätze [...]		
	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 der Auswahl eines Regelsatzes treten die Firewall-Regeln in Kraft, die unter diesem Regelsatz konfiguriert sind (siehe Kapitel 7.1.4). Regelsätze, die IP-Gruppen mit Hostnamen enthalten, sollten aus Sicherheitsgründen nicht in Firewall-Regeln verwendet werden, die als Aktion „Verwerfen“ oder „Abweisen“ ausführen. **Namen von Modbus-TCP-Regelsätzen**, sofern definiert. Bei der Auswahl eines Modbus-TCP-Regelsatzes treten die Firewall-Regeln in Kraft, die unter diesem Regelsatz konfiguriert sind (siehe Kapitel 7.2.1).
	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 – Funktion *Log* aktivieren – oder nicht – Funktion *Log* deaktivieren (werkseitig voreingestellt).

7.1.5 MAC-Filter

Dieser Menüpunkt gehört nicht zum Funktionsumfang der Serie FL MGUARD 2000.
Die Regeln für eingehende und ausgehende Verbindungen gelten nur für den Netzwerkmodus *Stealth*.



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.

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.

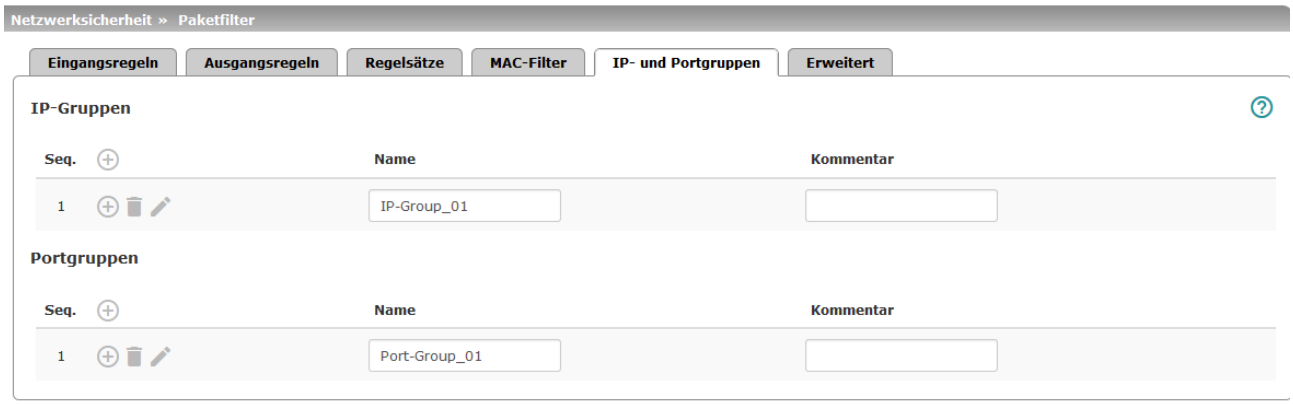
Im Gegensatz zum Paketfilter ist der MAC-Filter stateless. Wenn Regeln eingeführt werden, müssen ebenfalls entsprechende Regeln für die Gegenrichtung erstellt werden. Wenn keine Regel gesetzt ist, sind alle ARP- und IP-Pakete erlaubt.

Achten Sie auf die Hinweise auf dem Bildschirm, wenn Sie MAC-Filterregeln setzen. Die hier angegebenen Regeln haben Vorrang gegenüber den Paketfilter-Regeln. Der MAC-Filter unterstützt keine Logging Funktionalität.

Netzwerksicherheit >> Paketfilter >> MAC-Filter		
Eingehend	**Quell-MAC**	xx:xx:xx:xx:xx:xx steht für alle MAC-Adressen.
	Ziel-MAC	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.
	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.

Netzwerksicherheit >> Paketfilter >> MAC-Filter [...]		
	Kommentar	Ein frei wählbarer Kommentar für diese Regel.
Ausgehend	Die Erklärung unter „Eingehend“ gilt auch für „Ausgehend“.	

7.1.6 IP- und Portgruppen



Mithilfe von IP- und Portgruppen lassen sich Firewall- und NAT-Regeln in komplexen Netzwerkstrukturen einfacher anlegen und verwalten.

Hostnamen, IP-Adressen, IP-Bereiche und Netzwerke können in IP-Gruppen zusammengefasst und mit einem Namen bezeichnet werden. Ports oder Portbereiche lassen sich ebenfalls in Portgruppen zusammenfassen.

Wird eine Firewall- oder NAT-Regel angelegt, können die IP- oder Portgruppen direkt anstelle von IP-Adressen/IP-Bereichen bzw. Ports/Portbereichen in den entsprechenden Feldern ausgewählt und der Regel zugewiesen werden.

ACHTUNG: Unwirksame Firewallregeln durch leere IP- oder Portgruppen

Verwenden Sie keine leeren IP- oder Portgruppen, also angelegte Gruppen, in denen keine Werte konfiguriert sind. Firewallregeln, die auf leere IP- oder Portgruppen verweisen, sind unwirksam.

ACHTUNG: Bei der Verwendung von Hostnamen besteht grundsätzlich die Gefahr, dass ein Angreifer DNS-Anfragen manipuliert oder blockiert (u. a. *DNS spoofing*). Konfigurieren Sie deshalb im mGuard nur vertrauenswürdige und abgesicherte DNS-Server aus Ihrem internen Firmennetzwerk, um entsprechende Angriffe zu vermeiden.

IP-Gruppen, die Hostnamen enthalten, sollten aus Sicherheitsgründen nicht in Firewall-Regeln verwendet werden, die als Aktion „Verwerfen“ oder „Abweisen“ ausführen.

Verwendung von Hostnamen

Die Adressauflösung von Hostnamen erfolgt entsprechend den DNS-Einstellungen des mGuards (siehe „Netzwerk >> DNS“ auf Seite 160).

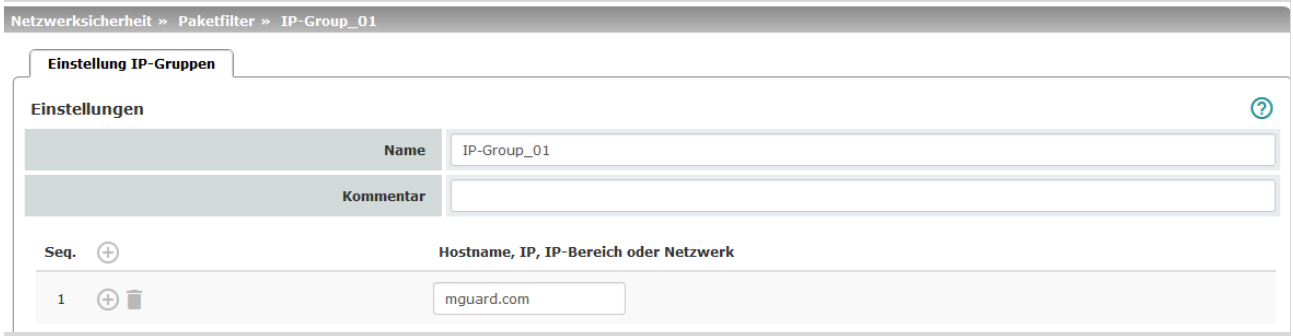
Wenn ein Hostname in mehrere IP-Adressen aufgelöst werden kann, werden alle vom DNS-Server zurückgelieferten IP-Adressen berücksichtigt.

Kann ein Hostnamen aus einer IP-Gruppe nicht aufgelöst werden, weil z. B. ein DNS-Server nicht konfiguriert wurde oder nicht erreichbar ist, wird dieser Host bei der Regel nicht berücksichtigt. Weitere Einträge in der IP-Gruppe sind davon nicht betroffen und werden berücksichtigt.

Wenn ein DNS-Server einen aufgelösten Hostnamen nach Ablauf der TTL mit einer anderen IP-Adresse auflöst, wird eine bestehende Verbindung mit der ursprünglichen IP-Adresse **nicht abgebrochen**.

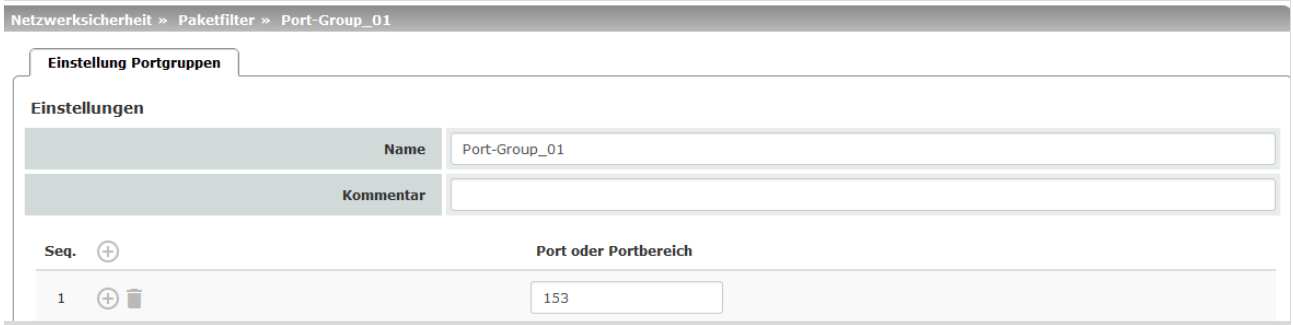
mGuard-Geräte der FL MGUARD 2000-Serie
Die Verwendung von Hostnamen in IP-Gruppen wird von Geräten der FL MGUARD 2000-Serie nicht unterstützt.

Netzwerksicherheit >> Paketfilter >> IP- und Portgruppen		
IP-Gruppen	**Name**	Sie können die IP-Gruppe frei benennen bzw. umbenennen.
	Kommentar	Ein frei wählbarer Kommentar für diese Gruppe/Regel.
Editieren	Nach Klicken auf das Icon **Zeile bearbeiten** erscheint folgende Registerkarte:	



Einstellung IP-Gruppen	**Name**	Sie können die IP-Gruppe frei benennen bzw. umbenennen.
	Kommentar	Ein frei wählbarer Kommentar für diese Gruppe/Regel.
	Hostname, IP, IP-Bereich oder Netzwerk	Die Einträge können einen Hostnamen (z. B. mguard.com), eine IP-Adresse (z. B. 192.168.3.1), einen IP-Adressbereich (z. B. 192.168.3.1-192.168.3.10) oder ein Netzwerk in CIDR-Schreibweise (z. B. 192.168.1.0/24) angeben. Die Verwendung von mehr als 200 Hostnamen in IP-Gruppen wird nicht unterstützt. Bei der Verwendung von Hostnamen besteht grundsätzlich die Gefahr, dass ein Angreifer DNS-Anfragen manipuliert oder blockiert (u. a. *DNS spoofing*). Konfigurieren Sie deshalb im mGuard nur vertrauenswürdige und abgesicherte DNS-Server aus Ihrem internen Firmennetzwerk, um entsprechende Angriffe zu vermeiden.
Portgruppen	**Name**	Sie können die Portgruppe frei benennen bzw. umbenennen.
	Kommentar	Ein frei wählbarer Kommentar für diese Gruppe/Regel.
Editieren	Nach Klicken auf das Icon **Zeile bearbeiten** erscheint folgende Registerkarte:	

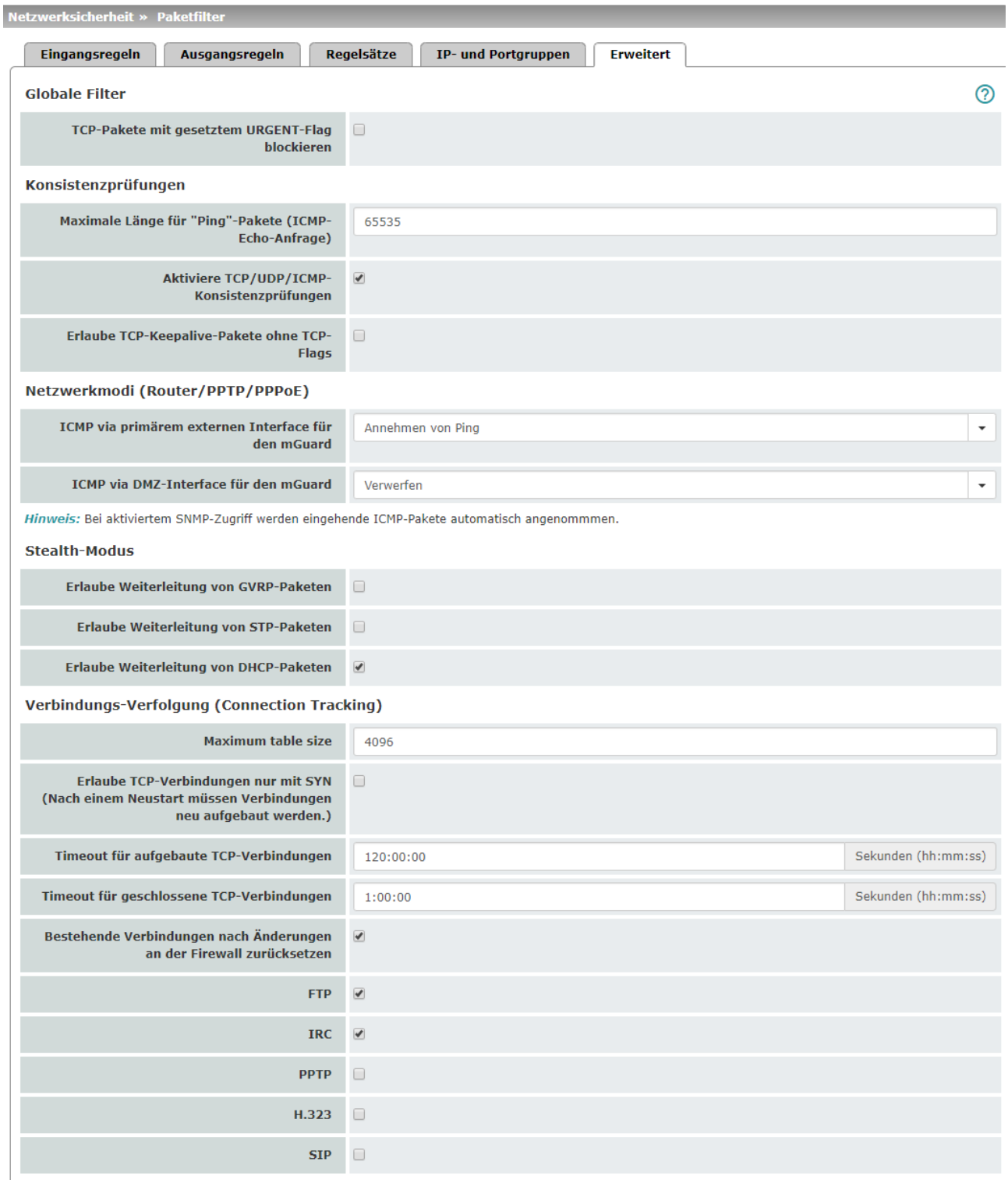
Netzwerksicherheit >> Paketfilter >> IP- und Portgruppen [...]



Einstellung Portgruppen	**Name**	Sie können die Portgruppe frei benennen bzw. umbenennen.
	Kommentar	Ein frei wählbarer Kommentar für diese Gruppe/Regel.
	Port oder Portbereich	Die Einträge können einen Port (z. B. pop3 oder 110) oder einen Portbereich angeben (z. B. 110:120 oder 110-120).

7.1.7 Erweitert

Die Einstellungen betreffen das grundlegende Verhalten der Firewall.



Netzwerksicherheit >> Paketfilter >> Erweitert		
Globale Filter (Dieser Menüpunkt gehört nicht zum Funktionsumfang der Serie FL MGUARD 2000.)	**TCP-Pakete mit gesetztem URGENT-Flag blockieren**	Bei aktivierter Funktion werden Pakete mit im TCP-Header gesetztem URGENT-Flag blockiert: – Im Netzwerkmodus „*Router*“ werden die Verbindungen, über die entsprechende Pakete gesendet werden, beendet. – Im Netzwerkmodus „*Stealth*“ werden die entsprechenden Pakete verworfen. TCP-Pakete mit gesetztem URGENT-Flag, die durch einen VPN-Tunnel geroutet werden, werden ebenfalls blockiert.
Konsistenzprüfungen (Dieser Menüpunkt gehört nicht zum Funktionsumfang der Serie FL MGUARD 2000.)	**Maximale Länge für „Ping“ Pakete (ICMP-Echo-Anfrage)**	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-Anfragen nicht blockiert werden.
	Aktiviere TCP/UDP/ICMP-Konsistenzprüfungen	Bei aktivierter Funktion führt der mGuard eine Reihe von Tests auf falsche Prüfsummen, Paketgrößen, usw. durch und verwirft Pakete, die die Tests nicht bestehen. Werkseitig ist die Funktion deaktiviert.
	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 **aktivierte Funktion** 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 „Verbindungs-Verfolgung (Connection Tracking)“ auf Seite 233). 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. Eine **Aktivierung** ist also eine Abschwächung der Sicherheitsfunktion, die der mGuard bietet.

Netzwerksicherheit >> Paketfilter >> Erweitert [...]		
Netzwerk-Modi (Router / PPTP / PPPoE)	**ICMP via primärem externen Interface für den mGuard** **ICMP via DMZ für den mGuard**	Mit dieser Option können Sie das Verhalten beim Empfang von ICMP-Nachrichten beeinflussen, die aus dem externen Netz über das primäre 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 zu allen IP-Adressen des mGuards werden verworfen. **Annehmen von Ping**: Nur Ping-Nachrichten (ICMP Typ 8) zu allen IP-Adressen des mGuards werden akzeptiert. **Alle ICMPs annehmen**: Alle Typen von ICMP-Nachrichten zu allen IP-Adressen des mGuards werden akzeptiert.
Stealth-Modus	**Erlaube Weiterleitung von GVRP-Paketen**	Das GARP VLAN Registration Protocol (GVRP) wird von GVRP-fähigen Switches verwendet, um Konfigurationsinformationen miteinander auszutauschen. Bei **aktivierter Funktion** können GVRP-Pakete den mGuard im *Stealth*-Modus passieren.
	Erlaube Weiterleitung von STP-Paketen	Das Spanning-Tree Protocol (STP) (802.1d) wird von Bridges und Switches verwendet, um Schleifen in der Verkabelung zu entdecken und zu berücksichtigen. Bei **aktivierter Funktion** können STP-Pakete den mGuard im *Stealth*-Modus passieren.
	Erlaube Weiterleitung von DHCP-Paketen	Bei **aktivierter Funktion** wird dem Client erlaubt, über DHCP eine IP-Adresse zu beziehen - unabhängig von den Firewall-Regeln für ausgehenden Datenverkehr. Werkseitig ist die Funktion **aktiviert**.

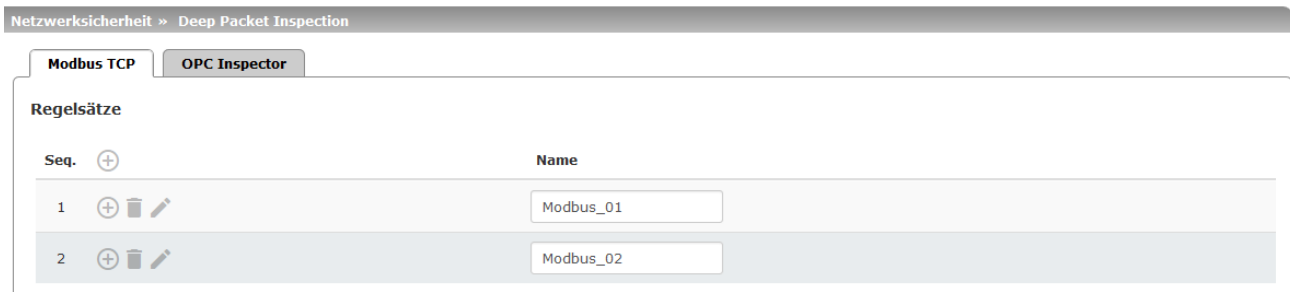
Netzwerksicherheit >> Paketfilter >> Erweitert [...]		
Verbindungs-Verfolgung (Connection Tracking)	**Maximale Zahl gleichzeitiger Verbindungen**	Dieser Eintrag legt eine Obergrenze fest. Diese ist so gewählt, dass sie bei normalem praktischen Einsatz nie erreicht wird. Bei Angriffen kann sie dagegen 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	SYN ist ein spezielles Datenpaket im TCP/IP-Verbindungsaufbau, das den Anfang des Verbindungsaufbaus markiert. **Funktion deaktiviert** (**Werkseinstellung**): 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. **Funktion akviert**: 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 die Funktion „Erlaube TCP-Verbindungen nur mit SYN“ aktiviert wurde, dann müssen alle abgelaufen Verbindungen neu aufgebaut werden. Standard: 120 Stunden (120:00:00) Die Eingabe kann aus Sekunden [ss], Minuten und Sekunden [mm:ss] oder Stunden, Minuten und Sekunden [hh:mm:ss] bestehen.
	Timeout für geschlossene TCP-Verbindungen	Der Timeout gibt an, wie lange der mGuard eine TCP-Verbindung noch offen hält, wenn zwar die eine Seite die Verbindung mit einem „FIN-Paket" beendet, die Gegenstelle dies jedoch noch nicht bestätigt hat. Standard: 1 Stunde (1:00:00) Die Eingabe kann aus Sekunden [ss], Minuten und Sekunden [mm:ss] oder Stunden, Minuten und Sekunden [hh:mm:ss] bestehen.

Netzwerksicherheit >> Paketfilter >> Erweitert [...]	
Bestehende Verbindungen nach Änderungen an der Firewall zurücksetzen	Bei **aktivierter Funktion (Werkseinstellung)** werden die bestehenden Verbindungen zurückgesetzt, – wenn die Funktion „Erlaube TCP-Verbindungen nur mit SYN“ aktiviert wurde und – wenn die Firewall-Regeln angepasst wurden oder – wenn die Funktion aktiviert 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 **inaktivierter Funktion** bleiben die Verbindungen bestehen, auch wenn die geänderten Firewall-Regeln diese nicht erlauben oder beenden würden.
FTP	Wird beim FTP-Protokoll eine ausgehende Verbindung hergestellt, um Daten abzurufen, gibt es zwei Varianten der Datenübertragung: 1. Beim „aktiven FTP“ stellt der angerufene Server im Gegenzug eine zusätzliche Verbindung zum Anrufer her, um auf dieser Verbindung die Daten zu übertragen. 2. 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“ **aktiviert** sein (Werkseinstellung).
IRC	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 **aktiviert** sein (Werkseinstellung).
PPTP	**Standard: deaktivert** Muss **aktiviert** sein, wenn von lokalen Rechnern ohne Zuhilfenahme des mGuards VPN-Verbindungen mittels PPTP zu externen Rechner aufgebaut werden können sollen.Muss **aktiviert** sein, wenn GRE-Pakete von intern nach extern weiter geleitet werden müssen.
H.323	**Standard: deaktivert** Protokoll, das zum Aufbau von Kommunikationssitzungen mit zwei oder mehr Teilnehmern dient. Wird für audio-visuelle Übertragungen verwendet. Dieses Protokoll ist älter als SIP.

Netzwerksicherheit >> Paketfilter >> Erweitert [...]		
	SIP	**Standard: deaktiviert** Das SIP (Session Initiation Protocol) dient zum Aufbau von Kommunikationssitzungen mit zwei oder mehr Teilnehmern. Wird häufig bei der IP-Telefonie verwendet. Bei **aktivierter Funktion** kann der mGuard das SIP verfolgen und dynamisch notwendige Firewall-Regeln einfügen, 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.

7.2 Netzwerksicherheit >> Deep Packet Inspection

7.2.1 Modbus TCP



Für die Integration von Automatisierungsgeräten wird in der Industrie häufig das Modbus-Protokoll eingesetzt. Es ermöglicht den Austausch von Prozessdaten zwischen Modbus-Kontrollern unabhängig von der Netzwerkstruktur. Modbus ist ein Client/Server-Protokoll.

Zur Übertragung von Daten im industriellen Ethernet wird die TCP/IP-Variante des Protokolls verwendet: **Modbus TCP**. Der Zugriff auf bestimmte Gerätedaten über das Modbus-TCP-Protokoll wird über sogenannte **Funktionscodes** gesteuert.

Die Übertragung über das Modbus-TCP-Protokoll erfolgt in der Regel über den **reservierten TCP-Port 502.**

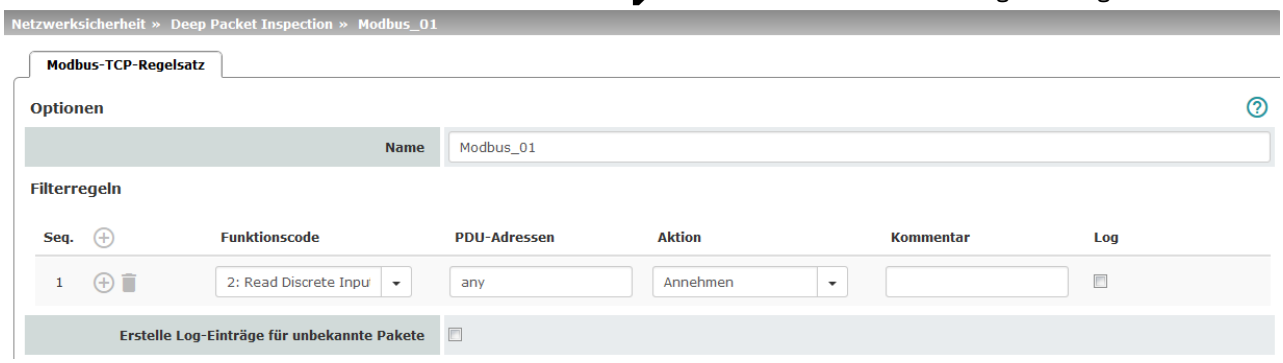
Deep Packet Inspection (DPI)

Der mGuard kann Pakete ein- und ausgehender Modbus-TCP-Verbindungen prüfen (*Deep Packet Inspection*) und bei Bedarf filtern. Geprüft werden die Nutzdaten der eingehenden Pakete. Antworten auf gefilterte Anfragen werden keiner DPI mehr unterzogen.

Pakete, die bestimmte Funktionscodes verwenden, können über definierte Regeln „verworfen“ oder „angenommen“ werden.

Enthält ein TCP-Paket mehr als eine *Protocol Data Unit* (PDU), wird das Paket grundsätzlich verworfen.

Nach Klicken auf das Icon **Zeile bearbeiten** erscheint folgende Registerkarte:



Netzwerksicherheit >> Deep Packet Inspection >> Modbus TCP >> Regelsätze >> Edit

Modbus-TCP-Regelsätze

Die Regeln für die Filterung von Modbus-TCP-Paketen werden in Regelsätzen konfiguriert. Diese Regelsätze können in den folgenden Firewall-Tabellen verwendet werden, wenn dort als Protokoll „TCP“ ausgewählt ist: Allgemeiner Paketfilter / DMZ / IPsec-VPN / OpenVPN.

Verwendet eine Firewall-Regel einen Modbus-TCP-Regelsatz, ist über eine betroffene Verbindung, die nicht das Modbus-Protokoll verwendet, kein Datenverkehr möglich.

Wenn der mGuard nicht bestimmen kann, ob ein Modbus-Paket ein- oder ausgehend ist, wird das Paket verworfen.

Dieser Fall tritt z. B. ein, wenn der Status der Verbindungs-Verfolgung (*Connection Tracking*) nach dem Aufbau der Verbindung gelöscht wurde und der mGuard somit das SYN-Paket der bestehenden Verbindung nicht registriert hat.

Optionen

Name — Ein beschreibender Name

Filterregeln

Funktionscode — **1 – 255 / Name des Funktionscodes / any**

Funktionscodes in Modbus-TCP-Verbindungen geben den Zweck der Datenübertragung an, d. h., welche Operation aufgrund der Anfrage des Clients (Masters) vom Server (Slave) ausgeführt werden soll.

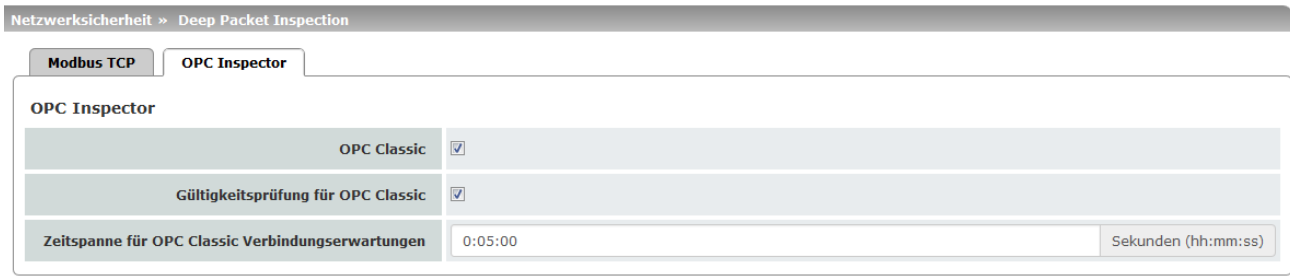
Sie können den Funktionscode aus der Drop-Down-Liste auswählen oder direkt in das Eingabefeld eingeben.

Netzwerksicherheit >> Deep Packet Inspection >> Modbus TCP >> Regelsätze >> Edit

PDU-Adressen	**0 – 65535 | any**
(Wird nur bei bestimmten Funktionscodes angezeigt)	Bestimmten Funktionscodes können verschiedene Adressen (als PDU-Adressen zur Basis 0) zugeordnet werden. Dabei kann es sich um einzelne PDU-Adressen (z. B. 47015) oder um Adressbereiche (z. B. 47010:47020) handeln. Der PDU-Adressbereich eingehender Pakete kann sich **teilweise oder vollständig** im angegebenen Adressbereich der Filter-Regel befinden. Wann eine Regel zutrifft, hängt davon ab, welche **Aktion (Verwerfen oder Annehmen)** die Regel ausführt: 1. **Verwerfen-Regel**: Ist als Aktion „Verwerfen“ ausgewählt, trifft die Regel zu (d. h. das Paket wird verworfen), wenn sich **mindestens eine Adresse** im Paket im angegebenen Adressbereich befindet. Sie trifft auch dann zu, wenn das Paket darüber hinaus weitere Adressen enthält, die sich nicht im angegebenen Adressbereich befinden. 2. **Annehmen-Regel**: Ist als Aktion „Annehmen“ ausgewählt, trifft die Regel zu (d. h. ein Paket wird angenommen), wenn sich **alle Adressen** im Paket im angegebenen Adressbereich befinden. Eine einzelne Adresse wird im Sinne des oben genannten Verhaltens als Bereich aufgefasst.
Aktion	**Annehmen** bedeutet, die Datenpakete dürfen passieren. **Verwerfen** bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass die TCP-Verbindung unbrauchbar wird. Sie kann also nicht zur weiteren Datenübertragung genutzt werden. Für folgende Modbus-Anfragen muss eine neue TCP-Verbindung aufgebaut werden. Sind mehrere 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. Wenn keine Regel zutrifft, wird das Paket verworfen.
Kommentar	Ein frei wählbarer Kommentar für diese Regel.
Log	Für jeden einzelnen Modbus-TCP-Filter können Sie festlegen, ob bei Greifen der Regel – das Ereignis protokolliert werden soll - Aktion *Log* aktivieren – oder nicht - Aktion *Log* deaktivieren (Standard).

Netzwerksicherheit >> Deep Packet Inspection >> Modbus TCP >> Regelsätze >> Edit		
	Erstelle Log-Einträge für unbekannte Pakete	Bei aktivierter Funktion werden auch die Pakete, die durch keine der erstellten Filterregeln erfasst werden, geloggt.

7.2.2 OPC Inspector



Netzwerksicherheit >> Deep Packet Inspection >> OPC Inspector

OPC Inspector

Die Nutzung des Netzwerk-Protokolls *OPC Classic* durch eine Firewall hindurch ist bislang nur möglich, wenn große Port-Bereiche geöffnet werden. Die Aktivierung der *OPC Classic*-Funktion erlaubt die einfache Nutzung dieses Netzwerk-Protokolls, ohne die Firewall des mGuard-Geräts unsicher konfigurieren zu müssen.

