Konfigurieren der mGuard Security-Appliances Firmware 8.8

Anwenderhandbuch

PHOENIX CONTACT
INSPIRING INNOVATIONS

Anwenderhandbuch
Konfigurieren der mGuard Security-Appliances (Referenzhandbuch)
Firmware 8.8

2021-08-24

Bezeichnung: UM DE MGUARD 8.8

Revision: 15

Artikel-Nr.: —

Dieses Handbuch ist gültig für das mGuard Software-Release 8.8 bei Verwendung mit den folgenden Geräten der mGuard-Familie (siehe „mGuard Firmware – Version 8.8.x - Release Notes“ für weitere Informationen):

- FL MGUARD RS4000 TX/TX (VPN)
- FL MGUARD RS4000 TX/TX VPN-M
- FL MGUARD RS4000-P
- FL MGUARD RS2000 TX/TX VPN
- FL MGUARD RS2000 TX/TX-B
- FL MGUARD RS4004 TX/DTX (VPN)
- FL MGUARD RS2005 TX VPN
- FL MGUARD CORE TX (VPN)
- TC MGUARD RS4000 3G VPN
- TC MGUARD RS2000 3G VPN
- TC MGUARD RS4000 4G VPN
- TC MGUARD RS2000 4G VPN
- TC MGUARD RS4000 4G VZW VPN
- TC MGUARD RS2000 4G VZW VPN
- TC MGUARD RS4000 4G ATT VPN
- TC MGUARD RS2000 4G ATT VPN
- FL MGUARD CENTERPORT
- mGuard centerport 2U (Innominate)
- FL MGUARD GT/GT (VPN)
- FL MGUARD PCI(E)4000 (VPN)
- FL MGUARD SMART2 (VPN)
- FL MGUARD DELTA TX/TX (VPN)

Bitte beachten Sie folgende Hinweise

Zielgruppe des Handbuchs

Der in diesem Handbuch beschriebene Produktgebrauch richtet sich ausschließlich an

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

Erklärungen zu den verwendeten Symbolen und Signalwörtern

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

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

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

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

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

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

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

So erreichen Sie uns

Internet

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

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

Ländervertretungen

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

Herausgeber

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
DEUTSCHLAND

Wenn Sie Anregungen und Verbesserungsvorschläge zu Inhalt und Gestaltung unseres Handbuchs haben, würden wir uns freuen, wenn Sie uns Ihre Vorschläge zusenden an:
tecdoc@phoenixcontact.com

Allgemeine Nutzungsbedingungen für Technische Dokumentation

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

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

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

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

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

Inhaltsverzeichnis

1 Grundlagen mGuard

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

- Industrial Security Netzwerkrouter (modellabhängig mit eingebautem 4- bzw. 5-Port-Switch und DMZ-Port)
- VPN-Router für sichere Datenübertragung über öffentliche Netze (Hardware-basierte DES-, 3DES- und 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.

1.1 Grundlegende Eigenschaften der mGuards

Die genannten Eigenschaften sind keine garantierten Eigenschaften, da sie grundsätzlich abhängig vom jeweiligen Gerät und von installierten Lizenzen sind.

Netzwerk-Features

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

Firewall-Features

- Stateful Packet Inspection
- Anti-Spoofing
- IP-Filter
- L2-Filter (nur im Stealth-Modus)
- NAT mit FTP-, IRC- und PPTP-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)

Anti-Virus-Features

- CIFS-Integritätsprüfung von Netzwerklaufwerken auf Veränderung von bestimmten Dateitypen (z. B. von ausführbaren Dateien).

VPN-Features (IPsec)

- Protokoll: IPsec (Tunnel- und Transport-Mode, XAuth/Mode Config)
- IPsec-Verschlüsselung in Hardware 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 1:1-NAT
- Standard-Route über VPN-Tunnel
- Weiterleiten von Daten zwischen VPNs (Hub and Spoke)
- Abhängig von der Lizenz: bis zu 250 VPN-Tunnel, bei mGuard centerport (Innominate)/FL MGUARD CENTERPORT bis zu 3000 aktive VPN-Tunnel
- Hardware-Beschleunigung für die Verschlüsselung im VPN-Tunnel (außer mGuard centerport (Innominate)/FL MGUARD CENTERPORT)

VPN-Features (OpenVPN)

- OpenVPN-Client
- OpenVPN-Verschlüsselung mit Blowfish, AES (128, 192, 256 Bit)
- 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)
- Abhängig von der Lizenz: bis zu 50 VPN-Tunnel

Weitere Features

- Remote Logging
- VPN-/Firewall-Redundanz (abhängig von der Lizenz)
- Administration unter Benutzung von SNMP v1-v3 und Phoenix Contact Device Manager (mGuard device manager (FL MGUARD DM))
- PKI-Unterstützung für HTTPS/SSH Remote Access
- Kann über die LAN-Schnittstelle als NTP- und DNS-Server agieren
- mGuard Secure Cloud kompatibel
- Plug-n-Protect Technologie
- Tracking und Zeitsynchronisation über GPS-/GLONASS-Ortungssystem (Produktabhängig)
- COM-Server

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.net/products.

1.2 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
- Mobilfunk-Router über integriertes Mobilfunkmodem

1.2.1 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.

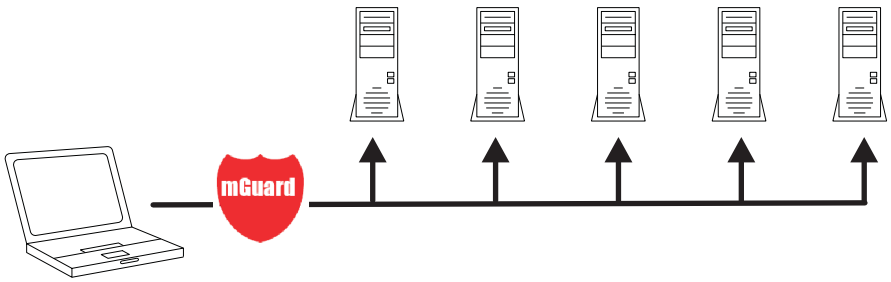


Bild 1-1 Stealth-Modus (Plug-n-Protect)

1.2.2 Netzwerkrouter

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

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

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

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

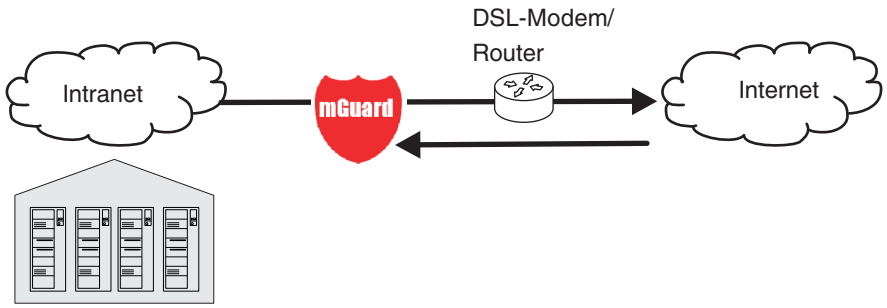


Bild 1-2 Netzwerk-Router

1.2.3 DMZ

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

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

Ein DMZ-Szenario lässt sich entweder durch zwei mGuards realisieren (siehe Bild 1-3), oder per dediziertem DMZ-Port des TC MGUARD RS4000 3G, TC MGUARD RS4000 4G oder FL MGUARD RS4004.

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

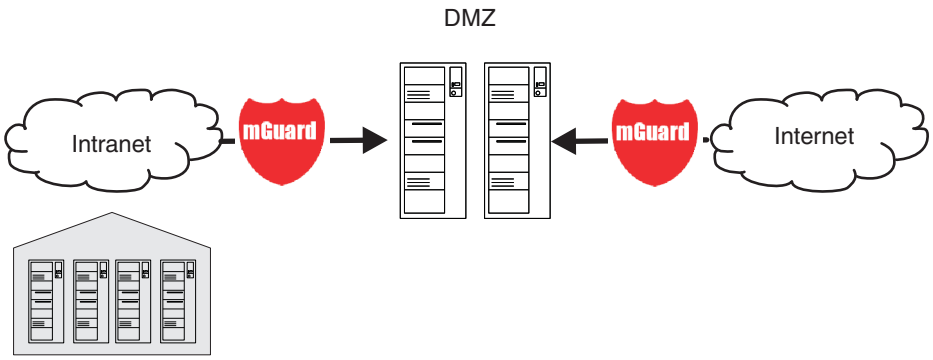


Bild 1-3 DMZ

1.2.4 VPN-Gateway

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

Auf den externen Rechnern muss dazu eine IPsec-fähige VPN-Client-Software installiert werden oder der Rechner wird mit einem mGuard ausgerüstet.

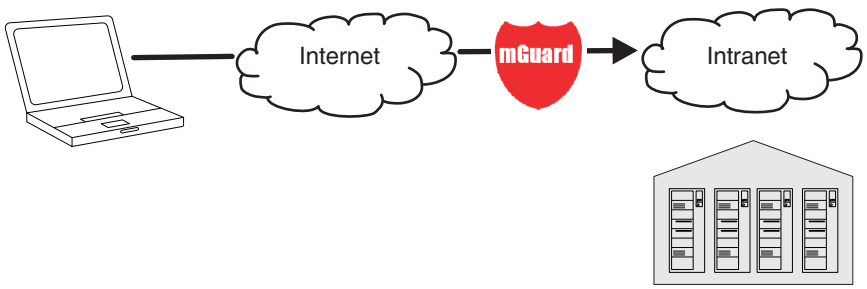


Bild 1-4 VPN-Gateway

1.2.5 WLAN über VPN

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

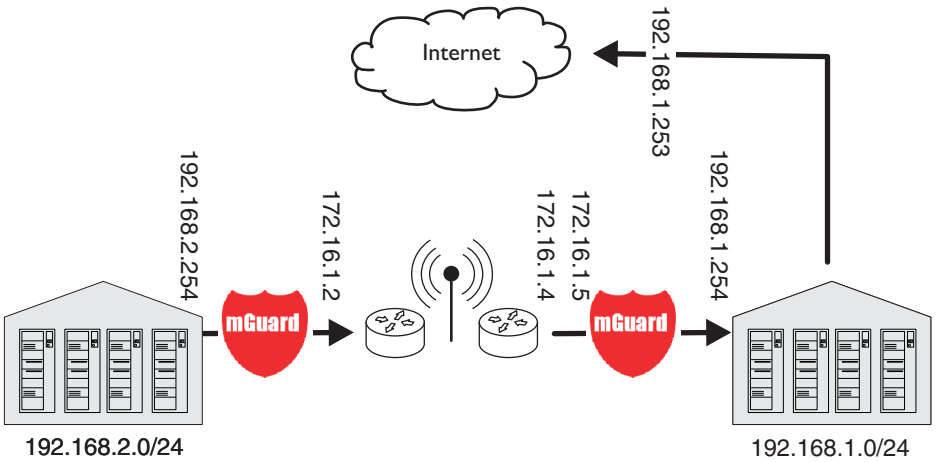


Bild 1-5 WLAN über VPN

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

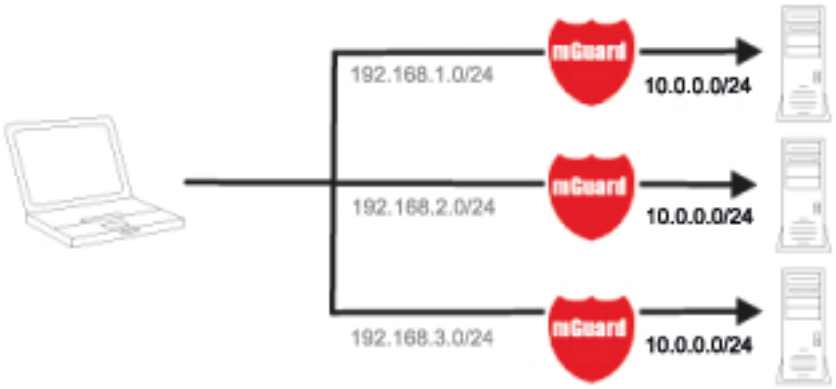
Verbindungstyp	Tunnel (Netz <-> Netz)
Lokales Netz	0.0.0.0
Adresse des Remote-Netzes	192.168.2.0/24

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

1.2.6 Auflösen von Netzwerkkonflikten



Auflösen von Netzwerkkonflikten

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

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

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

2 Hilfen zur Konfiguration

2.1 Sichere Verschlüsselung

Der mGuard bietet grundsätzlich 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 im mGuard ausgewählt und verwendet werden.

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)
– Verschlüsselter Zustandsabgleich von Redundanzpaaren (bis 8.7.1)

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

Weitergehende Informationen finden sich 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.

Grundsätzlich gilt Folgendes: Je länger die Schlüssellänge (in Bits) ist, die ein Verschlüsselungsalgorithmus verwendet (angegeben durch die angefügte Zahl), desto sicherer ist er.

Verschlüsselung	**Algorithmus**	**Verwendung**
	AES-256 AES-192 AES-128	Empfohlen
	3DES Blowfish	Möglichst nicht verwenden
	DES	Nicht verwenden
Hash/Prüfsumme	**Hash-Funktion**	**Verwendung**
	SHA-512 SHA-384 SHA-256	Empfohlen
	SHA-1	Möglichst nicht verwenden
	MD5	Nicht verwenden

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 grundsätzlich akzeptiert.

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

Erstellung sicherer X.509-Zertifikate

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

Benutzen Sie immer **aktuelle Programm-Versionen** der Software-Tools, um die Verwendung schwacher Verschlüsselungsalgorithmen bei der Erstellung von X.509-Zertifikaten zu vermeiden. Der Hash-Algorithmus MD5 sollte nicht und SHA-1 möglichst nicht verwendet werden.

Benutzen Sie bei der Erstellung von X.509-Zertifikaten **Schlüssellängen von mindestens 2048 Bit**.

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.

2.2 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

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 Verbindungen ohne gültiges Login gezählt wird, dann wird die Drossel wirksam. Die Drossel wird zurückgesetzt, wenn 30 Sekunden lang kein ungültiger Verbindungsversuch gestartet wurde. Jeder erneute Aufruf ohne gültiges Login von dieser IP-Adresse setzt den Timer um 30 Sekunden zurück.

Die Anzahl an gescheiterten Verbindungsversuchen bis die Drossel wirksam wird, hängt vom Protokoll ab

- 10 bei HTTPS
- 6 bei SSH, SNMP, COM-Server

2.3 Benutzerrollen

root	Benutzerrolle ohne Einschränkungen
admin	Administrator
netadmin	Administrator nur für das Netzwerk
audit	Auditor/Prüfer
mobile	Versenden von SMS

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

- Der Benutzer *root* hat einen uneingeschränkten Zugriff auf den mGuard.
- Der Benutzer *admin* hat ebenfalls einen funktional uneingeschränkten Zugriff auf den mGuard, jedoch ist die Anzahl der gleichzeitigen SSH-Sitzungen eingeschränkt.
- Dem Benutzer *netadmin* werden über den mGuard device manager (FL MGUARD DM) 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) eingeschaltet werden.
- Der Benutzer *mobile* kann über ein CGI-Script SMS-Nachrichten mit dem mGuard versenden. Weitere Funktionen sind dem Benutzer *mobile* nicht zugänglich (siehe „CGI-Interface“ auf Seite 477).

2.4 Eingabehilfe bei der Konfiguration (Systemnachrichten)

Ab der Firmware 8.0 werden geänderte oder ungültige Einträge 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.

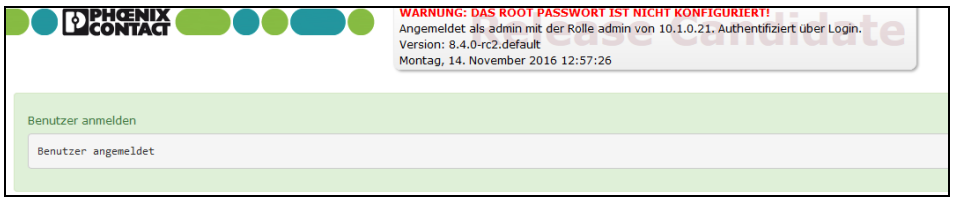


Bild 2-1 Beispiel für Systemnachricht

- **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 im oberen Bereich des Bildschirms angezeigt.

2.5 Bedienung der Web-Oberfläche

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

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

Arbeiten mit Registerkarten

– Sie können auf der betreffenden Registerkarte die gewünschten Einträge machen (siehe auch „Arbeiten mit sortierbaren Tabellen“ auf Seite 25).
– 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

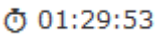
Zurücksetzen auf die alten Werte. Wenn Sie auf einer oder mehreren Konfigurationsseiten Werte eingetragen haben und diese noch nicht mit **Übernehmen** in Kraft gesetzt haben, können Sie mit **Zurücksetzen** die geänderten Werte auf die alten Werte zurücksetzen.

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 73).

Online-Hilfe

Verweis auf die **Online-Hilfe** zur installierten Firmwareversion.

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 Webbrowsers.

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

2.6 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

2.7 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.

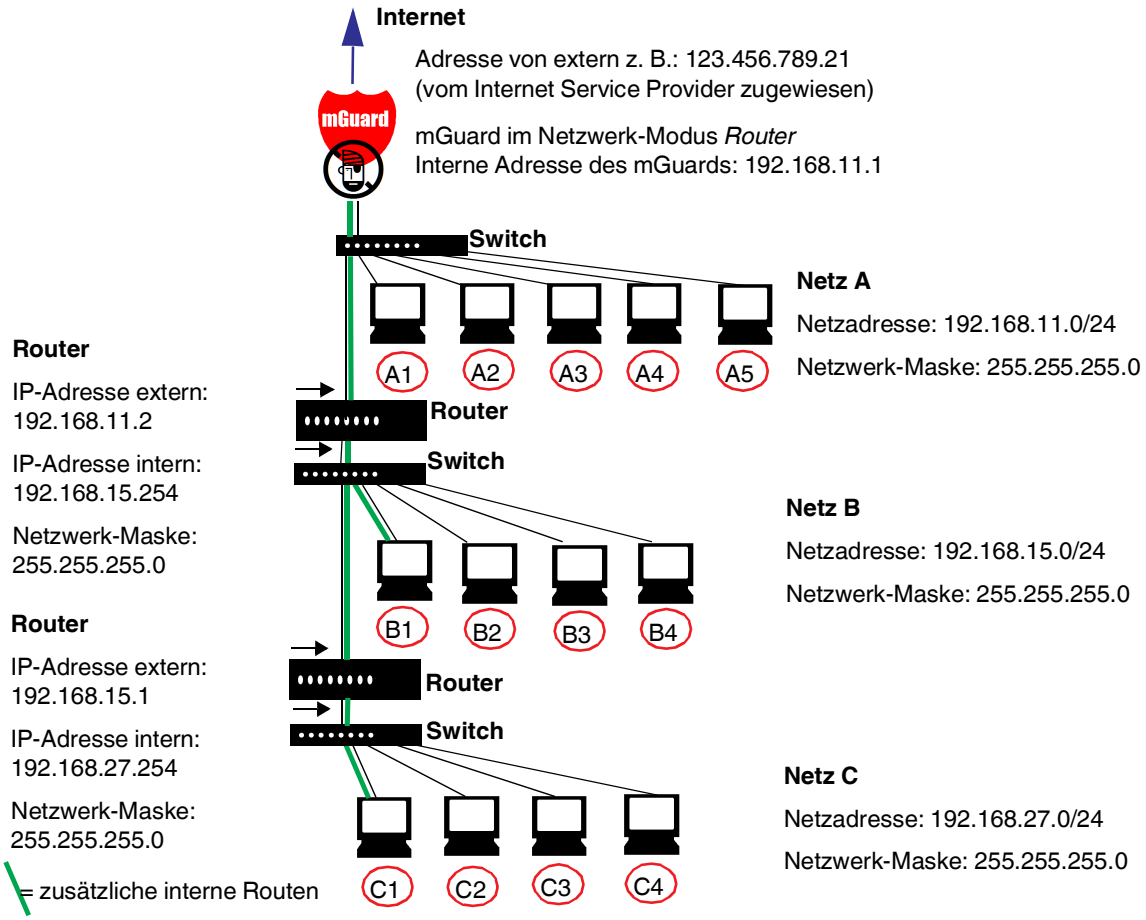


Tabelle 2-1 Netzwerk-Beispielskizze

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**
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**	

2.8 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 479)

3 Änderungen gegenüber der Vorversion

3.1 Übersicht der Änderungen in Version 8.8

Für eine detailliertere Übersicht der Änderungen siehe *mGuard-Firmware Version 8.8.x – Release Notes*.

Die folgenden Funktionen wurden in Firmwareversion 8.8 hinzugefügt oder entfernt:

– Filtern von TCP-Paketen mit gesetztem URGENT-Flag
– Verschlüsselter Zustandsabgleich in aktivierter Firewall- und VPN-Redundanz wird nicht mehr unterstützt

Filtern von TCP-Paketen mit gesetztem URGENT-Flag

IT-Sicherheitsexperten haben elf Sicherheitslücken im Echtzeit-Betriebssystem VxWorks aufgedeckt (*URGENT/11*). Sechs Sicherheitslücken erlauben es einem Angreifer, Code auf betroffenen Geräten zu installieren und auszuführen (*Remote Code Execution*):

– CVE-2019-12256
– CVE-2019-12257
– CVE-2019-12255
– CVE-2019-12260
– CVE-2019-12261
– CVE-2019-12263

Vorgeschaltete mGuard-Geräte können über ihre Firewall-Funktionalität betroffene Geräte vor diesbezüglichen Angriffen schützen (siehe detaillierte Beschreibung unter phoenixcontact.com).

mGuard-Firmwareversion 8.8.0 bietet dazu eine neue Funktion, mit der TCP-Pakete, die im TCP-Header ein URGENT-Flag gesetzt haben, blockiert werden können (siehe Kapitel 8.1.7: *TCP-Pakete mit gesetztem URGENT-Flag blockieren*).

Verschlüsselter Zustandsabgleich in aktivierter Firewall- und VPN-Redundanz wird nicht mehr unterstützt

Ab mGuard Firmwareversion 8.8.0 ist ein verschlüsselter Zustandsabgleich bei aktivierter Firewall- und VPN-Redundanz nicht mehr möglich.

Ein Update auf Firmware-Version 8.8.0 ist nur möglich, wenn die Funktion „Verschlüsselter Zustandsabgleich“ zuvor deaktiviert wurde.

3.2 Übersicht der Änderungen in Version 8.7

Für eine detailliertere Übersicht der Änderungen siehe *mGuard-Firmware Version 8.7.x – Release Notes*.

Die folgenden Funktionen wurden für die Firmwareversion 8.7 hinzugefügt:

– QoS-Funktionen in VPN-Verbindungen werden nicht mehr unterstützt
– Neue Versionen des Konfigurationsspeichers MEM PLUG werden unterstützt

QoS-Funktionen in VPN-Verbindungen werden nicht mehr unterstützt

Die folgenden *Quality of Service*-Funktionen wurden entfernt und werden in VPN-Verbindungen nicht mehr unterstützt:

– *Egress-Queues (VPN)*
– *Egress-Zuordnungen (VPN)*

Neue Versionen des Konfigurationsspeichers MEM PLUG werden unterstützt

Neue Versionen des externen Konfigurationsspeichers *MEM PLUG* mit höherer Kapazität für das Gerät FL MGUARD GT/GT werden unterstützt.

3.3 Übersicht der Änderungen in Version 8.6

Für eine detailliertere Übersicht der Änderungen siehe *mGuard-Firmware Version 8.6.x – Release Notes*.

Die folgenden Funktionen wurden für die Firmwareversion 8.6 hinzugefügt:

- BusyBox wurde aktualisiert
- SNMPv3-Benutzername und -Passwort können geändert werden
- Vereinfachte Suche nach Firewall-Regeln auf Grundlage der Log-Einträge
- NTP-Zeitsynchronisation über VPN möglich
- Im Stealth-Modus „Automatisch“ kann der mGuard den DNS-Server seines zu schützende Clients verwenden
- DHCP-Server über die DMZ-Schnittstelle verfügbar
- SSH-Fernzugang für den Benutzer root kann deaktiviert werden

BusyBox wurde aktualisiert

Das Programm BusyBox wurde auf Version 1.26.1 aktualisiert.

Benutzer, die UNIX-Dienstprogramme oder Shell-Skripte (z. B. Rollout-Scripts) auf dem mGuard ausführen, sollten diese auf geändertes Verhalten überprüfen.

SNMPv3-Benutzername und -Passwort können geändert werden

Der in früheren mGuard-Versionen fest vergebene SNMPv3-Benutzername „*admin*“ kann über die Web-Oberfläche, eine ECS-Konfiguration oder ein Rollout-Script geändert werden. Das Gleiche gilt für das zugehörige SNMPv3-Passwort (siehe „Verwaltung >> SNMP“ auf Seite 103).

Vereinfachte Suche nach Firewall-Regeln auf Grundlage der Log-Einträge

Das Anklicken eines Log-Eintrags des Netzwerksicherheits-Logs öffnet die Konfigurationsseite mit der Firewall-Regel, die den Log-Eintrag verursacht hat (siehe „Logging >> Logs ansehen“ auf Seite 431).

NTP-Zeitsynchronisation über VPN möglich

Die Anfrage des NTP-Servers zur Zeitsynchronisation kann, wenn ein passender VPN-Tunnel konfiguriert ist, über diesen VPN-Tunnel durchgeführt werden (siehe „NTP-Server“ auf Seite 51).

Im Stealth-Modus „Automatisch“ kann der mGuard den DNS-Server seines zu schützende Clients verwenden

Im Stealth-Modus *„Automatisch“* kann der mGuard automatisch den verwendeten DNS-Server seines zu schützenden Clients ermitteln und ebenfalls verwenden. Dazu muss in den DNS-Einstellungen als Nameserver *„Provider-definiert (d. h. via PPPoE oder DHCP)“* ausgewählt werden (siehe „Zu benutzende Nameserver“ auf Seite 217).

DHCP-Server über die DMZ-Schnittstelle verfügbar

Der mGuard kann auf der DMZ-Schnittstelle als DHCP-Server fungieren und anfragenden Clients automatisch eine Netzwerkkonfiguration über das DHCP-Protokoll zuweisen (siehe „DMZ DHCP“ auf Seite 228).

SSH-Fernzugang für den Benutzer root kann deaktiviert werden

Der SSH-Zugang kann für den Beutzer „*root*“ deaktiviert werden (siehe „Erlaube SSH-Zugang als Benutzer root“ auf Seite 55).

3.4 Übersicht der Änderungen in Version 8.5

Für eine detailliertere Übersicht der Änderungen siehe *mGuard-Firmware Version 8.5.x – Release Notes*.

Die folgenden Funktionen wurden für die Firmwareversion 8.5 hinzugefügt:

- Proxy-Authentifizierung durch VPN Path Finder
- SNMP-Trap „Service-Eingang/CMD“
- TLS-Authentifizierung in OpenVPN-Verbindungen
- Firewall-Funktionalität in mGuard-Geräten der RS2000-Serie
- Die Funktion CIFS-Anti-Virus-Scan-Connector entfällt
- 1:1-NAT in OpenVPN-Verbindungen
- COM-Server-Funktionalität wurde erweitert

Proxy-Authentifizierung durch VPN Path Finder

Die Path Finder-Funktion des initiierenden Gateways unterstützt die Proxy-Authentifizierungsmechanismen: „**NTLM**“, „**Basic**“ .

SNMP-Trap „Service-Eingang/CMD“

Der neue hardwarebezogene Trap „**Service-Eingang/CMD**“ wird gesendet, wenn ein Service-Eingang/CMD durch einen Schalter oder Taster geschaltet wird.

TLS-Authentifizierung in OpenVPN-Verbindungen

OpenVPN-Verbindungen können zusätzlich über den Austausch von statischen Pre-Shared-Keys (TLS-PSK) abgesichert werden.

1:1-NAT in OpenVPN-Verbindungen

In OpenVPN-Verbindungen kann lokales1:1-NAT verwendet werden.

Firewall-Funktionalität in mGuard-Geräten der RS2000-Serie

Die bisherige Funktionalität der sogenannten „2-Click-Firewall“ auf mGuard-Geräten der RS2000-Serie wurde erweitert. Das Anlegen von Firewall-Regeln und die Verwendung von IP- und Portgruppen ist nun möglich. Die Firewall-Zugriffe werden in Log-Dateien erfasst und dargestellt.

Die Funktion CIFS-Anti-Virus-Scan-Connector entfällt

Die Funktion CIFS-AV-Scan-Connector entfällt.

COM-Server-Funktionalität wurde erweitert

Die COM-Server-Funktionalität für die serielle Schnittstelle unterstützt zusätzlich Paketlängen von 7 Bit.

3.5 Übersicht der Änderungen in Version 8.4

Die folgenden Funktionen wurden für die Firmwareversion 8.4 hinzugefügt:

- Unterstützung des LTE-Mobilfunkmodems (4G)
- Automatische Anmeldung beim CDMA-Mobilfunkprovider
- Neustart des mGuards per SMS
- Modbus-TCP (Deep Packet Inspection)
- Verwendung von Hostnamen in IP-Gruppen (Firewall-Regeln)
- Zugriffsbeschränkung (intern/extern) für den mGuard-NTP-Server
- Geänderte Recovery-Prozedur
- Log-Eintrag für CMD-Kontakt

Unterstützung des LTE-Mobilfunkmodems (4G)

mGuard-Geräte mit eingebautem LTE-Mobilfunkmodem (4G) werden unterstützt.

Automatische Anmeldung beim CDMA-Mobilfunkprovider

Die Anmeldung und Aktivierung eines bereits beim CDMA-Mobilfunkprovider (Verizon – USA) registrierten Geräts erfolgt automatisch, sobald die Mobilfunkverbindung zum Provider das erste Mal aufgebaut wird („Mobile network cdma2000 OTASP Registration“ auf Seite 170).

Neustart des mGuards per SMS

mGuard-Geräte mit enthaltener Mobilfunk-Funktion können mit einer SMS-Nachricht und einem darin enthaltenem Token neu gestartet (rebootet) werden (siehe „Neustart“ auf Seite 127).

Modbus-TCP (Deep Packet Inspection)

Der mGuard kann ein- und ausgehende Modbus-TCP-Verbindungen, d. h. in der Regel Verbindungen an TCP-Port 502, prüfen (Deep Packet Inspection) und bei Bedarf filtern.

Die Regeln für die Filterung von Modbus-TCP-Paketen werden in Modbus-TCP-Regelsätzen konfiguriert. Diese Regelsätze können in den folgenden Firewall-Tabellen als Aktion ausgewählt werden: Allgemeiner Paketfilter / DMZ / GRE / IPsec VPN / OpenVPN-Client / PPP (siehe „Modbus TCP“ auf Seite 298).

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

In IP-Gruppen können neben IP-Adressen auch Hostnamen angegeben werden (DNS-basierte Firewall-Regeln).

Damit wird die Verwendung von Hostnamen in Firewall-Tabellen möglich, in denen IP-Gruppen ausgewählt werden können (siehe „IP- und Portgruppen“ auf Seite 289): Allgemeiner Paketfilter / DMZ / GRE / IPsec VPN / OpenVPN-Client / NAT / Benutzer-Firewall.

Zugriffsbeschränkung (intern/extern) für den mGuard-NTP-Server

Eingehende Anfragen an den NTP-Server des mGuards über beliebige Interfaces können mittels Firewall-Regeln beschränkt werden (siehe „Aktiviere NTP-Zeitsynchronisation“ auf Seite 51).

Geänderte Recovery-Prozedur

Vor der Durchführung der 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. Die vorher aktive Konfiguration kann über das Recovery-Konfigurationsprofil mit oder ohne Änderungen wiederhergestellt werden.

Log-Eintrag für CMD-Kontakt

Das Schalten eines CMD-Kontaktes (CMD 1–3) mittels angeschlossenem Schalter oder Taster erzeugt einen Log-Eintrag.

3.6 Übersicht der Änderungen in Version 8.3

Die folgenden Funktionen wurden für die Firmware Version 8.3 hinzugefügt:

- Aufbau von OpenVPN-Verbindungen
- Dynamisches Routing (OSPF)
- Unterstützung von GRE-Tunneln
- Unterstützung der Path Finder-Funktion des mGuard Secure VPN Clients
- Verwendung von IP- und Portgruppen
- Neue Zugriffsüberprüfung und veränderte Prüfberichtserstellung (Logging) bei CIFS
- Verbesserte Anzeige des VPN-Status (IPsec)
- Verbessertes Timeout-Verhalten bei VPN-Verbindungen
- Neues VPN-Lizenz-Modell
- Verbesserte Verwendung von Konfigurationsprofilen
- Optionale Nutzung des Proxy-Servers durch das sekundäre externe Interface
- Unterstützung von XAuth und Mode Config (iOS-Support)

Aufbau von OpenVPN-Verbindungen

Der mGuard kann als OpenVPN-Client VPN-Verbindungen zu Gegenstellen aufbauen, die OpenVPN als Server unterstützen (siehe „Menü OpenVPN-Client“ auf Seite 381).

Dynamisches Routing (OSPF)

Unterstützung des dynamischen Routing-Protokolls OSPF (Open Shortest Path First). Der mGuard kann als OSPF-Router dynamisch die Routen von benachbarten OSPF-Routern lernen und eigene sowie gelernte Routen weiterverbreiten. Dies erleichtert die Konfiguration von komplexen Netzwerkstrukturen, da weniger Routen statisch eingetragen werden müssen (siehe „Netzwerk >> Dynamisches Routing“ auf Seite 233).

Die OSPF-Routen können über jedes ausgewählte Interface (Intern, Extern, DMZ) und ebenfalls über IPsec-Verbindungen gelernt und weiterverbreitet werden (im Falle von IPsec unter Zuhilfenahme eines GRE-Tunnels).

Unterstützung von GRE-Tunneln

Der mGuard unterstützt die Verwendung von GRE-Tunneln. Damit ist es möglich, andere Netzwerk-Protokolle einzukapseln und in Form eines Tunnels über das Internet Protocol (IP) zu transportieren. Die dynamische Verbreitung von OSPF-Routen über IPsec-Verbindungen wird dadurch ermöglicht (siehe „Netzwerk >> GRE-Tunnel“ auf Seite 238).

Unterstützung der Path Finder-Funktion (mGuard Secure VPN Client)

Die Funktion „Path Finder“ ermöglicht den Verbindungsaufbau durch den mGuard Secure VPN Client, wenn sich dieser hinter einem Proxy-Server oder einer Firewall befindet (siehe „TCP-Kapselung mit aktivierter Funktion „Path Finder““ auf Seite 332).

Verwendung von IP- und Portgruppen

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

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 (siehe „IP- und Portgruppen“ auf Seite 289).

Neue Zugriffsüberprüfung und veränderte Prüfberichtserstellung (Logging) bei CIFS

Zugriffsüberprüfung

Um zu vermeiden, dass eine umfangreiche Integritätsprüfung aufgrund von fehlenden Zugriffsberechtigungen auf dem Ziellaufwerk abgebrochen wird, kann die Zugriffsberechtigung vor dem eigentlichen Scan geprüft werden. Diese Zugriffsüberprüfung verläuft deutlich schneller und erzeugt einen Prüfbericht, der heruntergeladen und analysiert werden kann. Sind alle Zugriffsberechtigungen gegeben, kann anschließend die Integritätsprüfung durchgeführt werden (siehe „CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung“ auf Seite 314).

Prüfbericht (Log-Datei)

Im Prüfbericht der Integritätsprüfung werden die alten Ergebnisse einer Prüfung nicht gelöscht, wenn eine neue Prüfung erfolgt. Der Bericht wir ferner um die neuen Ergebnisse ergänzt. Erreicht der Bericht eine bestimmte Dateigröße, wird er als Backup-Datei abgelegt, und ein neuer Prüfbericht wird erstellt. Erreicht dieser Prüfbericht ebenfalls eine bestimmte Dateigröße, wird die Backup-Datei mit dem neuen Bericht überschrieben, und ein weiterer Bericht wird angelegt (siehe „Prüfbericht“ auf Seite 322).

Verbesserte Anzeige des VPN-Status (IPsec)

Der Statusseite zur Anzeige von Informationen zu VPN-Verbindungen wurde überarbeitet. Der Status aller VPN-Verbindungen wird übersichtlich dargestellt („IPsec VPN >> IPsec Status“ auf Seite 378).

Neues VPN-Lizenz-Modell

Das neue VPN-Lizenz-Modell erlaubt es, mit allen VPN-Lizenzen Tunnelgruppen zu erstellen.

Die Lizenz begrenzt nun nicht mehr die Anzahl der aufgebauten Tunnel, sondern die Anzahl der verbundenen Gegenstellen (VPN-Peers). Werden zu einer Gegenstelle mehrere Tunnel aufgebaut, wird nur eine Gegenstelle gezählt, was eine Verbesserung zum alten Modell darstellt.

Der Lizenzstatus, also die Gesamtzahl und die aktuell verwendete Anzahl lizenzierter Gegenstellen, wird in den Menüs „IPsec VPN“ und „OpenVPN-Client“ übersichtlich dargestellt.

Verbesserte Verwendung von Konfigurationsprofilen

Bevor die Einstellungen von gespeicherten Konfigurationsprofilen in Kraft gesetzt werden, können die Veränderungen zur aktuellen Konfiguration sichtbar gemacht und so überprüft werden. Die Änderungen können unverändert übernommen werden. Einzelne Einstellungen können aber auch vor dem Übernehmen beliebig geändert werden (siehe „Konfigurationsprofile“ auf Seite 97).

Verbessertes Timeout-Verhalten bei VPN-Verbindungen

Der Timeout kann eine VPN-Verbindung stoppen, die über eine Schaltfläche in der Web-Oberfläche, SMS, Schalter, Taster oder das Skript nph-vpn.cgi gestartet wurde. Diese VPN-Verbindung wird nach Ablauf des Timeouts beendet und in den Zustand „Gestoppt“ versetzt.

Eine VPN-Verbindung, die durch Datenverkehr initiiert (aufgebaut) wird, wird ebenfalls per Timeout beendet. Diese VPN-Verbindung wird nach Ablauf des Timeouts allerdings nicht in den Zustand „Gestoppt“ versetzt, sondern verbleibt im Zustand „Gestartet“. Bei erneut auftretendem Datenverkehr wird die VPN-Verbindung wieder aufgebaut. Diese Funktion ist vor allem bei der Verwendung der mobilen Schnittstelle (3G) sinnvoll.

Unterstützung von XAuth und Mode Config (iOS-Support)

Der mGuard unterstützt jetzt die Authentifizierungsmethode „Extended Authentication“ (XAuth) und die häufig erforderliche Protokollerweiterung „Mode Config“ inklusive Split Tunneling als Server und als Client (u. a. Unterstützung von Apple iOS). Netzwerkeinstellungen, DNS- und WINS-Konfigurationen werden dem IPsec-Client vom IPsec-Server mitgeteilt (siehe „Mode Configuration“ auf Seite 346).

Optionale Nutzung des Proxy-Servers durch das sekundäre externe Interface

Wird ein Proxy-Server verwendet, kann das sekundäre externe Interface von dessen Nutzung ausgenommen werden. Dies kann sinnvoll sein, wenn es sich bei dem sekundären externen Interface um ein Mobilfunkmodem (3G) handelt (siehe „Netzwerk >> Proxy-Einstellungen“ auf Seite 231).

3.7 Übersicht der Änderungen in Version 8.1

Die folgenden Funktionen wurden für die Firmware Version 8.1 hinzugefügt.

- Benutzerfirewall in VPN-Verbindungen
- Dynamische Aktivierung der Firewall-Regeln
- Erweiterung der Funktion der Servicekontakte
- OPC Inspector zur Deep Packet Inspection für OPC Classic
- Erweiterte DynDNS-Anbieter
- Neuer Modus beim Authentisierungsverfahren Pre-Shared Key (PSK)
- In der Web-Oberfläche werden dynamische Änderungen grau gestellt.
- Ausführliches Logging von Modems

Benutzerfirewall in VPN-Verbindungen

Die Benutzerfirewall kann innerhalb von VPN-Verbindungen benutzt werden.

Bei der Benutzerfirewall kann nun eine VPN-Verbindung ausgewählt werden, in der die Benutzerfirewall-Regeln gültig sind (unter Netzwerksicherheit >> Benutzerfirewall >> Benutzerfirewall-Templates).

Dynamische Aktivierung der Firewall-Regeln (Conditional Firewall)

Die Firewall-Regeln können jetzt über ein externes Ereignis aktiviert werden:

- **Eine Schaltfläche in der Web-Oberfläche** (unter Netzwerksicherheit >> Paketfilter >> Regelsätze)
- **Eine API-Befehlszeile**, die über den Namen oder die Row-ID aktiviert wird. /Packages/mguard-api_0/mbin/action fwrules/[in]active <ROWID>
- /Packages/mguard-api_0/mbin/action_name fwrules/[in]active <NAME>
- **Ein extern angeschlossenen Taster/Schalter** (bei mGuards, die den Anschluss erlauben, siehe „Dynamische Aktivierung der Firewall-Regeln (Conditional Firewall)“ auf Seite 39)
- **Das Starten oder Stoppen einer VPN-Verbindung**. Es kann eingestellt werden, ob eine gestartete bzw. gestoppte VPN-Verbindung den Firewall-Regelsatz aktiviert oder inaktiviert. Ein erfolgreicher Aufbau der VPN-Verbindung ist dabei nicht von Bedeutung. (Das Starten der VPN-Verbindung kann über eine Schaltfläche in der Web-Oberfläche, SMS, Schalter, Taster, Datenverkehr oder das Skript nph-vpn.cgi erfolgen.)
- **Eine eingehende SMS** (nur beim TC MGUARD RS4000/RS2000 3G). Siehe „Token für SMS-Steuerung“ unter Netzwerksicherheit >> Paketfilter >> Regelsätze.
- **Das CGI-Interface**. Das CGI-Script „nph-action.cgi may“ kann benutzt werden, um Firewall-Regelsätze zu steuern.

Es kann automatisch eine E-Mail verschickt werden, wenn sich der Status der Firewall-Regelsätze ändert. Beim TC MGUARD RS4000/RS2000 3G kann in einem solchen Fall auch eine SMS verschickt werden.

Erweiterung der Funktion der Servicekontakte

An einige mGuards könnten Servicekontakte (Service I/Os) angeschlossen werden.

- TC MGUARD RS4000/RS2000 3G
- FL MGUARD RS4000/RS2000
- FL MGUARD RS
- FL MGUARD GT/GT

An die **Eingänge CMD 1-3** können ein Taster oder ein Ein-/Aus-Schalter angeschlossen werden. Der Taster oder Ein-/Aus-Schalter dient zum Auf- und Abbau von zuvor definierten VPN-Verbindungen oder der definierten Firewall-Regelsätze.

Dafür wird bei den VPN-Verbindungen eingestellt, ob die VPN-Verbindung über einen der Servicekontakte geschaltet werden soll (IPsec VPN >> Verbindungen >> Editieren >> Allgemein). Bei einem angeschlossenen Schalter kann das Verhalten des Schalters auch invertiert werden.

Für die Firewall-Regelsätze kann eingestellt werden, ob eine Regel über einen der Servicekontakte oder eine VPN-Verbindung geschaltet werden soll (Netzwerksicherheit >> Paketfilter >> Regelsätze).

Auf diese Weise können ein oder mehrere frei wählbare VPN-Verbindungen oder Firewall-Regelsätze geschaltet werden. Auch eine Mischung von VPN-Verbindungen und Firewall-Regelsätzen ist möglich.

Über die Web-Oberfläche wird angezeigt, welche VPN-Verbindungen und welche Firewall-Regelsätze an einen Eingang gebunden sind (Verwaltung >> Service I/O>> Servicekontakte).

Außerdem kann in der Web-Oberfläche das Verhalten der **Ausgänge ACK 1-3** eingestellt werden (Verwaltung >> Service I/O>> Servicekontakte).

Über die **Ausgänge ACK O1-2** können bestimmte VPN-Verbindungen oder Firewall-Regelsätze überwacht und über LEDs angezeigt werden.

Der **Alarmausgang ACK 03** überwacht die Funktion des mGuards und ermöglicht damit eine Ferndiagnose.

Durch den Alarmausgang wird Folgendes gemeldet, wenn das aktiviert worden ist.

– Der Ausfall der redundanten Versorgungsspannung
– Überwachung des Link-Status der Ethernet-Anschlüsse
– Überwachung des Temperaturzustandes
– Überwachung des Verbindungsstatus des internen Modems

OPC Inspector zur Deep Packet Inspection für OPC Classic

Bei dem Netzwerk-Protokoll OPC Classic haben zwischengeschaltete Firewalls praktisch keine Wirksamkeit. Zudem kann konventionelles NAT-Routing nicht eingesetzt werden.

Wenn die OPC Classic-Funktion aktiviert wird, werden die OPC-Pakete überwacht (siehe „OPC Inspector“ auf Seite 302).

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.

Weitere Funktionen

Erweiterte DynDNS-Anbieter

– Zum Aufbau von VPN-Verbindungen ist es hilfreich, wenn die Teilnehmer ihre IP-Adresse über einen DynDNS-Service beziehen.

  In Version 8.1 werden mehr DynDNS-Anbieter unterstützt.

Neuer Modus beim Authentisierungsverfahren Pre-Shared Key

Bei Wahl des Authentisierungsverfahrens Pre-Shared Key (PSK) kann der „Aggressive Mode“ gewählt werden (unter IPsec VPN >> Verbindungen >> Editieren >> Authentifizierung).

In der Web-Oberfläche werden dynamische Änderungen grau hervorgehoben.

In der Web-Oberfläche werden Statusmeldungen angezeigt, die laufend aktualisiert werden. Damit diese dynamischen Einträge besser zu erkennen sind, werden sie grau dargestellt.

Ausführliches Logging von Modems

Nur für mGuards, die über ein internes oder externes Modem verfügen oder Mobilfunk-fähig sind (unter Logging >> Einstellungen).

3.8 Übersicht der Änderungen in Version 8.0

Die folgenden Funktionen wurden für die Firmware Version 8.0 hinzugefügt.

Erweiterung der Konfiguration

- Verbessertes CIFS-Integrity-Monitoring (siehe „Neu im CIFS-Integrity-Monitoring“ auf Seite 42)
- Integrierter **COM-Server** für mGuard-Plattformen mit serieller Schnittstelle (siehe „Netzwerk >> Ethernet“ auf Seite 204)
- Konfigurierbare **Multicast-Unterstützung** für Geräte mit internem Switch, um Daten an eine Gruppe von Empfängern zu versenden, ohne dass diese vom Sender mehrmals versendet werden müssen (siehe „Multicast“ auf Seite 207)
- **VPN-Erweiterungen** (siehe „VPN-Erweiterungen“ auf Seite 43).
- **Dynamische Web-Oberfläche** zum Konfigurieren. Fehlerhafte Einträge werden farblich hervorgehoben und zusätzlich werden Hilfen in Form von Systemnachrichten angeboten.
- Unterstützung von 100 MBit/s SFPs für FL MGUARD GT/GT. SFPs sind wechselbare Schnittstellen für Ethernet oder Lichtwellenleiter in verschiedenen Ausprägungen.

Unterstützung der mGuard-Plattformen TC MGUARD RS4000 3G und TC MGUARD RS2000 3G

- Unterstützung von **Mobilfunk- und Ortungsfunktionen** (siehe „Netzwerk >> Mobilfunk“ auf Seite 165)
- **Unterstützung integrierter managed und unmanaged Switches** (siehe „Netzwerk >> Ethernet“ auf Seite 204)
- Unterstützung eines dedizierten **DMZ-Ports** (nur TC MGUARD RS4000 3G)

  Der DMZ-Port kann so eingestellt werden, dass er Pakete an das interne, externe oder sekundäre externe Interface weiterleitet.

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

Entfernte Funktionen

- HiDiscovery-Support
- Die Schaltfläche „Übernehmen“, bei der Änderungen nur für die aktuelle Seite übernommen wurden, wurde entfernt. Änderungen werden seitenübergreifend ausgeführt.

Neu im CIFS-Integrity-Monitoring

Zeitsteuerung

Die Zeitsteuerung ist in Version 8.0 verbessert worden. Jetzt ist mehr als ein Scan pro Tag möglich. Auch ein kontinuierliches Scannen kann eingestellt werden.

Wenn der Scan länger dauert als geplant, wird er abgebrochen. Man kann aber einstellen, dass regelmäßig ein Scan gestartet wird.

Erweiterte Anzeige des aktuellen Status

Jede Zeile des CIFS-Integrity-Monitoring zeigt zusätzlich diese Informationen an.

- den Status der gescannten Netzlaufwerke
- das Ergebnis des letzten oder den Fortschritt des laufenden Scans

Das Menü in der Web-Oberfläche ist erweitert worden, so dass Sie jetzt den Status jedes Scans einsehen können. Der Fortschrittsbalken zeigt die Anzahl der überprüften Dateien an.

VPN-Erweiterungen

Status der VPN-Verbindungen

Die Einstellung der VPN-Verbindung wird nun in „Deaktiviert“, „Gestartet“ und „Angehalten“ eingeteilt. Die Einstellung „Deaktiviert“ ignoriert die VPN-Verbindung, als wäre diese nicht konfiguriert. Sie kann damit auch nicht dynamisch aktiviert/deaktiviert werden. Die anderen beiden Einstellung bestimmen den Status der VPN-Verbindung beim Neustart der Verbindung oder beim Booten.

Die VPN-Verbindungen können in Version 8.0 über eine Schaltfläche in der Web-Oberfläche, über SMS, einen externen Schalter oder das Skript nph-vpn.cgi gestartet oder gestoppt werden. Alle VPN-Verbindungen werden dabei berücksichtigt. Pakete, die zu einer nicht deaktivierten VPN-Verbindung passen werden weitergeleitet, wenn die Verbindung aufgebaut ist, oder verworfen, wenn die Verbindung nicht aufgebaut ist. VPN-Verbindungen, die in der Vorversion als „Aktiv: Nein“ eingestellt wurden, werden nun als „Deaktiviert“ interpretiert.

Eindeutige Namen

In Version 8.0 werden die Namen von VPN-Verbindungen eindeutig gemacht. Während des Updates werden Namen, die doppelt vorhanden sind, mit einer Raute oder einer eindeutigen Zahl versehen.

Timeout für die VPN-Verbindung

Sie können einen Timeout einstellen, der die VPN-Verbindung abbricht, wenn sie über SMS, nph-vpn.cgi oder die Web-Oberfläche gestartet worden ist. Eine VPN-Verbindung, die von einer explizierten Anforderungen durch eine Anwendung gestartet worden ist, ist davon nicht betroffen.

Source based routing

Es können nun VPN-Tunnel konfiguriert werden, die sich nur im Quellnetz unterscheiden.

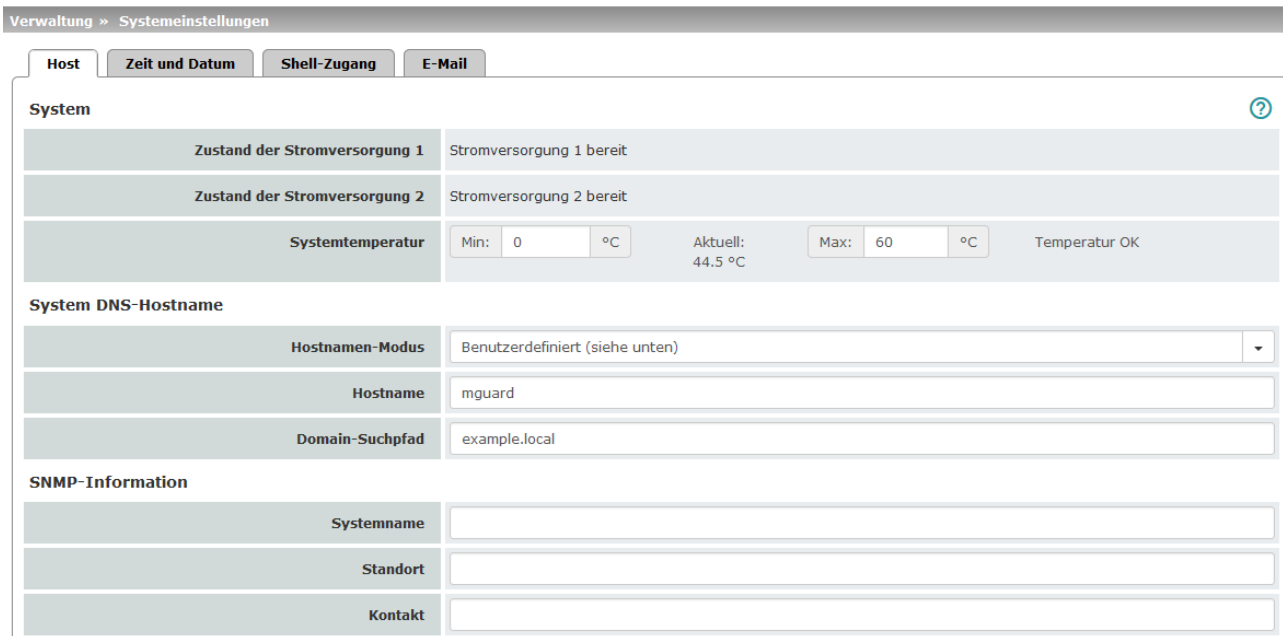
Die VPN-Konfiguration erlaubt ab Version 8.0 ein Remote-Netzwerk mit unterschiedlichen lokalen Netzwerken in einer Konfiguration. Die VPN-Tunnel-Gruppen werden so erweitert, dass sie es einer aufgebauten VPN-Verbindung erlauben, sich nur ein Subnetz aus dem lokalen Netzwerk auszuwählen. Das war in vorherigen Versionen nur für Remote-Netzwerke möglich.

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 243). Solange dies noch nicht geschehen ist, erhalten Sie oben auf der Seite einen Hinweis darauf.

4.1 Verwaltung >> Systemeinstellungen

4.1.1 Host

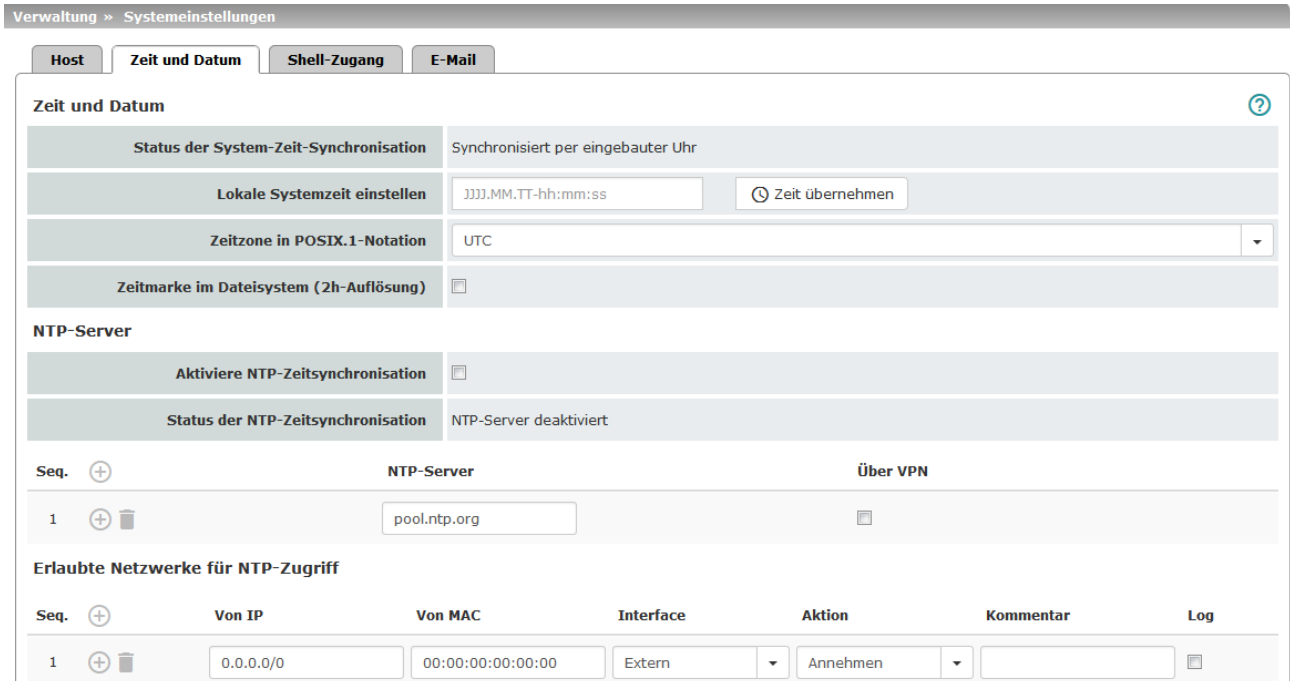


Verwaltung >> Systemeinstellung >> Host		
System	**Stromversorgung 1/2** (Nur TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4000, FL MGUARD RS4004, mGuard centerport (Innominate), FL MGUARD CENTERPORT, FL MGUARD RS, FL MGUARD GT/GT)	Zustand der beiden Netzteile
	Systemtemperatur (°C)	Wenn der angegebene Temperaturbereich unter- bzw. überschritten wird, wird ein SNMP-Trap ausgelöst.
	CPU-Temperatur (°C) (Nur mGuard centerport (Innominate), FL MGUARD CENTERPORT, nicht mit Firmware 7.6.0)	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 serielle Konsole – 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:** *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 45, „Shell-Zugang“ auf Seite 54). 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)
Tastatur (Nur mGuard centerport (Innominate), FL MGUARD CENTERPORT)	Die Einstellungen zur Benutzung einer Tastatur können nur bei den Geräten mGuard centerport (Innominate) und FL MGUARD CENTERPORT vorgenommen werden.	

Verwaltung >> Systemeinstellung >> Host [...]	
Tastaturbelegung	Auswahlliste zum Auswählen der passenden Tastenanordnung

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 48).

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. Die Einstellung der Systemzeit über GPS/GLONASS ist bei TC MGUARD RS4000/RS2000 3G ebenfalls möglich (siehe „Ortungssystem“ auf Seite 181) Stellen Sie Zeit und Datum korrekt ein, da sonst der mGuard bestimmte zeitabhängige Aktivitäten nicht starten kann (siehe „Zeitabhängige Aktivitäten“ auf Seite 48). 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 sichergestellt durch:

- **Kondensator** (nur TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS),
- **Batterie** (nur mGuard centerport (Innominate), FL MGUARD CENTERPORT, mGuard delta (Innominate)) oder
- **Akku** (nur FL MGUARD RS4000/RS2000, FL MGUARD RS4004/RS2005, FL MGUARD SMART2, FL MGUARD PCI(E)4000, FL MGUARD DELTA).

  Beim FL MGUARD RS4000/RS2000 hält der Akku 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 96, „Konfiguration holen“ auf Seite 117).
- **Das Unterbrechen der Verbindung zu bestimmter Uhrzeit beim Netzwerk-Modus PPPoE:**

  Dies ist der Fall, wenn unter dem Menüpunkt *Netzwerk >> Interfaces, Allgemein* der **Netzwerk-Modus** auf PPPoE und der **Automatische Reconnect** auf Ja gesetzt ist (siehe „PPPoE“ auf Seite 149).
- **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 259).
- **CIFS-Integritätsprüfung:**

  Die automatische regelmäßige Prüfung der Netzlaufwerke wird nur dann gestartet, wenn der mGuard eine gültige Zeit und ein gültiges Datum hat (siehe folgender Abschnitt).

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 **NTP-Status** wechselt eventuell erheblich später erst auf „synchronisiert“ (siehe dazu die Erklärung weiter unten zu **NTP-Status)**.
- **Synchronisiert per GPS/GLONASS:** TC MGUARD RS4000/RS2000 3G können über das Ortungssystem (GPS/GLONASS) die Systemzeit einstellen und synchronisieren (unter „Netzwerk >> Mobilfunk >> Ortungssystem“).

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. Stellen Sie ebenfalls die lokale Systemzeit ein, wenn unter dem Ortungssystem der Menüpunkt „Systemzeit aktualisieren“ auf „Ja“ gesetzt wurde (unter „Netzwerk >> Mobilfunk >> Ortungssystem“).

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. Der Zugriff auf den NTP-Server des mGuards ist standardmäßig nur 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. Eine initiale Zeitsynchronisation mit dem externen Zeit-Server erfolgt nach jedem Booten, es sei denn, der mGuard verfügt über eine eingebaute Uhr (bei *TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G*, *FL MGUARD RS4004/RS2005, FL MGUARD RS4000/RS2000, FL MGUARD PCI(E)4000, FL MGUARD DELTA*, *FL MGUARD GT/GT* und bei *FL MGUARD SMART2)*. Nach der initialen Zeitsynchronisation vergleicht der mGuard regelmäßig die Systemzeit mit den Zeit-Servern. In der Regel erfolgen Nachjustierungen nur noch im Sekundenbereich.
	NTP-Status	Anzeige des aktuellen NTP-Status. Gibt an, ob sich der auf dem mGuard selbst laufende NTP-Server mit hinreichender Genauigkeit mit den konfigurierten NTP-Servern synchronisiert hat. Wenn die Systemuhr des mGuards vor der Aktivierung der NTP-Zeitsynchronisation noch nie synchronisiert war, kann die Synchronisierung bis zu 15 Minuten dauern. Dennoch stellt der NTP-Server die Systemuhr des mGuards nach wenigen Sekunden auf die aktuelle Zeit um, sobald er erfolgreich einen der konfigurierten NTP-Server kontaktiert hat. Dann betrachtet der mGuard seine Systemzeit auch bereits als synchronisiert. Nachjustierungen erfolgen in der Regel nur noch im Sekundenbereich.
	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 Interface (LAN-Interface) möglich.

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.

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:

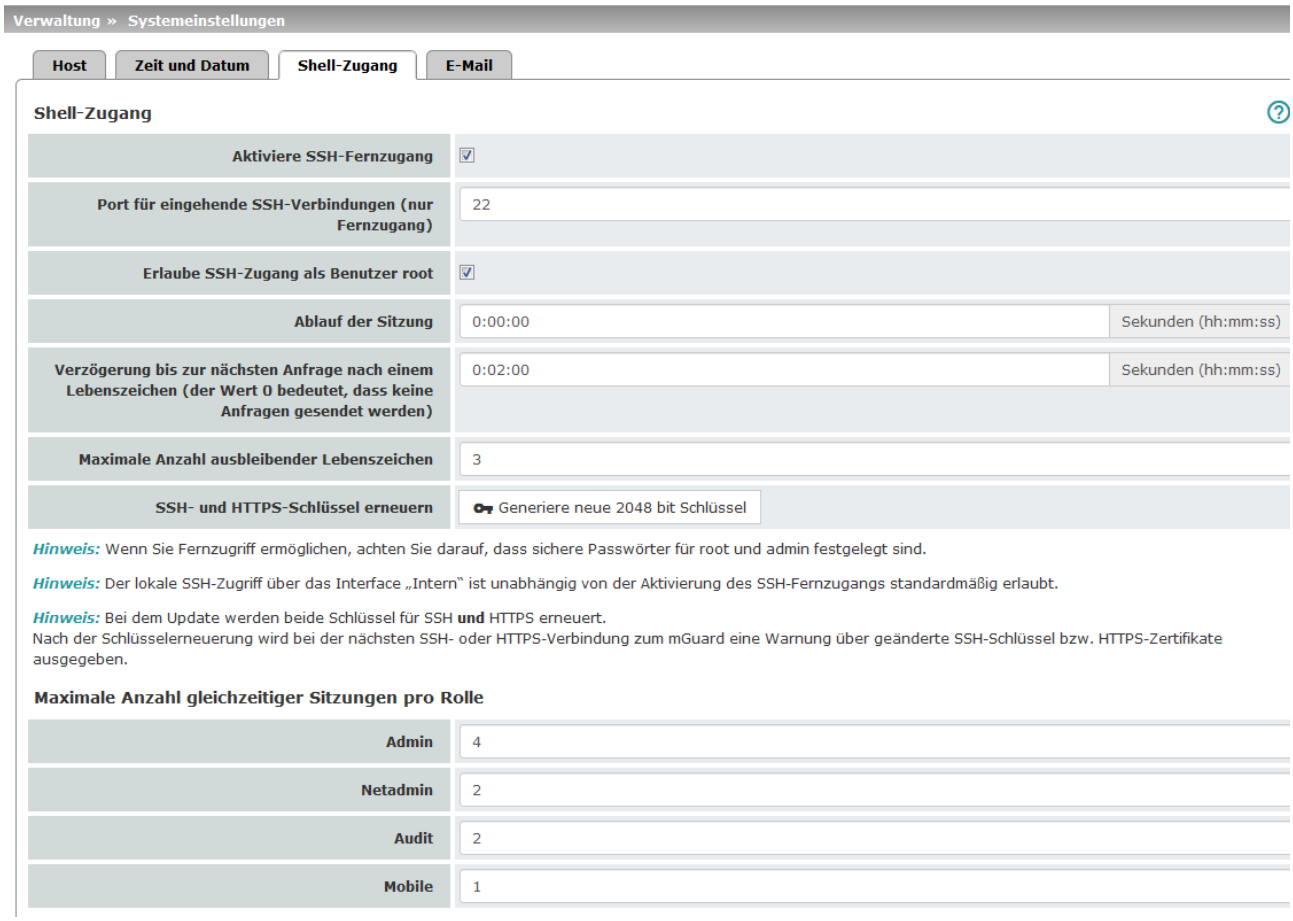
- Eine IP-Adresse.
- Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise (siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 26).
- **0.0.0.0/0** bedeutet alle Adressen.

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

Interface	**Intern / Extern / Extern 2 / DMZ / VPN / GRE / Einwahl**[1]
	Gibt an, für welches Interface die Regel gelten soll.
	Sind keine Regeln gesetzt oder greift keine Regel, gelten folgende Standardeinstellungen:
	NTP-Zugriffe sind erlaubt über *Intern.*
	Zugriffe über *Extern*, *Extern 2, DMZ, VPN, Einwahl* und *GRE* 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 (werkseitige Voreinstellung).

1 *Extern 2* und *Einwahl* nur bei Geräten mit serieller Schnittstelle (siehe „Netzwerk >> Interfaces“ auf Seite 135).

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 die serielle Schnittstelle oder 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 anschließenden 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: Der lokale SSH-Zugriff über das Interface „Intern“ ist unabhängig von der Aktivierung des SSH-Fernzugangs standardmäßig erlaubt.

Um Zugriffsmöglichkeiten auf den mGuard über das interne Interface differenziert festzulegen, müssen Sie die Funktion **Aktiviere SSH-Fernzugang** aktivieren und anschließend Firewall-Regeln für das interne Interface entsprechend definieren (siehe „Erlaubte Netzwerke“ auf Seite 59)

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 anschließenden 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 *Intern*, *VPN* und *Einwahl* möglich.

Um Zugriffsmöglichkeiten auf den mGuard differenziert festzulegen, müssen Sie die Firewall-Regeln für die verfügbaren Interfaces entsprechend definieren (siehe „Erlaubte Netzwerke“ auf Seite 59).