Wenn die OPC Classic-Funktion aktiviert wird, werden die OPC-Pakete überwacht. Die TCP-Ports, die innerhalb der ersten geöffneten Verbindung ausgehandelten werden, werden erkannt und für OPC-Pakete geöffnet. Wenn über diese Ports innerhalb eines konfigurierbaren Timeouts keine OPC-Pakete versendet werden, werden diese wieder geschlossen.

Wenn die OPC-Gültigkeitsprüfung aktiviert ist, dürfen über den OPC Classic-Port 135 ausschließlich OPC-Pakete gesendet werden.

OPC Classic

Beim Netzwerk-Protokoll OPC Classic beginnt eine Kommunikation immer über TCP-Port 135. Dann handeln Client und Server über diesen Port eine oder mehrere weitere Verbindungen auf neuen Ports aus. Um diese Verbindungen zuzulassen, musste man bisher alle Ports einer dazwischen geschalteten Firewall geöffnet lassen.

Wenn die Funktion OPC Classic aktiviert ist, dann reicht es, über die Firewall-Regeln einem Client-Server-Paar nur den TCP-Port 135 zu erlauben.

Der mGuard schaut in die Nutzdaten der Pakete (*Deep Packet Inspection*). Er prüft in den Nutzdaten, die über diesen Port versendet werden, ob eine neue Verbindung ausgehandelt wurde und öffnet den ausgehandelten Port. Hierzu muss die Kommunikation zwischen Client und Server auf Port 135 in beide Richtungen erlaubt werden.

Die Funktionalität von OPC Classic wird auch bei den NAT-Verfahren *IP Masquerading* und *1:1-NAT* unterstützt.

Gültigkeitsprüfung für OPC Classic

Wenn die Gültigkeitsprüfung für OPC Classic aktiviert ist, dann dürfen über den OPC Classic-Port 135 (TCP) und die neu ausgehandelten Ports nur OPC-Pakete gesendet werden.

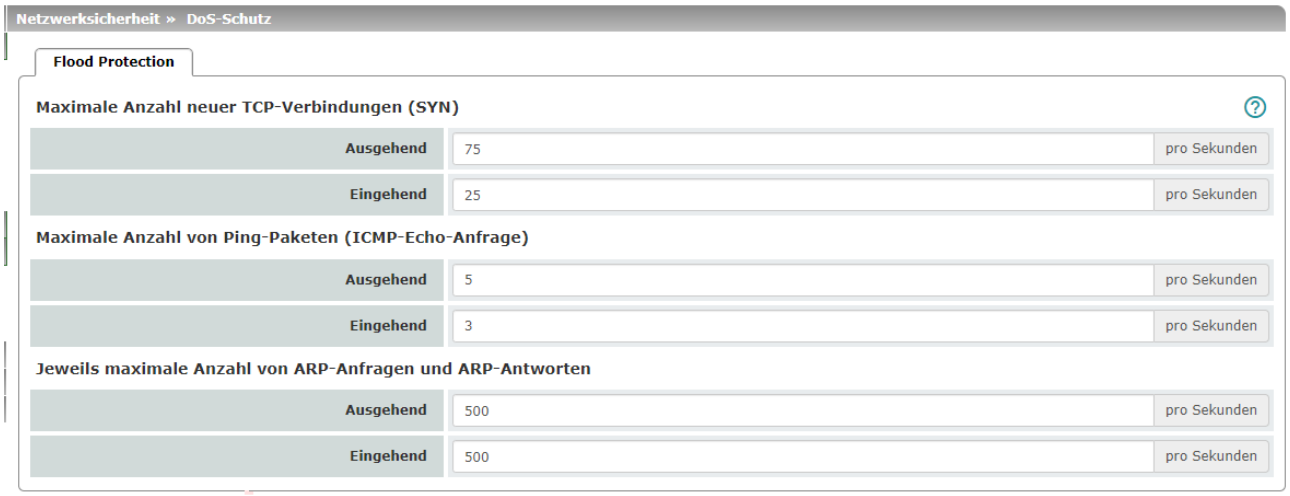
Netzwerksicherheit >> Deep Packet Inspection >> OPC Inspector		
	Zeitspanne für OPC Classic Verbindungs-erwartungen	Konfiguriert die Zeitspanne (Sekunden), in der OPC-Traffic erwartet wird. Eine bestehende OPC-Verbindung kann eine weitere Verbindung auf einem neuen Port aushandeln. Wenn die „Gültigkeitsprüfung für OPC Classic“ aktiviert ist, dürfen diese Verbindungen nur OPC-Verbindungen sein. Der mGuard legt eine neue dynamische Firewall-Regel an, wenn er im OPC-Traffic erkennt, dass eine neue OPC-Verbindung aufgebaut werden soll. Die dynamische Firewall-Regel akzeptiert sofort neue OPC-Verbindungen mit den ausgehandelten Parametern. Läuft der Timeout für die dynamische Firewall-Regel ab, wird die Regel gelöscht. Neue Verbindungen mit diesen Parametern werden dann nicht mehr akzeptiert. Bereits aufgebaute Verbindungen werden nicht geschlossen.

7.3 Netzwerksicherheit >> DoS-Schutz

7.3.1 Flood Protection

Dieses Menü steht **nicht** auf Geräten der FL MGUARD 2000-Serie zur Verfügung.

ACHTUNG: Firewall-Einstellung beeinflusst DoS-Schutz
Der DoS-Schutz des Geräts steht nicht zur Verfügung, wenn unter **Netzwerksicherheit >> Paketfilter >> Eingangsregeln** als **Allgemeine Firewall-Einstellung** „*Alle Verbindungen annehmen*“ ausgewählt ist (siehe „Eingangsregeln“ auf Seite 211).
Um den DoS-Schutz in diesem Fall bereitzustellen, müssen Sie die **Allgemeine Firewall-Einstellung** „*Wende das unten angegebene Regelwerk an*“ auswählen und anschließend eine Firewall-Regel erstellen, mit der alle Verbindungen angenommen werden.



Netzwerksicherheit >> DoS-Schutz >> Flood Protection		
Maximale Anzahl neuer TCP-Verbindungen (SYN)	**Ausgehend / Eingehend**	Ausgehend: Standard: 75 Eingehend: Standard: 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 [...]		
Maximale Anzahl von Ping-Paketen (ICMP-Echo-Anfrage)	**Ausgehend / Eingehend**	Ausgehend: Standard: 5 Eingehend: Standard: 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.
Jeweils maximale Anzahl von ARP-Anfragen und ARP-Antworten (Nur im Netzwerkmodus „Stealth“)	**Ausgehend / Eingehend**	Standard: 500 Maximalwerte für die zugelassenen ein- und ausgehenden ARP-Anfragen oder Antworten 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.

7.4 Netzwerksicherheit >> Benutzerfirewall

Dieses Menü steht **nicht** auf Geräten der FL MGUARD 2000-Serie zur Verfügung.

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 185).

Jedem Firewall-Benutzer kann ein Satz von Firewall-Regeln, ein sogenanntes Template, zugeordnet werden.

Wenn ein Benutzerfirewall-Template oder eine Firewall-Regel eines Templates hinzugefügt, geändert, gelöscht oder deaktiviert wird, sind sofort alle eingeloggten Firewall-Benutzer betroffen.

Bestehende Verbindungen werden unterbrochen. Eine Ausnahme bildet die Änderung von Benutzerfirewall-Regeln, wenn unter **„Netzwerksicherheit >> Paketfilter >> Erweitert“** die Funktion *„Bestehende Verbindungen nach Änderungen an der Firewall zurücksetzen“* deaktiviert ist. In diesem Fall wird eine Netzwerkverbindung, die aufgrund einer vorher erlaubten Regel besteht, nicht unterbrochen.

Wenn ein Firewall-Regelsatz (Template) deaktiviert wird, werden betroffene eingeloggte Firewall-Benutzer weiter als *eingeloggt* angezeigt. Die Firewall-Regeln aus dem **deaktivierten** Template gelten allerdings nicht mehr für sie.

Wenn ein Firewall-Regelsatz (Template) **deaktiviert** und anschließend wieder **aktiviert** wird, müssen sich betroffene eingeloggte Firewall-Benutzer zunächst ausloggen und dann wieder einloggen, um die Firewall-Regeln aus dem Template erneut für sich zu aktivieren.

7.4.1 Benutzerfirewall-Templates

Hier werden alle definierten Benutzerfirewall-Templates aufgelistet. Ein Template kann aus mehreren Firewall-Regeln bestehen. Ein Template kann mehreren Nutzern zugeordnet sein.

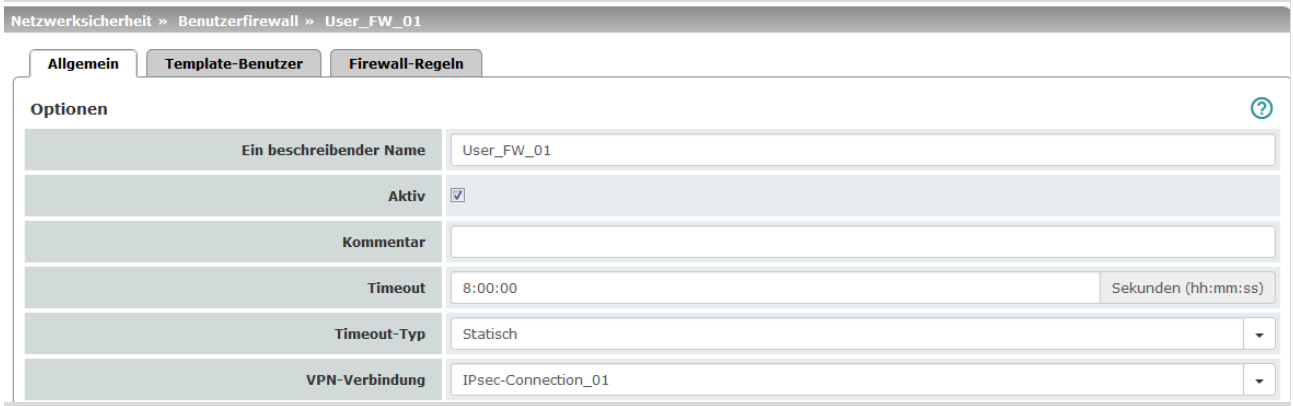
Template neu definieren:

- In der Tabelle der Templates auf das Icon ⊕ **Neue Zeile einfügen** klicken, um eine neue Tabellenzeile hinzuzufügen.
- Auf das Icon **Zeile bearbeiten** klicken.

Template bearbeiten:

- In der gewünschten Zeile auf das Icon **Zeile bearbeiten** klicken.

Netzwerksicherheit >> Benutzerfirewall >> Benutzerfirewall-Templates		
	Aktiv	Aktiviert / deaktiviert das betreffende Template.
	Ein beschreibender Name	Name des Templates. Der Name ist beim Erstellen des Templates festgelegt worden.
Allgemein	Nach Klicken auf das Icon **Zeile bearbeiten** erscheint folgende Registerkarte:	



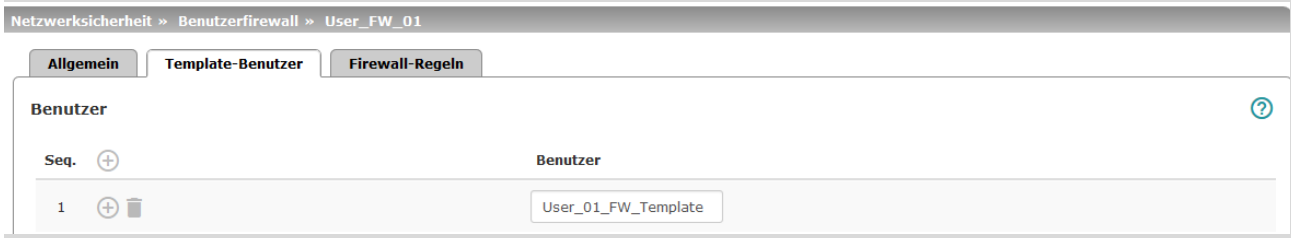
Optionen	**Ein beschreibender Name**	Sie können das Benutzerfirewall-Template frei benennen bzw. umbenennen.
	Aktiv	Bei aktivierter Funktion ist das Benutzerfirewall-Template aktiv, sobald sich Firewall-Benutzer beim mGuard anmelden, die auf der Registerkarte *Template Benutzer* (s. u.) erfasst sind 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: 8 Stunden (8:00:00) Gibt 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. Die Eingabe kann aus Sekunden [ss], Minuten und Sekunden [mm:ss] oder Stunden, Minuten und Sekunden [hh:mm:ss] bestehen.

Netzwerksicherheit >> Benutzerfirewall >> Benutzerfirewall-Templates [...]		
	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 Benutzer 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 „Timeout für aufgebaute TCP-Verbindungen“ auf Seite 233.) Hinzukommen zusätzlich 120 s nach Schließen der Verbindung. (Diese 120 s gelten auch nach dem Schließen durch den Benutzer.) – UDP: 30 s nach Datenverkehr in einer Richtung; 120 s nach Datenverkehr in beide Richtungen – ICMP: 30 s – Andere: 10 min
	VPN-Verbindung	Gibt die VPN-Verbindung an, in der diese Benutzerfirewall-Regel gültig ist. Bedingung ist ein bestehender Remote-Zugang durch den VPN-Tunnel auf die Web-Oberfläche.

Netzwerksicherheit >> Benutzerfirewall >> Benutzerfirewall-Templates >> Editieren > ...

Template-Benutzer

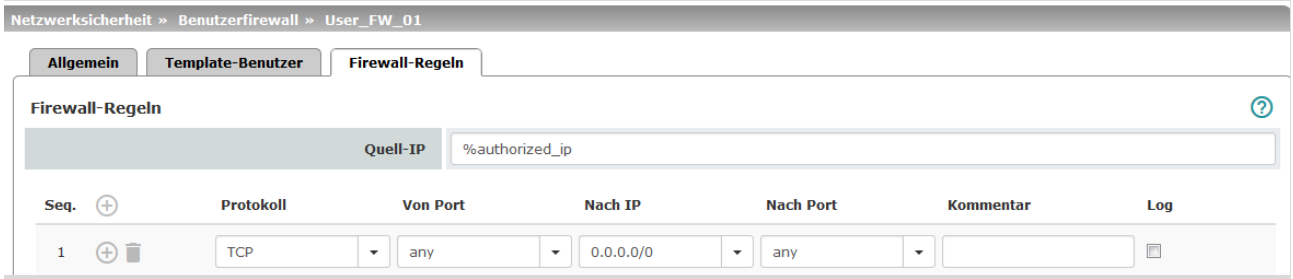
Geben Sie die Namen von Benutzern an. Die Namen müssen denen entsprechen, die unter Menü „Authentifizierung >> Firewall-Benutzer“ festgelegt sind (siehe Seite 185).



Firewall-Regeln

Firewall-Regeln für die Benutzerfirewall-Templates.

Wenn das Template mit **dynamischem Timeout** konfiguriert ist, setzen an dieser Stelle zugelassene UDP und andere Netzwerkpakete (außer ICMP) den dynamischen Timeout auf den Ausgangswert zurück.



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

(Nur 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).

Namen von Portgruppen, sofern definiert. Bei Angabe des Namens einer Portgruppe werden die Ports oder Portbereiche berücksichtigt, die unter diesem Namen gespeichert sind (siehe „IP- und Portgruppen“ auf Seite 227).

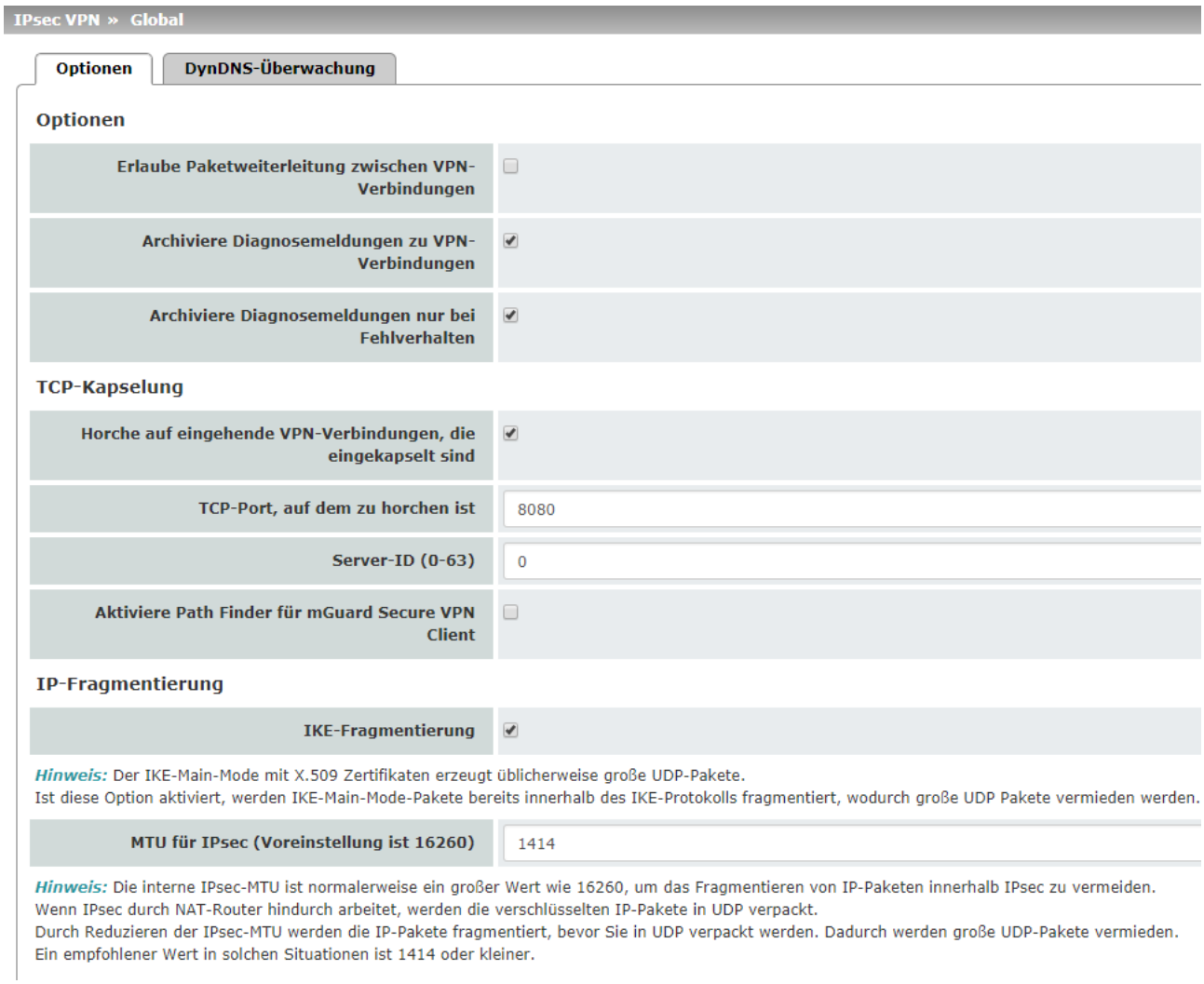
Netzwerksicherheit >> Benutzerfirewall >> Benutzerfirewall-Templates >> Editieren > ... [...]

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 43). **Namen von IP-Gruppen**, sofern definiert. Bei Angabe des Namens einer IP-Gruppe werden die Hostnamen, IP-Adressen, IP-Bereiche oder Netzwerke berücksichtigt, die unter diesem Namen gespeichert sind (siehe „IP- und Portgruppen“ auf Seite 227). Werden Hostnamen in IP-Gruppen verwendet, muss der mGuard so konfiguriert sein, dass der Hostname von einem DNS-Server in eine IP-Adresse aufgelöst werden kann. Kann ein Hostname aus einer IP-Gruppe nicht aufgelöst werden, wird dieser Host bei der Regel nicht berücksichtigt. Weitere Einträge in der IP-Gruppe sind davon nicht betroffen und werden berücksichtigt.
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 – Funktion *Log* aktivieren – oder nicht – Funktion *Log* deaktivieren (werkseitig voreingestellt).

8 Menü IPsec VPN

8.1 IPsec VPN >> Global

8.1.1 Optionen



IPsec VPN >> Global >> Optionen

Optionen

Erlaube Paketweiterleitung zwischen VPN-Verbindungen

Die Funktion 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-NAT für IPsec-Tunnelverbindungen“ auf Seite 278).

Die Funktion wird im Netzwerk-Modus *Stealth* nicht unterstützt.

Bei **deaktivierter Funktion** (Standard): VPN-Verbindungen existieren für sich separat. Es finden keine Paketweiterleitungen zwischen den konfigurierten VPN-Verbindungen statt.

Bei **aktivierter Funktion**: „Hub and Spoke“-Feature eingeschaltet: Der mGuard als Zentrale unterhält VPN-Verbindungen zu mehreren Zweigstellen, die dann auch untereinander kommunizieren können.

Die Einstellung ist auch für OpenVPN-Verbindungen gültig.

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 283).

Bei „Hub and Spoke“ wird 1:1-NAT der Gegenstelle nicht unterstützt.

IPsec VPN >> Global >> Optionen [...]		
	Archiviere Diagnosemeldungen zu VPN-Verbindungen	**Bei deaktivierter Funktion (Standard)** 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. Wenn sie ausreichend ist, können Sie die Funktion an dieser Stelle deaktivieren. **Bei aktivierter Funktion** 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: – In bestimmten Anwendungsumgebungen, z. B. wenn der mGuard per Maschinensteuerung über den CMD-Kontakt „bedient“ wird , steht die Möglichkeit, dass ein Anwender über die Web-basierte 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.

IPsec VPN >> Global >> Optionen [...]		
		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 (I-Kontakt) oder – über die Icon „Starten“ auf der Web-Oberfläche oder – über das CGI-Interface nph-vpn.cgi per Kommando „synup“ (siehe Application Note: „How to use the CGI Interface“). (Application Notes stehen im Download-Bereich von phoenixcontact.com/products bereit.) Archivierte Logeinträge überleben einen Neustart. Sie können als Bestandteil des Support-Snapshots (Menüpunkt *„Hardware“* heruntergeladen werden. Der Support Ihrer Bezugsquelle 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 Fehlverhalten (Nur wenn **Archivierung** aktiviert ist)	Sollen nach Einschalten der Archivierung nur solche Logeinträge archiviert werden, die bei fehlgeschlagenen Verbindungsaufbauversuchen erzeugt werden, aktivieren Sie die Funktion. Bei deaktivierter Funktion werden alle Logeinträge archiviert.

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 255).

TCP-Kapselung kann nur eingesetzt werden, wenn auf beiden Seiten des VPN-Tunnels ein mGuard (ab Version 6.1) eingesetzt wird. Die Funktion „Path Finder“ kann ab Version 8.3 eingesetzt werden und funktioniert ebenfalls mit dem mGuard Secure VPN Client.

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 erheblich langsamer.

Wenn beim mGuard unter Menüpunkt *„Netzwerk >> Proxy-Einstellungen“* festgelegt ist, 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 Authentication* 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.

Um die Funktion „Path Finder“ zum Aufbau einer VPN-Verbindung mit einem mGuard Secure VPN Client zu benutzen, muss die Funktion auf beiden Seiten der Verbindung (Server und Client) aktiviert werden.

TCP-Kapselung funktioniert nicht in Verbindung mit einer Authentifizierung über Pre-Shared Key (PSK).

TCP-Kapselung funktioniert nur, wenn eine der beiden Seiten auf Verbindungen wartet (**Verbindungsinitiierung: Warte**) und als **Adresse des VPN-Gateways der Gegenstelle „%any“** angegeben ist.

TCP-Kapselung mit aktivierter Funktion „Path Finder“

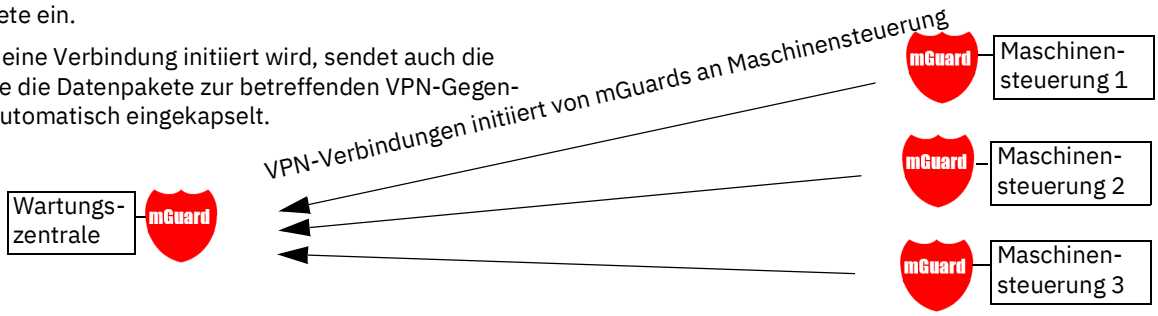
Die TCP-Kapselung mit aktivierter Funktion „Path Finder“ verbessert das Verhalten der oben beschriebenen Standard-TCP-Kapselung.

Wenn die Verbindung neu eingerichtet wird und keine Rückwärtskompatibilität notwendig ist, sollte die Funktion „Path Finder“ verwendet werden.

Wird eine VPN-Verbindung durch den mGuard Secure VPN Client gestartet, der sich hinter einem Proxy-Server oder einer Firewall befindet, muss die Funktion „Path Finder“ sowohl im mGuard Secure VPN Client als auch im mGuard (Server) aktiviert sein. Die über die VPN-Verbindung zu übertragenden Datenpakete werden dabei in TCP-Pakete eingekapselt (siehe „TCP-Kapselung“ auf Seite 253).

Als Teilnehmer der TCP-Kapselung initiieren die mGuards der Maschinensteuerungen 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

- **IPsec VPN >> Global >> Optionen**:
  - Horche auf eingehende VPN-Verbindungen, die eingekapselt sind: **Aktiviert**
- **IPsec VPN >> Verbindungen >> Allgemein**:
  - Adresse des VPN-Gateways der Gegenstelle: **%any**
  - Verbindungsinitiierung: **Warte**

mGuard**s an Maschinensteuererungen**

Erforderliche Grundeinstellungen

- **IPsec VPN >> Global >> Optionen**:
  - Horche auf eingehende VPN-Verbindungen, die eingekapselt sind: **Deaktiviert**
- **IPsec VPN >> Verbindungen >> 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: **TCP-Kapselung oder Path Finder**

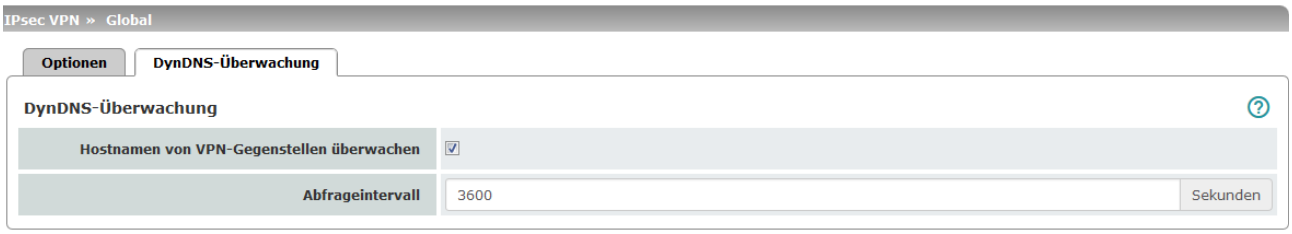
Bild 8-1 TCP-Kapselung bei einem Anwendungsszenario mit Wartungszentrale und ferngewarteten Maschinen über VPN-Verbindungen

IPsec VPN >> Global >> Optionen		
TCP-Kapselung	**Horche auf eingehende VPN-Verbindungen, die eingekapselt sind**	Standardeinstellung: **Deaktiviert** Nur bei Einsatz der Funktion TCP-Kapselung diese Funktion aktivieren. 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.
	TCP-Port, auf dem zu horchen ist (Bei TCP-Kapselung)	**Standard: 8080** Nummer des TCP-Ports, über den die zu empfangenen eingekapselten Datenpakete eingehen. Die hier angegebene Port-Nummer muss mit der Port-Nummer übereinstimmen, die beim mGuard der Gegenstelle als **TCP-Port des Servers, welcher 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 oder HTTPS), – mit dem Port, auf dem bei aktivierter Funktion „Path Finder“ gehorcht wird.
	Server-ID (0-63) **(Bei TCP-Kapselung)**	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.
	Aktiviere Path Finder für mGuard Secure VPN Client	Standardeinstellung: **Deaktiviert** Nur wenn der mGuard eine VPN-Verbindung von einem mGuard Secure VPN Client annehmen soll, der sich hinter einem Proxy-Server oder einer Firewall befindet, diese Funktion aktivieren. Die Funktion „Path Finder“ muss ebenfalls im mGuard Secure VPN Client aktiviert sein.

IPsec VPN >> Global >> Optionen [...]		
	TCP-Port, auf dem zu horchen ist (Bei Path Finder)	**Standard: 443** Nummer des TCP-Ports, über den die zu empfangenen eingekapselten Datenpakete eingehen. Die hier angegebene Port-Nummer muss mit der Port-Nummer übereinstimmen, die bei dem VPN-Client der Gegenstelle als **TCP-Port des Servers**, welcher die gekapselte Verbindung annimmt, festgelegt ist. Der **mGuard Secure VPN Client** verwendet als Ziel-Port immer Port 443. Nur für die Fälle, in denen der Port von einer Firewall zwischen dem mGuard Secure VPN Client und dem mGuard umgeschrieben wird, müsste der Port im mGuard geändert werden. **Es gilt folgende Einschränkung:** Der Port, auf dem zu horchen ist, darf nicht identisch sein – mit einem Port, der für Fernzugriffe benutzt wird (SSH oder HTTPS), – mit dem Port, auf dem bei aktivierter Funktion *TCP-Kapselung* gehorcht wird.
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, aktivieren Sie die Funktion.  Bei aktivierter Funktion 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.

8.1.2 DynDNS-Überwachung



Erläuterung zu DynDNS siehe „DynDNS“ auf Seite 164.

IPsec VPN >> Global >> Optionen		
DynDNS-Überwachung	**Hostnamen von VPN-Gegenstellen überwachen**	Wenn der mGuard die Adresse einer VPN-Gegenstelle als Hostname hat (siehe „VPN-Verbindung / VPN-Verbindungstunnel neu definieren“ auf Seite 261) und dieser Hostname bei einem DynDNS-Service registriert ist, 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	Standard: 300 Sekunden

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.

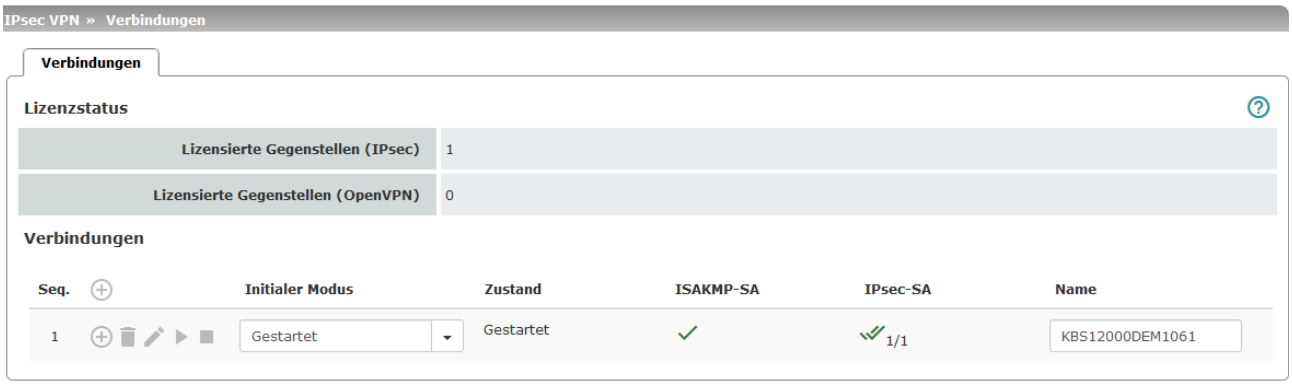
- Die mGuards, die im Netzwerk-Modus Stealth ausgeliefert werden, sind auf die Stealth-Konfiguration „Mehrere Clients“ voreingestellt. In diesem Modus müssen Sie, wenn Sie VPN-Verbindungen nutzen wollen, eine Management IP-Adresse und ein Standard-Gateway konfigurieren (siehe „Standard-Gateway“ auf Seite 145). 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, 5 und 14 – 18)
  - DES-, 3DES- oder AES-Verschlüsselung
  - MD5- und SHA-Hash-Algorithmen
  - Tunnel- oder Transport-Modus
  - XAuth und Mode Config
  - Quick Mode
  - Main Mode
  - SA-Lebensdauer (1 Sekunde bis 24 Stunden)
- Befindet sich die Gegenstelle hinter einem NAT-Router, so muss die Gegenstelle NAT-Traversal (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 Tunnelverbindungen möglich.
- Die Authentifizierung mittels „Pre Shared Key“ im Agressive Mode wird bei der Verwendung von „XAuth“/„Mode Config“ nicht unterstützt. Soll z. B. eine Verbindung vom iOS-oder Android-Client zum mGuard-Server hergestellt werden, muss die Authentifizierung via Zertifikat erfolgen.

Verschlüsselungs- und Hash-Algorithmen

Einige der zur Verfügung stehenden Algorithmen sind veraltet und werden nicht mehr als sicher angesehen. Sie sind deshalb nicht zu empfehlen. Aus Gründen der Abwärtskompatibilität können sie jedoch weiterhin ausgewählt und verwendet werden. Im WBM sind entsprechend veraltete Algorithmen oder unsichere Einstellungen mit einem Sternchen (*) markiert.

ACHTUNG: Verwenden Sie sichere Verschlüsselungs- und Hash-Algorithmen (siehe „Verwendung sicherer Verschlüsselungs- und Hash-Algorithmen“ auf Seite 35).

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-Verbindungstunneln 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.

IPsec VPN >> Verbindungen		
Lizenzstatus	**Lizenzierte Gegenstellen (IPsec)**	Anzahl der Gegenstellen, die aktuell eine VPN-Verbindung über das IPsec-Protokoll aufgebaut haben.
	Lizenzierte Gegenstellen (OpenVPN)	Anzahl der Gegenstellen, zu denen aktuell eine VPN-Verbindung über das OpenVPN-Protokoll aufgebaut ist.
Verbindungen	**Initialer Modus**	**Deaktiviert / Gestoppt / Gestartet** Die Einstellung „**Deaktiviert**“ deaktiviert die VPN-Verbindung permanent; sie kann weder gestartet noch gestoppt werden. Die Einstellungen „**Gestartet**“ und „**Gestoppt**“ bestimmen den Zustand der VPN-Verbindung nach einem Neustart/Booten des mGuards (z. B. nach einer Unterbrechung der Stromversorgung). VPN-Verbindungen, die nicht deaktiviert sind, können über Icons in der Web-Oberfläche, Schalter, Taster, Datenverkehr oder das Skript nph-vpn.cgi gestartet oder gestoppt werden.
	Zustand	Zeigt den aktuellen Aktivierungszustand der IPsec-VPN-Verbindung.
	ISAKMP-SA	Zeigt an, ob die entsprechende ISAKMP-SA aufgebaut wurde oder nicht.
	IPsec-SA	Zeigt an, wie viele der konfigurierten Tunnel aufgebaut sind. Die Anzahl der aufgebauten Tunnel kann höher als die Anzahl der konfigurierten Tunnel sein, wenn die Funktion „Tunnel-Gruppe“ genutzt wird.

IPsec VPN >> Verbindungen[...]		
	Name	Name der VPN-Verbindung

Verbindungen

VPN-Verbindung / VPN-Verbindungstunnel neu definieren

- In der Tabelle der Verbindungen auf das Icon ⊕ **Neue Zeile einfügen** klicken, um eine neue Tabellenzeile hinzuzufügen.
- Auf auf das Icon ✎ **Zeile bearbeiten** klicken.

VPN-Verbindung / VPN-Verbindungstunnel bearbeiten

- In der gewünschten Zeile auf das Icon ✎ **Zeile bearbeiten** klicken.

URL für Starten, Stoppen, Statusabfrage einer VPN-Verbindung

Die folgende URL kann verwendet werden, um VPN-Verbindungen, die sich im initialen Modus „**Gestartet**“ oder „**Gestoppt**“ befinden, zu starten, zu stoppen oder deren Verbindungsstatus abzufragen:

Beispiel

https://server/nph-vpn.cgi?name=verbindung&cmd=(up|down|status)
curl --insecure "https://admin:mGuard@192.168.1.1/nph-vpn.cgi?name=Athen&cmd=up“

Die Verwendung des Kommandozeilen-Tools *wget* wird nicht unterstützt. Ab mGuard-Firmware-Version 8.4.0 kann das Kommandozeilen-Tool *curl* verwendet werden (Parameter und Optionen abweichend!).

Das Admin-Passwort und der Name, auf den sich eine Aktion bezieht, dürfen ausschließlich folgende Zeichen enthalten:

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

Andere Sonderzeichen, z. B. das Leerzeichen oder das Fragezeichen, müssen entsprechend codiert werden (siehe „Codierung von Sonderzeichen (URL encoding)“ auf Seite 373).

Die Option ***--insecure*** (*curl*) sorgt dafür, dass das HTTPS-Zertifikat des mGuards nicht weiter geprüft wird.

Ein solches Kommando bezieht sich auf alle Verbindungstunnel, die unter dem betreffenden Namen, in diesem Beispiel *Athen*, zusammengefasst sind. Das ist der Name, der unter *„IPsec VPN >> Verbindungen >> Editieren >> Allgemein“* als *„Ein beschreibender Name für die Verbindung“* aufgeführt ist. Sofern Mehrdeutigkeit besteht, wirkt der Aufruf des URL nur auf den ersten Eintrag in der Liste der Verbindungen.

Ein Ansprechen einzelner Tunnel einer VPN-Verbindung ist nicht möglich. Wenn einzelne Tunnel deaktiviert sind, werden diese nicht gestartet. Damit hat das Starten und Stoppen auf diesem Wege keine Auswirkung auf die Einstellungen zu den einzelnen Tunneln (siehe „Transport- und Tunneleinstellungen“ auf Seite 272).

Wenn durch Verwendung der oben angegeben URL der Status einer VPN-Verbindung abgefragt wird, können folgende Antworten erwartet werden:

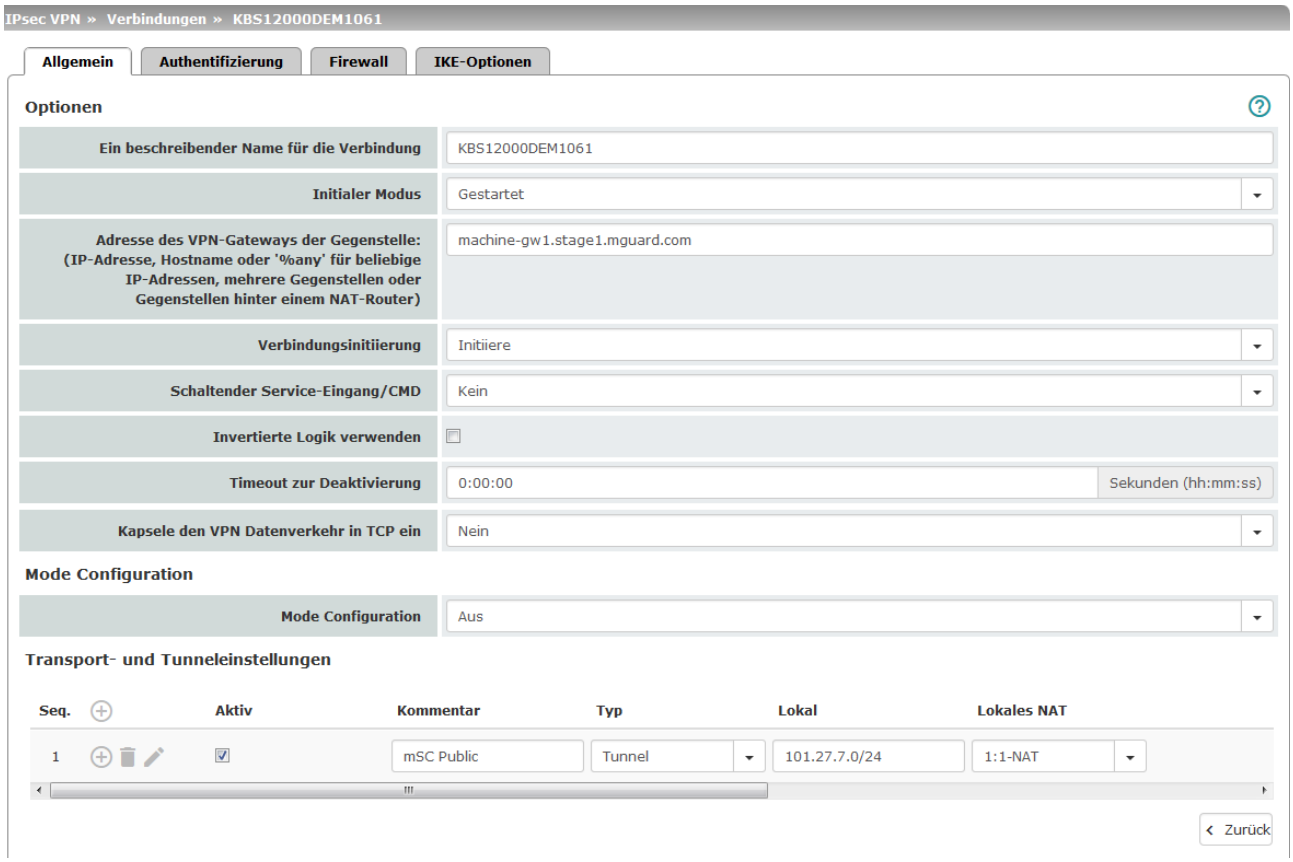
Tabelle 8-1 Status einer VPN-Verbindung

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 (I-Kontaktes) freigeschaltet worden ist.
ready	Die Verbindung ist bereit, selbst Tunnel aufzubauen oder hereinkommende Anfragen zum Tunnelaufbau zu erlauben.
active	Zu der Verbindung ist mindestens ein Tunnel auch wirklich aufgebaut.

VPN-Verbindung / VPN-Verbindungstunnel definieren

Nach Klicken auf das Icon **Zeile bearbeiten** erscheint je nach Netzwerk-Modus des mGuards folgende Seite.

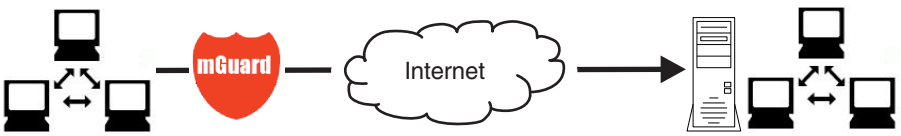
8.2.2 Allgemein



IPsec VPN >> Verbindungen >> Editieren >> Allgemein		
Optionen	**Ein beschreibender Name für die Verbindung**	Sie können die Verbindung frei benennen bzw. umbenennen. Werden weiter unten unter „“ mehrere Verbindungstunnel definiert, benennt dieser Name das gesamte Set der VPN-Verbindungstunnel, die unter diesem Namen zusammengefasst sind. Gemeinsamkeiten bei VPN-Verbindungstunneln: – gleiches Authentifizierungsverfahren, festgelegt auf der Registerkarte *Authentifizierung* (siehe „Authentifizierung“ auf Seite 283) – gleiche Firewall-Einstellungen – gleiche Einstellung der IKE-Optionen.

IPsec VPN >> Verbindungen >> Editieren >> Allgemein[...]		
	Initialer Modus	**Deaktiviert / Gestoppt / Gestartet** Die Einstellung „**Deaktiviert**“ deaktiviert die VPN-Verbindung permanent; sie kann weder gestartet noch gestoppt werden. Die Einstellungen „**Gestartet**“ und „**Gestoppt**“ bestimmen den Status der VPN-Verbindung nach einem Neustart/Booten des mGuards (z. B. nach einer Unterbrechung der Stromversorgung). VPN-Verbindungen, die nicht deaktiviert sind, können über Icons in der Web-Oberfläche, Schalter, Taster, Datenverkehr oder das Skript nph-vpn.cgi gestartet oder gestoppt werden.
	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 8-2 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 286) 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 253): 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	**Adresse des VPN-Gateways der Gegenstelle**	IP-Adresse, Hostname oder '%any' für beliebige IP-Adressen, mehrere Gegenstellen oder Gegenstellen hinter einem NAT-Router.
	Interface, das bei der Einstellung %any für das Gateway benutzt wird (Wenn bei „**Adresse des VPN-Gateways der Gegenstelle**“ **%any** angegeben wurde)	**Intern, Extern, Implizit ausgewählt durch die rechts angegebene IP-Adresse** 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.

IPsec VPN >> Verbindungen >> Editieren >> Allgemein [...]

	Die Auswahl von **DMZ** ist nur im Router-Modus möglich. Hierbei können VPN-Verbindungen zu Hosts in der DMZ aufgebaut werden sowie IP-Pakete aus der DMZ in eine VPN-Verbindung geroutet werden. **Implizit ausgewählt durch die unten angegebene IP-Adresse**: Hierbei wird statt eines dedizierten Interface eine IP-Adresse verwendet.
IP-Adresse, die bei der Einstellung %any für das Gateway benutzt wird	IP-Adresse, die bei der Einstellung **%any** für das Gateway benutzt wird.
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.) Wenn eine der beiden Gegenstellen per Datenverkehr initiiert, muss bei der anderen Gegenstelle **Warte** oder **Initiiere** ausgewählt werden. **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 [...]

Schaltender Service Eingang/CMD

Kein / Service-Eingang CMD 1-3 (I 1-3)

Die VPN-Verbindung kann über einen angeschlossenen Taster/Schalter geschaltet werden.

Der Taster/Schalter muss an einen der Servicekontakte (CMD 1-3 / I 1-3) angeschlossen sein.

Wenn das Starten und Stoppen der VPN-Verbindung über den CMD-Kontakt eingeschaltet ist, hat ausschließlich der CMD-Kontakt das Recht dazu.

Wenn am CMD-Kontakt ein Taster (statt eines Schalters - siehe unten) angeschlossen ist, kann der Verbindungsaufbau und -abbau aber auch gleichberechtigt und konkurrierend über die Kommandos des CGI-Skriptes nph-vpn.cgi erfolgen.

Invertierte Logik verwenden

Kehrt das Verhalten des angeschlossenen Schalters um.

Wenn der schaltende Service-Eingang als Ein-/Aus-Schalter konfiguriert ist, kann er z. B. eine VPN-Verbindung ein- und gleichzeitig eine andere, die invertierte Logik verwendet, ausschalten.

Timeout zur Deaktivierung

Zeit, nach der die VPN-Verbindung gestoppt wird, wenn sie über Schalter, Taster, nph-vpn.cgi oder die Web-Oberfläche gestartet worden ist. Der Timeout startet beim Übergang in den Zustand „Gestartet“.

Die Verbindung verbleibt nach Ablauf des Timeouts in dem Zustand „Gestoppt“, bis sie erneut gestartet wird.

Ausnahme „Initiierung durch Datenverkehr“

Eine durch Datenverkehr initiierte (aufgebaute) Verbindung wird nach Ablauf des Timeouts abgebaut, verbleibt aber in dem Zustand „Gestartet“. Der Timeout startet erst, wenn kein Datenverkehr mehr stattfindet.

Die Verbindung wird bei erneut auftretendem Datenverkehr wieder aufgebaut.

Zeit in Stunden, Minuten und/oder Sekunden (0:00:00 bis 720:00:00, etwa 1 Monate). Die Eingabe kann aus Sekunden [ss], Minuten und Sekunden [mm:ss] oder Stunden, Minuten und Sekunden [hh:mm:ss] bestehen.

Bei 0 ist diese Einstellung abgeschaltet.

IPsec VPN >> Verbindungen >> Editieren >> Allgemein [...]		

	Kapsele den VPN-Datenverkehr in TCP ein	**Nein / TCP-Kapselung / Path Finder (Standard: Nein)**
		
		Bei Anwendung der Funktion **TCP-Kapselung** (siehe „TCP-Kapselung“ auf Seite 253) diesen Schalter nur dann auf TCP-Kapselung 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.
		
		TPC-Kapselung kann ebenfalls mit der Funktion „**Path Finder**“ (siehe „TCP-Kapselung mit aktivierter Funktion „Path Finder““ auf Seite 254) verwendet werden. In diesem Fall den Schalter nur dann auf **Path Finder** setzen, wenn die Gegenstelle die Funktion „Path Finder“ ebenfalls unterstützt. Anschließend muss auch die Nummer des Ports angegeben werden, über den die Gegenstelle die eingekapselten Datenpakete empfängt.
		
		TCP-gekapselte bzw. Path Finder-Verbindungen verwenden nicht das UDP-Protokoll und die Standard-UDP-Ports 500 und 4500, um die Daten zu versenden. Stattdessen werden die verschlüsselten Daten (unter Verwendung des IKE-Protokolls und der ESP-Erweiterung) eingekapselt über eine TCP-Verbindung gesendet.
		
		Einstellung der Verbindungsinitiierung bei Verwendung von TCP-Kapselung / Path Finder.
		
		– 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.

	TCP-Port des Servers, welcher die gekapselte Verbindung annimmt (Nur sichtbar, wenn „Kapsele den VPN-Datenverkehr in TCP ein“ auf **TCP-Kapselung** oder **Path Finder** steht.)	**Standard: 8080** Nummer des Ports, über den die Gegenstelle die eingekapselten Datenpakete empfängt. Die hier angegebene Port-Nummer muss mit der Port-Nummer übereinstimmen, die beim mGuard der Gegenstelle als TCP-Port, auf dem zu horchen ist festgelegt ist (Menüpunkt „IPsec VPN >> Global >> Optionen“).
Mode Configuration	Der mGuard unterstützt die Authentifizierungsmethode „Extended Authentication“ (XAuth) und die häufig erforderliche Protokollerweiterung „Mode Config“ inklusive „Split Tunneling“ als Server und als Client (u. a. iOS- und Android-Unterstützung). Netzwerkeinstellungen, DNS- und WINS-Konfigurationen werden dem IPsec-Client vom IPsec-Server mitgeteilt.	

IPsec VPN >> Verbindungen >> Editieren >> Allgemein [...]

Mode Configuration

Aus / Server / Client (Standard: Aus)

Um als Server oder Client über eine IPsec-VPN-Verbindungen mit Gegenstellen zu kommunizieren, die „**XAuth**“ und „**Mode Config**“ benötigen, wählen Sie „Server“ oder „Client“ aus.

Aus: Kein „Mode Config“ verwenden.

Server: Der Gegenstelle die IPsec-Netzwerkkonfiguration mitteilen.

Client: Die von der Gegenstelle mitgeteilte IPsec-Netzwerkkonfiguration übernehmen und anwenden.

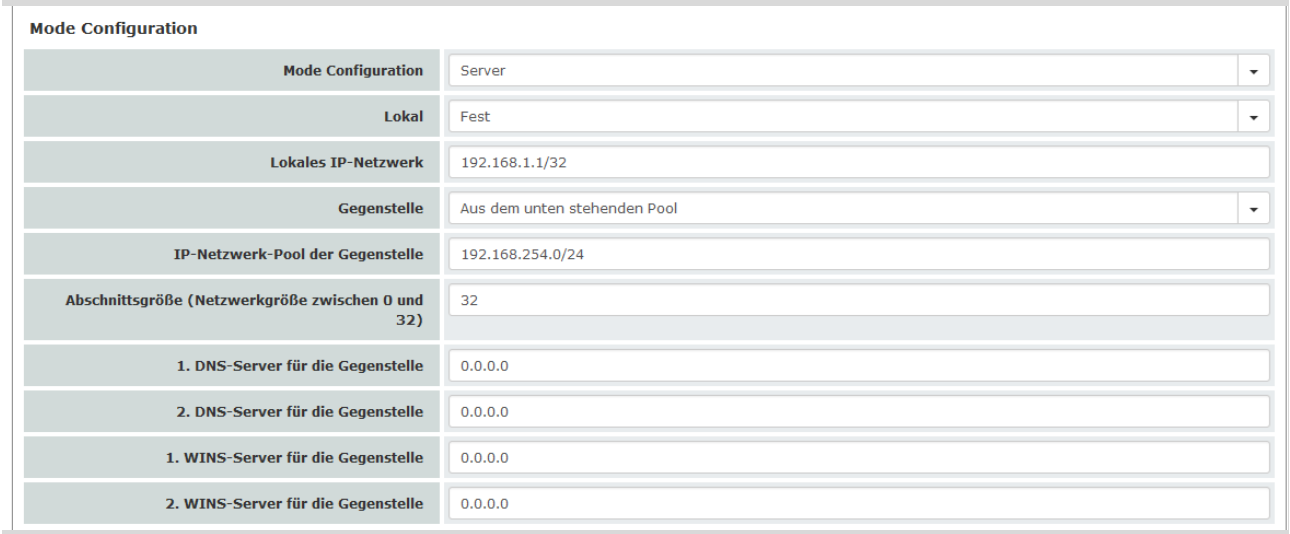
„Mode Config“ kann im „VPN-Aggressive-Mode“ („Aggressive Mode (unsicher)“ auf Seite 290) nicht genutzt werden.

Einstellungen als Server

Ermöglicht Clients, die „XAuth“ und „Mode Config“ benötigen (z. B. Apple iPad), eine IPsec-VPN-Verbindung zum mGuard aufzubauen. Die benötigten Werte zur Konfiguration der Verbindung (lokales und entferntes Netz) erhalten die Remote-Clients vom mGuard.

Soll eine Verbindung vom iOS-Client hergestellt werden, muss die Authentifizierung via Zertifikat erfolgen.

Der Zertifikatsname (CN) und der „Subject Alternative Name“ des mGuard-Maschinenzertifikats müssen identisch sein mit der IP-Adresse (oder dem Hostnamen/DNS-Namen), die der iOS-Client zum Aufbau einer VPN-Verbindung mit dem mGuard-Gerät verwendet (siehe „Authentifizierung >> Zertifikate“).



IPsec VPN >> Verbindungen >> Editieren >> Allgemein [...]		
	Lokal	**Fest / Aus der unten stehenden Tabelle** **Fest**: Das lokale Netz auf der Server-Seite wird manuell fest eingestellt und muss auf der Client-Seite (beim Remote-Client) ebenfalls manuell eingestellt werden. **Aus der unten stehenden Tabelle**: Das oder die lokalen Netze der Server-Seite werden dem Remote-Client über die Split-Tunneling-Erweiterung mitgeteilt. Eingabe in CIDR-Schreibweise (siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 43).
	Lokales IP-Netzwerk **(Wenn „Fest “ ausgewählt wurde)**	Lokales Netzwerk auf der Server-Seite in CIDR-Schreibweise.
	Netzwerke (Wenn „Aus der unten stehenden Tabelle“ ausgewählt wurde)	Lokale Netzwerke auf der Server-Seite in CIDR-Schreibweise.
	Gegenstelle	**Aus dem unten stehenden Pool / Aus der unten stehenden Tabelle** **Aus dem unten stehenden Pool** Der Server wählt dynamisch IP-Netzwerke für die Gegenstelle aus dem angegebenen Pool, entsprechend der ausgewählten Abschnittsgröße. **Aus der unten stehenden Tabelle** (Diese Funktion kann nur verwendet werden, wenn auf der Gegenstelle ein mGuard eingesetzt wird.) Die IP-Netzwerke der Gegenstelle werden dem Remote-Client über die Split-Tunneling-Erweiterung mitgeteilt.
	IP-Netzwerk-Pool der Gegenstelle **(Wenn „Aus diesem Pool“ ausgewählt wurde)**	Netzwerk-Pool, aus dem IP-Netzwerke für die Gegenstelle ausgewählt werden, in CIDR-Schreibweise.
	Abschnittsgröße (Netzwerkgröße zwischen 0 und 32) **(Wenn „Aus diesem Pool“ ausgewählt wurde)**	Abschnittsgröße, die die Größe der IP-Netzwerke bestimmt, die aus dem Netzwerk-Pool für die Gegenstelle entnommen werden können.
	Netzwerke (Wenn „Aus der unten stehenden Tabelle“ ausgewählt wurde)	IP-Netzwerke für die Gegenstelle in CIDR-Schreibweise.
	1. und 2. DNS-Server für die Gegenstelle	Adresse eines DNS-Servers, die der Gegenstelle mitgeteilt wird. Die Einstellung 0.0.0.0 bedeutet „keine Adresse“.

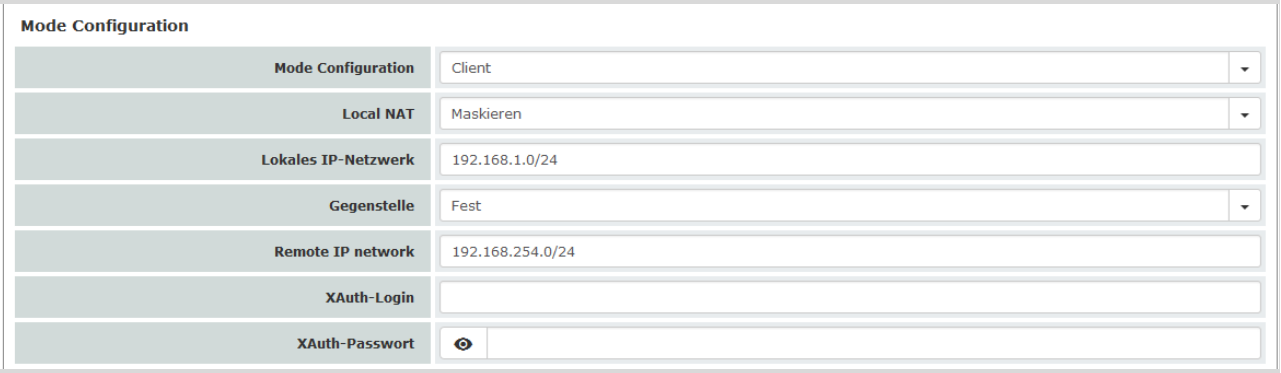
IPsec VPN >> Verbindungen >> Editieren >> Allgemein [...]

1. und 2. WINS-Server für die Gegenstelle

Adresse eines WINS-Servers, die der Gegenstelle mitgeteilt wird. Die Einstellung 0.0.0.0 bedeutet „keine Adresse“.

Einstellungen als Client

Ermöglicht dem mGuard, eine IPsec-VPN-Verbindung zu Servern aufzubauen, die „XAuth“ und „Mode Config“ benötigen. Die benötigten Werte (IP-Adresse/IP-Netzwerk) zur Konfiguration der Verbindung (lokales und entferntes Netz) erhält der mGuard optional vom Remote-Server der Gegenstelle.



Lokales NAT

(Nicht aktiv im Stealth-Modus „Automatisch“ und „Statisch“)

Kein NAT / Maskieren

Kein NAT

Vom Server ausgewählte lokale IP-Adressen können den Tunnel nutzen.

Maskieren

Der mGuard kann sein lokales Netz maskieren. Dazu muss das lokale Netz in CIDR-Schreibweise (siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 43) angegeben werden.

Lokales IP-Netzwerk

IP-Netzwerk am lokalen Interface des Clients, das maskiert wird.

Gegenstelle

Fest / Vom Server

Fest: Das lokale Netz auf der Client-Seite wird manuell fest eingestellt und muss auf der Server-Seite (beim Remote-Server) ebenfalls manuell eingestellt werden.

Vom Server: Das oder die Remote-Netzwerke der Server-Seite werden dem lokalen Client über die Split-Tunneling-Erweiterung mitgeteilt.

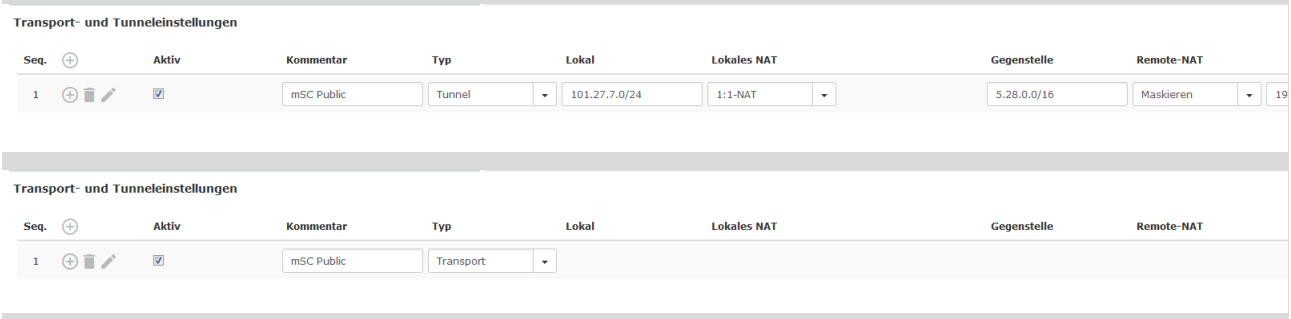
Verwendet der Remote-Server kein „Split Tunneling“, wird 0.0.0.0/0 verwendet.

IP-Netzwerk der Gegenstelle

(Wenn „Fest“ ausgewählt wurde)

Das Netzwerk des Remote-Servers in CIDR-Schreibweise.

IPsec VPN >> Verbindungen >> Editieren >> Allgemein [...]		
Transport- und Tunneleinstellungen	**XAuth-Login**	Manche Remote-Server benötigen zur Authentifizierung des Clients einen XAuth-Benutzernamen (Login) und ein XAuth-Passwort.
	XAuth-Passwort	Zugehöriges XAuth-Passwort



	Aktiv	Legen Sie fest, ob der Verbindungstunnel aktiv sein soll oder nicht.
	Kommentar	Frei einzugebender kommentierender Text. Kann leer bleiben.

IPsec VPN >> Verbindungen >> Editieren >> Allgemein [...]

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.

Sofern die Default-Route (0.0.0.0/0) als Gegenstelle eingetragen ist, werden die unter „Netzwerk >> NAT >> IP- und Port-Weiterleitung“ angegebenen Regeln mit Vorrang behandelt.

Damit ist sichergestellt, das Verbindungen ankommend an der WAN-Schnittstelle des mGuard, die Port-Weiterleitung weiterhin nutzen können. Diese Daten werden in diesem Fall nicht über VPN übertragen.

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

(Bei Verbindungstyp „Tunnel“)

Unter **Lokal** und **Gegenstelle** definieren Sie die Netzwerkbereiche für beide Tunnelenden.

Lokal: Hier geben Sie die Adresse des Netzes oder Computers an, das/der lokal am mGuard angeschlossen ist.

Gegenstelle

(Bei Verbindungstyp „Tunnel“ **(Netz ↔ Netz)**)

Gegenstelle: Hier geben Sie die Adresse des Netzes oder Computers an, das/der sich hinter dem Remote-VPN-Gateway befindet.

IPsec VPN >> Verbindungen >> Editieren >> Allgemein [...]

Lokales NAT

(Bei Verbindungstyp „Tunnel“)

Kein NAT / 1:1-NAT / Maskieren

Es können die IP-Adressen von Geräten umgeschrieben werden, die sich am jeweiligen Ende des VPN-Tunnels befinden.

Kein NAT: Es wird kein NAT vorgenommen.

Bei **1:1-NAT** werden die IP-Adressen von Geräten am lokalen Ende des Tunnels so ausgetauscht, dass jede einzelne gegen eine bestimmte andere umgeschrieben wird.

Erst nach Klicken auf das Icon **Zeile bearbeiten** können Sie für lokale Geräte 1:1-NAT-Regeln festlegen.