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, Extern 2, DMZ, VPN, GRE* und *Einwahl*.

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.

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

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

Im Unterschied hierzu kann die Verbindung auch abgebrochen werden, wenn die Funktionsfähigkeit der Verbindung nicht mehr gegeben ist, siehe „Verzögerung bis zur nächsten Anfrage nach einem Lebenszeichen“ auf Seite 57.

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. Der hier eingetragene Wert bezieht sich auf die Funktionsfähigkeit der verschlüsselten SSH-Verbindung. Solange diese gegeben ist, wird die SSH-Verbindung vom mGuard wegen dieser Einstellungen nicht beendet, selbst wenn der Benutzer während dieser Zeit keine Aktion ausführt. Da die Anzahl der gleichzeitig geöffneten Sitzungen begrenzt ist, ist es wichtig, abgelaufene Sitzungen zu beenden (siehe *„Maximale Anzahl gleichzeitiger Sitzungen pro Rolle“ auf Seite 58*). Deshalb wird ab Version 7.4.0 die Anfrage nach einem Lebenszeichen auf 120 Sekunden voreingestellt. Bei maximal drei Anfragen nach einem Lebenszeichen, wird eine abgelaufende Sitzung nach sechs Minuten entdeckt und entfernt. In vorherigen Versionen war die Voreinstellung „0“. 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 2048 bit Schlüssel** Schlüssel, die mit einer älteren Firmware erstellt worden sind, sind möglicherweise schwach und sollten erneuert werden. • Klicken Sie auf diese Schaltfläche, um neue Schlüssel zu erzeugen. • Beachten Sie die Fingerprints der neu generierten Schlüssel. • Loggen Sie sich über HTTPS ein und vergleichen Sie die Zertifikat-Informationen, die vom Web-Browser zur Verfügung gestellt werden.
Maximale Anzahl gleichzeitiger Sitzungen pro Rolle	Sie können die Anzahl der Benutzer begrenzen, die gleichzeitig auf die Kommandozeile des mGuards zugreifen dürfen. Der Benutzer „*root*“ hat immer uneingeschränkten Zugang. Die Anzahl der Zugänge für administrative Benutzerrollen (*admin, netadmin, audit* und *mobile*) können jeweils einzeln begrenzt werden. Die Berechtigungsstufen *netadmin* und *audit* beziehen sich auf Zugriffsrechte bei Zugriffen mit dem mGuard device manager (FL MGUARD DM). 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 2147483647 Für die Rolle „*admin*“ sind mindestens 2 gleichzeitig erlaubte Sitzungen erforderlich, damit sich „*admin*“ nicht selbst aust.
	Netadmin	0 bis 2147483647 Bei „0“ ist keine Sitzung erlaubt. Es kann sein, dass der Benutzer „*netadmin*“ nicht verwendet wird.
	Audit	0 bis 2147483647 Bei „0“ ist keine Sitzung erlaubt. Es kann sein, dass der Benutzer „*audit*“ nicht verwendet wird.
	Mobile	0 bis 2147483647 Bei „0“ ist keine Sitzung erlaubt. Es kann sein, dass der Benutzer „*mobile*“ nicht verwendet wird.

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

Erlaubte Netzwerke

(Nur wenn **Aktiviere SSH-Fernzugang** aktiviert ist)

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

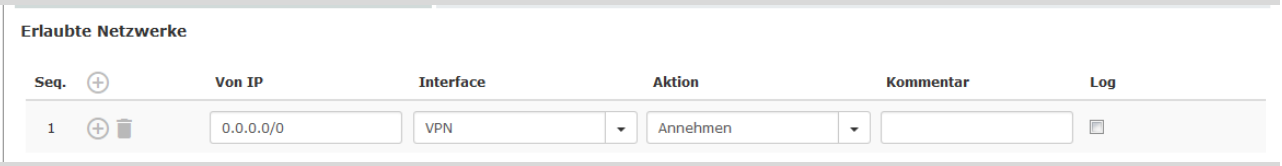
Die Regeln gelten für eingehende Datenpakete und können lizenz- und geräteabhängig für alle Interfaces konfiguriert werden.

Die hier angegebenen Regeln treten nur in Kraft, wenn die Funktion **Aktiviere SSH-Fernzugang** aktiviert ist. Zugriffe von *Intern* sind auch möglich, wenn diese Funktion deaktiviert ist.

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.

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 26.

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

Interface

(Die Auswahlmöglichkeit variiert je nach Gerät und installierten Lizenzen.)

Intern / Extern / Extern 2 / DMZ / VPN / GRE / Einwahl

Extern 2 und *Einwahl* nur bei Geräten mit serieller Schnittstelle, siehe „Netzwerk >> Interfaces“ auf Seite 135.

Gibt an, für welches Interface die Regel gelten soll.

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

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

Legen Sie die Zugriffsmöglichkeiten nach Bedarf fest.

ACHTUNG: Wenn Sie Zugriffe über *Intern, VPN, DMZ* oder *Einwahl* 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 (werkseitige Voreinstellung).

RADIUS-Authentifizierung

(Dieser Menüpunkt gehört nicht zum Funktionsumfang von TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005, FL MGUARD RS2000.)

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

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

Nutze RADIUS-Authentifizierung für den Shell-Zugang

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

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

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

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 anschließenden 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, audit* und *mobile)* können sich dann nicht mehr per SSH oder serieller Konsole beim mGuard anmelden.

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

Verwaltung >> Systemeinstellungen >> Shell-Zugang

X.509-Authentifizierung

(Dieser Menüpunkt gehört nicht zum Funktionsumfang von
TC MGUARD RS2000 3G,
TC MGUARD RS2000 4G,
FL MGUARD RS2005,
FL MGUARD RS2000.)

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 54).

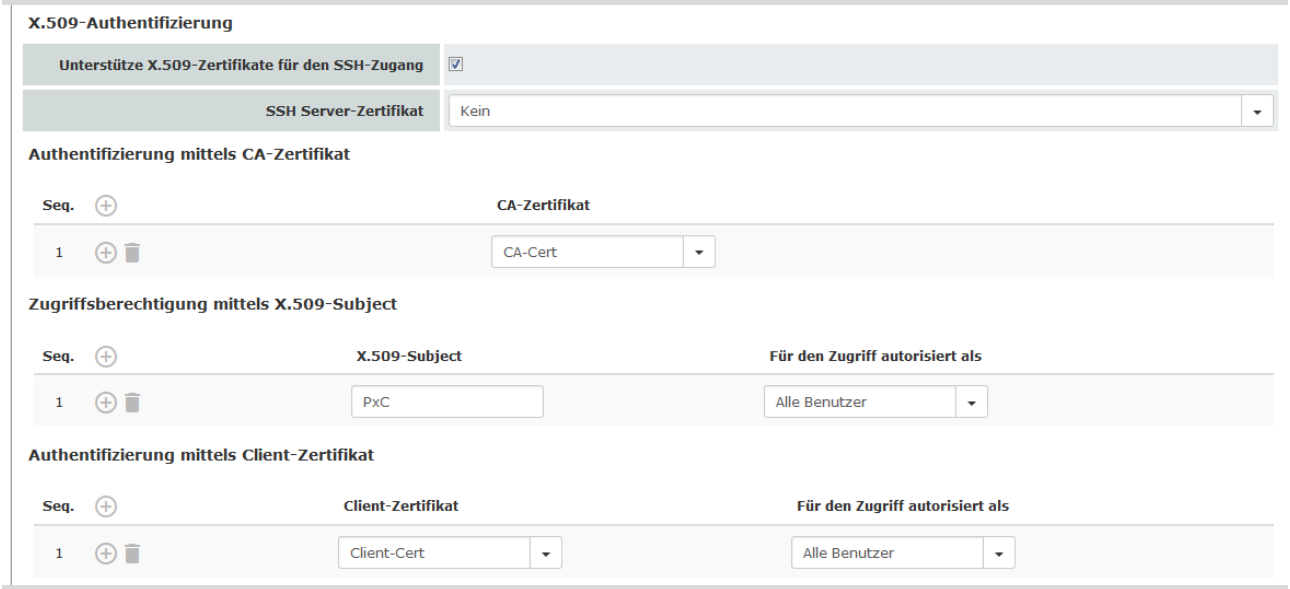
Wenn der Gültigkeitszeitraum des Client-Zertifikats vom mGuard geprüft wird (siehe „Zertifikatseinstellungen“ auf Seite 259), dann müssen irgend wann neue CA-Zertifikate am mGuard konfiguriert werden. Dies muss geschehen, bevor die SSH-Clienten ihre neuen Client-Zertifikate nutzen.

Wenn die CRL-Prüfung eingeschaltet ist (unter Authentifizierung >> Zertifikate >> Zertifikatseinstellungen), dann muss eine URL pro CA-Zertifikat vorgehalten werden, an der die entsprechende CRL verfügbar ist. Die URL und CRL müssen veröffentlicht werden, bevor der mGuard die CA-Zertifikate nutzt, um die Gültigkeit der von den VPN-Partnern vorgezeigten Zertifikate zu bestätigen.

Die hier angegebenen Regeln treten nur in Kraft, wenn die Funktion **Aktiviere SSH-Fernzugang** aktiviert ist. Zugriffe von *Intern* sind auch möglich, wenn diese Funktion deaktiviert ist.

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.

Wenn Sie Änderungen am Authentifizierungsverfahren vornehmen, sollten Sie den mGuard anschließenden 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 254).
SSH-Server-Zertifikat (2)	**Legt fest wie der mGuard den SSH-Client authentifiziert** Nachfolgend wird festgelegt, wie der mGuard die Authentizität des SSH-Clients prüft. Die Tabelle unten zeigt, welche Zertifikate dem mGuard zur Authentifizierung des SSH-Clients zur Verfügung stehen müssen, wenn der SSH-Client bei Verbindungsaufnahme eines der folgenden Zertifikatstypen vorzeigt: – ein von einer CA signiertes Zertifikat – ein selbst signiertes Zertifikat Zum Verständnis der nachfolgenden Tabelle siehe Kapitel „Authentifizierung >> Zertifikate“ .

Authentifizierung bei SSH

Die Gegenstelle zeigt vor:	Zertifikat (personenbezogen) von **CA signiert**	Zertifikat (personenbezogen) **selbst signiert**
Der mGuard authentifiziert die Gegenstelle anhand von...	⇕	⇕
	...allen CA-Zertifikaten, die mit dem von der Gegenstelle vorgezeigten Zertifikat die Kette bis zum Root-CA-Zertifikat bilden ggf. PLUS 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 anschließenden 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 471).*

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 / mobile

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, mobile*). 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).

Authentifizierung mittels Client-Zertifikat

Die Konfiguration ist in den folgenden Fällen erforderlich:

– SSH-Clients zeigen jeweils ein selbst signiertes Zertifikat vor.

– SSH-Clients zeigen jeweils ein von einer CA signiertes Zertifikat vor. Es soll eine Filterung erfolgen: Zugang erhält nur der, dessen Zertifikats-Kopie im mGuard als Gegenstellen-Zertifikat installiert ist und in dieser Tabelle dem mGuard als *Client-Zertifikat* zur Verfügung gestellt wird.

  Dieser Filter ist dem *Subject*-Filter darüber **nicht** nachgeordnet, sondern ist auf gleicher Ebene angesiedelt, ist also dem *Subject*-Filter mit einem logischen ODER beigeordnet.

Der Eintrag in diesem Feld legt fest, welches Client-Zertifikat (Gegenstellen-Zertifikat) der mGuard heranziehen soll, um die Gegenstelle, den SSH-Client, zu authentifizieren.

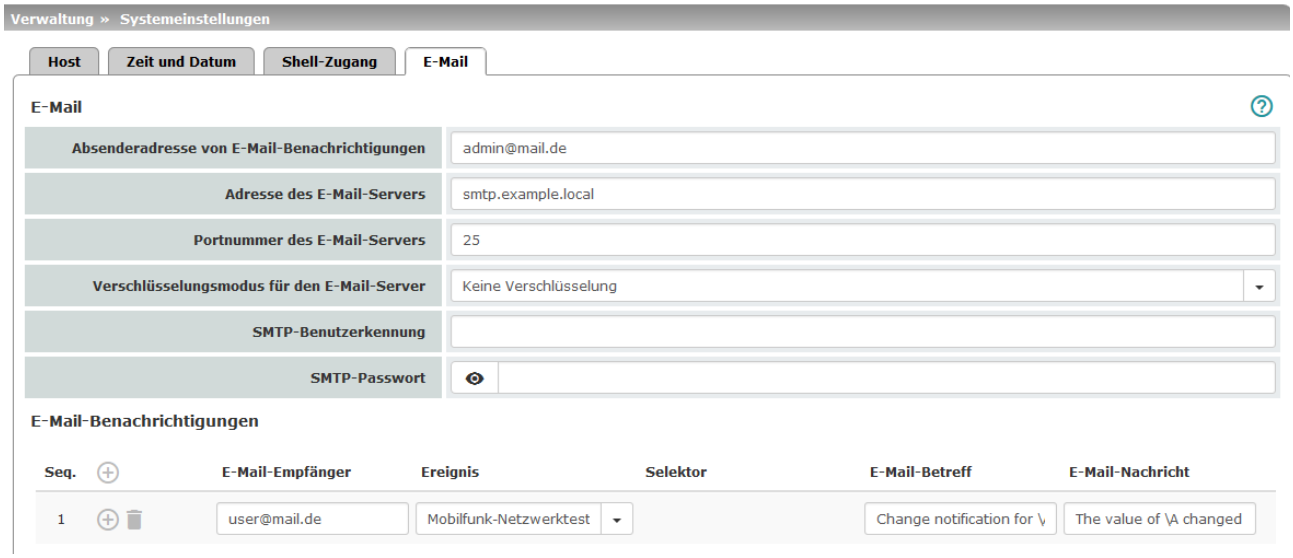
Dazu in der Auswahlliste eines der Client-Zertifikate auswählen. Die Auswahlliste stellt die Client-Zertifikate zur Wahl, die in den mGuard unter Menüpunkt *„Authentifizierung >> Zertifikate“* geladen worden sind.

Wenn Sie Änderungen am Authentifizierungsverfahren vornehmen, sollten Sie den mGuard anschließenden 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 / mobile** 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, mobile*). 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).

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
Verschlüsselungsmodus für den E-Mail-Server	**Keine Verschlüsselung / TLS-Verschlüsselung / TLS-Verschlüsselung mit StartTLS** Verschlüsselungsmodus für den E-Mail-Server
SMTP-Benutzerkennung	Benutzerkennung (Login)
SMTP-Passwort	Passwort für den E-Mail-Server

Verwaltung >> Systemeinstellungen >> E-Mail [...]		
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 70.
	Selektor	Hier kann eine konfigurierte VPN-Verbindung ausgewählt werden, die per E-Mail überwacht wird.
	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.
	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/ext1/ok	yes
	Konnektivitätsprüfung fehlgeschlagen		no
Gültigkeit der Positionsdaten	Ortungsdaten nicht gültig	/gps/valid	no
	Ortungsdaten gültig		yes
Telefonnummer und Inhalt der letzten eingehenden SMS		/gsm/incoming_sms	
Roaming-Status des Mobilfunkmodems	Beim eigenen Netzanbieter registriert	/gsm/roaming	no
	Bei fremdem Netzanbieter registriert		yes
	Nicht registriert		unknown
Mobilfunk-Registrierungszustand	Nicht im Mobilfunknetz registriert	/gsm/service	no
	Im Mobilfunknetz registriert		yes
Derzeit verwendeter SIM-Schacht	Verwende SIM 1	/gsm/selected_sim	1
	Verwende SIM 2		2
	SIM Schnittstelle deaktiviert		0
Mobilfunk-Betriebszustand der Fallback-SIM	Normaler Betrieb (Erste SIM)	/gsm/sim_fallback	no
	Fallback-Betrieb (Zweite SIM)		yes
Mobilfunk-Netzwerktests	Netzwerk-Tests sind deaktiviert	/gsm/network_probe	disabled
	Netzwerk-Tests sind aktiviert		enabled
	Netzwerk-Tests schlugen fehl		failed
	Netzwerk-Tests waren erfolgreich		succeeded
Zustand des Alarmausgangs	Alarmausgang geschlossen / high [OK]	/ihal/contact	close
	Alarmausgang ist offen / low [FEHLER]		open

Tabelle 4-2 Ereignistabelle

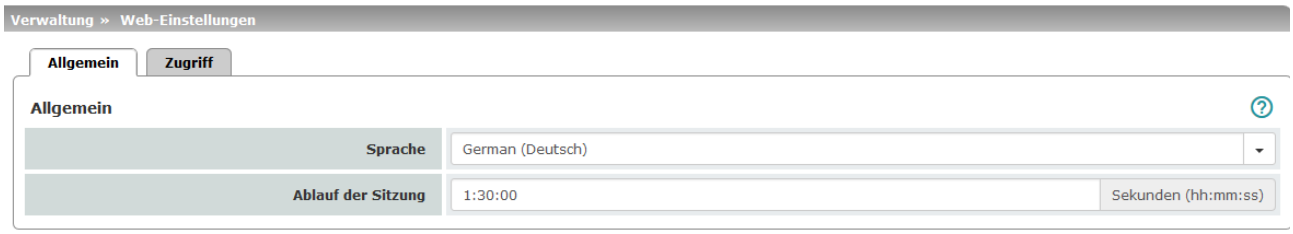
Klartext		Maschinenlesbar	
\A = Ereignis	**\V = Wert**	**\a = Ereignis**	**\v = Wert**
Aktivierungsgrund des Alarmausgangs	Kein Alarm	/ihal/contactreason	
	Keine Verbindung am externen Interface		link_ext
	Keine Verbindung am internen Interface		link_int
	Stromversorgung 1 defekt		psu1
	Stromversorgung 2 defekt		psu2
	Boardtemperatur außerhalb des konfigurierten Bereichs		temp
	Redundanz Konnektivitätsprüfung fehlgeschlagen		ccheck
	Das interne Modem ist offline		modem
	Keine Verbindung am LAN2-Interface		link_swp0
	Keine Verbindung am LAN3-Interface		link_swp1
	Keine Verbindung am LAN1-Interface		link_swp2
	Keine Verbindung am LAN4-Interface		link_swp3
	Keine Verbindung am LAN5-Interface		link_swp4
	Keine Verbindung am DMZ-Interface		link_dmz
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	Service Eingang/CMD1 aktiviert	/ihal/service/cmd1	on
	Service Eingang/CMD1 deaktiviert		off
Zustand des Eingangs/ CMD 2	Service Eingang/CMD2 aktiviert	/ihal/service/cmd2	on
	Service Eingang/CMD2 deaktiviert		off
Zustand des Eingangs/ CMD 3	Service Eingang/CMD3 aktiviert	/ihal/service/cmd3	on
	Service Eingang/CMD3 deaktiviert		off
Temperaturzustand des Gerätes	Temperatur OK	/ihal/temperature/board_alarm	ok
	Temperatur zu heiß		hot
	Temperatur zu kalt		cold
Temporärer Zustand des sekundären externen Interfaces	In Bereitschaft	/network/ext2up	no
	Aushilfsweise aktiviert		yes
Verbindungsstatus Mobilfunk Zustand des Modems	Nicht verbunden	/network/modem/state	offline
	Einwahl		dialing
	Verbunden		online
	Warten nach Initialisierung		init

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
	Geht in Bereitschaft		becomes_standby
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

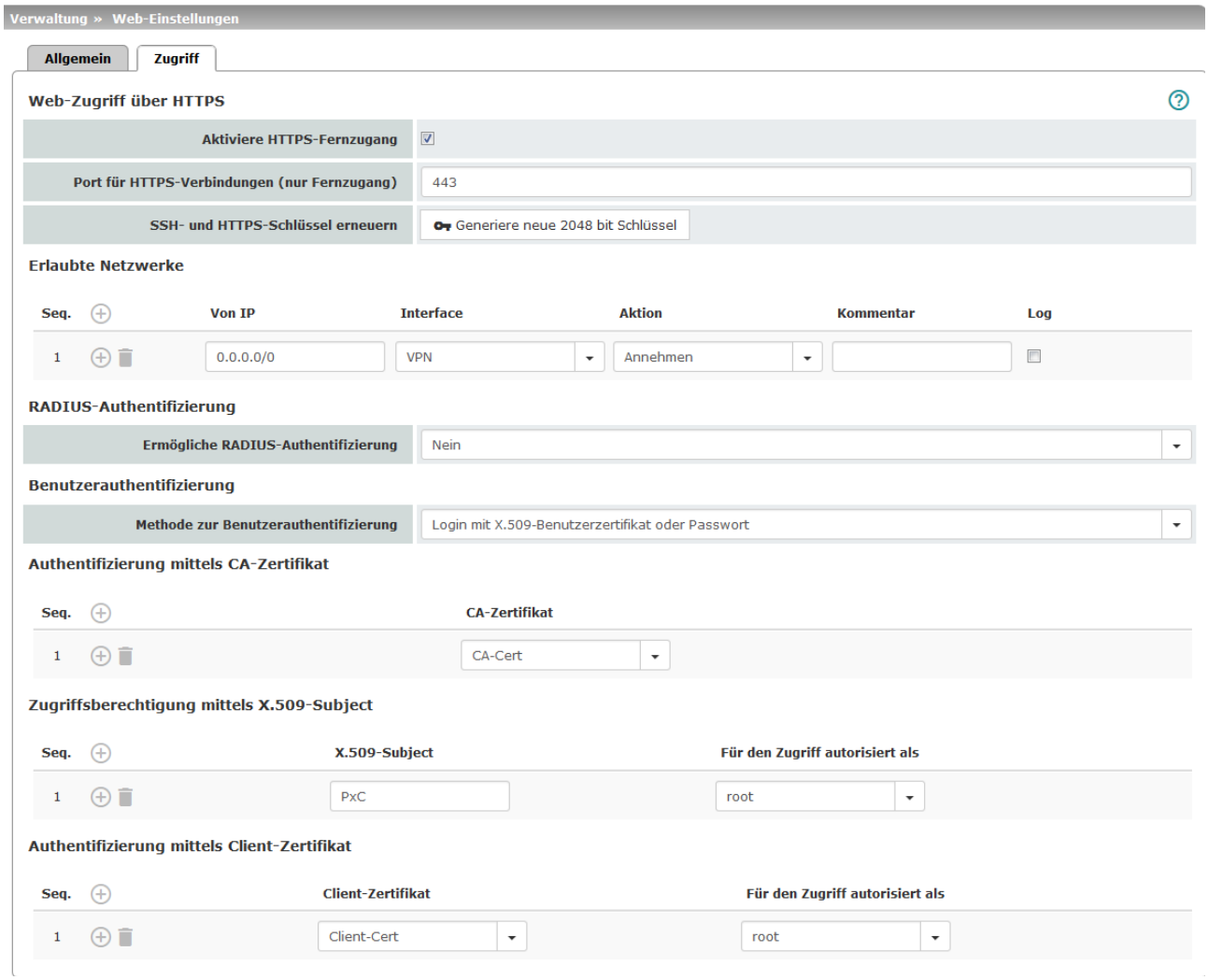
4.2 Verwaltung >> Web-Einstellungen

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 Webbrowser (z. B. Mozilla Firefox, Google Chrome, Microsoft Internet Explorer).

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

Wenn Sie Änderungen am Authentifizierungsverfahren vornehmen, sollten Sie den mGuard anschließenden 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: Der lokale HTTPS-Zugriff über das Interface „Intern“ ist unabhängig von der Aktivierung des HTTPS-Fernzugangs standardmäßig erlaubt.

Um Zugriffsmöglichkeiten auf den mGuard über das interne Interface differenziert festzulegen, müssen Sie die Funktion **Aktiviere HTTPS-Fernzugang** aktivieren und anschließend Firewall-Regeln für das interne Interface entsprechend definieren (siehe „Erlaubte Netzwerke“ auf Seite 76).

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 anschließenden 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 *Intern*, *VPN* und *Einwahl* möglich.

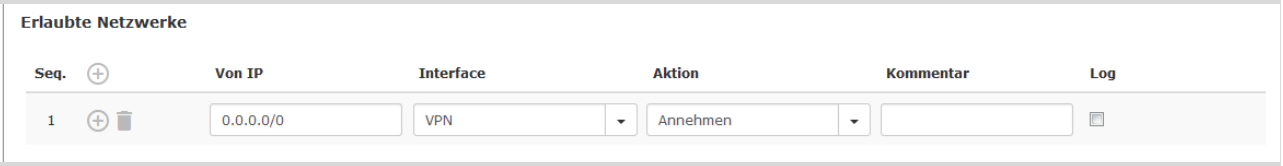
Um Zugriffsmöglichkeiten auf den mGuard differenziert festzulegen, müssen Sie die Firewall-Regeln für die verfügbaren Interfaces entsprechend definieren (siehe „Erlaubte Netzwerke“ auf Seite 76).

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, Extern 2, DMZ, VPN*, *GRE* und *Einwahl*. 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/
	SSH- und HTTPS-Schlüssel erneuern	**Generiere neue 2048 bit Schlüssel** Schlüssel, die mit einer älteren Firmware erstellt worden sind, sind möglicherweise schwach und sollten erneuert werden. • Klicken Sie auf diese Schaltfläche, um neue Schlüssel zu erzeugen. • Beachten Sie die Fingerprints der neu generierten Schlüssel. • Loggen Sie sich über HTTPS ein und vergleichen Sie die Zertifikat-Informationen, die vom Web-Browser zur Verfügung gestellt werden.
Erlaubte Netzwerke (Nur wenn **Aktiviere HTTPS-Fernzugang** aktiviert ist)	Sie können den HTTPS-Zugriff auf den mGuard mittels Firewall-Regeln auf ausgewählte Interfaces und Netzwerke beschränken. Die hier angegebenen Regeln treten nur in Kraft, wenn die Funktion **Aktiviere HTTPS-Fernzugang** aktiviert ist. Zugriffe von *Intern* sind auch möglich, wenn diese Funktion deaktiviert ist. 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. 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:**	

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



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 26.

Interface

(Die Auswahlmöglichkeit variiert je nach Gerät und installierten Lizenzen.)

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

Gibt an, für welches Interface die Regel gelten soll.

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

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

Legen Sie die Zugriffsmöglichkeiten nach Bedarf fest.

Wenn Sie Zugriffe über *Intern, DMZ, VPN* oder *Einwahl* 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 (werkseitige Voreinstellung).

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

RADIUS-Authentifizierung

(Dieser Menüpunkt gehört nicht zum Funktionsumfang von TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005, FL MGUARD RS2000.)

Benutzer können bei ihrer Anmeldung über einen RADIUS-Server authentifiziert werden. Nur bei den vordefinierten Benutzern *(root, admin, netadmin, audit, mobile* und *user)* wird das Passwort lokal geprüft.

Ermögliche RADIUS-Authentifizierung

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, mobile* und *user)* wird das Passwort lokal geprüft.

Wenn Sie Änderungen am Authentifizierungsverfahren vornehmen, sollten Sie den mGuard anschließenden 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).

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, mobile* und *user)* werden dann nicht mehr akzeptiert.

1 *Extern 2* und *Einwahl* nur bei Geräten mit serieller Schnittstelle (siehe „Netzwerk >> Interfaces“ auf Seite 135).

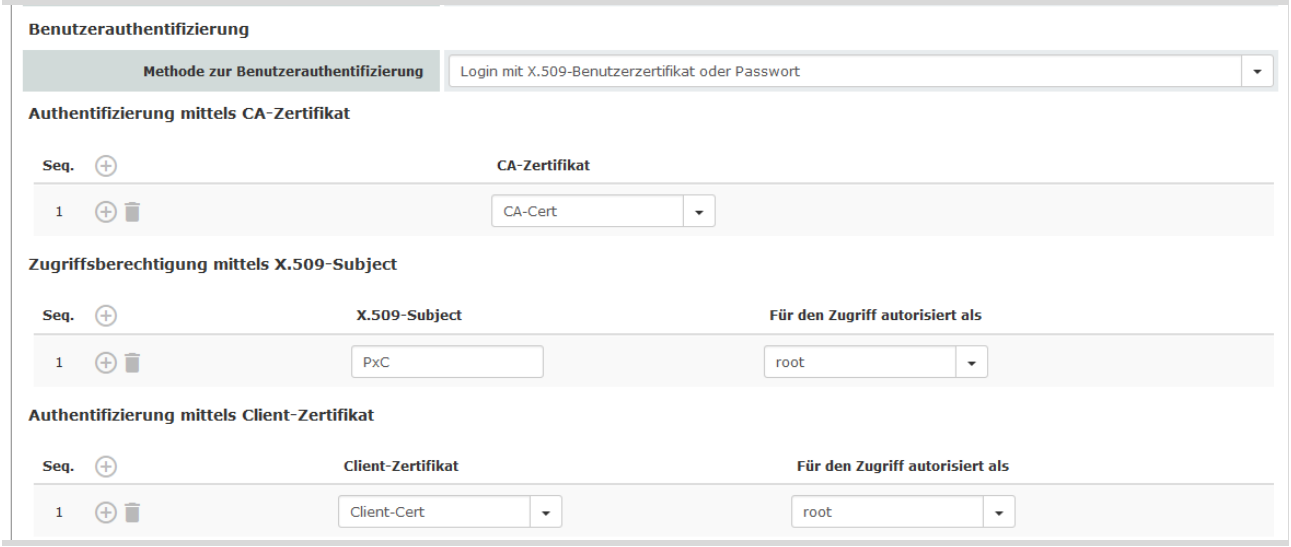
Verwaltung >> Web-Einstellung >> Zugriff

Benutzerauthentifizierung

(Dieser Menüpunkt gehört nicht zum Funktionsumfang von
TC MGUARD RS2000 3G,
TC MGUARD RS2000 4G,
FL MGUARD RS2005,
FL MGUARD RS2000.)

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 anschließenden 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 243). Außerdem gibt es die Möglichkeit der RADIUS-Authentifizierung (siehe Seite 250). Wenn Sie Passwörter ändern oder Änderungen am Authentifizierungsverfahren vornehmen, sollten Sie den mGuard anschließenden 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 selbst signiertes Zertifikat.

Zum Verständnis der nachfolgenden Tabelle siehe „Authentifizierung >> Zertifikate“ auf Seite 254.

X.509-Authentifizierung bei HTTPS

Die Gegenstelle zeigt vor:	Zertifikat (personenbezogen) von **CA signiert**[1]	Zertifikat (personenbezogen) **selbst signiert**
Der mGuard authentifiziert die Gegenstelle anhand von...	⇕	⇕
	...allen CA-Zertifikaten, die mit dem von der Gegenstelle vorgezeigten Zertifikat die Kette bis zum Root-CA-Zertifikat bilden ggf. PLUS 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 254).

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 anschließenden 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 471*).*

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

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

Mit * (Sternchen) im Feld *X.509-Subject* legen Sie fest, dass im vom 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.

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

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

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

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

Sollen bestimmte Attribute des Subjects ganz bestimmte Werte haben, damit der mGuard den 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.

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.

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

Für den Zugriff autorisiert als

root / admin / netadmin / audit / user / mobile

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

Für eine Beschreibung der Berechtigungsstufen *root, admin, mobile* und *user* siehe „Authentifizierung >> Administrative Benutzer“ auf Seite 243.

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

Authentifizierung mittels Client-Zertifikat

Die Konfiguration ist in den folgenden Fällen erforderlich:

– Von entfernt zugreifende Benutzer zeigen jeweils ein selbst signiertes Zertifikat vor.

– Von entfernt zugreifende Benutzer zeigen jeweils ein von einer CA signiertes Zertifikat vor. Es soll eine Filterung erfolgen: Zugang erhält nur der, dessen Zertifikats-Kopie im mGuard als Gegenstellen-Zertifikat installiert ist und in dieser Tabelle dem mGuard als *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 anschließenden 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.

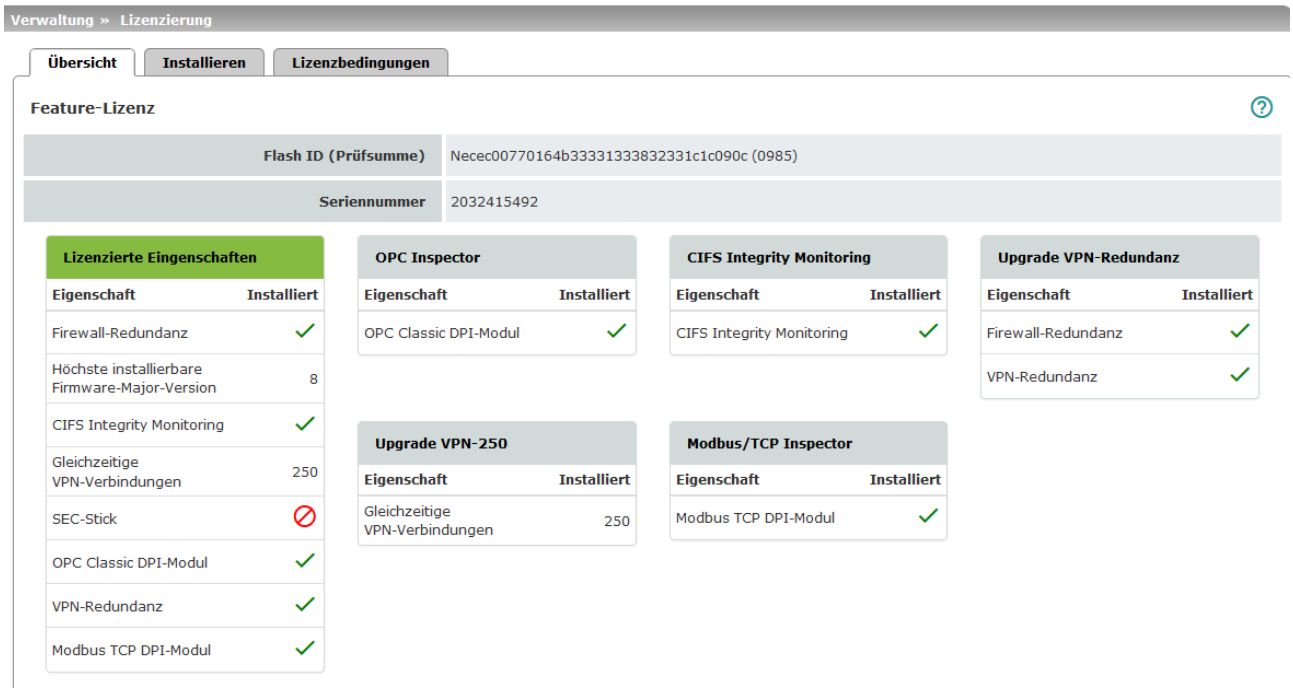
Weitere Informationen aus dem Zertifikat (Gültigkeitszeitraum, Aussteller und Verwendungszweck) werden bei der Prüfung nicht betrachtet.

Verwaltung >> Web-Einstellung >> Zugriff [...]		
	Für den Zugriff autorisiert als	**root / admin / netadmin / audit / user / mobile** Legt fest, welche Nutzer- bzw. Administratorrechte dem aus der Ferne zugreifenden Bediener eingeräumt werden. Für eine Beschreibung der Berechtigungsstufen *root, admin, mobile* und *user* siehe „Authentifizierung >> Administrative Benutzer“ auf Seite 243**.** Die Berechtigungsstufen *netadmin* und *audit* beziehen sich auf Zugriffsrechte bei Zugriffen mit dem mGuard device manager (FL MGUARD DM).

4.3 Verwaltung >> Lizenzierung

Zusätzliche optionale Lizenzen erhalten Sie bei Ihrer Bezugsquelle.

4.3.1 Übersicht



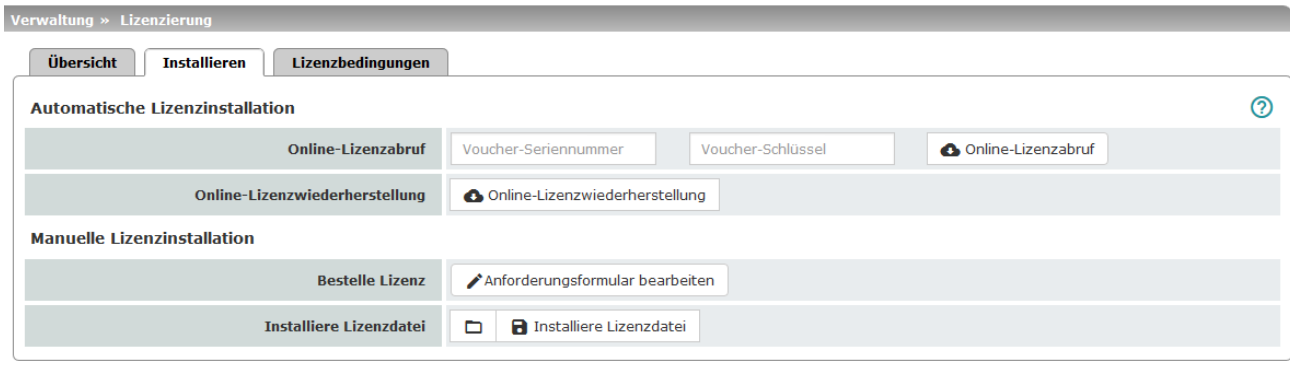
Ab Version 5.0 des mGuards bleiben Lizenzen auch nach Flashen der Firmware installiert.

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

Das gilt für Major-Release Upgrades, also z. B. bei einem Upgrade von Version 4.x.y zu Version 5.x.y zu Version 6.x.y.

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

4.3.2 Installieren



Eine VPN-1000- bzw. VPN-3000-Lizenz kann nur auf dem mGuard centerport (Innominate) und FL MGUARD CENTERPORT installiert werden.

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

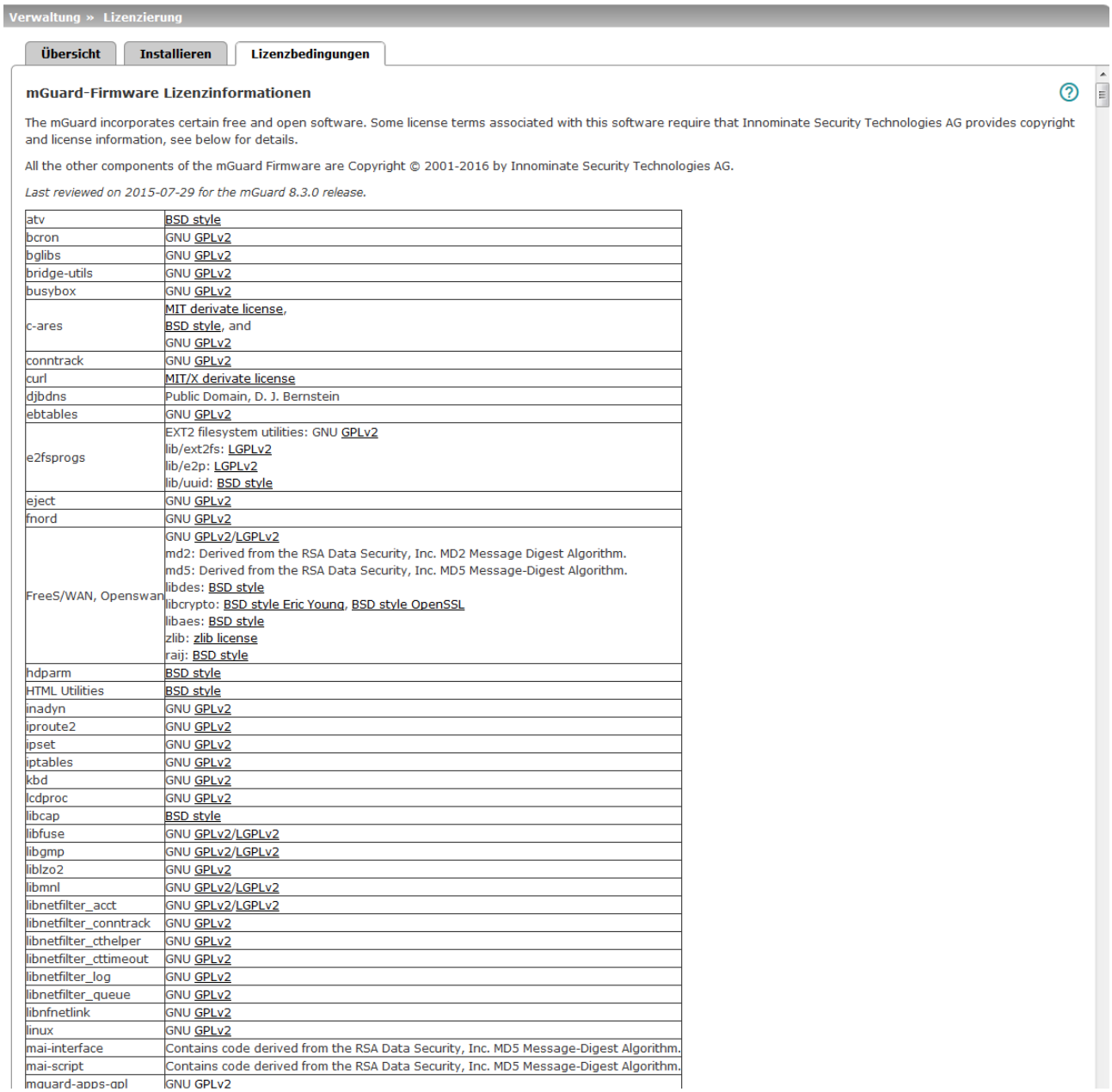
Im Voucher, den Sie beim Kauf des mGuards erhalten oder zusätzlich erworben haben, finden Sie eine Voucher-Seriennummer und einen Voucher-Schlüssel. Mit diesen können Sie die erforderliche Feature-Lizenzdatei anfordern, die Sie nach Erhalt installieren können.

Verwaltung >> Lizenzierung >> Installieren		
Automatische Lizenzinstallation	**Online-Lizenzabruf**	Geben Sie hier die Seriennummer, die auf dem Voucher aufgedruckt ist, sowie den dazugehörigen Voucher-Schlüssel ein, und klicken Sie anschließend auf die Schaltfläche „**Online-Lizenzabruf**“. Der mGuard baut nun eine Verbindung über das Internet auf und installiert bei einem gültigen Voucher die zugehörige Lizenz auf dem mGuard.
	Online-Lizenzwiederherstellung	Kann benutzt werden, falls die im mGuard installierten Lizenzen gelöscht wurden. Klicken Sie dazu auf die Schaltfläche „**Online-Lizenzwiederherstellung**“. Dann werden die Lizenzen, die zuvor für diesen mGuard ausgestellt waren, über das Internet vom Server geladen und installiert.
Manuelle Lizenzinstallation	**Bestelle Lizenz**	Nach einem Klick auf die Schaltfläche „Anforderungsformular bearbeiten“ wird über eine Internetverbindung ein Formular bereit gestellt, über das Sie die gewünschte Lizenz bestellen können. Geben Sie dort die folgenden Informationen ein: – **Voucher Serial Number:** Die Seriennummer, die auf Ihrem Voucher gedruckt ist – **Voucher Key:** Der Voucherschlüssel auf ihrem Voucher – **Flash Id:** Wird automatisch vorausgefüllt – **Serial Number:** Wird automatisch vorausgefüllt Nach dem Absenden des Formulars wird die Lizenzdatei zum Herunterladen bereitgestellt und kann im mGuard installiert werden (siehe „**Installiere Lizenzdatei“**).

Verwaltung >> Lizenzierung >> Installieren[...]		
	Installiere Lizenzdatei	Um eine Lizenz zu installieren, speichern Sie zunächst die Lizenz-Datei als separate Datei auf Ihrem Rechner und gehen dann wie folgt vor: • Klicken Sie auf die Schaltfläche „Keine Datei ausgewählt“. • Selektieren Sie die gewünschte Lizenzdatei (*.lic). Klicken Sie auf die Schaltfläche „**Installiere Lizenzdatei**“.

4.3.3 Lizenzbedingungen

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



Verwaltung » Lizenzierung

Übersicht | Installieren | Lizenzbedingungen

mGuard-Firmware Lizenzinformationen

The mGuard incorporates certain free and open software. Some license terms associated with this software require that Innominate Security Technologies AG provides copyright and license information, see below for details.

All the other components of the mGuard Firmware are Copyright © 2001-2016 by Innominate Security Technologies AG.

Last reviewed on 2015-07-29 for the mGuard 8.3.0 release.

atv	BSD style
bcron	GNU GPLv2
bglibs	GNU GPLv2
bridge-utils	GNU GPLv2
busybox	GNU GPLv2
c-ares	MIT derivate license, BSD style, and GNU GPLv2
conntrack	GNU GPLv2
curl	MIT/X derivate license
djbdns	Public Domain, D. J. Bernstein
ebtables	GNU GPLv2
e2fsprogs	EXT2 filesystem utilities: GNU GPLv2 lib/ext2fs: LGPLv2 lib/e2p: LGPLv2 lib/uuid: BSD style
eject	GNU GPLv2
fnord	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
hdparm	BSD style
HTML Utilities	BSD style
inadyn	GNU GPLv2
iproute2	GNU GPLv2
ipset	GNU GPLv2
iptables	GNU GPLv2
kbd	GNU GPLv2
lcdproc	GNU GPLv2
libcap	BSD style
libfuse	GNU GPLv2/LGPLv2
libgmp	GNU GPLv2/LGPLv2
liblzo2	GNU GPLv2
libmnl	GNU GPLv2/LGPLv2
libnetfilter_acct	GNU GPLv2/LGPLv2
libnetfilter_conntrack	GNU GPLv2
libnetfilter_cthelper	GNU GPLv2
libnetfilter_cttimeout	GNU GPLv2
libnetfilter_log	GNU GPLv2
libnetfilter_queue	GNU GPLv2
libnfnetlink	GNU GPLv2
linux	GNU GPLv2
mai-interface	Contains code derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm.
mai-script	Contains code derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm.
mguard-apps-gpl	GNU GPLv2

4.4 Verwaltung >> Update

Ob ein mGuard-Gerät auf die aktuelle oder eine andere Firmware-Version upgedatet werden kann, hängt von dessen Hardware-Architektur, der installierten Firmware-Version und installierten Lizenzen ab.

Update-Informationen finden Sie in den **Release Notes** der jeweiligen Firmware-Version und in dem **Anwenderhinweis** *FL/TC MGUARD-Geräte updaten und flashen* (verfügbar im PHOENIX CONTACT Web Shop oder unter help.mguard.com.).

Ein Update auf mGuard-Firmwareversion 8.8.x ist ausschließlich von Firmwareversionen ab 8.6.1 möglich.

Ein Update auf mGuard-Firmwareversion 8.6.1 ist von allen Firmwareversionen ab 7.6.0 möglich.

Geräte mit Mobilfunkeinheit und installierter **mGuard-Firmware <= 8.3.x** erhalten das **mGuard-Firmware-Update** zusammen mit dem **Firmware-Update der Mobilfunkeinheit**. Dadurch kann sich die Zeit des Updates auf mehrere Minuten verlängern (angezeigt durch das LED-Lauflicht im Bereich der Mobilfunkeinheit).

ACHTUNG: Eine Unterbrechung des Update-Vorgangs kann zu Schäden an der Mobilfunkeinheit führen.

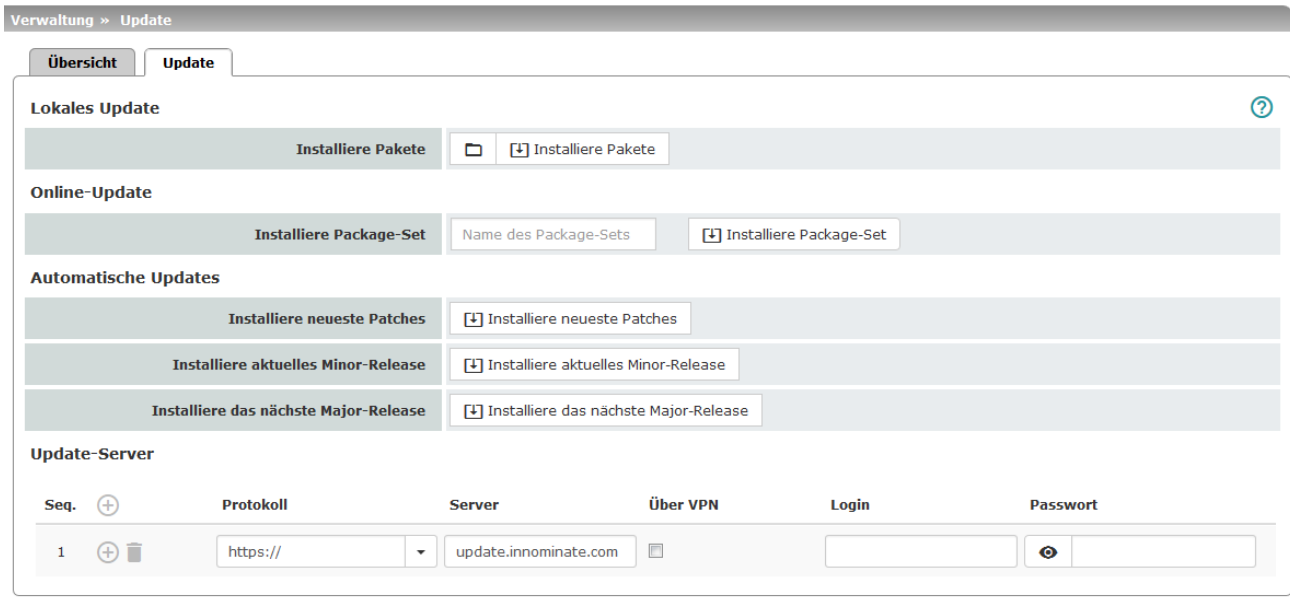
Schalten Sie das Gerät während des Update-Vorgangs nicht aus und unterbrechen Sie nicht die Stromversorgung des Geräts.

Ein laufender Update-Vorgang wird durch ein Lauflicht der drei LEDs (Signalstärke) neben den Antennenanschlüssen des Geräts signalisiert.

4.4.1 Übersicht

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

4.4.2 Update



Firmware-Updates mit eingeschalteter Firewall-Redundanz

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

Ausnahme hiervon sind die folgenden Geräte:

– FL MGUARD RS
– FL MGUARD SMART 533/266
– FL MGUARD PCI 533/266
– FL MGUARD BLADE
– mGuard delta (Innominate)

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

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

Firmware-Update durchführen

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

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

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

Abhängig von der Größe des Updates, kann dieses mehrere Minuten dauern.

Falls zum Abschluss des Updates ein Neustart erforderlich sein sollte, werden Sie durch eine Nachricht darauf hingewiesen.

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 Firmwareversion (siehe auch **Anwenderhinweis** *Update FL/TC MGUARD-Geräte* – AH DE MGUARD UPDATE). • **Beispiel**: *update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz*Dann die Schaltfläche **Installiere Pakete** klicken. Für Geräte mit Mobilfunkeinheit und installierter **mGuard-Firmwareversion <= 8.3.x** gilt: Ein lokales Update auf eine **mGuard-Firmwareversion 8.4.0 oder höher** ist nicht möglich, da die dazu notwendige Aktualisierung der Modem-Firmware nicht lokal durchgeführt werden kann. Führen Sie in den oben genannten Fällen ein **Online Update** oder **Flash-Update** durch.
Online-Update	**Installiere Package Set**	Um ein Online-Update durchzuführen, gehen Sie wie folgt vor: • Stellen Sie sicher, dass unter **Update-Server** mindestens ein gültiger Eintrag vorhanden ist. Die dafür nötigen Angaben haben Sie von Ihrem Lizenzgeber erhalten. • Geben Sie den Namen des Package-Sets ein. Der Name des Package Sets ist abhängig von der aktuell installierten Firmwareversion (siehe auch Anwenderhinweis „Update FL/TC MGUARD“ - AH DE MGUARD UPDATE). Beispiel: *update-8.{0-5}-8.6.1.default* • Dann die Schaltfläche **Installiere Package-Set** klicken.

Verwaltung >> Update [...]

Automatische Updates

Dieses ist eine Variante des Online-Updates, bei welcher der mGuard das benötigte Package-Set eigenständig ermittelt.

Ab mGuard-Firmwareversion 8.4 kann ein automatisches Update über die konfigurierten Update-Server auch auf der Kommandozeile gestartet werden (siehe „Kommandozeilen-Tool „mg““ auf Seite 478).

– 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 8.0.**1** ist ein Patch-Release zur Version 8.0.**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 8.**1.0** ist ein Minor-Release zur Version 8.**0.1**.

Installiere das nächste Major-Release

Die Version **8**.6.0 ist ein Major-Release zur Version **7**.6.8.

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.

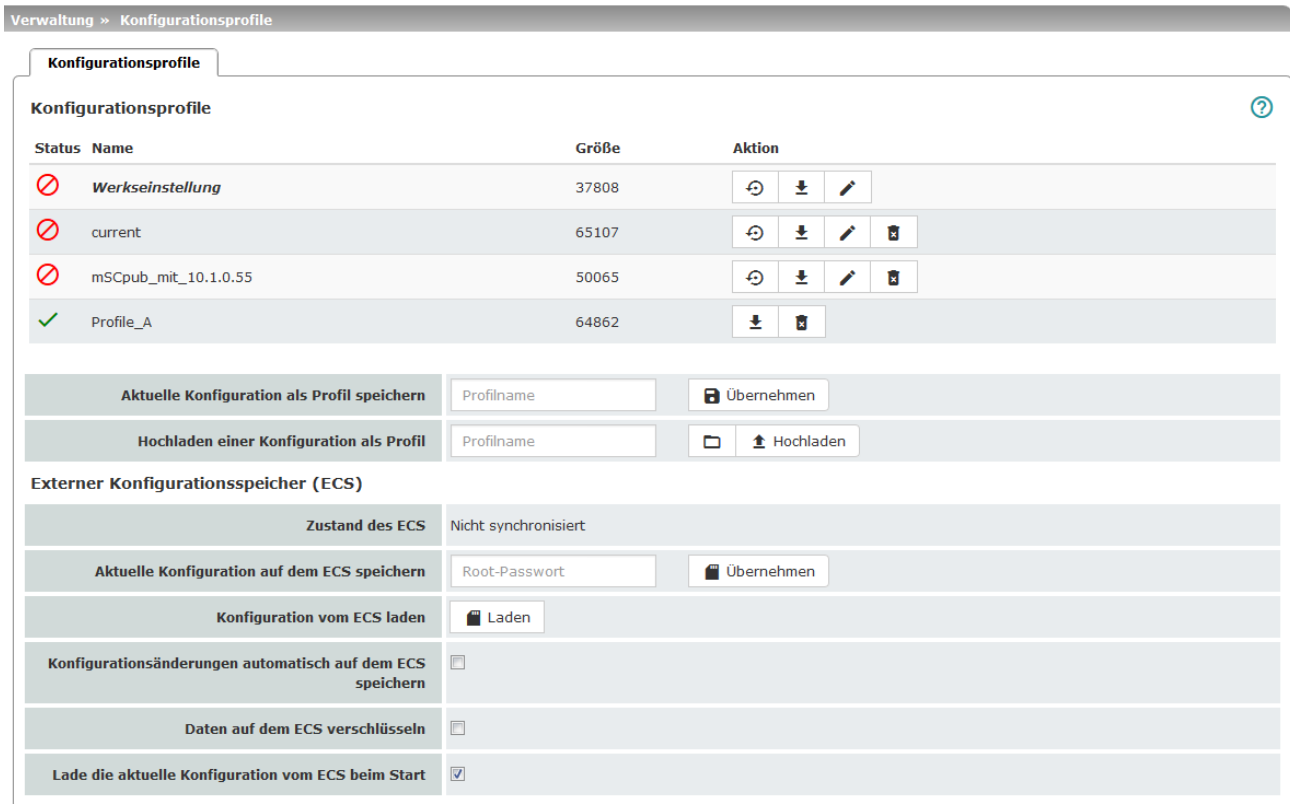
Server

Hostname oder IP-Adresse des Servers, der die Update-Dateien bereitstellt.

Verwaltung >> Update [...]		
	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.

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.

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

Konfigurationsprofile können bei bestimmten Modellen auch auf einem externen Konfigurationsspeicher (ECS) abgelegt werden.

– **SD-Karte:** TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS4004/RS2005, FL MGUARD RS4000/RS2000, FL MGUARD DELTA, FL MGUARD PCI(E)4000, FL MGUARD CENTERPORT
– **V.24/USB-Speicherstick:**, mGuard centerport (Innominate), FL MGUARD CENTERPORT
– **MEM PLUG**: FL MGUARD GT/GT

  Unverschlüsselte Konfigurationsprofile können beim FL MGUARD GT/GT auf dem externen Konfigurationsspeicher (**MEM PLUG**) abgelegt werden, der an die M12-Buchse des Geräts angeschlossen wird. Der MEM PLUG liegt in zwei Versionen mit unterschiedlicher Speicherkapazität vor (FL MEM PLUG und FL MEM PLUG 2).

Die Speicherkapazität der MEM PLUGs ist kleiner als die Speicherkapazität des mGuard-Geräts.
Komplexe Konfigurationen z. B. mit einer großen Anzahl konfigurierter Firewall-Regeln und/oder VPN-Verbindungen können zu großen Konfigurationsprofilen führen, für die die Speicherkapazität eines MEM PLUG nicht ausreichend ist.
Verwenden Sie zur Sicherung Ihrer Konfigurationen FL MEM PLUG 2 mit höherer Kapazität (Bestellnummer: 1032962), um das Risiko einer nicht ausreichenden Speicherkapazität zu minimieren.

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

Ab mGuard-Firmwareversion 7.6.1 können bei mGuard-Geräten der Plattform 2 (nicht bei FL MGUARD GT/GT) Konfigurationsprofile auf dem mGuard verschlüsselt 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 101.)

Recovery-Prozedur

Ab Firmware 8.4.0 wird vor der Durchführung einer Recovery-Prozedur 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.

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

Verwaltung >> Konfigurationsprofile [...]

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.

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.)

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.

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.

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.

Externer Konfigurationsspeicher (ECS)

Auf dem mGuard abgespeicherte Konfigurationsprofile können auf externe Konfigurationsspeicher (ECS) exportiert und von diesen erneut in mGuard-Geräte importiert werden.

Je nach verwendetem Gerät und technischer Voraussetzung dienen verschiedene externe Konfigurationsspeicher (u. a. SD-Karten oder USB-Flash-Laufwerke) als Speichermedien. Die exportierte Datei erhält die Dateiendung „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.net/products

Um die Datei in ein mGuard-Gerät zu importieren, muss die SD-Karte oder das USB-Flash-Laufwerk in den mGuard eingelegt bzw. angeschlossen 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.

Verwaltung >> Konfigurationsprofile [...]

Zustand des ECS	Der aktuelle Zustand wird dynamisch aktualisiert. (Siehe „Zustand des ECS“ in „Ereignistabelle“ auf Seite 70).
Aktuelle Konfiguration auf dem ECS speichern (Nur beim TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS4004/RS2005, FL MGUARD RS4000/RS2000, FL MGUARD GT/GT, FL MGUARD DELTA, FL MGUARD PCI(E)4000, mGuard centerport (Innominate) und FL MGUARD CENTERPORT)	Beim Austausch durch ein Ersatzgerät kann das Konfigurationsprofil des ursprünglichen Gerätes mit Hilfe des ECS übernommen werden. Voraussetzung hierfür ist, dass das Ersatzgerät noch „root“ als Passwort für den Benutzer „root“ verwendet. Wenn das Root-Passwort auf dem Ersatzgerät ungleich „root“ ist, dann muss dieses Passwort in das Feld **„Root-Passwort“** eingegeben werden. Übernehmen Sie die Eingabe mit einem Klick auf die Schaltfläche **Übernehmen**. Die Speicherkapazität der MEM PLUGs ist kleiner als die Speicherkapazität des mGuard-Geräts. Komplexe Konfigurationen z. B. mit einer großen Anzahl konfigurierter Firewall-Regeln und/oder VPN-Verbindungen können zu großen Konfigurationsprofilen führen, für die die Speicherkapazität eines MEM PLUGS nicht ausreichend ist. Verwenden Sie zur Sicherung Ihrer Konfigurationen FL MEM PLUG 2 (Bestellnummer: 1032962), um das Risiko einer nicht ausreichenden Speicherkapazität zu minimieren.
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.

Verwaltung >> Konfigurationsprofile [...]

Konfigurationsänderungen automatisch auf dem ECS speichern

(Nur beim TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS4004/RS2005, FL MGUARD RS4000/RS2000, FL MGUARD GT/GT, FL MGUARD DELTA, FL MGUARD PCI(E)4000, mGuard centerport (Innominate), FL MGUARD CENTERPORT)

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.

Das Speichern der Konfiguration auf einem ECS, insbesondere auf dem MEM PLUG, kann je nach Konfiguration mehrere Minuten dauern.

Auf dem MEM PLUG 2 dauert das Speichern in der Regel 16 Minuten oder länger.

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.

Auch wenn der ECS nicht angeschlossen, voll oder defekt ist, werden Konfigurationsänderungen ausgeführt. Entsprechende Fehlermeldungen erscheinen im Logging (siehe „Logging >> Logs ansehen“ auf Seite 431).

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

Daten auf dem ECS verschlüsseln

(Nur beim TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS4004/RS2005, FL MGUARD RS4000/RS2000, FL MGUARD PCI(E)4000, FL MGUARD DELTA, mGuard centerport (Innominate) und FL MGUARD CENTERPORT)

Bei aktivierter Funktion werden die Konfigurationsänderungen verschlüsselt auf einem ECS abgespeichert. Ab mGuard-Firmwareversion 7.6.1 können bei mGuard-Geräten der Plattform 2 (nicht bei FL MGUARD GT/GT) Konfigurationsprofile auf dem mGuard verschlüsselt werden. Damit wird der Rollout von mGuards erleichtert.

Sie können mehrere mGuard-Konfigurationen auf einer SD-Karte (beim mGuard centerport (Innominate), FL MGUARD CENTERPORT auch auf einem USB-Stick) 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.

Verwaltung >> Konfigurationsprofile [...]

	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. 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.

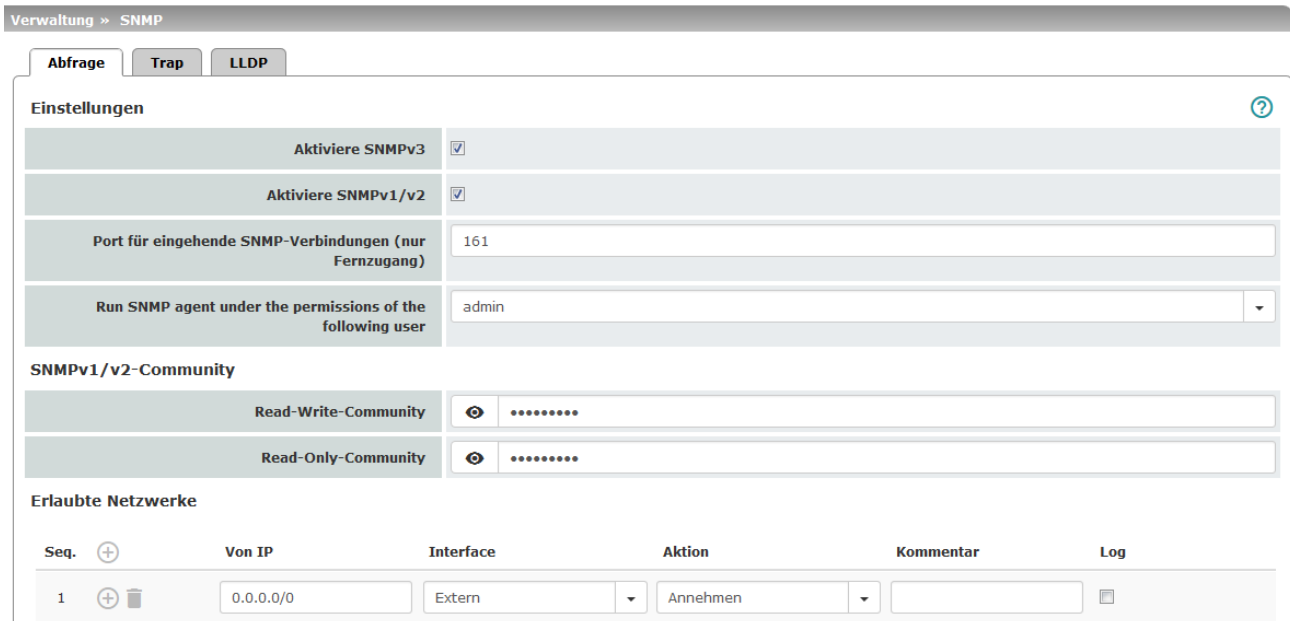
Das SNMP (Simple Network Management Protocol) wird vorzugsweise in komplexeren Netzwerken benutzt, um den Zustand und den Betrieb von Geräten zu überwachen oder zu konfigurieren.

Ab mGuard-Firmware 8.4 ist es 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.net/products.

4.6.1 Abfrage



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

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

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

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 des Fernzugangs ist der Zugriff über *Intern*, *Einwahl* 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!)

Ab mGuard-Firmwareversion 8.6.0 können die SNMPv3-Zugangsdaten **Benutzername** und **Passwort** 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 [...]