Beim **Maskieren** werden die IP-Adressen von Geräten am lokalen Ende des Tunnels gegen eine für alle Geräte identische IP-Adresse ausgetauscht.

Remote-NAT

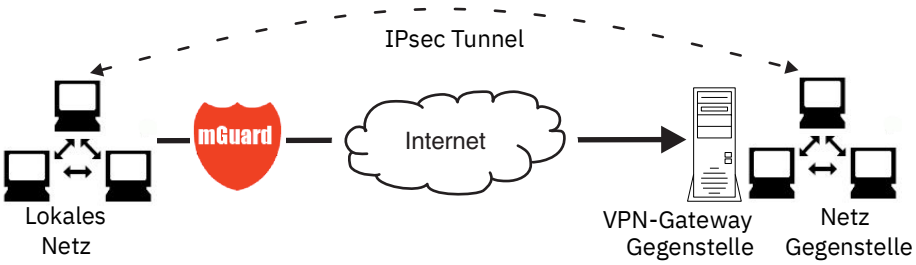
(Bei Verbindungstyp „Tunnel“)

Kein NAT / 1:1-NAT / Maskieren

Kein NAT: Es wird kein NAT vorgenommen.

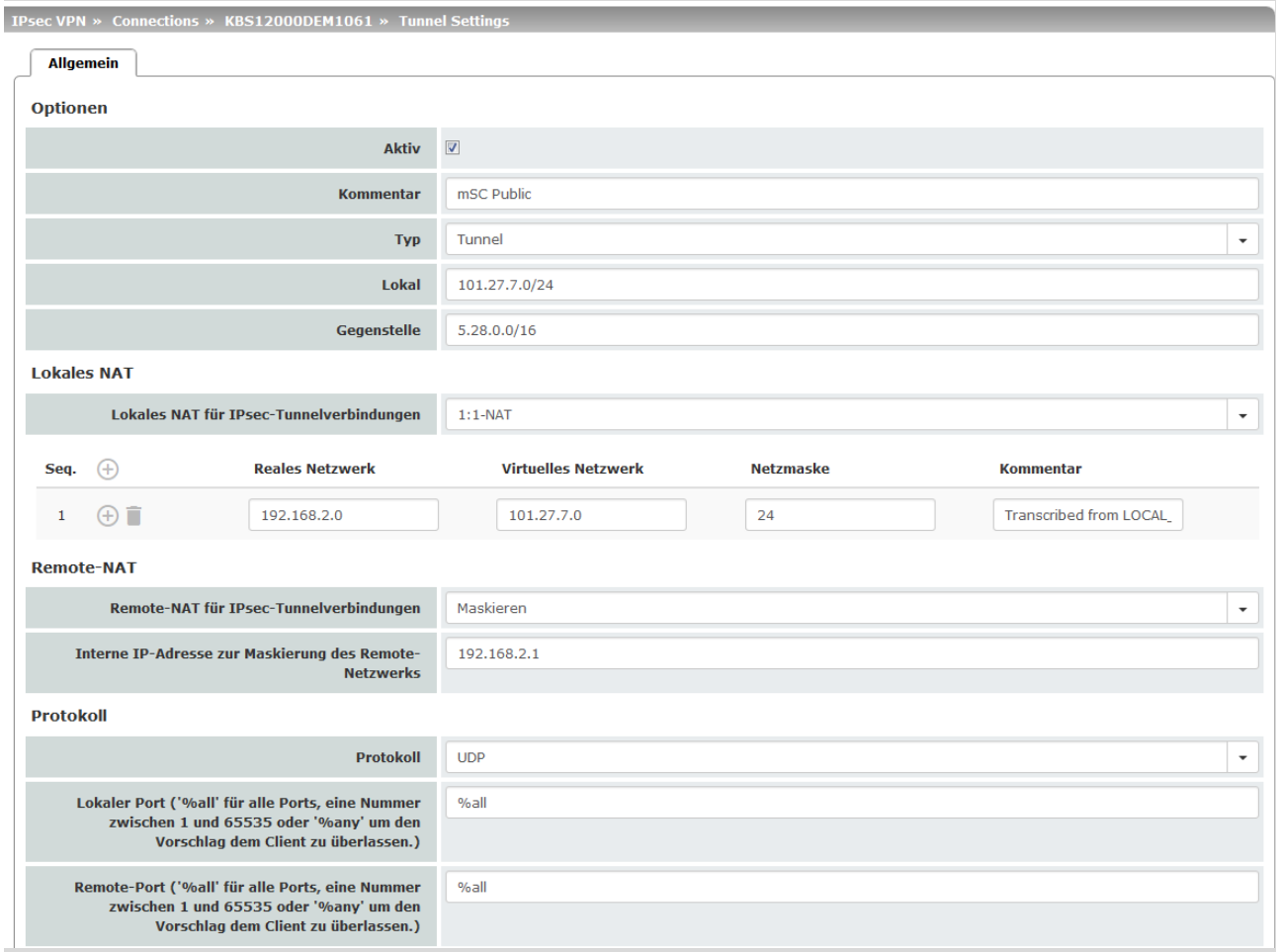
Bei **1:1-NAT** werden die IP-Adressen von Geräten der Gegenstelle des Tunnels so ausgetauscht, dass jede einzelne gegen eine bestimmte andere umgeschrieben wird.

Beim **Maskieren** werden die IP-Adressen von Geräten der Gegenstelle gegen eine für alle Geräte identische IP-Adresse ausgetauscht.



Um weitere Einstellungen vorzunehmen, klicken Sie auf das Icon **Zeile bearbeiten**. Es öffnet sich das Fenster „IPsec VPN >> Verbindungen >> Transport- und Tunneleinstellungen >> Allgemein“.

IPsec VPN >> Verbindungen >> Editieren >> Allgemein [...]



Transport- und Tunneleinstellungen (Editieren)

Optionen

Aktiv — Legen Sie fest, ob der Verbindungstunnel aktiv sein soll oder nicht.

Kommentar — Frei einzugebender kommentierender Text. Kann leer bleiben.

IPsec VPN >> Verbindungen >> Editieren >> Allgemein [...]

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.

Sofern die Default-Route (0.0.0.0/0) als Gegenstelle eingetragen ist, werden die unter „Netzwerk >> NAT >> IP- und Port-Weiterleitung“ angegebenen Regeln mit Vorrang behandelt.

Damit ist sichergestellt, das Verbindungen ankommend an der WAN-Schnittstelle des mGuard, die Port-Weiterleitung weiterhin nutzen können. Diese Daten werden in diesem Fall nicht über VPN übertragen.

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
(Bei Verbindungstyp „Tunnel“)

Unter **Lokal** und **Gegenstelle** definieren Sie die Netzwerkbereiche für beide Tunnelenden.

Lokal: Hier geben Sie die Adresse des Netzes oder Computers an, das/der lokal am mGuard angeschlossen ist.

Gegenstelle
(Bei Verbindungstyp „Tunnel“)

Gegenstelle: Hier geben Sie die Adresse des Netzes oder Computers an, das/der sich hinter dem Remote-VPN-Gateway befindet.

IPsec VPN >> Verbindungen >> Editieren >> Allgemein [...]

Lokales NAT

Lokales NAT für IPsec-Tunnelverbindungen
(Bei Verbindungstyp „Tunnel“)

Kein NAT / 1:1-NAT / Maskieren

Es können die IP-Adressen von Geräten umgeschrieben werden, die sich am jeweiligen Ende des VPN-Tunnels befinden.

Kein NAT: Es wird kein NAT vorgenommen.

Bei **1:1-NAT** werden die IP-Adressen von Geräten am lokalen Ende des Tunnels so ausgetauscht, dass jede einzelne gegen eine bestimmte andere umgeschrieben wird.

Beim **Maskieren** werden die IP-Adressen von Geräten am lokalen Ende des Tunnels gegen eine für alle Geräte identische IP-Adresse ausgetauscht.

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 hier definiert wird.
– deren Zieladresse im Netzwerk *der Gegenstelle* liegt, wenn dort kein 1:1-NAT für die Gegenstelle eingestellt ist.

Die Datenpakete von lokalen Geräten bekommen eine Quelladresse entsprechend der eingestellten Adresse unter *Lokal* zugewiesen und werden durch den VPN-Tunnel gesendet.

Sie können für lokale Geräte 1:1-NAT-Regeln für jeden VPN-Tunnel festlegen. So kann ein IP-Bereich, der über eine weites Netzwerk verstreut ist, gesammelt und durch einen schmalen Tunnel geschickt werden.

Lokale 1:1-NAT-Netzwerke müssen in aufsteigender Reihenfolge, beginnend mit dem kleinsten Netzwerk bis hin zum größten Netzwerk, angegeben werden.

Reales Netzwerk Konfiguriert die „von IP“-Adresse für 1:1-NAT.

IPsec VPN >> Verbindungen >> Editieren >> Allgemein [...]		
	Virtuelles Netzwerk	Konfiguriert die umgeschriebene IP-Adresse für 1:1-NAT.
	Netzmaske	Die Netzmaske als Wert zwischen 1 und 32 für die reale und virtuelle Netzwerkadresse (siehe auch „CIDR (Classless Inter-Domain Routing)“ auf Seite 43).
	Kommentar	Kann mit kommentierendem Text gefüllt werden.
	Interne Netzwerkadresse für lokales Maskieren (Bei Auswahl „Maskieren“)	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 hier definiert wird. – deren Zieladresse im Netzwerk *Gegenstelle* liegt, wenn kein 1:1-NAT für das *Gegenstelle*-NAT eingestellt ist. In dieser Einstellung ist als VPN-Netzwerk nur eine IP-Adresse (Subnetzmaske /32) zugelassen. Das zu maskierende Netzwerk wird auf diese IP-Adresse umgeschrieben. 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-Tunnelverbindungen (Bei Verbindungstyp „Tunnel“)	**Kein NAT / 1:1-NAT / Maskieren** Es können die IP-Adressen von Geräten umgeschrieben werden, die sich am jeweiligen Ende des VPN-Tunnels befinden. Bei **Remote-1:1-NAT** werden die IP-Adressen von Geräten der Gegenstelle des Tunnels so ausgetauscht, dass jede einzelne gegen eine bestimmte andere umgeschrieben wird. Beim **Maskieren** des Netzwerks der Gegenstelle werden die IP-Adressen von Geräten der Gegenstelle gegen eine für alle Geräte identische IP-Adresse ausgetauscht.

IPsec VPN >> Verbindungen >> Editieren >> Allgemein [...]		
	Netzwerkadresse für 1:1-NAT im Remote-Netz (Bei Auswahl „1:1-NAT“)	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 hier unter Lokal definiert wird. Die Datenpakete bekommen eine Zieladresse aus dem Netzwerk, das unter Gegenstelle eingestellt ist. Wenn nötig, wird auch die Quelladresse ersetzt (siehe Lokal). Danach werden die Datenpakete durch den VPN-Tunnel gesendet.
	Interne IP-Adresse zur Maskierung des Remote-Netzwerks (Bei Auswahl „Maskieren“)	In dieser Einstellung ist als VPN-Netzwerk nur eine IP-Adresse (Subnetzmaske /32) zugelassen. Das zu maskierende Netzwerk wird auf diese IP-Adresse umgeschrieben. 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.
Protokoll	**Protokoll**	**Alle** bedeutet: TCP, UDP, ICMP und andere IP-Protokolle **Lokaler Port (nur bei TCP / UDP)**: Nummer des zu verwendenden Ports. Wählen Sie „%all“ für alle Ports, eine Nummer zwischen 1 und 65535 oder „%any“, um den Vorschlag dem Client zu überlassen. **Remote-Port (nur bei TCP / UDP)**: Nummer des zu verwendenden Ports. Wählen Sie „%all“ für alle Ports, eine Nummer zwischen 1 und 65535 oder „%any“, um den Vorschlag dem Client zu überlassen.
Dynamisches Routing	**Füge Kernel-Route zum Remote-Netz hinzu, um die Weiterverbreitung durch OSPF zu ermöglich** (Nur wenn **OSPF** aktiviert ist)	Bei aktivierter Funktion wird eine Kernel-Route zum Remote-Netz (Gegenstelle) hinzugefügt, um die Weiterverbreitung durch OSPF zu ermöglichen.

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
- **Lokal:** %all
- **Gegenstelle:** %all
- **PFS**: Nein („Perfect Forward Secrecy (PFS)“ auf Seite 298)

Festlegung einer Standard-Route über das VPN

Die Adresse 0.0.0.0/0 gibt eine *Standard-Route über das VPN* an.

Bei dieser Adresse 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 Tunnelgruppen

Mit der Option „Tunnelgruppen“ wird nicht mehr die Anzahl der aufgebauten Tunnel begrenzt, sondern die Anzahl der verbundenen Gegenstellen (VPN-Peers). Werden zu einer Gegenstelle mehrere Tunnel aufgebaut, wird nur eine Gegenstelle gezählt.

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 **Gegenstelle** 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 **Gegenstelle** beim lokalen und bei entfernten mGuards könnten zum Beispiel wie folgt lauten:

Lokaler mGuard			Entfernter **mGuard A**	
Lokal	Gegenstelle		Lokal	Gegenstelle
10.0.0.0/8	10.0.0.0/8	>	10.1.7.0/24	10.0.0.0/8
			Entfernter **mGuard B**	
			Lokal	Gegenstelle
		>	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.

Maskieren

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.

Maskieren schafft hier Abhilfe:

Die im Netzwerk einer Zweigstelle angeschlossenen Rechner treten durch das Maskieren 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.

Netzwerkadresse für das Maskieren

Sie geben den IP-Adressenbereich an, für den das Maskieren 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.

Maskieren kann in folgenden Netzwerk-Modi verwendet werden: Router und Stealth (nur Stealth-Modus „Mehrere Clients“).

Für IP-Verbindungen, die durch eine VPN-Verbindung mit aktiviertem Maskieren vermittelt werden, werden die Firewall-Regeln für ausgehende Daten in der VPN-Verbindung auf die originale Quelladresse der Verbindung angewendet.

1:1-NAT

Kann nur für VPN-Typ *Tunnel* verwendet werden.

Mit Hilfe von 1:1-NAT im VPN können weiterhin die tatsächlich genutzten Netzwerkadressen zur Angabe des Tunnelanfangs oder -endes angegeben werden, unabhängig von den mit der Gegenseite vereinbarten Tunnelparametern:

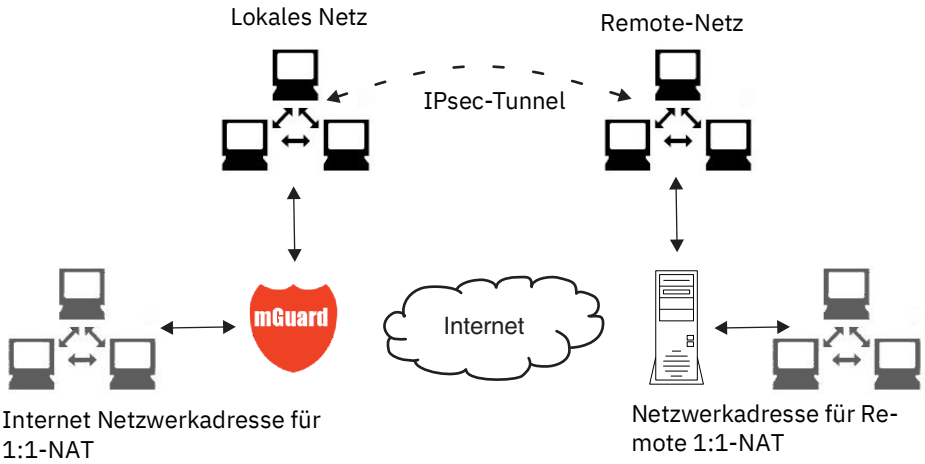


Bild 8-3 1:1-NAT

8.2.3 Authentifizierung

IPsec VPN >> Verbindungen >> Editieren >> Authentifizierung

Authentifizierung

Authentisierungs-verfahren

Es gibt 2 Möglichkeiten:

– X.509-Zertifikat (Standard)
– Pre-Shared Key (PSK)

ACHTUNG: Unsichere PSK-Authentisierung
Die Authentisierung mittels Pre-Shared-Keys (PSK) gilt als unsicher und sollte nicht mehr verwendet werden. Verwenden Sie aus Sicherheitsgründen zur Authentisierung X.509-Zertifikate.

Je nachdem, welches Verfahren Sie auswählen, zeigt die Seite unterschiedliche Einstellmöglichkeiten.

Bei Authentisierungsverfahren X.509-Zertifikat

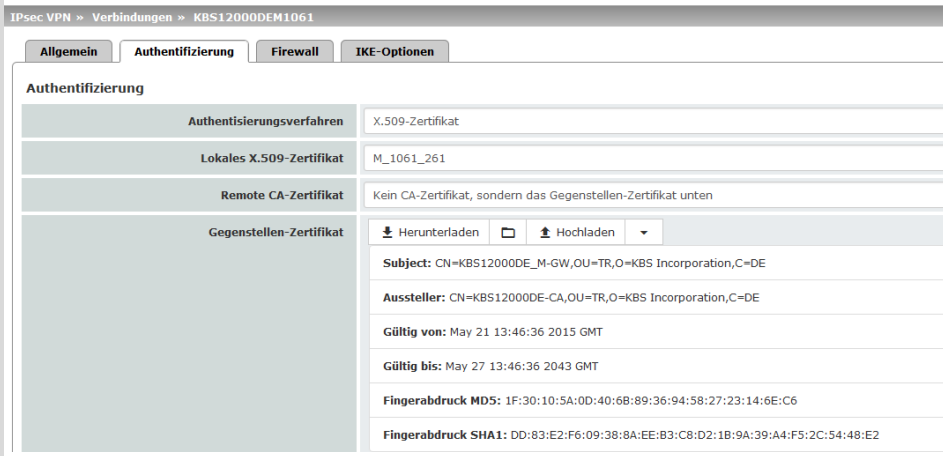
Dieses Verfahren wird von den meisten neueren IPsec-Implementierungen unterstützt. (Dabei besitzt jeder VPN-Teilnehmer einen privaten geheimen Schlüssel sowie einen öffentlichen Schlüssel in Form eines X.509-Zertifikats, welches weitere Informationen über seinen Eigentümer und einer Beglaubigungsstelle (Certification Autority, CA) enthält.)

Es muss Folgendes festgelegt werden:

– Wie sich der mGuard bei der Gegenstelle authentisiert.
– Wie der mGuard die entfernte Gegenstelle authentifiziert

IPsec VPN >> Verbindungen >> Editieren >> Authentifizierung

....wie sich der mGuard bei der Gegenstelle authentisiert.



Lokales X.509-Zertifikat

(Bei Authentisierungsverfahren „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.

Falls nur der Eintrag *Kein* zu sehen ist, muss erst ein Zertifikat installiert werden. Der Eintrag *Kein* 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 selbstsigniertes Maschinenzertifikat

Remote CA-Zertifikat

Folgende Auswahlmöglichkeiten stehen zur Verfügung:

– Ausgestellt von einer vertrauenswürdigen CA
– Kein CA-Zertifikat, sonder das Gegenstellen-Zertifikat unten
– Name eines CA-Zertifikats, wenn verfügbar

Gegenstellen-Zertifikat

(Bei Authentifizierung mittels Gegenstellen-Zertifikat)

Sie können das Gegenstellen-Zertifikat hochladen. Das Zertifikat wird ausgewählt und in der Liste der Gegenstellen-Zertifikate gespeichert (siehe „Gegenstellen-Zertifikate“ auf Seite 203).

Zum Verständnis der nachfolgenden Tabelle siehe Kapitel „Authentifizierung >> Zertifikate“ auf Seite 192.

Authentifizierung bei VPN

Die Gegenstelle zeigt vor:	Maschinenzertifikat von **CA signiert**	Maschinenzertifikat **selbstsigniert**
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 192*; 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.

Eine bestehende VPN-Verbindung wird jedoch durch ein zurückgezogenes Zertifikat nicht umgehend beendet, wenn das CRL-Update während der bestehenden VPN-Verbindung erfolgt. Ein erneuter Schlüsselaustausch (*rekeying*) oder das erneute Starten der VPN-Verbindung ist dann jedoch nicht mehr möglich.

Remote CA-Zertifikat

Selbstsigniertes Maschinenzertifikat

Wenn sich die VPN-Gegenstelle mit einem **selbstsignierten** 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 286).

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 286).

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.

- **Keine Datei ausgewählt...** klicken, um die Datei zu selektieren
- **Hochladen** klicken.
  Danach wird der Inhalt der Zertifikatsdatei angezeigt.

IPsec VPN >> Verbindungen >> Editieren >> Authentifizierung	
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 im Feld *Gegenstelle* den entsprechenden Eintrag.

IPsec VPN >> Verbindungen >> Editieren >> Authentifizierung [...]

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 Names*, 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 367.)

Statt „Subject“ wurde früher die Bezeichnung „Distinguished Name“ verwendet.

IPsec VPN >> Verbindungen >> Editieren >> Authentifizierung [...]

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.

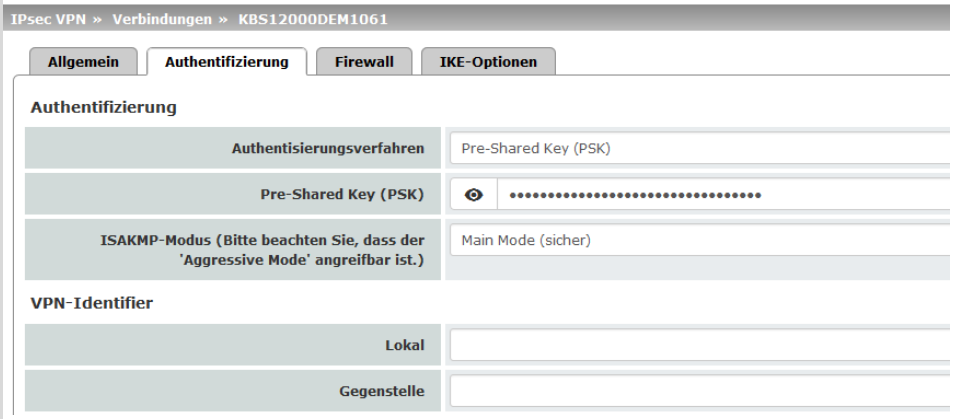
Bei den Attributen müssen Anzahl und Reihenfolge mit denen in den Zertifikaten übereinstimmen, auf die der Filter angewendet wird.

Achten Sie auf Groß- und Kleinschreibung.

IPsec VPN >> Verbindungen >> Editieren >> Authentifizierung [...]

Authentifizierung

Bei Authentisierungsverfahren Pre-Shared Key (PSK)



Dieses Verfahren wird vor allem durch ältere IPsec Implementierungen unterstützt. Dabei authentifizieren sich beide Seiten des VPNs über den gleichen PSK.

ACHTUNG: Unsicheres Authentisierungsverfahren
Die Authentisierung mittels Pre-Shared-Key (PSK) gilt als unsicher und sollte nicht mehr verwendet werden. Verwenden Sie aus Sicherheitsgründen zur Authentisierung X.509-Zertifikate.

Um den verabredeten Schlüssel dem mGuard zur Verfügung zu stellen, gehen Sie wie folgt vor:

- Tragen Sie ins Eingabefeld **Pre-Shared 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.

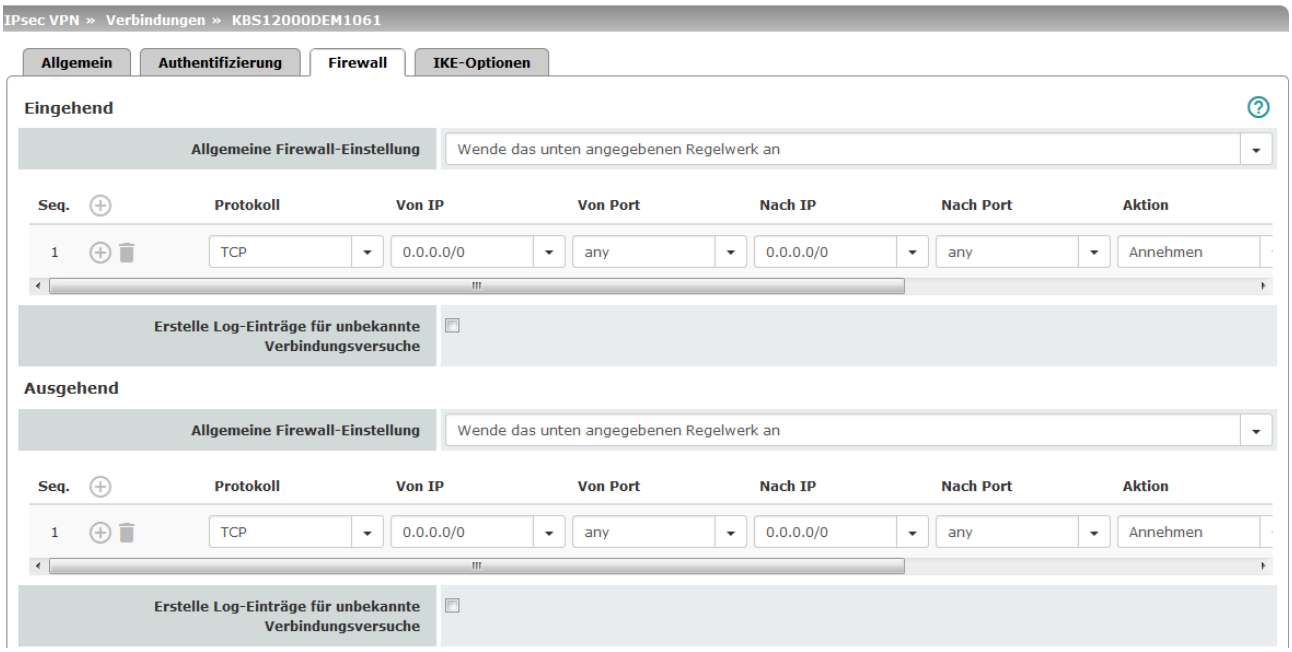
Wenn PSK mit der Einstellung „Aggressive Mode (unsicher)“ genutzt wird, dann muss beim Initiator der Verbindung unter „IKE-Optionen“ ein fester Diffie-Hellmann-Algorithmus ausgewählt werden.

Wenn PSK mit der Einstellung „Aggressive Mode (unsicher)“ genutzt wird, dann sollten beim Responder der Verbindung unter „IKE-Optionen“ alle Diffie-Hellmann-Algorithmen ausgewählt werden.

Wenn ein fester Diffie-Hellmann-Algorithmus verwendet wird, dann muss er bei allen Verbindungen mit der Einstellung „Aggressive Mode (unsicher)“ gleich sein.

IPsec VPN >> Verbindungen >> Editieren >> Authentifizierung [...]		
	ISAKMP-Modus	**Main Mode (sicher)** Beim Main Mode handelt derjenige, der die Verbindung aufnehmen will (Initiator) mit dem Antwortenden (Responder) eine ISAKMP-SA aus. Wir empfehlen im Main Mode den Einsatz von Zertifikaten. **Aggressive Mode (unsicher)** Der Aggressive Mode ist nicht so streng verschlüsselt wie der Main Mode. Ein Grund für den Einsatz dieses Modus kann sein, dass die Adresse des Initiators dem Responder nicht von vornherein bekannt ist und beide Seiten Pre-shared Keys zur Authentifizierung einsetzen wollen. Ein anderer Grund kann sein, dass ein schnellerer Verbindungsaufbau gewünscht wird und die Richtlinien des Responders ausreichend bekannt sind, z. B. bei einem Mitarbeiter, der auf das Firmennetz zugreifen will. Bedingung: – Nicht zusammen mit der Redundanz-Funktion einsetzbar. – Zwischen Peers muss der gleiche Mode eingesetzt werden. – Der Agressive Mode wird in Verbindung mit XAuth/Mode Config nicht unterstützt. – Wenn zwei VPN-Clients hinter demselben NAT-Gateway die gleiche Verbindung zu einem VPN-Gateway aufbauen, müssen sie den gleichen PSK verwenden. VPN-Verbindungen im Aggressive Mode und mit PSK-Authentifizierung, die durch ein NAT-Gateway erfolgen sollen, müssen sowohl auf dem Client als auch auf dem Gateway eindeutige VPN-Identifier verwenden.
VPN Identifier	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“)	

8.2.4 Firewall



Firewall eingehend, Firewall ausgehend

Während die unter dem Menüpunkt *Netzwerksicherheit* vorgenommenen Einstellungen sich nur auf Nicht-VPN-Verbindungen beziehen (siehe oben unter „Menü Netzwerksicherheit“ auf Seite 209), 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 209, „Netzwerksicherheit >> Paketfilter“ auf Seite 209, „Erweitert“ auf Seite 230).

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** die Funktion **Erlaube Paketweiterleitung zwischen VPN-Verbindungen aktiviert** 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, 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	**Allgemeine Firewall-Einstellung**	**Alle eingehenden Verbindungen annehmen**, die Datenpakete aller eingehenden Verbindungen werden angenommen. **Alle eingehenden Verbindungen verwerfen**, die Datenpakete aller eingehenden Verbindungen werden verworfen. **Nur Ping zulassen,** die Datenpakete aller eingehenden Verbindungen werden verworfen, mit Ausnahme der Ping-Pakete (ICMP). **Wende das unten angegebene Regelwerk an,** blendet weitere Einstellmöglichkeiten ein.
	Die folgenden Einstellungen sind nur sichtbar, wenn „**Wende das unten angegebene Regelwerk an**“ eingestellt ist.	

IPsec VPN >> Verbindungen >> Editieren >> Firewall

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 43).

Namen von IP-Gruppen, sofern definiert. Bei Angabe des Namens einer IP-Gruppe werden die Hostnamen, IP-Adressen, IP-Bereiche oder Netzwerke berücksichtigt, die unter diesem Namen gespeichert sind (siehe „IP- und Portgruppen“ auf Seite 227).

Werden Hostnamen in IP-Gruppen verwendet, muss der mGuard so konfiguriert sein, dass der Hostname von einem DNS-Server in eine IP-Adresse aufgelöst werden kann.

Kann ein Hostname aus einer IP-Gruppe nicht aufgelöst werden, wird dieser Host bei der Regel nicht berücksichtigt. Weitere Einträge in der IP-Gruppe sind davon nicht betroffen und werden berücksichtigt.

Auf Geräten der FL MGUARD 2000-Serie ist die Verwendung von Hostnamen in IP-Gruppen nicht möglich.

Eingehend:

- Von IP: die IP-Adresse im VPN-Tunnel
- Nach IP die 1:1-NAT-Adresse bzw. die reale Adresse

Ausgehend:

- Von IP: die 1:1-NAT-Adresse bzw. die reale Adresse
- Nach IP: die IP-Adresse im VPN-Tunnel

Von Port / Nach Port

(Nur bei den Protokollen TCP und UDP)

any bezeichnet jeden beliebigen Port.

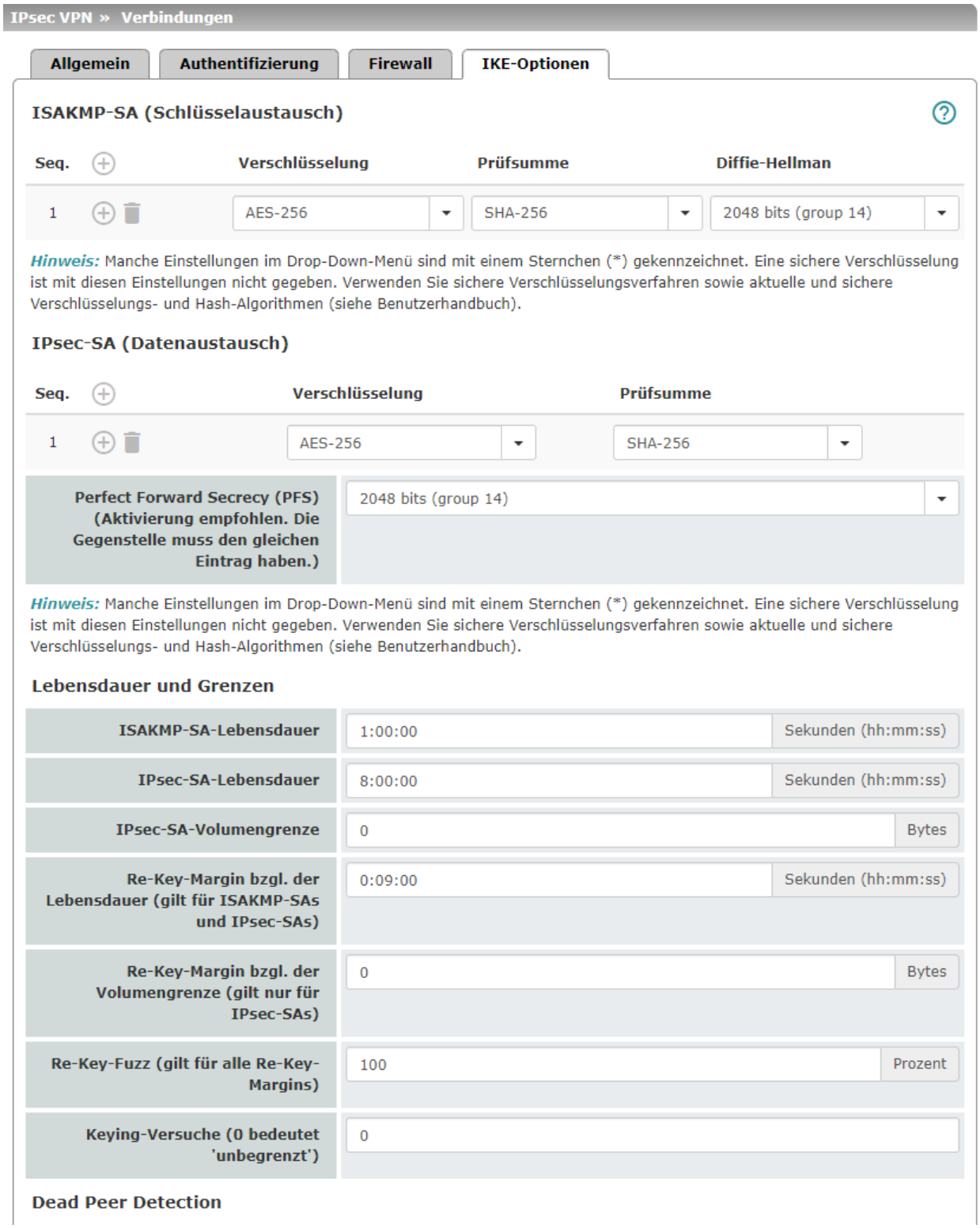
startport:endport (z. B. 110:120) bezeichnet einen Portbereich.

Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben (z. B. 110 für pop3 oder pop3 für 110).

Namen von Portgruppen, sofern definiert. Bei Angabe des Namens einer Portgruppe werden die Ports oder Portbereiche berücksichtigt, die unter diesem Namen gespeichert sind (siehe „IP- und Portgruppen“ auf Seite 227).

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. **Namen von Regelsätzen**, sofern definiert. Bei Angabe eines Namens für Regelsätze treten die Firewall-Regeln in Kraft, die unter diesem Namen konfiguriert sind (siehe Registerkarte „Regelsätze“). Regelsätze, die IP-Gruppen mit Hostnamen enthalten, sollten aus Sicherheitsgründen nicht in Firewall-Regeln verwendet werden, die als Aktion „Verwerfen“ oder „Abweisen“ ausführen. Auf Geräten der FL MGUARD 2000-Serie ist die Verwendung von Regelsätzen nicht möglich. **Namen von Modbus-TCP-Regelsätzen**, sofern definiert. Bei der Auswahl eines Modbus-TCP-Regelsatzes treten die Firewall-Regeln in Kraft, die unter diesem Regelsatz konfiguriert sind (siehe Kapitel 7.2.1).
	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 – Funktion *Log* aktivieren – oder nicht – Funktion *Log* deaktivieren (Standard).
	Log-Einträge für unbekannte Verbindungsversuche	Bei aktivierter Funktion werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden.
Ausgehend	Die Erklärung unter „Eingehend“ gilt auch für „Ausgehend“.	

8.2.5 IKE-Optionen



IPsec VPN >> Verbindungen >> Editieren >> IKE-Optionen

ISAKMP-SA (Schlüssel-austausch)

Algorithmen

(Diese Präferenzliste beginnt mit dem bevorzugtesten Algorithmenpaar.)

Verwenden Sie sicherer Algorithmen

Einige der zur Verfügung stehenden Algorithmen sind veraltet und werden nicht mehr als sicher angesehen. Sie sind deshalb nicht zu empfehlen. Aus Gründen der Abwärtskompatibilität können sie jedoch weiterhin ausgewählt und verwendet werden. Im WBM sind entsprechend veraltete Algorithmen oder unsichere Einstellungen mit einem Sternchen (*) markiert.

Siehe „Verwendung sicherer Verschlüsselungs- und Hash-Algorithmen“ .

Vereinbaren Sie mit dem Administrator der Gegenstelle, welches Verschlüsselungsverfahren verwendet werden soll.

Verschlüsselung **DES*, 3DES*, AES-128*, AES-192*, AES-256 (Standard)**

Verwenden Sie sicherer Algorithmen

Einige der zur Verfügung stehenden Algorithmen sind veraltet und werden nicht mehr als sicher angesehen. Sie sind deshalb nicht zu empfehlen. Aus Gründen der Abwärtskompatibilität können sie jedoch weiterhin ausgewählt und verwendet werden. Im WBM sind entsprechend veraltete Algorithmen oder unsichere Einstellungen mit einem Sternchen (*) markiert.

Siehe „Verwendung sicherer Verschlüsselungs- und Hash-Algorithmen“ .

Grundsätzlich gilt Folgendes: Je länger die Schlüssellänge (in Bits) ist, die ein Verschlüsselungsalgorithmus verwendet (angegeben durch die angefügte Zahl), desto sicherer ist er.

Der Verschlüsselungsvorgang ist umso zeitaufwändiger, 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.

IPsec VPN >> Verbindungen >> Editieren >> IKE-Optionen		
	Prüfsumme	**MD5*, SHA-1*, SHA-256 (Standard), SHA-384, SHA-512** 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. **Verwenden Sie sicherer Algorithmen** Einige der zur Verfügung stehenden Algorithmen sind veraltet und werden nicht mehr als sicher angesehen. Sie sind deshalb nicht zu empfehlen. Aus Gründen der Abwärtskompatibilität können sie jedoch weiterhin ausgewählt und verwendet werden. Im WBM sind entsprechend veraltete Algorithmen oder unsichere Einstellungen mit einem Sternchen (*) markiert. Siehe „Verwendung sicherer Verschlüsselungs- und Hash-Algorithmen“ .
	Diffie-Hellman	Das Schlüsselaustausch-Verfahren Diffie-Hellmann ist nicht für alle Algorithmen verfügbar. Sie können hier die Bit-Tiefe der Verschlüsselung einstellen. **Verwenden Sie sicherer Algorithmen** Einige der zur Verfügung stehenden Algorithmen sind veraltet und werden nicht mehr als sicher angesehen. Sie sind deshalb nicht zu empfehlen. Aus Gründen der Abwärtskompatibilität können sie jedoch weiterhin ausgewählt und verwendet werden. Im WBM sind entsprechend veraltete Algorithmen oder unsichere Einstellungen mit einem Sternchen (*) markiert. Siehe „Verwendung sicherer Verschlüsselungs- und Hash-Algorithmen“ .
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. Der zur Auswahl stehende mit „Null“ bezeichnete Algorithmus beinhaltet keinerlei Verschlüsselung.	

IPsec VPN >> Verbindungen >> Editieren >> IKE-Optionen

Algorithmen

Siehe oben: ISAKMP-SA (Schlüsselaustausch).

Soll der Datenaustausch ohne Verschlüsselung stattfinden, muss im Drop-Down-Menü „Verschlüsselung“ der Eintrag „Null“ ausgewählt werden.

Verwenden Sie sicherer Algorithmen

Einige der zur Verfügung stehenden Algorithmen sind veraltet und werden nicht mehr als sicher angesehen. Sie sind deshalb nicht zu empfehlen. Aus Gründen der Abwärtskompatibilität können sie jedoch weiterhin ausgewählt und verwendet werden. Im WBM sind entsprechend veraltete Algorithmen oder unsichere Einstellungen mit einem Sternchen (*) markiert.

Siehe „Verwendung sicherer Verschlüsselungs- und Hash-Algorithmen“ .

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. Phoenix Contact empfiehlt aus Sicherheitsgründen die Aktivierung von PFS mit einer Schlüssellänge von mindestens 2048 Bits.

Verwenden Sie sicherer Algorithmen

Einige der zur Verfügung stehenden Algorithmen sind veraltet und werden nicht mehr als sicher angesehen. Sie sind deshalb nicht zu empfehlen. Aus Gründen der Abwärtskompatibilität können sie jedoch weiterhin ausgewählt und verwendet werden. Im WBM sind entsprechend veraltete Algorithmen oder unsichere Einstellungen mit einem Sternchen (*) markiert.

Siehe „Verwendung sicherer Verschlüsselungs- und Hash-Algorithmen“ .

Wenn die Gegenstelle PFS unterstützt, wählen Sie aus Gründen der Sicherheit nach Möglichkeit eine Schlüssellänge von mindestens **2048 Bits**. Die Auswahl **Ja*** könnte dazu führen, dass eine niedrigere Schlüssellänge verwendet wird.

Ist die Gegenstelle ein IPsec/L2TP-Client, dann setzen Sie *Perfect Forward Secrecy (PFS)* auf **Nein***.

IPsec VPN >> Verbindungen >> Editieren >> IKE-Optionen		
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 (hh:mm:ss). Standard: 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 (hh:mm:ss). Standard: 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. Standard: 540 Sekunden (9 Minuten).
	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.

IPsec VPN >> Verbindungen >> Editieren >> IKE-Optionen		
	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. Standard: 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.
Dead Peer Detection	Wenn die Gegenstelle das Dead Peer Detection (DPD) Protokoll unterstützt, können die jeweiligen Partner erkennen, ob die IPsec-Verbindung noch aktiv 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. Standard: 30 Sekunden (0:00:30).
	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 (0:02:00). 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**).

8.3 IPsec VPN >> L2TP über IPsec

Diese Einstellungen gelten nicht im Stealth-Modus.
Unter Windows 7 ist die Verwendung des MD5-Algorithmus nicht möglich. Der MD5-Algorithmus muss durch SHA-1 ersetzt werden.

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.

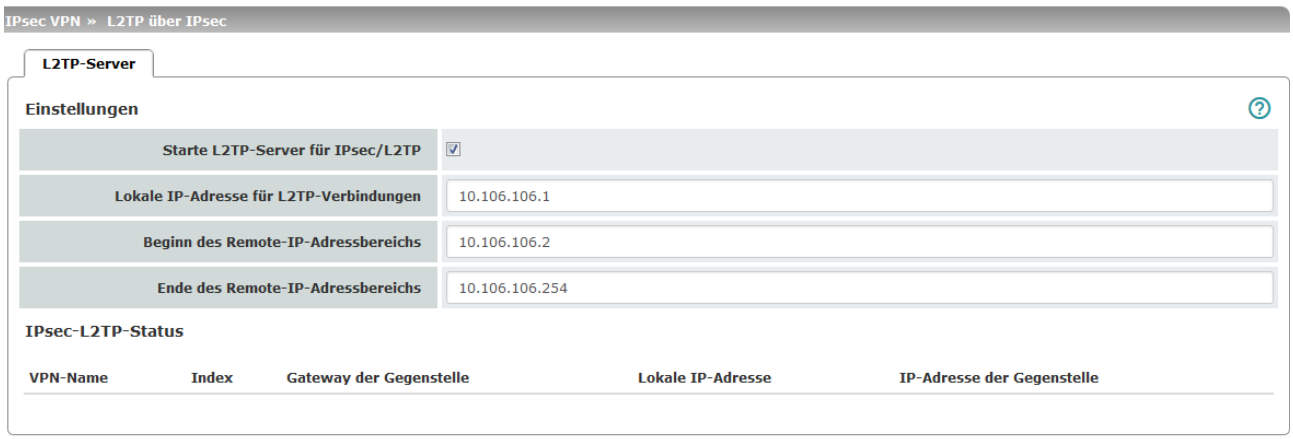
Um IPsec/L2TP zu nutzen muss der L2TP-Server aktiviert werden sowie eine oder mehrere IPsec-Verbindungen mit den folgenden Eigenschaften eingerichtet werden:

- **Typ**: Transport
- **Protokoll**: UDP
- **Lokal:** %all
- **Gegenstelle:** %all
- **PFS**: Nein

Siehe

- „IPsec VPN >> Verbindungen >> Editieren >> Allgemein“ auf Seite 263
- „IPsec VPN >> Verbindungen >> Editieren >> IKE-Optionen“, „Perfect Forward Secrecy (PFS)“ auf Seite 298

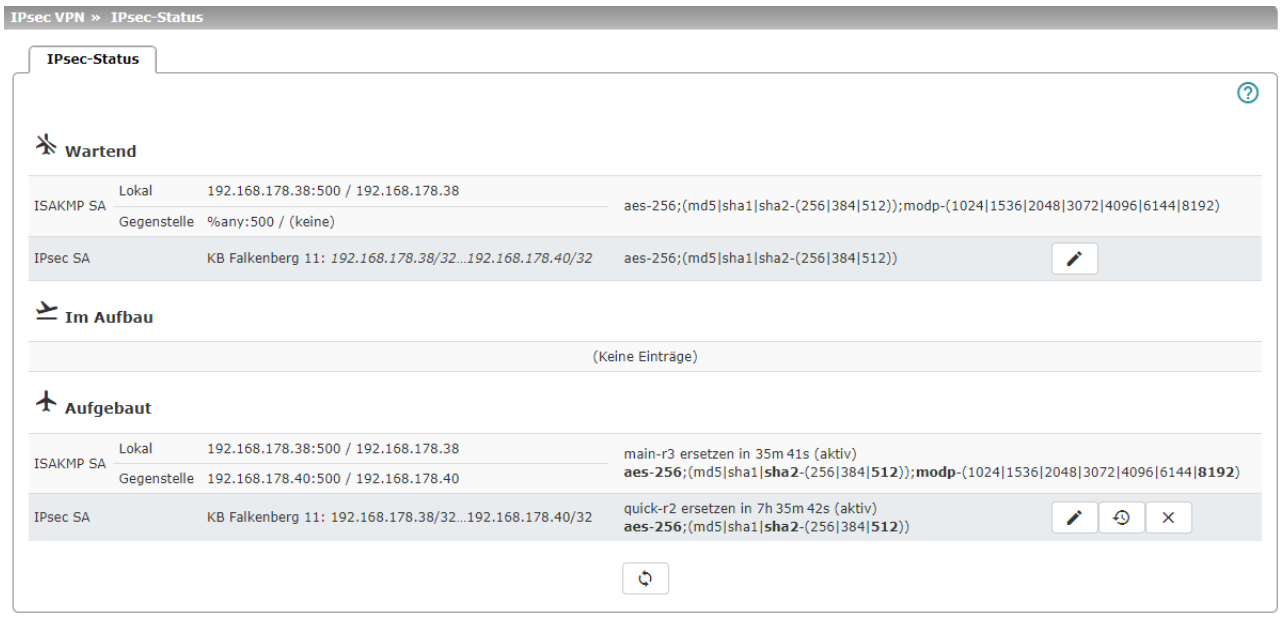
8.3.1 L2TP-Server



IPsec VPN >> L2TP über IPsec >> L2TP-Server		
Einstellungen	**Starte L2TP-Server für IPsec/L2TP**	Wollen Sie IPsec/L2TP-Verbindungen ermöglichen, aktivieren Sie die Funktion. Über IPsec können dann zum mGuard L2TP-Verbindungen aufgebaut werden, über welche den Clients dynamisch IP-Adressen innerhalb des VPNs zugeteilt werden.

IPsec VPN >> L2TP über IPsec >> L2TP-Server		
	Lokale IP-Adresse für L2TP-Verbindungen	Nach dem obigen Screenshot teilt der mGuard der Gegenstelle mit, er habe die Adresse 10.106.106.1.
	Beginn / Ende des Remote-IP-Adressbereichs	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.

8.4 IPsec VPN >> IPsec Status



Informiert über den aktuellen Status der konfigurierten IPsec-Verbindungen.

Wartend: Zeigt alle nicht aufgebauten VPN-Verbindungen an, die mittels einer Initiierung durch Datenverkehr gestartet werden oder auf einen Verbindungsaufbau warten.

Im Aufbau: Zeigt alle VPN-Verbindungen an, die aktuell versuchen, eine Verbindung aufzubauen.

Die ISAKMP SA wurde aufgebaut und die Authentifizierung der Verbindungen war erfolgreich. Verbleibt die Verbindung im Status „Verbindungsaufbau“, stimmten gegebenenfalls andere Parameter nicht: Stimmt der Verbindungstyp (Tunnel, Transport) überein? Wenn Tunnel gewählt ist, stimmen die Netzbereiche auf beiden Seiten überein?

Aufgebaut: Zeigt alle VPN-Verbindungen an, die eine Verbindung erfolgreich aufgebaut haben.

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

Icons

Aktualisieren Um die angezeigten Daten zu aktualisieren, klicken Sie auf das Icon **Aktualisieren**.

Neustart Um eine VPN-Verbindung mit allen Instanzen/Tunneln zu trennen und dann neu zu starten, klicken Sie auf das entsprechende Icon **Neustart**.

Editieren Um eine VPN-Verbindung neu zu konfigurieren, klicken Sie auf das entsprechende Icon **Zeile bearbeiten**.

Löschen Um eine Instanz / einen VPN-Tunnel einer VPN-Verbindung zu beenden, klicken Sie auf das entsprechende Icon **Löschen**.

Verbindung, ISAKMP-SA-Status, IPsec-SA-Status

ISAKMP SA	**Lokal**	– lokale IP-Adresse – lokaler Port – ID = Subject eines X.509-Zertifikats	Zustand, Lebensdauer und Verschlüsselungsalgorithmus der Verbindung (Fett = aktiv)
	Gegenstelle	– Remote-IP-Adresse – lokaler Port – ID = Subject eines X.509-Zertifikats	
IPsec SA		– Name der Verbindung – lokale Netze...Remote-Netze	Zustand, Lebensdauer und Verschlüsselungsalgorithmus der Verbindung (Fett = aktiv)

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.

9 Menü OpenVPN-Client

9.1 OpenVPN-Client >> Verbindungen

Mit OpenVPN kann eine verschlüsselte VPN-Verbindung zwischen dem mGuard als OpenVPN-Client und einer Gegenstelle (OpenVPN-Server) hergestellt werden. Zur Verschlüsselung und Authentifizierung wird die OpenSSL-Bibliothek genutzt. Der Transport der Daten geschieht über die Protokolle TCP oder UDP.

Der OpenVPN-Client unterstützt folgende TLS-Versionen: TLS 1.0, TLS 1.1, TLS 1.2 und TLS 1.3.

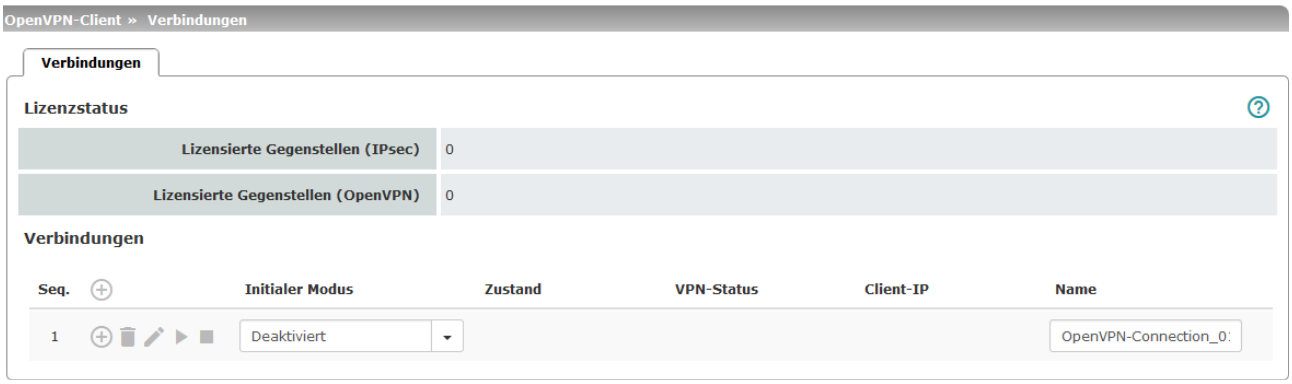
Wählen Sie aus Sicherheitsgründen die Versionen TLS 1.2 oder 1.3 als „Niedrigste unterstützte TLS-Version“ , um sichere TLS-verschlüsselte Verbindungen zu gewährleisten.

Voraussetzungen für eine VPN-Verbindung

Generelle Voraussetzung für eine VPN-Verbindung ist, dass die IP-Adressen der VPN-Gegenstellen 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 „Standard-Gateway“ auf Seite 145). Alternativ können Sie eine andere Stealth-Konfiguration als „mehrere Clients“ wählen oder einen anderen Netzwerk-Modus verwenden.
- Damit eine OpenVPN-Verbindung erfolgreich aufgebaut werden kann, muss die VPN-Gegenstelle das OpenVPN-Protokoll als OpenVPN-Server unterstützen.

9.1.1 Verbindungen



Liste aller VPN-Verbindungen, die definiert worden sind.

Jeder hier aufgeführte Verbindungsname kann eine einzige VPN-Verbindung bezeichnen. Sie haben die Möglichkeit, neue VPN-Verbindungen zu definieren, VPN-Verbindungen zu aktivieren / deaktivieren, die Eigenschaften einer VPN-Verbindung zu ändern (editieren) und Verbindungen zu löschen.

OpenVPN-Client >> Verbindungen		
Lizenzstatus	**Lizenzierte Gegenstellen (IPsec)**	Anzahl der Gegenstellen, die aktuell eine VPN-Verbindung über das IPsec-Protokoll aufgebaut haben.
	Lizenzierte Gegenstellen (OpenVPN)	Anzahl der Gegenstellen, zu denen aktuell eine VPN-Verbindung über das OpenVPN-Protokoll aufgebaut ist.
Verbindungen	**Initialer Modus**	**Deaktiviert / Gestoppt / Gestartet** Die Einstellung „**Deaktiviert**“ deaktiviert die VPN-Verbindung permanent; sie kann weder gestartet noch gestoppt werden. Die Einstellungen „**Gestartet**“ und „**Gestoppt**“ bestimmen den Status der VPN-Verbindung nach einem Neustart/Booten des mGuards (z. B. nach einer Unterbrechung der Stromversorgung). VPN-Verbindungen, die nicht deaktiviert sind, können über Icons in der Web-Oberfläche, SMS, Schalter oder Taster gestartet oder gestoppt werden.
	Zustand	Zeigt den aktuellen Aktivierungszustand der OpenVPN-Verbindung.
	VPN-Status	Zeigt an, ob die entsprechende OpenVPN-Verbindung aufgebaut wurde oder nicht.
	Client-IP	IP-Adresse des OpenVPN-Interface.
	Name	Name der VPN-Verbindung

Verbindungen

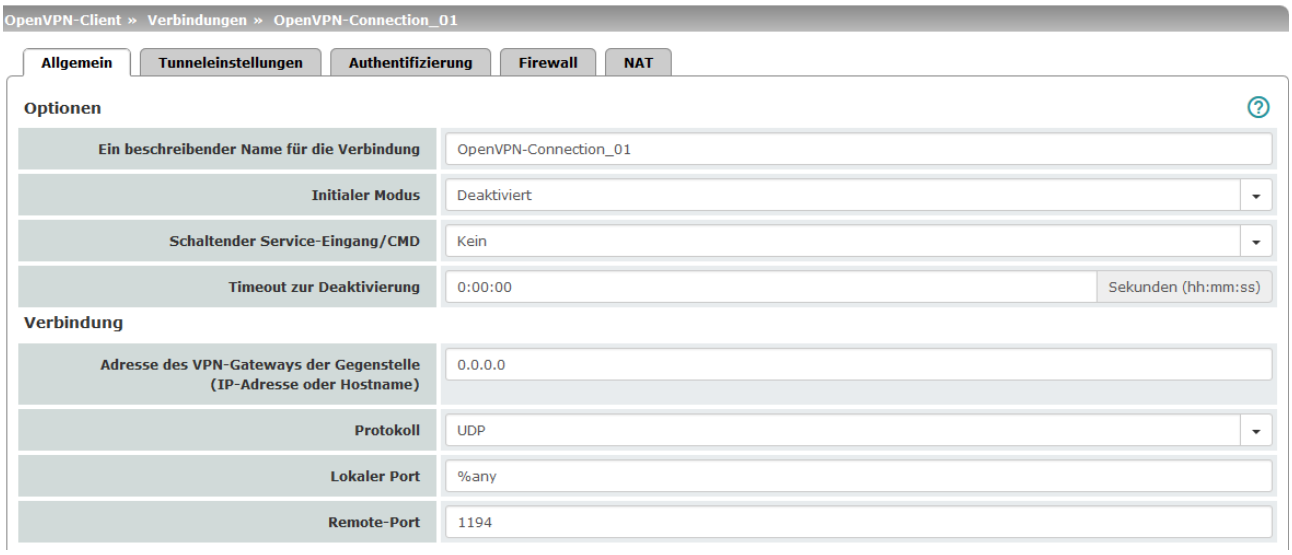
VPN-Verbindung neu definieren

- In der Tabelle der Verbindungen auf das Icon ⊕ **Neue Zeile einfügen** klicken, um eine neue Tabellenzeile hinzuzufügen.
- Auf das Icon ✎ **Zeile bearbeiten** klicken.

VPN-Verbindung bearbeiten

In der gewünschten Zeile auf das Icon ✎ **Zeile bearbeiten** klicken.

9.1.2 Allgemein



OpenVPN-Client >> Verbindungen >> Editieren >> Allgemein

Optionen

Ein beschreibender Name für die Verbindung

Sie können die Verbindung frei benennen bzw. umbenennen.

Initialer Modus

Deaktiviert / Gestoppt / Gestartet

Die Einstellung „**Deaktiviert**“ deaktiviert die VPN-Verbindung permanent; sie kann weder gestartet noch gestoppt werden.

Die Einstellungen „**Gestartet**“ und „**Gestoppt**“ bestimmen den Status der VPN-Verbindung nach einem Neustart/Booten des mGuards (z. B. nach einer Unterbrechung der Stromversorgung).

VPN-Verbindungen, die nicht deaktiviert sind, können über Icons in der Web-Oberfläche, SMS, Schalter oder Taster gestartet oder gestoppt werden.

Schaltender Service Eingang/CMD

Kein / Service-Eingang CMD 1-3 (I 1-3)

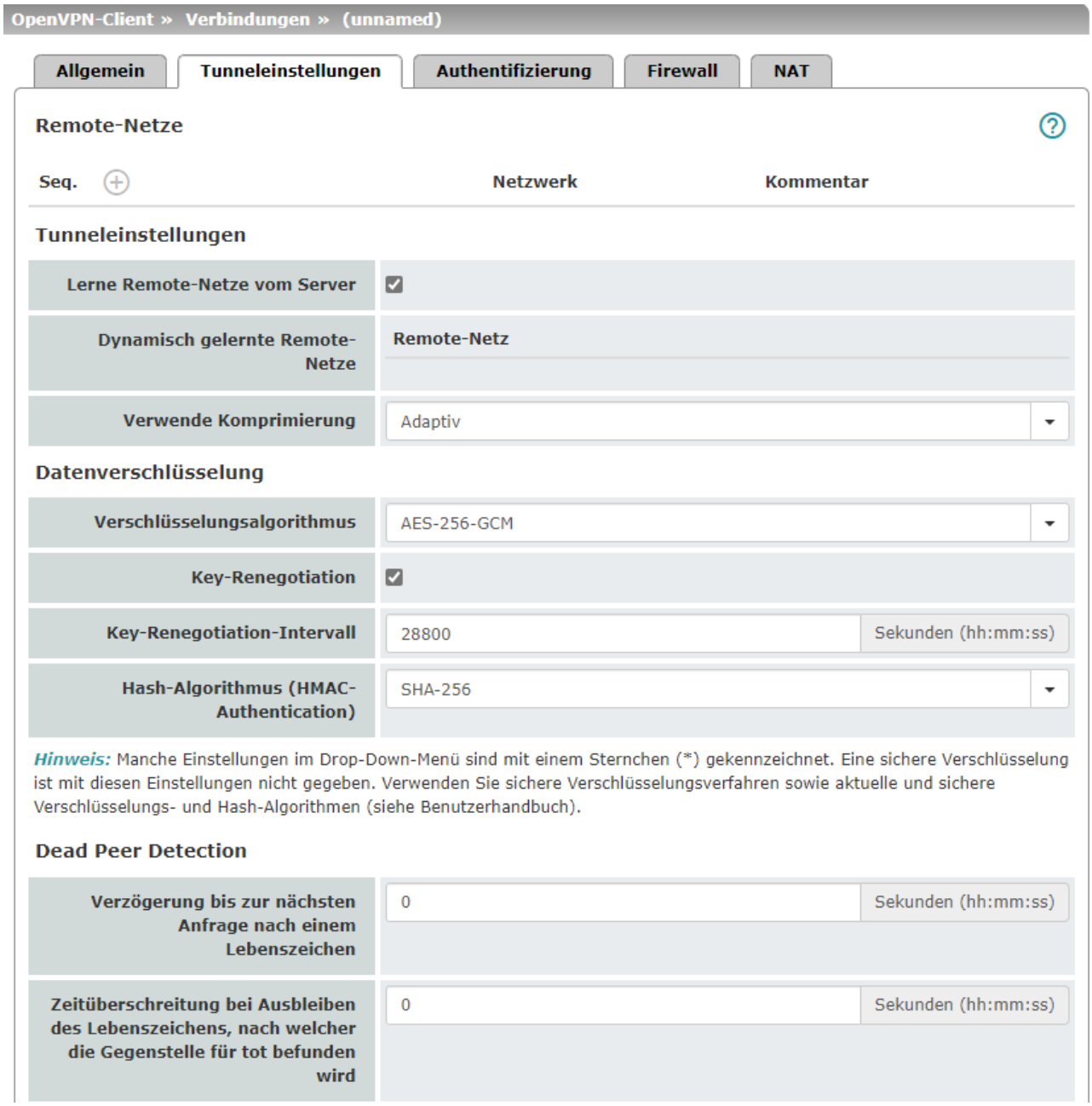
Die VPN-Verbindung kann über einen angeschlossenen Taster/Schalter geschaltet werden.

Der Taster/Schalter muss an einen der Servicekontakte (CMD 1-3 / I 1-3) angeschlossen sein.

Wenn das Starten und Stoppen der VPN-Verbindung über den CMD-Kontakt eingeschaltet ist, hat ausschließlich der CMD-Kontakt das Recht dazu.