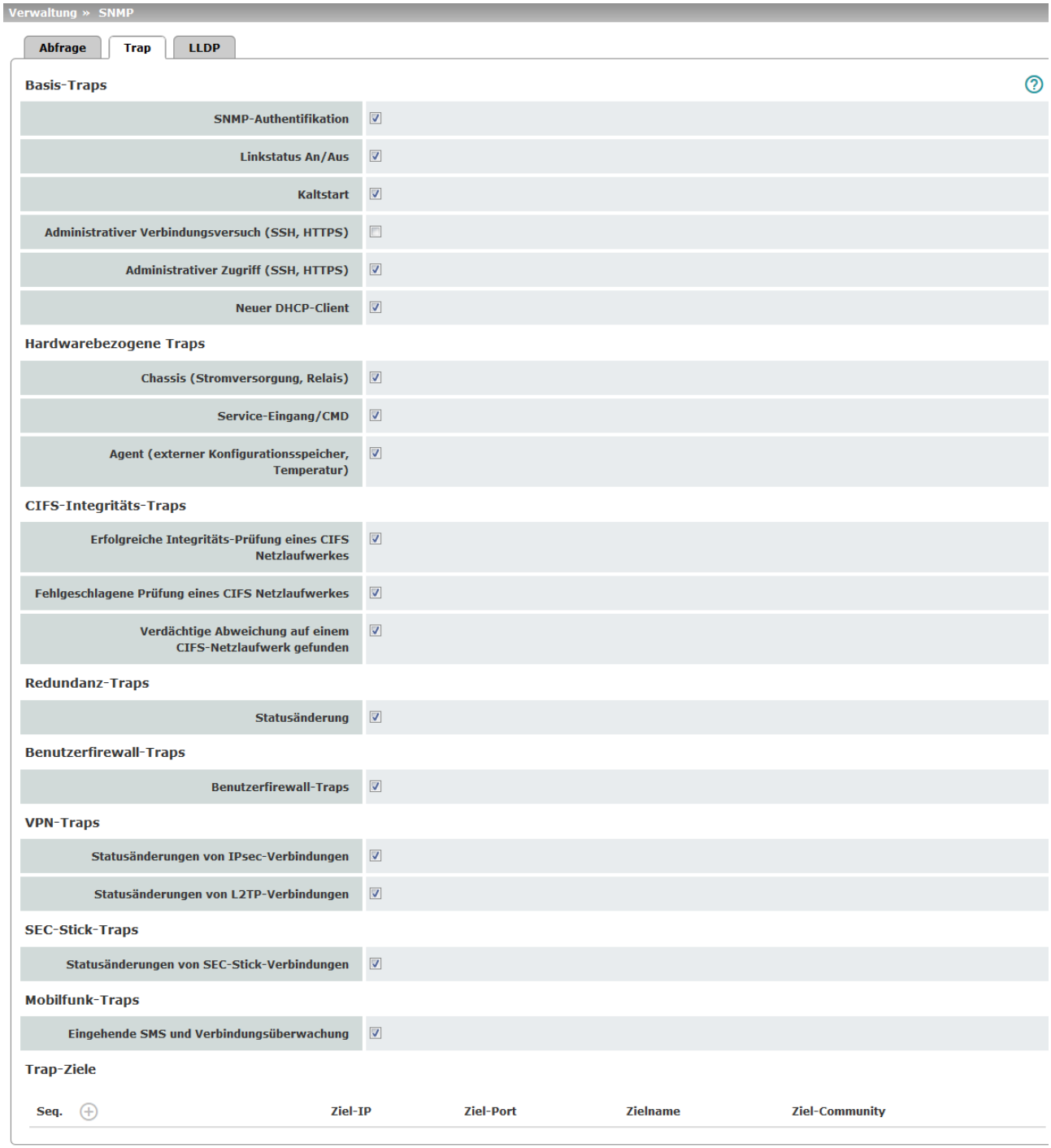
	Aktiviere SNMPv1/v2	Aktivieren Sie die Funktion, wenn Sie zulassen wollen, dass der mGuard per SNMPv1/v2 überwacht werden kann. Zusätzlich müssen Sie unter **SNMPv1/v2-Community** die Login-Daten angeben. Nach Aktivierung des Fernzugangs ist der Zugriff über *Intern*, *Einwahl* und *VPN* möglich. Um 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, Extern 2, DMZ, VPN, GRE* und *Einwahl*. 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. 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 26). – **0.0.0.0/0** bedeutet alle Adressen.
	Interface	**Intern / Extern / Extern 2 / DMZ / VPN / GRE / Einwahl**[1] Gibt an, für welches Interface die Regel gelten soll. Sind keine Regeln gesetzt oder greift keine Regel, gelten folgende Standardeinstellungen: SNMP-Überwachung ist erlaubt über *Intern, DMZ, VPN* und *Einwahl*. Zugriffe über *Extern*, *Extern 2* und *GRE* werden verwehrt. Legen Sie die Überwachungsmöglichkeiten nach Bedarf fest. **ACHTUNG:** Wenn Sie Zugriffe über *Intern, DMZ, VPN* oder *Einwahl* 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.

Verwaltung >> SNMP >> Abfrage [...]		
	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 (werkseitige Voreinstellung).

[1] *Extern 2* und *Einwahl* nur bei Geräten mit serieller Schnittstelle (siehe „Netzwerk >> Interfaces“ auf Seite 135).

4.6.2 Trap


Verwaltung » SNMP
Abfrage
Trap
LLDP
Basis-Traps
SNMP-Authentifikation
Linkstatus An/Aus
Kaltstart
Administrativer Verbindungsversuch (SSH, HTTPS)
Administrativer Zugriff (SSH, HTTPS)
Neuer DHCP-Client
Hardwarebezogene Traps
Chassis (Stromversorgung, Relais)
Service-Eingang/CMD
Agent (externer Konfigurationsspeicher, Temperatur)
CIFS-Integritäts-Traps
Erfolgreiche Integritäts-Prüfung eines CIFS Netzlaufwerkes
Fehlgeschlagene Prüfung eines CIFS Netzlaufwerkes
Verdächtige Abweichung auf einem CIFS-Netzlaufwerk gefunden
Redundanz-Traps
Statusänderung
Benutzerfirewall-Traps
Benutzerfirewall-Traps
VPN-Traps
Statusänderungen von IPsec-Verbindungen
Statusänderungen von L2TP-Verbindungen
SEC-Stick-Traps
Statusänderungen von SEC-Stick-Verbindungen
Mobilfunk-Traps
Eingehende SMS und Verbindungsüberwachung
Trap-Ziele
Seq.
Ziel-IP
Ziel-Port
Zielname
Ziel-Community

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 **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 354), 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 355), 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.

Verwaltung >> SNMP >> Trap [...]

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 öffnet per SSH oder über die serielle Schnittstelle. Der Trap enthält die IP-Adresse der Login-Anfrage. Wurde diese Anfrage über die serielle Schnittstelle abgesetzt, lautet der Wert 0.0.0.0.
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.

Verwaltung >> SNMP >> Trap [...]

Hardwarebezogene Traps

(Nur
TC MGUARD RS4000/RS2000 3G,
TC MGUARD RS4000/RS2000 4G,
FL MGUARD RS4004/RS2005,
FL MGUARD RS4000/RS2000,
FL MGUARD RS)

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).

Service-Eingang/CMD

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.

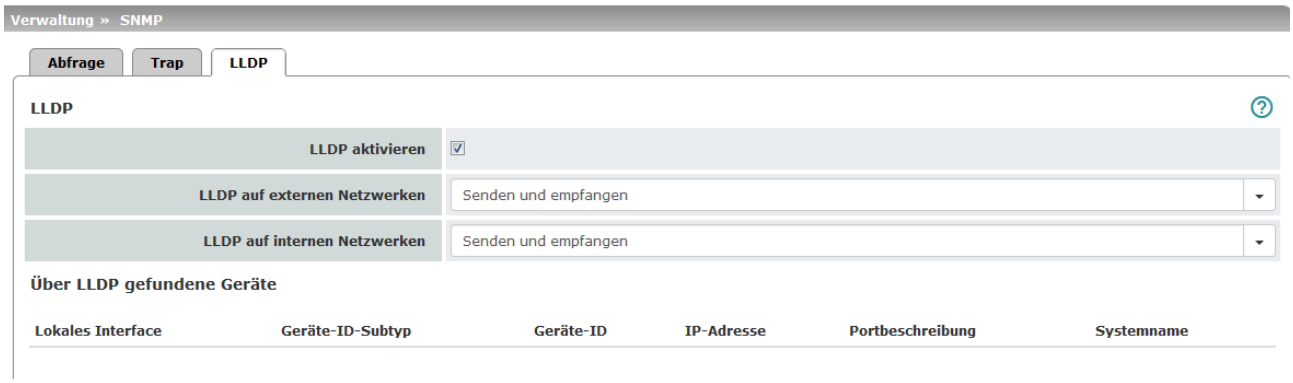
Verwaltung >> SNMP >> Trap [...]		
FL MGUARD BLADE Controller-Traps (Nur FL MGUARD BLADE)	**Statusänderung von Blades** (Umstecken, Ausfall)	**Trap-Beschreibung** – enterprise-oid : mGuardTrapBladeCTRL – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapBladeCtrlPowerStatus (2) – additional : mGuardTrapBladeRackID, mGuardTrapBladeSlotNr, mGuardTrapBladeCtrlPowerStatus Wird gesendet, wenn der Stromversorgungsstatus des Blade Pack wechselt. – enterprise-oid : mGuardTrapBladeCTRL – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapBladeCtrlRunStatus (3) – additional : mGuardTrapBladeRackID, mGuardTrapBladeSlotNr, mGuardTrapBladeCtrlRunStatus Wird gesendet, wenn der Blade-Ausführungsstatus wechselt.
	Neukonfiguration von Blades (Backup/Restore)	**Trap-Beschreibung** – enterprise-oid : mGuardTrapBladeCtrlCfg – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapBladeCtrlCfgBackup (1) – additional : mGuardTrapBladeRackID, mGuardTrapBladeSlotNr, mGuardTrapBladeCtrlCfgBackup Wird gesendet bei Auslösung des Konfigurations-Backups zum FL MGUARD BLADE-Controller. – enterprise-oid : mGuardTrapBladeCtrlCfg – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapBladeCtrlCfgRestored 2 – additional : mGuardTrapBladeRackID, mGuardTrapBladeSlotNr, mGuardTrapBladeCtrlCfgRestored Wird gesendet bei Auslösung der Konfigurations-Wiederherstellung vom FL MGUARD BLADE-Controller.
CIFS-Integritäts-Traps (Nicht beiTC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005, FL MGUARD RS2000)	**Erfolgreiche Integritäts-Prüfung eines CIFS-Netzlaufwerkes**	**Trap-Beschreibung** – enterprise-oid : mGuardTrapCIFSScan – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapCIFSScanInfo (1) – additional : mGuardTResCIFSShare, mGuardTResCIFSScanError, mGuardTResCIFSNumDiffs Wird gesendet, wenn die CIFS-Integritätsprüfung erfolgreich abgeschlossen worden ist.

Verwaltung >> SNMP >> Trap [...]		
	Fehlgeschlagene Prüfung eines CIFS-Netzlaufwerkes	**Trap-Beschreibung** – enterprise-oid : mGuardTrapCIFSScan – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapCIFSScanFailure (2) – additional : mGuardTResCIFSShare, mGuardTResCIFSScanError, mGuardTResCIFSNumDiffs Wird gesendet, wenn CIFS-Integritätsprüfung fehlgeschlagen ist.
	Verdächtige Abweichung auf einem CIFS-Netzlaufwerk gefunden	**Trap-Beschreibung** – enterprise-oid : mGuardTrapCIFSScan – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapCIFSScanDetection (3) – additional : mGuardTResCIFSShare, mGuardTResCIFSScanError, mGuardTResCIFSNumDiffs Wird gesendet, wenn bei der CIFS-Integritätsprüfung eine Abweichung festgestellt worden ist.
Redundanz-Traps (Nicht bei TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005, FL MGUARD RS2000)	**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.

Verwaltung >> SNMP >> Trap [...]		
Benutzerfirewall-Traps (Nicht bei TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005, FL MGUARD RS2000)	**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 – enterprise-oid : mGuardTrapUserFirewall – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapUserFirewallAuthError TRAP-TYPE (3) – additional : mGuardTResUserFirewallUsername, mGuardTResUserFirewallSrcIP, mGuardTResUserFirewallAuthenticationMethod Wird gesendet bei einem Authentifizierungs-Fehler.
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.
Mobilfunk-Traps (Nur TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G)	**Eingehende SMS und Verbindungsüberwachung**	Ermöglicht Traps für die Mobilfunkverbindung. Traps werden gesendet, wenn eine SMS empfangen wird oder die Mobilfunkverbindung ausfällt.
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



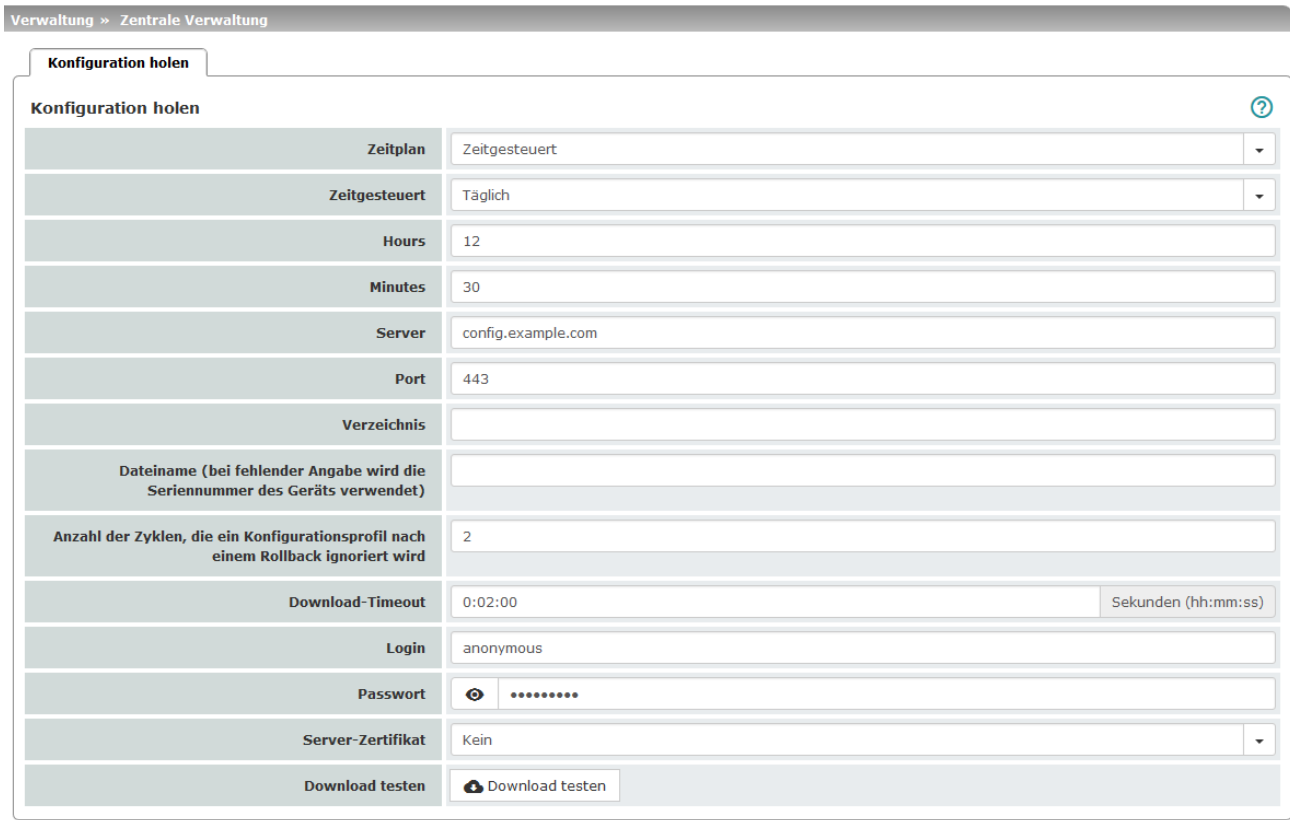
Mit LLDP (Link Layer Discovery Protocol, IEEE 802.1AB/D13) können mit geeigneten Abfragemethoden Informationen über die Netzwerk-Infrastruktur automatisch ermittelt werden. Ein System, das LLDP benutzt, kann so konfiguriert werden, dass es auf LLDP-Informationen lauscht oder LLDP-Informationen versendet. 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 45, „Zeit und Datum“ auf Seite 47). 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 selbst signiertes Zertifikat des Konfigurations-Servers angegeben werden oder
- das Wurzelzertifikat der CA (Certification Authority), welche das Zertifikat des Servers ausgestellt hat. Das gilt dann, wenn es sich beim Zertifikat des Konfigurations-Servers um ein von einer CA signiertes Zertifikat handelt (statt um ein selbst signiertes)

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 in der rechten Spalte angezeigt.

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

4.8 Verwaltung >> Service I/O

Dieses Menü steht **nur** auf dem **TC MGUARD RS4000/RS2000 3G**, **TC MGUARD RS4000/RS2000 4G**, **FL MGUARD RS4004/RS2005**, **FL MGUARD RS4000/RS2000**, **FL MGUARD RS**, **FL MGUARD GT/GT** zur Verfügung.

An einige mGuards könnten Servicekontakte (Service I/Os) angeschlossen werden.

- **TC MGUARD RS4000/RS2000 3G,**
- **TC MGUARD RS4000/RS2000 4G**
- **FL MGUARD RS4004/RS2005**
- **FL MGUARD RS4000/RS2000**
- **FL MGUARD RS**
- **FL MGUARD GT/GT**

Der Anschluss der Servicekontakte wird im Anwenderhandbuch zu den Geräten beschrieben (UM DE MGUARD DEVICES).

Eingang/CMD I1, CMD I2, CMD I3

An die Eingänge können Taster oder Ein-/Aus-Schalter angeschlossen werden. Es können ein oder mehrere frei wählbare VPN-Verbindungen oder Firewall-Regelsätze über den entsprechenden Schalter geschaltet werden. Auch eine Mischung von VPN-Verbindungen und Firewall-Regelsätzen ist möglich. Über die Web-Oberfläche wird angezeigt, welche VPN-Verbindungen und welche Firewall-Regelsätze an diesen Eingang gebunden sind.

Der Taster oder Ein-/Aus-Schalter dient zum Auf- und Abbau von zuvor definierten VPN-Verbindungen oder der Aktivierung von definierten Firewall-Regelsätzen.

Meldekontakt (Meldeausgang) ACK O1, O2

Sie können einstellen, ob bestimmte VPN-Verbindungen oder Firewall-Regelsätze überwacht und über LEDs angezeigt werden.

Wenn VPN-Verbindungen überwacht werden, zeigt eine leuchtende LED, dass diese VPN-Verbindungen bestehen.

Alarmausgang ACK O3

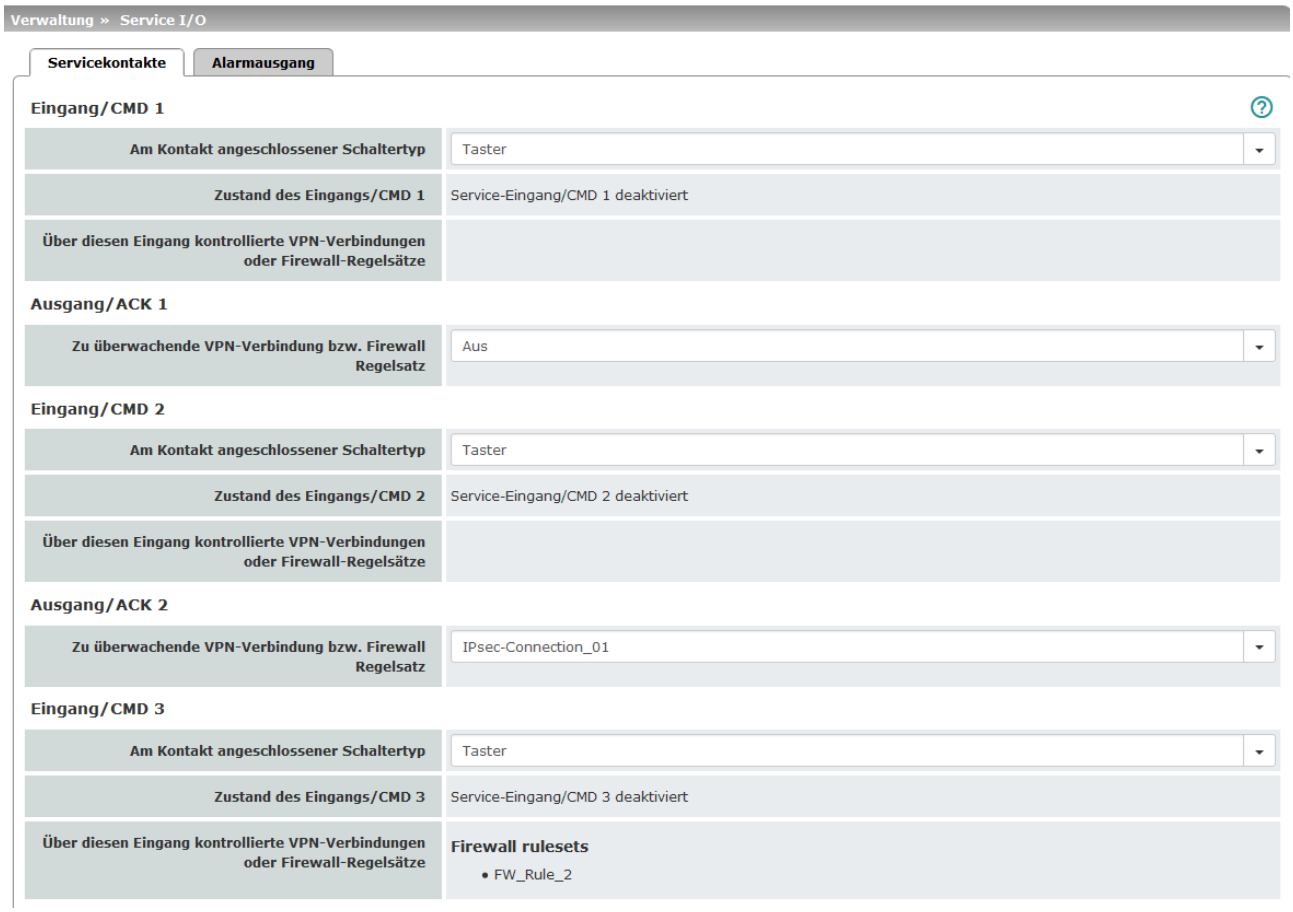
Der Alarmausgang überwacht die Funktion des mGuards und ermöglicht damit eine Ferndiagnose.

Die zugehörige LED leuchtet rot, wenn der Alarmausgang aufgrund eines Fehlers Low-Pegel einnimmt (invertierte Logik).

Durch den Alarmausgang wird folgendes gemeldet, wenn das aktiviert worden ist.

- Der Ausfall der redundanten Stromversorgung
- Überwachung des Link-Status der Ethernet-Anschlüsse
- Überwachung des Temperaturzustandes
- Überwachung des Verbindungsstatus der Redundanz
- Überwachung des Verbindungsstatus des internen Modems

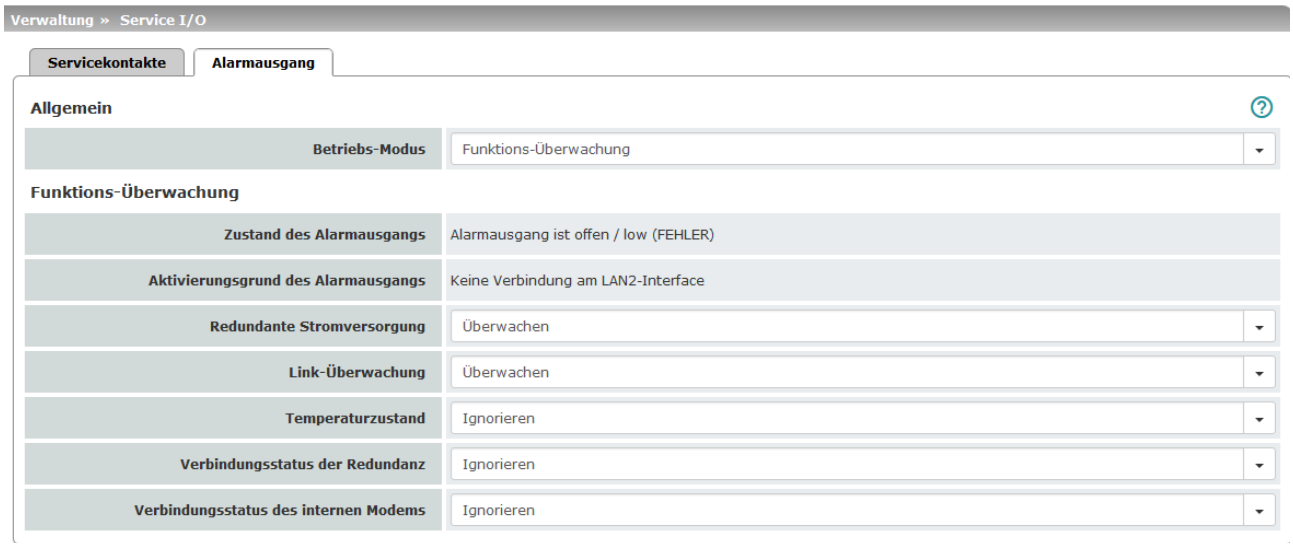
4.8.1 Servicekontakte



Verwaltung >> Service I/O>> Servicekontakte		
Eingang/CMD 1-3	**Am Kontakt angeschlossener Schaltertyp**	**Taster / Ein-/Aus-Schalter** Auswahl des Typs des angeschlossen Schalters.
	Zustand des Eingangs/CMD 1–3	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 FL MGUARD RS4000/RS2000, TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS4004/RS2005, FL MGUARD RS und FL MGUARD GT/GT verfügen 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	**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) signalisiert.

4.8.2 Alarmausgang

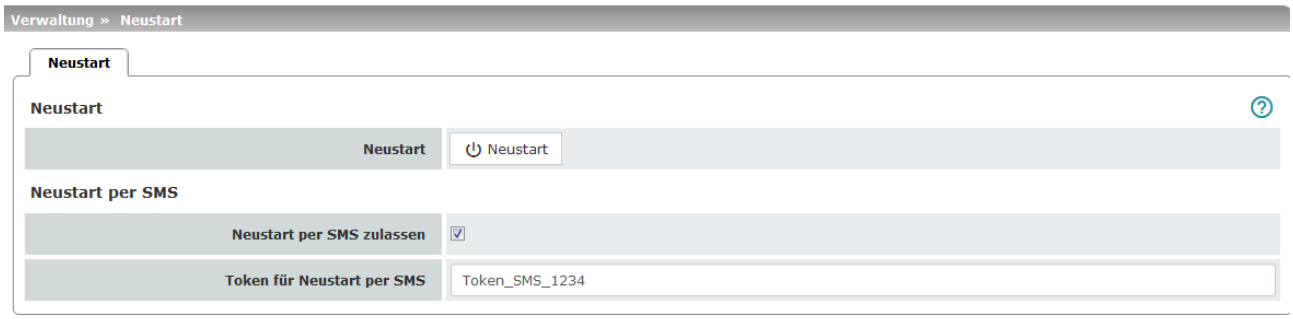


Verwaltung >> Service I/O >> Alarmausgang		
Allgemein	**Betriebsmodus**	**Funktions-Überwachung / Manuelle Einstellung** Der Alarmausgang kann automatisch durch die **Funktions-Überwachung** geschaltet werden (Standard) oder durch **Manuelle Einstellung**.
	Manuelle Einstellung	**Geschlossen / Offen (Alarm)** Hier kann der gewünschte Zustand des Alarmausgangs gewählt werden (zur Funktionskontrolle): Wird der Zustand manuell auf **Offen (Alarm)** gestellt, leuchtet die LED FAULT nicht rot (kein Alarm).
Funktions-Überwachung	**Aktueller Zustand**	Anzeige des Zustandes des Alarmausganges.
	Redundante Stromversorgung	Bei **Ignorieren** hat der Zustand der Stromversorgung keinen Einfluss auf den Alarmausgang. Bei **Überwachen** wird der Alarmausgang geöffnet, wenn eine der zwei Versorgungsspannungen ausfällt.
	Link-Überwachung	**Ignorieren/Überwachen** 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 ein-Link keine Konnektivität aufweist. Stellen Sie dazu unter *Netzwerk* >> *Ethernet* >> *MAU-Einstellungen* unter „Link-Überwachung“ die Links ein, die überwacht werden sollen.

Verwaltung >> Service I/O >> Alarmausgang [...]		
	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 des internen Modems	Nur wenn ein internes Modem vorhanden und eingeschaltet ist (TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS mit internem Analog-Modem oder ISDN-Modem). Bei **Ignorieren** hat der Verbindungsstatus des internen Modems keinen Einfluss auf den Alarmausgang. Bei **Überwachen** wird der Alarmausgang geöffnet, wenn das interne Modem keine Verbindung hat.
	Verbindungsstatus der Redundanz	Nur wenn die Funktion **Redundanz** genutzt wird (siehe Kapitel 17). Bei **Ignorieren** hat die Konnektivitätsprüfung keinen Einfluss auf den Alarmausgang. Bei **Überwachen** wird der Alarmausgang geöffnet, wenn die Konnektivitätsprüfung fehlschlägt. Das ist unabhängt davon, ob der mGuard aktiv oder im Bereitschaftszustand ist.

4.9 Verwaltung >> Neustart

4.9.1 Neustart



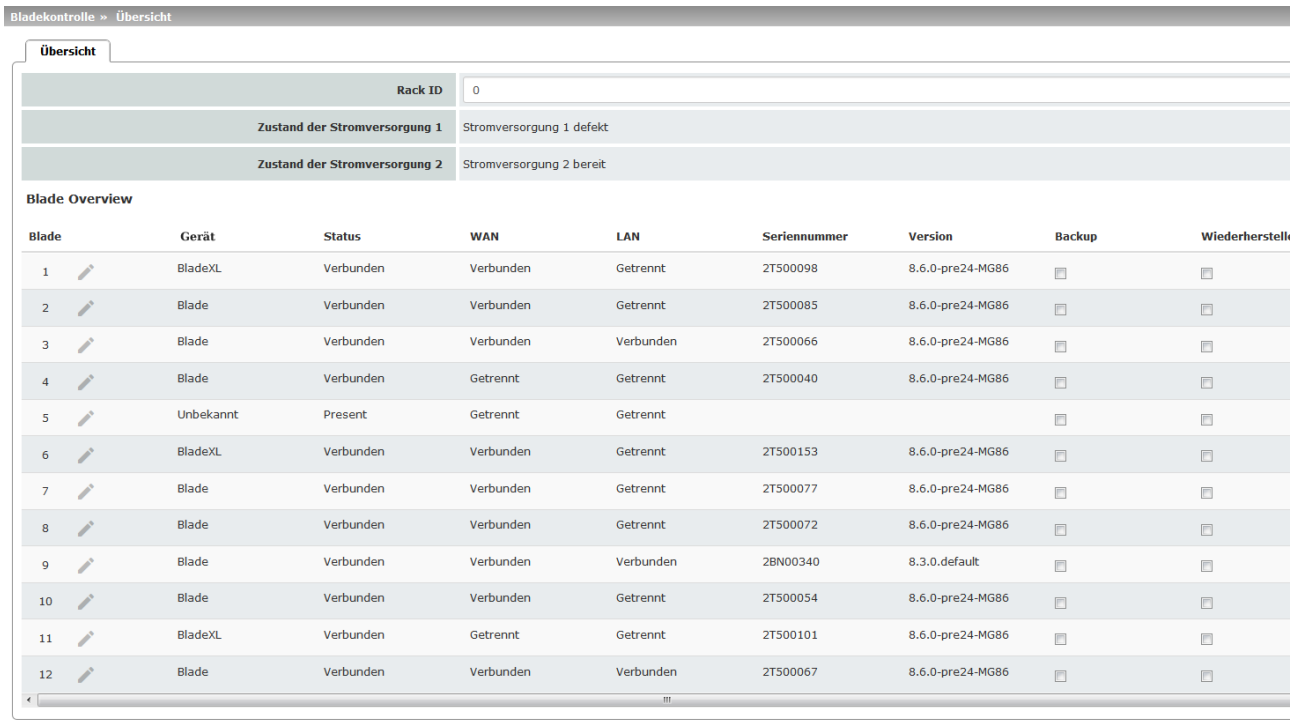
Verwaltung >> Neustart >> Neustart		
Neustart	**Neustart**	Ein Klick auf die Schaltfläche „**Neustart**“ startet den mGuard neu (Reboot). Das Gerät benötigt ca. 60 Sekunden für den Neustart. Ein Neustart hat den selben Effekt wie die vorübergehende Unterbrechung der Stromzufuhr. Der mGuard wird aus- und wieder eingeschaltet. Ein Neustart ist erforderlich im Fehlerfall. Außerdem kann ein Neustart nach einem Software-Update erforderlich sein.
Neustart per SMS (Nur TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G)	**Neustart per SMS zulassen**	Ab mGuard-Firmwareversion 8.4 ist es möglich, den mGuard per SMS neu zu starten (Reboot). Bei **aktivierter Funktion** kann der mGuard über eine eingehende SMS neu gestartet werden (Reboot). Die SMS muss das Kommando „*system/reboot*“ gefolgt von einem konfigurierten Token (s. u.) enthalten. Beispiel: *system/reboot* mytoken1234 Bei **deaktivierter Funktion** ist ein Neustart per SMS nicht möglich (werkseitige Voreinstellung).
	Token für Neustart per SMS	Token für den Neustart des mGuards per SMS.

5 Menü Bladekontrolle

In mGuard-Firmware-Version **8.4 und 8.5** ist die Konfiguration des **FL MGUARD BLADE-Controllers** nicht möglich.

Dieses Menü steht nur auf dem **FL MGUARD BLADE-Controller** zur Verfügung. Benutzen Sie aus Kompatibilitätsgründen immer den neuesten Blade-Einschub als Controller.

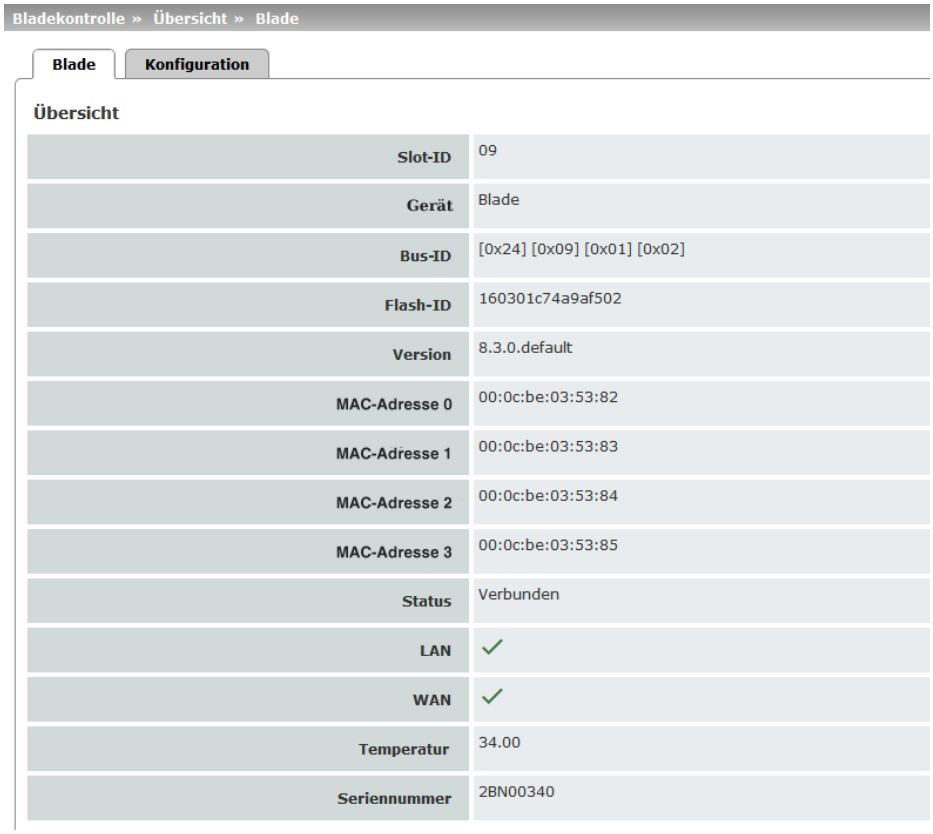
5.1 Bladekontrolle >> Übersicht



Bladekontrolle >> Übersicht >> Übersicht		
Übersicht	**Rack ID**	Die ID des Racks, in dem sich das Blade befindet. Auf dem Controller kann dieser Wert für alle Blades konfiguriert werden.
	Zustand der Stromversorgung P1/P2	Status der Netzteile P1 und P2. – Stromversorgung 1/2 bereit – Stromversorgung 1/2 defekt
Übersicht Blades	**Blade**	Nummer des Slots, in dem das Blade steckt.
	Gerät	Name des Geräts, z. B. „blade“ oder „blade XL“.

Bladekontrolle >> Übersicht >> Übersicht[...]		
	Status	– **Gezogen** (Der Slot ist leer) – **Gesteckt** (Ein Gerät befindet sich im Slot, ist aber nicht funktionsbereit) – **Verbunden** (Ein Gerät befindet sich im Slot und arbeitet korrekt) – **Konfiguration wurde geändert** (Die Konfiguration des Geräts hat sich geändert) – **Konfiguration wird heruntergeladen** (Das Konfigurationsprofil des Geräts wird auf den Blade-Controller kopiert) – **Konfiguration wird hochgeladen** (Das Konfigurationsprofil wird von dem Blade-Controller auf das Gerät kopiert)
	WAN	Status des WAN-Ports.
	LAN	Status des LAN-Ports.
	Seriennummer	Seriennummer des mGuards.
	Version	Softwareversion des mGuards.
	Sichern	**Backup**: Für diesen Slot ist die automatische Konfigurationssicherung auf dem Controller aktiviert oder deaktiviert.
	Wiederherstellen	**Restore**: Für diesen Slot ist das automatische Zurückspielen der Konfiguration (Neukonfiguration) nach Austausch des Blades aktiviert oder deaktiviert.

5.1.1 Blade (in Slot #...)

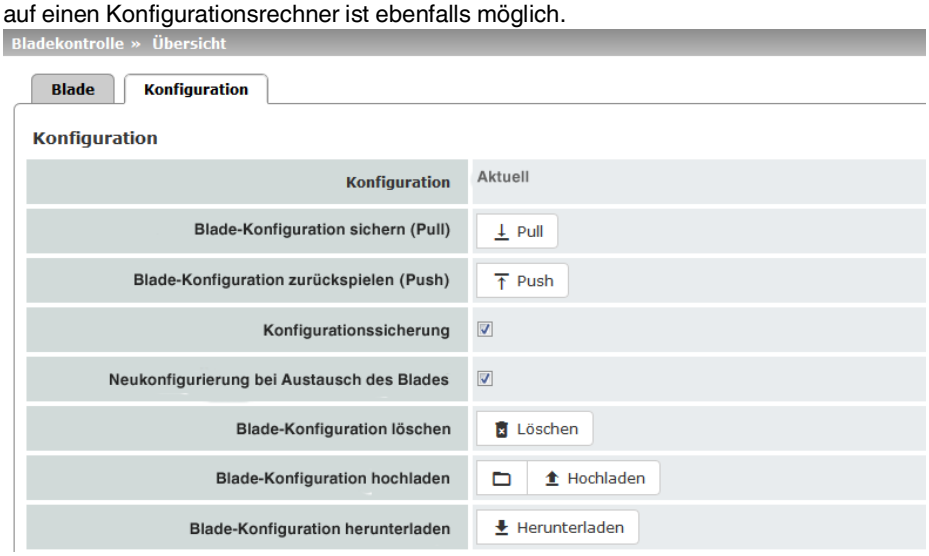


Ein Klick auf das Icon **Zeile bearbeiten** öffnet eine Übersichtsseite mit Statusinformationen über das Blade im ausgewählten Slot.

Bladekontrolle >> Übersicht >> Blade (für Blade in Slot #...)		
Übersicht	**Slot-ID**	Die Nummer bzw. Slot-ID des verwendeten Slots im Blade-Rack.
	Gerät	Name/Gerätetyp des Geräts, z. B. „blade“ oder „blade XL“
	Bus-ID	ID dieses Slots am Steuerbus der Bladebase
	Flash-ID	Flash-ID des Flashspeichers des mGuards
	Version	Die Version der auf dem mGuard installierten Software
	MAC-Adresse (0 ... 3)	Alle für diesen mGuard reservierten MAC-Adressen
	Status	Status des mGuards.
	LAN	Status der LAN-Schnittstelle
	WAN	Status der WAN-Schnittstelle
	Temperatur	Temperatur des Geräts. Bei Geräten, die über keinen Temperatursensor verfügen, wird *N/A* angezeigt.
	Seriennummer	Seriennummer des mGuards.

5.1.2 Konfiguration

Auf der Registerkarte **Konfiguration** können Konfigurationen des Blades in dem ausgewählten Slot auf dem Controller gespeichert oder in das Blade zurückgespielt werden. Dieser Vorgang kann automatisch erfolgen. Das Herunter- und Hochladen von Konfigurationen auf einen Konfigurationsrechner ist ebenfalls möglich.



Bladekontrolle >> Übersicht >> Konfiguration		
Konfiguration	**Konfiguration**	Zeigt den Status der gespeicherten Konfiguration für das Blade in diesem Slot an: – Kein Konfigurationsprofil angegeben – Aktuell – Veraltet – Datei wird kopiert – Blade-Wechsel erkannt – [---] (Kein Blade vorhanden)
	Blade-Konfiguration sichern (Pull)	Die Konfiguration des Blades in diesem Slot wird auf dem Blade-Controller gespeichert (*Pull*).
	Blade-Konfiguration zurückspielen (Push)	Die auf dem Blade-Controller gespeicherte Konfiguration des Blades in diesem Slot wird auf das Blade zurückgespielt (*Push*) und angewendet.

Wurde nach einer manuellen Konfigurationssicherung (*Pull*) das Blade umkonfiguriert, aber die neue Konfiguration nicht erneut mittels *Pull* auf dem Blade-Controller gesichert, ist die im Blade-Controller gespeicherte Konfiguration veraltet.

Der Status der Konfiguration wird als **„Veraltet“** angezeigt.

Stellen Sie in diesem Fall sicher, dass die gewünschte Konfiguration auf dem Blade-Controller gespeichert wird (*Pull*-Befehl).

Bladekontrolle >> Übersicht >> Konfiguration		
	Konfigurationssicherung	Bei aktivierter Funktion werden die auf dem Blade vorgenommenen Konfigurationsänderungen automatisch auf dem Blade-Controller gespeichert. Dies entspricht der manuellen Speicherung mittels *Pull*-Befehl (siehe oben).
	Neukonfiguration bei Austausch des Blades	Beim Austausch des Blades in diesem Slot wird die auf dem Blade-Controller gespeicherte Konfiguration auf das neue Gerät in diesem Slot übertragen.
	Blade-Konfiguration löschen	Löscht die auf dem Blade-Controller gespeicherte Konfiguration für das Gerät in diesem Slot.
	Blade-Konfiguration hochladen	Lädt ein auf dem lokalen Konfigurationsrechner gespeichertes Konfigurationsprofil für diesen Slot auf den Blade-Controller hoch.
	Blade-Konfiguration herunterladen	Lädt das auf dem Blade-Controller gespeicherte Konfigurationsprofil für diesen Slot auf den lokalen Konfigurationsrechner herunter.

6 Menü Netzwerk

6.1 Netzwerk >> Interfaces

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

	Ethernet: Intern: LAN Extern: WAN	Serielle Schnitt-stelle	Eingebau-tes Modem	Serielle Konsole über USB[1]
FL MGUARD RS4000/RS2000	**ja**	**ja**	**nein**	**nein**
FL MGUARD RS4004	**LAN: 4 WAN: 1 DMZ: 1**	**ja**	**nein**	**nein**
FL MGUARD RS2005	**LAN: 5 WAN: 1**	**ja**	**nein**	**nein**
TC MGUARD RS4000 3G, TC MGUARD RS4000 4G	**LAN: 4 WAN: 1 DMZ: 1**	**ja**	**ja**	**nein**
TC MGUARD RS2000 3G, TC MGUARD RS2000 4G	**LAN: 4 WAN: nein DMZ: nein**	**ja**	**ja**	**nein**
FL MGUARD CENTERPORT	**LAN: 1 WAN: 1 DMZ: 1**	**ja**	**nein**	**nein**
FL MGUARD SMART2	**ja**	**nein**	**nein**	**ja**
FL MGUARD GT/GT, FL MGUARD RS, FL MGUARD PCI 533/266, FL MGUARD BLADE, FL MGUARD DELTA, mGuard centerport (Innominate), mGuard delta (Innominate)	**ja**	**ja**	**nein**	**nein**
FL MGUARD PCI(E)4000	**ja**	**nein**	**nein**	**nein**
FL MGUARD RS (ISDN/analog)	**ja**	**ja**	**ja**	**nein**
FL MGUARD SMART 533/266	**ja**	**nein**	**nein**	**nein**

[1] Siehe „Serielle Konsole über USB“ auf Seite 201.

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

Die Details dazu müssen auf den Registerkarten *Allgemein, Ausgehender Ruf, Einwahl* und *Modem/Konsole* konfiguriert werden. Für weitere Erläuterungen zur Nutzungsmöglichkeit der seriellen Schnittstelle (und eines eingebauten Modems) siehe „Modem“ auf Seite 194.

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 6 erhöht (**WAN + 6**).

Beispiel:

- WAN: 00:a0:45:eb:28:9d
- LAN: 00:a0:45:eb:28:9e
- DMZ: 00:a0:45:eb:28:a3

6.1.1 Überblick: Netzwerk-Modus „Router“

Werkseitige Voreinstellung bei TC MGUARD RS4000/RS2000 4G, TC MGUARD RS4000/RS2000 3G, FL MGUARD RS4004/RS2005, FL MGUARD GT/GT, mGuard centerport (Innominate), FL MGUARD CENTERPORT, FL MGUARD BLADE-Controller, mGuard delta (Innominate)

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.

– FL MGUARD SMART2: Der WAN-Port ist die Ethernet-Buchse.

LAN-Port

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

– FL MGUARD SMART2: Der LAN-Port ist der Ethernet-Stecker.
– Im *Power-over-PCI-Modus* ist der LAN-Port durch die LAN-Buchse des FL MGUARD PCI(E)4000, FL MGUARD PCI 533/266 gegeben.

Wie auch in den anderen Modi stehen die Sicherheitsfunktionen Firewall und VPN (lizenzabhängig) 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 209).

Nur dann erhalten die Rechner im angeschlossenen lokalen Netz über den mGuard Zugriff auf das Internet. Ist NAT nicht aktiviert, können eventuell nur VPN-Verbindungen genutzt werden.

Im Netzwerk-Modus *Router* kann zusätzlich ein sekundäres externes Interface konfiguriert werden (siehe „Sekundäres externes Interface“ auf Seite 157).

Es gibt mehrere Router-Modi, je nach Internetanbindung:

– Statisch
– DHCP
– PPPoE
– PPPT
– Modem
– Eingebautes Modem/Eingebautes Mobilfunkmodem

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.

Router-Modus: PPPoE

Der *PPPoE*-Modus entspricht dem Router-Modus mit DHCP – mit einem Unterschied: Für den Anschluss ans externe Netzwerk (Internet, WAN) wird das PPPoE-Protokoll verwendet, das von vielen DSL-Modems (bei DSL-Internetzugang) verwendet wird. Die externe IP-Adresse, unter der der mGuard von entfernten Gegenstellen aus erreichbar ist, wird vom Provider festgelegt.

Wird der mGuard im *PPPoE*-Modus betrieben, muss bei lokal angeschlossenen Rechnern der mGuard als Standard-Gateway festgelegt sein.

Das heißt, dass bei diesen Rechnern die IP-Adresse des LAN-Ports des mGuards als Adresse des Standard-Gateway anzugeben ist.

Arbeitet der mGuard im *PPPoE*-Modus, muss NAT aktiviert werden, um Zugriff auf das Internet zu erhalten.

Ist NAT nicht aktiviert, können eventuell nur VPN-Verbindungen genutzt werden.

Für die weitere Konfiguration des Netzwerk-Modus *PPPoE* siehe „PPPoE“ auf Seite 149.

Router-Modus: PPTP

Ähnlich dem *PPPoE*-Modus. In Österreich zum Beispiel wird statt des PPPoE-Protokolls das PPTP-Protokoll zur DSL-Anbindung verwendet.

(PPTP ist das Protokoll, das ursprünglich von Microsoft für VPN-Verbindungen benutzt worden ist.)

Wird der mGuard im *PPTP*-Modus betrieben, muss bei lokal angeschlossenen Rechnern der mGuard als Standard-Gateway festgelegt sein.

Dass heißt, dass bei diesen Rechnern die IP-Adresse des LAN-Ports des mGuards als Standard-Gateway anzugeben ist.

Wird der mGuard im *PPTP*-Modus betrieben, sollte NAT aktiviert werden, um aus dem lokalen Netz heraus Zugriff auf das Internet zu erhalten (siehe „Netzwerk >> NAT“ auf Seite 209).

Ist NAT nicht aktiviert, können eventuell nur VPN-Verbindungen genutzt werden.

Für die weitere Konfiguration des Netzwerk-Modus *PPTP* siehe „PPTP“ auf Seite 150.

Router-Modus: Modem

Nur bei *FL MGUARD RS4000/RS2000, TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS4004/RS2005*, *mGuard centerport (Innominate)*, *FL MGUARD CENTERPORT*, FL MGUARD RS, *FL MGUARD BLADE, mGuard delta (Innominate), FL MGUARD DELTA*

Wird der Netzwerk-Modus *Modem* gewählt, wird die externe Ethernet-Schnittstelle des mGuards deaktiviert, und der Datenverkehr vom und zum WAN läuft über die von außen zugängliche serielle Schnittstelle (Serial Port) des mGuards.

An der seriellen Schnittstelle wird ein externes Modem angeschlossen, das die Verbindung ins Telefonnetz herstellt. Die Anbindung an WAN oder das Internet erfolgt dann (per externem Modem) über das Telefonnetz.

Wenn Sie die Adresse des mGuards ändern (z. B. durch Wechsel des Netzwerk-Modus von *Stealth* auf *Router*), dann ist das Gerät nur noch unter der neuen Adresse zu erreichen. Erfolgte die Änderung der Konfiguration über den LAN-Port, so erhalten Sie eine Rückmeldung über die neue Adresse, bevor die Änderung aktiv wird. Bei Konfigurationsänderungen über den WAN-Port erhalten Sie keine Rückmeldung.

Wenn Sie den Modus auf *Router* oder *PPPoE* oder *PPTP* stellen und dann die IP-Adresse des LAN-Ports und/oder die lokale Netzmaske ändern, achten Sie unbedingt darauf, dass Sie korrekte Werte angeben. Sonst ist der mGuard unter Umständen nicht mehr erreichbar.

Für die weitere Konfiguration des Netzwerk-Modus *Eingebautes Mobilfunkmodem / Eingebautes Modem / Modem* siehe „Ausgehender Ruf“ auf Seite 184.

Nach Auswahl des Netzwerk-Modus *Modem* geben Sie auf der Registerkarte **Ausgehender Ruf** und/oder **Einwahl** die für die Modemverbindung erforderlichen Parameter an (siehe „Ausgehender Ruf“ auf Seite 184 und „Einwahl“ auf Seite 191).

Im Netzwerk-Modus *Modem* steht die serielle Schnittstelle des mGuards nicht für die ppp-Einwahloption und nicht für Konfigurationszwecke zur Verfügung (siehe „Modem“ auf Seite 194).

Auf der Registerkarte Modem nehmen Sie Anschlusseinstellungen für ein externes Modem vor (siehe „Modem“ auf Seite 194).

Router-Modus: Eingebautes Modem

Nur bei FL MGUARD RS **mit** eingebautem Modem oder ISDN-Terminaladapter

Wird der Netzwerk-Modus *Eingebautes Modem* gewählt, wird die externe Ethernet-Schnittstelle des mGuards deaktiviert, und der Datenverkehr vom und zum WAN läuft über das im mGuard eingebaute Modem bzw. den eingebauten ISDN-Terminaladapter. Dieses bzw. dieser muss am Telefonnetz angeschlossen sein. Die Anbindung ans Internet erfolgt dann über das Telefonnetz.

Nach Auswahl von *Eingebautes Modem* werden die Felder zur Festlegung der Parameter für eine Modemverbindung eingeblendet.

Für die weitere Konfiguration des Netzwerk-Modus *Eingebautes Modem / Modem* (siehe „Ausgehender Ruf“ auf Seite 184).

Router-Modus: Eingebautes Mobilfunkmodem

Nur bei TC MGUARD RS4000/RS2000 3G und TC MGUARD RS4000/RS2000 4G.

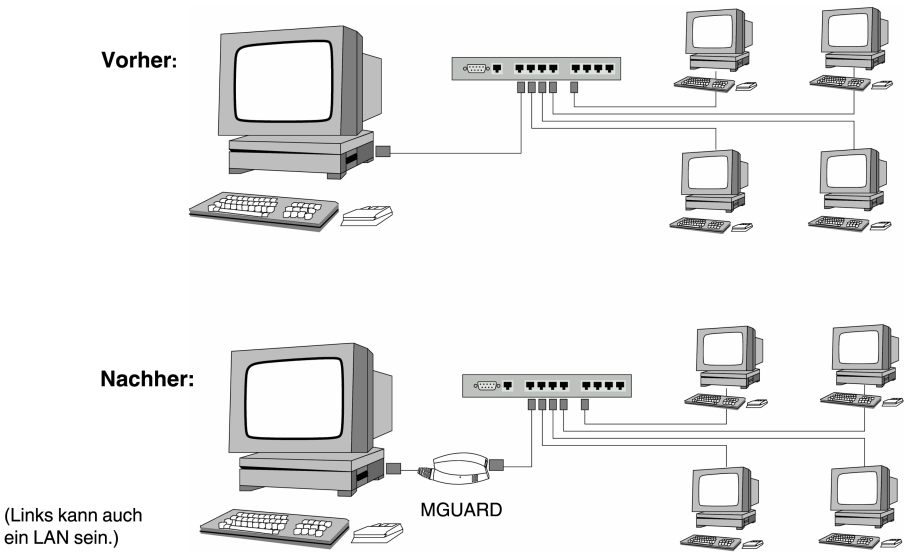
Wenn der Netzwerk-Modus *Eingebautes Mobilfunkmodem* gewählt wird, wird der Datenverkehr statt über den WAN-Port des mGuards über das eingebaute Mobilfunkmodem geleitet.

Für die weitere Konfiguration des Netzwerk-Modus *Eingebautes Modem / Modem* (siehe „Ausgehender Ruf“ auf Seite 184).

6.1.2 Überblick: Netzwerk-Modus „Stealth“

Werkseitige Voreinstellung bei FL MGUARD RS4000/RS2000, FL MGUARD RS, FL MGUARD SMART2, FL MGUARD PCI(E)4000, FL MGUARD PCI 533/266, FL MGUARD DELTA

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 (lizenzabhängig) 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.

Im Netzwerk-Modus *Stealth* kann zusätzlich ein sekundäres externes Interface konfiguriert werden (siehe „Sekundäres externes Interface“ auf Seite 157).

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, Lizenzaktualisierungen oder Aufbau von VPN-Verbindungen) ist es erforderlich, dass der mGuard auch im Stealth-Modus eigenen 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 (werkseitige Voreinstellung)

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 153.

6.1.3 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.
	Sekundäre externe IP-Adresse (Nur wenn das sekundäre externe Interface aktiviert ist)	Nur Anzeige: Die Adressen, unter denen der mGuard von Geräten des externen Netzes aus über das sekundäre externe Interface erreichbar ist.
	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.
	Verbindungsstatus des Modems zum Datennetz (Nur bei Geräten mit internem Modem)	Anzeige des Status des internen Modems (Mobilfunkmodem vom TC MGUARD RS4000/RS2000 3G / TC MGUARD RS4000/RS2000 4G und des internen Analog-Modems beim FL MGUARD RS).

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

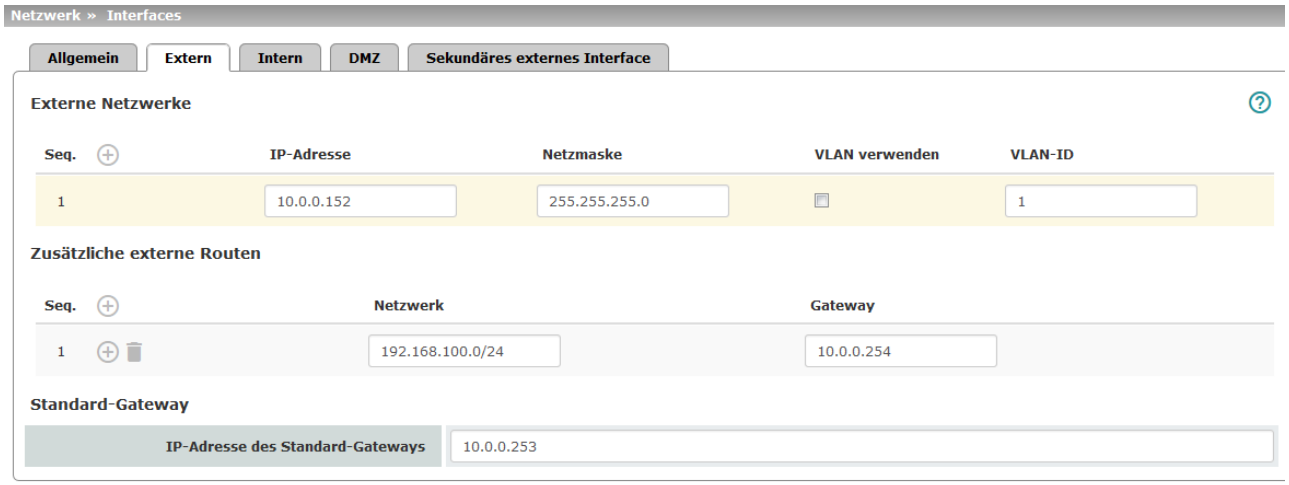
Netzwerk-Modus	**Netzwerk-Modus**	**Router / Stealth** Der mGuard muss auf den Netzwerk-Modus gestellt werden, der seiner Einbindung in das Netzwerk entspricht. Je nachdem, auf welchen Netzwerk-Modus der mGuard gestellt ist, ändert sich auch die Seite mit den auf ihr angebotenen Konfigurationsparametern. Der Netzwerkmodus „Stealth“ ist für den **TC MGUARD RS2000 3G** und **TC MGUARD RS2000 4G** nicht verfügbar, da er keine kabelgebundene WAN-Schnittstelle hat. Siehe auch: „Überblick: Netzwerk-Modus „Router““ auf Seite 137 und „Überblick: Netzwerk-Modus „Stealth““ auf Seite 140.
	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 / PPPoE / PPTP / Modem[1] / Eingebautes Modem[1] / Eingebautes Mobilfunkmodem[1]** Für eine umfassende Beschreibung siehe: – „Router-Modus: Statisch“ auf Seite 138 – „Router-Modus: DHCP“ auf Seite 138 – „Router-Modus: PPPoE“ auf Seite 138 und „PPPoE“ auf Seite 149 – „Router-Modus: PPTP“ auf Seite 138 und „PPTP“ auf Seite 150 – „Router-Modus: Modem“ auf Seite 138 und „Ausgehender Ruf“ auf Seite 184

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, Lizenzaktualisierungen oder Aufbau von VPN-Verbindungen) ist es erforderlich, dass der mGuard auch im Stealth-Modus eigenen 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** (Standard) Wie bei **Automatisch**, es können jedoch mehr als nur ein Rechner am LAN-Port (gesicherter Port) des mGuards angeschlossen sein und somit mehrere IP-Adressen am LAN-Port (gesicherter Port) des mGuards verwendet werden.
Automatische Konfiguration: Ignoriere NetBIOS über TCP auf TCP-Port 139 (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.

[1] *M*odem/Eingebautes Modem/Eingebautes Mobilfunkmodem steht nicht bei allen mGuard-Modellen zur Verfügung (siehe „Netzwerk >> Interfaces“ auf Seite 135)

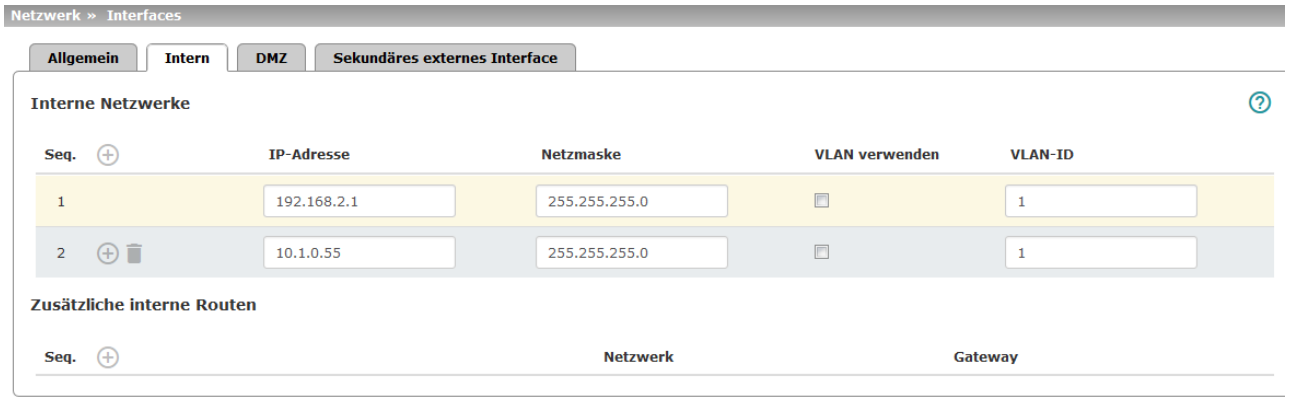
6.1.4 Extern



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 475. – 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 233). Im **Router-Modus „DHCP“** kann dem WAN-Interface keine OSPF-Area zugewiesen werden.
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 26).
	Gateway — Das Gateway, über welches dieses Netzwerk erreicht werden kann. Siehe auch „Netzwerk-Beispielskizze“ auf Seite 27.

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. Wenn der mGuard den Übergang zum Internet herstellt, wird diese IP-Adresse vom Internet Service Provider (ISP) vorgegeben. Wird der mGuard innerhalb des LANs eingesetzt, wird die IP-Adresse des Standard-Gateways vom Netzwerk-Administrator vorgegeben. Wenn das lokale Netz dem externen Router nicht bekannt ist, z. B. im Falle einer Konfiguration per DHCP, dann sollten Sie unter Netzwerk >> NAT Ihr lokales Netz angeben (siehe Seite 209).

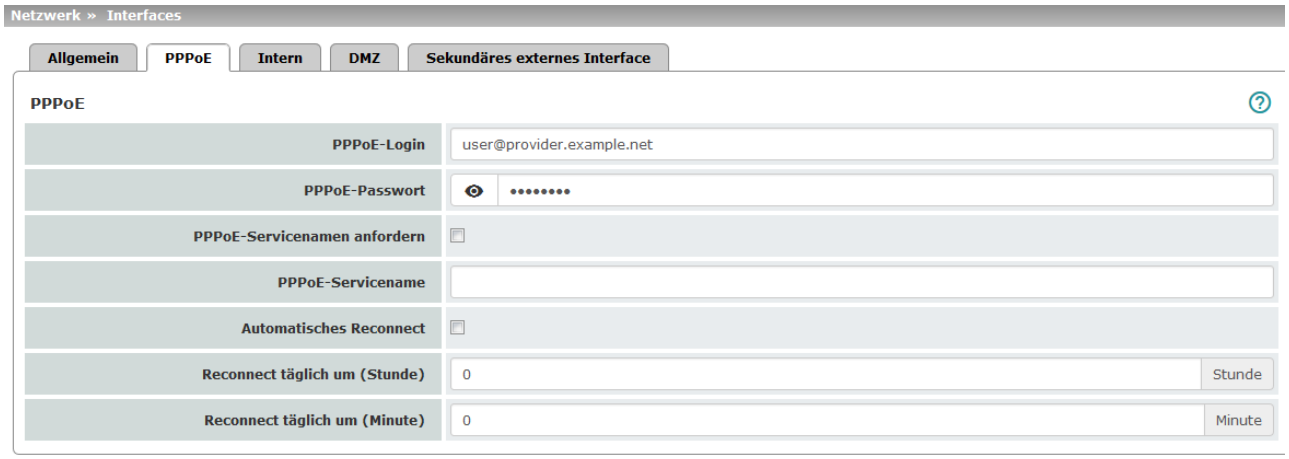
6.1.5 Intern



Netzwerk >> Interfaces >> Intern (Netzwerk-Modus = „Router“)		
Interne Netzwerke	**IP-Adresse**	Interne IP ist die IP-Adresse, unter der der mGuard von Geräten des lokal angeschlossenen Netzes erreichbar ist. Im **Router**-/**PPPoE**-/**PPTP**-/**Modem**-Modus ist werkseitig voreingestellt: – IP-Adresse: **192.168.1.1** – Netzmaske: **255.255.255.0** Sie können weitere Adressen festlegen, unter 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.
	IP-Adresse	IP-Adresse, unter welcher der mGuard über seinen LAN-Port erreichbar sein soll.
	Netzmaske	Die Netzmaske des am LAN-Port angeschlossenen Netzes.
	Verwende VLAN	Wenn die IP-Adresse innerhalb eines VLANs liegen soll, aktivieren Sie die Funktion.
	VLAN-ID	– Eine VLAN-ID zwischen 1 und 4095. – Eine Erläuterung des Begriffes „VLAN“ befindet sich im Glossar auf 475. – 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 233). Im **Router-Modus „DHCP“** kann dem WAN-Interface keine OSPF-Area zugewiesen werden.
Zusätzliche Interne Routen	Wenn am lokal angeschlossen Netz weitere Subnetze angeschlossen sind, können Sie zusätzliche Routen definieren.	

Netzwerk >> Interfaces >> Intern (Netzwerk-Modus = „Router“) [...]		
	Netzwerk	Das Netzwerk in CIDR-Schreibweise angeben (siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 26).
	Gateway	Das Gateway, über welches dieses Netzwerk erreicht werden kann. Siehe auch „Netzwerk-Beispielskizze“ auf Seite 27.

6.1.6 PPPoE



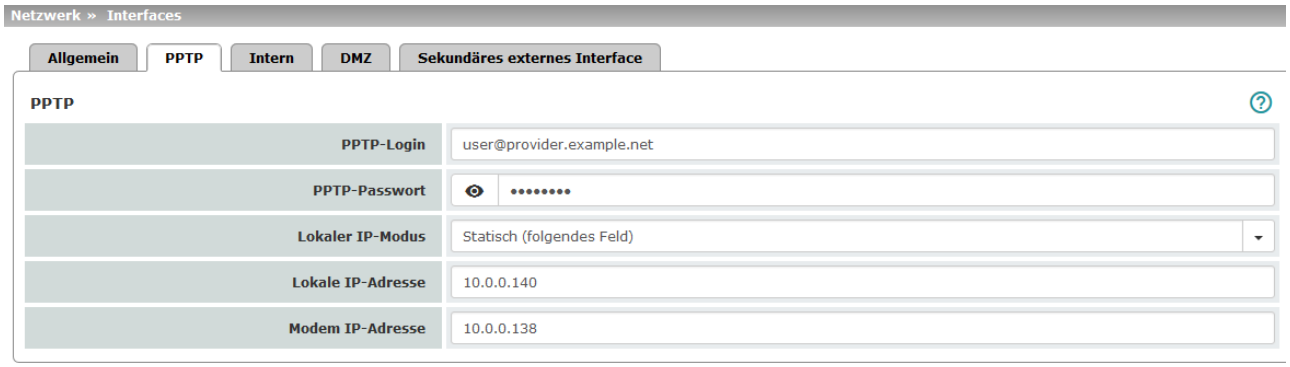
Netzwerk >> Interfaces >> PPPoE (Netzwerk-Modus = „Router“, Router-Modus = „PPPoE“)

PPPoE

Für Zugriffe ins Internet gibt der Internet Service Provider (ISP) dem Benutzer eine Benutzerkennung (Login) und ein Passwort. Diese werden abfragt, wenn Sie eine Verbindung ins Internet herstellen wollen.