	Invertierte Logik verwenden	Kehrt das Verhalten des angeschlossenen Schalters um. Wenn der schaltende Service-Eingang als Ein-/Aus-Schalter konfiguriert ist, kann er z. B. eine VPN-Verbindung ein- und gleichzeitig eine andere, die invertierte Logik verwendet, ausschalten.
	Timeout zur Deaktivierung	Zeit, nach der die VPN-Verbindung gestoppt wird, wenn sie über Schalter, Taster oder die Web-Oberfläche gestartet worden ist. Der Timeout startet beim Übergang in den Zustand „Gestartet“. Die Verbindung verbleibt nach Ablauf des Timeouts in dem Zustand „Gestoppt“, bis sie erneut gestartet wird. Zeit in Stunden, Minuten und/oder Sekunden (0:00:00 bis 720:00:00, etwa 1 Monate). Die Eingabe kann aus Sekunden [ss], Minuten und Sekunden [mm:ss] oder Stunden, Minuten und Sekunden [hh:mm:ss] bestehen. Bei 0 ist diese Einstellung abgeschaltet.
Verbindung	**Adresse des VPN-Gateways der Gegenstelle**	**IP-Adresse oder Hostname der des VPN-Gateways der Gegenstelle**
	Protokoll	**TCP / UDP** Das vom OpenVPN-Server verwendete Netzwerkprotokoll muss an dieser Stelle im mGuard ebenfalls ausgewählt werden.
	Lokaler Port	Port des lokalen OpenVPN-Clients, von dem aus die Verbindung mit einem OpenVPN-Server initiiert wird. Werte: 1 – 65535; Default: %any (Auswahl wird der Gegenstelle überlassen
	Remote-Port	Port des Remote-OpenVPN-Servers, der auf Anfragen des OpenVPN-Clients antworten soll. Werte: 1 – 65535; Default: 1194

9.1.3 Tunneleinstellungen



OpenVPN-Client >> Verbindungen >> Editieren >> Tunneleinstellungen		
Remote-Netze	**Netzwerk**	Adressen der Netze, die sich hinter dem OpenVPN-Server (VPN-Gateway der Gegenstelle) befinden (CIDR-Schreibweise).
	Kommentar	Optional: kommentierender Text.

Tunneleinstellungen

Lerne Remote-Netze vom Server

Bei **aktivierter Funktion** (Standard) werden Remote-Netze automatisch vom Server gelernt, wenn der Server entsprechend konfiguriert ist.

Die Routen zu Remote-Netzen sind dem mGuard nur bekannt, wenn die entsprechende VPN-Verbindung aufgebaut ist.

Solange diese VPN-Verbindung nicht besteht, wird der Netzwerkverkehr an die entsprechenden IP-Adressen folglich nicht geblockt, sondern kann unverschlüsselt über ein anderes Interface versendet werden.

In diesem Fall müssten entsprechende Firewall-Regeln erstellt werden.

Routen zu Remote-Netzen hinter dem OpenVPN-Server können auch von höher priorisierten Routen auf anderen Interfaces überschrieben werden, z. B. wenn Routen mit einem kleineren Ziel-Netzwerk bestehen.

Wenn beispielsweise 10.0.0.0/8 eine Route über das OpenVPN-Interface und 10.1.0.0/16 eine Route über das externe Interface ist, wird der Netzwerkverkehr an die IP-Adresse 10.1.0.1 unverschlüsselt über das externe Interface versendet.

Bei **deaktivierter Funktion** werden die statisch eingetragenen Routen verwendet.

Dynamisch gelernte Remote-Netze

Dynamisch gelernte Remote-Netze werden angezeigt.

Verwende Komprimierung

Ja / **Nein** / **Adaptiv / Deaktiviert**

Sie können auswählen, ob eine Komprimierung immer, nie oder adaptiv (je nach Art des Traffics angepasst) angewendet wird.

Die Option **Deaktiviert** deaktiviert die Komprimierung vollständig, indem die Benutzung von *liblzo* bzw. *comp-lzo* deaktiviert wird.

Beachten Sie, dass Server und Client die gleichen Komprimierungs-Einstellungen verwenden müssen. Dies betrifft insbesondere die Benutzung von *liblzo* bzw. *comp-lzo*.

Datenverschlüsselung	**Verschlüsselungsalgorithmus**	**AES-128-CBC*** / **AES-192-CBC*** / **AES-256-CBC*** / **AES-128-GCM*** / **AES-192-GCM*** / **AES-256-GCM (Standard)** Vereinbaren Sie mit dem Administrator der Gegenstelle, welcher Verschlüsselungsalgorithmus verwendet werden soll. **Verwenden Sie sicherer Algorithmen** Einige der zur Verfügung stehenden Algorithmen sind veraltet und werden nicht mehr als sicher angesehen. Sie sind deshalb nicht zu empfehlen. Aus Gründen der Abwärtskompatibilität können sie jedoch weiterhin ausgewählt und verwendet werden. Im WBM sind entsprechend veraltete Algorithmen und unsichere Einstellungen mit einem Sternchen (*) markiert. Siehe „Verwendung sicherer Verschlüsselungs- und Hash-Algorithmen“ . Grundsätzlich gilt Folgendes: Je länger die Schlüssellänge (in Bits) ist, die ein Verschlüsselungsalgorithmus verwendet (angegeben durch die angefügte Zahl), desto sicherer ist er. Der Verschlüsselungsvorgang ist umso zeitaufwändiger, je länger der Schlüssel ist.
	Hash-Algorithmus (HMAC-Authentication)	**SHA-1*, SHA-256 (Standard), SHA-512** Hash-Funktion zur Berechnung der Prüfsumme, die zur Absicherung der verschlüsselten OpenVPN-Verbindung zwischen OpenVPN-Server und mGuard-Client verwendet wird. **Verwenden Sie sicherer Algorithmen** Einige der zur Verfügung stehenden Algorithmen sind veraltet und werden nicht mehr als sicher angesehen. Sie sind deshalb nicht zu empfehlen. Aus Gründen der Abwärtskompatibilität können sie jedoch weiterhin ausgewählt und verwendet werden. Im WBM sind entsprechend veraltete Algorithmen und unsichere Einstellungen mit einem Sternchen (*) markiert. Siehe „Verwendung sicherer Verschlüsselungs- und Hash-Algorithmen“ .
	Key-Renegotiation	Bei **aktivierter Funktion** (Standard) wird der mGuard versuchen, einen neuen Schlüssel zu vereinbaren, wenn die Gültigkeit des alten abläuft.
	Key-Renegotiation-Intervall	Zeitspanne, nach der die Gültigkeit des aktuellen Schlüssels abläuft und eine neuer Schlüssel zwischen Server und Client vereinbart wird. Zeit in hh:mm:ss (Standard: 8 h)

Dead Peer Detection

Wenn die Gegenstelle Dead Peer Detection unterstützt, können die jeweiligen Partner erkennen, ob die OpenVPN-Verbindung noch aktiv ist oder neu aufgebaut werden muss.

Verzögerung bis zur nächsten Anfrage nach einem Lebenszeichen

Zeitspanne, nach welcher DPD Keep Alive-Anfragen gesendet werden sollen. Diese Anfragen testen, ob die Gegenstelle noch verfügbar ist.

Zeit in hh:mm:ss

Default: 0:00:00 (DPD ist ausgeschaltet)

Zeitüberschreitung bei Ausbleiben des Lebenszeichens, nach welcher die Gegenstelle für tot befunden wird

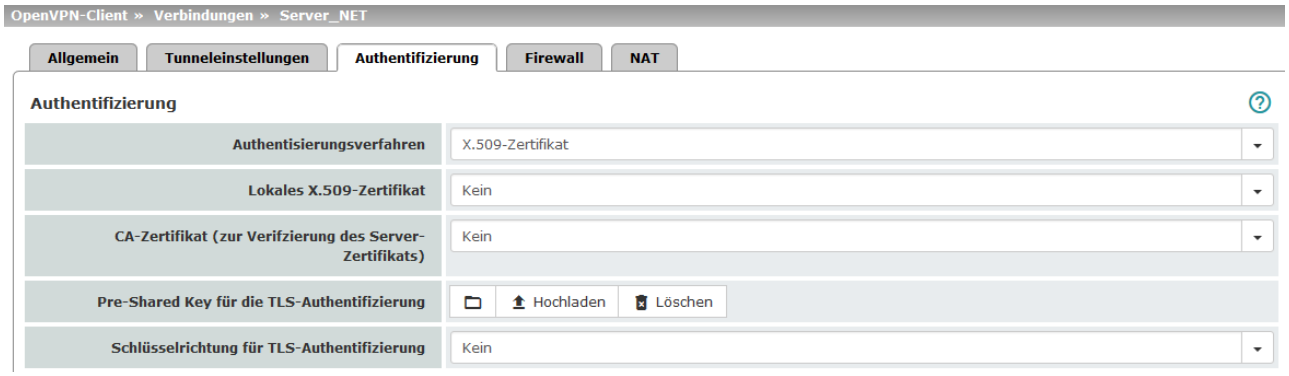
Zeitspanne, nach der die Verbindung zur Gegenstelle für tot erklärt werden soll, wenn auf die Keep Alive-Anfragen keine Antwort erfolgte.

Zeit in hh:mm:ss

Wenn keine Antwort erfolgt, wird die Verbindung vom mGuard neu initiiert.

Default: 0:00:00 (DPD ist ausgeschaltet)

9.1.4 Authentifizierung



OpenVPN-Client >> Verbindungen >> Editieren >> Authentifizierung

Authentifizierung

Authentisierungsverfahren

Es gibt drei Möglichkeiten für den mGuard, sich als OpenVPN-Client bei einem OpenVPN-Server zu authentifizieren:

- X.509-Zertifikat (Standard)
- Login/Passwort
- X.509-Zertifikat + Login/Passwort

Je nachdem, welches Verfahren Sie auswählen, zeigt die Seite unterschiedliche Einstellmöglichkeiten.

Login

Bei Authentisierungsverfahren Login/Passwort

Benutzerkennung (Login), mit der sich der mGuard beim OpenVPN-Server authentifiziert.

Passwort

Verabredetes Passwort, das bei der Authentifizierung mit einer Benutzerkennung (Login) verwendet wird.

Um eine hinreichende Sicherheit zu erzielen, sollte die Zeichenfolge aus ca. 30 nach dem Zufallsprinzip ausgewählten Klein- und Großbuchstaben sowie Ziffern bestehen.

Bei Authentisierungsverfahren X.509-Zertifikat

Jeder VPN-Teilnehmer besitzt 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

OpenVPN-Client >> 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.

Falls nur der Eintrag *Kein* zu sehen ist, muss erst ein Zertifikat installiert werden. Der Eintrag *Kein* darf nicht belassen werden, weil sonst keine X.509-Authentifizierung möglich ist.

CA-Zertifikat (zur Verifizierung des Server-Zertifikats)

An dieser Stelle ist ausschließlich das CA-Zertifikat von der CA (Certification Authority) zu referenzieren (in der Auswahlliste auszuwählen), welche das von der VPN-Gegenstelle (OpenVPN-Server) vorgezeigte Zertifikat signiert hat.

Die Verifizierung mit einem CA-Zertifikat ist auch erforderlich, wenn als Authentisierungsverfahren „Benutzerkennung/Passwort“ ausgewählt ist.

Die weiteren CA-Zertifikate, die mit dem von der Gegenstelle vorgezeigten Zertifikat die Kette bis zum Root-CA-Zertifikat bilden, müssen dann in den mGuard importiert werden – unter Menüpunkt „Authentifizierung >> Zertifikate“ auf Seite 192.

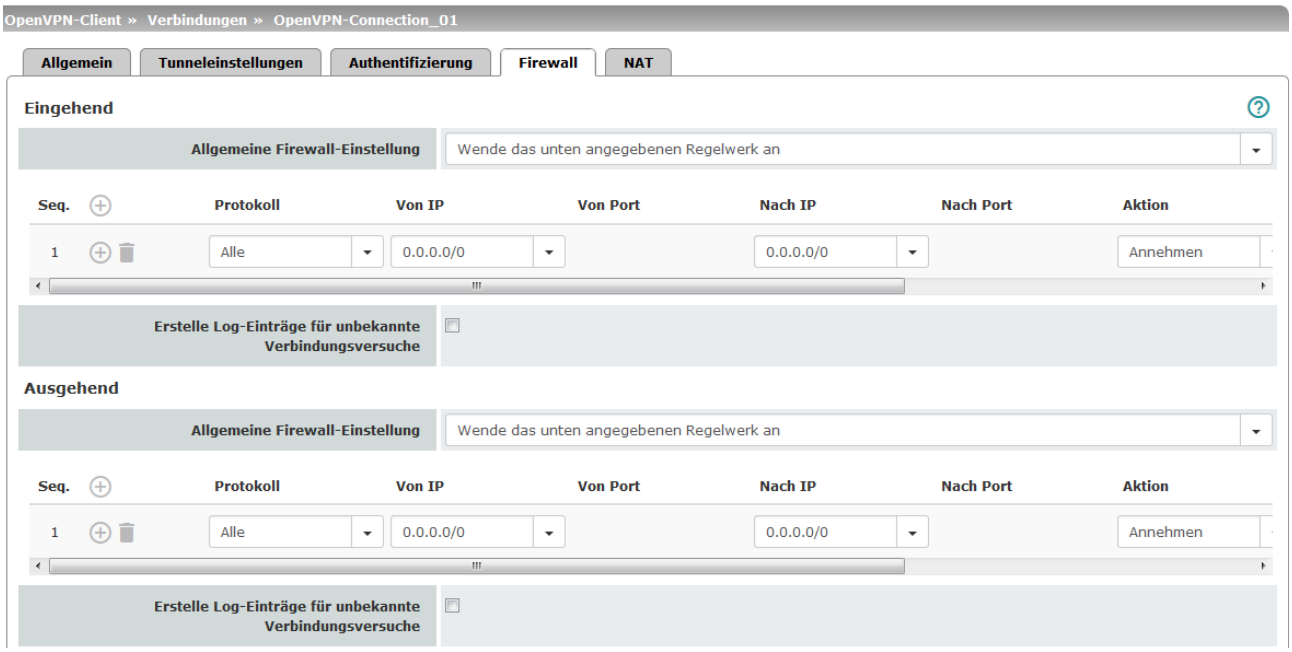
Falls nur der Eintrag *Kein* zu sehen ist, muss erst ein Zertifikat importiert werden. Der Eintrag *Kein* darf nicht belassen werden, weil sonst keine Authentifizierung des VPN-Servers möglich ist.

Die Auswahlliste stellt alle CA-Zertifikate zur Wahl, die unter Menüpunkt „Authentifizierung >> Zertifikate“ in den mGuard importiert wurden.

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.

OpenVPN-Client >> Verbindungen >> Editieren >> Authentifizierung		
	Pre-Shared Key für die TLS-Authentifizierung	Zur Erhöhung der Sicherheit (z. B. Verhinderung von DoS-Angriffen) kann die Authentifizierung der OpenVPN-Verbindung zusätzlich über Pre-Shared-Keys (TLS-PSK) abgesichert werden. Dazu muss eine statische PSK-Datei (z. B. *ta.key*) zunächst erzeugt und auf beiden OpenVPN-Gegenstellen (Server und Client) installiert und aktiviert werden. Die PSK-Datei kann – vom OpenVPN-Server erzeugt werden **oder** – aus einer beliebigen Datei (8 – 2048 Bytes) bestehen. Wird die Datei vom Server erzeugt, kann zusätzlich die Schlüsselrichtung ausgewählt werden (siehe unten). Um TLS-Authentifizierung zu aktivieren, muss eine PSK-Datei über das Icon 🗀 ausgewählt und über die Schaltfläche **Hochladen** hochgeladen werden. Um die TLS-Authentifizierung zu deaktivieren, muss die Datei über die Schaltfläche **Löschen** gelöscht werden. Die Schaltfläche **Löschen** ist immer sichtbar, d. h. auch dann, wenn keine PSK-Datei hochgeladen oder eine hochgeladene PSK-Datei gelöscht wurde.
	Schlüsselrichtung für die TLS-Authentifizierung	**Kein / 0 / 1** **Kein** Muss ausgewählt werden, wenn die PSK-Datei **nicht** vom OpenVPN-Server erzeugt wurden. **0 und 1** Kann ausgewählt werden, wenn die PSK-Datei vom OpenVPN-Server erzeugt wurde. Die Auswahl auf Client- und Serverseite muss dabei komplementär (0 <–>1 oder 1 <–> 0) oder identisch (Kein <–> Kein) erfolgen. Fehlerhafte Einstellungen führen dazu, dass die Verbindung nicht aufgebaut wird und ein Log-Eintrag erstellt wird.

9.1.5 Firewall



Firewall eingehend, Firewall ausgehend

Während die unter dem Menüpunkt *Netzwerksicherheit* vorgenommenen Einstellungen sich nur auf Nicht-VPN-Verbindungen beziehen (siehe oben unter „Menü Netzwerksicherheit“ auf Seite 209), 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 209, „Netzwerksicherheit >> Paketfilter“ auf Seite 209, „Erweitert“ auf Seite 230).

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 *Single-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 unter dem Menüpunkt *IPsec VPN >> Global* auf der Registerkarte *Optionen* die Funktion **Erlaube Paketweiterleitung zwischen VPN-Verbindungen** aktiviert, werden für die in den mGuard eingehende Datenpakete die Regeln unter Firewall **eingehend** angewendet und für die ausgehende Datenpakete die Regeln unter Firewall **ausgehend**. Das gilt ebenso für OpenVPN-Verbindungen wie für IPsec-Verbindungen.

Fallen die ausgehenden Datenpakete unter die selbe Verbindungsdefinition, 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.

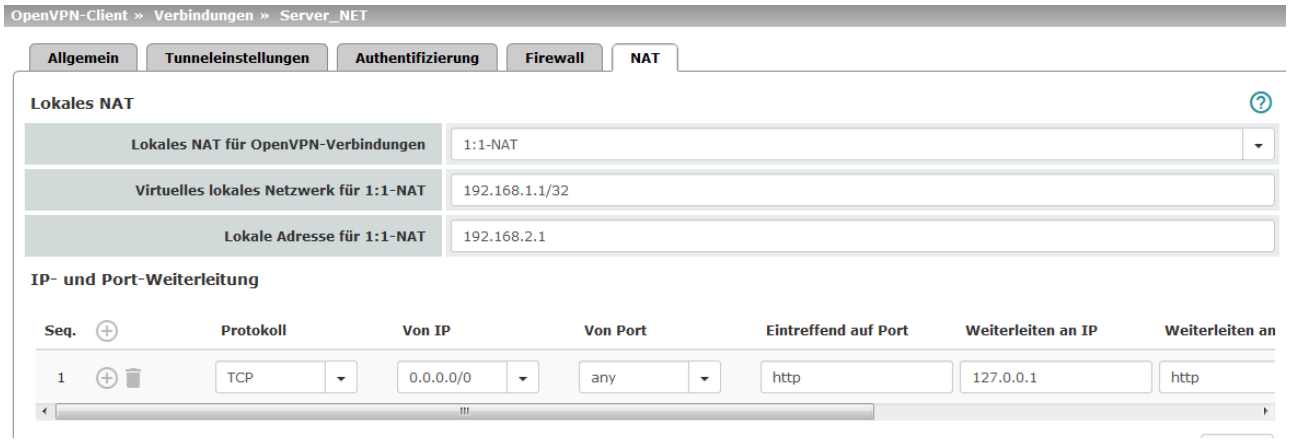
OpenVPN-Client >> Verbindungen >> Editieren >> Firewall		
Eingehend	**Allgemeine Firewall-Einstellung**	**Alle eingehenden Verbindungen annehmen**, die Datenpakete aller eingehenden Verbindungen werden angenommen. **Alle eingehenden Verbindungen verwerfen**, die Datenpakete aller eingehenden Verbindungen werden verworfen. **Nur Ping zulassen,** die Datenpakete aller eingehenden Verbindungen werden verworfen, mit Ausnahme der Ping-Pakete (ICMP). **Wende das unten angegebene Regelwerk an,** blendet weitere Einstellmöglichkeiten ein.
	Die folgenden Einstellungen sind nur sichtbar, wenn „**Wende das unten angegebene Regelwerk an**“ eingestellt ist.	

OpenVPN-Client >> Verbindungen >> Editieren >> Firewall

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 43). **Namen von IP-Gruppen**, sofern definiert. Bei Angabe eines Namens einer IP-Gruppe werden die Hostnamen, IP-Adressen, IP-Bereiche oder Netzwerke berücksichtigt, die unter diesem Namen gespeichert sind (siehe „IP- und Portgruppen“ auf Seite 227). Werden Hostnamen in IP-Gruppen verwendet, muss der mGuard so konfiguriert sein, dass der Hostname von einem DNS-Server in eine IP-Adresse aufgelöst werden kann. Kann ein Hostname aus einer IP-Gruppe nicht aufgelöst werden, wird dieser Host bei der Regel nicht berücksichtigt. Weitere Einträge in der IP-Gruppe sind davon nicht betroffen und werden berücksichtigt. Auf Geräten der FL MGUARD 2000-Serie ist die Verwendung von Hostnamen in IP-Gruppen nicht möglich. **Eingehend**: – Von IP: die IP-Adresse im VPN-Tunnel – Nach IP die 1:1-NAT-Adresse bzw. die reale Adresse **Ausgehend**: – Von IP: die 1:1-NAT-Adresse bzw. die reale Adresse – Nach IP: die IP-Adresse im VPN-Tunnel
Von Port / Nach Port **(Nur 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). **Namen von Portgruppen**, sofern definiert. Bei Angabe eines Namens einer Portgruppe werden die Ports oder Portbereiche berücksichtigt, die unter diesem Namen gespeichert sind (siehe „IP- und Portgruppen“ auf Seite 227).

OpenVPN-Client >> 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. **Namen von Regelsätzen**, sofern definiert. Bei Angabe eines Namens für Regelsätze treten die Firewall-Regeln in Kraft, die unter diesem Namen konfiguriert sind (siehe Registerkarte „Regelsätze“). Regelsätze, die IP-Gruppen mit Hostnamen enthalten, sollten aus Sicherheitsgründen nicht in Firewall-Regeln verwendet werden, die als Aktion „Verwerfen“ oder „Abweisen“ ausführen. Auf Geräten der FL MGUARD 2000-Serie ist die Verwendung von Regelsätzen nicht möglich. **Namen von Modbus-TCP-Regelsätzen**, sofern definiert. Bei der Auswahl eines Modbus-TCP-Regelsatzes treten die Firewall-Regeln in Kraft, die unter diesem Regelsatz konfiguriert sind (siehe Kapitel 7.2.1).
	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 – Funktion *Log* aktivieren – oder nicht – Funktion *Log* deaktivieren (Standard).
	Log-Einträge für unbekannte Verbindungsversuche	Bei aktivierter Funktion werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden.
Ausgehend	Die Erklärung unter „Eingehend“ gilt auch für „Ausgehend“.	

9.1.6 NAT



Die IP-Adresse (OpenVPN-Client-IP-Adresse), die der mGuard als OpenVPN-Client verwendet, wird ihm vom OpenVPN-Server der Gegenstelle zugewiesen.

Wenn kein NAT verwendet wird, müssen die lokalen Netze des mGuards, von denen aus die OpenVPN-Verbindung genutzt werden soll, statisch im OpenVPN-Server konfiguriert werden. Es empfiehlt sich daher, NAT zu verwenden, d. h., lokale Routen (lokale IP-Adressen innerhalb des privaten Adressraums) auf die OpenVPN-Client-IP-Adresse umzuschreiben, damit Geräte im lokalen Netzwerk die OpenVPN-Verbindung nutzen können.

OpenVPN-Client >> Verbindungen >> Editieren >> NAT

Lokales NAT

Das Gerät kann bei ausgehenden Datenpaketen die in ihnen angegebenen Absender-IP-Adressen aus seinem internen Netzwerk auf seine OpenVPN-Client-IP-Adresse umschreiben, eine Technik, die als NAT (Network Address Translation) bezeichnet wird.

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 sollen.

In der **Werkseinstellung (0.0.0.0/0)** werden alle Netzwerke hinter dem mGuard maskiert und können die OpenVPN-Verbindung nutzen.

Lokales NAT für OpenVPN-Verbindungen

Kein NAT / 1:1-NAT / Maskieren

Es können die IP-Adressen von Geräten umgeschrieben werden, die sich am lokalen Ende des OpenVPN-Tunnels befinden (d. h. hinter dem mGuard).

Kein NAT: Es wird kein NAT vorgenommen.

Bei **1:1-NAT** werden die IP-Adressen von Geräten am lokalen Ende des Tunnels so ausgetauscht, dass jede einzelne gegen eine bestimmte andere umgeschrieben wird.

Beim **Maskieren** werden die IP-Adressen von Geräten am lokalen Ende des Tunnels gegen eine für alle Geräte identische IP-Adresse ausgetauscht.

OpenVPN-Client >> Verbindungen >> Editieren >> NAT

Virtuelles lokales Netzwerk für 1:1-NAT

(Wenn „1:1-NAT“ ausgewählt wurde)

Konfiguriert den virtuellen IP-Adressbereich, auf den die realen lokalen IP-Adressen bei Verwendung von 1:1-NAT umgeschrieben werden.

Die angegebene Netzmaske in CIDR-Schreibweise gilt ebenfalls für die *Lokale Adresse für 1:1-NAT* (siehe unten).

Wenn unter *IPsec VPN >> Global >> Optionen* die Funktion **Erlaube Paketweiterleitung zwischen VPN-Verbindungen** aktiviert wurde, wird die Nutzung der virtuellen lokalen Netzwerkadressen in anderen OpenVPN-Verbindungen nicht unterstützt.

Lokale Adresse für 1:1-NAT

(Wenn „1:1-NAT“ ausgewählt wurde)

Konfiguriert den lokalen IP-Adressbereich, aus dem IP-Adressen durch die Verwendung von 1:1-NAT auf die virtuelle IP-Adressen im oben definierten *Virtuellen Lokalen Netzwerk für 1:1-NAT* (siehe oben) umgeschrieben werden.

Es gilt die für das *Virtuelle lokale Netzwerk für 1:1-NAT* angegebene Netzmaske (siehe oben).

Netzwerk

(Wenn „Maskieren“ ausgewählt wurde)

Interne Netzwerke, deren Geräte-IP-Adressen auf die OpenVPN-Client-IP-Adresse umgeschrieben werden.

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 43).

Die Maskierung von Remote-Netzen kann unter *Netzwerk >> NAT >> Maskierung* (siehe „Maskierung“ auf Seite 153) konfiguriert werden.

Wenn die Funktion **Lokales NAT / Maskieren** benutzt wird, muss zusätzlich IP- und Port-Weiterleitung genutzt werden (siehe unten), um aus dem Remote-Netz auf Geräte im lokalen Netz des mGuards zugreifen zu können.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

IP- und Port-Weiterleitung

Listet die festgelegten Regeln zur IP- und Port-Weiterleitung (DNAT = Destination-NAT) auf.

Bei IP- und Port-Weiterleitung (**DNAT**) geschieht Folgendes: Der Header eingehender Datenpakete aus dem OpenVPN-Tunnel, die an die OpenVPN-Client-IP-Adresse 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 die Port-Nummer im Header eingehender Datenpakete werden geändert.

Wird Port-Weiterleitung angewendet, passieren die Pakete die mGuard-Firewall ohne Berücksichtigung der unter *„Netzwerksicherheit >> Paketfilter >> Eingangsregeln“* konfigurierten Regeln.

OpenVPN-Client >> Verbindungen >> Editieren >> NAT

Protokoll: TCP / UDP / GRE

Geben Sie hier das Protokoll an, auf das sich die Regel beziehen soll (**TCP** / **UDP** / **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 43).

Namen von IP-Gruppen, sofern definiert. Bei Angabe eines Namens einer IP-Gruppe werden die Hostnamen, IP-Adressen, IP-Bereiche oder Netzwerke berücksichtigt, die unter diesem Namen gespeichert sind (siehe „IP- und Portgruppen“ auf Seite 227).

Werden Hostnamen in IP-Gruppen verwendet, muss der mGuard so konfiguriert sein, dass der Hostname von einem DNS-Server in eine IP-Adresse aufgelöst werden kann.

Kann ein Hostname aus einer IP-Gruppe nicht aufgelöst werden, wird dieser Host bei der Regel nicht berücksichtigt. Weitere Einträge in der IP-Gruppe sind davon nicht betroffen und werden berücksichtigt.

Von Port

Absenderport, für den Weiterleitungen durchgeführt werden sollen.

any bezeichnet jeden beliebigen Port.

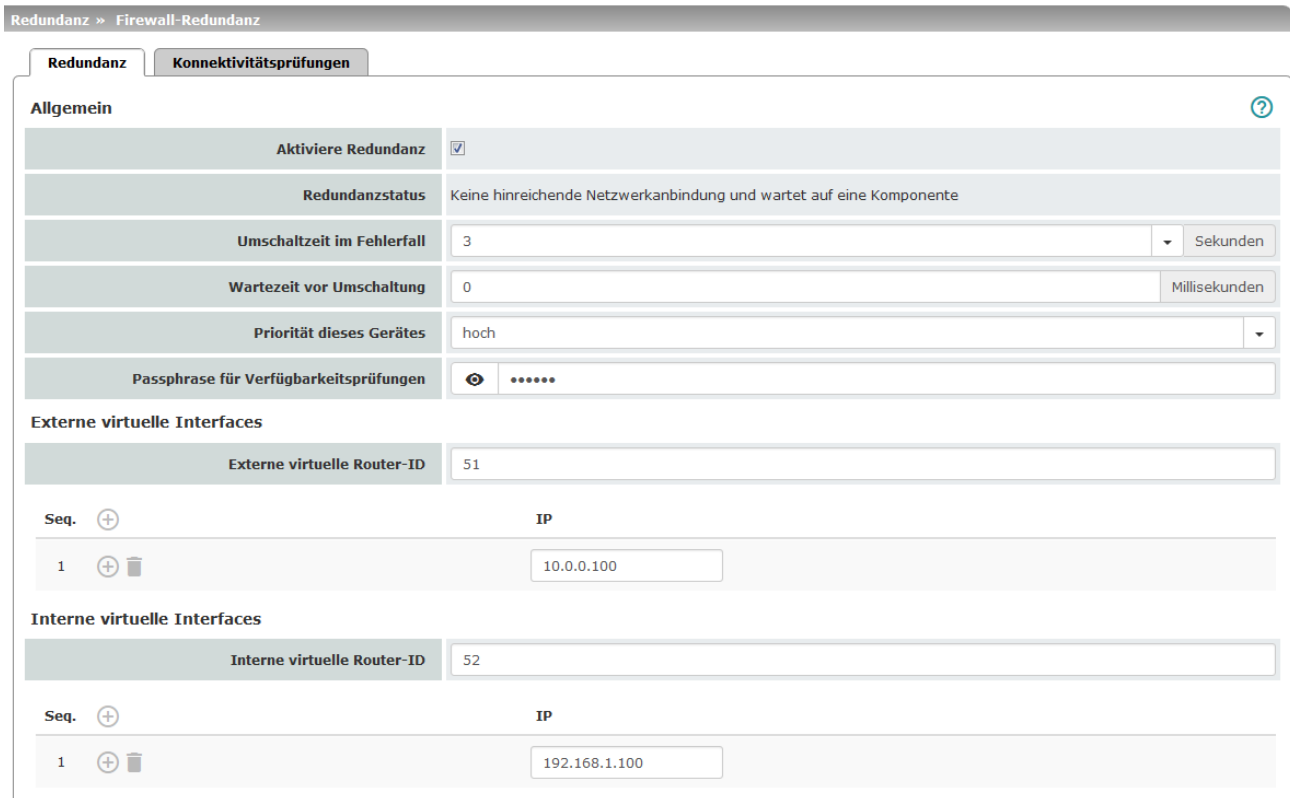
Er kann entweder über die Port-Nummer oder über den entsprechenden Servicenamen angegeben werden, z. B. *pop3* für Port 110 oder *http* für Port 80.

Namen von Portgruppen, sofern definiert. Bei Angabe eines Namens einer Portgruppe werden die Ports oder Portbereiche berücksichtigt, die unter diesem Namen gespeichert sind (siehe „IP- und Portgruppen“ auf Seite 227).

OpenVPN-Client >> Verbindungen >> Editieren >> NAT		
	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	Interner Port, an den die Datenpakete weitergeleitet werden sollen und auf den der Original-Port umgeschrieben wird.
	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 - Funktion *Log* aktivieren. – oder nicht - Funktion *Log* deaktivieren setzen (Standard).

10 Menü Redundanz

	Die Firewall-Redundanz kann aktuell nur aktiviert werden, wenn keine VPN-Verbindungen auf dem Gerät konfiguriert sind.
	Die Firewall-Redundanz steht **nicht** auf den Geräten der FL MGUARD 2000-Serie zur Verfügung.
	Eine ausführliche Darstellung zum Thema Redundanz finden Sie in Kapitel 13, „Redundanz“.
	Um die Redundanzfunktion zu nutzen, muss auf beiden Geräten die gleiche Firmware installiert sein.
	Bei aktivierter Redundanzfunktion kann VLAN im Stealth-Modus nicht verwendet werden.