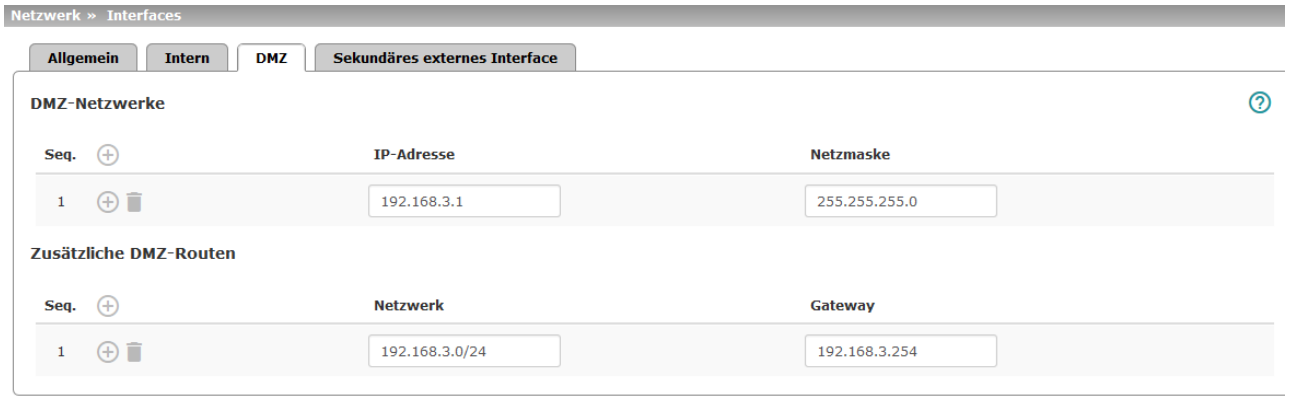
PPPoE-Login	Benutzerkennung (Login), die der Internet Service Provider (ISP) anzugeben fordert, wenn Sie eine Verbindung ins Internet herstellen wollen.
PPPoE-Passwort	Passwort, das der Internet Service Provider anzugeben fordert, wenn Sie eine Verbindung ins Internet herstellen wollen.
PPPoE-Servicenamen anfordern	Bei aktivierter Funktion fordert der PPPoE-Client des mGuards den unten genannten Servicenamen beim PPPoE-Server an. Ansonsten wird der PPPoE-Servicename nicht verwendet.
PPPoE-Servicename	PPPoE-Servicename
Automatisches Reconnect	Bei aktivierter Funktion müssen Sie im nachfolgenden Feld **Reconnect täglich um** die Uhrzeit angeben. Dieses Feature dient dazu, das von vielen Internet Providern sowieso erzwungene Trennen und Wiederverbinden mit dem Internet in eine Zeit zu legen, wenn es den Geschäftsbetrieb nicht stört. Bei Einschalten dieser Funktion greift diese nur dann, wenn die Synchronisation mit einem Zeit-Server erfolgt ist (siehe „Verwaltung >> Systemeinstellungen“ auf Seite 45, „Zeit und Datum“ auf Seite 47).
Reconnect täglich um (Stunde)	Angabe der Uhrzeit (Stunde), falls *Automatisches Reconnect* (s. o.) stattfindet.
Reconnect täglich um (Minute)	Angabe der Uhrzeit (Minute), falls *Automatisches Reconnect* (s. o.) stattfindet.

6.1.7 PPTP



Netzwerk >> Interfaces >> PPTP (Netzwerk-Modus = „Router“, Router-Modus = „PPTP“)		
PPTP	Für Zugriffe ins Internet gibt der Internet Service Provider (ISP) dem Benutzer eine Benutzerkennung (Login) und ein Passwort. Diese werden abgefragt, wenn Sie eine Verbindung ins Internet herstellen wollen.	
	PPTP-Login	Benutzerkennung (Login), die der Internet Service Provider anzugeben fordert, wenn Sie eine Verbindung ins Internet herstellen wollen.
	PPTP-Passwort	Passwort, das der Internet Service Provider anzugeben fordert, wenn Sie eine Verbindung ins Internet herstellen wollen.
	Lokaler IP-Modus	**Statisch / Über DHCP** **Über DHCP** Werden die Adressdaten für den Zugang zum PPTP-Server vom Internet Service Provider per DHCP geliefert, wählen Sie diese Option. Dann ist kein Eintrag unter **Lokale IP-Adresse** zu machen. **Statisch (folgendes Feld)** Werden die Adressdaten für den Zugang zum PPTP-Server **nicht** per DHCP vom Internet Service Provider geliefert, dann muss die lokale IP-Adresse angegeben werden.
	Lokale IP-Adresse	IP-Adresse, unter der der mGuard vom PPTP-Server aus zu erreichen ist.
	Modem IP-Adresse	IP-Adresse des PPTP-Servers des Internet Service Providers.

6.1.8 DMZ



Netzwerk >> Interfaces >> DMZ (Netzwerk-Modus = „Router“)

DMZ-Netzwerke

(Nur bei TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4004, FL MGUARD CENTERPORT)

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

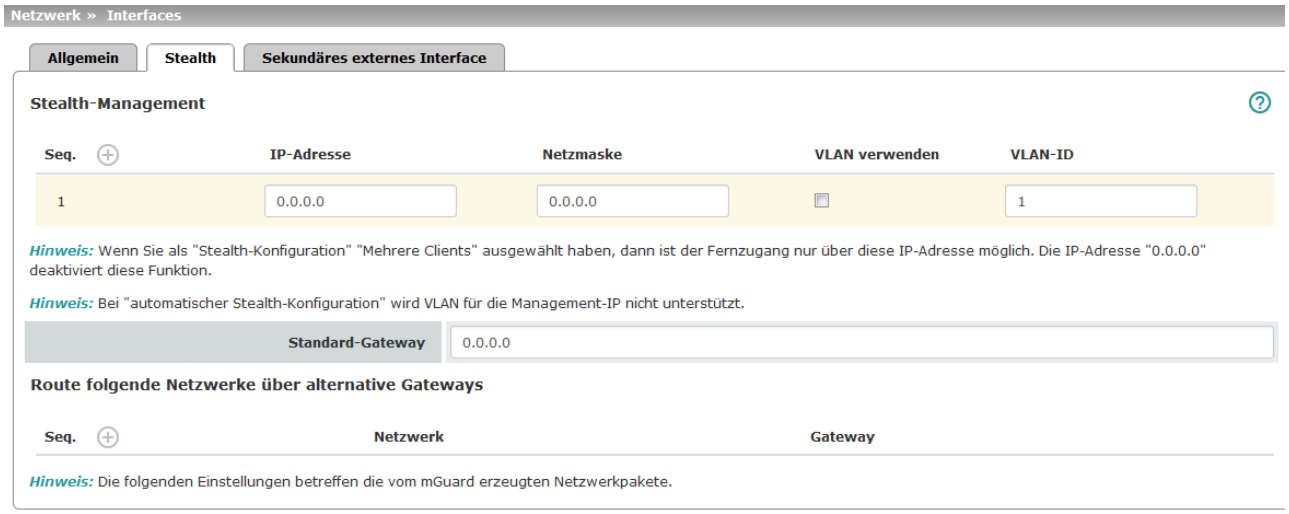
(Nur wenn **OSPF** aktiviert ist)

Verknüpft die statischen Adressen/Routen der DMZ- Netzwerkschnittstelle mit einer OSPF-Area (siehe „Netzwerk >> Dynamisches Routing“ auf Seite 233).

Im **Router-Modus „DHCP“** kann dem WAN-Interface keine OSPF-Area zugewiesen werden.

Netzwerk >> Interfaces >> DMZ (Netzwerk-Modus = „Router“)[...]		
Zusätzliche DMZ-Routen	Wenn am DMZ weitere Subnetze angeschlossen sind, können Sie zusätzliche Routen definieren.	
	Netzwerk	Das Netzwerk in CIDR-Schreibweise angeben (siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 26). Default:192.168.3.0/24
	Gateway	Das Gateway, über welches dieses Netzwerk erreicht werden kann. Siehe auch „Netzwerk-Beispielskizze“ auf Seite 27. Default: 192.168.3.254

6.1.9 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.

Ist das sekundäre externe Interface aktiviert (siehe „Sekundäres externes Interface“ auf Seite 157) gilt Folgendes:

Sind die Routing-Einstellungen in der Weise in Kraft, dass der Datenverkehr zur **Stealth Management IP-Adresse** über das sekundäre externe Interface geroutet würde, wäre damit eine Ausschlusssituation gegeben, d. h. der mGuard wäre nicht mehr lokal administrierbar.

Um das zu verhindern hat der mGuard einen Mechanismus eingebaut, der dafür sorgt, dass in einem solchen Fall die Stealth Management IP-Adresse vom lokal angeschlossenem Rechner (oder Netz) erreichbar bleibt.

Netzwerk >> Interfaces >> Stealth (Netzwerk-Modus = „Stealth“) [...]

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.

VLAN verwenden

IP-Adresse und Netzmaske des VLAN-Ports.

Wenn die IP-Adresse innerhalb eines VLANs liegen soll, aktivieren Sie die Funktion.

VLAN kann im Stealth-Modus nicht bei gleichzeitig aktivierter Redundanzfunktion verwendet werden.

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 475.
- 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.

Netzwerk >> Interfaces >> Stealth (Netzwerk-Modus = „Stealth“) [...]

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

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 26).

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 27).

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

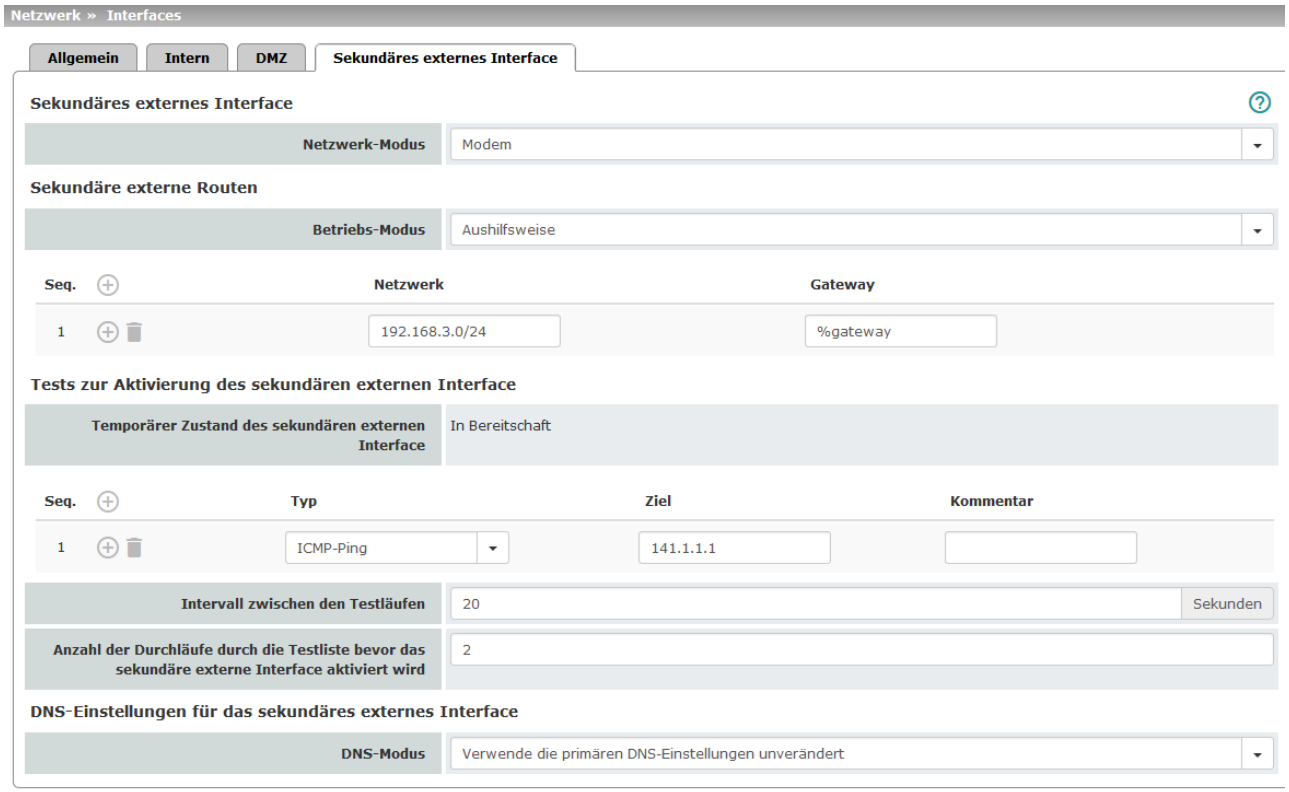
Das ist die physikalische Adresse der Netzwerkkarte des lokalen Rechners, an dem der mGuard angeschlossen ist.

- Die MAC-Adresse ermitteln Sie wie folgt:

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

Netzwerk >> Interfaces >> Stealth (Netzwerk-Modus = „Stealth“) [...]	
	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)

6.1.10 Sekundäres externes Interface



Netzwerk >> Interfaces >> Sekundäres externes Interface

Sekundäres externes Interface

(Nicht bei TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005, FL MGUARD RS2000)

Nur bei Netzwerk-Modus *Router* **mit** Router-Modus *Statisch*/*DHCP* oder Netzwerk-Modus *Stealth*.

Nur bei *FL MGUARD RS4000, FL MGUARD RS4004, mGuard centerport (Innominate), FL MGUARD CENTERPORT, FL MGUARD RS, FL MGUARD BLADE, mGuard delta (Innominate):*

In diesen Netzwerk-Modi kann die serielle Schnittstelle des mGuards als zusätzliches **sekundäres externes Interface** konfiguriert werden.

Nur bei *TC MGUARD RS4000 3G*: Im Netzwerk-Modus „Router“ mit Router-Modus „Statisch“ oder „DHCP“ kann das eingebaute Mobilfunkmodem des mGuards als zusätzliches sekundäres externes Interface konfiguriert werden.

Über das sekundäre externe Interface kann *permanent* oder *aushilfsweise* Datenverkehr ins externe Netz (WAN) geführt werden.

Bei aktiviertem sekundärem externen Interface gilt Folgendes:

Netzwerk >> Interfaces >> Sekundäres externes Interface [...]

Im Netzwerk-Modus *Stealth*

Nur der vom mGuard erzeugte Datenverkehr wird dem Routing unterzogen, das für das sekundäre externe Interface festgelegt ist, nicht der Datenverkehr, der von einem lokal angeschlossenem Rechner ausgeht. Auch kann auf lokal angeschlossene Rechner nicht von entfernt zugegriffen werden, nur ein Fernzugriff auf den mGuard selber ist - bei entsprechender Konfiguration - möglich.

VPN-Datenverkehr kann - wie im Netzwerk-Modus Router - von und zu den lokal angeschlossenen Rechnern fließen. Denn dieser wird vom mGuard verschlüsselt und gilt daher als vom mGuard erzeugt.

Im Netzwerk-Modus *Router*

Aller Datenverkehr, also der von und zu lokal angeschlossenen Rechnern und der, welcher vom mGuard erzeugt wird, kann über das sekundäre externe Interface ins externe Netz (WAN) geführt werden.

Netzwerk-Modus

Aus / Modem / Eingebautes Mobilfunkmodem

Aus

(Standard). Wählen Sie diese Einstellung, wenn die Betriebsumgebung des mGuards kein sekundäres externes Interface braucht. Dann können Sie die serielle Schnittstelle (oder das eingebaute Modem - falls vorhanden) für andere Zwecke nutzen (siehe „Modem“ auf Seite 194).

Modem/Eingebautes Modem

Bei Auswahl einer dieser Optionen wird der Datenverkehr ins externe Netz (WAN) über das sekundäre externe Interface geführt, entweder *permanent* oder *aushilfsweise*.

Das sekundäre externe Interface wird über die serielle Schnittstelle des mGuards und ein daran angeschlossenes externes Modem gebildet.

Eingebautes Mobilfunkmodem

Die Firmware ab 5.2 unterstützt ein externes oder internes Modem als Rückfallebene für das externe Interface. Ab Version 8.0 schließt das auch das interne Mobilfunkmodem des TC MGUARD RS4000 3G ein.

Das Modem kann dauerhaft (*permanent*) als sekundäres externes Interface genutzt werden.

Es kann im Fall eines Netzwerk-Fehlers auch vorübergehend (*aushilfsweise*) als sekundäres externes Interface genutzt werden.

Es unterstützt dedizierte Routen und die DNS-Konfiguration.

Netzwerk >> Interfaces >> Sekundäres externes Interface [...]

Sekundäre externe Routen

(Nicht bei TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005, FL MGUARD RS2000)

Hinweise zu den Betriebs-Modi: Permanent / Aushilfsweise

Sowohl in der Betriebsart **Permanent** als auch in der Betriebsart **Aushilfsweise** muss dem mGuard für das sekundäre externe Interface das Modem zur Verfügung stehen, damit der mGuard über das am Modem angeschlossene Telefonnetz eine Verbindung zum WAN (Internet) herstellen kann.

Welche Datenpakete über das **primäre externe Interface** (Ethernet-Schnittstelle) und welche Datenpakete über das **sekundäre externe Interface** gehen, entscheiden die Routing-Einstellungen, die für diese beiden externen Interfaces in Kraft sind. Ein Datenpaket kann also grundsätzlich nur das Interface nehmen, dessen Routing-Einstellung für das vom Datenpaket angesteuerte Ziel passend ist.

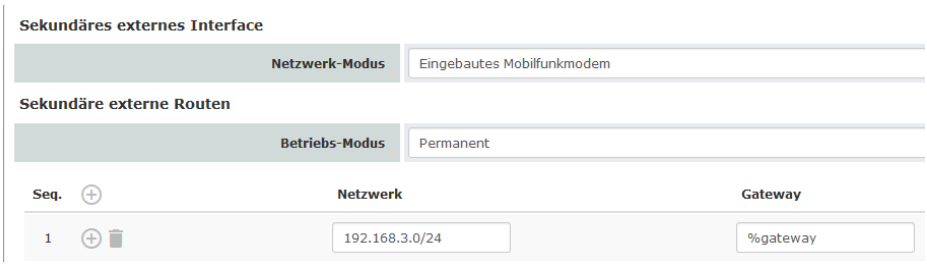
Für die Anwendung von Routing-Angaben gelten folgende Regeln:

Sind mehrere Routing-Angaben für des Ziel eines Datenpaketes passend, entscheidet das kleinste in den Routing-Angaben definierte Netz, das auf ein Datenpaket-Ziel passt, welche Route dieses Paket nimmt.

Betriebs-Modus

Permanent / Aushilfsweise

Nach Auswahl des Netzwerk-Modus *Modem*, *Eingebautes Modem* oder *Eingebautes Mobilfunkmodem* für das sekundäre externe Interface muss der Betriebs-Modus des sekundären externen Interface festgelegt werden (siehe „Beispiel zur Anwendung von Routing-Angaben:“ auf Seite 163).



Permanent

Datenpakete, deren Ziel den Routing-Einstellungen entspricht, die für das sekundäre externe Interface festgelegt sind, werden immer über dieses externe Interface geleitet. Das sekundäre externe Interface ist immer aktiviert.

Aushilfsweise

Datenpakete, deren Ziel den Routing-Einstellungen entspricht, die für das sekundäre externe Interface festgelegt sind, werden nur dann über dieses externe Interface geleitet, wenn zusätzlich weitere zu definierende Bedingungen erfüllt werden. Nur dann wird das sekundäre externe Interface aktiviert, und die Routing-Einstellungen für das sekundäre externe Interface treten in Kraft (siehe „Tests zur Aktivierung des sekundären externen Interface“ auf Seite 161).

Netzwerk >> Interfaces >> Sekundäres externes Interface [...]		
	Netzwerk	Machen Sie hier die Angabe für das Routing zum externen Netzwerk. Sie können mehre Routing-Angaben machen. Datenpakete, die für diese Netze bestimmt sind, werden dann über das sekundäre externe Interface zum entsprechenden Netz - *permanent* oder *aushilfsweise* - geleitet.
	Gateway	Geben Sie hier die IP-Adresse des Gateways an, über das die Vermittlung in das vorgenannte externe Netzwerk erfolgt - sofern diese IP-Adresse bekannt ist. Bei Einwahl ins Internet über die Telefonnummer des Internet Service Providers wird die Adresse des Gateways normalerweise erst nach Einwahl bekannt. In diesem Fall ist **%gateway** als Platzhalter in das Feld einzutragen.

Netzwerk >> Interfaces >> Sekundäres externes Interface [...]

Tests zur Aktivierung des sekundären externen Interface

(Nur Betrieb-Modus **Aushilfsweise**)

Ist der Betriebs-Modus des sekundären externen Interface auf **Aushilfsweise** gestellt, dann wird durch periodisch durchgeführte Ping-Tests Folgendes überprüft: Ist ein bestimmtes Ziel oder sind bestimmte Ziele erreichbar, wenn Datenpakete dorthin ihren Weg aufgrund aller für den mGuard festgelegten Routing-Einstellungen - außer der für das sekundäre externe Interface - nehmen? Nur wenn **keiner** der Ping-Tests erfolgreich ist, geht der mGuard davon aus, dass es zurzeit nicht möglich ist, das/die Ziel(e) über das primäre externe Interface (= Ethernet-Schnittstelle oder WAN-Port des mGuards) zu erreichen. In diesem Fall wird das sekundäre externe Interface aktiviert, so dass - bei entsprechender Routing-Einstellung für das sekundäre externe Interface - die Datenpakete über dieses Interface geleitet werden.

Das sekundäre externe Interface bleibt so lange aktiviert, bis bei nachfolgenden Ping-Tests der mGuard ermittelt, dass das bzw. die Ziel(e) wieder erreichbar sind. Wird diese Bedingung erfüllt, werden die Datenpakete wieder über das **primäre** externe Interface geleitet und das **sekundäre** externe Interface wird deaktiviert.

Die fortlaufend durchgeführten Ping-Tests dienen also dazu zu überprüfen, ob bestimmte Ziele über das primäre externe Interface erreichbar sind. Bei Nichterreichbarkeit wird das sekundäre externe Interface für die Dauer der Nichterreichbarkeit aktiviert.

Erfolgreicher Ping-Test

Ein Ping-Test gilt dann als erfolgreich absolviert, wenn der mGuard innerhalb von 4 Sekunden eine positive Reaktion auf das ausgesandte Ping-Request Paket erhält. Bei einer positiven Reaktion gilt die Gegenstelle als erreichbar.

Bei der Programmierung von Ping-Tests ist Folgendes zu beachten:

Es ist sinnvoll, mehrere Ping-Tests zu programmieren. Denn es könnte sein, dass ein einzelner getesteter Dienst gerade gewartet wird. Solch ein Fall sollte nicht die Auswirkung haben, dass das sekundäre externe Interface aktiviert und eine Kosten verursachende Wählverbindung über das Telefonnetz hergestellt wird.

Da durch die Ping-Tests Netzwerkverkehr erzeugt wird, sollte deren Anzahl und die Häufigkeit ihrer Durchführung angemessen festgelegt werden. Auch sollte vermieden werden, dass das sekundäre externe Interface zu frühzeitig aktiviert wird. Bei den einzelnen Ping-Requests gilt eine Timeout-Zeit von 4 Sekunden. Das bedeutet, dass nach dem Starten eines Ping-Tests der nächste Ping-Test nach 4 Sekunden startet, wenn der vorige negativ war.

Typ

Legen Sie den Ping-Typ des Ping-Request-Pakets fest, das der mGuard zum Gerät mit der IP-Adresse aussenden soll, die Sie unter **Ziel** angeben.

Sie können mehrere solcher Ping-Tests auch zu unterschiedlichen Zielen konfigurieren.

Netzwerk >> Interfaces >> Sekundäres externes Interface [...]		
		IKE-Ping Ermittelt, ob unter der angegebenen IP-Adresse ein VPN-Gateway erreichbar ist. **ICMP-Ping** Ermittelt, ob unter der angegebenen IP-Adresse ein Gerät erreichbar ist. Der gebräuchlichste Ping-Test. Die Reaktion auf solche Ping-Tests ist bei manchen Geräten aber ausgeschaltet, so dass sie nicht reagieren, obwohl sie erreichbar sind. **DNS-Ping** Ermittelt, ob unter der angegebenen IP-Adresse ein funktionierender DNS-Server erreichbar ist. An den DNS-Server mit der angegebenen IP-Adresse wird eine generische Anfrage gerichtet, auf die jeder DNS-Server - sofern erreichbar - eine Antwort gibt.
	Ziel	IP-Adresse des Test-Ziels.
	Intervall zwischen den Starts der Testläufe (Sekunden)	Die oben unter **Tests zur Aktivierung...** definierten Ping-Tests werden nacheinander durchgeführt. Die einmalige sequentielle Durchführung der definierten Ping-Tests wird als *Testlauf* bezeichnet. Testläufe werden in Zeitabständen kontinuierlich wiederholt. Das in diesem Feld angegebene Intervall gibt an, wie lange der mGuard nach dem Start eines Testlaufs abwartet, um den nächsten Testlauf zu starten. Die Testläufe werden nicht unbedingt vollständig abgearbeitet: Sobald ein Ping-Test eines Testlaufs erfolgreich ist, werden die folgenden Ping-Tests desselben Testlaufs ausgelassen. Dauert ein Testlauf länger als das festgelegte Intervall, dann wird der nächste Testlauf direkt im Anschluss gestartet.
	Anzahl der Durchläufe durch die Testliste, bevor das sekundäre externe Interface aktiviert wird	Gibt an, wie viele nacheinander durchgeführte Testläufe mit negativem Ausgang es geben muss, damit der mGuard das sekundäre externe Interface aktiviert. Ein Testlauf hat dann einen negativen Ausgang, wenn **keiner** der darin enthaltenen Ping-Tests erfolgreich war. Die hier festgelegte Anzahl gibt auch an, wie oft nach Aktivierung des sekundären externen Interface die Testläufe in Folge erfolgreich sein müssen, damit es wieder deaktiviert wird.
DNS-Einstellungen für das sekundäre externe Interface	**DNS-Modus**	Nur relevant bei aktiviertem sekundärem externem Interface im Betriebs-Modus **Aushilfsweise**: Der hier ausgewählte DNS-Modus legt fest, welche DNS-Server der mGuard verwendet für aushilfsweise herzustellende Verbindungen über das sekundäre externe Interface.

Netzwerk >> Interfaces >> Sekundäres externes Interface [...]

	Verwende die primären DNS-Einstellungen unverändert Es werden die DNS-Server benutzt, welche unter Netzwerk >> DNS-Server (siehe „Netzwerk >> DNS“ auf Seite 216) definiert sind. **DNS-Root-Nameserver** Anfragen werden an die Root-Nameserver im Internet gerichtet, deren IP-Adressen im mGuard gespeichert sind. Diese Adressen ändern sich selten. **Provider definiert (via PPP-Auswahl)** Es werden die Domain Name Server des Internet Service Providers benutzt, der den Zugang zum Internet zur Verfügung stellt. **Benutzerdefiniert (unten stehende Liste)** Ist diese Einstellung gewählt, nimmt der mGuard mit den Domain Name Servern Verbindung auf, die in der nachfolgenden Liste *Benutzerdefinierte Nameserver* aufgeführt sind.
DNS-Server (Nur bei DNS-Modus **Benutzerdefiniert**)	In dieser Liste können Sie die IP-Adressen von Domain Name Servern erfassen. Diese benutzt der mGuard bei der Kommunikation über das sekundäre externe Interface, wenn dieses aushilfsweise aktiviert ist.

Beispiel zur Anwendung von Routing-Angaben:

- Die externe Route des **primären** externen Interface ist z. B. mit 10.0.0.0/8 angegeben, die externe Route des **sekundären** externen Interface mit 10.1.7.0/24. Dann werden Datenpakete zum Netz 10.1.7.0/24 über das sekundäre externe Interface geleitet, obwohl für sie die Routing-Angabe für das primäre externe Interface auch passt. Begründung: Die Routing-Angabe für das sekundäre externe Interface bezeichnet ein kleineres Netz (10.1.7.0/24 < 10.0.0.0/8).
- (Diese Regel gilt nicht im Netzwerk-Modus *Stealth* in Bezug auf die Stealth Management IP-Adresse (siehe Hinweis unter „Stealth-Management“ auf Seite 153).
- Sind die Routing-Angaben für das primäre und das sekundäre externe Interface identisch, dann „gewinnt“ das sekundäre externe Interface, d. h. die Datenpakete mit passender Zieladresse werden über das sekundäre externe Interface geleitet.
- Die Routing-Einstellungen für das sekundäre externe Interface treten nur dann in Kraft, wenn das sekundäre externe Interface aktiviert ist. Das ist insbesondere dann zu berücksichtigen, wenn die Routing-Angaben für des primäre und das sekundäre externe Interface sich überschneiden oder gleich sind und durch die Priorität des sekundären externen Interface eine Filterwirkung mit folgendem Effekt erzielt wird: Datenpakete, die aufgrund ihres Zieles sowohl für das primäre als auch das sekundäre externe Interface passen, gehen auf jeden Fall über das sekundäre externe Interface, aber nur, wenn dieses aktiviert ist.
- „Aktiviert“ bedeutet im Betriebs-Modus **Aushilfsweise** Folgendes: Nur wenn bestimmte Bedingungen erfüllt werden, wird das sekundäre externe Interface aktiviert, und erst dann wirken sich die Routing-Einstellungen des sekundären externen Interface aus.

Die Netzwerkadresse 0.0.0.0/0 bezeichnet generell das größte definierbare Netz, also das Internet

Im Netzwerk-Modus Router kann das lokale Netz, das am mGuard angeschlossen ist, über das sekundäre externe Interface erreicht werden, sofern die Firewall-Einstellungen so festgelegt sind, dass sie das zulassen.

6.2 Netzwerk >> Mobilfunk

Dieses Menü steht **nur** auf dem **TC MGUARD RS4000/RS2000 3G** und **TC MGUARD RS4000/RS2000 4G** zur Verfügung.

Mobilfunkstandard

TC MGUARD RS4000/RS2000 3G unterstützt den Aufbau eines WANs per Mobilfunk. Die folgenden Mobilfunkstandards werden unterstützt.

- GSM
- GSM with GPRS
- GSM with EGPRS
- 3G/UMTS
- 3G/UMTS with HSDPA
- 3G/UMTS with HSUPA
- 3G/UMTS with HSDPA and HSUPA
- 3G/UMTS with HSPA+
- CDMA 1xRTT (nur 3G-Geräte)
- CDMA EVDO (nur 3G-Geräte)

TC MGUARD RS4000/RS2000 4G unterstützt **zusätzlich** zu den oben genannten den Mobilfunkstandard:

- 4G (LTE)

TC MGUARD RS4000/RS2000 4G ATT unterstützt ausschließlich:

- 3G/UMTS
- 4G (LTE)

TC MGUARD RS4000/RS2000 4G VZW unterstützt ausschließlich:

- 4G (LTE)

Informationen zu den verwendeten Frequenzbereichen finden Sie auf der Webseite des jeweiligen Produkts im Phoenix Contact E-Shop:
phoenixcontact.net/product/<Artikelnummer>

Zusätzlich werden bei den Geräten **TC MGUARD RS4000/RS2000 3G / 4G** die Ortungssysteme GPS und GLONASS für die Ortung und die Zeitsynchronisation unterstützt. Beachten Sie, dass die Zeitsynchronisation und die Positionsdaten der Ortungssysteme durch Störsignale manipuliert werden können (GPS-Spoofing).

Aufbau einer Mobilfunkverbindung

Antenne

Um eine Mobilfunkverbindung aufzubauen, muss mindestens eine passende **Antenne** an den Antennenanschluss (ANT) des Geräts angeschlossen werden (siehe Anwenderhandbuch zu den Geräten: UM DE MGUARD DEVICES unter phoenixcontact.net/products). Bei der Verwendung von LTE sollte zur Verbesserung der Mobilfunkverbindung (Diversity) eine zweite Antenne an das Gerät angeschlossen werden.

Informationen zu empfohlenen Antennen erhalten Sie auf den entsprechenden mGuard-Produktseiten unter phoenixcontact.net/products).

SIM-Karte

Die Geräte TC MGUARD RS4000/RS2000 3G und TC MGUARD RS4000/RS2000 4G benötigen bei der Verwendung von GSM / UMTS / LTE mindestens eine gültige **Mini-SIM-Karte** im 2FF-/ ID-000-Format, über die er sich einem Mobilfunknetz zuordnet und authentifiziert.

Die Geräte können mit zwei SIM-Karten ausgestattet werden. Die SIM-Karte in Schacht SIM 1 ist die primäre SIM-Karte, über die in der Regel die Verbindung aufgebaut wird. Wenn diese Verbindung ausfällt, kann auf die zweite SIM-Karte in Schacht SIM 2 zurückgegriffen werden (siehe „SIM-Fallback“ auf Seite 174). Sie können einstellen, ob und unter welchen Bedingungen die Verbindung dann wieder auf die primäre SIM-Karte zurückgestellt wird.

CDMA

Beim Mobilfunkstandard CDMA wird die Verbindung zum Mobilfunk-Provider ohne SIM-Karte hergestellt. CDMA wird in den USA vom US-Mobilfunk-Provider „Verizon“ verwendet und erfordert eine gesonderte Registrierung.

LEDs

Der Zustand der SIM-Karten wir über zwei LEDs an der Front der Geräte angezeigt. Die LEDs SIM1 und SIM2 leuchten grün, wenn die SIM-Karte aktiv ist. Ist die SIM-Karte defekt oder die PIN falsch bzw. nicht eingegeben, blinkt die LED kontinuierlich grün.

Qualität der Mobilfunkverbindung

Die Signalstärke der Mobilfunkverbindung wird über drei LEDs an der Front der Geräte angezeigt. Die LEDs funktionieren als Bargraph.

Tabelle 6-1 LED-Anzeige der Signalstärke

LED 1 Untere LED	LED 2 Mittlere LED	LED 3 Oberste LED	Signalstärke	
Aus	Aus	Aus	-113 dBm ... -111 dBm	Sehr schlechter bis kein Netzempfang
Gelb	Aus	Aus	-109 dBm ... -89 dBm	Ausreichender Netzempfang
Gelb	Grün	Aus	-87 dBm ... -67 dBm	Guter Netzempfang
Gelb	Grün	Grün	-65 dBm ... -51 dBm	Sehr guter Netzempfang

Für eine stabile Datenübertragung empfehlen wir mindestens einen guten Netzempfang.

TC MGUARD RS2000 3G / TC MGUARD RS2000 4G

Beim **TC MGUARD RS2000 3G und TC MGUARD RS2000 4G** steht das WAN nur über den Mobilfunk zur Verfügung, da keine WAN-Schnittstelle vorhanden ist. Die Mobilfunk-Funktion ist voreingestellt. Die Geräte können nur im Router-Modus betrieben werden.

Der Status der Mobilfunkverbindung kann per SNMP abgefragt werden. SNMP-Traps werden in folgenden Fällen versendet:

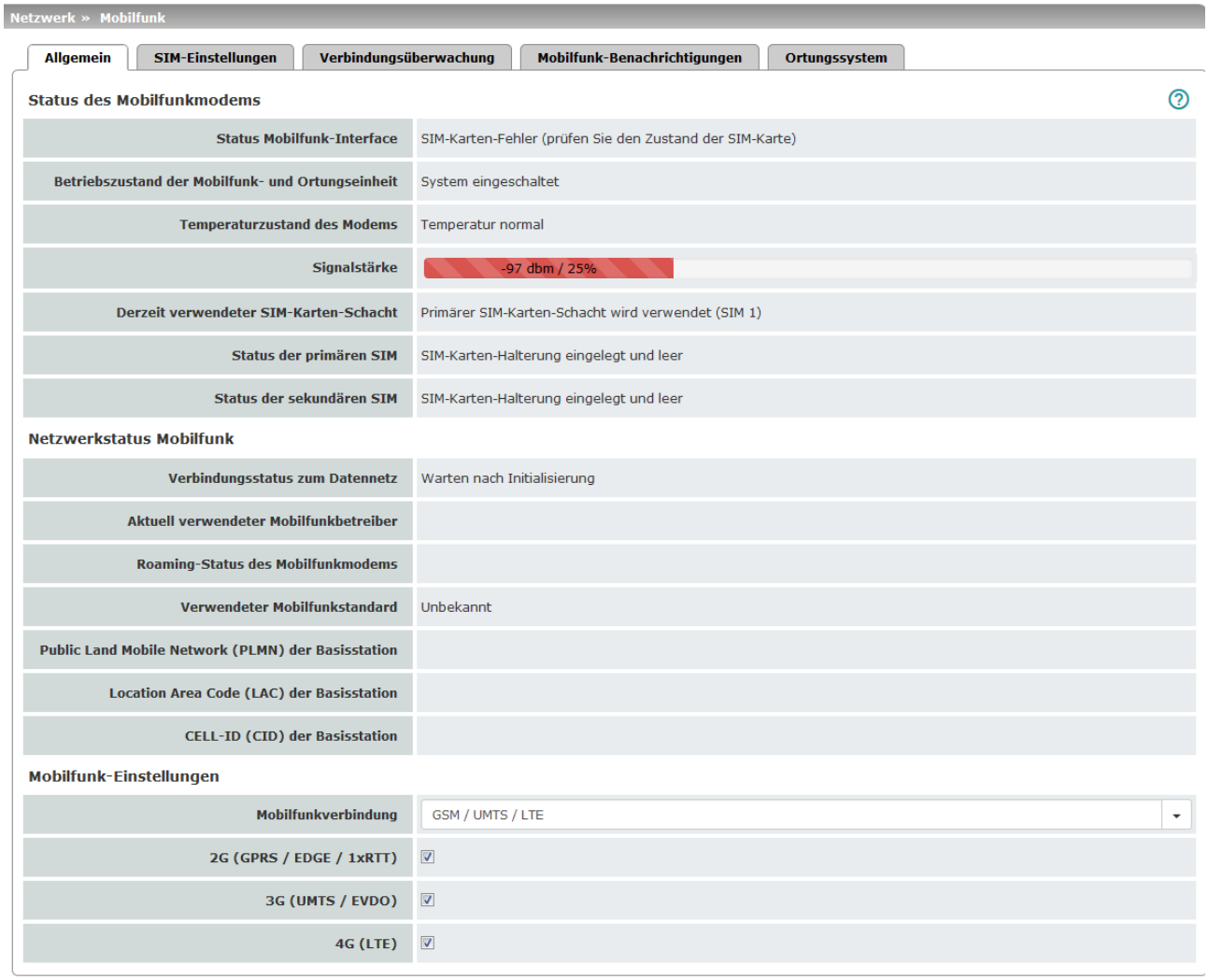
– Eingehende SMS (mGuardEDSGsmIncomingSMS)
– Eingehender Anruf (nur bis mGuard-Firmware-Version 8.3)
– Fehler bei der Mobilfunkverbindung (Ping-Tests) (mGuardEDSGsmNetworkProbe)

Sie können die SNMP-Unterstützung unter **Verwaltung >> SNMP** ein- und ausschalten.

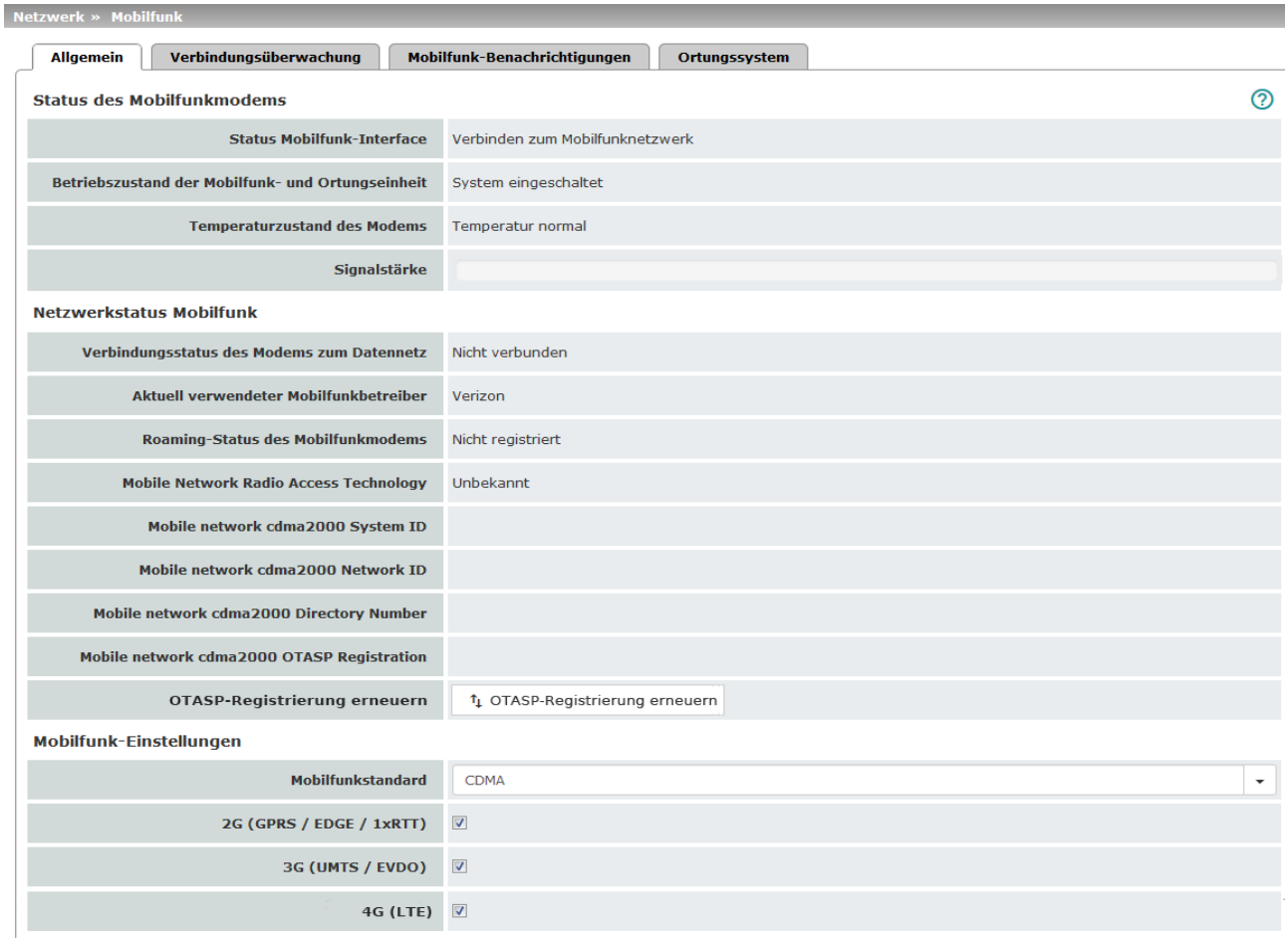
6.2.1 Allgemein

Je nach verwendetem Mobilfunkstandard (GSM/UMTS/LTE oder CDMA) werden unterschiedliche Statusmeldungen angezeigt.

Anzeige bei Auswahl GSM / UMTS / LTE (geräteabhängig)



Anzeige bei Auswahl CDMA



Netzwerk >> Mobilfunk>> Allgemein		
Status Mobilfunkmodem	**Status Mobilfunk-Interface**	Gibt den Status der *State Machine* des Mobilfunkmodems wieder (z. B. Einwahl ins Datennetz oder SIM-Karten-Fehler).
	Betriebszustand der Mobilfunk- und Ortungseinheit	Betriebszustand: System abgeschaltet / System eingeschaltet
	Temperaturzustand des Modems	Temperaturzustand des Mobilfunkmodems Beim Über- oder Unterschreiten einer kritischen Temperatur schaltet sich das Mobilfunkmodem ab.
	Signalstärke	Stärke des Mobilfunk-Signals, von 0 % ... 100 %, -113 dBm ... > - 51 dBm. Die optimale Empfangsleistung liegt bei 100 % Signalstärke und - 51 dBm Dämpfung.
	Derzeit verwendeter SIM-Karten-Schacht	Zeigt an, welcher SIM-Karten-Schacht verwendet wird (SIM 1 oder SIM 2).

Netzwerk >> Mobilfunk>> Allgemein [...]		
Netzwerkstatus Mobilfunk	**Status der primären SIM**	Status der SIM-Karte bzw. SIM-Karten-Halterung in Schacht 1.
	Status der sekundären SIM	Status der SIM-Karte bzw. SIM-Karten-Halterung in Schacht 2.
	Verbindungsstatus des Modems zum Datennetz	Verbindungsstatus zum mobilen Datennetz: Offline / Einwahl / Online
	Aktuell verwendeter Mobilfunkbetreiber	Name des Mobilfunkproviders, der aktuell vom mGuard verwendet wird.
	Roaming-Status des Mobilfunkmodems	Mögliche Status: – Beim eigenen Netzanbieter registriert – Bei einem fremden Netzanbieter registriert – Nicht registriert
	Verwendeter Mobilfunkstandard	Aktuell verwendeter Mobilfunkstandard
	Public Land Mobile Network (PLMN) der Basisstation (Nur bei Netzwerkverbindung „GSM/UMTS/LTE“)	**PLMN**: Eindeutige Identifikationsnummer des der Basisstation zugeordneten Providers Die PLMN setzt sich aus dem dreistelligen Mobile Country Code (**MCC)** und dem zweistelligen Mobile Network Code (**MNC)** zusammen (MCC + MNC = PLMN).
	Local Area Code (LAC) der Basisstation (Nur bei Netzwerkverbindung „GSM/UMTS/LTE“)	**LAC**: Gebietskennzahl, Standort im Mobilfunknetz (in Dezimal-Schreibweise)
	Cell-ID (CID) der Basisstation (Nur bei Netzwerkverbindung „GSM/UMTS/LTE“)	**CID**: Eindeutige Identifikationsnummer der Mobilfunkzelle
	Mobile network cdma2000 System ID (Nur bei Netzwerkverbindung „CDMA“)	**SID**: System-Identifikationsnummer der CDMA-Mobilfunkzelle
	Mobile network cdma2000 Network ID (Nur bei Netzwerkverbindung „CDMA“)	**NID**: Netzwerk-Identifikationsnummer der CDMA-Mobilfunkzelle
	Mobile network cdma2000 Directory Number (Nur bei Netzwerkverbindung „CDMA“)	Rufnummer (**Mobile Directory Number – MDN**), die dem mGuard vom CDMA-Netzwerkprovider (z. B. Verizon) zugewiesen wird. Gültig für den nordamerikanischen Nummerierungsplan (North American Numbering Plan – NANP). Die Nummer wird erst nach einer erfolgreichen Registrierung beim CDMA-Netzwerkprovider (z. B. Verizon OTASP) angezeigt (s. u.).

Netzwerk >> Mobilfunk>> Allgemein [...]

Mobile network cdma2000 OTASP Registration

(Nur bei Netzwerkverbindung „CDMA“)

Damit der mGuard im Mobilfunk-Netzwerk des CDMA-Providers (z. B. Verizon) betrieben werden kann, müssen die dafür notwendigen Konfigurationen einmalig vom CDMA-Netzwerkprovider angefordert und heruntergeladen werden.

Nur möglich bei einer bestehenden Mobilfunkverbindung in das CDMA-Mobilfunknetz.

Bis mGuard-Firmwareversion 8.3: Mit einem Klick auf die Schaltfläche „Verizon Registrierung“ wird die Konfiguration heruntergeladen (OTASP-Methode). Der mGuard muss dazu zuvor bei Verizon angemeldet und freigeschaltet werden.

Ab mGuard-Firmwareversion 8.4: Die Konfiguration wird automatisch heruntergeladen, sobald sich der **bei Verizon angemeldete und freigeschaltete** mGuard erstmalig über CDMA mit dem Verizon-Netz verbindet.

Nach einer erfolgreichen Registrierung wird die MDN unter „**Mobile network cdma2000 Directory Number**“ angezeigt.

OTASP-Registrierung erneuern

Wenn ein bereits registriertes mGuard-Gerät mit einem neuen Mobilfunkvertrag (z. B. *data plan* von Verizon) und einer neuen Mobilfunknummer betrieben werden soll, muss die Registrierung erneut durchgeführt werden.

Mit einem Klick auf die Schaltfläche „**OTASP-Registrierung erneuern**“ wird die neue Konfiguration heruntergeladen. Nach einer erfolgreichen Registrierung wird die neue MDN unter „**Mobile network cdma2000 Directory Number**“ angezeigt.

Nur möglich bei einer bestehenden Mobilfunkverbindung in das CDMA-Mobilfunknetz.

Um die Registrierung auf der Kommandozeile zu erneuern, muss folgender Befehl eingegeben werden:
perform_action cdma/otasp_verizon .

Netzwerk >> Mobilfunk>> Allgemein [...]

Mobilfunk-Einstellungen

Die explizite Auswahl von Mobilfunkfrequenzen ist ab mGuard-Firmware-Version 8.4 nicht mehr notwendig und möglich. Es erfolgt lediglich die Auswahl des Mobilfunkstandards.

Ab mGuard-Firmware-Version 8.4 gilt: Die Auswahl des Mobilfunkstandards kann auf einen Standard beschränkt oder dem Modem überlassen werden. Folgende Einstellungen sind möglich:

1. Ist nur einer der drei geräteabhängig verfügbaren Standards (2G, 3G und 4G) ausgewählt, wird ausschließlich dieser verwendet.
2. Ist mehr als ein Standard ausgewählt, verhält sich das Modem wie folgt:
   - **2G und 4G**: Diese Auswahl ist nicht zulässig!
   - **2G und 3G**: Die Übertragungsart wird automatisch durch das Modem bestimmt.
   - **3G und 4G**: Die Übertragungsart wird automatisch durch das Modem bestimmt.
   - **2G, 3G und 4G**: Die Übertragungsart wird automatisch durch das Modem bestimmt.

Mobilfunkstandard
(Geräteabhängig)

Keine Mobilfunkverbindung: Mobilfunkverbindung abgeschaltet

GSM / UMTS / LTE: Mobilfunkverbindung über den Provider der SIM-Karte

CDMA: Mobilfunkverbindung über das CDMA-Verfahren ohne SIM-Karte. Die Anmeldung und Freischaltung beim CDMA-Provider (z. B. Verizon) erfolgt mittels MEID-Code, der auf dem Gehäuse des verwendeten Geräts aufgedruckt ist. Die Registrierung und das Herunterladen der Konfiguration erfolgen ab mGuard-Firmwareversion 8.4 automatisch (s. o.).

2G (GPRS / EDGE / 1xRTT)
(Geräteabhängig)

Je nach ausgewähltem Mobilfunkstandard werden die Daten mittels GPRS/EDGE (**GSM/UMTS/LTE**) oder 1xRTT (**CDMA**) übertragen.

3G (UMTS / EVDO)
(Geräteabhängig)

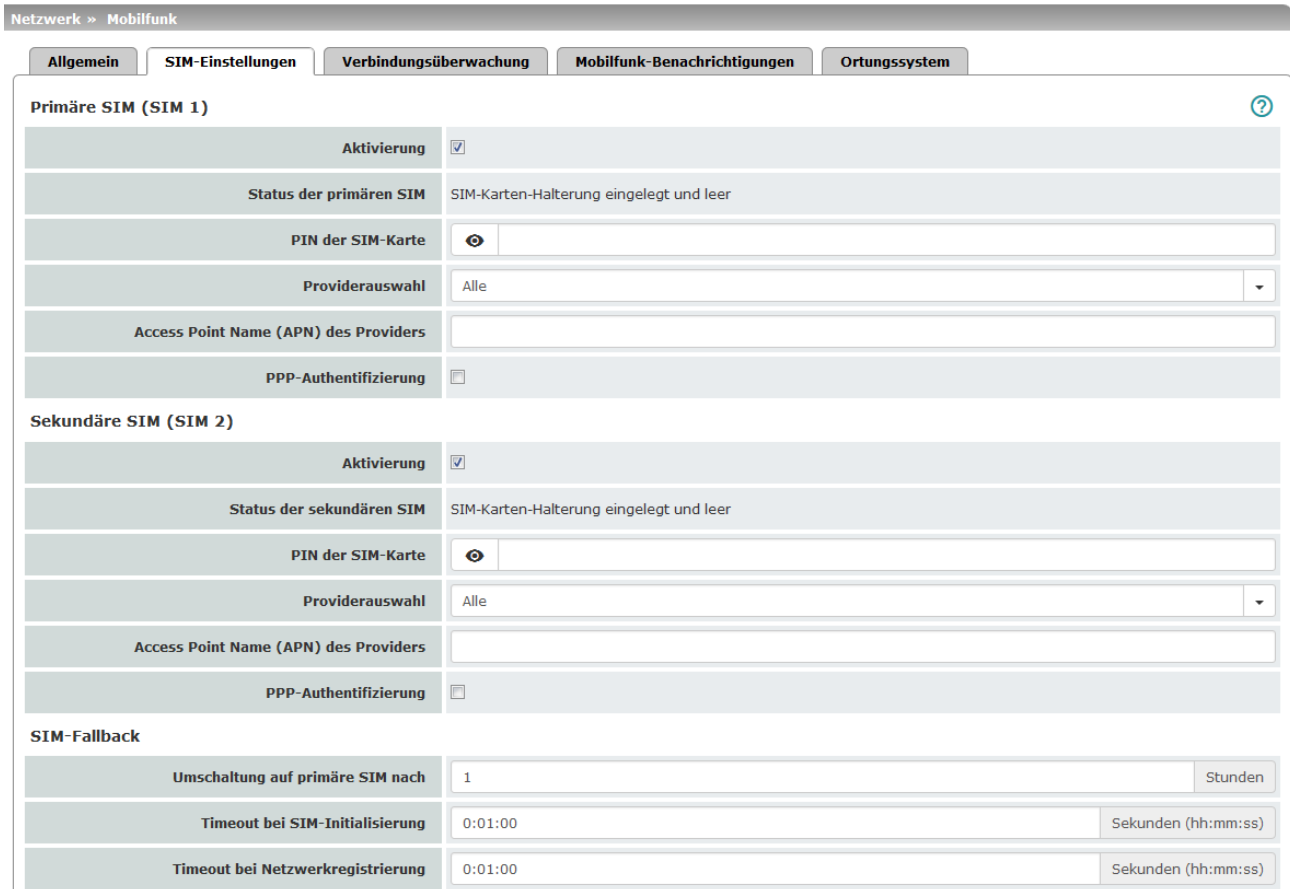
Je nach ausgewähltem Mobilfunkstandard werden die Daten mittels UMTS (**GSM/UMTS/LTE**) oder EVDO (**CDMA**) übertragen.

4G (LTE)
(Geräteabhängig)

Die Daten werden mittels LTE (**GSM/UMTS/LTE**) übertragen.

6.2.2 SIM-Einstellungen

Wird nicht angezeigt bei **verwendetem Mobilfunkstandard „CDMA“**.



Die Geräte TC MGUARD RS4000/RS2000 3G und TC MGUARD RS4000/RS2000 4G können mit zwei SIM-Karten ausgestattet werden.

Die Geräte TC MGUARD RS4000/RS2000 4G ATT und VZW können nur mit *einer* SIM-Karte betrieben werden. *SIM-Fallback* ist nicht möglich.

Wenn zwei SIM-karten verwendet werden, gilt Folgendes: Die SIM-Karte in Schacht SIM 1 ist die **primäre SIM-Karte**, über die in der Regel die Verbindung aufgebaut wird. Wenn diese Verbindung ausfällt, kann auf die **sekundäre SIM-Karte** in Schacht SIM 2 zurückgegriffen werden. Dazu müssen beide SIM-Karten aktiviert und konfiguriert werden. Es ist auch möglich, nur die primäre oder nur die sekundäre SIM-Karte allein zu verwenden.

Die primäre SIM-Karte (SIM 1) in Schacht 1 übernimmt die Mobilfunkverbindung in diesen Fällen:

– Bei einem Neustart des mGuards
– Bei einem erneuten Login beim Mobilfunk-Provider
– Bei einem Fehler in der Mobilfunkverbindung der SIM 2 (siehe Verbindungsüberwachung)
– Beim Erreichen der Zeitüberschreitung, die unter „Umschaltung auf primäre SIM nach“ eingestellt ist (siehe SIM-Fallback)

Die sekundäre SIM-Karte (SIM 2) in Schacht 2 übernimmt die Mobilfunkverbindung, wenn die Verbindung über die primäre SIM-Karte (SIM 1) ausfällt. Die sekundäre SIM-Karte (SIM 2) behält die Verbindung, bis einer der oben genannten Fälle eintritt.

Netzwerk >> Mobilfunk >> SIM-Einstellungen

Die Einstellungen für die **Sekundäre SIM (SIM 2)** erfolgen analog zur **Primären SIM (SIM 1)** und werden nicht gesondert beschrieben.

Die Geräte TC MGUARD RS4000/RS2000 4G ATT und VZW können nur mit der **Primären SIM-Karte** betrieben werden.

Primäre SIM (SIM 1)

Aktivierung

Sie können die Verwendung der SIM-Karte aktivieren oder deaktivieren.

Status der primären SIM

Folgende Status werden angezeigt:

- SIM-Karten-Halterung eingelegt und leer (ohne SIM-Karte)
- SIM-Karten-Halterung fehlt (weder SIM-Karte noch Halterung vorhanden)
- PIN notwendig
- SIM-Karte autorisiert (PIN)
- Falsche PIN
- PUK notwendig (wenn die PIN zu oft falsche eingegeben wurde)
- SIM-Karten-Fehler

PIN der SIM-Karte

Vom Mobilfunk-Provider bereitgestellter Zahlencode. Bei SIM-Karten ohne PIN wird dieses Feld freigelassen.

Providerauswahl

Sie können die Anmeldung der SIM-Karte auf **einen Provider** aus der Liste beschränken oder **alle Provider** zulassen.

Wenn **Alle** ausgewählt ist, wird automatisch ein geeigneter und zur Verfügung stehender Provider ausgewählt.

APN manuell auswählen

(Nur bei TC MGUARD RS4000/RS2000 4G ATT und VZW)

Default: Deaktiviert

Der Access Point Name (APN) wird bei den Geräten TC MGUARD RS4000/RS2000 4G ATT und VZW automatisch vom Provider übermittelt und vom Gerät angewendet.

Treten bei der automatischen Übermittlung Fehler auf, muss die Funktion *APN manuell auswählen* aktiviert werden und der APN im Feld *Access Point Name (APN) des Providers* eingetragen werden (siehe unten).

Access Point Name (APN) des Providers

Tragen Sie hier den Namen des Zugangs-Gateways für die Paketdatenübertragung Ihres Mobilfunk-Providers ein. Die APN erhalten Sie von Ihrem Mobilfunk-Provider.

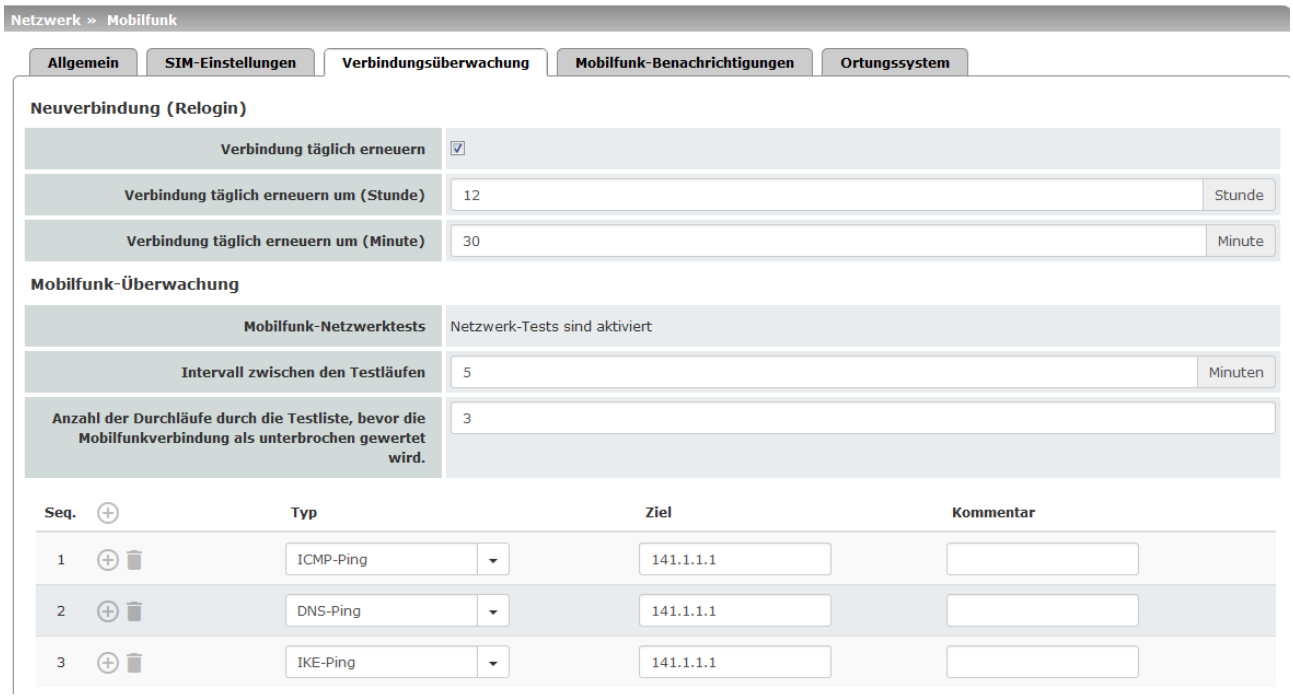
APN

(Nur bei TC MGUARD RS4000/RS2000 4G ATT und VZW)

Der automatisch vom Provider bezogene oder manuell angegebene APN wird angezeigt.

Netzwerk >> Mobilfunk >> SIM-Einstellungen [...]		
	Telefonnummer (Nur bei TC MGUARD RS4000/RS2000 4G VZW)	Die der SIM-Karte zugeordnete Telefonnummer wird angezeigt.
	Status der OTA-Registrierung (Nur bei TC MGUARD RS4000/RS2000 4G VZW)	Status der Registrierung bei dem Mobilfunkbetreiber *Verizon*.
	PPP-Authentifizierung	Bei manchen Mobilfunk-Providern ist für die Übertragung von Paketdaten eine PPP-Authentifizierung notwendig. Wenn Sie die Funktion aktivieren, müssen zusätzlich die entsprechenden Zugangsdaten (Login und Passwort) angegeben werden.
	PPP-Login (Nur bei aktivierter Funktion „PPP-Authentifizierung“)	Geben Sie hier die PAP- oder CHAP-Benutzerkennung (Login) zur Anmeldung am Zugangs-Gateway des Mobilfunk-Providers an. Diese Information erhalten Sie von Ihrem Mobilfunk-Provider.
	PPP-Passwort (Nur bei aktivierter Funktion „PPP-Authentifizierung“)	Geben Sie hier das PAP- oder CHAP-Benutzerpasswort zur Anmeldung am Zugangs-Gateway des Mobilfunk-Providers an. Diese Information erhalten Sie von Ihrem Mobilfunk-Provider.
SIM-Fallback (Nur wenn beide SIM-Karten aktiviert sind) (Nicht bei TC MGUARD RS2000/4000 4G VZW und TC MGUARD RS2000/4000 4G ATT)	**Umschaltung auf primäre SIM nach**	Gibt die Zeit in Stunden an (0 – 24), nach deren Ablauf von der sekundären (SIM 2) auf die primäre SIM-Karte (SIM 1) zurückgeschaltet wird, sofern die Prüfung der Ziele erfolgreich ist. Im Fehlerfall wird sofort auf die primäre SIM-Karte zurückgeschaltet. Ist der Wert „0“ angegeben, wird erst im Fehlerfall oder nach einem Neustart auf die primäre SIM-Karte zurückgeschaltet.
	Timeout bei SIM-Initialisierung	Maximaler Zeitraum für die SIM-Initialisierung. Wird der Zeitraum überschritten, wird auf die andere SIM umgeschaltet, wenn diese aktiviert ist. Andernfalls wird die Initialisierung der aktivierten SIM wiederholt.
	Timeout bei Netzwerkregistrierung	Maximaler Zeitraum zwischen erfolgter SIM-Initialisierung und der Verbindung mit dem Sprachnetzwerk (SMS-Versand möglich). Wird der Zeitraum überschritten, wird auf die andere SIM umgeschaltet, wenn diese aktiviert ist. Andernfalls wird gewartet, bis das Mobilfunkmodem wieder eine Verbindung mit dem Sprachnetzwerk herstellen kann.

6.2.3 Verbindungsüberwachung



Netzwerk >> Mobilfunk >> Verbindungsüberwachung

Neuverbindung (Relogin)

Verbindung täglich erneuern

Die Verbindung zum Mobilfunk-Provider wird täglich zu einem festgelegten Zeitpunkt getrennt und neu aufgebaut, um damit eine Zwangstrennung durch den Provider zu vermeiden.

Verbindung täglich erneuern um (Stunden) (Minute)

(Nur bei aktivierter Funktion „Verbindung täglich erneuern“)

Uhrzeit, um die die Verbindung erneuert wird.

Voraussetzung: Die Uhrzeit des mGuards muss erfolgreich synchronisiert sein (siehe „Zeit und Datum“ auf Seite 47).

Standard: 0 h : 0 m

Werte: 0 – 23 Stunden und 0 – 59 Minuten

Netzwerk >> Mobilfunk >> Verbindungsüberwachung

Mobilfunk-Überwachung

Um die Verfügbarkeit der Mobilfunkverbindung zu erhöhen, sollten Netzwerktests möglichst aktiviert werden. Dies gilt unabhängig vom Mobilfunk-Verfahren (CDMA bzw. GSM/ UMTS/LTE) oder der Anzahl verwendeter SIM-Karten.

Mit den folgenden Testzielen können Sie prüfen, ob bei einer aktiven Mobilfunkverbindung mit Paketdatenübertragung tatsächlich Daten übertragen werden können.

Dazu werden Testziele (Hosts) im Internet in bestimmten Intervallen angepingt und somit geprüft, ob mindestens eines dieser Ziele erreichbar ist. Wenn die definierten Ziele nach festgelegten Intervallen nicht erreicht werden können, wird die Mobilfunkverbindung als fehlerhaft erkannt.

Wenn zwei SIM-Karten konfiguriert sind, wird die Mobilfunkverbindung mit der aktuell nicht verwendeten SIM-Karte neu aufgebaut.

Bei nur einer aktivierten SIM-Karte oder im Verfahren CDMA wird das Mobilfunkmodem zurückgesetzt und anschließend die Mobilfunkverbindung neu aufgebaut.

Zustandsänderungen der Mobilfunk-Überwachung können darüber hinaus per E-Mail, SMS oder SNMP-Trap versendet werden.

Mobilfunk-Netzwerktests

Status der Netzwerküberwachung

Die Überwachung wird nur unter folgenden Bedingungen aktiviert:

- Als Netzwerk- bzw. Router-Modus ist „Eingebautes Mobilfunkmodem“ ausgewählt.
- Mindestens ein Testziel ist konfiguriert

Intervall zwischen den Testläufen (Minuten)

Zeit zwischen zwei Testdurchläufen in Minuten

Wert: 2 - 60 Minuten (Standard: 5 Minuten)

Anzahl der Durchläufe durch die Testliste bevor die Mobilfunkverbindung als unterbrochen gewertet wird

Anzahl der Wiederholungen, bis die Mobilfunkverbindung als abgebrochen gilt.