10.1 Redundanz >> Firewall-Redundanz

10.1.1 Redundanz

Redundanz >> Firewall-Redundanz >> Redundanz		
Allgemein	**Aktiviere Redundanz**	**Deaktiviert** (Standard): Die Firewall-Redundanz ist ausgeschaltet. **Aktiviert**: Die Firewall-Redundanz ist aktiviert.
	Redundanzstatus	Zeigt den aktuellen Status an.
	Umschaltzeit im Fehlerfall	Zeit, die im Fehlerfall maximal verstreichen darf, bevor auf das andere mGuard-Gerät 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-Gerät, das aktiv sein soll, die Priorität **hoch**. Das Gerät in Bereitschaft bekommt die Priorität **niedrig**. Beide Geräte eines Redundanzpaares dürfen entweder eine unterschiedliche Priorität oder die Priorität **hoch** haben. Setzen Sie niemals **beide** mGuard-Geräte eines Redundanzpaares auf die Priorität **niedrig**.

Redundanz >> Firewall-Redundanz >> Redundanz

Passphrase für Verfügbarkeitstest

Bei einem mGuard-Gerät, das 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:

Stellen Sie das neue Passwort an beiden mGuard-Geräten 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 328.

Sobald ein Redundanzpaar ein neues Passwort erhalten hat, handelt es selbst aus, wann es unterbrechungsfrei zum neuen Passwort wechseln kann.

Wenn ein Gerät während des Passwort-Wechsels ausfällt, gibt es diese Fälle:

- Die Passwort-Erneuerung wurde an allen mGuard-Geräten gestartet und dann unterbrochen, z. B. durch einen Netzwerk-Fehler. Dieser Fall wird automatisch behoben.
- Die Passwort-Erneuerung wurde an allen mGuard-Geräten gestartet. Aber dann fällt ein Gerät aus und muss ausgetauscht werden.
- Die Passwort-Erneuerung wurde gestartet, aber nicht an allen Geräten, weil diese ausgefallen sind. Sobald ein fehlerhaftes Gerät wieder online ist, muss die Passwort-Erneuerung gestartet werden. Bei einem ausgetauschten Gerät muss dieses zunächst mit dem alten Passwort konfiguriert werden, bevor es angeschlossen wird.

Redundanz >> Firewall-Redundanz >> Redundanz

Vorgehensweise bei einem falschem Passwort

Wenn Sie versehentlich bei einem Gerät ein falsches Passwort eingegeben haben, dann gehen Sie wie hier beschrieben vor.

Wenn Sie das alte Passwort noch kennen, gehen Sie so vor:

- Rekonfigurieren Sie das Gerät, bei dem das falsche Passwort eingetragen wurde, noch einmal mit dem alten Passwort.
- Warten Sie bis das Gerät 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 Gerät auslesen können.
- Wenn das andere Gerät ausgeschaltet ist oder fehlt, dann können Sie bei dem aktiven Gerät, das sie versehentlich das falsche Passwort eingestellt haben, einfach das korrekte neue Passwort eintragen. Sorgen Sie dafür, dass das andere Gerät das gleiche Passwort erhält, bevor er wieder in Betrieb geht.
- Wenn das andere Gerät das neue Passwort bereits verwendet, dann müssen Sie sicherstellen, dass das Gerät 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 Geräte ein Fehler bei der Redundanz vorliegt. Ein Gerät 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 Gerät ein.
  - Nehmen Sie das nicht aktive Gerät wieder in Betrieb. Stecken Sie zum Beispiel das Ethernet-Kabel wieder ein oder stellen Sie die alten Einstellungen für die Konnektivitätsprüfung wieder her.

Externe virtuelle Interfaces

Externe virtuelle Router-ID

1, 2, 3, ... 255 (Standard: 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 Geräte 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 VRRP (*Virtuell Router Redundancy Protokoll*) nutzt. Die hier eingestellte ID muss sich unterscheiden von den IDs der Geräte, die VRRP oder CARP nutzen und sich im selben Ethernet-Segment befinden.

Redundanz >> Firewall-Redundanz >> Redundanz		
	Externe virtuelle IP-Adressen (IP)	Default: 10.0.0.100 Nur im Netzwerk-Modus „Router“ IP-Adressen, die von beiden mGuard-Geräten als virtuelle IP-Adresse des externen Interfaces geteilt wird. Diese IP-Adressen müssen für beide Geräte 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. Das aktive Gerät kann auf dieser IP-Adresse ICMP-Anfragen erhalten. Er reagiert auf diese ICMP-Anfragen wie es im Menü unter *„Netzwerksicherheit >> Paketfilter >> Erweitert“* eingestellt ist. Für die virtuelle IP-Adressen werden keine Netzwerkmasken oder VLAN IDs 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. Das Gerät 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.
Interne virtuelle Interfaces	**Interne virtuelle Router-ID**	1, 2, 3, ... 255 (Standard: 52) 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 Geräte 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.

Redundanz >> Firewall-Redundanz >> Redundanz		
	Interne virtuelle IP-Adressen (IP)	Wie unter *„Externe virtuelle IP-Adressen (IP)“* beschrieben, aber mit zwei Ausnahmen Unter **Interne virtuelle IP-Adresse (IP)** 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 konfiguriert 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 >> Erweitert“*.

10.1.2 Konnektivitätsprüfung

Bei jedem Gerät eines Redundanzpaares wird kontinuierlich geprüft, ob auf der internen und externen Netzwerk-Schnittstelle jeweils eine Verbindung besteht, über die Netzwerkpakete weitergeleitet werden können.

Da die Redundanzfunktion auf der DMZ-Schnittstelle nicht anwendbar ist, werden Netzwerkverbindungen über eine vorhandene DMZ-Schnittstelle nicht geprüft.

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. Bei **Nur Prüfung des Ethernet-Links** wird nur der Verbindungsstatus der Ethernet-Verbindung geprüft. 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.

Redundanz >> Firewall-Redundanz >> Konnektivitätsprüfung		
	Ergebnis der Konnektivitätsprüfung des externen Interface	Zeigt an, ob die Konnektivitätsprüfung erfolgreich war (grüner Haken).
	Status der Konnektivitätsprüfung des externen Interface	Zeigt den Status der Konnektivitätsprüfung an.
Primäre externe Ziele (für ICMP Echo-Anfragen) (Nicht bei Auswahl **Nur Prüfung des Ethernet-Links**.)	**IP**	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 externe Ziele (für ICMP Echo-Anfragen) (Nicht bei Auswahl **Nur Prüfung des Ethernet-Links**.)	**IP**	(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. Bei **Nur Prüfung des Ethernet-Links** wird nur der Verbindungsstatus der Ethernet-Verbindung geprüft. Eine Prüfung des Ethernet-Links ist bei Geräten mit internem Switch nicht möglich. 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.
	Ergebnis der Konnektivitätsprüfung des internen Interface	Zeigt an, ob die Konnektivitätsprüfung erfolgreich war (grüner Haken).

Redundanz >> Firewall-Redundanz >> Konnektivitätsprüfung		
	Status der Konnektivitätsprüfung des internen Interface	Zeigt den Status der Konnektivitätsprüfung an.
Primäre interne Ziele (für ICMP Echo-Anfragen) (Nicht bei Auswahl **Nur Prüfung des Ethernet-Links**.)		(Siehe oben) Voreingestellt: 192.168.1.30, für neue Adressen 192.168.1.31
Sekundäre interne Ziele (für ICMP Echo-Anfragen) (Nicht bei Auswahl **Nur Prüfung des Ethernet-Links**.)		(Siehe oben) Voreingestellt: 192.168.1.30, für neue Adressen 192.168.1.31

10.2 Ring-/Netzkopplung

10.2.1 Ring-/Netzkopplung

Redundanz >> Firewall-Redundanz >> Ring-/Netzkopplung		
Settings	**Aktiviere Ring-/Netzkopplung/Dual Homing**	Bei Aktivierung wird im Stealth-Modus der Status der Ethernetverbindung von einem 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.

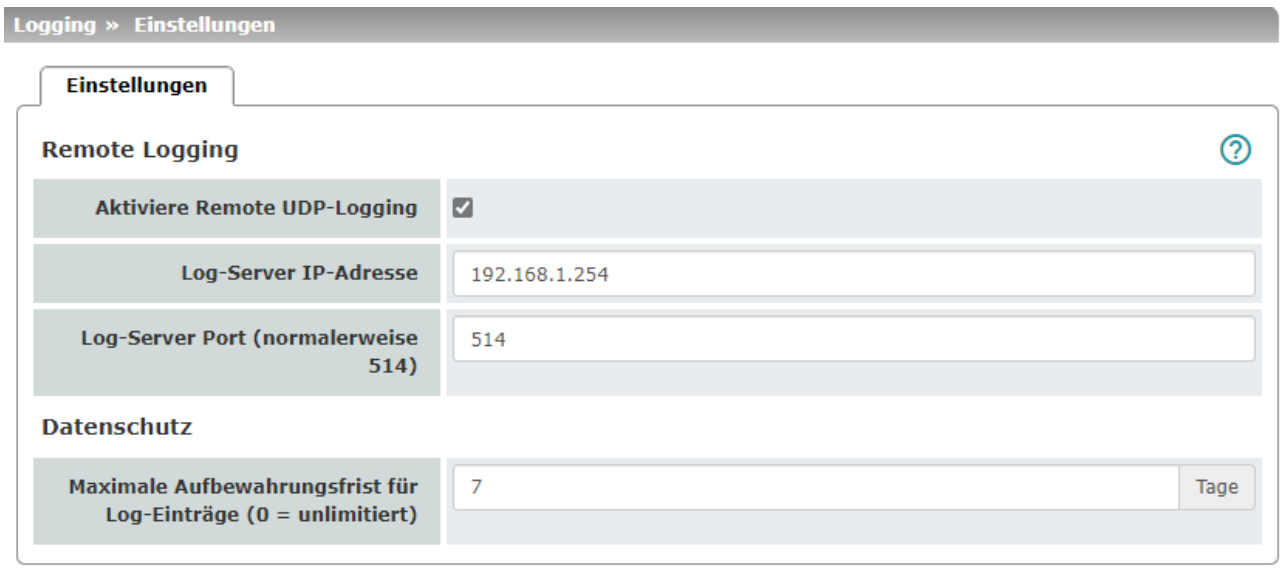
11 Menü Logging

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 338).

11.1 Logging >> Einstellungen

11.1.1 Einstellungen



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.

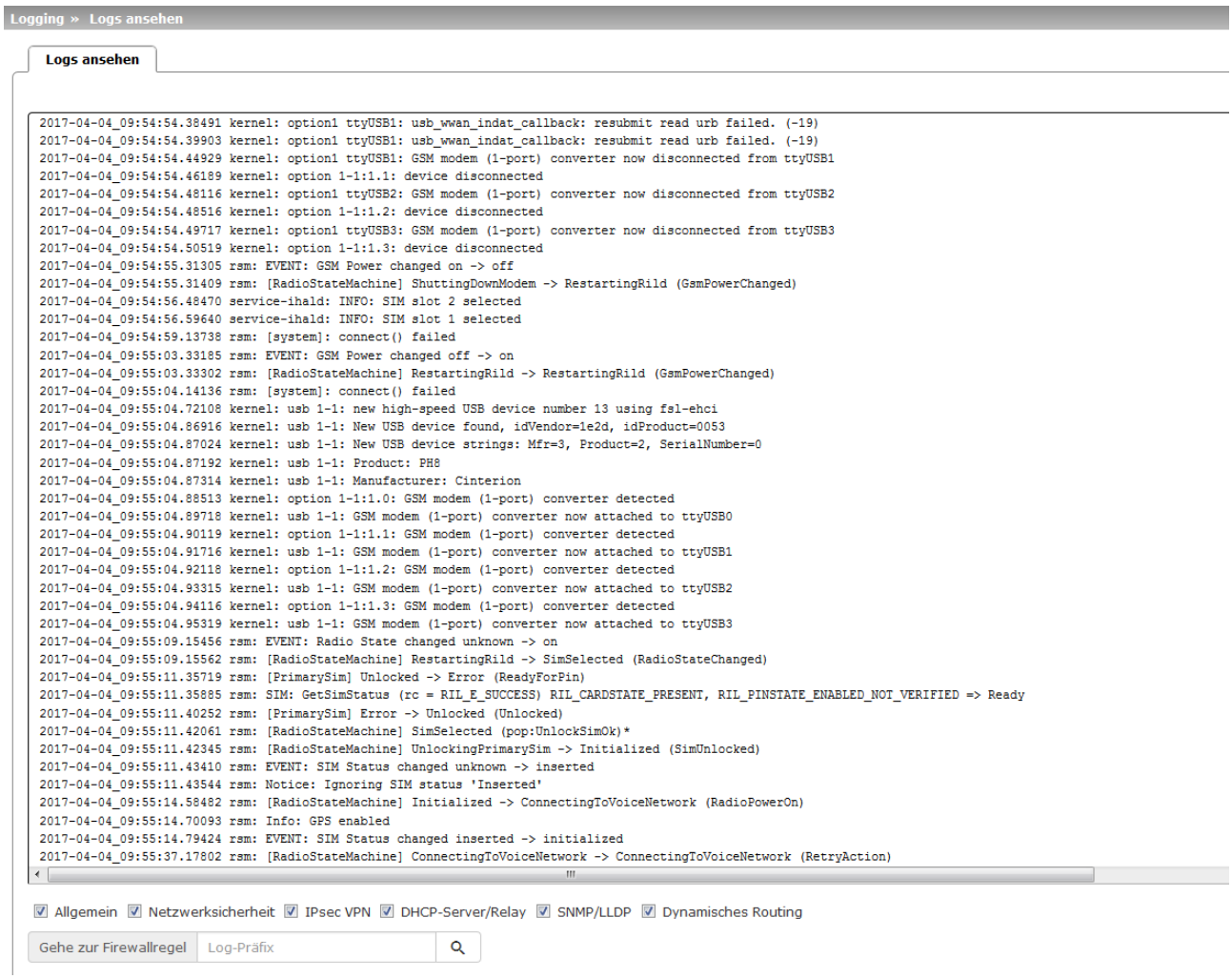
Um das zu verhindern, ist es möglich, die Log-Einträge auf einen externen Rechner (Remote-Server) zu übertragen. Das liegt auch dann nahe, sollte eine zentrale Verwaltung der Protokollierungen mehrerer mGuards erfolgen.

Logging >> Einstellungen	
Remote Logging	Über die Funktion Remote Logging können die Log-Einträge zu einem externen Log-Server (Syslog-Server) übertragen werden. Um auf dem externen Log-Server zu prüfen, ob regelmäßig Log-Einträge übertragen werden, wird ca. alle 30 Minuten ein Log-Eintrag „UPTIME“ erstellt und an den Syslog-Server gesendet. Der Log-Eintrag zeigt die jeweils aktuelle Uptime des mGuard-Gerätes. Beispiel: 2024-12-25_08:20:00.90770 uptime-audit: -------- UPTIME: 29 min --------

Logging >> Einstellungen [...]		
	Aktiviere Remote UDP-Logging	Sollen alle Log-Einträge zum externen (unten angegebenen) Log-Server übertragen werden, aktivieren Sie die Funktion.
	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	Geben Sie den Port des Log-Servers an, zu dem die Log-Einträge per UDP übertragen werden sollen. Standard: 514 .
		Wenn Log-Meldungen über einen VPN-Tunnel auf einen Remote-Server übertragen werden sollen, dann muss sich die IP-Adresse des Remote-Servers in dem Netzwerk befinden, das in der Definition der VPN-Verbindung als Gegenstellen-Netzwerk angegeben ist. Und die interne IP-Adresse muss sich in dem Netzwerk befinden, das in der Definition der VPN-Verbindung als **Lokal** angegeben ist (siehe „IPsec VPN >> Verbindungen >> Editieren >> Allgemein“).
		– Wenn dabei die Option „IPsec VPN >> Verbindungen >> Editieren >> Allgemein“, **Lokal** auf **1:1-NAT** gestellt (siehe Seite 277), gilt Folgendes: Die interne IP-Adresse muss sich in dem angegebenen lokalen Netzwerk befinden. – Wenn dabei die Option „IPsec VPN >> Verbindungen >> Editieren >> Allgemein“, Gegenstelle auf **1:1-NAT** gestellt (siehe Seite 278), gilt Folgendes: Die IP-Adresse des Remote-Log-Servers muss sich in dem Netzwerk befinden, das in der Definition der VPN-Verbindung als **Gegenstelle** angegeben ist.
Datenschutz	Log-Einträge können personenbezogene Daten beinhalten. Um grundsätzliche Anforderungen an den Datenschutz zu beachten, ist es möglich, Log-Einträge nur für einen begrenzten Zeitraum auf dem Gerät zu speichern. Nach Ablauf einer konfigurierbaren Speicherfrist werden Log-Einträge auf dem Gerät automatisch gelöscht. Log-Einträge, die zusätzlich auf einen externen Log-Server (Syslog-Server) übertragen werden, werden nach Ablauf der Speicherfrist nur lokal auf dem Gerät gelöscht. Die datenschutzkonforme Aufbewahrung der übertragenen Log-Einträge muss daher zusätzlich auf dem externen Log-Server sichergestellt werden.	

Logging >> Einstellungen [...]		
	Maximale Aufbewahrungsfrist für Log-Einträge (0 = unlimitiert)	**Standard: 0 (kein Limit)** Gibt an, nach wie vielen Tagen ein lokal gespeicherter Log-Eintrag auf dem Gerät **spätestens** gelöscht wird. Der Wert 0 (Werkseinstellung) bedeutet, dass keine maximale Aufbewahrungsfrist für die Löschung von Log-Einträgen besteht. Beachten Sie, dass aus technischen Gründen Log-Einträge bereits vor Ablauf der eingetragenen Speicherfrist gelöscht werden können. Generell gilt: Ist der maximal verfügbare Speicherplatz für die Protokollierungen auf dem Gerät erschöpft, werden automatisch die ältesten Log-Einträge durch neue überschrieben. Wird das Gerät neu gestartet, werden alle Log-Einträge gelöscht. Log-Einträge, die auf einen externen Log-Server (Remote-Logging) übertragen werden, müssen separat gelöscht werden. Maximale Aufbewahrungsfrist: 365 Tage

11.2 Logging >> Logs ansehen



mGuard-Geräte verfügen je nach Modell über unterschiedliche Funktionen. Entsprechend der jeweils verfügbaren Funktionen können die Log-Einträge nach Kategorien gefiltert werden, sodass nur die gewünschten Log-Einträge im WBM sichtbar sind.

Damit eine oder mehrerer Kategorien angezeigt werden, aktivieren Sie das/die Kontrollkästchen der gewünschten Kategorie(n). Die Log-Einträge werden entsprechend der Auswahl fortlaufend aktualisiert.

Um die fortlaufende Aktualisierung der Log-Einträge zu unterbrechen bzw. fortzusetzen, klicken Sie auf die Schaltfläche ⏸ **Pause** bzw. ▶ **Weiter**.

Zugriff auf Log-Einträge

Der Zugriff auf die Log-Einträge kann auf unterschiedlichen Wegen erfolgen.

Tabelle 11-1 Log-Einträge einsehen

mGuard	UDP	Web-Oberfläche (Web UI)
/var/log/dhclient	Nein	Allgemein
/var/log/dhcp-ext	Nein	DHCP Server/Relay
/var/log/dhcp-int	Nein	DHCP Server/Relay
/var/log/dhcp-dmz	Nein	DHCP Server/Relay
/var/log/dnscache	Nein	Nein
/var/log/dynrouting	socklog	Dynamisches Routing
/var/log/firestarter	svlogd	IPsec VPN
/var/log/firewall	svlogd	Netzwerksicherheit
/var/log/fwrulesetd	socklog	Netzwerksicherheit
/var/log/https	Nein	Nein
/var/log/ipsec	socklog	IPsec VPN
/var/log/l2tp	Nein	IPsec VPN
/var/log/lldpd	Nein	SNMP/LLDP
/var/log/maid	Nein	Allgemein
/var/log/main	socklog	Allgemein
/var/log/maitrigger	Nein	Nein
/var/log/openvpn	socklog	OpenVPN Client
/var/log/pluto	svlogd	IPsec VPN
/var/log/psm-sanitize	Nein	Allgemein
/var/log/pullconfig	socklog	Allgemein
/var/log/redundancy	socklog	Allgemein
/var/log/snmp	Nein	SNMP/LLDP
/var/log/tinydns	Nein	Allgemein
/var/log/userfwd	socklog	Netzwerksicherheit

11.2.1 Kategorien der Log-Einträge

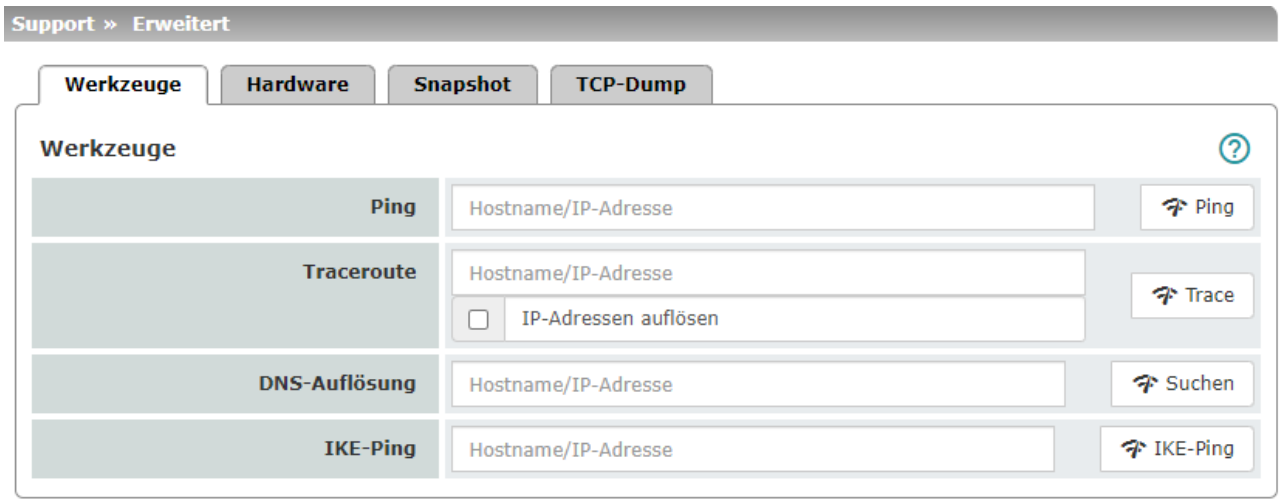
Logging >> Logs ansehen >> Kategorien	
Allgemein	Log-Einträge, die den anderen Kategorien nicht zugeordnet werden können. Beispiele (ohne Zeitstempel): **HTTPS (Login/Logout)** – Webinterface: Failed login for '*******' role '*******' from 192.168.1.55 by Web – Webinterface: Accepted login for 'user1' role 'admin' from 192.168.1.55 by Web – Webinterface: Logout for 'user1' role 'admin' from 192.168.1.55 by timeout **SSH (Login)** – sshd[28296]: Accepted password for admin from 192.168.1.55 port 49248 ssh2 – inno-sshlimitd: accepting new connection at fd 6 – inno-sshlimitd: allow session 1 of maximum 4 for role admin (class 1) at fd 6 – ssh[28472]: session start for user 'admin' **Aktion** – maid[12138]: User 'user1' performed a configuration change with role 'admin': maid[12138]: NTP_ENABLE set to 'no'
Netzwerksicherheit / Firewall	Ist bei Festlegung von Firewall-Regeln das Protokollieren von Ereignissen festgelegt (Log = aktiviert), 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-ID 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: ***fw-vpn-in*** bzw. ***fw-vpn-out***

Logging >> Logs ansehen >> Kategorien	
	– Firewall-Regeln bei OpenVPN-Verbindungen: Menü „OpenVPN-Client >> Verbindungen >> Editieren >> Firewall“, eingehend / ausgehend Log-ID: ***fw-openvpn-in*** bzw. ***fw-openvpn-out*** Menü „OpenVPN-Client >> Verbindungen >> Editieren >> NAT“ Log-ID: ***fw-openvpn-portfw*** – 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 bei Zugriff auf den mGuard über NTP: Menü Verwaltung >> Systemeinstellung >> „Zeit und Datum“ Log-ID: ***fw-ntp-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***
	Suche nach Firewall-Regel auf Grundlage eines Netzwerksicherheits-Logs Firewall-Log-Einträge sind in der Liste blau markiert und mit einem Hyperlink hinterlegt. Ein Klick auf den Firewall-Log-Eintrag, z. B. *fw-https-access-1-1ec2c133-dca1-1231-bfa5-000cbe01010a* öffnet die Konfigurationsseite (Menü >> Untermenü >> Registerkarte) mit der Firewall-Regel, die den Log-Eintrag verursacht hat.
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.
OpenVPN	Listet alle OpenVPN-Ereignisse auf.
DHCP-Server/Relay	Meldungen der unter „Netzwerk >> DHCP“ konfigurierbaren Dienste.
SNMP/LLDP	Meldungen der unter „Verwaltung >> SNMP“ konfigurierbaren Dienste.
Dynamisches Routing	Listet alle Ereignisse auf, die durch dynamisches Routing erzeugt werden.

12 Menü Support

12.1 Support >> Erweitert

12.1.1 Werkzeuge

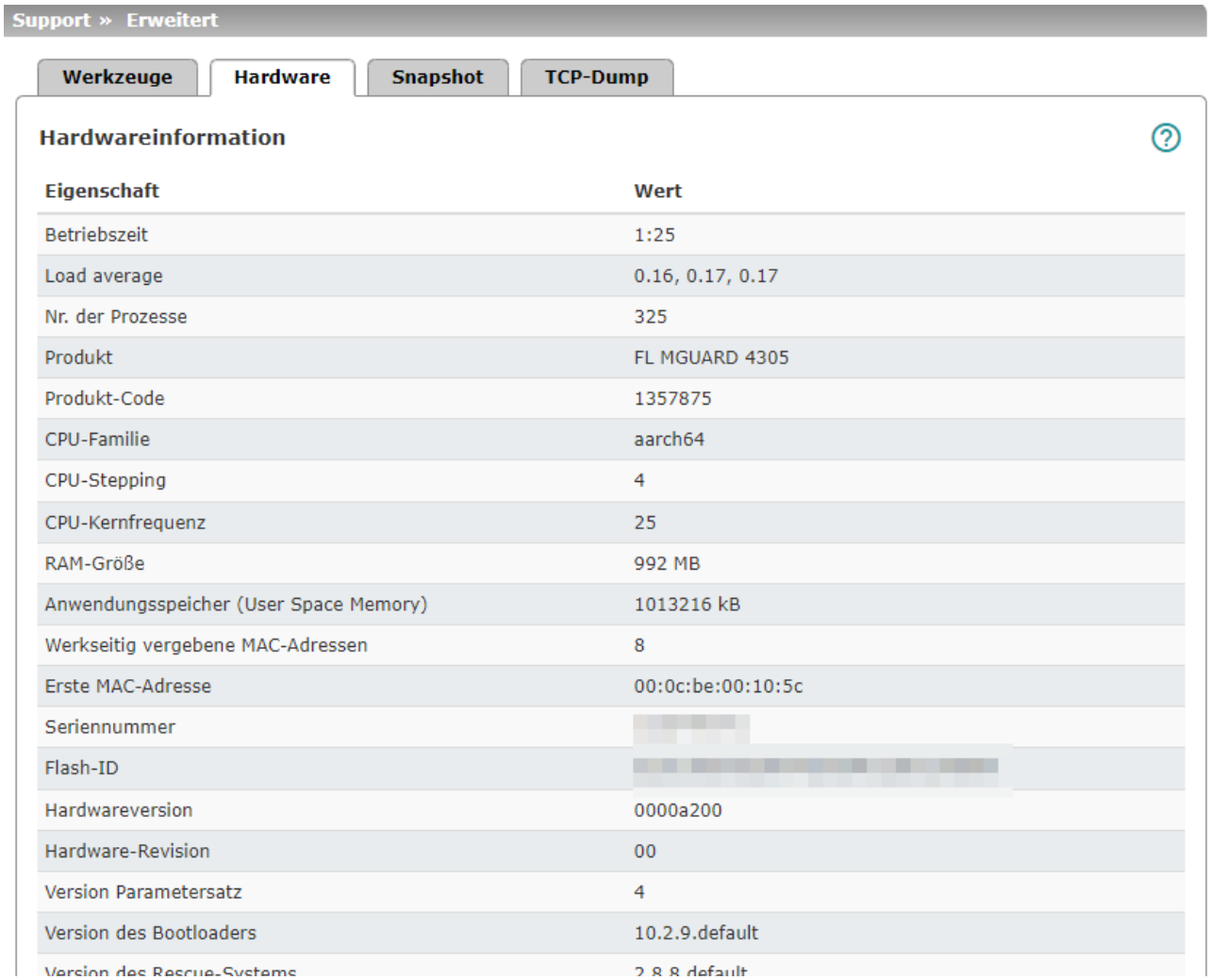


Support >> Erweitert >> Werkzeuge	
Ping	**Ziel**: Sie wollen überprüfen, ob eine Gegenstelle über ein Netzwerk erreichbar ist. **Vorgehen**: • In das Feld **Hostname/IP-Adresse** die IP-Adresse oder den Hostnamen der Gegenstelle eingeben. Dann auf die Schaltfläche **Ping** klicken. Sie erhalten daraufhin eine entsprechende Meldung.
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 **IP-Adressen nicht in Hostnamen auflösen** (= Häkchen setzen). • Dann auf die Schaltfläche **Trace** klicken. Sie erhalten daraufhin eine entsprechende Meldung.
DNS-Auflösung	**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 **Suchen** klicken. Sie erhalten daraufhin die Antwort, wie sie der mGuard aufgrund seiner DNS-Konfiguration ermittelt.

Support >> Erweitert >> Werkzeuge	
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 **IKE-Ping** klicken. • Sie erhalten eine entsprechende Meldung.

12.1.2 Hardware

Diese Seite listet verschiedene Hardware-Eigenschaften des mGuards auf.



MAC-Adressen

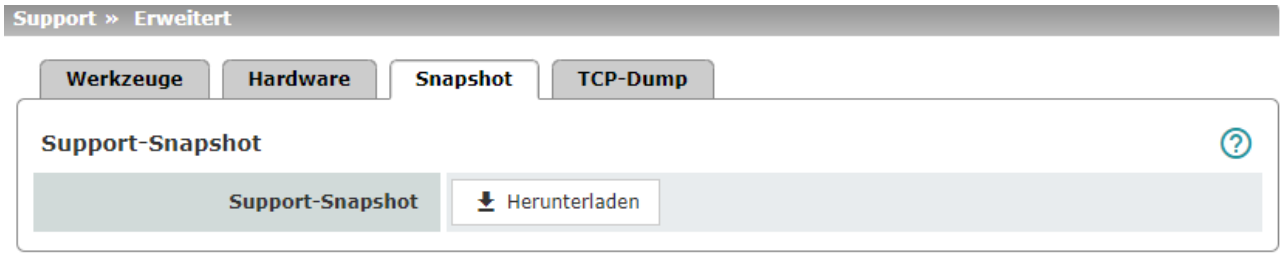
Die vom Hersteller festgelegte MAC-Adresse des WAN-Interface ist auf dem Typenschild des Geräts angegeben. Die weiteren MAC-Adressen (LAN/DMZ [optional]) lassen sich wie folgt berechnen:

- **WAN-Interface:** siehe Typenschild.
- **LAN-Interface:** Die MAC-Adresse des WAN-Interface um 1 erhöht (**WAN + 1**). Geräte mit integriertem Switch: Alle Switch-Ports verwenden die gleiche MAC-Adresse.
- **DMZ-Interface:** Die MAC-Adresse des WAN-Interface um 4 erhöht (**WAN + 4**).

Beispiel:

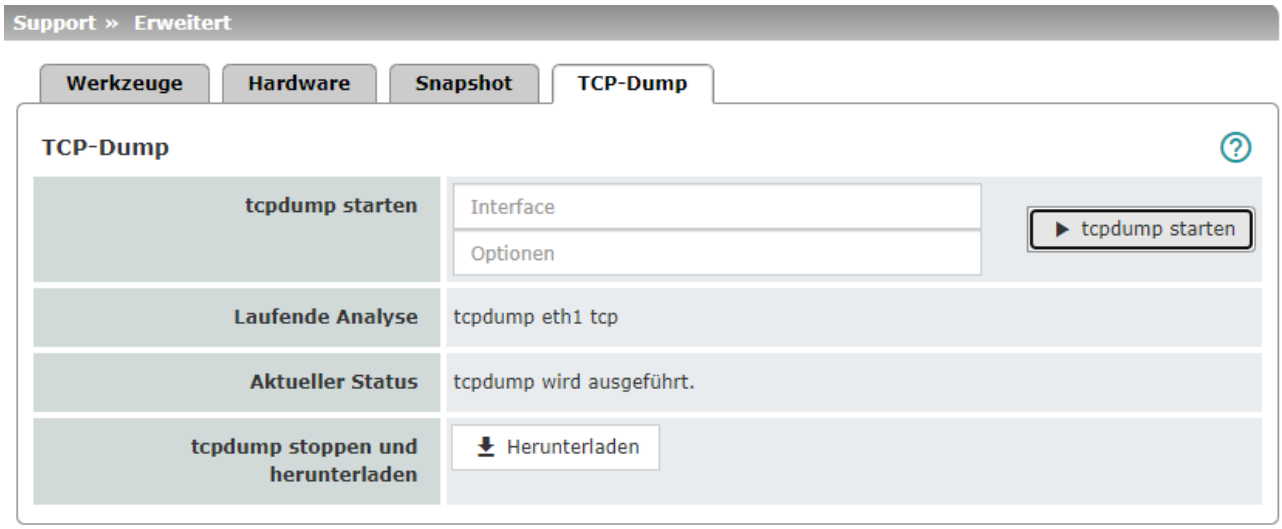
- WAN: 00:a0:45:eb:28:9d
- LAN: 00:a0:45:eb:28:9e
- DMZ: 00:a0:45:eb:28:a1

12.1.3 Snapshot



Support >> Erweitert >> Snapshot		
Support-Snapshot	**Support-Snapshot**	Erstellt eine komprimierte Datei (im tar.gz-Format), in der alle aktuellen Konfigurations-Einstellungen 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 **Support-Snapshot** oder einen **Support-Snapshot mit persistenten Logs** zu erstellen, gehen Sie wie folgt vor: • Die Schaltfläche **Herunterladen** klicken. • Die Datei speichern (unter dem Namen **snapshot-YYYY.MM.DD-hh.mm.ss.tar.gz** bzw. **snapshot-all-YYYY.MM.DD-hh.mm.ss.tar.gz**) Stellen Sie die Datei dem Support Ihres Anbieters zur Verfügung, wenn dies erforderlich ist.

12.1.4 TCP-Dump



Support >> Erweitert >> TCP-Dump

TCP-Dump

Mithilfe einer Paketanalyse (*tcpdump*) kann der Inhalt von Netzwerkpaketen analysiert werden, die über ein ausgewähltes Netzwerk-Interface gesendet oder empfangen werden. Welche Netzwerkpakete analysiert werden, wird über Filteroptionen bestimmt.

Das Ergebnis der Analyse wird in einer Datei (**.tar.gz*) gespeichert, heruntergeladen und auf dem Gerät gelöscht.

Wenn die Datei (**.tar.gz*) eine Größe von 50 MB überschreitet, wird der Prozess *tcpdump* automatisch gestoppt. Die Datei wird auf dem Gerät gespeichert und kann anschließend heruntergeladen werden. Nachdem die Datei heruntergeladen wurde, wird sie auf dem Gerät gelöscht.

tcpdump starten

Interface

Nur Datenpakete, die über das ausgewählte Netzwerk-Interface gesendet oder empfangen werden, werden analysiert.

- WAN-Interface (XF1):
  - **eth0**
- LAN-Interface (XF2–4 bzw. 2–5):
  - **eth1** (nur Netzwerk-Modus *Router*)
  - **br0** (nur Netzwerk-Modus *Stealth*)
  - **swp0** (nur FL MGUARD 2105/4305)
  - **swp1** (nur FL MGUARD 2105/4305)
  - **swp2** (nur FL MGUARD 2105/4305)
  - **swp3** (nur FL MGUARD 2105)
- DMZ-Interface (XF5):
  - **dmz0** (nur FL MGUARD 4305)

Support >> Erweitert >> TCP-Dump

	Optionen Durch die Angabe von Optionen kann die Paketanalyse auf eine Auswahl der unten stehenden Elemente beschränkt werden. Optionen können über die logischen Verknüpfungen „and, or, not“ verknüpft werden. Beispiel: *tcp and net 192.168.1.0/24 and not port 443* Zur Verfügung stehende Optionen: – **tcp**: TCP-Protokoll – **udp**: UDP-Protokoll – **arp**: ARP-Protokoll – **icmp**: ICMP-Protokoll – **esp**: ESP-Protokoll – **host <ip>**: IPv4-Adresse – **port <1-65535>**:Netzwerkport (Portnummer oder Servicename) – **net <nw_cidr>**: Netzwerk (in CIDR-Schreibweise, z. B. 192.168.1.0/24) – **and, or, not**: Logische Verknüpfungen **Schaltfläche „tcpdump starten“** • Klicken Sie auf die Schaltfläche „**tcpdump starten**“, um eine Analyse zu starten.
Laufende Analyse	Zeigt während einer laufenden Analyse, für welches Interface und mit welchen Optionen *tcpdump* ausgeführt wird.
Aktueller Status	Zeigt den Status der Analyse.
tcpdump stoppen und herunterladen	**Schaltfläche „Herunterladen“** • Klicken Sie auf die Schaltfläche **Herunterladen**, – um eine laufende Analyse zu stoppen und die Daten herunterzuladen oder – um Daten herunterzuladen, die nach einer automatisch gestoppten Analyse auf dem Gerät gespeichert wurden. Die erfassten Paketinhalte werden in einer Datei (**.tar.gz*) zusammengefasst und automatisch vom Gerät heruntergeladen. Anschließend wird die Datei auf dem Gerät gelöscht. Der Zeitpunkt des Herunterladens der Datei wird im Dateinamen wie folgt angegeben: <YYYY.MM.DD-hh.mm.ss> Beispiel: *tcpdump-2024.06.10-09.47.54.tar.gz*

13 Redundanz

Die Funktionen der Firewall-Redundanz stehen **nicht** auf den Geräten der FL MGUARD 2000-Serie zur Verfügung.

Bei jedem Gerät eines Redundanzpaares wird kontinuierlich geprüft, ob auf der internen und externen Netzwerk-Schnittstelle jeweils eine Verbindung besteht, über die Netzwerkpakete weitergeleitet werden können.
Da die Redundanzfunktion auf der DMZ-Schnittstelle nicht anwendbar ist, werden Netzwerkverbindungen über eine vorhandene DMZ-Schnittstelle nicht geprüft.

Es gibt verschiedene Möglichkeiten mit dem mGuard Fehler so zu kompensieren, dass eine bestehende Verbindung nicht unterbrochen wird.

- **Firewall-Redundanz:** Sie können zwei baugleiche mGuard-Geräte zu einem Redundanzpaar zusammenzufassen, bei dem im Fehlerfall der eine die Funktion des anderen übernimmt.
- **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.

13.1 Firewall-Redundanz

Mit Hilfe der Firewall-Redundanz ist es möglich, zwei baugleiche mGuard-Geräte zu einem Redundanzpaar (einem virtuellen Router) zusammenzufassen. Dabei übernimmt ein mGuard-Gerät in einem Fehlerfall die Funktion des anderen. Beide Geräte laufen synchron, sodass bei einem Wechsel die bestehende Verbindung nicht unterbrochen wird.

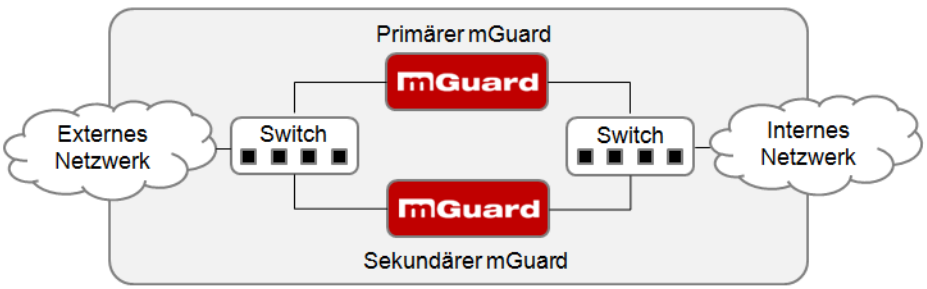


Bild 13-1 Firewall-Redundanz (Beispiel)

Grundbedingungen für die Firewall-Redundanz

- Nur baugleiche mGuard-Geräte können ein Redundanzpaar bilden.
- Im Netzwerk-Modus „Router“ wird die Firewall-Redundanz nur mit dem Router-Modus „Statisch“ unterstützt.
- Im Netzwerk-Modus „Stealth“ wird die Firewall Redundanz nur in der Stealth-Konfiguration „Mehrere Clients“, unterstützt.
- Weitere Einschränkungen siehe „Voraussetzungen für die Firewall-Redundanz“ auf Seite 352 und „Grenzen der Firewall-Redundanz“ auf Seite 361.

13.1.1 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 Gerät eines Redundanzpaares wird kontinuierlich geprüft, ob auf der internen und externen Netzwerk-Schnittstelle jeweils eine Verbindung besteht, über die Netzwerkpakete weitergeleitet werden können.

Da die Redundanzfunktion auf der DMZ-Schnittstelle nicht anwendbar ist, werden Netzwerkverbindungen über eine vorhandene DMZ-Schnittstelle nicht geprüft.

Jedes mGuard-Gerät 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 Gerät eines Redundanzpaares wird außerdem kontinuierlich geprüft, ob ein aktives mGuard-Gerät vorhanden ist und ob dieses aktiv bleiben soll. Dafür wird eine Variante des CARP (*Common Address Redundancy Protocol*) verwendet.

Das aktive mGuard-Gerät sendet ständig Anwesenheitsnachrichten über sein internes und externes Netzwerk-Interface, während beide Geräte 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-Gerät in einer bestimmten Zeit keine Anwesenheitsnachricht erhält. Außerdem wird die Prüfung nicht bestanden, wenn ein Gerät 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

Das mGuard-Gerät, das sich im Zustand der Bereitschaft befindet, erhält eine Kopie des Zustandes des aktuell aktiven mGuard-Geräts.

Dazu gehört eine Datenbank mit den weitergeleiteten Netzwerkverbindungen. Diese Datenbank wird laufend durch die weitergeleiteten Netzwerkpakete aufgebaut und erneuert. Die unverschlüsselten Zustandsdaten werden über die physikalische LAN-Schnittstelle übertragen und niemals über das virtuelle Netzwerk-Interface gesendet.

ACHTUNG: Unverschlüsselte Datenübertragung

Die Verbindungsdaten aus den Firewall-Tabellen des Redundanzpaares werden unverschlüsselt über das LAN-Netzwerk übertragen.

Verwenden Sie die Redundanzfunktion nur in einer sicheren Netzwerkumgebung, in der das LAN-Netzwerk vollständig unter der Kontrolle des Betreibers steht.

Um den internen Datenverkehr gering zu halten, kann ein VLAN so konfiguriert werden, dass es die Abgleichsdaten in eine separate Multicast- und Broadcast-Domain verlagert.

Virtuelle IP-Adressen

Jedes mGuard-Gerät wird mit virtuellen IP-Adressen konfiguriert. Deren Anzahl hängt von dem verwendeten Netzwerk-Modus ab. Bei einem Redundanzpaar müssen Sie beiden mGuard-Geräten die gleichen virtuellen IP-Adressen zuweisen. Die virtuellen IP-Adressen werden vom Gerät 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 Geräte 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 Geräte eine Weiterleitung von speziellen UDP/TCP-Ports von einer virtuellen IP-Adresse zu anderen IP-Adressen, sofern letztere vom Gerät erreicht werden können. Zusätzlich maskiert das mGuard-Gerät Daten mit virtuellen IP-Adressen, wenn Masquerading-Regeln eingerichtet sind.

Statusüberwachung

Die Statusüberwachung entscheidet darüber, ob das Gerät im Zustand „aktiv“, in „Bereitschaft“ oder im „Fehlerzustand“ ist. Jedes mGuard-Gerät entscheidet autonom über seinen Zustand, basierend auf den Informationen, die von anderen Komponenten bereitgestellt werden. Die Statusüberwachung sorgt dafür, dass nicht zwei Geräte 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.

13.1.2 Zusammenarbeit der Firewall-Redundanz-Komponenten

Während des Betriebes interagieren die Komponenten folgendermaßen: Beide mGuard-Geräte führen fortlaufend für ihre beiden Netzwerk-Schnittstellen (internes und externes Interface) eine Konnektivitätsprüfung durch. Außerdem wird fortlaufend eine Verfügbarkeitsprüfung gemacht. Dazu lauscht jedes Gerät kontinuierlich auf Anwesenheitsnachrichten (CARP) und das aktive Gerät sendet diese zusätzlich.

Auf Grundlage der Informationen aus der Konnektivitäts- und - Verfügbarkeitsprüfung weiß die Statusüberwachung, in welchem Zustand sich die mGuard-Geräte befinden. Die Statusüberwachung sorgt dafür, dass das aktive Gerät seine Daten auf das andere Gerät spiegelt (Zustandsabgleich).

13.1.3 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 Phoenix Contact auf.

13.1.4 Voraussetzungen für die Firewall-Redundanz

- Um die Redundanz-Funktion zu nutzen, muss auf beiden **mGuard**-Geräten die gleiche Firmwareversion installiert sein.
- Jeder Satz von Zielen für die Konnektivitätsprüfung kann nicht mehr als zehn Ziele beinhalten. (Ohne eine Obergrenze kann eine Failover-Zeit nicht garantiert werden.)
  „Redundanz >> Firewall-Redundanz >> Redundanz“
  - >> *„Externes Interface“* >> *„Primäre externe Ziele (für ICMP Echo-Anfragen)“*
  - >> *„Externes Interface“* >> *„Sekundäre externe Ziele (für ICMP Echo-Anfragen)“*
  - >> *„Internes Interface“* >> *„Primäre externe Ziele (für ICMP Echo-Anfragen)“*
  - >> *„Internes Interface“* >> *„Sekundäre externe 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 externe 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.

13.1.5 Umschaltzeit im Fehlerfall

Von der Variablen **Umschaltzeit im Fehlerfall** errechnet das mGuard-Gerät automatisch die Zeitabstände für die Konnektivitäts- und Verfügbarkeitsprüfung.

Konnektivitätsprüfung

In der Tabelle 13-1 werden die Faktoren angegeben, die die Zeitabstände für die Konnektivitätsprüfung bestimmen.

Für die Konnektivitätsprüfung werden ICMP-Echo-Requests verschickt, die 64 Byte 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 ICMP-Echo-Reply hat die gleiche Größe.

In Tabelle 13-1 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 Gerät 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 tatsächliche Latenzzeit kann unter ungünstigen Umständen (Fehler der Konnektivitätsprüfung) den doppelten Wert der konfigurierten Latenzzeit annehmen.
– 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 13-1 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 Tabelle 13-1 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 ICMP-Echo-Reply hat die gleiche Größe.

Tabelle 13-2 zeigt die maximale Frequenz, mit der Anwesenheitsnachrichten (CARP) vom aktiven mGuard-Gerät gesendet werden. Sie zeigt außerdem die Bandbreite, die dabei verbraucht wird. Die Frequenz hängt von der Priorität des Geräts und der *„Umschaltzeit im Fehlerfall“* ab.

Tabelle 13-2 zeigt außerdem die maximale Latenzzeit, die das Gerät für das Netzwerk toleriert, das die Anwesenheitsnachrichten (CARP) überträgt. Wenn diese Latenzzeit überschritten wird, kann das Redundanzpaar ein undefiniertes Verhalten zeigen.

Tabelle 13-2 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	37600 Bit/s
3 s	16,6 pro Sekunde	8,3 pro Sekunde	60 ms	12533 Bit/s
10 s	5 pro Sekunde	2,5 pro Sekunde	200 ms	3760 Bit/s

13.1.6 Fehlerkompensation durch die Firewall-Redundanz

Die Firewall-Redundanz dient dazu, den Ausfall von Hardware auszugleichen.

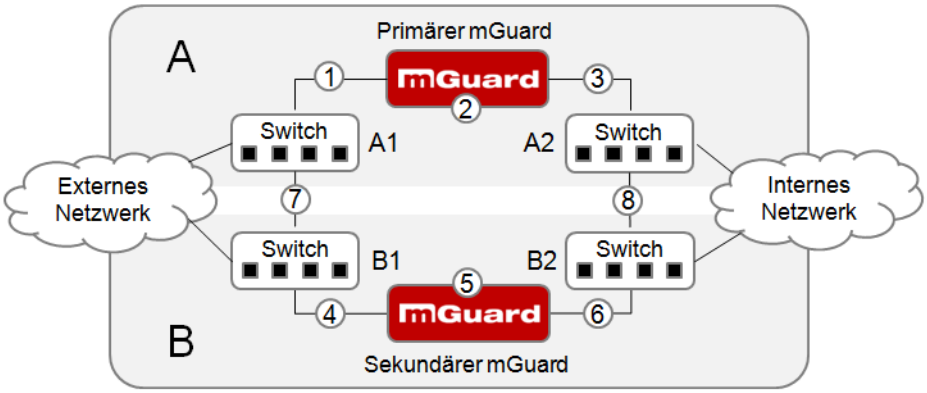


Bild 13-2 Mögliche Fehlerorte (1 ... 8)

In Bild 13-2 wird ein Aufbau gezeigt, der verschiedene Fehlerorte zeigt (unabhängig vom Netzwerk-Modus).

Jeder der beiden Geräte 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 mGuard-Geräte 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 13-2 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 13-2).

13.1.7 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 „Erweitert“ auf Seite 230), 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

13.1.8 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 Remote-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 331). 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 353 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.

13.1.9 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 DHCP-Server,
  - ein DHCP-Relay,
  - eine Benutzer-Firewall und
- 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)
- Nach einer **Netzwerk-Lobotomie** sind möglicherweise einige Netzwerkverbindungen unterbrochen. (Siehe „Wiederherstellung bei einer Netzwerk-Lobotomie“ auf Seite 356).
- Nach einem Failover können **semi-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 356 und „Failover beim Aufbau von semi-unidirektionalen Verbindungen“ auf Seite 356.)
- 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.

14 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 370). Andererseits sind Konzepte möglich, die die aufwendige Administrierbarkeit von symmetrischen Schlüsseln vermeiden.

DES / 3DES

Die Verschlüsselungsalgorithmen **DES** und **3DES** gelten als nicht mehr sicher und sollten nach Möglichkeit nicht mehr verwendet werden. Als Alternative wird die Verwendung des Verschlüsselungsalgorithmus **AES** empfohlen.

Aus Gründen der Abwärtskompatibilität können die Verschlüsselungsalgorithmen DES und 3DES weiter genutzt werden. Für mehr Informationen siehe „Verwendung sicherer Verschlüsselungs- und Hash-Algorithmen“ auf Seite 35.

Der von IBM stammende und von der NSA überprüfte symmetrische Verschlüsselungsalgorithmus (→ „Symmetrische Verschlüsselung“ auf Seite 370) 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 369) 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 selbstsigniert. 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. Das heißt, 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 möglichen 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 bezeichnet 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.

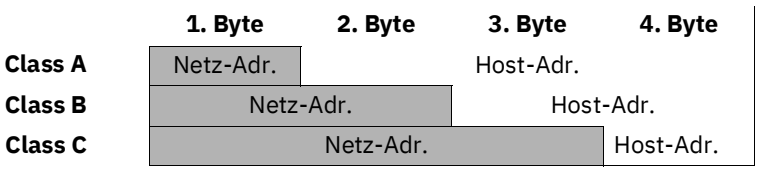
IP-Adresse

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. 128.111.10.21. 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 364) 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 369).

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=Phoenix Contact,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 14-1 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: OU=Entwicklung
O	Organization	Gibt die Organisation bzw. die Firma an. Beispiel: O=Phoenix Contact
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 Port-Nummer zugeordnet. Über sie ist es möglich zwischen zwei Rechnern mehrere UDP oder TCP Verbindungen zu unterscheiden und somit gleichzeitig zu nutzen.

Bestimmte Port-Nummern 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 Ausstel-

lers 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 E-Mail 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 364)

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.

15 Anhang

15.1 CGI-Interface

Die zusätzlichen HTTPS-Schnittstellen *nph-vpn.cgi, nph-diag.cgi, nph-status.cgi* und *nph-action.cgi* sind als CGI-Skripte (**C**ommon **G**ateway **I**nterface) implementiert.

Für weitergehende Informationen zur Verwendung der CGI-Interfaces siehe *mGuard-Anwenderhilfen* (UM DE MGUARD APPNOTES), erhältlich unter phoenixcontact.com/products oder help.mguard.com.

Beim Ausführen der Skripte *nph-vpn.cgi, nph-diag.cgi, nph-status.cgi* und *nph-action.cgi*, dürfen in Benutzerkennungen, Passwörtern und sonstigen benutzerdefinierten Namen (z. B. der Name einer VPN-Verbindung), ausschließlich folgende Zeichen verwendet werden:

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

Sollen andere Sonderzeichen verwendet werden, z. B. das Leerzeichen oder das Fragezeichen, müssen diese der nachfolgenden Tabelle entsprechend codiert werden (URL encoding).

Die Verwendung des Kommandozeilen-Tools *wget* wird nicht unterstützt. Stattdessen kann das Kommandozeilen-Tool *curl* verwendet werden (Parameter und Optionen abweichend!).

Beispiele:

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

curl --insecure "https://admin:mGuard@192.168.1.1/nph-action.cgi?action=tools%2Ftcpdump-start&interface=eth1"

Die Option ***--insecure*** (*curl*) sorgt dafür, dass das HTTPS-Zertifikat des mGuards nicht weiter geprüft wird.

Tabelle 15-1 Codierung von Sonderzeichen (URL encoding)

(Space)	!	"	#	$	%	&	'	(	)	*	+
%20	%21	%22	%23	%24	%25	%26	%27	%28	%29	%2A	%2B

,	/	:	;	=	?	@	[	\	]	{	|	}
%2C	%2F	%3A	%3B	%3D	%3F	%40	%5B	%5C	%5D	%7B	%7C	%7D

15.2 Kommandozeilen-Tool „mg“

Die folgenden Befehle können durch die Benutzer **root** und **admin** auf der Kommandozeile des mGuards ausgeführt werden.

Tabelle 15-2 Kommandozeilen-Tool „mg“

Befehl	Parameter	Beschreibung
mg update	*patches*	Es wird ein automatisches Online-Update durchgeführt, bei welchem der mGuard das benötigte Package-Set eigenständig ermittelt (siehe „Automatische Updates“ auf Seite 96). **Patch-Releases** beheben Fehler der vorherigen Versionen und haben eine Versionsnummer, welche sich nur in der dritten Stelle ändern.
	minor	**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.
	major	
mg status	*/network/dns-servers*	**Benutzte DNS-Server** Hier wird der Name der DNS-Server angezeigt, die vom mGuard zur Namensauflösung benutzt werden.
	/network/if-state/ext1/gw	**Aktive Standard-Route über** Hier wird die IP-Adresse angezeigt, über die der mGuard versucht, ihm unbekannte Netze zu erreichen.
	/network/if-state/ext1/ip	**Externe IP-Adresse** Die Adressen, unter denen der mGuard von Geräten des externen Netzes aus erreichbar ist. Im Stealth-Modus übernimmt der mGuard die Adresse des lokal angeschlossenen Rechners als seine externe IP.
	/network/if-state/ext1/net-mask	**Netzmaske der externen IP-Adresse.**

15.3 LED-Statusanzeige und Blinkverhalten

15.3.1 Darstellung der Systemzustände

Die Systemzustände (Status-, Alarm- oder Fehlermeldungen), die über das Leucht- bzw. Blinkverhalten der LED-Dioden angezeigt werden, entnehmen Sie bitte Tabelle 15-3.

Weitere Informationen zu Fehler- und Systemzuständen entnehmen Sie bitte den entsprechenden Log-Dateien

Tabelle 15-3 Durch das Leucht- und Blinkverhalten der LEDs dargestellte Systemzustände

PF1 (grün)	PF2 (grün)	PF3 (grün)	PF4 (grün)	PF5 (ERR) (rot)	FAIL (FAULT) (rot)	Beschreibung des Systemzustands
Betriebsbereit						
Herz-schlag						Der Systemstatus ist OK. Die LED PF1 blinkt im Rhythmus „Herzschlag“.
Systemstart						
Herz-schlag				ON (ca. 20 sec)	**ON** (ca. 20 sec)	Das System bootet. Alle LEDs der Ethernet-Ports (LNK/ACT und SPD) leuchten kurz rot/grün. Alle PF-LEDs (PF1–5) leuchten kurz orange. Die LED PF1 blinkt im Rhythmus „Herzschlag“.
Herz-schlag				Blink 500/500	ON	Das Starten des Gerätes ist nach einer Integritätsprüfung des Dateisystems fehlgeschlagen. Das Dateisystem ist beschädigt oder wurde manipuliert. Das Gerät kann nur durch einen Rescue Flash wieder in Betrieb genommen werden.
Herz-schlag	ON (orange) (3 sec)					ECS: Die Konfiguration wurde erfolgreich vom ECS geladen und angewendet.
Update						
				Blink 500/500		Der Austausch des Bootloaders ist aufgrund eines Hardwaredefekts fehlgeschlagen.
				Blink 500/500		Ein anderer schwerer Fehler ist aufgetreten.
Funktions-Überwachung / Alarmausgang						
Herz-schlag					ON	Keine Konnektivität auf der WAN-Schnittstelle (Linküberwachung am Gerät konfigurierbar)
Herz-schlag					ON	Keine Konnektivität auf der LAN-Schnittstelle (Linküberwachung am Gerät konfigurierbar)
Herz-schlag					ON	Spannungsversorgung 1 oder 2 ausgefallen (Alarm am Gerät konfigurierbar)
Herz-schlag					ON	Temperatur zu hoch / zu niedrig (Alarm am Gerät konfigurierbar)

Tabelle 15-3 Durch das Leucht- und Blinkverhalten der LEDs dargestellte Systemzustände

PF1 (grün)	PF2 (grün)	PF3 (grün)	PF4 (grün)	PF5 (ERR) (rot)	FAIL (FAULT) (rot)	Beschreibung des Systemzustands
Herz-schlag					ON	(Redundanz) Verbindungsprüfung fehlgeschlagen (Alarm am Gerät konfigurierbar)
Herz-schlag					ON	Administrator-Passwörter nicht konfiguriert (Alarm am Gerät konfigurierbar)
Kontrollierbare VPN-Verbindungen/Firewall-Regelsätze (über Servicekontakte)						
Herz-schlag		Blink				**Servicekontakt O1:** Die über den Servicekontakt O1 geschaltete VPN-Verbindung wird aufgebaut.
Herz-schlag		ON				**Servicekontakt O1:** Die über den Servicekontakt O1 geschaltete VPN-Verbindung wurde erfolgreich aufgebaut. ODER **Servicekontakt O1:** Der über den Servicekontakt O1 geschaltete Firewall-Regelsatz wurde erfolgreich aktiviert .
Herz-schlag			Blink			**Servicekontakt O2:** Die über den Servicekontakt O2 geschaltete VPN-Verbindung wird aufgebaut.
Herz-schlag			ON			**Servicekontakt O2:** Die über den Servicekontakt O2 geschaltete VPN-Verbindung wurde erfolgreich aufgebaut. ODER **Servicekontakt O2:** Der über den Servicekontakt O2 geschaltete Firewall-Regelsatz wurde erfolgreich aktiviert.
Externer Konfigurationsspeicher (ECS)						
Herz-schlag	ON (orange) (3 sec)					ECS: Die Konfiguration wurde erfolgreich vom ECS geladen und angewendet.
Herz-schlag				ON (3 sec)		ECS: Das ECS ist inkompatibel.
Herz-schlag				ON (3 sec)		ECS: Die Kapazität des ECS ist erschöpft.
Herz-schlag				ON (3 sec)		ECS: Das Root-Passwort aus dem ECS stimmt nicht überein.
Herz-schlag				ON (3 sec)		ECS: Die Konfiguration konnte nicht aus dem ECS geladen werden.
Herz-schlag				ON (3 sec)		ECS: Die Konfiguration konnte nicht im ECS gespeichert werden.
Recovery-Prozedur						
Herz-schlag				ON (2 sec)		RECOVERY: Das Wiederherstellungsverfahren ist fehlgeschlagen.

Tabelle 15-3 Durch das Leucht- und Blinkverhalten der LEDs dargestellte Systemzustände

PF1 (grün)	PF2 (grün)	PF3 (grün)	PF4 (grün)	PF5 (ERR) (rot)	FAIL (FAULT) (rot)	Beschreibung des Systemzustands
ON (2 sec) Herz-schlag						RECOVERY: Das Wiederherstellungsverfahren war erfolgreich.
Flash-Prozedure						
ON					ON	FLASH-PROZEDUR: Die Flash-Prozedur wurde gestartet. Bitte warten.
Running light	Running light	Running light			ON	FLASH-PROZEDUR: Die Flash-Prozedur wird ausgeführt.
Blink 50/800	Blink 50/800	Blink 50/800			ON	FLASH-PROZEDUR: Die Flash-Prozedur war erfolgreich.
				ON		FLASH-PROZEDUR: Die Flash-Prozedur ist fehlgeschlagen.
				Blink 50/100 (5 sec)		FLASH-PROZEDUR WARNUNG: Austausch des Rettungssystems. Schalten Sie das Gerät nicht aus. Wenn das Blinken aufhört, ist der Austausch des Rettungssystems beendet.
				ON		FLASH-PROZEDUR: Die DHCP/BOOTP-Anforderungen sind fehlgeschlagen.
				ON		FLASH-PROZEDUR: Das Einbinden (Mounten) des Datenspeichers (data storage device) ist fehlgeschlagen.
				ON		FLASH-PROZEDUR: Das Löschen der Dateisystem-Partition ist fehlgeschlagen.
				ON		FLASH-PROZEDUR: Das Laden des Firmware-Images ist fehlgeschlagen.
				ON		FLASH-PROZEDUR: Die Signatur des Firmware-Images ist ungültig.
				ON		FLASH-PROZEDUR: Das Installationsskript konnte nicht geladen werden.
				ON		FLASH-PROZEDUR: Die Signatur des Installationsskripts ist ungültig.
				ON		FLASH-PROZEDUR: Das Rollout-Skript ist fehlgeschlagen.

Bitte beachten Sie folgende Hinweise

Allgemeine Nutzungsbedingungen für Technische Dokumentation

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

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

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

Dieses Handbuch ist einschließlich aller darin enthaltenen Abbildungen urheberrechtlich geschützt. Jegliche Veränderung des Inhaltes oder eine auszugsweise Veröffentlichung sind nicht erlaubt.

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

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

So erreichen Sie uns

Internet

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

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

Ländervertretungen

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

Herausgeber

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

Wenn Sie Anregungen und Verbesserungsvorschläge zu Inhalt und Gestaltung unseres Handbuchs haben, würden wir uns freuen, wenn Sie uns Ihre Vorschläge zusenden an:
tecdoc@phoenixcontact.com

Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Phone: +49 5235 3-00
Fax: +49 5235 3-41200
Email: info@phoenixcontact.com
phoenixcontact.com

© Phoenix Contact 2025-01-30

110191_de_09
Item No. –09