Wert: 1 - 5 (Standard: 3)

Netzwerk >> Mobilfunk >> Verbindungsüberwachung

Testziele

Typ: Der Ping-Typ kann für jedes Testziel getrennt konfiguriert werden:

– **ICMP-Ping** (ICMP Echo Request, ICMP Echo Reply):
  Ermittelt, ob unter der angegebenen IP-Adresse ein Gerät erreichbar ist.
  Der gebräuchlichste Ping-Test. Die Reaktion auf solche Ping-Tests ist bei manchen Geräten aber ausgeschaltet, so dass sie nicht reagieren, obwohl sie erreichbar sind.
– **DNS-Ping** (DNS-Query auf UDP-Port 53):
  Ermittelt, ob unter der angegebenen IP-Adresse ein funktionierender DNS-Server erreichbar ist.
  An den DNS-Server mit der angegebenen IP-Adresse wird eine generische Anfrage gerichtet, auf die jeder erreichbare DNS-Server eine Antwort gibt.
– **IKE-Ping** (IPsec-IKE-Query auf UDP-Port 500):
  Ermittelt, ob unter der angegebenen IP-Adresse ein VPN-Gateway erreichbar ist.

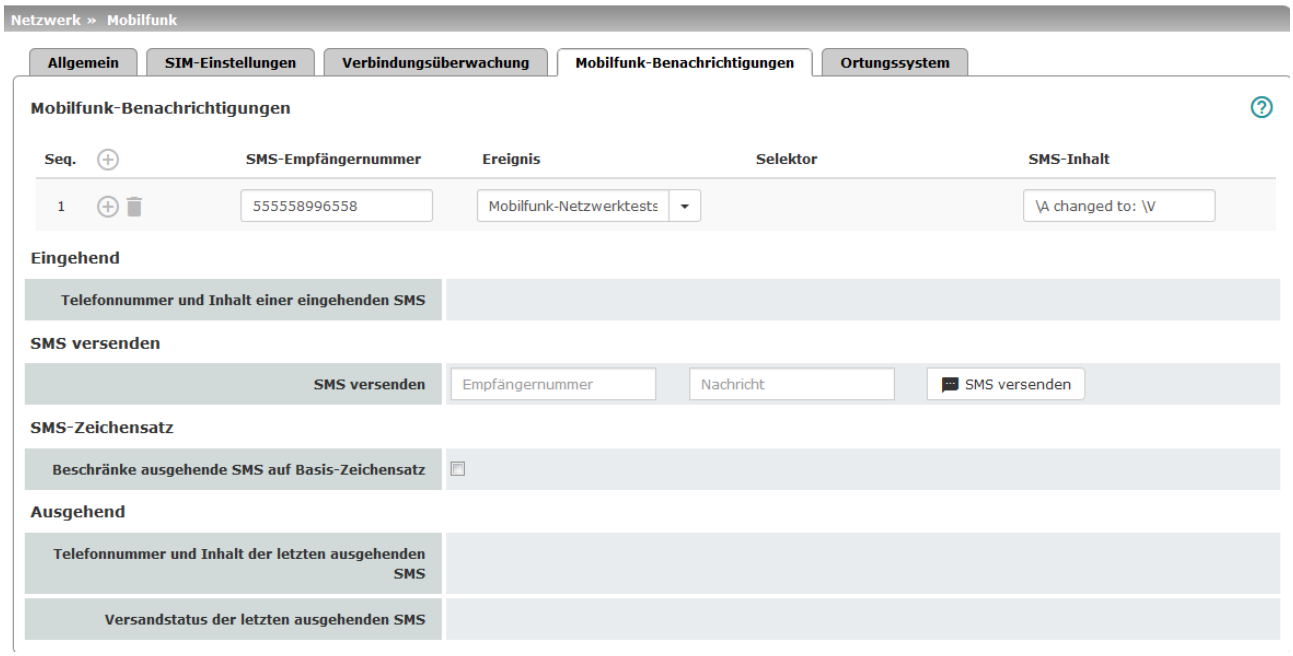
Ziel: Sie können Testziele als Hostname oder IP-Adresse angeben. Die Test-Ziele werden in der angegebenen Reihenfolge abgearbeitet.

Wenn ein Mobilfunk-Provider einen Hostnamen nicht auflösen kann, leitet er die Anfrage häufig auf seine eigene Internet-Domain um. Damit erscheint das Testziel immer erreichbar.

Um dieses Problem zu vermeiden, sollten als Ziel IP-Adressen statt Hostnamen verwendet werden.

Kommentar: Ein frei wählbarer Kommentar.

6.2.4 Mobilfunk-Benachrichtigungen



Die Geräte TC MGUARD RS4000/RS2000 3G und TC MGUARD RS4000/RS2000 4G können SMS-Nachrichten versenden und empfangen.

SMS können über folgende Mechanismen versendet werden:

– Web-Oberfläche
– Kommandozeile

Dazu müssen Sie die Empfängernummer gefolgt von einem Leerzeichen eingeben und daran die Nachricht anschließen:

/Packages/mguard-api_0/mbin/action gsm/sms "<Empfängernummer> <Nachricht>"

Bei auswählbaren Ereignissen können SMS-Nachrichten an frei definierbare Mobilfunk-Empfänger gesendet werden. Eine vollständige Liste aller Ereignisse finden Sie unter „Ereignistabelle“ auf Seite 70.

Eingehende SMS können z. B. zur Steuerung von VPN-Verbindungen oder Firewall-Regelsätzen verwendet werden (siehe „Token für SMS-Steuerung“ auf Seite 284 und 345).

Netzwerk >> Mobilfunk >> Mobilfunk-Benachrichtigungen

Mobilfunk-Benachrichtigungen

Es können beliebige SMS-Empfänger mit vordefinierten Ereignissen und einer frei definierbaren Nachricht verknüpft werden. Die Liste wird von oben nach unten abgearbeitet.

ACHTUNG: Je nach Konfiguration kann die Anzahl der verschickten Kurznachrichten sehr hoch sein. Es wird empfohlen, einen Mobilfunktarif auszuwählen, der eine pauschale Abrechnung von versendeten SMS vorsieht.

SMS-Empfängernummer Empfängernummer für die SMS

Netzwerk >> Mobilfunk >> Mobilfunk-Benachrichtigungen [...]		
	Ereignis	Wenn das ausgewählte Ereignisses eintritt, wird die damit verknüpfte Empfängernummer angewählt und an diese wird das Ereignis als SMS geschickt. Zusätzlich kann eine SMS-Nachricht hinterlegt und gesendet werden. Eine vollständige Liste aller Ereignisse finden Sie unter „Ereignistabelle“ auf Seite 70.
	Selektor (Bei entsprechender Auswahl des Ereignisses „Aktivierungszustand OpenVPN- bzw. IPsec-VPN-Verbindung)	Hier kann eine konfigurierte VPN-Verbindung ausgewählt werden, die per SMS überwacht wird.
	SMS-Inhalt	Sie können hier den Text eingeben, der als SMS verschickt wird. Maximal 160 Zeichen aus dem GSM-Basis-Alphabet (siehe SMS-Zeichensatz) oder 70 Unicode-Symbole. 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 (siehe „Ereignistabelle“ auf Seite 70).
Eingehend	Eingehende SMS können dazu benutzt werden, VPN-Verbindungen zu initiieren (start) oder zu beenden (stop). Die SMS muss einen zuvor für die jeweilige VPN-Verbindung konfigurierten Token und das entsprechende Kommando enthalten.	
	Telefonnummer und Inhalt der letzten eingehenden SMS	Zeigt die Absendernummer und den Textinhalt der zuletzt eingegangenen SMS an.
SMS versenden	**SMS versenden**	**Empfängernummer** Geben Sie die Telefonnummer des Empfängers der SMS ein (maximal 20 Ziffern und ein '+' für internationale Telefonnummern). **Nachricht** Geben Sie hier den Text ein, der als SMS verschickt werden soll. Maximal 160 Zeichen aus dem GSM-Basis-Alphabet (siehe SMS-Zeichensatz) oder 70 Unicode-Symbole. **SMS versenden** Klicken Sie auf die Schaltfläche „SMS versenden“, um die Nachricht zu versendet.

Netzwerk >> Mobilfunk >> Mobilfunk-Benachrichtigungen [...]		
SMS-Zeichensatz	In Firmware-Versionen vor 8.3 wurde versucht, eine maximale Zeichenmenge in einer SMS zu übertragen. Da sich einige Telekommunikationsanbieter nicht an Standards halten, wurden manche SMS nicht exakt (wortwörtlich) übertragen. Dies führt in automatisierten Anwendungen zu Problemen. Um eine wörtliche Übertragung sicherzustellen, sollten die verwendeten Zeichen auf folgenden Basis-Zeichensatz beschränkt werden: – (Leerzeichen) – 0-9 – a-z – A-Z – ! " # % & ( ) * + , - / : ; < = > ?	
	Beschränke ausgehende SMS auf Basis-Zeichensatz	Um die Verwendung des Basis-Zeichensatzes zu erzwingen, aktivieren Sie die Funktion. Nach der Aktivierung wird eine durch den mGuard versendete SMS nicht in die eingestellte Sprache der Web-Benutzeroberfläche übersetzt; es wird immer Englisch verwendet. Versendete E-Mail-Nachrichten sind davon nicht betroffen.
Ausgehend	**Telefonnummer und Inhalt der letzten ausgehenden SMS**	Absendernummer und Textinhalt der letzten gesendeten SMS.
	Versandstatus der letzten ausgehenden SMS	Versandstatus der letzten gesendeten SMS.

6.2.5 Ortungssystem

Dieses Menü steht geräteabhängig nicht auf allen Mobilfunkgeräten zur Verfügung.

Netzwerk >> Mobilfunk >> Ortungssystem

Die Verwendung des Ortungssystems ist nur mit einer passenden GPS-Antenne möglich. Informationen zu empfohlenen Antennen erhalten Sie auf den entsprechenden mGuard-Produktseiten unter phoenixcontact.net/products).

Einstellungen	**Ortungssystem aktivieren**	Wenn Sie die Funktion aktivieren, wird die Position des mGuards bestimmt.
	Systemzeit aktualisieren	Bei aktivierter Funktion erfolgt die Zeitsynchronisierung der lokalen Systemzeit durch das verwendete Ortungssystem. Ist gleichzeitig die Zeitsynchronisation mittels NTP-Server aktiviert (siehe „Aktiviere NTP-Zeitsynchronisation“ auf Seite 51), werden alle vorliegenden Quellen zur Zeitbestimmung verwendet.
Aktuelle Position	**Gültigkeit der Positionsdaten**	Zeigt an, ob valide Positionsdaten für den mGuard verfügbar sind.
	Empfangene Satelliten	Zeigt die Anzahl der für den mGuard verfügbaren GPS/GLONASS-Satelliten an, die für eine Positionsbestimmung zur Verfügung stehen.
	Breitengrad der aktuellen Position	Zeigt den aktuellen Breitengrad der mGuard-Position an.
	Längengrad der aktuellen Position	Zeigt den aktuellen Längengrad der mGuard-Position an.
	In OpenStreetMap anzeigen	Aus den Positionsdaten des mGuards wird ein Link zu OpenStreetMap erzeugt, mit dem ein Web-Browser eine Kartenansicht der aktuellen Position des mGuards anzeigen kann.

6.3 Serielle Schnittstelle

Der Netzwerk-Modus **Modem** ist verfügbar bei:
FL MGUARD RS4000/RS2000, TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G,FL MGUARD RS4004/RS2005, mGuard centerport (Innominate), FL MGUARD CENTERPORT, FL MGUARD RS, FL MGUARD BLADE.

Der Netzwerk-Modus **Eingebautes Mobilfunkmodem** ist zusätzlich verfügbar beim *TC MGUARD RS4000/RS2000 3G* und *TC MGUARD RS4000/RS2000 4G*.

Der Netzwerk-Modus **Eingebautes Modem** ist zusätzlich verfügbar bei: *FL MGUARD RS*, wenn dieser über ein eingebautes Modem oder einen eingebauten ISDN-Terminaladapter verfügt (optional).

Bei allen oben aufgeführten Geräten wird im Netzwerk-Modus *Modem* bzw. *Eingebautes (Mobilfunk-)Modem* der Datenverkehr statt über den WAN-Port des mGuards über die serielle Schnittstelle geleitet und von dort geht es so weiter.

– A – Der Datenverkehr wird über die von außen zugängliche serielle Schnittstelle (Serial Port), an die ein externes Modem angeschlossen werden muss, geleitet.
– B – Der Datenverkehr wird über das eingebaute (Mobilfunk-)Modem / den eingebauten ISDN-Terminaladapter geleitet, wenn vorhanden.

Sowohl bei Möglichkeit A als auch bei B wird per Modem bzw. ISDN-Terminaladapter über das Telefonnetz die Verbindung zum ISP und damit ins Internet hergestellt.

Im Netzwerk-Modus *Modem* steht die serielle Schnittstelle des mGuards nicht für die ppp-Einwahloption und nicht für Konfigurationszwecke zur Verfügung (siehe S. „Modem“ auf Seite 194).

Nach Auswahl des Netzwerk-Modus **Modem**[1] geben Sie auf der Registerkarte **Ausgehender Ruf** und/oder **Eingehender Ruf** die für die Modemverbindung erforderlichen Parameter an (siehe „Ausgehender Ruf“ auf Seite 184 und „Einwahl“ auf Seite 191).

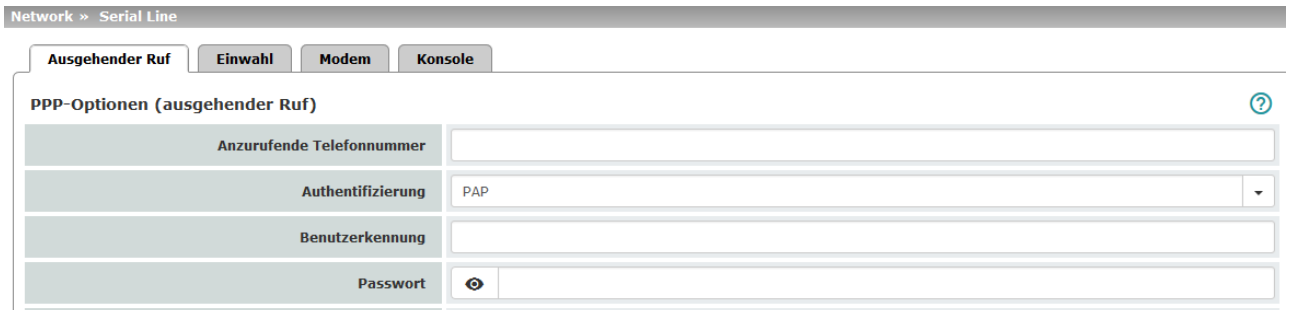
[1] Beim FL MGUARD RS mit eingebautem Modem oder ISDN-Terminaladapter ist **Eingebautes Modem** als Option verfügbar und beim TC MGUARD RS4000/RS2000 3G und TC MGUARD RS4000/RS2000 4G ist **Eingebautes Mobilfunkmodem** als Option verfügbar

Auf der Registerkarte ***Modem*** nehmen Sie Anschlusseinstellungen für ein externes Modem vor (siehe „Modem“ auf Seite 194).

Bei der seriellen Schnittstelle handelt es sich um eine DTE-Schnittstelle.

6.3.1 Ausgehender Ruf

Nur *TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4000, FL MGUARD RS4004, mGuard centerport (Innominate), FL MGUARD CENTERPORT, FL MGUARD RS, FL MGUARD BLADE, FL MGUARD DELTA, mGuard delta (Innominate)*



Netzwerk >> Serielle Schnittstelle >> Ausgehender Ruf

PPP-Optionen (ausgehender Ruf)

(Nicht bei TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005, FL MGUARD RS2000)

Diese Einstellungen sind nur notwendig, wenn der mGuard eine Datenverbindung ins WAN (Internet) über eines dieser Interfaces herstellen soll.

- Über das primäre externe Interface (Netzwerk-Modus *Modem* oder *Eingebautes (Mobilfunk-)Modem*)
- Über das sekundäre externe Interface (zusätzlich im Netzwerk-Modus *Stealth* oder *Router* verfügbar)

Anzurufende Telefonnummer

Telefonnummer des Internet Service Providers. Nach Herstellung der Telefonverbindung wird darüber die Verbindung ins Internet hergestellt.

Befehlssyntax: Zusammen mit dem bereits vorangestellten Modemkommando ATD zum Wählen ergibt sich für das angeschlossene Modem z. B. folgende Wählsequenz: ATD765432

Standardmäßig wird das kompatiblere Pulswahlverfahren benutzt, das auf jeden Fall funktioniert.

Es können Wählsonderzeichen in die Wählsequenz aufgenommen werden.

Netzwerk >> Serielle Schnittstelle >> Ausgehender Ruf [...]

HAYES-Wählsonderzeichen

– **W :** Weist das Modem an, an dieser Stelle eine Wählpause einzulegen, bis das Freizeichen zu hören ist.

  Wird verwendet, wenn das Modem an einer Nebenstellenanlage angeschlossen ist, bei der für Anrufe „nach draußen“ mit einer bestimmten Nummer (z. B. 0) zunächst das externe Festnetz (das Amt) geholt werden muss und erst dann die Telefonnummer des gewünschten Teilnehmers gewählt werden kann.

  Beispiel: ATD0W765432

– **T** : Wechsel auf Tonwahlverfahren.

  Soll bei Anschluss an einen tonwahlfähigen Telefonanschluss das schnellere Tonwahlverfahren verwendet werden, setzen Sie das Wählsonderzeichen T vor die Rufnummer. Beispiel: ATDT765432

Authentifizierung

PAP / CHAP / Keine

– **PAP** = Password Authentication Protocol
– **CHAP** = Challenge Handshake Authentication Protocol.

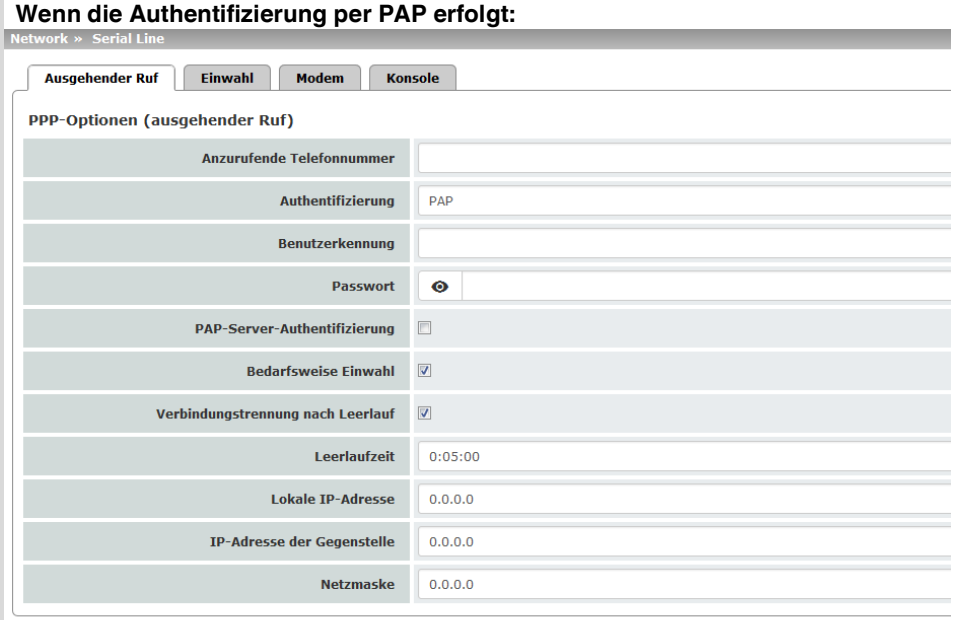
Das sind Bezeichnungen für Verfahren zur sicheren Übertragung von Authentifizierungsdaten über das Point-to-Point Protocol.

Wenn der Internet Service Provider verlangt, dass sich der Benutzer mit Benutzername und Passwort anmeldet, wird PAP oder CHAP als Authentifizierungsverfahren benutzt. Benutzername und Passwort sowie eventuell weitere Angaben, die der Benutzer für den Aufbau einer Verbindung ins Internet angeben muss, werden dem Benutzer vom Internet Service Provider mitgeteilt.

Je nachdem, ob **PAP** oder **CHAP** oder **Keine** ausgewählt wird, erscheinen unterhalb die entsprechenden Felder. In diese tragen Sie die entsprechenden Daten ein.

Netzwerk >> Serielle Schnittstelle >> Ausgehender Ruf [...]

Wenn die Authentifizierung per PAP erfolgt:



Benutzerkennung Benutzername, zur Anmeldung beim Internet-Service-Provider, um Zugang zum Internet zu erhalten.

Passwort Passwort, zur Anmeldung beim Internet-Service-Provider angegeben, um Zugang zum Internet zu erhalten.

PAP-Server-Authentifizierung Bei aktivierter Funktion werden die nachfolgen 2 Eingabefelder eingeblendet:

Benutzerkennung des Servers

Passwort des Servers Benutzername und Passwort, die der mGuard beim Server abfragt. Nur wenn der Server die verabredete Benutzernamen/Passwort-Kombination liefert, erlaubt der mGuard die Verbindung.

Nachfolgend aufgeführte Felder Siehe unter „Wenn als Authentifizierung „Keine“ festgelegt wird“ auf Seite 188.

Netzwerk >> Serielle Schnittstelle >> Ausgehender Ruf [...]

Wenn die Authentifizierung per CHAP erfolgt:

Lokaler Name

Ein Name für den mGuard, mit dem er sich beim Internet Service Provider meldet. Eventuell hat der Service Provider mehrere Kunden und muss durch die Nennung des Namens erkennen können, wer sich bei ihm einwählen will.

Nachdem der mGuard sich mit diesem Namen beim Internet Service Provider angemeldet hat, vergleicht der Service Provider dann auch das angegebene Passwort für die Client-Authentifizierung (siehe unten).

Nur wenn der Name dem Service Provider bekannt ist und das Passwort stimmt, kann die Verbindung erfolgreich aufgebaut werden.

Name der Gegenstelle

Ein Name, den der Internet Service Provider dem mGuard nennen wird, um sich zu identifizieren. Der mGuard wird keine Verbindung zum Service Provider aufbauen, wenn dieser nicht den richtigen Namen nennt.

Passwort für die Client-Authentifizierung

Passwort, das zur Anmeldung beim Internet Service Provider angegeben werden muss, um Zugang zum Internet zu erhalten.

CHAP-Server-Authentifizierung:

Bei aktivierter Funktion werden die nachfolgen 2 Eingabefelder eingeblendet:

Passwort für die Server-Authentifizierung

Passwort, das der mGuard beim Server abfragt. Nur wenn der Server das verabredete Passwort liefert, erlaubt der mGuard die Verbindung.

Nachfolgend aufgeführte Felder

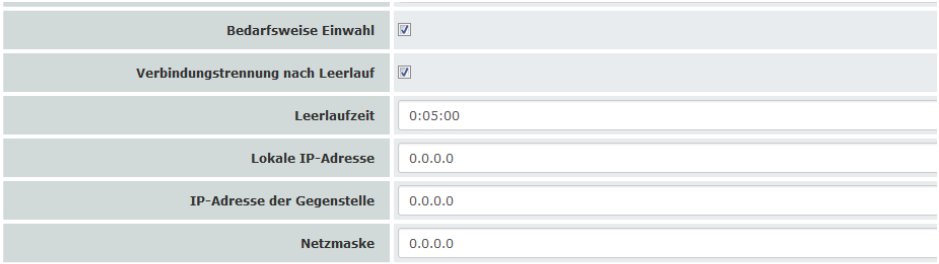
Siehe „Wenn als Authentifizierung „Keine“ festgelegt wird“ auf Seite 188.

Netzwerk >> Serielle Schnittstelle >> Ausgehender Ruf [...]

Wenn als Authentifizierung „Keine“ festgelegt wird

In diesem Fall werden die Felder ausgeblendet, die die Authentifizierungsmethoden **PAP** oder **CHAP** betreffen.

Es bleiben dann nur die Felder unterhalb sichtbar, die weitere Einstellungen festlegen.



Weitere gemeinsame Einstellungen

Netzwerk >> Interfaces >> Ausgehender Ruf

PPP Optionen (abgehender Ruf)

Bedarfsweise Einwahl

Unabhängig von der Aktivierung gilt: Es ist immer der mGuard, der die Telefonverbindung aufbaut.

Bei aktivierter Funktion (Standard): Diese Einstellung ist sinnvoll bei Telefonverbindungen, deren Kosten nach der Verbindungsdauer berechnet werden.

Der mGuard befiehlt dem Modem erst dann, eine Telefonverbindung aufzubauen, wenn auch wirklich Netzwerkpakete zu übertragen sind. Er weist dann auch das Modem an, die Telefonverbindung wieder abzubauen, sobald für eine bestimmte Zeit keine Netzwerkpakete mehr zu übertragen gewesen sind (siehe Wert in *Verbindungstrennung nach Leerlauf*). Auf diese Weise bleibt der mGuard allerdings nicht ständig von außerhalb, d. h. für eingehende Datenpakete, erreichbar.

Netzwerk >> Interfaces >> Ausgehender Ruf [...]

Der mGuard baut über das Modem auch oft oder sporadisch dann eine Verbindung auf bzw. hält eine Verbindung länger, wenn folgende Bedingungen zutreffen:

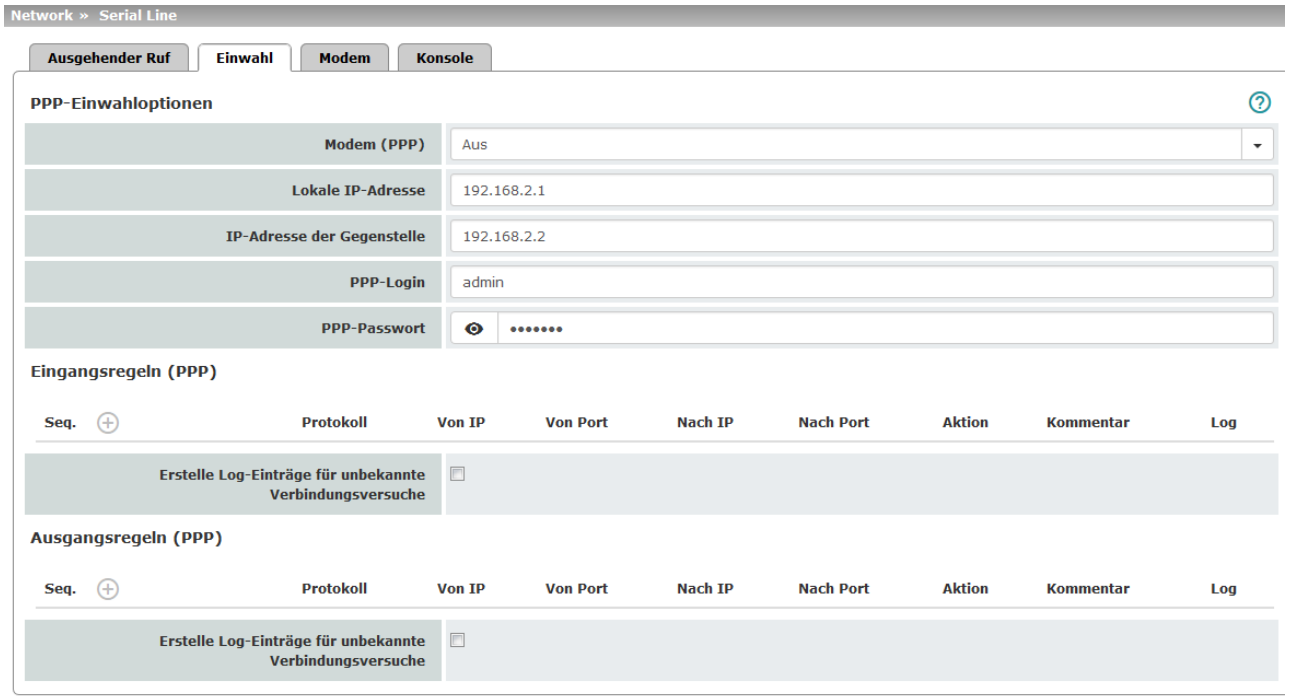
- Oft: Der mGuard ist so konfiguriert, dass er seine Systemzeit (Datum und Uhrzeit) regelmäßig mit einem externen NTP-Server synchronisiert.
- Sporadisch: Der mGuard agiert als DNS-Server und muss für einen Client eine DNS-Anfrage durchführen.
- Nach einem Neustart: Eine aktive VPN-Verbindung ist auf **Initiiere** gestellt. Dann wird jedes mal nach einem Neustart des mGuards eine Verbindung aufgebaut.
- Nach einem Neustart: Bei einer aktiven VPN-Verbindung ist das Gateway der Gegenstelle als Hostname angegeben. Dann muss der mGuard nach einem Neustart bei einem DNS-Server die zum Hostnamen gehörige IP-Adresse anfordern.
- Oft: Es sind VPN-Verbindungen eingerichtet und es werden regelmäßig DPD-Nachrichten gesendet (siehe „Dead Peer Detection“ auf Seite 375).
- Oft: Der mGuard ist so konfiguriert ist, dass er seine externe IP-Adresse regelmäßig einem DNS-Service, z. B. DynDNS, mitteilt, damit er unter seinem Hostnamen erreichbar bleibt.
- Oft: Die IP-Adressen von VPN-Gateways von Gegenstellen müssen beim DynDNS-Service angefordert bzw. durch Neuanfragen auf dem aktuellen Stand gehalten werden.
- Sporadisch: Der mGuard ist so konfiguriert, dass SNMP-Traps zum entfernten Server gesendet werden.
- Sporadisch: Der mGuard ist so konfiguriert, dass er den Fernzugriff per HTTPS, SSH oder SNMP zulässt und annimmt. (Dann sendet der mGuard Antwortpakete an jede IP-Adresse, von der ein Zugriffsversuch erfolgt (sofern die Firewall-Regeln den Zugriff zulassen würden)).
- Oft: Der mGuard ist so konfiguriert, dass er in regelmäßigen Abständen Verbindung zu einem HTTPS Server aufnimmt, um gegebenenfalls ein dort vorliegendes Konfigurationsprofil herunterzuladen (siehe „Verwaltung >> Zentrale Verwaltung“ auf Seite 117).

Bei deaktivierter Funktion baut der mGuard mit Hilfe des angeschlossenen Modems so früh wie möglich nach seinem Neustart oder nach Aktivierung des Netzwerk-Modus *Modem* die Telefonverbindung auf. Diese bleibt dann dauerhaft bestehen, unabhängig davon, ob Daten übertragen werden oder nicht. Wird die Telefonverbindung dennoch unterbrochen, versucht der mGuard, sie sofort wiederherzustellen. So entsteht eine ständige Verbindung, also praktisch eine Standleitung. Auf diese Weise bleibt der mGuard auch ständig von außerhalb, d. h. für eingehende Datenpakete, erreichbar.

Netzwerk >> Interfaces >> Ausgehender Ruf [...]	
Verbindungstrennung nach Leerlauf	Wird nur beachtet, wenn *Bedarfsweise Einwahl* aktiviert ist. Bei aktivierter Funktion (Standard) trennt der mGuard die Telefonverbindung, sobald über die unter *Leerlaufzeit* angegebene Zeitdauer kein Datenverkehr stattfindet. Zur Trennung der Telefonverbindung gibt der mGuard dem angeschlossenen Modem das entsprechende Kommando. Bei deaktivierter Funktion gibt der mGuard dem angeschlossenen Modem kein Kommando, die Telefonverbindung zu trennen.
Leerlaufzeit (Sekunden)	Standard: 300 Sekunden (0:05:00) Findet nach Ablauf der hier angegebenen Zeit weiterhin kein Datenverkehr statt, kann der mGuard die Telefonverbindung trennen (siehe oben unter *Verbindungstrennung nach Leerlauf*). Die Eingabe kann aus Sekunden [ss], Minuten und Sekunden [mm:ss] oder Stunden, Minuten und Sekunden [hh:mm:ss] bestehen.
Lokale IP-Adresse	IP-Adresse der seriellen Schnittstelle des mGuards, die jetzt als WAN-Schnittstelle fungiert. Wird diese IP-Adresse vom Internet Service Provider dynamisch zugewiesen, übernehmen Sie den voreingestellten Wert: 0.0.0.0. Sonst, d. h. bei Zuteilung einer festen IP-Adresse, tragen Sie diese hier ein.
IP-Adresse der Gegenstelle	IP-Adresse der Gegenstelle. Bei Anbindung ans Internet ist das die IP-Adresse des Internet Service Providers, über die der Zugang ins Internet bereit gestellt wird. Da für die Verbindung das Point-to-Point Protocol (PPP) verwendet wird, muss im Normalfall diese IP-Adresse nicht spezifiziert werden, so dass Sie den voreingestellten Wert übernehmen: 0.0.0.0.
Netzmaske	Die hier anzugegebene Netzmaske gehört zu den beiden IP-Adressen *Lokale IP-Adresse* und *IP-Adresse der Gegenstelle*. Üblich ist, dass entweder alle drei Werte (*Lokale IP-Adresse, IP-Adresse der Gegenstelle, Netzmaske*) fest eingestellt werden oder auf dem Wert 0.0.0.0 verbleiben. Auf der Registerkarte *Modem* nehmen Sie Anschlusseinstellungen für ein externes Modem vor (siehe „Modem“ auf Seite 194).

6.3.2 Einwahl

Nur *TC MGUARD RS4000 3G, FL MGUARD RS4004, FL MGUARD RS4000, mGuard centerport (Innominate), FL MGUARD CENTERPORT*, *FL MGUARD RS*, *FL MGUARD BLADE, FL MGUARD DELTA, mGuard delta (Innominate)*



Netzwerk >> Interfaces >> Einwahl

PPP-Einwahloptionen

(Nicht bei TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005, FL MGUARD RS2000)

Nur *TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4004, FL MGUARD RS4000, mGuard centerport (Innominate), FL MGUARD CENTERPORT*, *FL MGUARD RS*, *FL MGUARD BLADE, FL MGUARD DELTA, mGuard delta (Innominate).*

Ist nur dann zu konfigurieren, wenn der mGuard die ppp-Einwahl erlauben soll, entweder über

- ein an der seriellen Schnittstelle angeschlossenes Modem oder
- ein gebautes Modem (als Option beim FL MGUARD RS)
- ein eingebautes Mobilfunkmodem (beim *TC MGUARD RS4000 3G,* TC MGUARD RS4000 4G).

Die ppp-Einwahl kann für Zugriffe ins LAN (oder auf den mGuard für Konfigurationszwecke) genutzt werden (siehe „Modem“ auf Seite 194).

Wird das Modem für ausgehende Rufe verwendet, indem es als primäre externe Schnittstelle (Netzwerk-Modus *Modem)* des mGuards oder als dessen sekundäre externe Schnittstelle (wenn aktiviert im Netzwerk-Modus *Stealth* oder *Router*) fungiert, steht es nicht für die ppp-Einwahloption zur Verfügung.

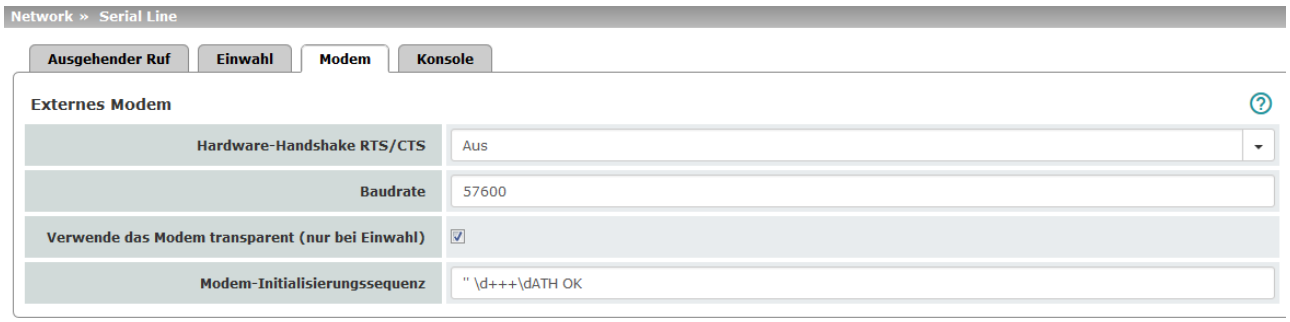
Netzwerk >> Interfaces >> Einwahl [...]		
	Modem (PPP) (Nur TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4000, FL MGUARD RS4004, FL MGUARD RS (ohne eingebautes Modem/ISDN-TA), FL MGUARD DELTA, mGuard delta (Innominate))	**Aus / Internes Modem / Externes Modem** Der Schalter **muss** auf Aus stehen, wenn keine serielle Schnittstelle und kein internes Modem für die ppp-Einwahloption genutzt werden soll. Steht dieser Schalter auf **Internes/Externes Modem**, steht die ppp-Einwahloption zur Verfügung. Die Anschlusseinstellungen für das angeschlossene externe Modem sind auf der Registerkarte *Modem* vorzunehmen.
	Modem (PPP) (Nur bei FL MGUARD RS (mit eingebautem Modem / ISDN-TA))	**Aus / Eingebautes Modem / Externes Modem** Der Schalter **muss** auf **Aus** stehen, wenn die serielle Schnittstelle nicht für die ppp-Einwahloption genutzt werden soll. Steht dieser Schalter auf **Externes Modem**, steht die PPP-Einwahloption zur Verfügung. Dann muss an der seriellen Schnittstelle ein externes Modem angeschlossen sein. Die Anschlusseinstellungen für das angeschlossene externe Modem sind auf der Registerkarte *Modem* vorzunehmen. Steht dieser Schalter auf **Eingebautes Modem**, steht die PPP-Einwahloption zur Verfügung. In diesem Fall erfolgt die Modemverbindung nicht über die auf seiner Frontseite befindliche Buchse *Serial* sondern über die Klemmleiste unten, über die das eingebaute Modem bzw. der eingebaute ISDN-Terminaladapter mit dem Telefonnetz verbunden wird. Die Anschlusseinstellungen für das eingebaute Modem sind auf der Registerkarte *Modem* vorzunehmen. Bei Nutzung der Option **Eingebautes Modem** ist es zusätzlich möglich, die serielle Schnittstelle zu benutzen. Zu dessen Nutzungsmöglichkeiten siehe „Modem“ auf Seite 194.
	Lokale IP-Adresse	IP-Adresse des mGuards, unter der er bei einer PPP-Verbindung erreichbar ist.
	IP-Adresse der Gegenstelle	IP-Adresse der Gegenstelle von der PPP-Verbindung.
	PPP-Login	Benutzerkennung (Login), welche die PPP-Gegenstelle angeben muss, um per PPP-Verbindung Zugriff auf den mGuard zu bekommen.
	PPP-Passwort	Das Passwort, welches die PPP-Gegenstelle angeben muss, um per PPP-Verbindung Zugriff auf den mGuard zu bekommen.
Eingangsregeln (PPP)	Firewall-Regeln für eingehende PPP-Verbindungen zum LAN Interface. Sind mehrere Firewall-Regeln gesetzt, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Sollten nachfolgend in der Regelliste weitere Regeln vorhanden sein, die auch passen würden, werden diese ignoriert. Bei den Angaben haben Sie folgende Möglichkeiten:	
Firewall-Eingangsregeln (serielle Schnittstelle)	**Protokoll**	**Alle** bedeutet: TCP, UDP, ICMP, GRE und andere IP-Protokolle

Netzwerk >> Interfaces >> Einwahl [...]		
	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 26).
	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).
	Aktion	**Annehmen** bedeutet, die Datenpakete dürfen passieren. **Abweisen** bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. **Verwerfen** bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information über deren Verbleib erhält. **Namen von Regelsätzen**, sofern definiert. Bei der Auswahl eines Regelsatzes treten die Firewall-Regeln in Kraft, die unter diesem Regelsatz konfiguriert sind (siehe „Regelsätze“ auf Seite 282). 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 „Modbus TCP“ auf Seite 298).
	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 (werkseitige Voreinstellung).
	Log-Einträge für unbekannte Verbindungsversuche	Bei aktivierter Funkion werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden.
Ausgangsregeln (PPP)	Firewall-Regeln für ausgehende PPP-Verbindungen vom LAN Interface. Die Parameter entsprechen denen von *Eingangsregeln (PPP)*. Diese Ausgangsregeln gelten für Datenpakete, die bei einer durch PPP-Einwahl initiierten Datenverbindung nach außen gehen.	

6.3.3 Modem

Nur *TC MGUARD RS4000 3G, TC MGUARD RS2000 3G (nur Konsole), FL MGUARD RS4004, FL MGUARD RS4000/RS2000, mGuard centerport (Innominate), FL MGUARD CENTERPORT, FL MGUARD RS, FL MGUARD SMART2, FL MGUARD DELTA* (**nicht** *FL MGUARD SMART 533/266, FL MGUARD PCI(E)4000, FL MGUARD BLADE.).*

Einige mGuard-Modelle verfügen über eine von außen zugängliche serielle Schnittstelle, der FL MGUARD RS optional zusätzlich über ein eingebautes Modem (siehe „Netzwerk >> Interfaces“ auf Seite 135).



Nutzungsarten der seriellen Schnittstelle

Die serielle Schnittstelle kann alternativ wie folgt genutzt werden:

Primäres externes Interface
(Dieser Menüpunkt gehört nicht zum Funktionsumfang von TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005, FL MGUARD RS2000)

Als **primäres externes Interface**, wenn unter *Netzwerk* >> *Interfaces*, auf der Registerkarte *Allgemein* als Netzwerk-Modus *Modem* eingestellt ist (siehe „Netzwerk >> Interfaces“ auf Seite 135 und „Allgemein“ auf Seite 142).

In diesem Fall wird der Datenverkehr nicht über den WAN-Port (= Ethernet-Schnittstelle) abgewickelt, sondern über die serielle Schnittstelle.

Sekundäres externes Interface
(Dieser Menüpunkt gehört nicht zum Funktionsumfang von TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005, FL MGUARD RS2000)

Als **sekundäres externes Interface**, wenn unter *Netzwerk* >> *Interfaces*, Registerkarte *Allgemein* das *sekundäre externe Interface* aktiviert und *Modem* ausgewählt ist (siehe „Netzwerk >> Interfaces“ auf Seite 135 und „Allgemein“ auf Seite 142).

In diesem Fall wird Datenverkehr - permanent oder aushilfsweise - über die serielle Schnittstelle abgewickelt.

Einwahl ins LAN oder für Konfigurationszwecke
(Dieser Menüpunkt gehört nicht zum Funktionsumfang von TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005, FL MGUARD RS2000)

Für die **Einwahl ins LAN oder für Konfigurationszwecke** (siehe auch „Einwahl“ auf Seite 191). Es gibt folgende Möglichkeiten:

– An die serielle Schnittstelle des mGuards wird ein Modem angeschlossen, das am Telefonnetz (Festnetz oder GSM-Netz) angeschlossen ist.

  (Beim FL MGUARD RS **mit** eingebautem Modem oder ISDN-Terminaladapter erfolgt der Anschluss ans Telefonnetz über die Klemmleiste unten am Gerät.)

  Dann kann von einem entfernten PC, der ebenfalls mit einem Modem oder ISDN-Adapter am Telefonnetz angeschlossen ist, zum mGuard eine PPP-Wählverbindung (PPP = Point-to-Point Protocol) aufgebaut werden.

Diese Verwendungsart wird als PPP-Einwahloption bezeichnet. Sie kann für den Zugriff ins LAN benutzt werden, das sich hinter dem mGuard befindet, oder für die Konfiguration des mGuards. In Firewall-Auswahllisten wird für diese Verbindungsart die Interface-Bezeichnung *Einwahl* verwendet.

Damit Sie mit einem Windows-Rechner über die Wählverbindung auf das LAN zugreifen können, muss auf diesem Rechner eine Netzwerkverbindung eingerichtet sein, in der die Wählverbindung zum mGuard definiert ist. Außerdem muss für diese Verbindung die IP-Adresse des mGuards (oder dessen Hostname) als Gateway definiert werden, damit die Verbindungen ins LAN darüber geroutet werden.

Um auf die Web-Konfigurationsoberfläche des mGuards zuzugreifen, müssen Sie in die Adressenzeile des Web-Browser die IP-Adresse des mGuards (oder dessen Hostname) eingeben.

– Die serielle Schnittstelle des mGuards wird mit der seriellen Schnittstelle eines PCs verbunden.

  Auf dem PC wird mittels eines Terminalprogramms die Verbindung zum mGuard gestellt und die Konfiguration wird über die Kommandozeile des mGuards durchgeführt.

Sofern an der seriellen Schnittstelle ein externes Modem angeschlossen ist, sind gegebenenfalls weiter unten unter *Externes Modem* die passenden Einstellungen zu machen, unabhängig davon, für welche Nutzungsart Sie die serielle Schnittstelle und das an ihr angeschlossene Modem einsetzen.

Netzwerk >> Serielle Schnittstelle >> Modem

Externes Modem (Nicht bei TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005, FL MGUARD RS2000)	**Hardware-Handshake RTS/CTS**	**Aus / Ein** Bei **Ein** findet bei der PPP-Verbindungen Flusssteuerung durch RTS- und CTS-Signale statt.
	Baudrate	**Standard: 57600 / (FL MGUARD GT/GT: 38400).** Übertragungsgeschwindigkeit für die Kommunikation zwischen mGuard und Modem, die über das serielle Verbindungskabel zwischen den beiden Geräten verläuft. Der Wert sollte so hoch eingestellt werden, wie es das Modem unterstützt. Ist der Wert niedriger eingestellt als die Geschwindigkeit, welche das Modem auf der Telefonleitung erreichen kann, dann wird die Telefonleitung nicht voll ausgenutzt.
	Verwende das Modem transparent (nur bei Einwahl)	Wird das externe Modem zur Einwahl verwendet (siehe Seite 191), dann bedeutet die Aktivierung der Funktion, dass der mGuard das Modem nicht initialisiert. Die nachfolgend konfigurierte Modem-Initialisierungssequenz wird nicht beachtet. So kann entweder ein Modem angeschlossen werden, das von selbst Anrufe annimmt (Standard-Profil des Modems beinhaltet „Auto-Answer“), oder es kann anstelle des Modems ein Null-Modem-Kabel zu einem Computer und darüber das PPP-Protokoll verwendet werden.
	Modem-Initialisierungssequenz	Gibt die Initialisierungssequenz an, die der mGuard zum angeschlossenen Modem sendet. Standard: '' \d+++\dATH OK Schlagen Sie im Handbuch zum Modem nach, wie die Initialisierungssequenz für diese Modem lautet.

Netzwerk >> Serielle Schnittstelle >> Modem [...]

Die Initialisierungssequenz ist eine Folge von Zeichenketten, die vom Modem erwartet werden und von Befehlen, die daraufhin an das Modem gesendet werden, damit das Modem eine Verbindung aufbauen kann.

Die voreingestellte Initialisierungssequenz hat folgende Bedeutung:

" (zwei einfache, direkt hintereinander gesetzte Anführungszeichen)	Die leere Zeichenkette innerhalb der Anführungsstriche bedeutet, dass der mGuard am Anfang keine Information vom angeschlossene Modem erwartet, sondern direkt den folgenden Text an das Modem sendet.
\d+++\dATH	Diese Zeichenkette sendet der mGuard an das Modem, um dessen Bereitschaft zum Annehmen von Kommandos festzustellen.
OK	Gibt an, dass der mGuard vom Modem die Zeichenkette ***OK*** als Antwort auf ***\d+++\dATH*** erwartet.

Bei vielen Modem-Modellen ist es möglich, Modem-Voreinstellungen im Modem selber abzuspeichern. Doch sollte auf diese Möglichkeit besser verzichtet werden.

Initialisierungssequenzen sollten statt dessen lieber extern, d. h. beim mGuard konfiguriert werden. Dann kann bei einem Defekt des Modems dieses schnell und problemlos ausgetauscht werden, ohne auf Modem-Voreinstellungen zu achten.

Soll das externe Modem für eingehende Rufe verwendet werden, ohne dass die Modem-Voreinstellungen darauf ausgelegt sind, dann müssen Sie dem Modem mitteilen, dass es hereinkommende Rufe nach dem Klingeln annehmen soll.

Bei Verwendung des erweiterten HAYES-Befehlssatzes geschieht dies durch das Anhängen der Zeichen „ ***AT&S0=1 OK***“ (ein Leerzeichen gefolgt von „***AT&S0=1***“, gefolgt von einem Leerzeichen, gefolgt von „***OK***“) an die Initialisierungssequenz.

Manches externe Modem benötigt gemäß seiner Werkseinstellungen zur korrekten Funktion die physikalische Verbindung mit der DTR-Leitung der seriellen Schnittstelle.

Weil die mGuard-Modelle diese Leitung an der externen seriellen Schnittstelle nicht zur Verfügung stellen, muss dann die obige Initialisierungssequenz um die anzuhängenden Zeichen „ ***AT&D0 OK***“ (ein Leerzeichen gefolgt von „***AT&D0***“, gefolgt von einem Leerzeichen, gefolgt von „***OK***“) erweitert werden. Gemäß des erweiterten HAYES-Befehlssatz bedeutet diese Sequenz, dass das Modem die DTR-Leitung nicht verwendet.

Soll das externe Modem für ausgehende Rufe verwendet werden, ist es an einer Nebenstellenanlage angeschlossen, und erzeugt diese Nebenstellenanlage kein Freizeichen nach dem Abheben, dann muss das Modem angewiesen werden, vor dem Wählen nicht auf ein Freizeichen zu warten.

In diesem Fall erweitern Sie die Initialisierungssequenz um die anzuhängenden Zeichen „ ***ATX3 OK***“ (ein Leerzeichen gefolgt von „***ATX3***“, gefolgt von einem Leerzeichen, gefolgt von „***OK***“).

In dem Fall sollten Sie in die *Anzurufende Telefonnummer* nach der Ziffer zur Amtsholung das Steuerzeichen „***W***“ einfügen, damit auf das Freizeichen gewartet wird.

Beim FL MGUARD RS mit eingebautem Modem / eingebautem ISDN-Modem (ISDN-Terminaladapter)

Der FL MGUARD RS verfügt optional über ein eingebautes Analog-Modem / einen eingebauten ISDN-Terminaladapter. Das eingebaute Modem bzw. der eingebaute ISDN-Terminaladapter kann wie folgt benutzt werden:

Primäres externes Interface

– Als **primäres externes Interface**, wenn unter *Netzwerk* >> *Interfaces*, auf der Registerkarte *Allgemein* als Netzwerk-Modus *Eingebautes Modem* eingestellt ist (siehe „Netzwerk >> Interfaces“ auf Seite 135 und „Allgemein“ auf Seite 142). In diesem Fall wird der Datenverkehr nicht über den WAN-Port (= Ethernet-Schnittstelle) abgewickelt, sondern über dieses Modem.

Sekundäres externes Interface

– Als **sekundäres externes Interface**, wenn unter *Netzwerk* >> *Interfaces*, Registerkarte *Allgemein* das *sekundäre externe Interface* aktiviert und *Eingebautes Modem* ausgewählt ist (siehe „Netzwerk >> Interfaces“ auf Seite 135 und „Allgemein“ auf Seite 142). In diesem Fall wird Datenverkehr auch über die serielle Schnittstelle abgewickelt.

PPP-Einwahloption

– für die PPP-Einwahloption (siehe „Nutzungsarten der seriellen Schnittstelle“ auf Seite 194)

Beachten Sie, dass die serielle Schnittstelle des Gerätes zusätzlich vergleichbare Nutzungsmöglichkeiten zur Verfügung stellt (siehe oben). So kann beim FL MGUARD RS mit eingebautem Modem z. B. der normale Datenverkehr über eine Modemverbindung erfolgen (Netzwerk-Modus *Modem*) und gleichzeitig eine zweite Modemverbindung für die PPP-Einwahloption genutzt werden.

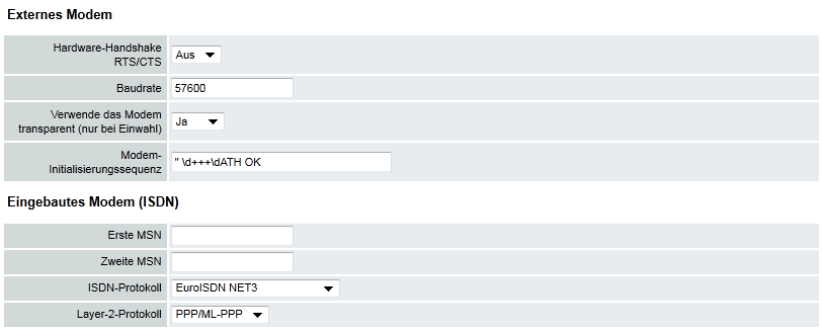
Beim FL MGUARD RS mit eingebautem Modem

Zusätzlich beim FL MGUARD RS mit eingebautem Modem (analog)

Netzwerk >> Interfaces >> Modem/Konsole (Beim FL MGUARD RS mit eingebautem Modem)		
Externes Modem	**Wie beim TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4004, FL MGUARD RS (ohne eingebautes Modem), FL MGUARD DELTA, mGuard centerport (Innominate), FL MGUARD CENTERPORT, FL MGUARD BLADE, mGuard delta (Innominate):** Konfiguration wie oben für **Externes Modem** (siehe „Externes Modem“ auf Seite 195).	
Eingebautes Modem (analog)	**Staat**	Hier muss der Staat angegeben werden, in dem der mGuard mit seinem eingebautem Modem betrieben wird. Nur dann ist gewährleistet, dass sich das eingebaute Modem gemäß der in diesem Staat gültigen Fernmeldevorschriften verhält und z. B. Rufton und Wählton richtig erkennt und entsprechend reagiert.
	Nebenstelle (bzgl. Amtsholung)	Bei **Nein** erwartet der mGuard bei Anschaltung ans Telefonnetz den Wählton, wenn der mGuard die Gegenstelle anwählen will. Bei **Ja** erwartet der mGuard keinen Wählton sondern beginnt gleich mit der Anwahl der Gegenstelle. Dieses Verhalten kann notwendig sein, wenn das eingebaute Modem des mGuards an einer privaten Nebenstellenanlage angeschlossen ist, bei der beim „Abheben“ kein Wählton ausgegeben wird. Wenn zur Anwahl nach draußen (Amtsholung) eine bestimmte Nummer, z. B. „0“ gewählt werden muss, ist diese der anzuwählenden Telefonnummer der gewünschten Gegenstelle voran zu stellen.
	Lautstärke (eingebauter Lautsprecher)	
	Lautsprechernutzung	Diese beiden Einstellungen legen fest, was der eingebaute Lautsprecher des mGuards wiedergeben soll und in welcher Lautstärke.

Beim FL MGUARD RS mit eingebautem ISDN-Terminaladapter

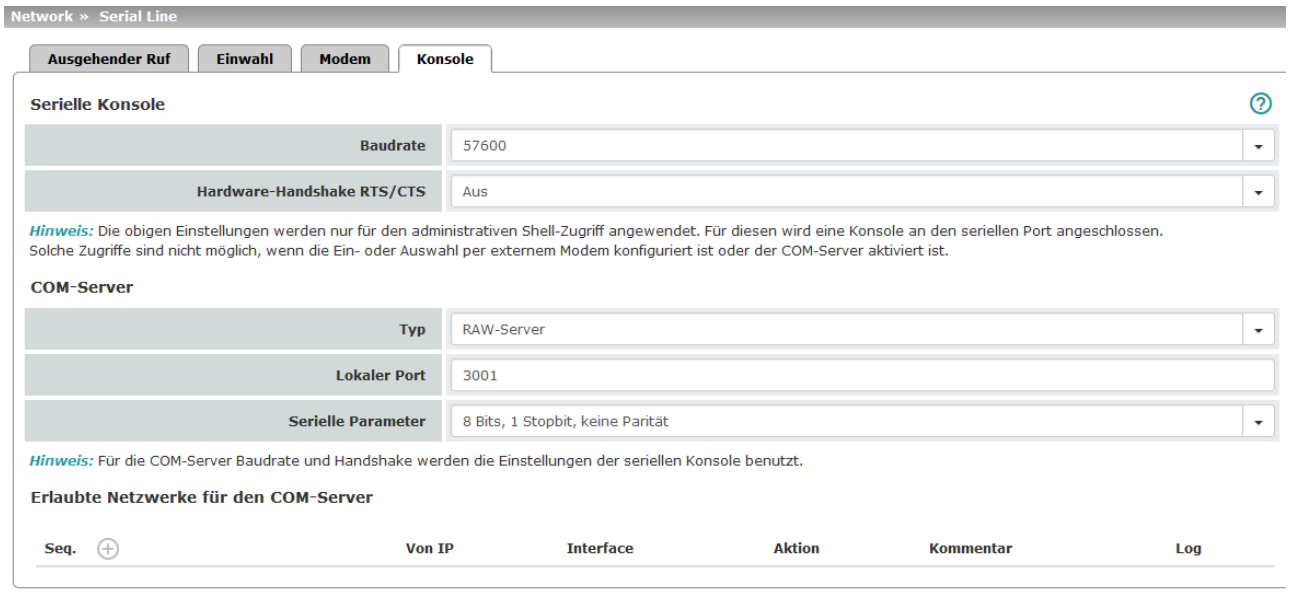
Zusätzlich beim FL MGUARD RS mit eingebautem Modem (ISDN)



Netzwerk >> Interfaces >> Modem/Konsole (Beim FL MGUARD RS mit ISDN-Terminaladapter)		
Externes Modem	**Wie beim FL MGUARD RS4000, TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4004, FL MGUARD RS (ohne eingebautes Modem), mGuard centerport (Innominate), FL MGUARD CENTERPORT, FL MGUARD BLADE, mGuard delta (Innominate):**	
	Konfiguration wie oben für **Externes Modem** (siehe „Externes Modem“ auf Seite 195).	
Eingebautes Modem (ISDN)	**Erste MSN**	Bei ausgehenden Rufen überträgt der mGuard die hier eingetragene MSN (Multiple Subscriber Number) zur angerufenen Gegenstelle. Außerdem ist der mGuard unter dieser MSN für eingehende Anrufe erreichbar (sofern Einwahl ermöglicht ist, siehe Registerkarte Allgemein). Max. 25 Ziffern/Zeichen; folgende Sonderzeichen können verwendet werden: *****, **#**, **:** (Doppelpunkt)
	Zweite MSN	Soll der mGuard für Einwahl (sofern ermöglicht) zusätzlich unter einer anderen Nummer erreichbar sein, tragen Sie hier eine zweite MSN ein.
	ISDN-Protokoll	In Deutschland und vielen anderen europäischen Länder wird das ISDN-Protokoll EuroISDN verwendet, auch NET3 genannt. Ansonsten ist länderspezifisch festgelegt, welches ISDN-Protokoll benutzt wird. Muss gegebenenfalls bei der zuständigen Telefongesellschaft erfragt werden
	Layer-2-Protokoll	Das Regelwerk, über das sich der ISDN-Terminaladapter des lokalen mGuard mit seiner ISDN-Gegenstelle verständigt. Das ist im Allgemeinen das ISDN-Modem des Internet Service Providers, über das die Verbindung ins Internet hergestellt wird. Muss beim Internet Service Provider erfragt werden. Sehr häufig wird PPP/ML-PPP verwendet.

6.3.4 Konsole

Nur *TC MGUARD RS4000 3G, TC MGUARD RS2000 3G (nur Konsole), FL MGUARD RS4004, FL MGUARD RS4000/RS2000, mGuard centerport (Innominate), FL MGUARD CENTERPORT, FL MGUARD RS, FL MGUARD SMART2* , *FL MGUARD DELTA* (**nicht** *FL MGUARD SMART 533/266, FL MGUARD PCI(E)4000, FL MGUARD BLADE).*



Netzwerk >> Serielle Schnittstelle >> Konsole

Serielle Konsole

Die nachfolgende Einstellungen für *Baudrate* und *Hardware-Handshake* gelten nur für eine Konfigurationsverbindung, wenn wie oben beschrieben ein Terminal bzw. ein PC mit Terminalprogramm an der seriellen Schnittstelle angeschlossen wird.

Die Einstellungen sind nicht gültig, wenn ein externes Modem angeschlossen wird. Die Einstellung dafür erfolgt unter „Modem“ auf Seite 194.

Baudrate

9600 / 19200 / 38400 / 57600 (Standard) / 115200

(**Standard FL MGUARD GT/GT: 38400**)

Über die Auswahlliste wird festgelegt, mit welcher Übertragungsgeschwindigkeit die serielle Schnittstelle arbeiten soll.

Hardware-Handshake RTS/CTS

Aus / Ein

Bei **Ein** findet eine Flusssteuerung durch RTS- und CTS-Signale statt.

Netzwerk >> Serielle Schnittstelle >> Konsole [...]

	Serielle Konsole über USB (Nur FL MGUARD SMART2)	Bei deaktivierter Funktion nutzt der FL MGUARD SMART2 den USB-Anschluss ausschließlich zur Stromversorgung. Bei aktivierter Funktion stellt der FL MGUARD SMART2 zusätzlich über die USB-Schnittstelle eine serielle Schnittstelle für den angeschlossenen Rechner zur Verfügung. Auf dem Rechner kann mit Hilfe eines Terminal-Programmes auf die serielle Schnittstelle zugegriffen werden. Über die serielle Schnittstelle stellt der FL MGUARD SMART2 eine Konsole zur Verfügung, die dann im Terminal-Programm genutzt werden kann. Um die serieller Konsole über USB zu benutzen, benötigen Sie unter Windows einen speziellen Treiber. Dieser kann direkt vom mGuard heruntergeladen werden.
	Serieller USB-Treiber (Windows) (Nur FL MGUARD SMART2)	Klicken Sie auf die Schaltfläche „Lade Windows-Treiber von diesem Gerät herunter“, um den Windows-Treiber herunterzuladen.
COM-Server (Nur bei mGuard-Plattformen mit serieller Schnittstelle)	Die mGuard-Plattformen mit serieller Schnittstelle verfügen ab Firmware 8.0 über einen integrierten COM-Server. Dieser ermöglicht einen Datenaustausch der seriellen Schnittstelle über eine IP-Verbindung. Es stehen drei Optionen zur Verfügung. – **RFC 2217** (Telnet-Server, konform zur RFC 2217). In diesem Modus kann die serielle Schnittstelle über eine Client-Software im Netzwerk konfiguriert werden. Der Telnet-Server ist unter dem Port erreichbar, der unter **„Lokaler Port“** definiert wird. – **RAW-Client** In diesem Modus initiiert der mGuard eine Verbindung zu der Adresse, die unter **„IP-Adresse der Gegenstelle“** eingestellt wird. Die Verbindung läuft über den Port, der unter **„Remote-Port“** konfiguriert wird. Die Schnittstelle kann hier konfiguriert werden („Serielle Parameter“). Für die Baudrate und den Hardware-Handshake werden die Einstellungen der seriellen Konsole genutzt (siehe „Externes Modem“ unter „Netzwerk >> Serielle Schnittstelle >> Modem“). – **RAW-Server** Verhält sich wie der RAW-Client. Allerdings antwortet der RAW-Server auf eingehende Verbindungen unter dem Port, der unter **„Lokaler Port“** konfiguriert ist.	
	Typ	Hier kann ausgewählt werden, in welcher Ausprägung der COM-Server agieren soll. Möglich sind: RFC 2217, RAW-Client, RAW-Server.
	IP-Adresse der Gegenstelle (Nur bei Typ **RAW-Client)**	**Standard: 10.1.0.254** Definiert die IP-Adresse der Gegenstelle.
	Lokaler Port (Nur bei Typ **RFC 2217** und **RAW-Server**)	**Standard: 3001** Definiert, auf welchem Port der COM-Server reagieren soll. Werte: 1 – 65535.

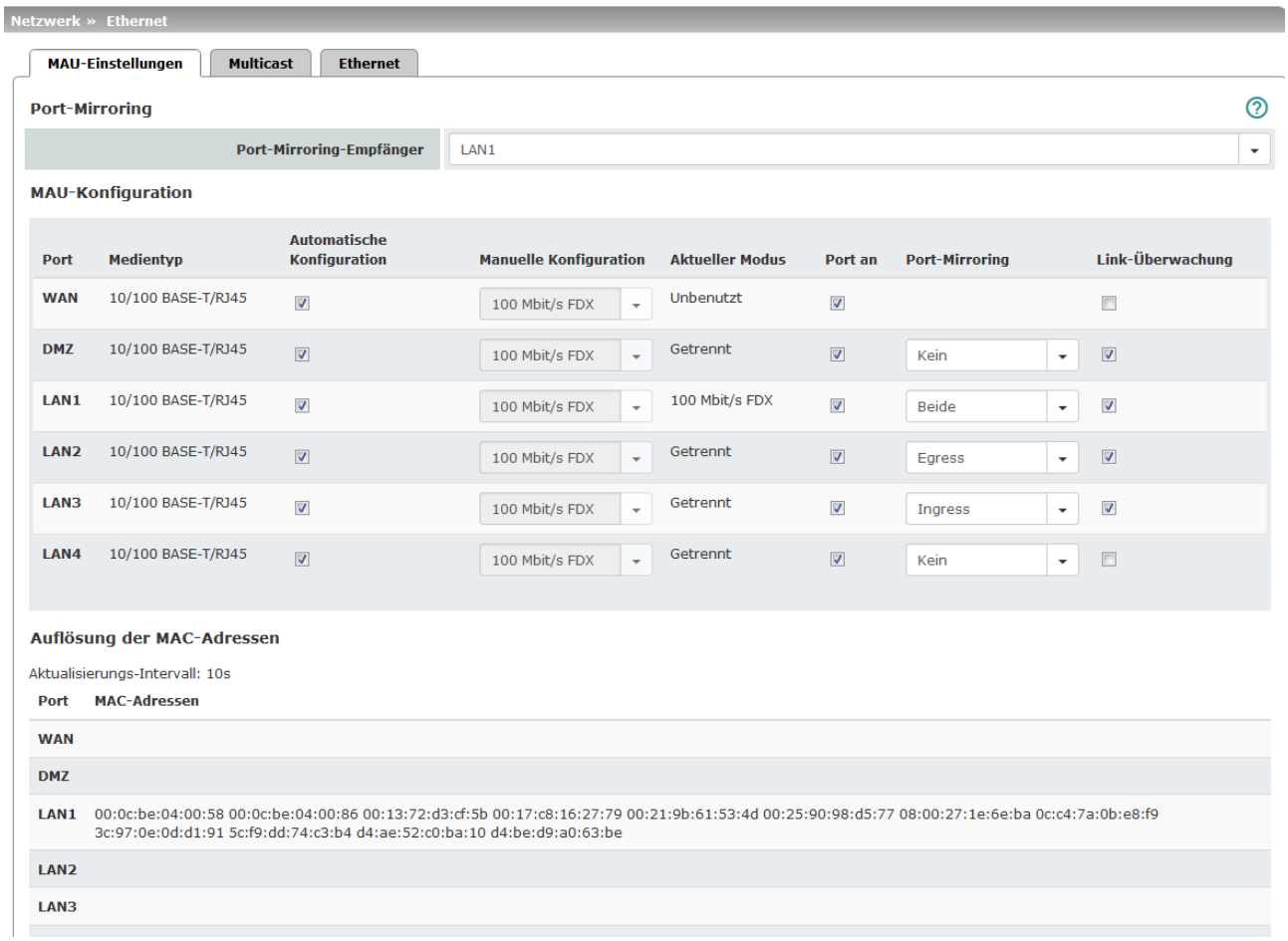
Netzwerk >> Serielle Schnittstelle >> Konsole [...]

	Remote-Port (Nur bei Typ **RAW-Client)**	**Standard: 3001** Definiert, an welchen Port der RAW-Client die Daten sendet. Werte: 1 – 65535.
	Über VPN (Nur bei Typ **RAW-Client)**	Die Anfrage des COM-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 **Über VPN** 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.
	Serielle Parameter	Definiert die Paritäts- und Stopbits der seriellen Schnittstelle. Unterstützte Paketlängen der seriellen Schnittstelle: 8 Bit / 7 Bit. – 8 Bits (7 Bits), 1 Stopbit, keine Parität (Standard mit 8 Bit) – 8 Bits (7 Bits), 1 Stopbit, gerade Parität – 8 Bits (7 Bits), 1 Stopbit, ungerade Parität – 8 Bits (7 Bits), 2 Stopbits, keine Parität – 8 Bits (7 Bits), 2 Stopbits, gerade Parität – 8 Bits (7 Bits), 2 Stopbits, ungerade Parität
Erlaubte Netzwerke für den COM-Server	Um einen nicht-autorisierten Zugriff auf den COM-Server zu verhindern, können Zugriffsregeln für den COM-Server definiert werden. Die Standardregel lässt keine Zugriffe über das externe Interface zu.	
	Von 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 26).
	Interfaces	**Intern / Extern / Extern 2 / DMZ / VPN / GRE / Einwahl** Schnittstelle, für die diese Regel angewendet werden soll.

Netzwerk >> Serielle Schnittstelle >> Konsole [...]		
	Aktion	**Annehmen** bedeutet, dass die Datenpakete passieren dürfen. **Abweisen** bedeutet, dass die Datenpakete zurückgewiesen werden. Der Absender erhält eine Information über die Zurückweisung. **Verwerfen** bedeutet, dass die Datenpakete nicht passieren dürfen. Der Absender erhält keine Information über deren Verbleib.
	Kommentar	Ein frei wählbarer Kommentar für diese Regel.
	Log	Für jede Firewall-Regel können Sie festlegen, ob beim Greifen der Regel das Ereignis protokolliert werden soll.

6.4 Netzwerk >> Ethernet

6.4.1 MAU-Einstellungen



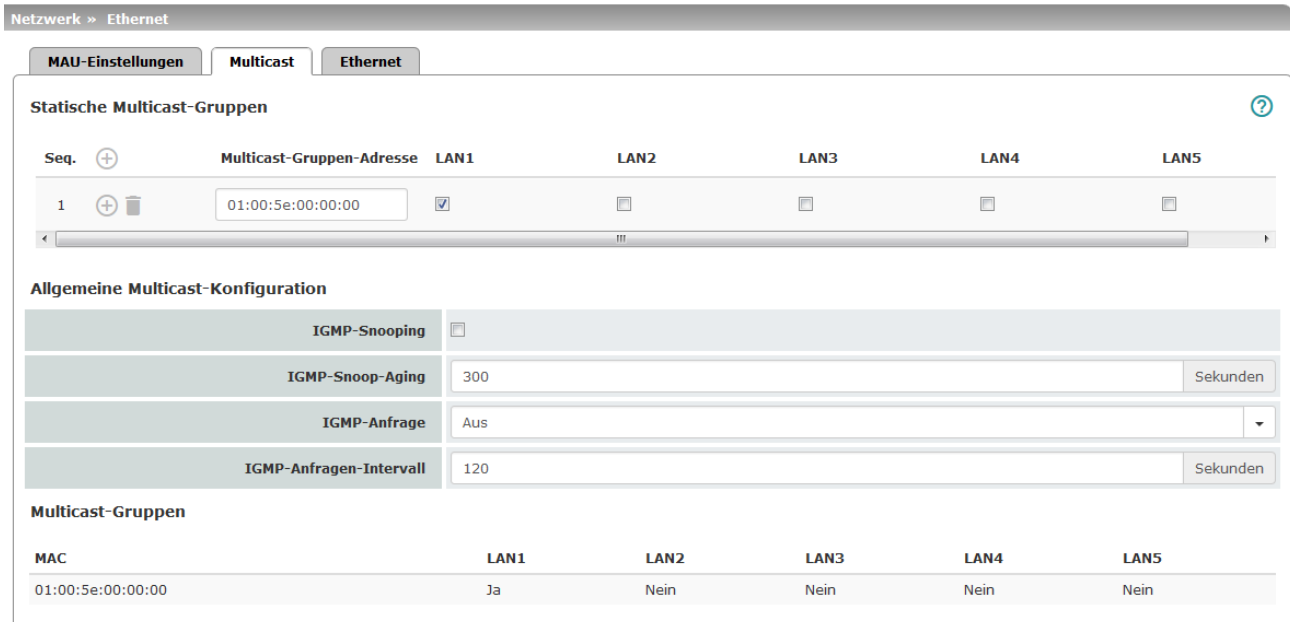
Netzwerk >> Ethernet >> MAU-Einstellungen		
Port Mirroring (Nur bei TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4004)	**Port-Mirroring-Empfänger**	Der integrierte Switch beherrscht das Port-Mirroring, um den Netzwerkverkehr zu beobachten. Dabei können Sie entscheiden, welche Ports Sie beobachten wollen. Der Switch schickt dann Kopien von Datenpaketen der beobachteten Ports an einen dafür ausgewählten Port. Die Port-Mirroring-Funktion ermöglicht es, beliebige Pakete an einen bestimmten Empfänger weiterzuleiten. Sie können den Empfänger-Port oder die Spiegelung der ein- und ausgehende Pakete von jedem Switch-Port auswählen.
MAU-Konfiguration (Nicht bei TC MGUARD RS2000 3G, TC MGUARD RS2000 4G)	Konfiguration und Statusanzeige der Ethernet-Anschlüsse:	

Netzwerk >> Ethernet >> MAU-Einstellungen [...]		
	Port	Name des Ethernet-Anschlusses, auf welchen sich die Zeile bezieht.
	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.
	Aktuelle Betriebsart	Die aktuelle Betriebsart des Netzwerkanschlusses.
	Port an	Schaltet den Ethernet-Anschluss auf Ein oder Aus. Die Funktion **Port an** wird **nicht** unterstützt vom mGuard centerport (Innominate), FL MGUARD CENTERPORT. Die Funktion **Port an** wird mit Einschränkung unterstützt von: **mGuard delta (Innominate)**: hier lässt sich die interne Seite (Switch-Ports) nicht abschalten. **FL MGUARD PCI 533/266**: hier lässt sich im Treibermodus die interne Netzwerkschnittstelle nicht abschalten (wohl aber im Power-over-PCI-Modus).
	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	Die Port Mirroring-Funktion ermöglicht es, beliebige Pakete an einen bestimmten Empfänger weiterzuleiten. Sie können den Empfänger-Port oder die Spiegelung der ein- und ausgehende Pakete von jedem Switch-Port auswählen.
Auflösung der MAC-Adressen (Nur bei TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4004)	**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 TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4004)	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

Netzwerk >> Ethernet >> MAU-Einstellungen [...]		
	TX-Oktette	Gesendetes Datenvolumen
	RX-FCS-Fehler	Anzahl an empfangenen Frames mit ungültiger Prüfsumme
	RX-gültige Oktette	Volumen der empfangene gültigen Daten

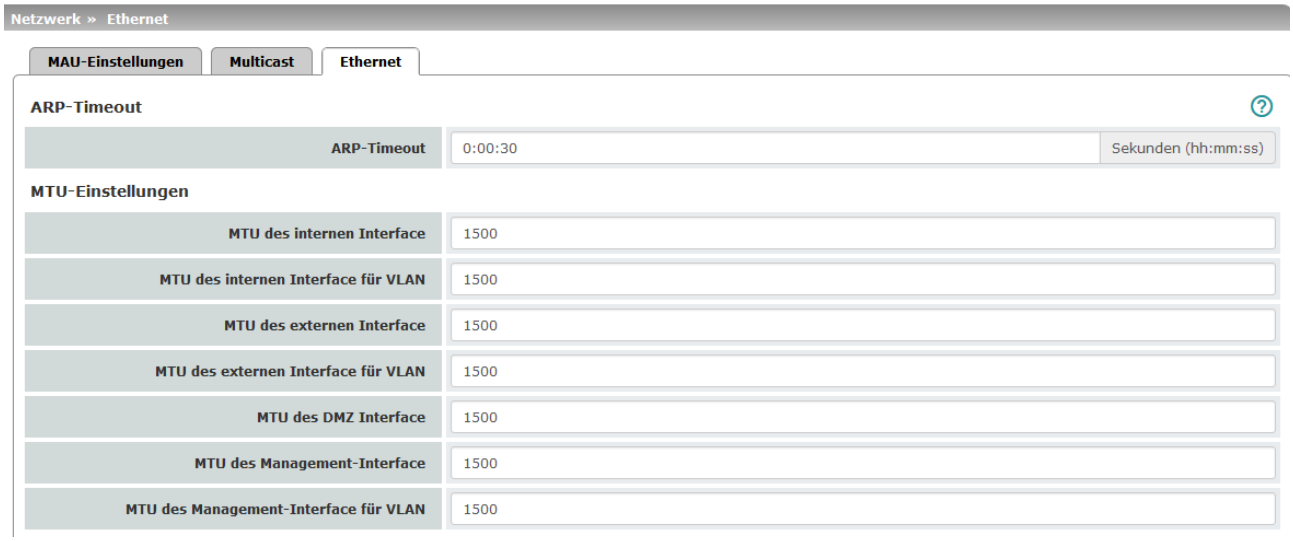
6.4.2 Multicast

Nur verfügbar beim TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4004.



Netzwerk >> Ethernet >> Multicast		
Statische Multicast-Gruppen	**Statische Multicast-Gruppen**	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 (LAN1 ... LAN5) weitergeleitet.
Allgemeine Multicast-Konfiguration	**IGMP-Snooping**	Durch IGMP-Snooping garantiert der Switch, dass Multicast-Daten nur über Ports weitergeleitet werden, die für diese Anwendung vorgesehen sind.
	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 (Version v3 wird nicht unterstützt)
	IGMP-Anfrage-Intervall	Abstand, in dem IGMP-Anfragen erzeugt werden in Sekunden
Multicast-Gruppen	Anzeige der Multicast-Gruppen. Die Anzeige enthält alle statischen Einträge und die dynamischen Einträge, die durch IGMP-Snooping entdeckt werden.	

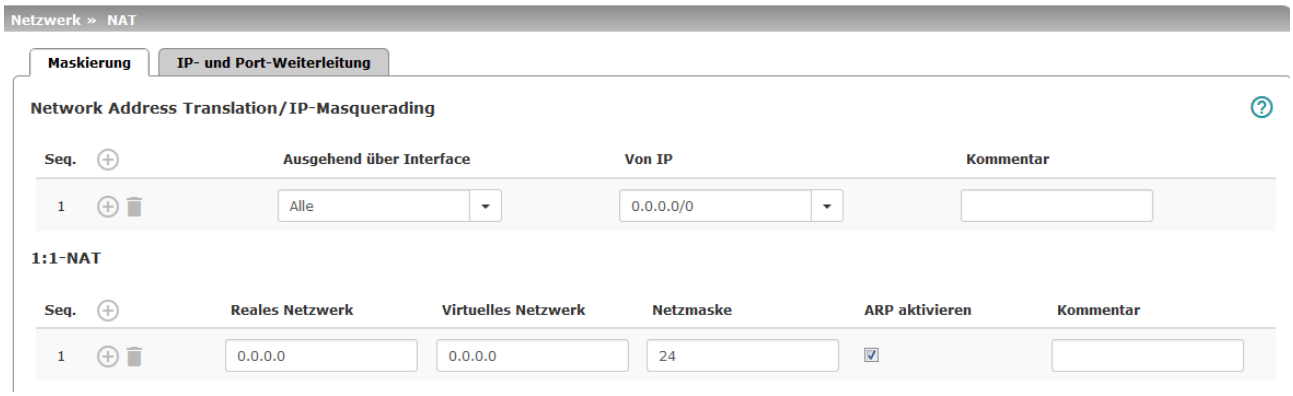
6.4.3 Ethernet



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. 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.

6.5 Netzwerk >> NAT

6.5.1 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 den internen Geräten zu verbergen. Dazu können Sie unter **Ausgehend über Interface** die Auswahl **Intern** einstellen. Die Einstellung **Intern** ermöglicht die Kommunikation zwischen zwei separaten IP-Netzen, bei denen die IP-Geräte keine (sinnvolle) Standard-Route bzw. differenziertere Routing-Einstellungen konfiguriert haben (z. B. SPSsen ohne entsprechende Einstellung). Dazu müssen unter **1:1-NAT** die entsprechenden Einstellungen vorgenommen werden.

Dieses Verfahren wird auch *IP-Masquerading* genannt.

Werkseinstellung: Es findet kein NAT statt.

Arbeitet der mGuard im *PPPoE/PPTP*-Modus, muss NAT aktiviert werden, um Zugriff auf das Internet zu erhalten. Ist NAT nicht aktiviert, können nur VPN-Verbindungen genutzt werden.

Bei der Verwendung von mehreren statischen IP-Adressen für den WAN-Port wird immer die erste IP-Adresse der Liste für IP-Masquerading verwendet.

Im Stealth-Modus werden die Regeln nicht angewendet.

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

Ausgehend über Interface	Intern / Extern / Extern 2 / DMZ / Alle Externen[1] Gibt an, über welches Interface die Datenpakete ausgehen, damit sich die Regel auf sie bezieht. Mit **Alle Externen** sind die Interfaces **Extern** und **Extern 2** gemeint Es wird eine Maskierung definiert, die im Router-Modus für Netzwerk-Datenströme gilt. Diese Datenströme werden so initiiert, dass sie zu einem Zielgerät führen, das über die ausgewählte Netzwerkschnittstelle des mGuards erreichbar ist. Dafür ersetzt der mGuard in allen zugehörigen Datenpaketen die IP-Adresse des Initiators durch eine geeignete IP-Adresse der ausgewählten Netzwerkschnittstelle. Die Wirkung ist analog zu den anderen Werten derselben Variablen. Dem Ziel des Datenstroms bleibt die IP-Adresse des Initiators verborgen. Insbesondere benötigt das Ziel keine Routen, nicht einmal eine Standard-Route (Standard-Gateway), um in so einem Datenstrom zu antworten.

Stellen Sie die Firewall so ein, dass die gewünschten Verbindungen erlaubt sind. Für Ein- und Ausgangsregeln gilt, dass die Quelladresse noch dem ursprünglichen Absender entspricht, wenn die Firewall-Regeln angewendet werden.

Beachten Sie bei den Einstellungen „Extern / Extern 2 / Alle Externen“ die Ausgangsregeln (siehe „Ausgangsregeln“ auf Seite 276).

Beachten Sie bei der Einstellung „Intern“ die Eingangsregeln (siehe „Eingangsregeln“ auf Seite 273).

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 26). **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 289).

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.

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

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.

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.

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

1:1-NAT kann nicht auf das Interface *Extern 2* angewendet werden.

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

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.

Ab mGuard-Firmware 8.0.0 ist 1:1-NAT 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).

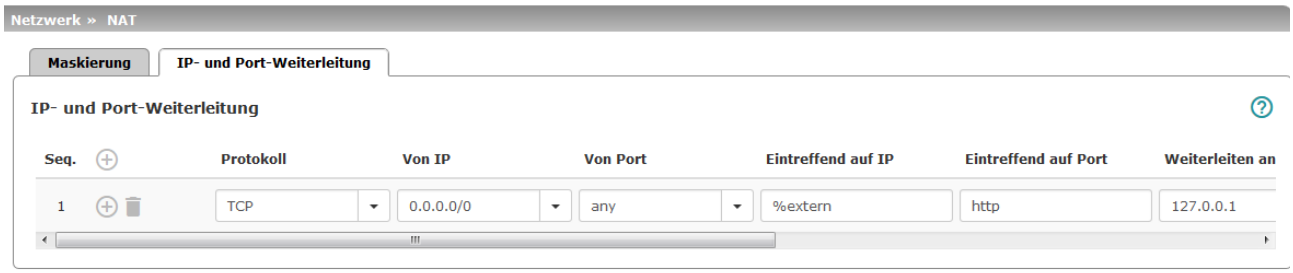
Die virtuellen IP-Adressen dürfen nicht vergeben sein und von anderen Clients verwendet werden.

Ab mGuard-Firmware 8.0.0 ist 1:1-NAT zwischen allen Interfaces möglich (LAN <–> WAN, LAN <–> DMZ, DMZ <–> WAN).

Netzwerk >> NAT >> Maskierung [...]		
	Netzmaske	Die Netzmaske als Wert zwischen 1 und 32 für die lokale und externe Netzwerkadresse (siehe auch „CIDR (Classless Inter-Domain Routing)“ auf Seite 26).
	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.
	Kommentar	Kann mit kommentierendem Text gefüllt werden.

[1] *Extern 2* und *Alle Externen* nur bei Geräten mit serieller Schnittstelle: *TC MGUARD RS4000/RS2000 3G,TC MGUARD RS4000/RS2000 4G , FL MGUARD RS4004/RS2005, FL MGUARD RS4000/RS2000, mGuard centerport (Innominate), FL MGUARD CENTERPORT, FL MGUARD RS, FL MGUARD BLADE, FL MGUARD DELTA, mGuard delta (Innominate)* (siehe „Sekundäres externes Interface“ auf Seite 157).

6.5.2 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.

Port-Weiterleitung kann nicht angewendet werden bei Verbindungen, die über das Interface *Extern 2*[1] initiiert werden.

[1] *Extern 2* nur bei Geräten mit serieller Schnittstelle

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

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 26).

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 289).

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 289).

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.

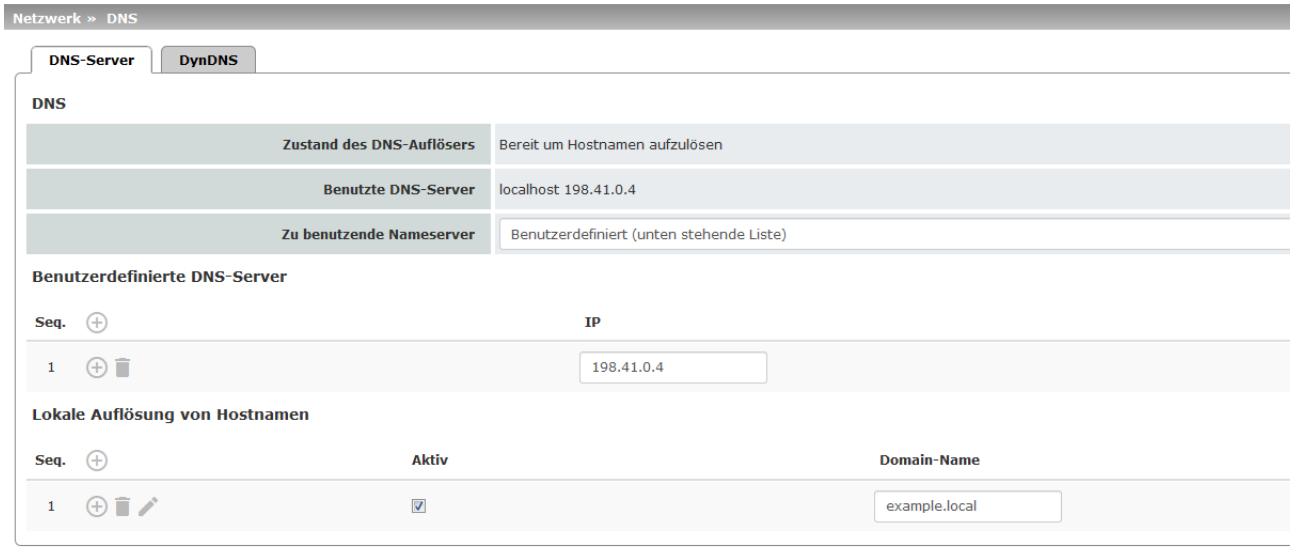
Er kann entweder über die Port-Nummer oder über den entsprechenden Servicenamen angegeben werden, z. B. *pop3* für Port 110 oder *http* für Port 80.

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 (werkseitige Voreinstellung).

6.6 Netzwerk >> DNS

6.6.1 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. **DNS Cache Status** — 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 PPPoE oder 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 *PPPoE*-, im *PPTP*-, *Modem*-Modus oder im *Router*-Modus mit DHCP arbeitet. **Ab mGuard-Firmwareversion 8.6.0** kann die Einstellung 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.	
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.	

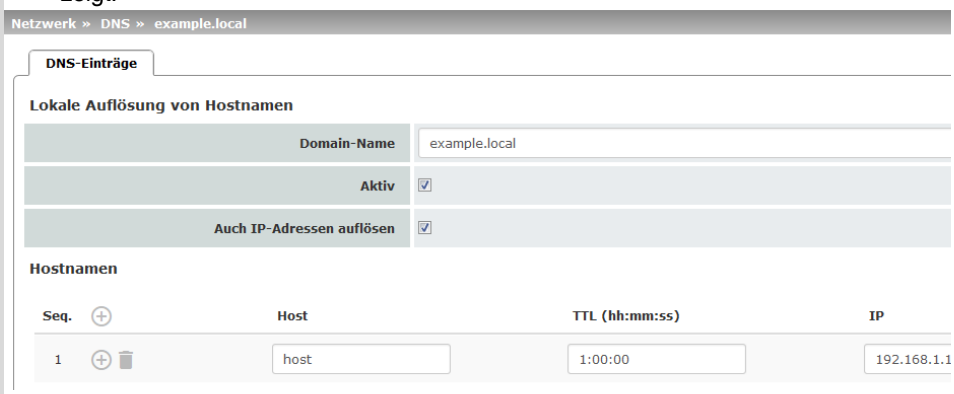
Netzwerk >> DNS >> DNS-Server [...]

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 der Hosts
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)
Abkürzung für **T**ime **T**o **L**ive. Standard: 3600 Sekunden (1:00:00)

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.

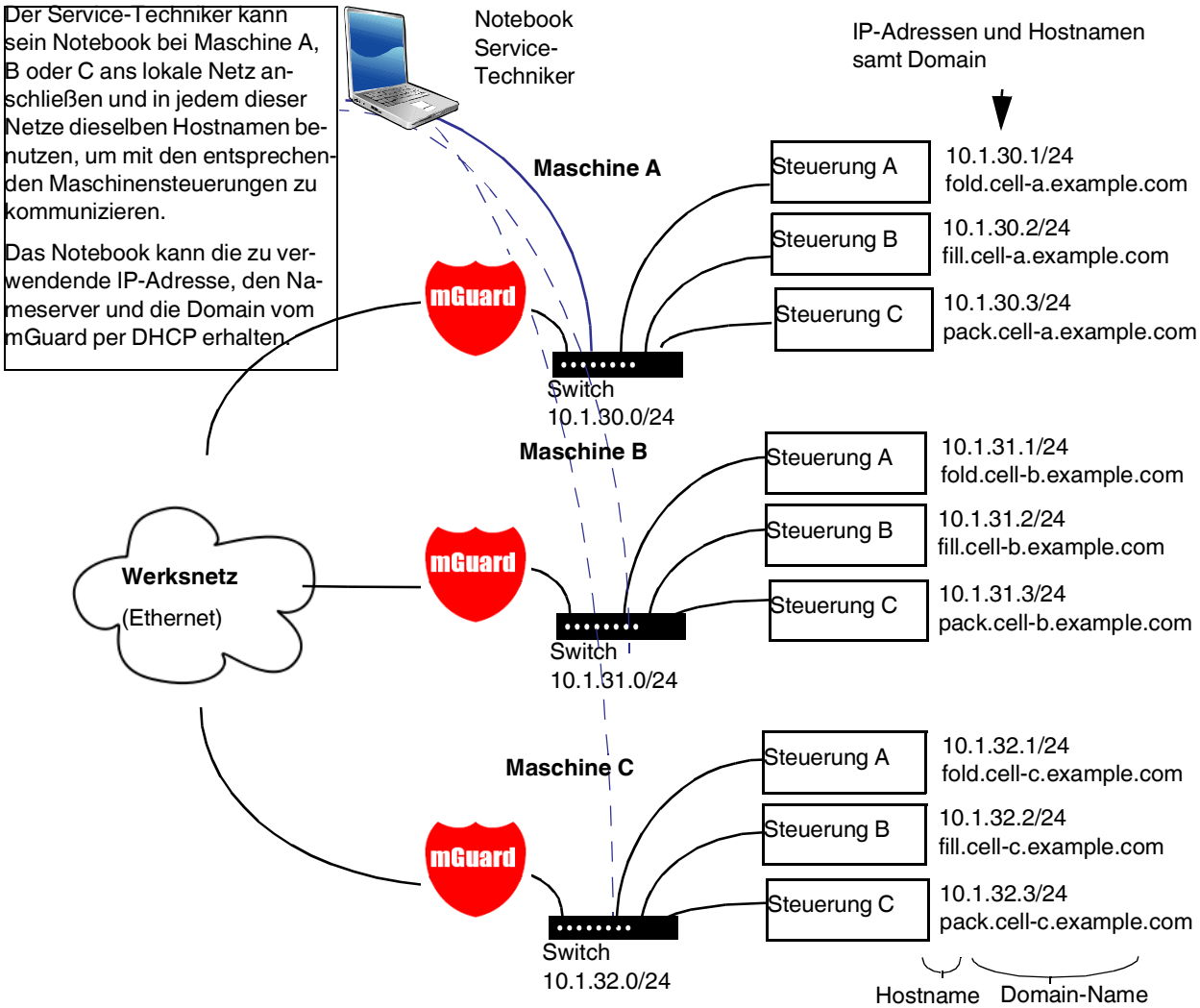
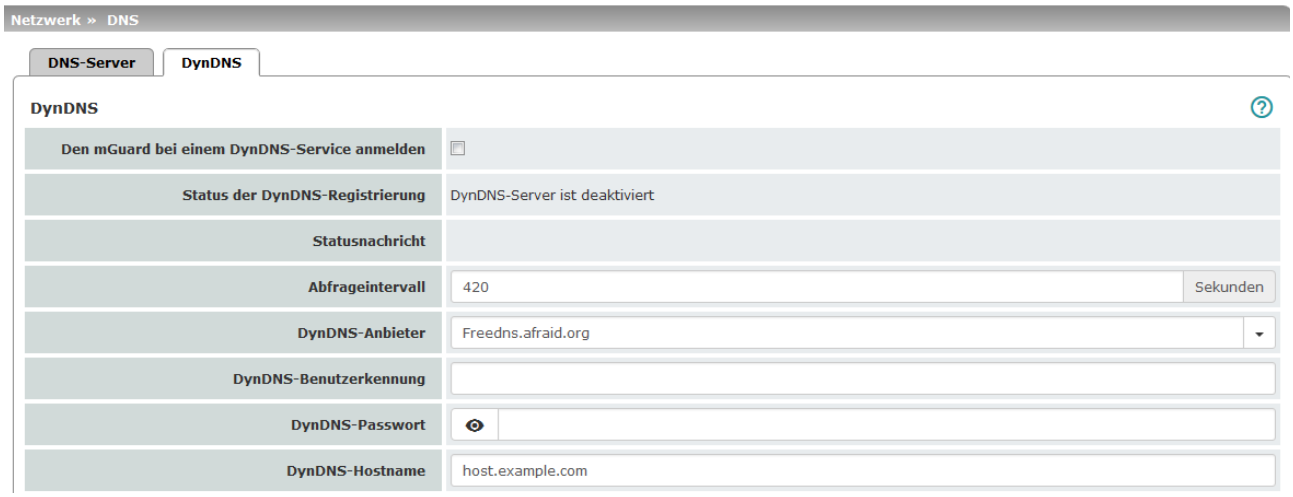


Bild 6-1 Lokale Auflösung von Hostnamen

6.6.2 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.

Beachten Sie beim Einsatz von TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, dass DynDNS nicht von allen Mobilfunk-Providern zugelassen wird.

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.

Abfrageintervall (Sekunden)

Standard: 420 (Sekunden). Immer wenn sich die IP-Adresse des eigenen Internet-Anschlusses ändert, informiert der mGuard den DynDNS-Service über die neue IP-Adresse. 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.

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.

Netzwerk >> DNS >> DynDNS [...]		
	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.

6.7 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.

Die Menüpunkte **Externes DHCP** und **DMZ DHCP** gehören nicht zum Funktionsumfang von FL MGUARD RS2000, TC MGUARD RS2000 3G, TC MGUARD RS2000 4G und FL MGUARD RS2005.

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

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

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

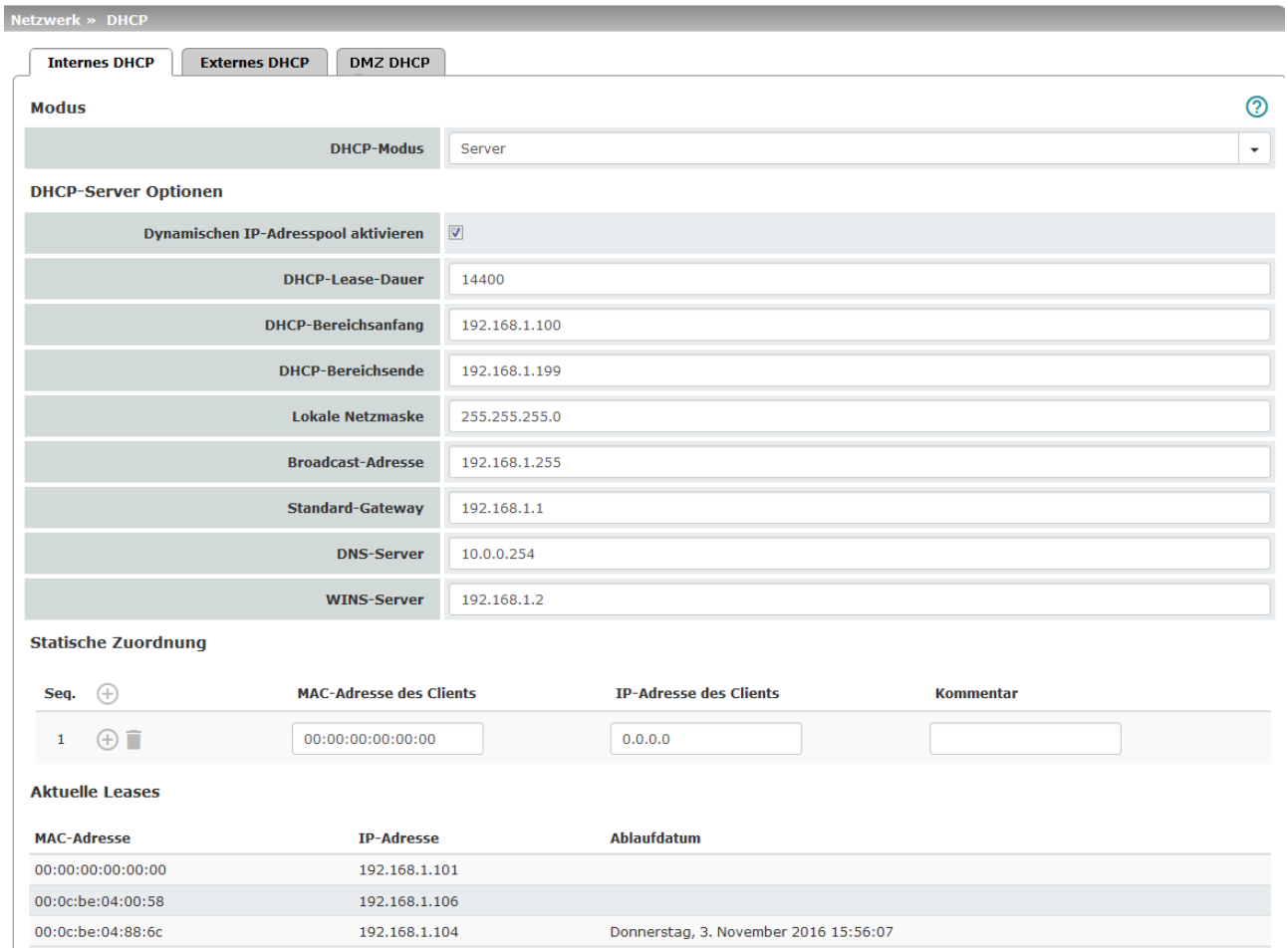
Dazu unter Windows XP

- Im Start-Menü „Systemsteuerung, Netzwerkverbindungen“ wählen.
- Das Symbol des LAN-Adapters mit der rechten Maustaste anklicken und im Kontextmenü auf „Eigenschaften“ klicken.
- Auf der Registerkarte „Allgemein“ unter „Diese Verbindung verwendet folgende Elemente“ den Eintrag „Internetprotokoll (TCP/IP“) markieren und auf die Schaltfläche „Eigenschaften“ klicken.
- Machen Sie im Dialogfeld „Eigenschaften von Internetprotokoll (TCP/IP)“ die entsprechenden Angaben bzw. Einstellungen.

Dazu unter Windows 7

- Über das Start-Menü auswählen: „Systemsteuerung >> Netzwerk und Internet >> Netzwerk- und Freigabecenter“.
- Unter „Verbindungen:“ auf „LAN-Verbindung“ klicken.
- Im Fenster „Status von LAN-Verbindung“ auf die Schaltfläche „Eigenschaften“ klicken (Administrator-Rechte erforderlich).
- Im Fenster „Eigenschaften von LAN-Verbindung“ die Zeile „Internetprotokoll Version 4 (TCP/IPv4)“ auswählen und auf die Schaltfläche „Eigenschaften“ klicken.
- Machen Sie im Dialogfeld „Eigenschaften von Internetprotokoll Version 4 (TCP/IPv4)“ die entsprechenden Angaben bzw. Einstellungen.

6.7.1 Internes / Externes DHCP



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**, wenn der mGuard als eigenständiger DHCP-Server arbeiten soll. Dann werden unten auf der Registerkarte entsprechende Einstellmöglichkeiten eingeblendet (siehe „DHCP-Modus: **Server**“).

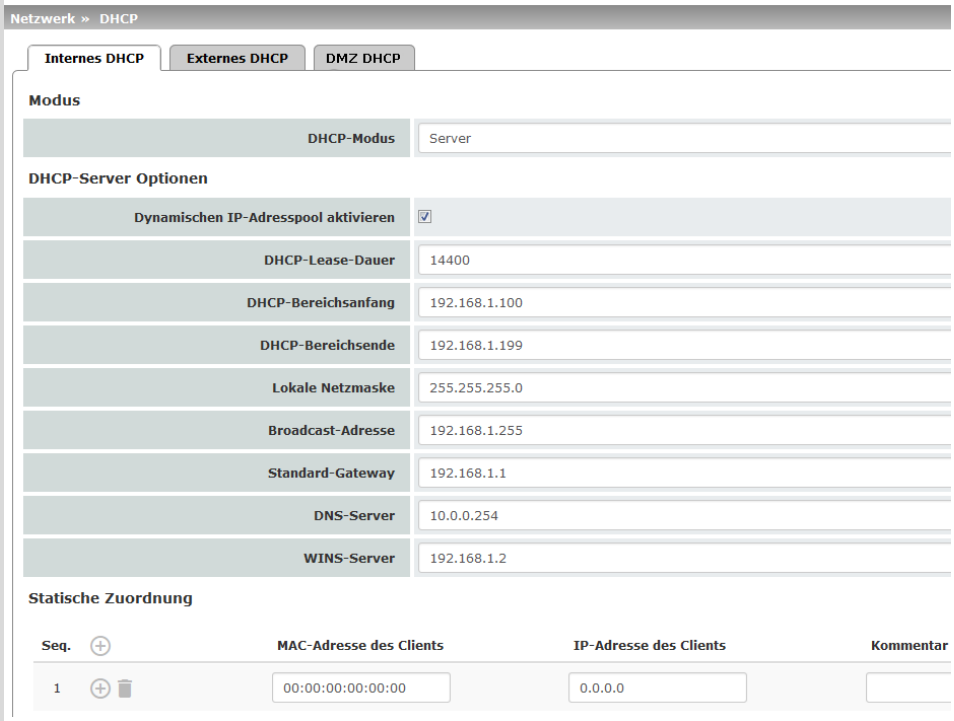
Setzen Sie ihn auf **Relay**, wenn der mGuard DHCP-Anfragen an einen anderen DHCP-Server weiterleiten soll. Dann werden unten auf der Registerkarte entsprechende Einstellmöglichkeiten eingeblendet (siehe „DHCP-Modus: **Relay**“).

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 95/98/ME**: • Starten Sie **winipcfg** in einer DOS-Box. **Windows NT/2000/XP/**: • Starten Sie **ipconfig /all** in einer Eingabeaufforderung. Die MAC-Adresse wird als „Physikalische Adresse“ angezeigt. **Linux**: • Rufen Sie in einer Shell **/sbin/ifconfig** oder **ip link show** auf.

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

Bei den Angaben haben Sie folgende Möglichkeiten:

– MAC-Adresse des Clients/Rechners (ohne Leerzeichen oder Bindestriche).
– IP-Adresse des Clients

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.

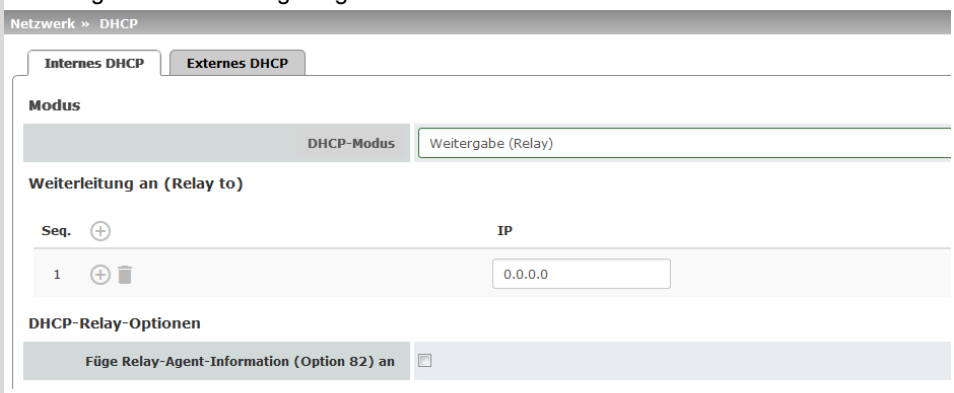
Es sollte nur ein DHCP-Server pro Subnetz verwendet werden.

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

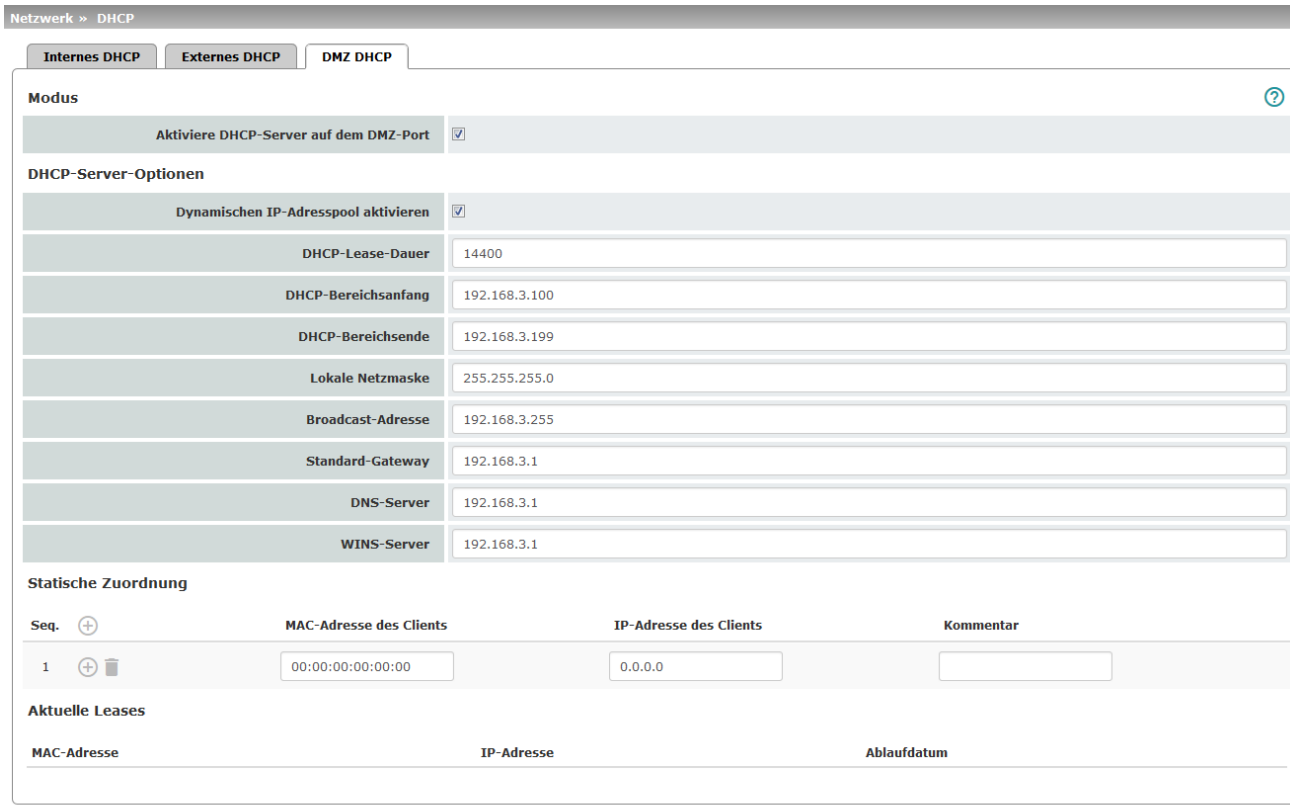
Im *Stealth*-Modus des mGuards wird der DHCP-Modus *Relay* nicht unterstützt. Wird der mGuard im *Stealth*-Modus betrieben und ist der DHCP-Modus *Relay* ausgewählt, wird diese Einstellung ignoriert. Aufgrund der Natur des *Stealth*-Modus werden DHCP-Anfragen des Rechners und die entsprechenden Antworten jedoch durchgeleitet.

DHCP-Server, zu denen weitergeleitet werden soll

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

Netzwerk >> DHCP >> Internes DHCP[...]		
	Füge Relay-Agent-Information (Option 82) an	Beim Weiterleiten können zusätzliche Informationen nach RFC 3046 für die DHCP-Server angefügt werden, an welche weitergeleitet wird.

6.7.2 DMZ DHCP



Ab **mGuard-Firmwareversion 8.6.0** wurde die DHCP-Server-Funktionalität des mGuards auf sein DMZ-Interface (DMZ-Port) erweitert. Der mGuard kann am DMZ-Port angeschlossenen Clients automatisch eine Netzwerkkonfiguration über das DHCP-Protokoll zuweisen.

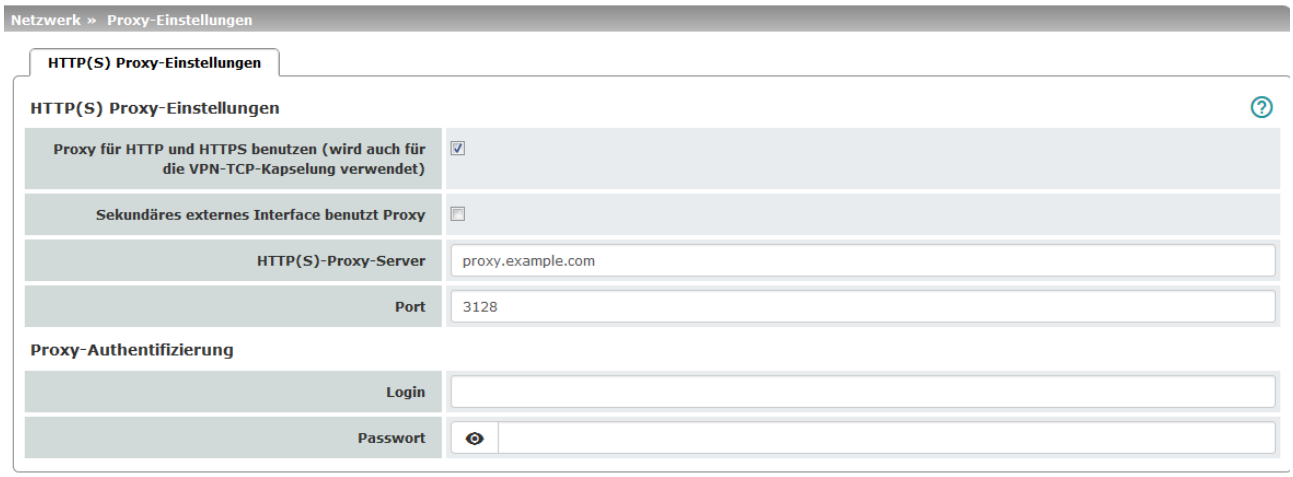
Netzwerk >> DHCP >> DMZ DHCP		
Modus	**Aktiviere DHCP-Server auf dem DMZ-Port**	Aktiviert den DHCP-Server auf dem DMZ-Interface. Bei deaktivierter Funktion beantwortet der mGuard keine DHCP-Anfragen auf dem DMZ-Interface.
DHCP-Server-Optionen	**Dynamischen IP-Adresspool aktivieren**	Bei aktivierter Funktion 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).
	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.

Netzwerk >> DHCP >> DMZ DHCP[...]		
	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 95/98/ME**: • Starten Sie **winipcfg** in einer DOS-Box. **Windows NT/2000/XP/**: • Starten Sie **ipconfig /all** in einer Eingabeaufforderung. Die MAC-Adresse wird als „Physikalische Adresse“ angezeigt. **Linux**: • Rufen Sie in einer Shell **/sbin/ifconfig** oder **ip link show** auf. 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.	

6.8 Netzwerk >> Proxy-Einstellungen

6.8.1 HTTP(S) Proxy-Einstellungen



Für folgende vom mGuard selbst ausgeführte Aktivitäten kann hier ein Proxy-Server angegeben werden:

- CRL-Download
- Firmware-Update
- regelmäßiges Holen des Konfigurationsprofils von zentraler Stelle
- Wiederherstellung von Lizenzen

Netzwerk >> Proxy-Einstellungen >> HTTP(S) Proxy-Einstellungen		
HTTP(S) Proxy-Einstellungen	**Proxy für HTTP und HTTPS benutzen**	Bei 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 331). 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.
	Sekundäres externes Interface benutzt Proxy	Aktivieren Sie die Funktion nur, wenn die Verbindung (HTTP oder HTTPS) des sekundären externen Interfaces ebenfalls über einen Proxy-Server hergestellt werden soll (siehe „Sekundäres externes Interface“ auf Seite 157).
	HTTP(S)-Proxy-Server	Hostname oder IP-Adresse des Proxy-Servers
	Port	Nummer des zu verwendenden Ports, z. B. 3128

Netzwerk >> Proxy-Einstellungen >> HTTP(S) Proxy-Einstellungen		
Proxy-Authentifizierung	**Login**	Benutzerkennung (Login) zur Anmeldung beim Proxy-Server
	Passwort	Passwort zur Anmeldung beim Proxy-Server

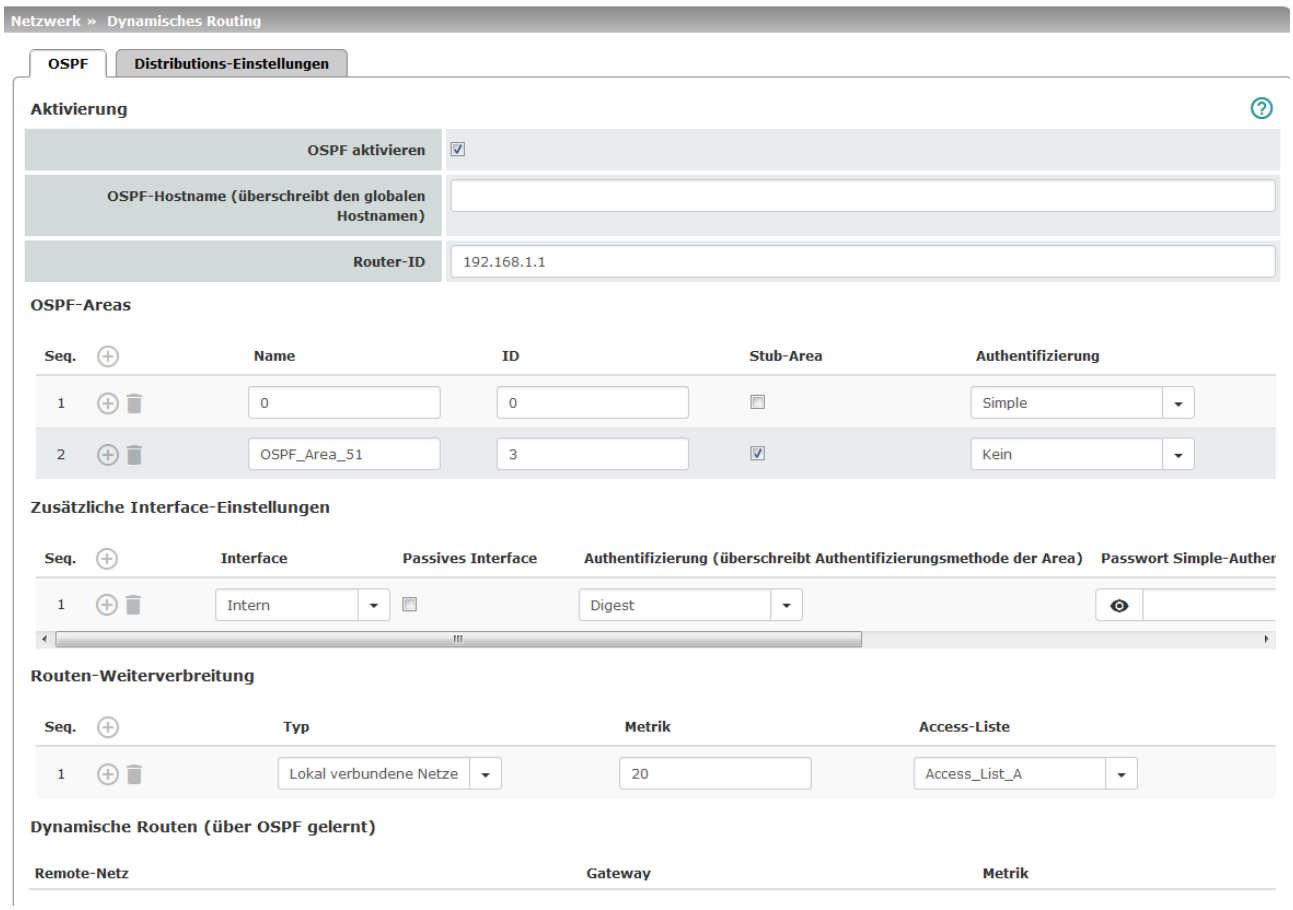
6.9 Netzwerk >> Dynamisches Routing

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. Im **Router-Modus „DHCP“** kann dem WAN-Interface keine OSPF-Area zugewiesen werden.

6.9.1 OSPF



OSPF lässt sich für interne, externe und DMZ-Interfaces konfigurieren. Soll OSPF in IPsec-Verbindungen verwendet werden, müssen die OSPF-Pakete (Multicast) in einem GRE-Tunnel (Unicast) gekapselt werden.

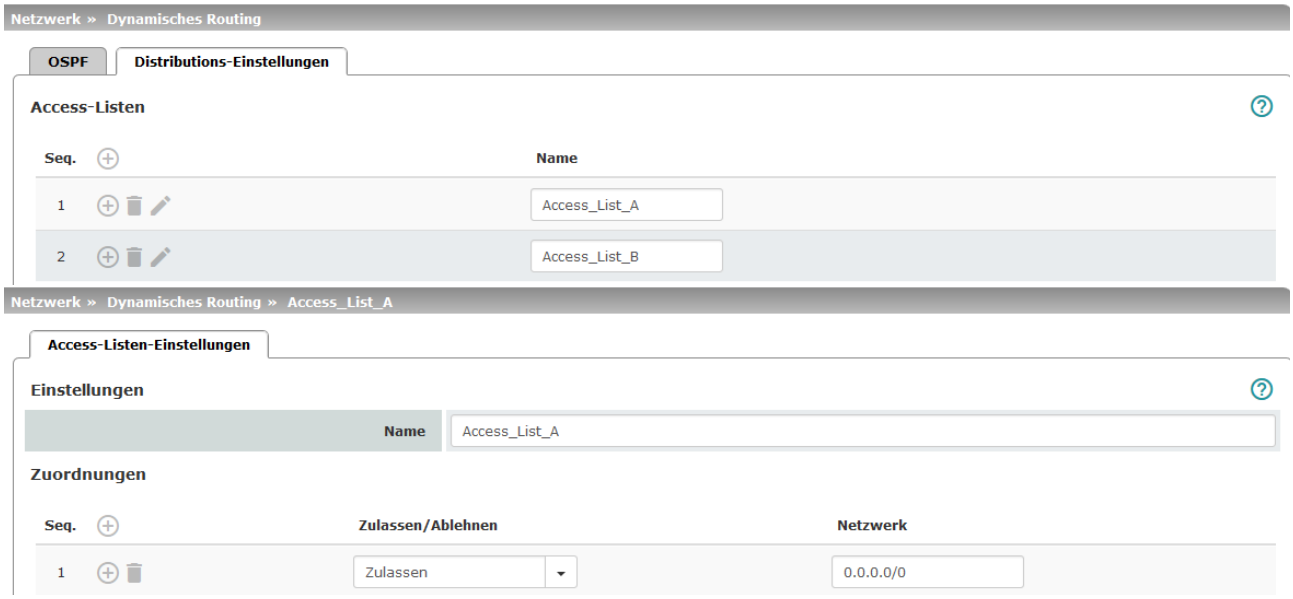
Es können mehrere OSPF-Areas konfiguriert werden, um lokale Routen weiterzuverbreiten und externe Routen zu lernen. Der Status aller gelernten Routen wird in einer Tabelle angezeigt.

Netzwerk >> Dynamisches Routing >> OSPF		
Aktivierung	**OSPF aktivieren**	Bei deaktivierter Funktion (Standard): OSPF ist auf dem Gerät deaktiviert. Bei aktivierter Funktion: Das dynamische Routing über das OSPF-Protokoll ist auf dem Gerät aktiviert. Neue Routen werden von benachbarten OSPF-Routern gelernt und weiterverbreitet. Im **Router-Modus „DHCP“** kann dem WAN-Interface keine OSPF-Area zugewiesen werden. Neue Einstellungsmöglichkeiten unter „Netzwerk >> Interfaces“ , „IPsec VPN >> Verbindungen“ und „Netzwerk >> GRE-Tunnel“ .
	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-, OpenVPN- und GRE-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.

6.9.2 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 Distribution Settings 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 135)
- statische Routen, die als Externe, Interne oder DMZ-Netzwerke eingetragen sind (siehe „Netzwerk >> Interfaces“ auf Seite 135)
- Routen, die über OpenVPN in die Kernel-Routing-Tabelle eingetragen werden (siehe „Menü OpenVPN-Client“ auf Seite 381)
- Routen die über die GRE-Tunnel-Konfiguration in die Kernel-Routing-Tabelle eingetragen werden (siehe „Netzwerk >> GRE-Tunnel“ auf Seite 238)

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** (Standard) 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.

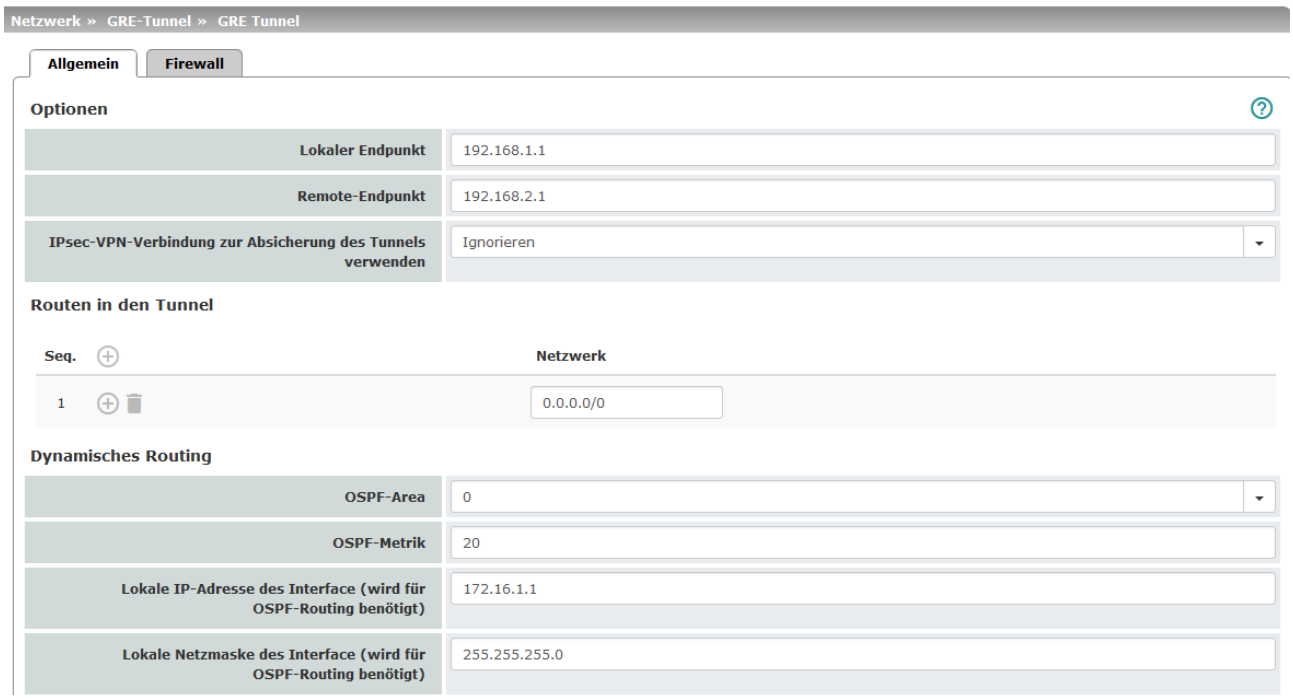
6.10 Netzwerk >> GRE-Tunnel

Generic Routing Encapsulation (GRE) ist ein Netzwerk-Protokoll, das verwendet wird, um andere Protokolle (u. a. das Routing-Protokoll OSPF) einzukapseln und in einem GRE-Tunnel über eine Unicast-IP-Verbindungen zu transportieren. OSPF-Routen können somit auch über IPsec-VPN-Verbindungen gelernt und weiterverbreitet werden.

Um sicherzustellen, dass GRE-Pakete durch eine sicheren IPsec-Tunnel geleitet werden, kann für jeden GRE-Tunnel eine bereits konfigurierte IPsec-Verbindung ausgewählt werden.

Die Verwendung von GRE-Tunneln über IPsec-Verbindungen des Verbindungstyps „**Transport**“ ist nicht möglich.

6.10.1 Allgemein



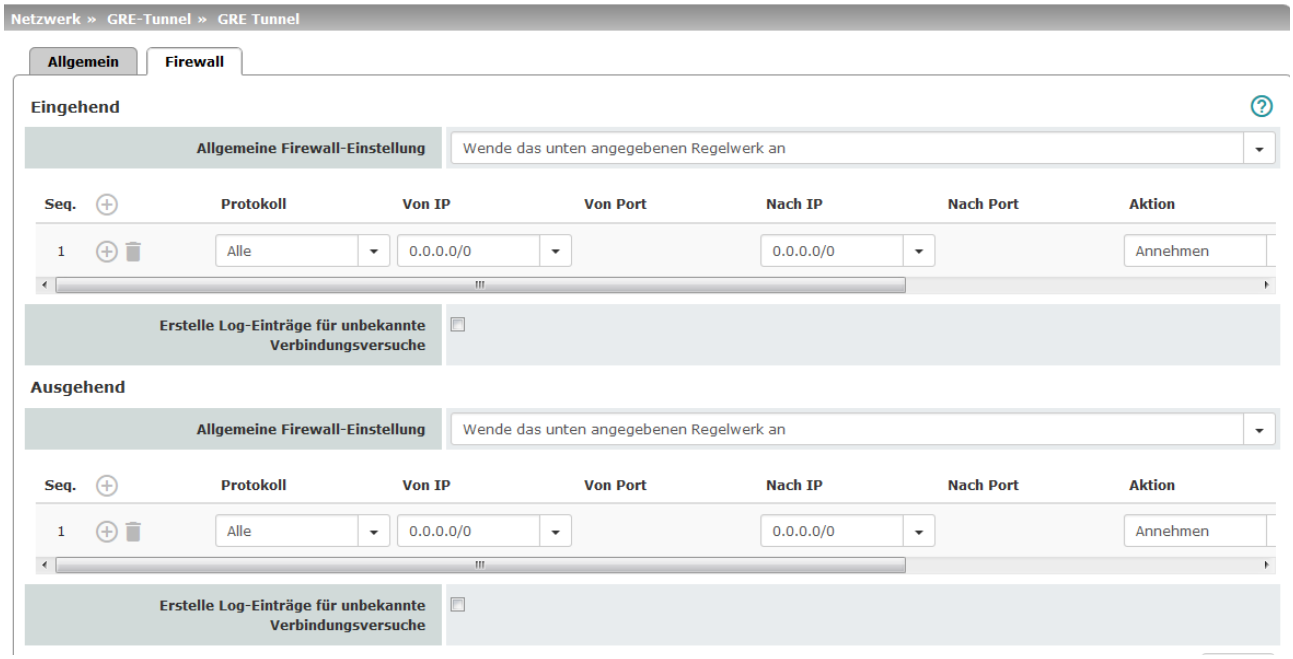
Netzwerk >> GRE-Tunnel >> Editieren >> Allgemein

Optionen

ACHTUNG: Um den GRE-Tunnel durch eine verschlüsselte IPsec-Verbindung zu leiten, müssen dessen lokaler und Remote-Endpunkt innerhalb der IPsec-Verbindung liegen.

Netzwerk >> GRE-Tunnel >> Editieren >> Allgemein		
	Lokaler Endpunkt	Lokale IP-Adresse, von der aus der GRE-Tunnel aufgebaut wird. Die IP-Adresse muss bereits unter *„Netzwerk >> Interfaces“* für den mGuard selbst konfiguriert sein.
	Remote-Endpunkt	Remote-IP-Adresse, zu der der GRE-Tunnel aufgebaut wird. Die IP-Adresse muss ebenfalls auf der Gegenstelle konfiguriert werden.
	IPsec-VPN-Verbindung zur Absicherung des Tunnels verwenden	Für die ausgewählte IPsec-Verbindung wird geprüft, ob der GRE-Tunnel durch diese geroutet und damit geschützt wird, d. h. ob beide Endpunkte innerhalb der IPsec-Netze (Lokal und Remote) liegen.
Routen in den Tunnel	**Netzwerk**	Alle Netzwerke der Gegenstelle, die gekapselt über den GRE-Tunnel erreicht werden sollen, werden an dieser Stelle eingetragen. Es können mehrere Routen für jeden GRE-Tunnel konfiguriert werden. **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 26).
Dynamisches Routing	**OSPF-Area**	Verknüpft das virtuelle GRE-Interface mit einer OSPF-Area (siehe „Netzwerk >> Dynamisches Routing“ auf Seite 233).
	OSPF-Metrik	Numerisches Maß für die Güte einer Verbindung durch den GRE-Tunnel.
	Lokale IP-Adresse des Interface	IP-Adresse des virtuellen GRE-Interface (wird für den Austausch von Routing-Informationen zwischen OSPF-Routern benötigt). Auf der Gegenstelle muss entsprechend eine IP-Adresse im gleichen Netz für das GRE-Interface konfiguriert werden.
	Lokale Netzmaske des Interface	Netzmaske des virtuellen GRE-Interface.

6.10.2 Firewall



Firewall eingehend, Firewall ausgehend

Während sich die im Menü Netzwerksicherheit vorgenommenen Einstellungen nur auf Nicht-VPN-Verbindungen bzw. Nicht-GRE-Verbindungen beziehen (siehe „Menü Netzwerksicherheit“ auf Seite 271), beziehen sich die Einstellungen an dieser Stelle ausschließlich auf die GRE-Verbindung, die auf diesem Registerkarten-Set definiert ist.

Wenn Sie mehrere GRE-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 GRE-Firewall ist werkseitig so voreingestellt, dass für die GRE-Verbindung alles zugelassen ist.

Für jede einzelne GRE-Verbindung gelten aber unabhängig voneinander gleichwohl die erweiterten Firewall-Einstellungen, die weiter oben definiert und erläutert sind (siehe „Menü Netzwerksicherheit“ auf Seite 271, „Netzwerksicherheit >> Paketfilter“ auf Seite 271, „Erweitert“ auf Seite 292).

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.

Netzwerk >> GRE-Tunnel >> 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.

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 26).

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 289).

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 mGuard-Geräten der RS2000-Serie ist die Verwendung von Hostnamen in IP-Gruppen nicht möglich.

Eingehend:

- Von IP: die IP-Adresse im GRE-Tunnel
- Nach IP die 1:1-NAT-Adresse bzw. die reale Adresse

Ausgehend:

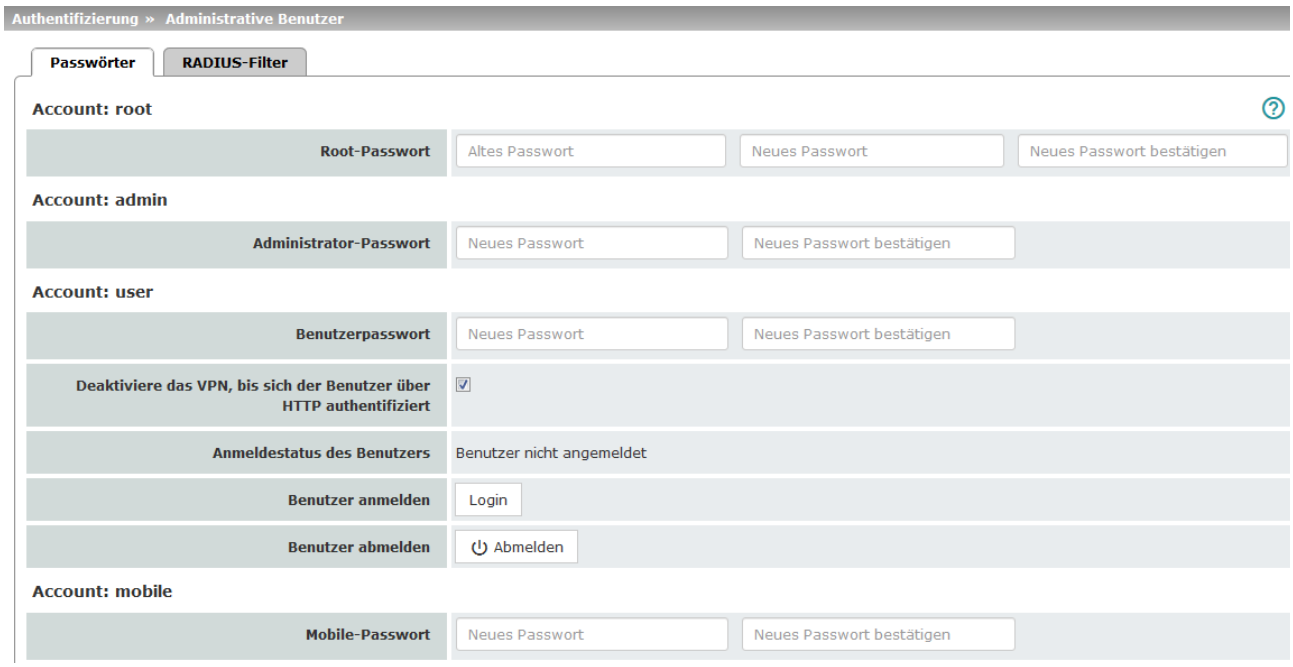
- Von IP: die 1:1-NAT-Adresse bzw. die reale Adresse
- Nach IP: die IP-Adresse im GRE-Tunnel

Netzwerk >> GRE-Tunnel >> Editieren >> Firewall		
	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 289).
	Aktion	**Annehmen** bedeutet, die Datenpakete dürfen passieren. **Abweisen** bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. **Verwerfen** bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information über deren Verbleib erhält. **Namen von Regelsätzen**, sofern definiert. Bei Angabe eines Namens für Regelsätze treten die Firewall-Regeln in Kraft, die unter diesem Namen konfiguriert sind (siehe „Regelsätze“ auf Seite 282). Regelsätze, die IP-Gruppen mit Hostnamen enthalten, sollten aus Sicherheitsgründen nicht in Firewall-Regeln verwendet werden, die als Aktion „Verwerfen“ oder „Abweisen“ ausführen. Auf mGuard-Geräten der RS2000-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 „Modbus TCP“ auf Seite 298).
	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 (Default-Einstellung).
	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“.	

7 Menü Authentifizierung

7.1 Authentifizierung >> Administrative Benutzer

7.1.1 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.

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

Account: root

Root-Passwort

Bietet vollständige Rechte für alle Parameter des mGuards.

Hintergrund: Nur diese Berechtigungsstufe erlaubt unbegrenzten Zugriff auf das Dateisystem des mGuards.

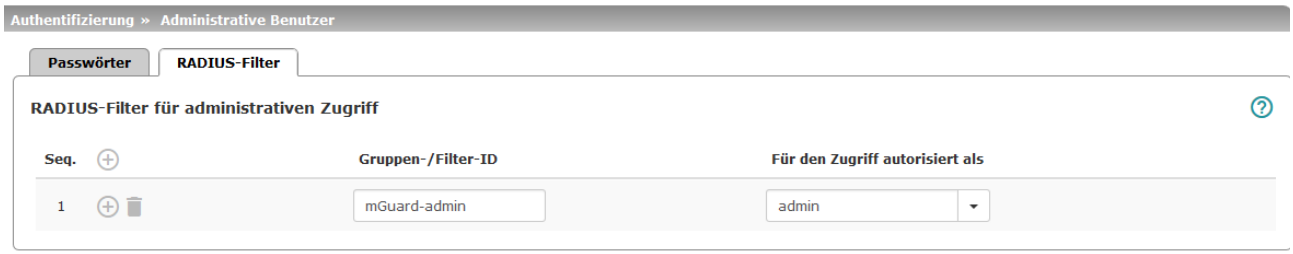
Benutzername (nicht änderbar): **root**

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.

Authentifizierung >> Administrative Benutzer >> Passwörter [...]		
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 HTTP authentifiziert	Ist ein Benutzerpasswort festgelegt und aktiviert, dann muss der Benutzer nach jedem Neustart des mGuards bei Zugriff auf eine beliebige HTTP URL dieses Passwort angeben, **damit die VPN-Verbindungen des mGuards aktiviert werden**. Werkseitig ist die Funktion deaktiviert. Bei aktivierter Funktion können VPN-Verbindungen erst dann genutzt werden, wenn sich ein Benutzer mittels HTTP gegenüber dem mGuard ausgewiesen hat. Alle HTTP Verbindung werden auf den mGuard umgeleitet, solange die Authentifizierung erforderlich ist. Die Änderung dieser Option wird erst mit dem nächsten Neustart aktiv. 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**.
Account: mobile (Nur TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G)	**Mobile-Passwort**	Werkseitig ist kein Mobile-Passwort voreingestellt. Um eines festzulegen, geben Sie in beide Eingabefelder übereinstimmend das gewünschte Passwort ein.

7.1.2 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 anschließenden neu starten, um bestehende Sitzungen mit nicht mehr gültigen Zertifikaten oder Passwörtern sicher zu beenden.

Authentifizierung >> Administrative Benutzer >> RADIUS-Filter

(Dieser Menüpunkt gehört nicht zum Funktionsumfang von TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005, FL MGUARD RS2000.)

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

- für den Shell-Zugang siehe Menü: *Verwaltung >> Systemeinstellungen >> Shell-Zugang*
- über den Web-Zugriff siehe Menü: *Verwaltung >> Web-Einstellungen >> Zugriff*

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

Nachdem ein RADIUS-Server das Passwort eines Benutzers positiv geprüft hat, sendet der RADIUS-Server dem mGuard in seiner Antwort eine Liste von Filter-IDs.

Diese Filter-IDs sind in einer Datenbank des Servers dem Benutzer zugeordnet. Über sie weist der mGuard die Gruppe zu und damit die Autorisierung als „admin“, „netadmin“ oder „audit“.

Eine erfolgreiche Authentifizierung wird im Logging des mGuards vermerkt. Weitere Aktionen des Benutzers werden dort mit seinem ursprünglichen Namen protokolliert. Die Log-Nachrichten werden an einen Remote-Server weitergeleitet, sofern ein Remote-Server vom mGuard freigegeben ist.

Aktionen, die festgehalten werden, sind:

- Login,
- Logout,
- Start eines Firmware-Updates,
- Ändern der Konfiguration und
- das Ändern des Passwortes eines der vordefinierten Benutzer *(root, admin, netadmin, audit, mobile and user)*.

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)

7.2 Authentifizierung >> Firewall-Benutzer

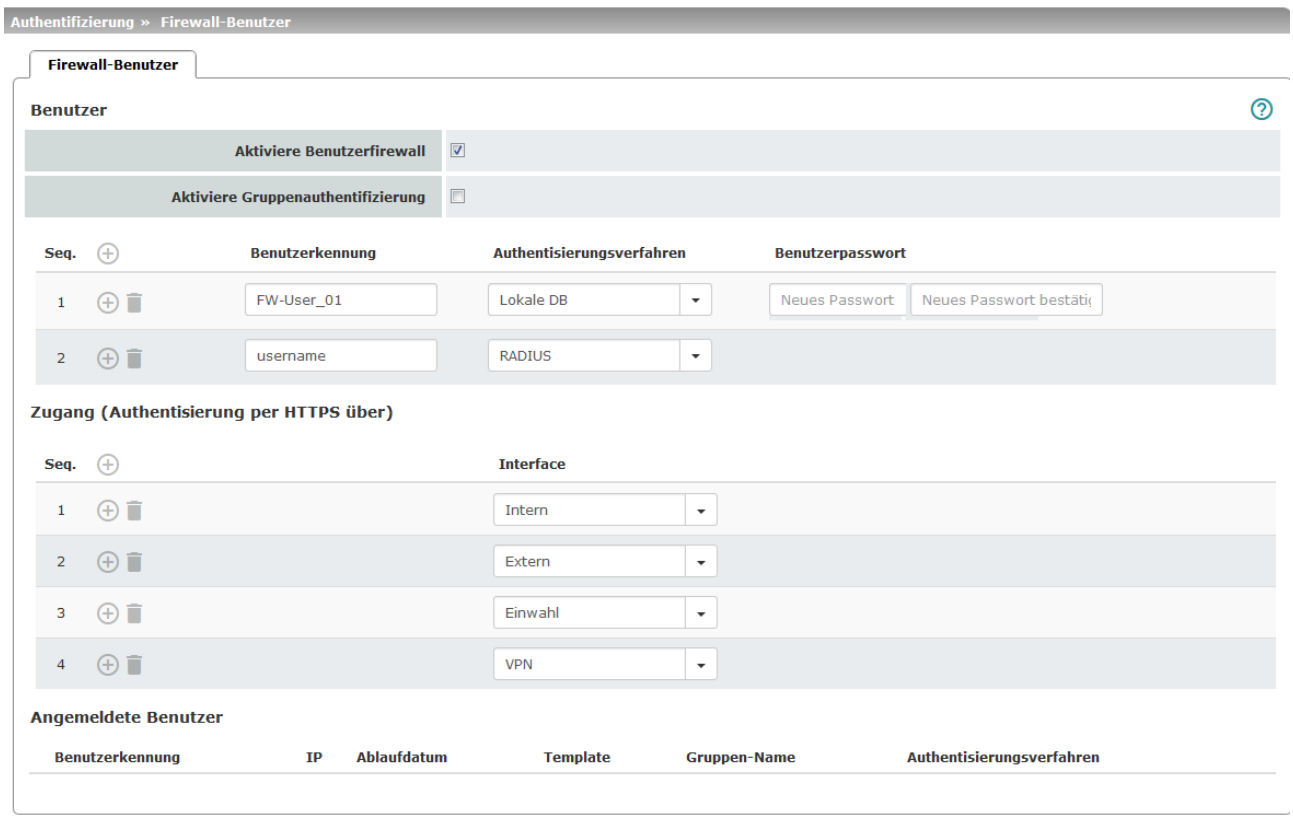
Um z. B. privates Surfen im Internet zu unterbinden, wird unter *Netzwerksicherheit >> Paketfilter >> DMZ* jede ausgehende Verbindung unterbunden (nicht betroffen: VPN).

Unter *Netzwerksicherheit >> Benutzerfirewall* können für bestimmte Firewall-Benutzer anders lautende Firewall-Regeln definiert werden, z. B. dass für diese jede ausgehende Verbindung erlaubt ist. Diese Benutzerfirewall-Regel greift, sobald sich der oder die betreffende(n) Firewall-Benutzer angemeldet haben, für die diese Benutzerfirewall-Regel gilt, siehe *„Netzwerksicherheit >> Benutzerfirewall“ auf Seite 306*.

7.2.1 Firewall-Benutzer

Dieses Menü steht **nicht** auf dem **FL MGUARD RS2000, TC MGUARD RS2000 3G, TC MGUARD RS2000 4G** und **FL MGUARD RS2005** 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 anschließenden 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.

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 308.

Interface

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

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 74).

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.

1 *DMZ* nur bei Geräten mit DMZ-Schnittstelle.

2 *Extern 2* und *Einwahl* nur bei Geräten mit serieller Schnittstelle (siehe „Netzwerk >> Interfaces" auf Seite 135).

7.3 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.

Damit die RADIUS-Authentifizierung aktiv wird, müssen Sie unter *Authentifizierung >> Firewall-Benutzer* bei dem Unterpunkt *Aktiviere Gruppenauthentifizierung* die Auswahl **Ja** einstellen und als *Authentifizierungsmethode* den Punkt *RADIUS auswählen.*

Unter Authentifizierung >> RADIUS-Server wird eine Liste von RADIUS-Servern erstellt, die durch den mGuard verwendet wird. Diese Liste wird auch verwendet, wenn beim administrativen Zugriff (SSH/HTTPS), die RADIUS-Authentifizierung aktiviert ist.

Wenn die RADIUS-Authentifizierung aktiv ist, wird der Log-in-Versuch von einem nicht vordefinierten Benutzer (nicht: *root, admin, netadmin, audit* oder *user)* an alle hier aufgelisteten RADIUS-Server weitergeleitet. Die erste Antwort, die der mGuard von einem der RADIUS-Server erhält, entscheidet über das Gelingen des Authentifizierungsversuches.

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

Authentifizierung >> RADIUS

RADIUS-Server

(Dieser Menüpunkt gehört nicht zum Funktionsumfang von TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005, FL MGUARD RS2000.)

RADIUS-Timeout

Legt fest (in Sekunden), wie lange der mGuard auf die Antwort des RADIUS-Servers wartet. Standard: 3 Sekunden.

RADIUS-Wiederholungen

Legt fest, wie oft bei Überschreitung des RADIUS-Timeouts Anfragen an den RADIUS-Server wiederholt werden. Standard: 3.

Authentifizierung >> RADIUS [...]		
	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, mit Ausnahme der Umlaute. Die NAS-ID ist ein RADIUS-Attribut, das der Client nutzen kann, um sich selbst beim RADIUS-Server zu identifizieren. Die NAS-ID kann anstelle einer IP-Adresse genutzt werden, um den Clienten zu identifzieren. Sie muss einzigartig im Bereich des RADIUS-Servers sein.
	Server	Name des RADIUS-Servers oder dessen IP-Adresse Wir empfehlen, wenn möglich IP-Adressen statt Namen als Server anzugeben. Sonst muss der mGuard zuerst die Namen auflösen, bevor er Authentifizierungsanfragen an den RADIUS-Server senden kann. Dies kostet beim Einloggen Zeit. Außerdem kann unter Umständen keine Authentifizierung stattfinden, wenn eine Namensauflösung fehl schlägt, weil z. B. der DNS nicht erreichbar ist oder der Name im DNS gelöscht wurde.

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.

7.4 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 473).

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*.

Selbst signierte Zertifikate

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

Selbst signierte Zertifikate werden benutzt, wenn die Kommunikationspartner den Vorgang der X.509-Authentifizierung verwenden wollen oder müssen, ohne ein offizielles Zertifikat zu haben oder zu benutzen. Diese Art der Authentifizierung sollte aber nur unter Kommunikationspartnern Verwendung finden, die sich „gut kennen“ und deswegen vertrauen. Sonst sind solche Zertifikate unter dem Sicherheitsaspekt genauso wertlos wie z. B. selbst erstellte Ausweispapiere, die keinen Behördenstempel tragen.

Zertifikate werden von kommunizierenden Maschinen / Menschen bei der Verbindungsaufnahme einander „vorgezeigt“, sofern zur Verbindungsaufnahme die X.509-Authentifizierung verwendet wird. Beim mGuard können das die folgenden Anwendungen sein:

- Authentifizierung der Kommunikationspartner bei der Herstellung von VPN-Verbindungen mittels IPsec (siehe „IPsec VPN >> Verbindungen“ auf Seite 336, „Authentifizierung“ auf Seite 359).
- Authentifizierung der Kommunikationspartner bei der Herstellung von VPN-Verbindungen mittels OpenVPN (siehe „OpenVPN-Client >> Verbindungen“ auf Seite 381, „Authentifizierung“ auf Seite 388).
- Verwaltung des mGuards per SSH (Shell Zugang) (siehe „Verwaltung >> Systemeinstellung >> Host“ auf Seite 45, „Shell-Zugang“ auf Seite 54).
- Verwaltung des mGuards per HTTPS (siehe „Verwaltung >> Web-Einstellungen“ auf Seite 73, „Zugriff“ auf Seite 74).

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 256).

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 261).

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 468).

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 selbst signiertes Zertifikat entstehen soll. (Hinweise zum Selbstausstellen gibt ein Dokument, welches von der Webseite phoenixcontact.net/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 263) 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 anschließenden 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) **selbst signiert**
Der mGuard authentifiziert die Gegenstelle anhand von...		
	... allen CA-Zertifikaten, die mit dem von der Gegenstelle vorgezeigten Zertifikat die Kette bis zum Root-CA-Zertifikat bilden ggf. PLUS Gegenstellen-Zertifikaten, **wenn** sie als Filter verwendet werden.[1]	Gegenstellen-Zertifikat

1 (Siehe „Verwaltung >> Systemeinstellungen“ auf Seite 45, „Shell-Zugang“ auf Seite 54)

Authentifizierung bei HTTPS

Die Gegenstelle zeigt vor:	Zertifikat (personenbezogen) von **CA signiert**[1]	Zertifikat (personenbezogen) **selbst signiert**
Der mGuard authentifiziert die Gegenstelle anhand von...		
	...allen CA-Zertifikaten, die mit dem von der Gegenstelle vorgezeigtem Zertifikat die Kette bis zum Root-CA-Zertifikat bilden ggf. PLUS Gegenstellen-Zertifikaten, **wenn** sie als Filter verwendet werden.[2]	Gegenstellen-Zertifikat

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

2 (Siehe „Verwaltung >> Web-Einstellungen“ auf Seite 73, „Zugriff“ auf Seite 74)

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.

7.4.1 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:

– selbst signierte 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) bekannt ist, entweder

– durch die eingebaute Uhr (bei *TC MGUARD RS4000/RS2000 3G*, TC MGUARD RS4000/RS2000 4G, *FL MGUARD RS2005, FL MGUARD RS4000/RS2000,* FL MGUARD GT/GT, *mGuard centerport (Innominate), FL MGUARD CENTERPORT, FL MGUARD RS*, *mGuard delta (Innominate)*, *FL MGUARD SMART2*) oder
– durch Synchronisierung der Systemzeit (siehe „Zeit und Datum“ auf Seite 47).

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 267) 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.

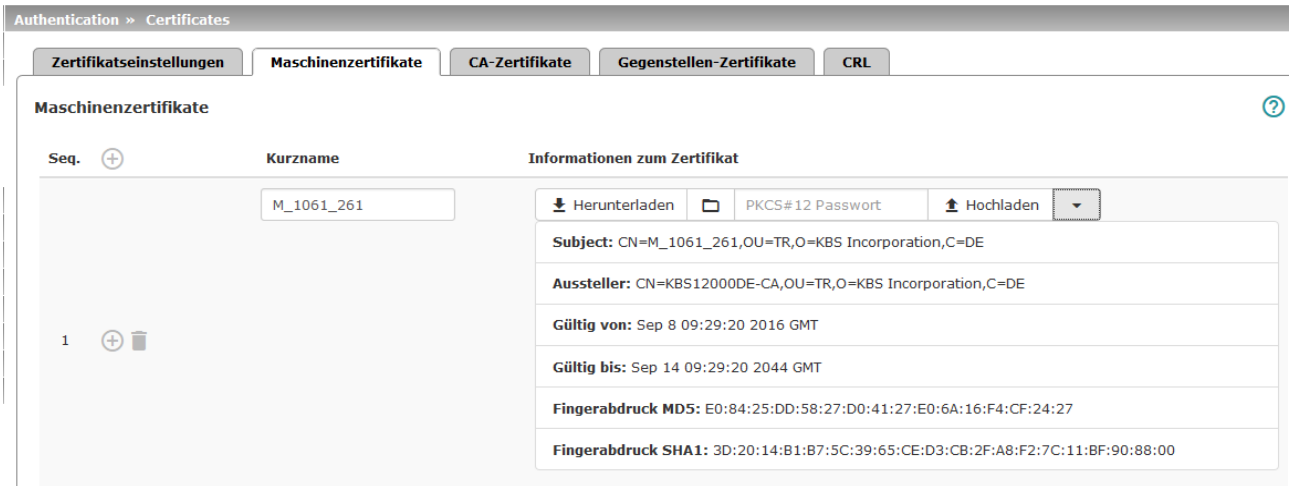
CRL-Download-Intervall

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 267) 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.

7.4.2 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 254.

Durch das Importieren einer PKCS#12-Datei erhält der mGuard einen privaten Schlüssel und das dazu gehörige Maschinenzertifikat. Es können mehrere PKCS#12-Dateien in den mGuard geladen werden, so dass der mGuard bei unterschiedlichen Verbindungen jeweils das gewünschte selbst signierte oder von einer CA signierte Maschinenzertifikat verwenden kann, um es der Gegenstelle vorzuzeigen.

Zur Verwendung eines an dieser Stelle installierten Maschinenzertifikats muss bei der Konfiguration von Anwendungen (SSH, VPN) **zusätzlich** auf dieses Maschinenzertifikat referenziert werden, um es für die jeweilige Verbindung bzw. die jeweilige Fernzugriffsart zu benutzen.

Beispiel für importierte Maschinenzertifikate (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.

7.4.3 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 254.

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

Authentifizierung >> Zertifikate >> CA-Zertifikate

Vertauenswürdige CA-Zertifikate	**Zeigt die aktuell importierten CA-Zertifikate an.**

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

CA-Zertifikat importieren

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.

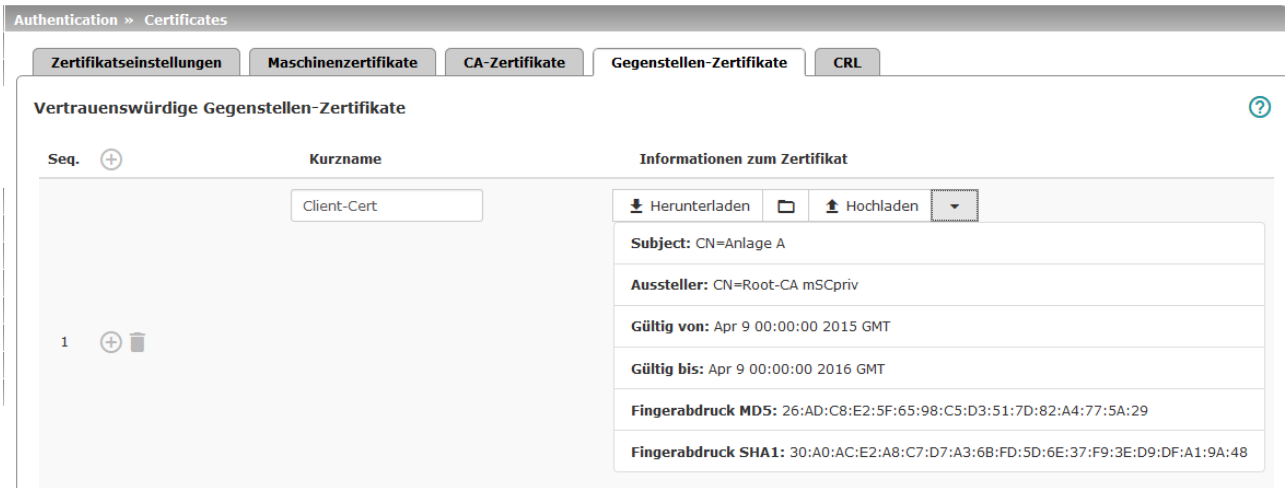
Zertifikats-Kopie erstellen und herunterladen

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.

7.4.4 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 254.

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.

7.4.5 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 259).

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 259) 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.

8 Menü Netzwerksicherheit

Dieses Menü steht **nicht** auf dem **FL MGUARD BLADE-Controller** zur Verfügung. Auf dem **FL MGUARD RS2000, TC MGUARD RS2000 3G**, **TC MGUARD RS2000 4G** und **FL MGUARD RS2005** steht das Menü in reduzierter Form zur Verfügung.

8.1 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

- 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 336, „Firewall“ auf Seite 367).
- **Benutzer-Firewall**. Wenn sich Benutzer anmelden, für die Benutzer-Firewall-Regeln definiert sind, werden vorrangig diese Regeln angewandt (siehe „Netzwerksicherheit >> Benutzerfirewall“ auf Seite 306), 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 RS2000-Serie

FL MGUARD RS2000, TC MGUARD RS2000 3G, TC MGUARD RS2000 4G und FL MGUARD RS2005 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 289).

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.

8.1.1 Eingangsregeln

Netzwerksicherheit >> Paketfilter >> Eingangsregeln

Eingehend

Listet die eingerichteten Firewall-Regeln auf. Sie gelten für eingehende Datenverbindungen, die von extern initiiert wurden.

Für die mGuard-Geräte der RS2000-Serie gelten gesonderte Firewall-Einstellungen (siehe „Firewall-Einstellungen bei Geräten der RS2000-Serie“ auf Seite 271).

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 304).

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 / Extern 2 / Alle Gibt an, über welches Interface die Datenpakete eingehen, damit sich die Regel auf sie bezieht. Mit **Alle** sind die Interfaces **Extern** und **Extern 2** gemeint. Diese Interfaces stehen nur bei mGuard-Modellen mit von außen zugänglicher serieller Schnittstelle 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 26). **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 mGuard-Geräten der RS2000-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 „Regelsätze“ auf Seite 282). Regelsätze, die IP-Gruppen mit Hostnamen enthalten, sollten aus Sicherheitsgründen nicht in Firewall-Regeln verwendet werden, die als Aktion „Verwerfen“ oder „Abweisen“ ausführen. Auf mGuard-Geräten der RS2000-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 „Modbus TCP“ auf Seite 298).
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 (werkseitige Voreinstellung).
Log-Einträge für unbekannte Verbindungsversuche	Bei aktivierter Funktion werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden. (Werkseitige Voreinstellung: **deaktiviert**)

8.1.2 Ausgangsregeln

Netzwerksicherheit >> Paketfilter >> Ausgangsregeln

Ausgehend

Listet die eingerichteten Firewall-Regeln auf. Sie gelten für ausgehende Datenverbindungen, die von intern initiiert wurden, um mit einer entfernten Gegenstelle zu kommunizieren.

Für die mGuard-Geräte der RS2000-Serie gelten gesonderte Firewall-Einstellungen (siehe „Firewall-Einstellungen bei Geräten der RS2000-Serie“ auf Seite 271).

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 26).

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 mGuard-Geräten der RS2000-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.

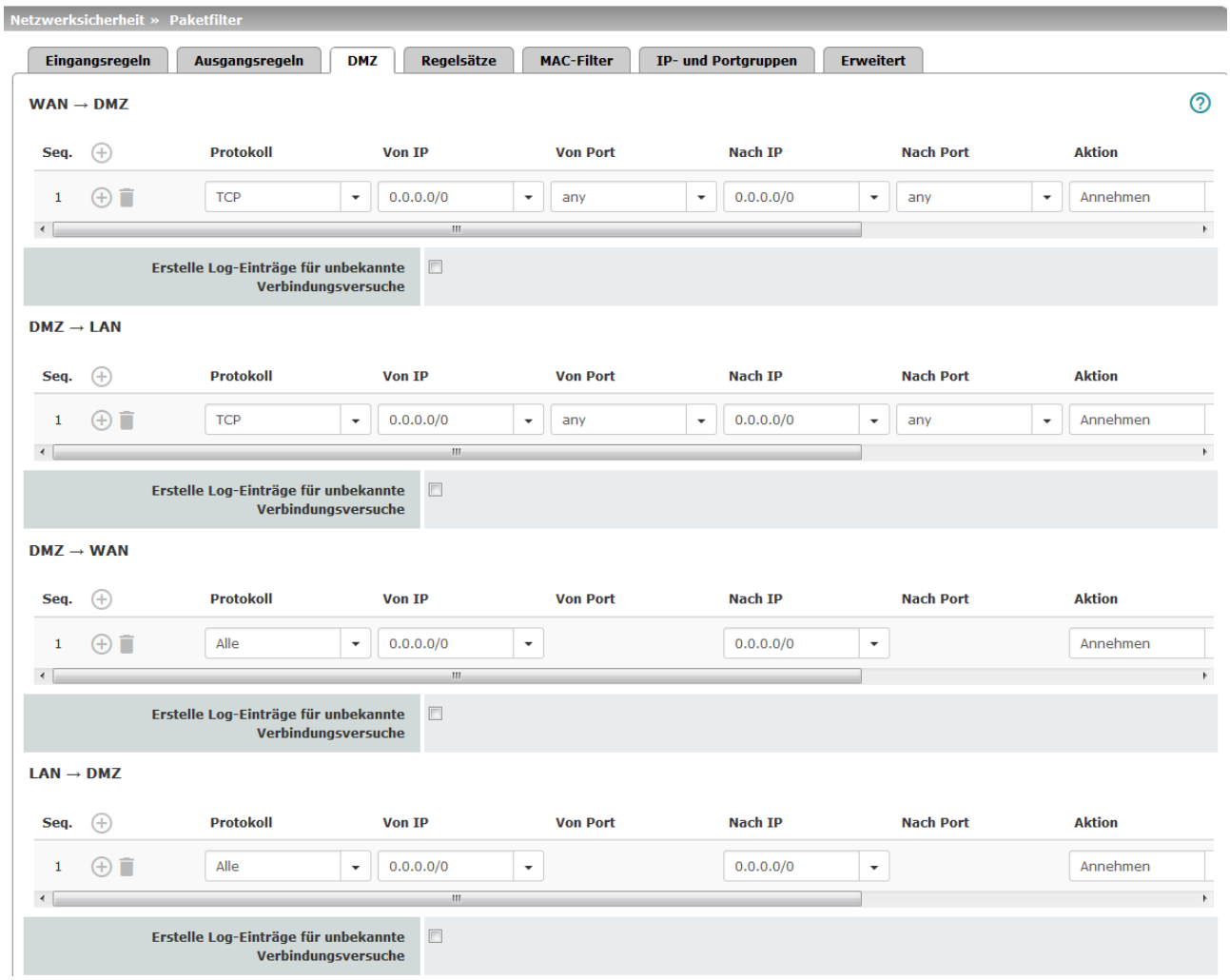
Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben (z. B. 110 für pop3 oder pop3 für 110).

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 „Regelsätze“ auf Seite 282). Regelsätze, die IP-Gruppen mit Hostnamen enthalten, sollten aus Sicherheitsgründen nicht in Firewall-Regeln verwendet werden, die als Aktion „Verwerfen“ oder „Abweisen“ ausführen. Auf mGuard-Geräten der RS2000-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 „Modbus TCP“ auf Seite 298).
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 (werkseitige Voreinstellung).
Log-Einträge für unbekannte Verbindungsversuche	Bei aktivierter Funktion werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden. (Werkseitige Voreinstellung: **deaktiviert**)

8.1.3 DMZ



Netzwerksicherheit >> Paketfilter >> DMZ

Firewall-Regeln für die DMZ

(Nur bei TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4004, FL MGUARD CENTERPORT)

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 26).

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.

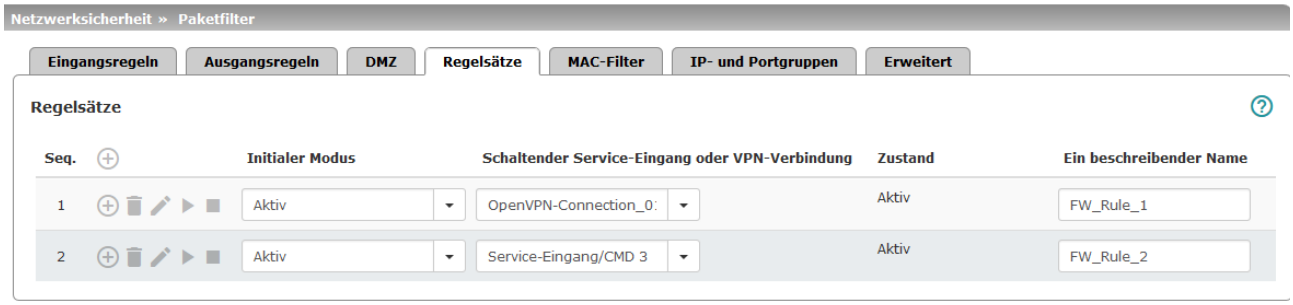
Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben (z. B. 110 für pop3 oder pop3 für 110).

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 „Regelsätze“ auf Seite 282). 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 „Modbus TCP“ auf Seite 298).
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 (werkseitige Voreinstellung).
Log-Einträge für unbekannte Verbindungsversuche	Bei aktivierter Funktion werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden. (Werkseitige Voreinstellung: **deaktiviert**)

8.1.4 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 122).

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.

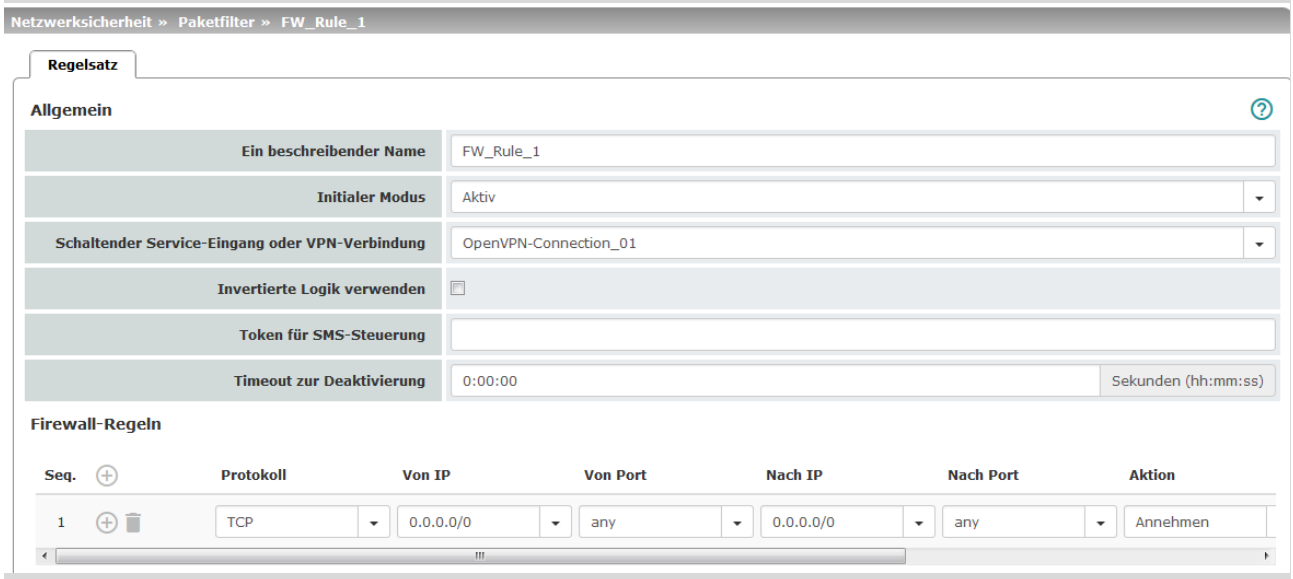
Es gibt zwei Wege, den mGuard so einzurichten, dass er mit dem Ausschalten eines Firewall-Regelsatzes auch die zugehörigen Verbindungen unterbricht.

– 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 von TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005, FL MGUARD RS2000.)	**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, 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) 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, 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) 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.
	Token für SMS-Steuerung	Nur verfügbar beim TC MGUARD RS4000 3G, TC MGUARD RS4000 4G. Eingehende SMS können dazu benutzt werden, Firewall-Regelsätze zu aktivieren oder zu inaktivieren. Die SMS muss das Kommando „fwrules/active“ bzw. „fwrules/inactive“ gefolgt von dem Token enthalten.
	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 26).

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.

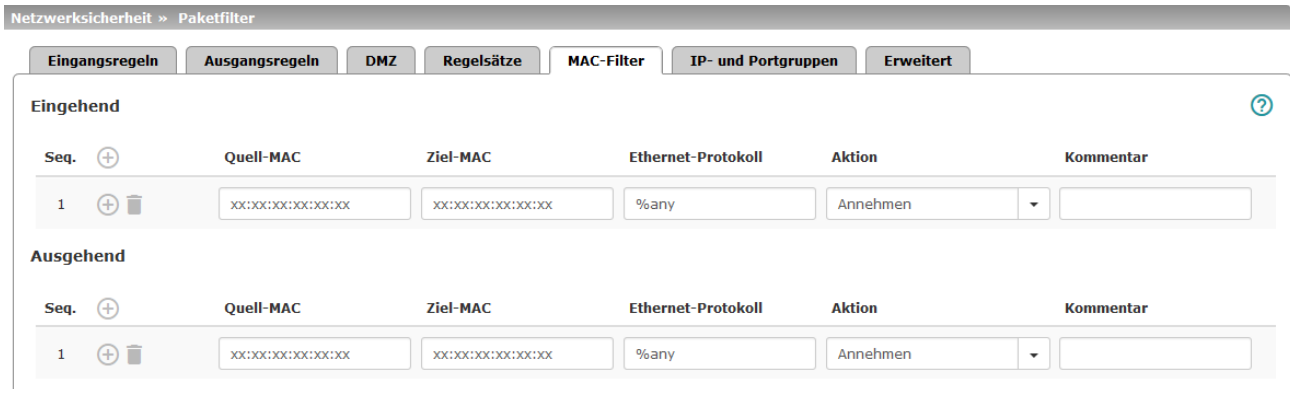
Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben (z. B. 110 für pop3 oder pop3 für 110).

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 „Regelsätze“ auf Seite 282). 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 „Modbus TCP“ auf Seite 298).
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).

8.1.5 MAC-Filter



Der MAC-Filter „Eingehend“ wird auf Frames angewendet, die der mGuard an der WAN-Schnittstelle empfängt. Der MAC-Filter „Ausgehend“ wird auf Frames angewendet, die der mGuard an der LAN-Schnittstelle empfängt. Datenpakete, die bei Modellen mit serieller Schnittstelle[1] per Modemverbindung ein- bzw. ausgehen, werden vom MAC-Filter nicht erfasst, weil hier kein Ethernet-Protokoll angewendet wird.

Im *Stealth*-Modus können neben dem Paketfilter (Layer 3/4), der den Datenverkehr z. B. nach ICMP-Nachrichten oder TCP/UDP-Verbindungen filtert, zusätzlich MAC-Filter (Layer 2) gesetzt werden. Ein MAC-Filter (Layer 2) filtert nach MAC-Adressen und Ethernet-Protokollen.

Im Gegensatz zum Paketfilter ist der MAC-Filter stateless. 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

(Dieser Menüpunkt gehört nicht zum Funktionsumfang von
TC MGUARD RS2000 3G,
TC MGUARD RS2000 4G,
FL MGUARD RS2005,
FL MGUARD RS2000.)

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.

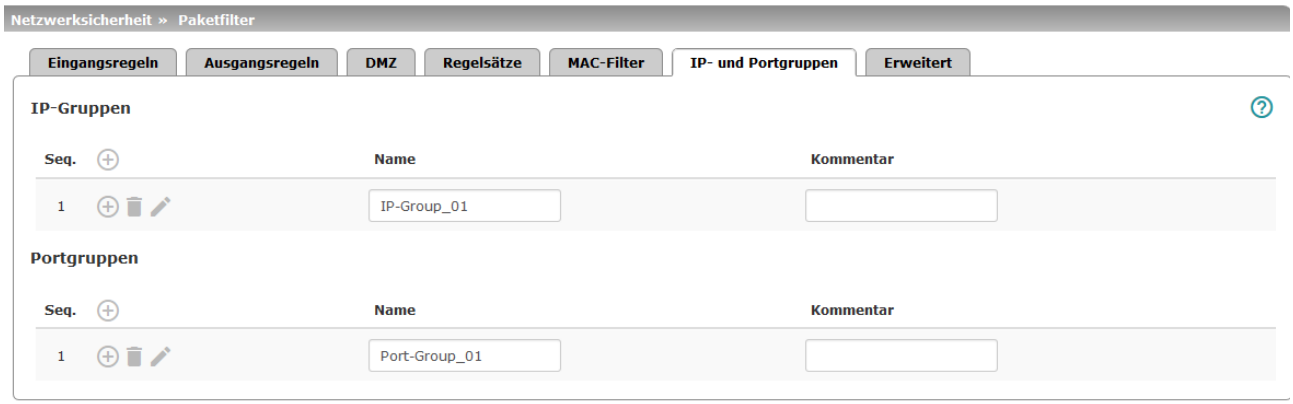
Weitere Protokolle können mit dem Namen oder in HEX angegeben werden, zum Beispiel:

– IPv4 oder 0800
– ARP oder 0806

[1] *TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS4004/RS2005, FL MGUARD RS4000/RS2000, mGuard centerport (Innominate), FL MGUARD CENTERPORT, FL MGUARD RS, FL MGUARD BLADE, mGuard delta (Innominate)*

Netzwerksicherheit >> Paketfilter >> MAC-Filter [...]		
	Aktion	**Annehmen** bedeutet, die Datenpakete dürfen passieren. **Verwerfen** bedeutet, die Datenpakete werden verworfen.
	Kommentar	Ein frei wählbarer Kommentar für diese Regel.
Ausgehend	Die Erklärung unter „Eingehend“ gilt auch für „Ausgehend“.	

8.1.6 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: 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 216).

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**.

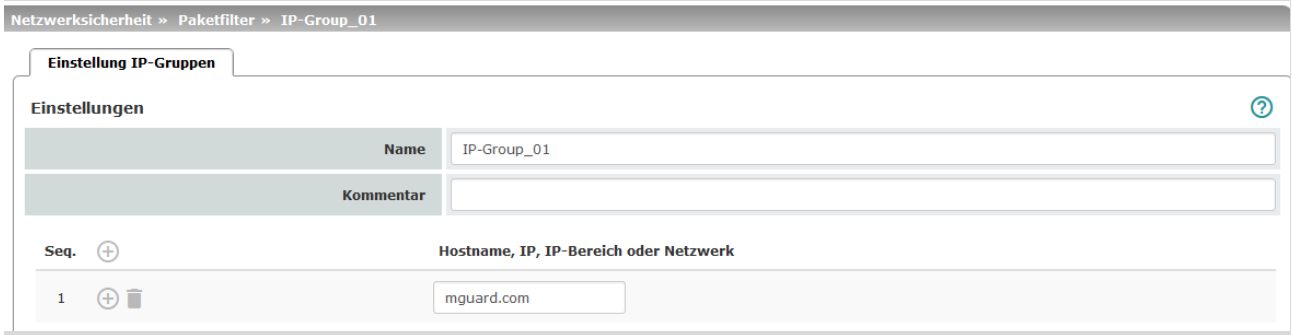
mGuard-Geräte der RS2000-Serie

Die Verwendung von Hostnamen in IP-Gruppen wird von mGuard-Geräten der RS2000-Serie nicht unterstützt.

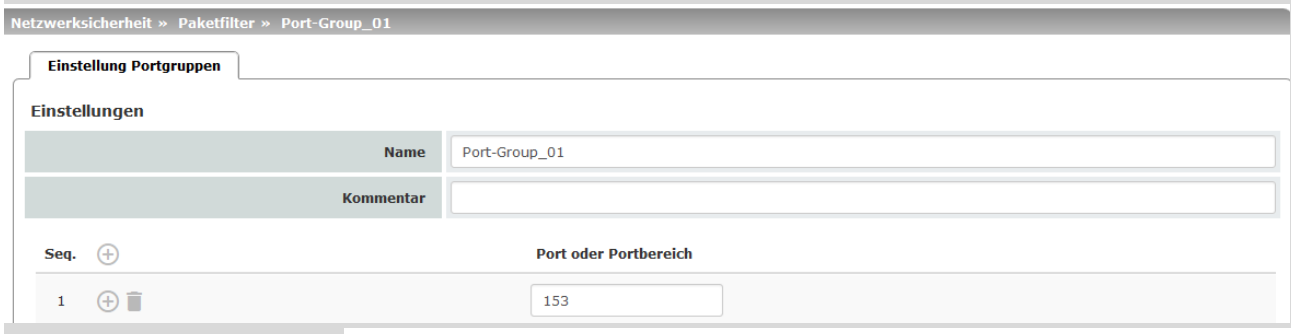
Netzwerksicherheit >> Paketfilter >> IP- und Portgruppen		
IP-Gruppen	**Name**	Sie können die IP-Gruppe frei benennen bzw. umbenennen.

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

	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:

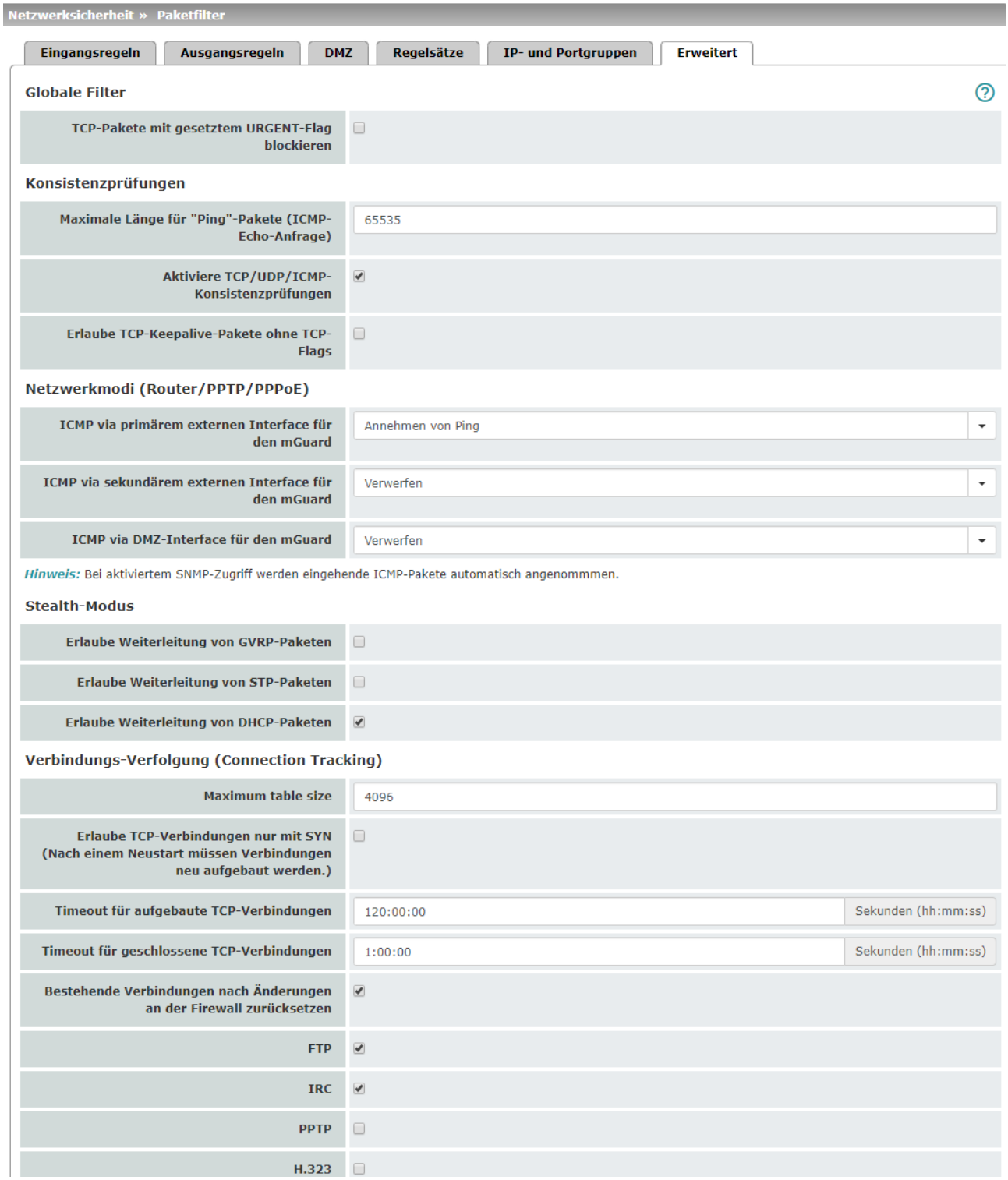


Einstellung Portgruppen	**Name**	Sie können die Portgruppe frei benennen bzw. umbenennen.

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

8.1.7 Erweitert

Die Einstellungen betreffen das grundlegende Verhalten der Firewall.



Netzwerksicherheit >> Paketfilter >> Erweitert		
Globale Filter (Dieser Menüpunkt gehört nicht zum Funktionsumfang von TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005, FL MGUARD RS2000.)	**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 von TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005, FL MGUARD RS2000.)	**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 295). 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 sekundärem 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 / sekundäre externe Interface an den mGuard gesendet werden. Unabhängig von der hier festgelegten Einstellung werden bei aktiviertem SNMP-Zugriff eingehende ICMP-Pakete immer angenommen. **Verwerfen**: Alle ICMP-Nachrichten 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**.

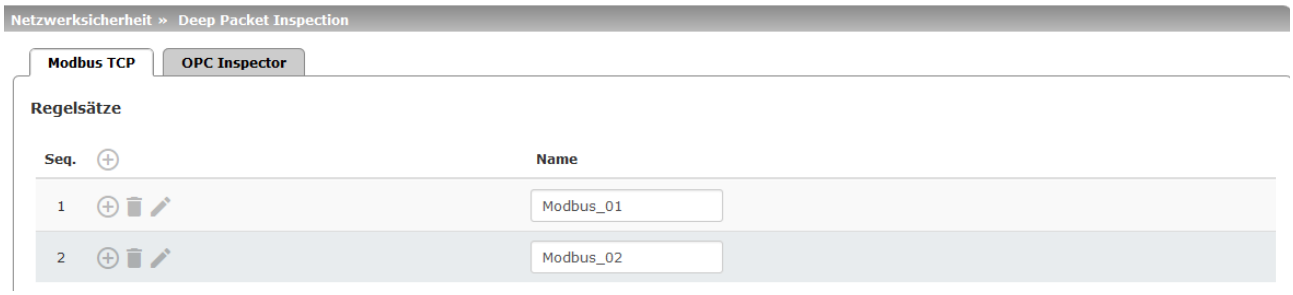
Netzwerksicherheit >> Paketfilter >> Erweitert [...]		
Verbindungs-Verfolgung (Connection Tracking)	**Maximale Zahl gleichzeitiger Verbindungen**	Dieser Eintrag legt eine Obergrenze fest. Diese ist so gewählt, dass sie bei normalem praktischen Einsatz nie erreicht wird. Bei Angriffen kann sie dagegen 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** (**Standard**): Der mGuard erlaubt auch Verbindungen, deren Anfang er nicht registriert hat. D. h. der mGuard kann bei Bestehen einer Verbindung einen Neustart durchführen, ohne dass die Verbindung abreißt. **Funktion aktiviert**: 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. Voreinstellung: 120 Tage (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. Voreinstellung: 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 (Standard)** 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: Beim „aktiven FTP“ stellt der angerufene Server im Gegenzug eine zusätzliche Verbindung zum Anrufer her, um auf dieser Verbindung die Daten zu übertragen. Beim „passiven FTP“ baut der Client diese zusätzliche Verbindung zum Server zur Datenübertragung auf. Damit die zusätzlichen Verbindungen von der Firewall durchgelassen werden, muss FTP **aktiviert** sein (Standard).
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 (Standard).
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.

8.2 Netzwerksicherheit >> Deep Packet Inspection

8.2.1 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.**

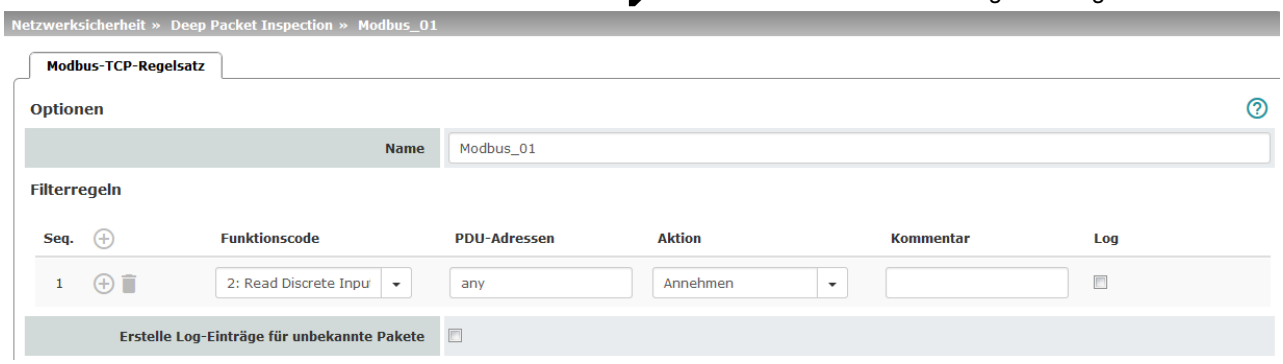
Deep Packet Inspection (DPI)

Der mGuard kann Pakete ein- und ausgehende 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

Modbus-TCP-Regelsätze können nur verwendet werden, wenn ein passender Lizenzschlüssel installiert ist (*Modbus TCP Inspector*).

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 / GRE / IPsec-VPN / OpenVPN / PPP.

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.

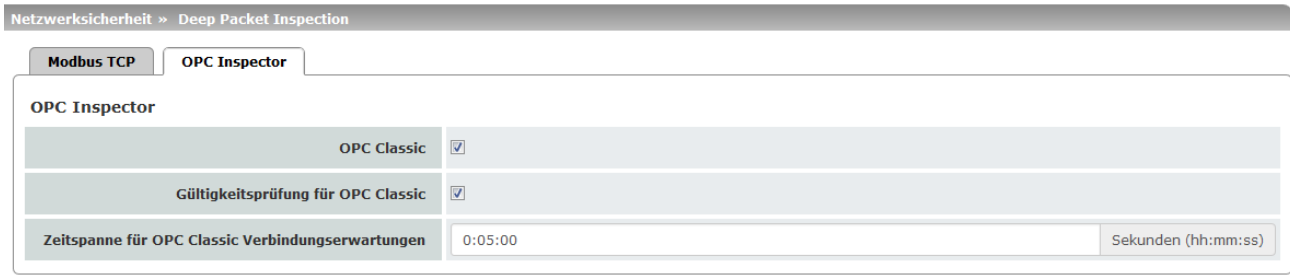
Sie können den Funktionscode aus der Drop-Down-Liste auswählen oder direkt in das Eingabefeld eingeben.

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

PDU-Adressen (Wird nur bei bestimmten Funktionscodes angezeigt)	**0 – 65535	any** 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.

Netzwerksicherheit >> Deep Packet Inspection >> Modbus TCP >> Regelsätze >> Edit		
	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 (werkseitige Voreinstellung).
	Erstelle Log-Einträge für unbekannte Pakete	Bei aktivierter Funktion werden auch die Pakete, die durch keine der erstellten Filterregeln erfasst werden, geloggt.

8.2.2 OPC Inspector



Netzwerksicherheit >> Deep Packet Inspection >> OPC Inspector		
OPC Inspector	**OPC Classic**	Sie können diese Funktion nur aktivieren, wenn ein passender Lizenzschlüssel installiert ist (OPC Inspector). Bei 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 **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.

8.3 Netzwerksicherheit >> DoS-Schutz

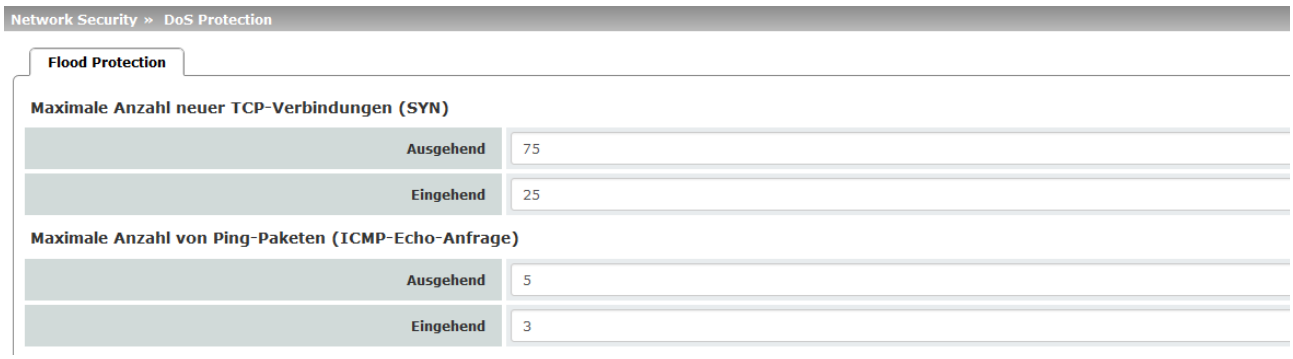
8.3.1 Flood Protection

Dieses Menü steht **nicht** auf dem **FL MGUARD RS2000, TC MGUARD RS2000 3G, TC MGUARD RS2000 4G** und **FL MGUARD RS2005** 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 273).

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: Werkseinstellung: 75 Eingehend: Werkseinstellung: 25 Maximalwerte für die zugelassenen ein- und ausgehenden TCP-Verbindungen pro Sekunde. Sie sind so gewählt, dass sie bei normalem praktischen Einsatz nie erreicht werden. Bei Angriffen können sie dagegen leicht erreicht werden, so dass durch die Begrenzung ein zusätzlicher Schutz eingebaut ist. Sollten in Ihrer Betriebsumgebung besondere Anforderungen vorliegen, dann können Sie die Werte erhöhen.

Netzwerksicherheit >> DoS-Schutz >> Flood Protection [...]		
Maximale Anzahl von Ping-Paketen (ICMP-Echo-Anfrage)	**Ausgehend / Eingehend**	Ausgehend: Werkseinstellung: 5 Eingehend: Werkseinstellung: 3 Maximalwerte für die zugelassenen ein- und ausgehenden „Ping“-Pakete pro Sekunde. Sie sind so gewählt, dass sie bei normalem praktischen Einsatz nie erreicht werden. Bei Angriffen können sie dagegen leicht erreicht werden, so dass durch die Begrenzung ein zusätzlicher Schutz eingebaut ist. Sollten in Ihrer Betriebsumgebung besondere Anforderungen vorliegen, dann können Sie die Werte erhöhen. Der Wert **0** bewirkt, dass kein „Ping“ Paket durchgelassen bzw. eingelassen wird.
Jeweils maximale Anzahl von ARP-Anfragen und ARP-Antworten (Nur im Netzwerkmodus „Stealth“)	**Ausgehend / Eingehend**	Werkseinstellung: 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.

8.4 Netzwerksicherheit >> Benutzerfirewall

Dieses Menü steht **nicht** auf dem **FL MGUARD RS2000, TC MGUARD RS2000 3G**, **TC MGUARD RS2000 4G** und **FL MGUARD RS2005** 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 247).

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.

8.4.1 Benutzerfirewall-Templates

Hier werden alle definierten Benutzerfirewall-Templates aufgelistet. Ein Template kann aus mehreren Firewall-Regeln bestehen. Ein Template kann mehreren Nutzern zugeordnet sein.

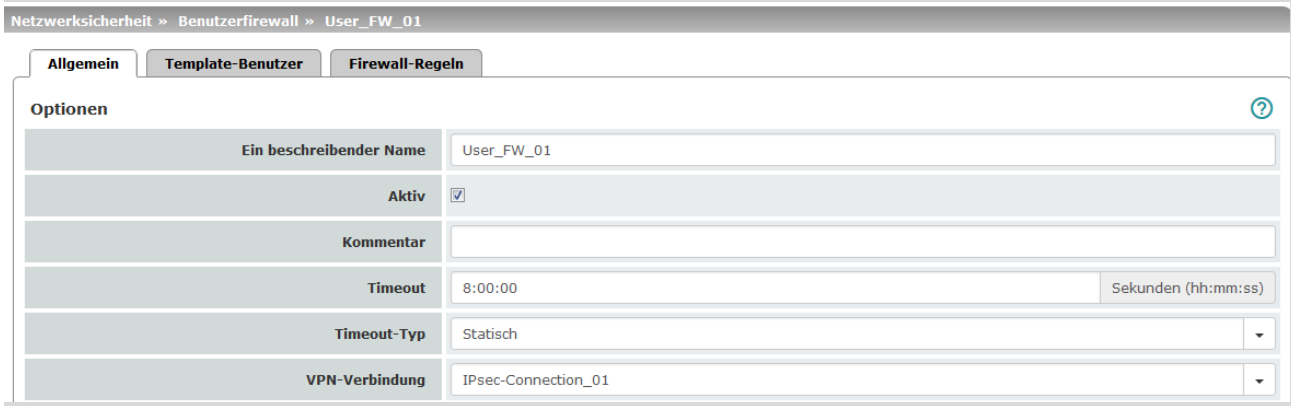
Template neu definieren:

- 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.

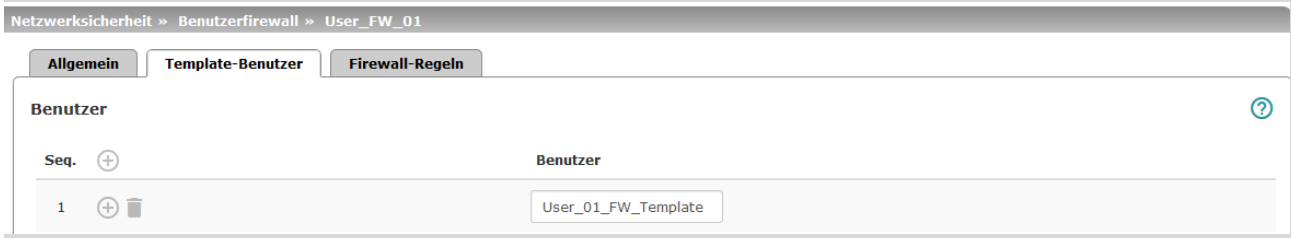
Netzwerksicherheit >> Benutzerfirewall >> Benutzerfirewall-Templates [...]

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 295.) 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; 180 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

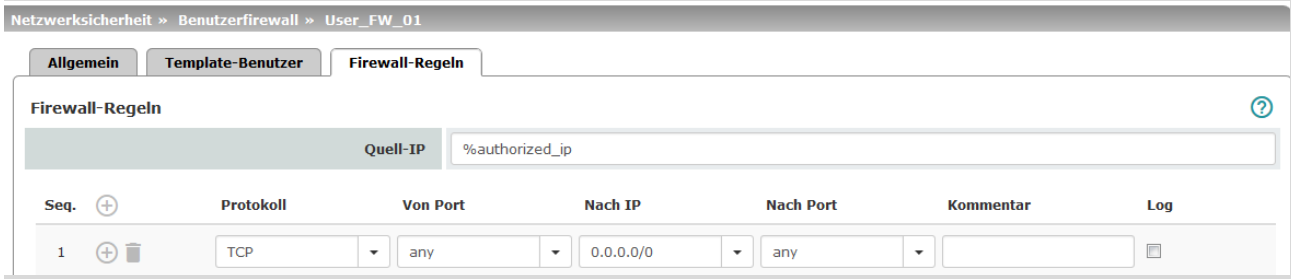
Geben Sie die Namen von Benutzern an. Die Namen müssen denen entsprechen, die unter Menü Authentifizierung >> Firewall-Benutzer festgelegt sind (siehe Seite 247).



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 289).

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 26). **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 289). 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).

9 Menü CIFS-Integrity-Monitoring

Das CIFS-Integrity-Monitoring steht **nicht** für den **FL MGUARD RS2000, TC MGUARD RS2000 3G, TC MGUARD RS2000 4G** und **FL MGUARD RS2005** zur Verfügung.

Es darf **nicht** auf dem **FL MGUARD BLADE Controller** verwendet werden.

Im Netzwerk-Modus Stealth ist ohne Management-IP keine CIFS-Integritätsprüfung möglich.

Die Funktion **CIFS-Anti-Virus-Scan-Connector** wird ab mGuard-Firmwareversion 8.5 nicht mehr unterstützt.

CIFS-Integritätsprüfung

Bei der **CIFS-Integritätsprüfung** werden Windows-Netzlaufwerke daraufhin geprüft, ob sich bestimmte Dateien (z. B. *.exe, *.dll) verändert haben. Eine Veränderung dieser Dateien deutet auf einen Virus oder unbefugtes Eingreifen hin.

Einstellmöglichkeiten für die CIFS-Integritätsprüfung

- Welche Netzlaufwerke dem mGuard bekannt sind (siehe „CIFS-Integrity-Monitoring >> Netzlaufwerke“ auf Seite 312).
- Welche Art von Zugriff erlaubt ist (siehe „CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Einstellungen“ auf Seite 315)
- In welchem Abstand die Laufwerke geprüft werden sollen (siehe „CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Einstellungen >> Editieren >> Überprüftes Netzlaufwerk“ auf Seite 317).
- Welche Dateitypen geprüft werden sollen (siehe „CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Muster für Dateinamen >> Edit“ auf Seite 325).

Form, in der gewarnt werden soll, wenn eine Veränderung festgestellt wird (z. B. per E-Mail, siehe „CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Einstellungen“ auf Seite 315, oder per SNMP, siehe „CIFS-Integritäts-Traps“ auf Seite 112).

9.1 CIFS-Integrity-Monitoring >> Netzlaufwerke

Voraussetzungen

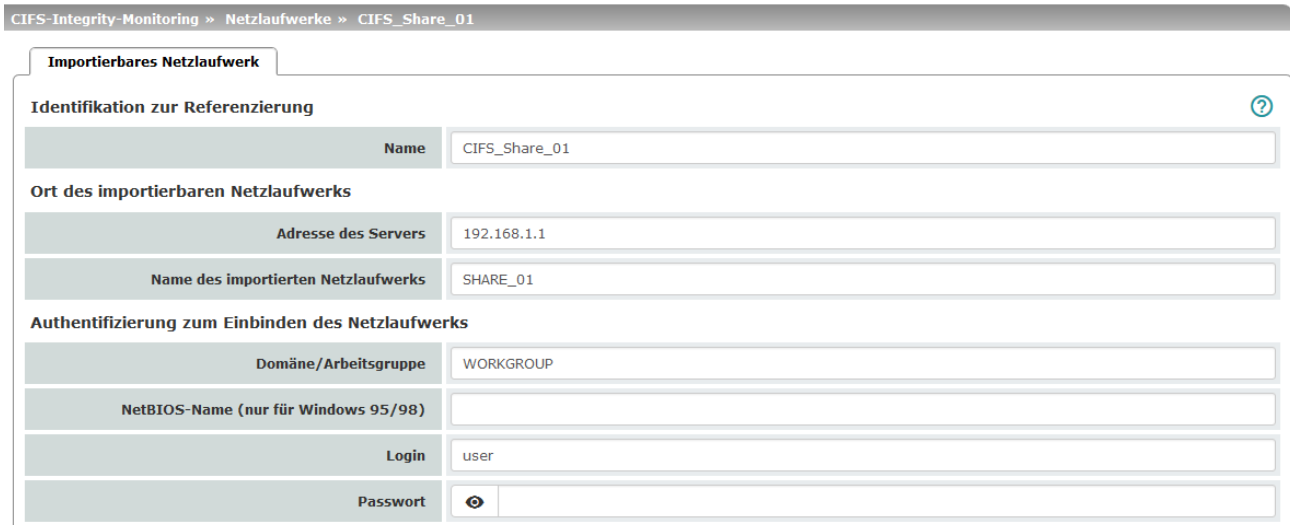
Sie können hier die Netzlaufwerke angeben, die der mGuard regelmäßig prüfen soll.

Damit diese Netzlaufwerke tatsächlich geprüft werden können, müssen Sie zusätzlich bei der CIFS-Integritätsprüfung auf diese Netzlaufwerke verweisen.

Die Verweise auf die Netzlaufwerke können Sie bei der CIFS-Integritätsprüfung einstellen, siehe „Überprüftes CIFS-Netzlaufwerk“ auf Seite 316.

9.1.1 Netzlaufwerke

CIFS-Integrity-Monitoring >> Netzlaufwerke		
Importierbare Netzlaufwerke	**Name**	Name des Netzlaufwerkes, das geprüft werden soll. (Interner Name, der in der Konfiguration verwendet wird.)
	Adresse des Servers	IP-Adresse oder DNS-Hostname des freigebenden Servers.
	Name des importierten Netzlaufwerks	Freigabename für das Netzlaufwerk, das geprüft werden soll. Klicken Sie auf das Icon **Zeile bearbeiten**, um Einstellungen vorzunehmen.



CIFS-Integrity-Monitoring >> Netzlaufwerke >> Editieren		
Identifikation zur Referenzierung	**Name**	Name des Netzlaufwerkes, das geprüft werden soll. (Interner Name, der in der Konfiguration verwendet wird.)
Ort des importierbaren Netzlaufwerks	**Adresse des Servers**	IP-Adresse oder DNS-Hostname des freigebenden Servers.
	Name des importierten Netzwerkes	Freigabename für das Netzlaufwerk, das geprüft werden soll.
Authentifizierung zum Anbinden des Netzlaufwerks	**Domäne/Arbeitsgruppe**	Name der Arbeitsgruppe, zu der das Netzlaufwerk gehört.
	NetBIOS Name (nur für Windows 95/98)	Name für das NetBIOS bei Windows 95/98-Rechner
	Login	Login (Benutzerkennung) für den Server
	Passwort	Passwort für den Login

9.2 CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung

Bei der **CIFS-Integritätsprüfung** werden Windows-Netzlaufwerke daraufhin geprüft, ob sich bestimmte Dateien (z. B. *.exe, *.dll) verändert haben. Eine Veränderung dieser Dateien deutet auf einen Virus oder unbefugtes Eingreifen hin.

Integritätsdatenbank

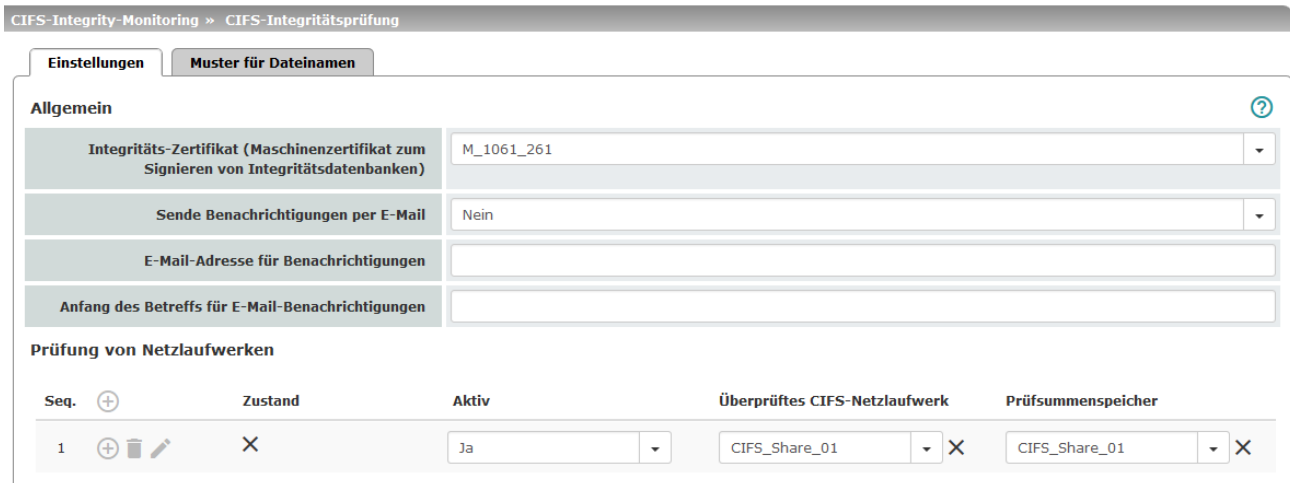
Wenn ein zu prüfenden Netzlaufwerk neu konfiguriert wird, muss eine Integritätsdatenbank angelegt werden.

Diese Integritätsdatenbank dient als Vergleichsgrundlage für die regelmäßige Prüfung des Netzlaufwerks. Darin sind die Prüfsummen aller zu überwachender Dateien aufgezeichnet. Die Integritätsdatenbank selbst ist gegen Manipulation gesichert.

Die Integritätsdatenbank wird entweder auf explizite Veranlassung erstellt (siehe *CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Einstellungen >> Editieren >> Verwaltung*, *Aktionen*) oder zum Zeitpunkt der ersten regulären Prüfung des Laufwerkes.

Nach einer gewollten Manipulation der relevanten Dateien des Netzlaufwerks muss die Integritätsdatenbank neu erstellt werden. Solange keine (gültige) Integritätsdatenbank besteht, kann eine unerlaubte Manipulation der relevanten Dateien nicht entdeckt werden.

9.2.1 Einstellungen



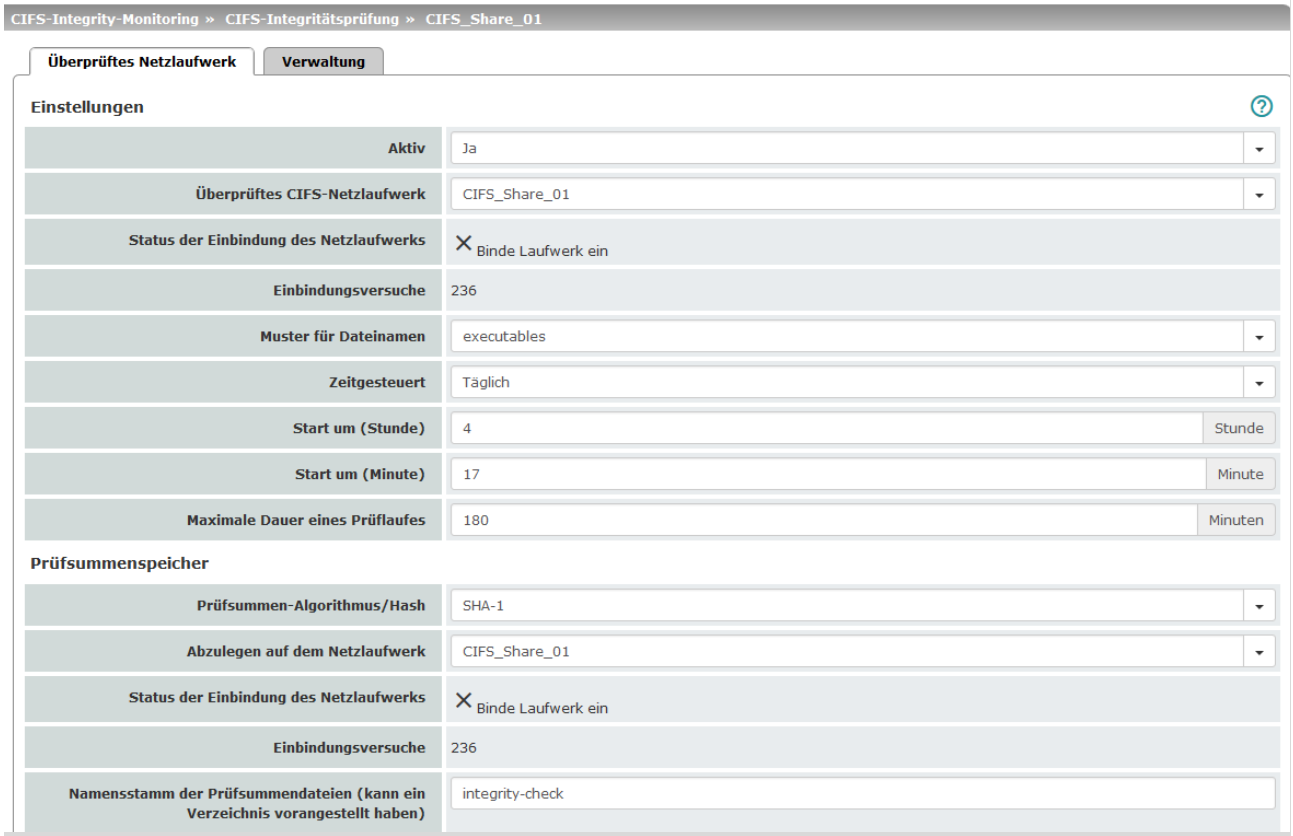
CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Einstellungen		
Allgemein	**Integritätszertifikat (Maschinenzertifikat zum Signieren von Integritätsdatenbanken)**	Dient zum Signieren und Prüfen der Integritätsdatenbank, damit diese nicht unbemerkt durch einen Angreifer ausgetauscht oder manipuliert werden kann. Informationen zu Zertifikaten finden Sie unter „Maschinenzertifikate“ auf Seite 261.
	Sende Benachrichtigung per E-Mail	**Nach jeder Prüfung**: An die unten angegebene Adresse wird nach jeder Prüfung eine E-Mail verschickt. **Nein:** An die unten angegebene Adresse wird keine E-Mail verschickt. **Nur bei Fehlern und Abweichungen**: An die unten angegebene Adresse wird eine E-Mail verschickt, wenn bei der CIFS-Integritätsprüfung eine Abweichung entdeckt worden ist, oder wenn die Prüfung auf Grund eines Zugriffsfehlers nicht stattfindet.
	E-Mail Adresse für Benachrichtigungen	An diese Adresse wird eine E-Mail verschickt, entweder nach jeder Prüfung oder nur, wenn bei der CIFS-Integritätsprüfung eine Abweichung entdeckt worden ist, oder die Prüfung auf Grund eines Zugriffsfehlers nicht stattfinden konnte.
	Anfang des Betreffs für E-Mail-Benachrichtigungen	Text für die Betreffzeile der E-Mail-Nachricht.

CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Einstellungen [...]		
Prüfung von Netzlaufwerken (Wenn Netzlaufwerke definiert sind)	**Zustand**	Zustand des Netzlaufwerks: – Das Netzlaufwerk wurde noch nie überprüft. Eine Integritätsdatenbank liegt wahrscheinlich nicht vor. – Die letzte Prüfung war erfolgreich. – Der Vorgang wurde aufgrund eines nicht erwarteten Ereignisses abgebrochen. Bitte prüfen Sie die Log-Dateien. – Die letzte Prüfung wurde nach Ablauf eines Timeouts abgebrochen. – Die Integritätsdatenbank ist nicht vorhanden oder unvollständig. – Die Signatur der Integritätsdatenbank ist ungültig. – Die Integritätsdatenbank wurde mit einem anderen Prüfsummen-Algorithmus erstellt. – Die Integritätsdatenbank liegt in der falschen Version vor. – Das zu prüfende Netzlaufwerk ist nicht verfügbar. – Das als Prüfsummenspeicher verwendete Netzlaufwerk ist nicht verfügbar. – Eine Datei konnte aufgrund eines I/O-Fehlers nicht gelesen werden (siehe Prüfbericht). – Der Verzeichnisbaum konnte aufgrund eines I/O-Fehlers nicht vollständig durchlaufen werden (siehe Prüfbericht). – Auf alle Dateien im Netzlaufwerk kann erfolgreich zugegriffen werden. Eine Integritätsprüfung kann erfolgen.
	Aktiv	**Ja**: Die Prüfung für dieses Netzlaufwerk wird regelmäßig ausgelöst. **Nein**: Es wird keine Prüfung für dieses Netzlaufwerk ausgelöst. Der mGuard hat dieses Laufwerk nicht verbunden. Ein Status kann nicht eingesehen werden. **Ausgesetzt**: Die Prüfung wird bis auf Weiteres ausgesetzt. Ein Status kann eingesehen werden.
	Überprüftes CIFS-Netzlaufwerk	Name des zu prüfenden Netzlaufwerkes (wird unter *CIFS-Integrity-Monitoring >> Netzlaufwerke >> Editieren* angelegt).
	Prüfsummenspeicher	Um die Prüfung durchführen zu können, muss der mGuard ein Netzlaufwerk zum Auslagern der Dateien zur Verfügung gestellt bekommen. Der Prüfsummenspeicher darf über die externe Netzwerkschnittstelle erreichbar sein.
Aktion	Klicken Sie auf das Icon **Zeile bearbeiten**, um für die Prüfung der Netzlaufwerke weitere Einstellungen vorzunehmen.	

Einstellungen >> Prüfung von Netzlaufwerken >> Edit >> Überprüftes Netzlaufwerk

(siehe unten)

CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Einstellungen >> Editieren >> Überprüftes Netzlaufwerk



Einstellungen	**Aktiv**	**Ja**: Die Prüfung für dieses Netzlaufwerk wird regelmäßig ausgelöst. **Nein**: Es wird keine Prüfung für dieses Netzlaufwerk ausgelöst. Der mGuard hat dieses Laufwerk nicht verbunden. Ein Status kann nicht eingesehen werden. **Ausgesetzt**: Die Prüfung wird bis auf Weiteres ausgesetzt. Ein Status kann eingesehen werden.
	Überprüftes CIFS-Netzlaufwerk	Name des zu prüfenden Netzlaufwerkes (wird unter *CIFS-Integrity-Monitoring >> Netzlaufwerke >> Editieren* angelegt).
	Status der Einbindung des Netzlaufwerks	Zeigt den Status der Einbindung des Netzlaufwerks an.
	Versuche	Anzahl der erfolglosen Einbindungsversuche seit der letzten Umkonfiguration des Netzlaufwerks oder nach Neustart des mGuards.

CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Einstellungen >> Editieren >> Überprüftes Netzlaufwerk [...]

Muster für Dateinamen

Es werden bestimmte Datei-Typen geprüft (z. B. nur ausführbare Dateien wie *.exe, *.dll).

Sie können die Regeln dafür unter *CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Muster für Dateinamen >> Edit* einstellen.

Lassen Sie keine Dateien prüfen, die im Regelbetrieb verändert werden, da sonst Fehlalarme ausgelöst werden.

Lassen Sie keine Dateien prüfen, die gleichzeitig **exklusiv** von anderen Programmen geöffnet werden müssen, da dies zu Zugriffskonflikten führen kann.

Zeitgesteuert

Sonntags, Montags, Dienstags, ... , Täglich, Mehrmals täglich, Ständig

Sie können täglich, mehrmals täglich oder an einem bestimmte Wochentag die Prüfung starten.

Damit die Zeitsteuerung funktioniert, muss die Systemzeit des mGuards gesetzt sein.

Solange die Systemzeit nicht synchronisiert ist werden keine Integritätsprüfungen durchgeführt.

Dies kann manuell oder über NTP geschehen (siehe „Zeit und Datum“ auf Seite 47).

Eine Überprüfung wird nur gestartet, wenn der mGuard zum eingestellten Zeitpunkt in Betrieb ist. Ist er außer Betrieb, wird eine Prüfung nicht nachgeholt, wenn der mGuard später in Betrieb genommen wird.

Wenn zum Zeitpunkt des nächsten Starts die vorherige Prüfung noch läuft, wird der Start der nächsten Prüfung entsprechend verschoben.

Wenn eine Prüfung durch Umkonfiguration in weniger als einer Minute starten würde, wird sie erst zum nächsten Intervall gestartet.

Sie können die Prüfung auch manuell starten (siehe *CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Einstellungen >> Editieren >> Verwaltung, Aktionen*).

Start um (Stunde)

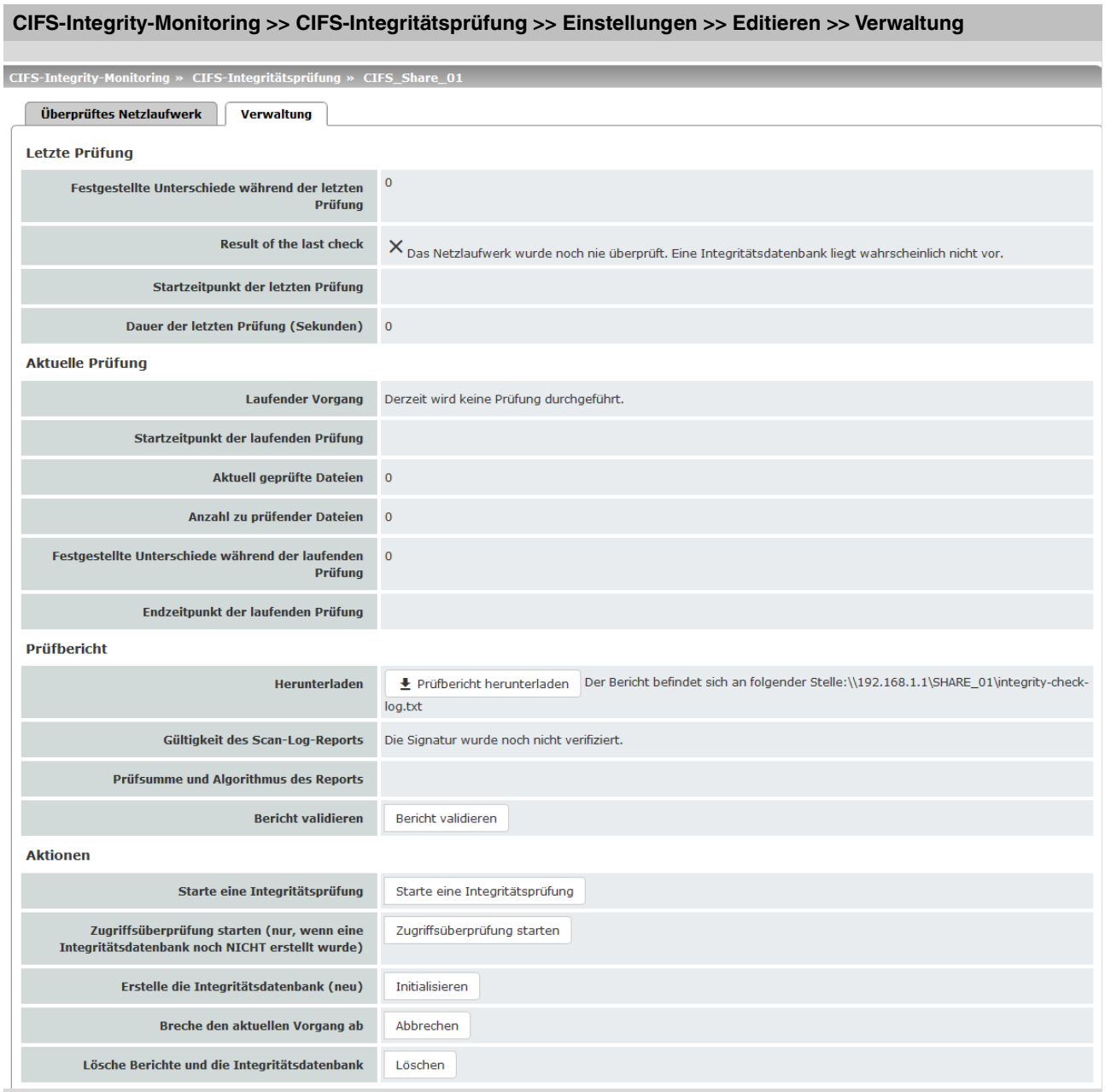
Uhrzeit, zu der die Prüfung startet (Stunde).

Bei Auswahl von „Mehrmals täglich“ alle: 1 h, 2 h, 3 h, 4 h, 6 h, 8 h, 12 h

CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Einstellungen >> Editieren >> Überprüftes Netzlaufwerk [...]		
	Start um (Minute)	Uhrzeit, zu der die Prüfung startet (Minute). Bei Auswahl von „Mehrmals täglich“ alle: 1 h, 2 h, 3 h, 4 h, 6 h, 8 h, 12 h
	Maximale Dauer eines Prüflaufes	Maximale Dauer des Prüfablaufes in Minuten. So können Sie sicherstellen, dass die Prüfung rechtzeitig (z. B. vor Beginn des Schichtbetriebes) abgeschlossen sein wird.
Prüfsummenspeicher	**Prüfsummen-algorithmus/Hash**	**MD5, SHA-1, SHA-256** (Default) Prüfsummenalgorithmen wie MD5, SHA-1 oder SHA-256 helfen zu überprüfen, ob eine Datei verändert wurde. SHA-256 gilt als sicherer als SHA-1, benötigt aber länger in der Verarbeitung. Die Verwendung von MD5 und SHA-1 wird aus Sicherheitsgründen nicht mehr empfohlen (Siehe „Verwendung sicherer Verschlüsselungs- und Hash-Algorithmen“ auf Seite 19).
	Abzulegen auf dem Netzlaufwerk	Um die Prüfung durchführen zu können, muss der mGuard ein Netzlaufwerk zum Auslagern der Dateien zur Verfügung gestellt bekommen. Der Prüfsummenspeicher darf über die externe Netzwerkschnittstelle erreichbar sein. Dasselbe Netzlaufwerk kann für verschiedene zu prüfende Netzlaufwerke als Prüfsummenspeicher verwendet werden. Der Namensstamm für die Prüfsummendateien muss dann allerdings eindeutig gewählt werden. Der mGuard merkt sich, welchen Versionstand die Prüfsummendateien auf dem Netzlaufwerk haben müssen. Wenn es zum Beispiel notwendig ist, nach einem Defekt des Netzlaufwerkes dessen Inhalt von einem Backup wieder herzustellen, dann werden zu alte Prüfsummendateien bereitgestellt werden, und der mGuard würde Abweichungen erkennen. In diesem Fall muss die Integritätsdatenbank neu erstellt werden (siehe *CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Einstellungen >> Editieren >> Verwaltung, Aktionen*).
	Status der Einbindung des Netzlaufwerks	Zeigt den Status der Einbindung des Netzlaufwerks an.
	Einbindungsversuche	Anzahl der Einbindungsversuche seit der letzten Umkonfiguration des Netzlaufwerks oder nach Neustart des mGuards.

CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Einstellungen >> Editieren >> Überprüftes Netzlaufwerk [...]		
	Namensstamm der Prüfsummendateien (kann ein Verzeichnis vorangestellt haben)	Die Prüfsummendateien werden auf dem oben genannten Netzlaufwerk abgelegt. Sie können Sie auch in einem eigenen Verzeichnis ablegen. Der Verzeichnisname darf nicht mit einem Backslash (\) beginnen. Beispiel: Prüfsummenverzeichnis\integrity-checksum Es gibt ein Verzeichnis „Prüfsummenverzeichnis“ in dem Dateien liegen, die mit „integrity-checksum“ beginnen.

Einstellungen >> Prüfung von Netzlaufwerken >> Edit >> Verwaltung



Letzte Prüfung

(Ergebnisse werden nur angezeigt, wenn eine Prüfung stattgefunden hat.)

Festgestellte Unterschiede während der letzten Prüfung

Anzahl der gefundenen Unterschiede auf dem Netzlaufwerk.

Ergebnis der letzten Prüfung

Das Ergebnis der letzten Prüfung (siehe „Zustand“ auf Seite 316)

CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Einstellungen >> Editieren >> Verwaltung [...]		
	Startzeitpunkt der letzten Prüfung	Wochentag, Monat, Tag, HH:MM:SS koordinierte Weltzeit (UTC, Coordinated Universal Time). Die Landeszeit kann von dieser Zeit abweichen. **Beispiel**: Die Standardzeit in Deutschland ist die mitteleuropäische Zeit (MEZ), die gleich der UTC plus einer Stunde ist. Während der Sommerzeit gilt die mitteleuropäische Sommerzeit, die der UTC plus zwei Stunden entspricht.
	Dauer der letzten Prüfung (Sekunden)	Dauer der Prüfung in Sekunden.
Aktuelle Prüfung (Ergebnisse werden nur angezeigt, wenn eine Prüfung stattgefunden hat.)	**Laufender Vorgang**	Aktueller Betriebszustand während der Prüfung: – Derzeit wird keine Prüfung durchgeführt. – Die Prüfung dieses Netzlaufwerks ist ausgesetzt. – Gerade läuft eine Prüfung des Laufwerkes. – Eine Integritätsdatenbank wird erstellt. – Zugriffsberechtigungen werden geprüft.
	Startzeitpunkt der laufenden Prüfung	Startzeitpunkt, an dem die laufenden Integritätsprüfung gestartet wurde.
	Aktuell geprüfte Dateien	Anzahl der Dateien, die während der laufenden Prüfung geprüft wurden.
	Anzahl zu prüfender Dateien	Gesamtzahl der Dateien, die geprüft werden sollen.
	Festgestellte Unterschiede während der laufenden Prüfung	Anzahl der gefundenen Unterschiede auf dem Netzlaufwerk.
	Endzeitpunkt der laufenden Prüfung	Voraussichtlicher Zeitpunkt, zu dem die Prüfung abgeschlossen ist.
Prüfbericht	**Herunterladen**	Hier finden Sie den Prüfbericht. Er kann über die Schaltfläche „**Bericht herunterladen**“ heruntergeladen werden. Der Bericht wird als Log-Datei mit dem Dateinamen „integrity-check-log.txt“ auf dem überprüften Netzlaufwerk abgelegt. Bei jeder neue Prüfung wird die Log-Datei um die Ergebnisse der neuen Prüfung erweitert. Erreicht die Datei eine Dateigröße von 32 MB, wird sie umbenannt in „integrity-check-log.txt.1“ (Backup-Datei). Eine neue Log-Datei „integrity-check-log.txt“ mit den Ergebnissen der aktuellen Prüfung wird angelegt. Erreicht diese Datei eine Dateigröße von 32 MB wird sie ebenfalls in „integrity-check-log.txt.1“ umbenannt, und die existierende Datei „integrity-check-log.txt.1“ wird unwiderruflich überschrieben. Die Integrität der Log-Dateien wird über die Erstellung von Prüfsummen sichergestellt. Durch einen Klick auf die Schaltfläche **„Bericht validieren“** wird geprüft, ob der Bericht in der vom mGuard erstellten Form unverändert vorliegt (Prüfung mit Hilfe von Signatur und Zertifikat).

CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Einstellungen >> Editieren >> Verwaltung [...]		
	Gültigkeit des Scan-Log-Reports	Ergebnis der Signaturprüfung: – Die Signatur wurde noch nicht verifiziert. – Die Signatur ist gültig. – FEHLER: Der Bericht fehlt. – FEHLER: Der Prüfbericht gehört nicht zu diesem Gerät oder er ist nicht aktuell. – FEHLER: Der Prüfbericht wurde mit einem anderen Prüfsummen-Algorithmus erstellt. – FEHLER: Der Prüfbericht wurde verfälscht. – FEHLER: Der Prüfbericht ist nicht verfügbar. Prüfen Sie, ob das Netzlaufwerk eingebunden (mounted) ist.
	Prüfsumme und Algorithmus des Reports	Prüfsumme und Algorithmus
	Bericht validieren	Die Signatur des Prüfberichts wird überprüft.
Aktionen	**Starte eine Integritätsprüfung**	Durch einen Klick auf die Schaltfläche **Integritätsprüfung starten**, wird mit der Integritätsprüfung begonnen. Das Ergebnis der Prüfung kann durch einen Klick auf die Schaltfläche **Bericht herunterladen** im Prüfbericht eingesehen werden. Eine **Integritätsprüfung** kann erst dann durchgeführt werden, wenn zuvor eine **Integritätsdatenbank** erstellt wurde.
	Zugriffsüberprüfung starten (nur, wenn eine Integritätsdatenbank noch NICHT erstellt wurde)	**ACHTUNG: Eine bestehende Integritätsdatenbank wird gelöscht!** Führen Sie die **Zugriffsüberprüfung** nur durch, wenn noch keine **Integritätsdatenbank** erstellt wurde oder eine neue erstellt werden soll. Durch einen Klick auf die Schaltfläche **Zugriffsüberprüfung starten** wird geprüft, ob auf dem importierten Netzlaufwerk Dateien vorhanden sind, auf die der mGuard nicht zugreifen kann. Damit wird im Vorfeld verhindert, dass eine umfangreichere **Erstellung der Integritätsdatenbank** aufgrund fehlender Berechtigungen abgebrochen wird. Nach einer **Zugriffsüberprüfung** muss die **Integritätsdatenbank** mit einem Klick auf die Schaltfläche **Initialisieren** neu erstellt werden (siehe unten). Das Ergebnis der Prüfung kann durch einen Klick auf die Schaltfläche **Bericht herunterladen** im Prüfbericht eingesehen werden.

CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Einstellungen >> Editieren >> Verwaltung [...]

Erstelle die Integritätsdatenbank (neu)

Vor der Erstellung einer Integritätsdatenbank sollte zunächst eine **Zugriffsüberprüfung** durchgeführt werden. Fehlende Zugriffsberechtigungen können so frühzeitig erkannt werden.

Eine bestehende Integritätsdatenbank wird durch eine Zugriffsüberprüfung gelöscht!

Der mGuard legt eine Datenbank mit Prüfsummen an, um festzustellen ob sich Dateien verändert haben. Eine Veränderung von ausführbaren Dateien deutet auf einen Virenbefall hin.

Wenn jedoch diese Dateien absichtlich verändert worden sind, muss durch einen Klick auf die **Schaltfläche Initialisieren** eine neue Datenbank erzeugt werden, um Fehlalarme zu verhindern.

Das Erzeugen einer Integritätsdatenbank ist auch sinnvoll, wenn Netzlaufwerke neu eingerichtet worden sind. Ansonsten wird statt der Prüfung beim ersten Prüftermin eine Integritätsdatenbank eingerichtet (wenn zuvor keine **Zugriffsüberprüfung** durchgeführt wurde).

Breche den aktuelle Vorgang ab

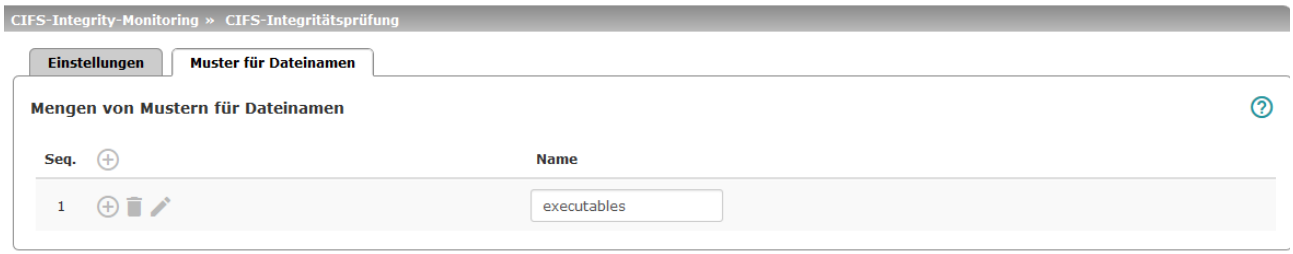
Durch einen Klick auf die Schaltfläche **Abbrechen**, wird die Integritätsprüfung gestoppt.

Lösche Berichte und die Integritätsdatenbank

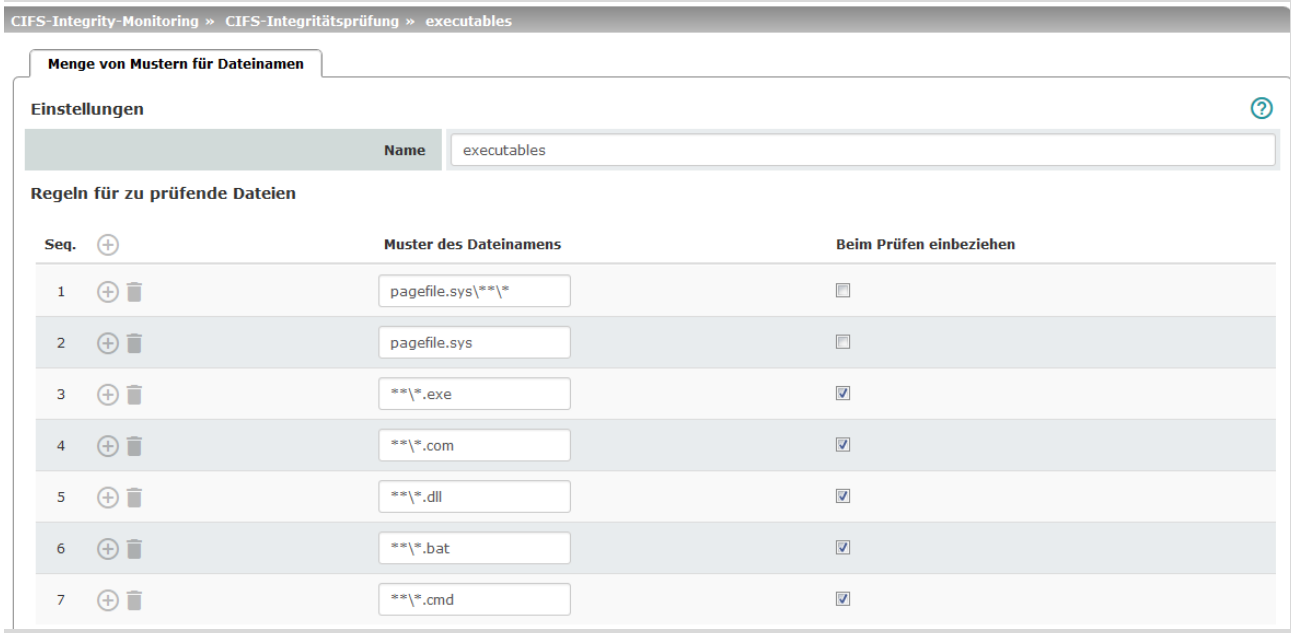
Durch einen Klick auf die Schaltfläche **Löschen** werden die vorhandenen Berichte/Datenbanken gelöscht.

Für eine weitere Integritätsprüfung muss eine neue Integritätsdatenbank angelegt werden. Sie können dies über die Schaltfläche **Initialisieren** anstoßen**.** Ansonsten wird eine neue Integritätsdatenbank zum nächsten Prüftermin automatisch angelegt (wenn zuvor keine **Zugriffsüberprüfung** durchgeführt wurde). Dieser Vorgang ist nicht sichtbar.

9.2.2 Muster für Dateinamen



CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung >> Muster für Dateinamen >> Edit



Mengen von Mustern für Dateinamen	**Name**	Frei definierbarer Name für einen Satz von Regeln für die zu prüfenden Dateien. Dieser Name muss unter **CIFS-Integrity-Monitoring >>CIFS-Integritätsprüfung >> Einstellungen >> Prüfung von Netzlaufwerken >> Editieren** ausgewählt sein, damit das Muster aktiv wird. Klicken Sie auf das Icon **Zeile bearbeiten**, um einen Satz von Regeln für die zu prüfenden Dateien festzulegen und unter dem definierten Namen zu speichern.

CIFS-Integrity-Monitoring >>CIFS-Integritätsprüfung >> Menge von Mustern für Dateinamen >> Editieren

Regeln für zu prüfende Dateien

Muster des Dateinamens

Dabei gibt es folgende Regeln:

****.exe* bedeutet, dass Dateien einbezogen (oder ausgenommen) werden, die in einem beliebigen Verzeichnis liegen und die Dateiendung **.exe* haben.

Nur ein Platzhalter (***) ist pro Verzeichnis oder Dateiname erlaubt.

Platzhalter stehen für beliebige Zeichen, z. B. findet *win**.exe* Dateien mit der Endung *.exe*, die in einem Verzeichnis liegen, dass mit *win*... beginnt.

**** am Anfang bedeutet, dass in einem beliebigen Verzeichnis gesucht wird, auch in der obersten Ebene, wenn diese leer ist. Es kann nicht mit Zeichen kombiniert werden (z. B. *c*** ist nicht erlaubt).

Beispiel: *Name*****.exe* bezieht alle Dateien mit der Endung .exe ein, die in dem Verzeichnis „*Name*“ und beliebigen Unterverzeichnissen liegen.

Fehlende Dateien führen zu einem Alarm. Fehlende Dateien sind Dateien, die beim Initialisieren vorhanden waren.

Ebenso gibt es einen Alarm, wenn zusätzliche Dateien vorhanden sind.

Beim Prüfen einbeziehen

Funktion aktivieren (= einbeziehen): Die Dateien werden in die Prüfung einbezogen.

(Jeder Dateiname wird mit den Mustern der Reihe nach verglichen. Der erste Treffer entscheidet, ob die Datei in die Integritätsprüfung einbezogen wird. Ohne einen Treffer wird die Datei nicht einbezogen.)

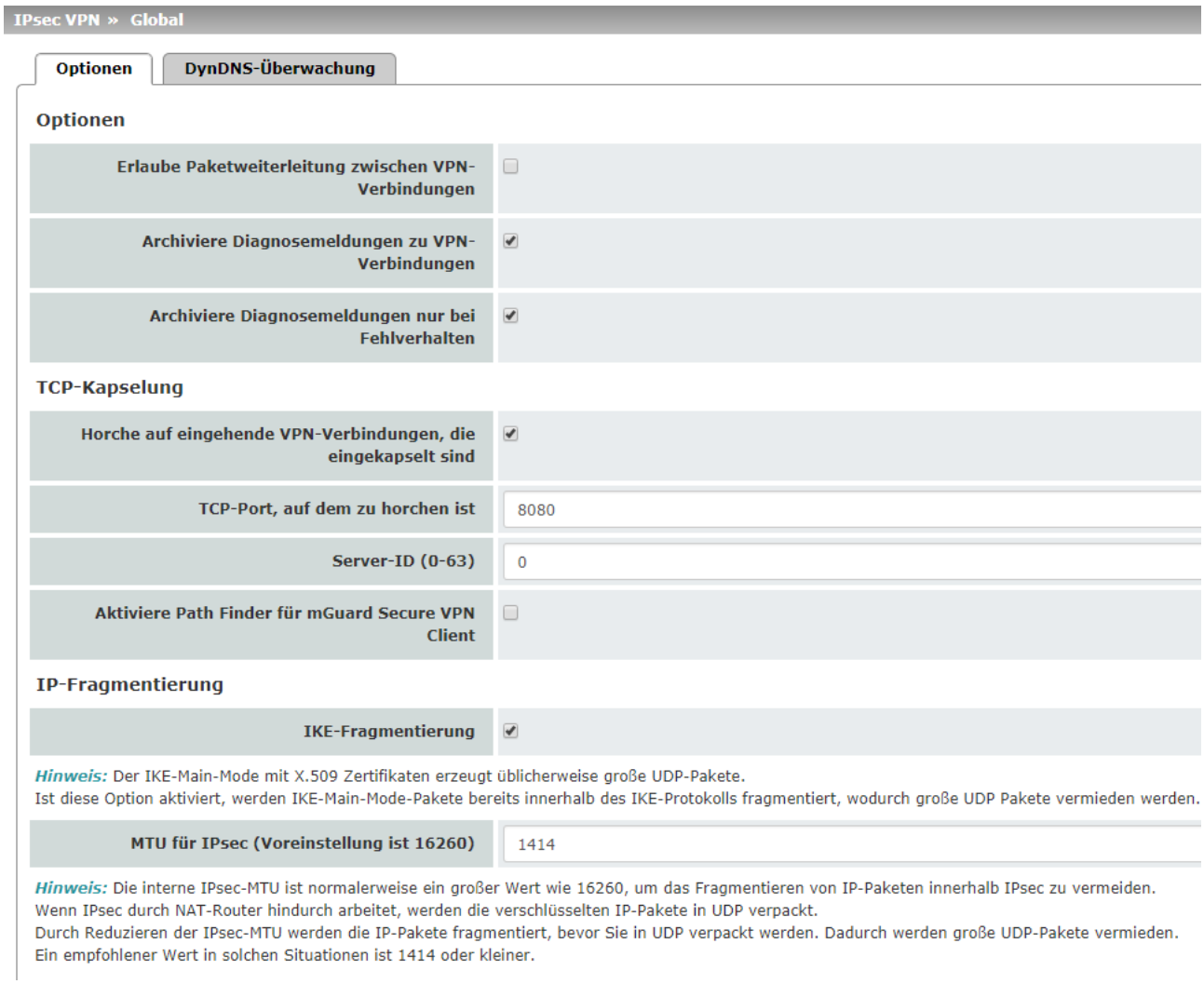
Funktion deaktivieren (= ausnehmen): Die Dateien werden aus der Prüfung ausgenommen.

10 Menü IPsec VPN

Dieses Menü steht **nicht** auf dem **FL MGUARD BLADE-Controller** zur Verfügung.

10.1 IPsec VPN >> Global

10.1.1 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 355).

Die Funktion wird im Netzwerk-Modus *Stealth* nicht unterstützt.

Bei **deaktivierter Funktion** (werkseitige Voreinstellung): 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- und GRE-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 359).

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 (nur bei *FL MGUARD RS4000/RS2000, TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS4004/RS2005* und beim *FL MGUARD RS, FL MGUARD GT/GT*), 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 oder – über SMS 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.net/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 333).

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 Authentification* und *NTLM* gegenüber dem Proxy.

Damit die TCP-Kapselung durch einen HTTP-Proxy hindurch funktioniert, muss einerseits der Proxy explizit in den Proxy-Einstellungen (Menüpunkt *Netzwerk* >> *Proxy-Einstellungen*) benannt werden (darf also kein transparenter Proxy sein) und andererseits muss dieser Proxy die HTTP-Methode CONNECT verstehen und erlauben.

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“

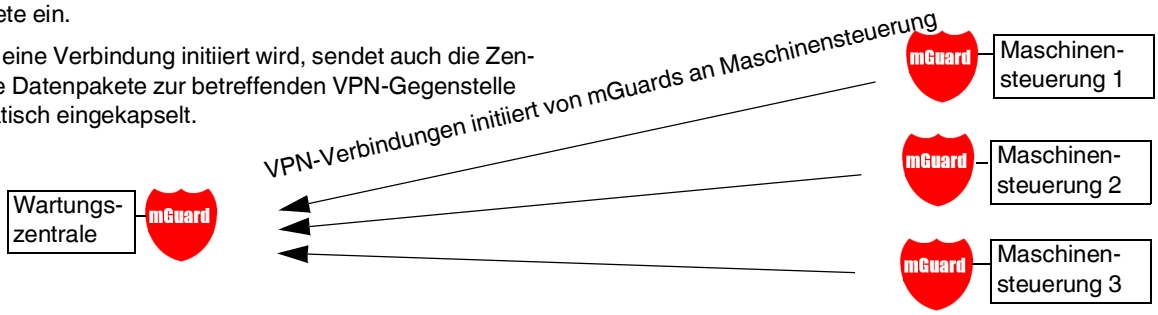
Die TCP-Kapselung mit aktivierter Funktion „Path Finder“ verbessert das Verhalten der oben beschriebenen Standard-TCP-Kapselung.

Wenn die Verbindung neu eingerichtet wird und keine Rückwärtskompatibilität notwendig ist, sollte die Path Finder Funktion 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 331).

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**

mGuards 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**

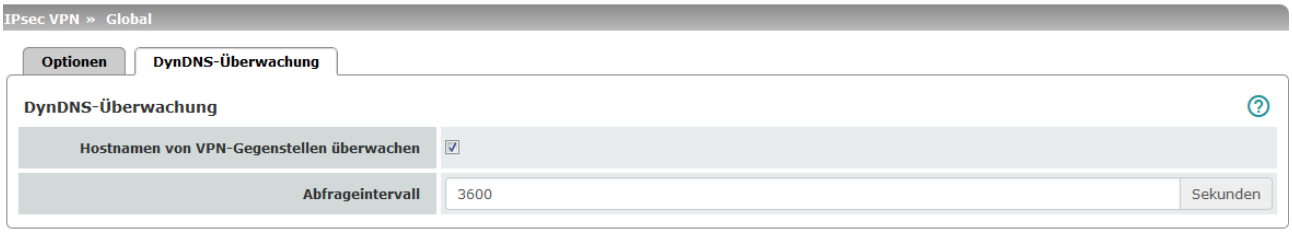
Bild 10-1 TCP-Kapselung bei einem Anwendungsszenario mit Wartungszentrale und ferngewarteten Maschinen über VPN-Verbindungen

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, HTTPS oder SEC-Stick), – 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, HTTPS oder SEC-Stick), – 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.

10.1.2 DynDNS-Überwachung



Erläuterung zu DynDNS siehe „DynDNS“ auf Seite 220.

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 338) 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

10.2 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 154). 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)

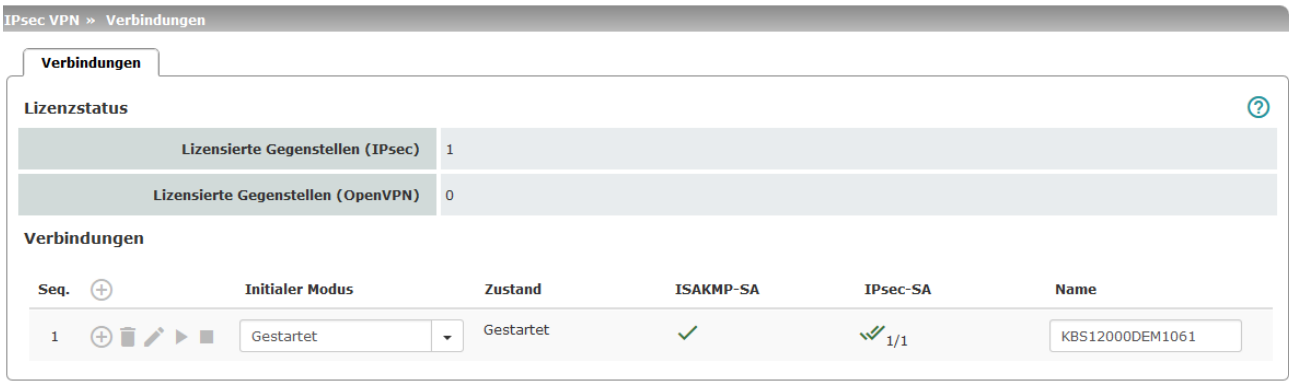
  Ist die Gegenstelle ein Rechner unter Windows 2000, muss dazu das *Microsoft Windows 2000 High Encryption Pack* oder mindestens das *Service Pack 2* installiert sein.
- Befindet sich die Gegenstelle hinter einem NAT-Router, so muss die Gegenstelle NAT-Traversal (NAT-T) unterstützen. Oder aber der NAT-Router 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 im mGuard ausgewählt und verwendet werden.

ACHTUNG: Verwenden Sie sichere Verschlüsselungs- und Hash-Algorithmen
(siehe „Verwendung sicherer Verschlüsselungs- und Hash-Algorithmen“ auf Seite 19).

10.2.1 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, SMS, 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 (nur mGuard-Firmwareversionen < 8.4.0)

https://server/nph-vpn.cgi?name=verbindung&cmd=(up|down|status)
wget --no-check-certificate "https://admin:mGuard@192.168.1.1/nph-vpn.cgi?name=Athen&cmd=up"

Die Verwendung des Kommandozeilen-Tools *wget* funktioniert nur im Zusammenspiel mit mGuard-Firmwareversionen < 8.4.0. Ab mGuard-Firmwareversion 8.4.0 kann das Kommandozeilen-Tool *curl* verwendet werden (Parameter und Optionen abweichend!). Beispiel: *curl --insecure "https://admin:mGuard@192.168.1.1/nph-vpn.cgi?name=Athen&cmd=up“*

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 477).

Die Option ***--no-check-certificate*** (*wget*) bzw. ***--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 349).

Wenn durch Verwendung der oben angegeben URL der Status einer VPN-Verbindung abgefragt wird, können folgende Antworten erwartet werden:

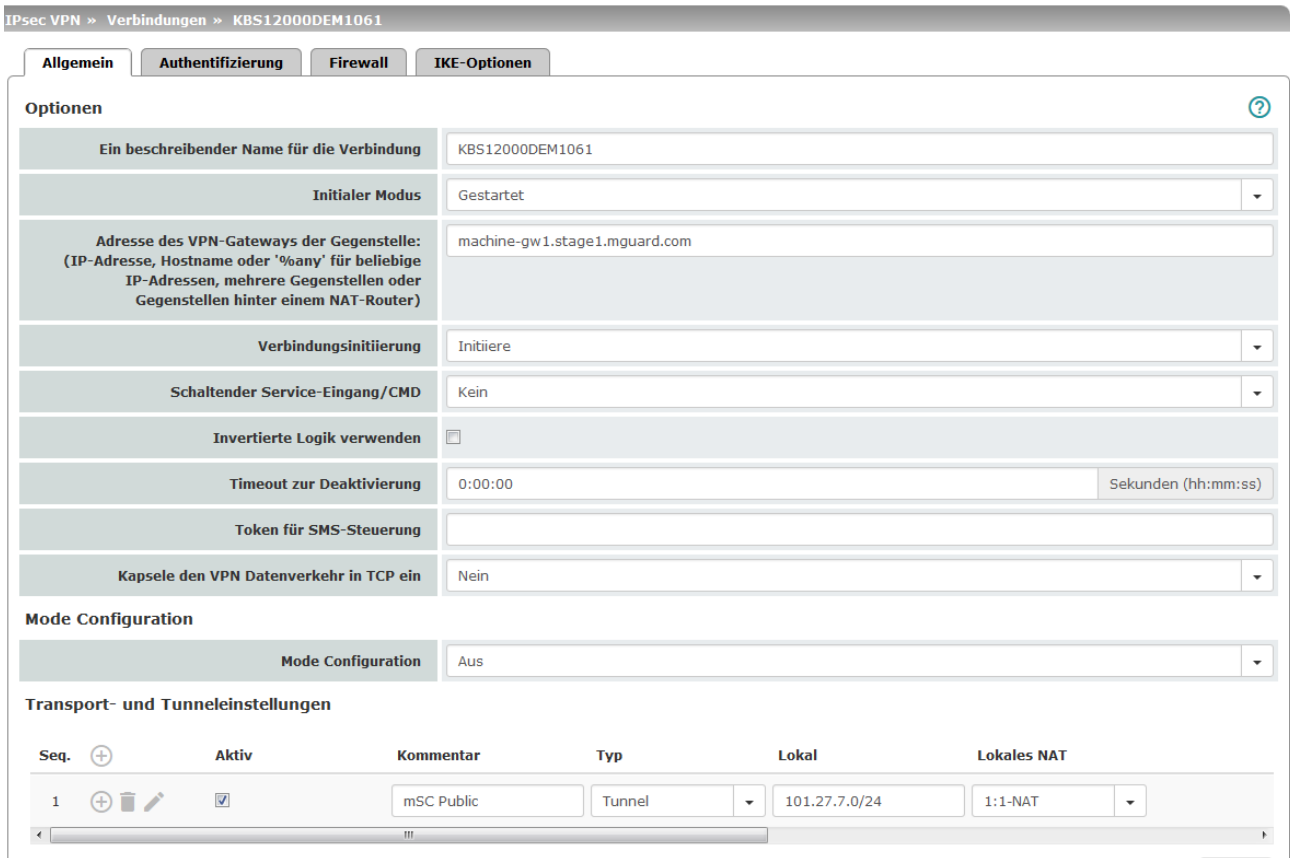
Tabelle 10-1 Status einer VPN-Verbindung

Antwort	Bedeutung
unknown	Eine VPN-Verbindung mit dem Namen existiert nicht.
void	Die Verbindung ist aufgrund eines Fehlers inaktiv, zum Beispiel weil das externe Netzwerk gestört ist oder weil der Hostname der Gegenstelle nicht in eine IP-Adresse aufgelöst werden konnte (DNS). Die Antwort "void" wird von der CGI-Schnittstelle auch herausgegeben, ohne dass ein Fehler vorliegt. Zum Beispiel, wenn die VPN-Verbindung entsprechend der Konfiguration deaktiviert ist (Spalte auf **Nein**) und nicht vorübergehend mit Hilfe der CGI-Schnittstelle oder des CMD-Kontaktes freigeschaltet worden ist.
ready	Die Verbindung ist bereit, selbst 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.

10.2.2 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 359)
- 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, SMS, 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

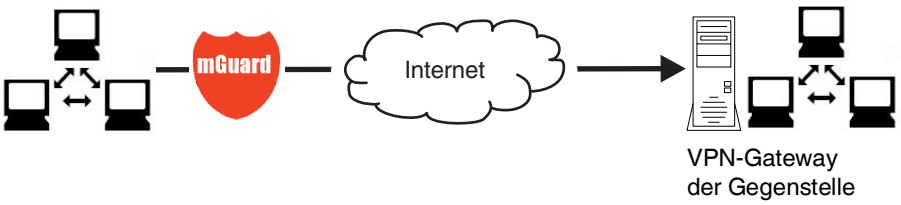


Bild 10-2 Die Adresse des Übergangs zum privaten Netz, in dem sich der entfernte Kommunikationspartner befindet.

- 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 362) 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 331): 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, Extern 2, Einwahl, DMZ, Implizit ausgewählt durch die rechts angegebene IP-Adresse** *Extern 2* und *Einwahl* nur bei Geräten mit serieller Schnittstelle, siehe „Netzwerk >> Interfaces“ auf Seite 135. 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

(Nur verfügbar beim TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS4000/RS2000, FL MGUARD GT/GT, FL MGUARD RS4004/RS2005, FL MGUARD RS.)

Kein / Service-Eingang CMD 1-3

Die VPN-Verbindung kann über einen angeschlossenen Taster/Schalter geschaltet werden.

Der Taster/Schalter muss an einen der Servicekontakte (CMD 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 oder per SMS erfolgen.

Wenn eine VPN-Verbindung über einen VPN-Schalter gesteuert wird, dann kann die VPN-Redundanz nicht aktiviert werden.

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 SMS, 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 [...]		
	Token für SMS-Steuerung (Nur verfügbar beim TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G.)	Eingehende SMS können dazu benutzt werden, VPN-Verbindungen zu initiieren (start) oder zu beenden (stop). Die SMS muss das Kommando „vpn/start“ bzw. „vpn/stop“ gefolgt von dem Token enthalten.

	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 331) 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 332) 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.
		Bei TCP-Kapselung / Path Finder wird der mGuard nicht versuchen, die VPN-Verbindung über die Standard IKE-Verschlüsselung (UDP-Port 500 und 4500) herzustellen, sondern sie immer über das TCP-Protokoll verschicken.
		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).

IPsec VPN >> Verbindungen >> Editieren >> Allgemein [...]

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.

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 in Verbindung mit „VPN-Redundanz“ („VPN-Redundanz“ auf Seite 455) und im „VPN-Aggressive-Mode“ („Aggressive Mode (unsicher)“ auf Seite 366) nicht genutzt werden.

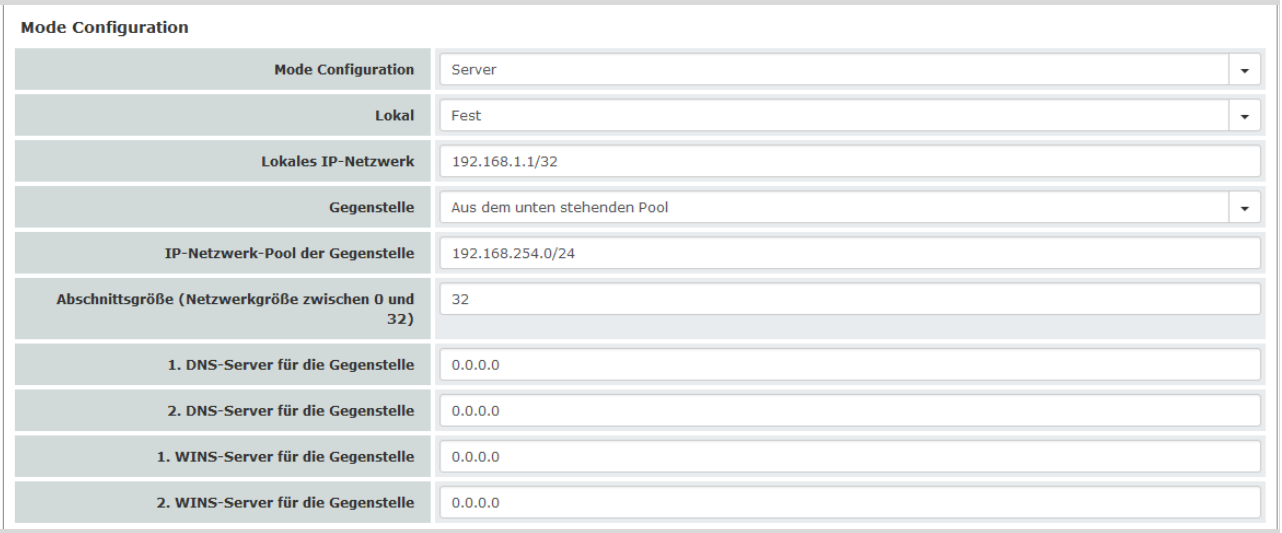
Einstellungen als Server

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) des vom iOS-Client verwendeten mGuard-Maschinenzertifikats muss identisch sein mit der externen IP-Adresse oder dem DNS-Namen des mGuards (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 26).

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.)

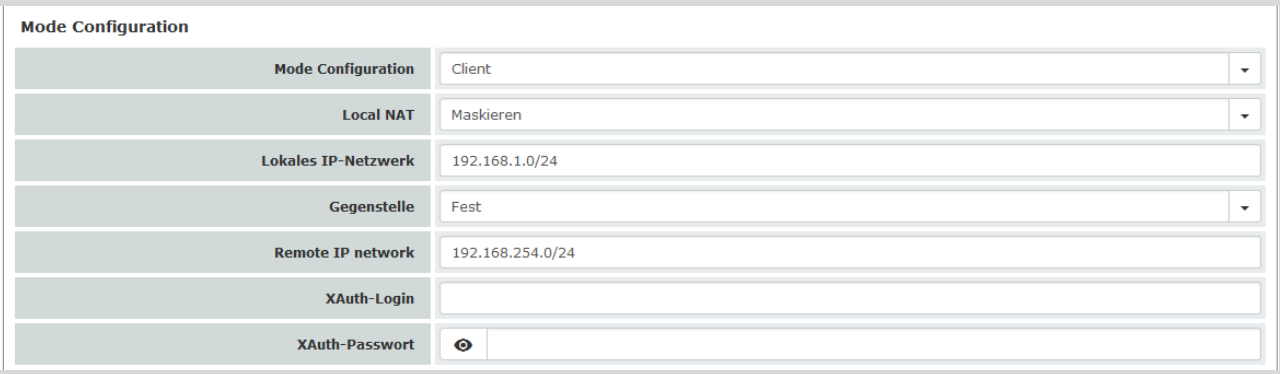
Die IP-Netzwerke der Gegenstelle werden dem Remote-Client über die Split-Tunneling-Erweiterung mitgeteilt.

IPsec VPN >> Verbindungen >> Editieren >> Allgemein [...]

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“.
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

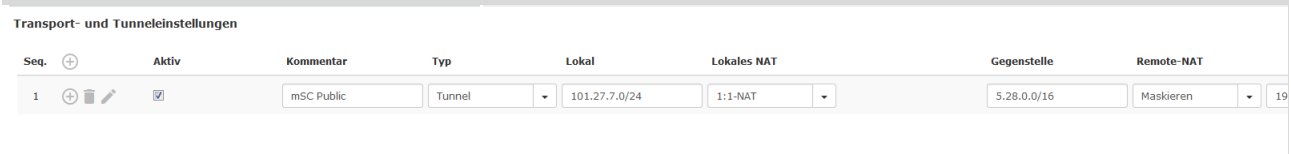
Ermöglicht dem mGuard, eine IPsec-VPN-Verbindung zu Servern aufzubauen, die „XAuth“ und „Mode Config“ benötigen. Die benötigten Werte (IP-Adresse/IP-Netzwerk) zur Konfiguration der Verbindung (lokales und entferntes Netz) erhält der mGuard optional vom Remote-Server der Gegenstelle.

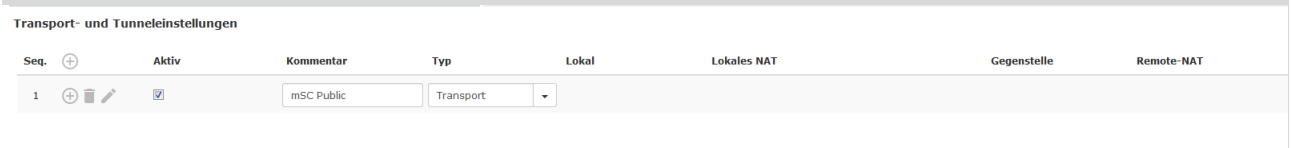


Lokales NAT (Nicht aktiv im Stealth-Modus „Automatisch“ und „Statisch“)	**Kein NAT / Maskieren** **Kein NAT** Vom Server ausgewählte lokale IP-Adressen können den Tunnel nutzen. **Maskieren** Der mGuard kann sein lokales Netz maskieren. Dazu muss das lokale Netz in CIDR-Schreibweise (siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 26) angegeben werden.
Lokales IP-Netzwerk	IP-Netzwerk am lokalen Interface des Clients, das maskiert wird.

IPsec VPN >> Verbindungen >> Editieren >> Allgemein [...]

	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.
	XAuth-Login	Manche Remote-Server benötigen zur Authentifizierung des Clients einen XAuth-Benutzernamen (Login) und ein XAuth-Passwort.
	XAuth-Passwort	Zugehöriges XAuth-Passwort
Transport- und Tunneleinstellungen		





	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

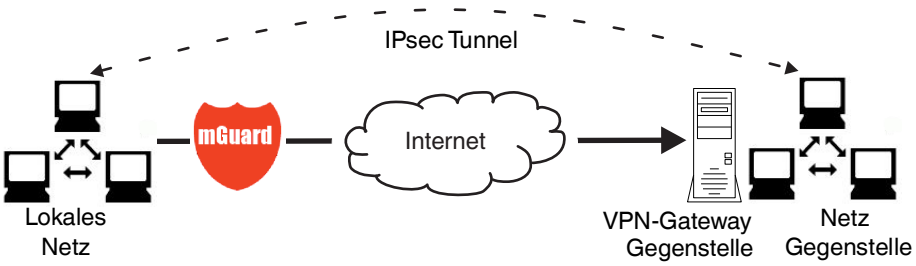
(Bei Verbindungstyp „Tunnel“)

Kein NAT / 1:1-NAT / Maskieren

Kein NAT: Es wird kein NAT vorgenommen.

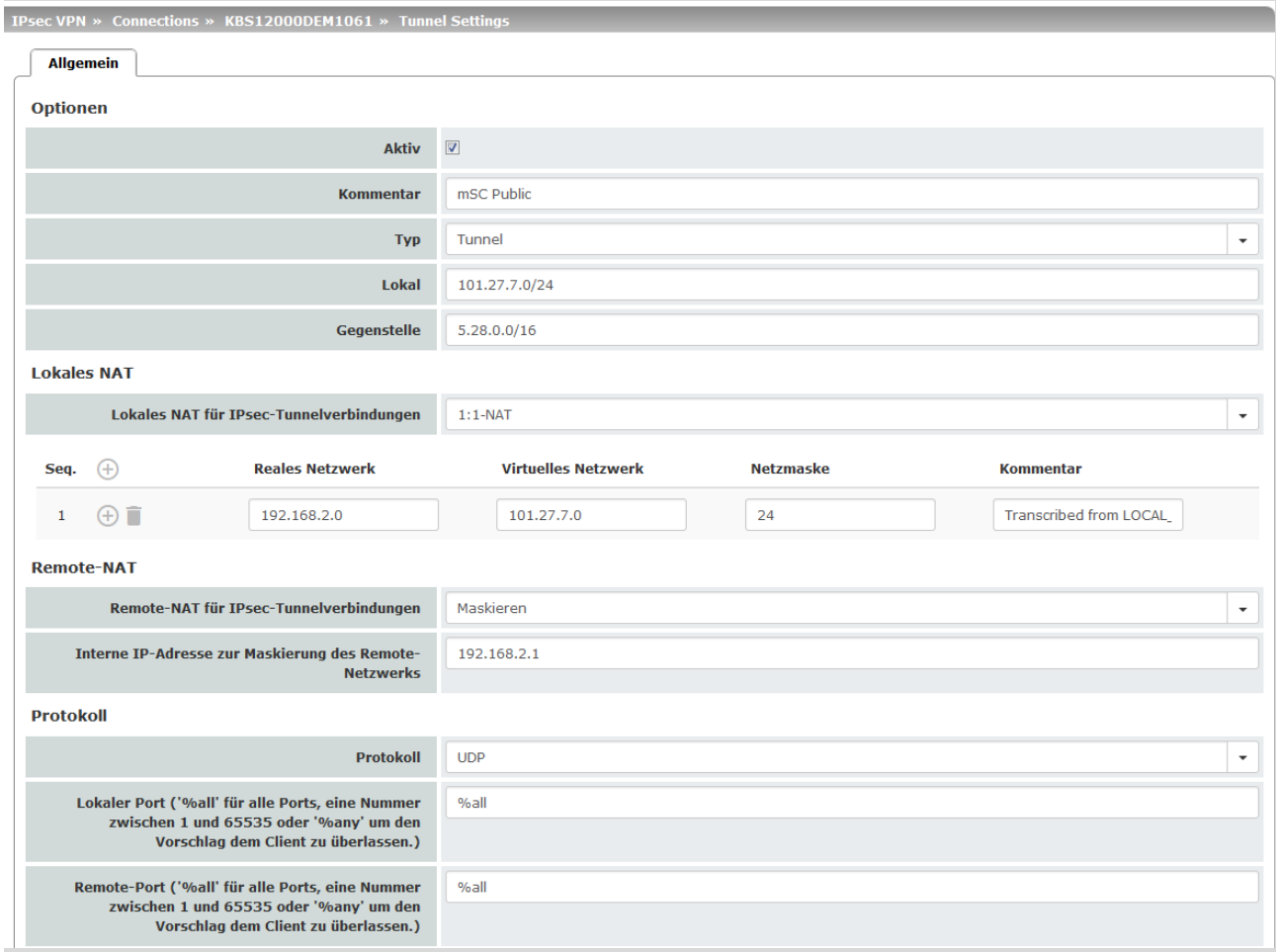
Bei **1:1-NAT** werden die IP-Adressen von Geräten der Gegenstelle des Tunnels so ausgetauscht, dass jede einzelne gegen eine bestimmte andere umgeschrieben wird.

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 [...]



Optionen

Transport- und Tunneleinstellungen (Editieren)

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.

Virtuelles Netzwerk Konfiguriert die umgeschriebene IP-Adresse für 1:1-NAT.

IPsec VPN >> Verbindungen >> Editieren >> Allgemein [...]		
	Netzmaske	Die Netzmaske als Wert zwischen 1 und 32 für die reale und virtuelle Netzwerkadresse (siehe auch „CIDR (Classless Inter-Domain Routing)“ auf Seite 26).
	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.
	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.

IPsec VPN >> Verbindungen >> Editieren >> Allgemein [...]		
	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 ermöglichen** (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 373)

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

Das VPN-Lizenz-Modell (seit mGuard Firmwareversion 8.3) erlaubt es, mit allen VPN-Lizenzen Tunnelgruppen zu erstellen.

Die Lizenz begrenzt nun nicht mehr die Anzahl der aufgebauten Tunnel, sondern die Anzahl der verbundenen Gegenstellen (VPN-Peers). Werden zu einer Gegenstelle mehrere Tunnel aufgebaut, wird nur eine Gegenstelle gezählt, was eine Verbesserung zum alten Modell darstellt.

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, PPPoE, PPTP, Modem, Eingebautes Modem, Eingebautes Mobilfunkmodem und Stealth (nur Stealth-Modus „Mehrere Clients“).

Modem / Eingebautes Modem / Eingebautes Mobilfunkmodem: Steht nicht bei allen mGuard-Modellen zur Verfügung (siehe „Netzwerk >> Interfaces“ auf Seite 135).

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:

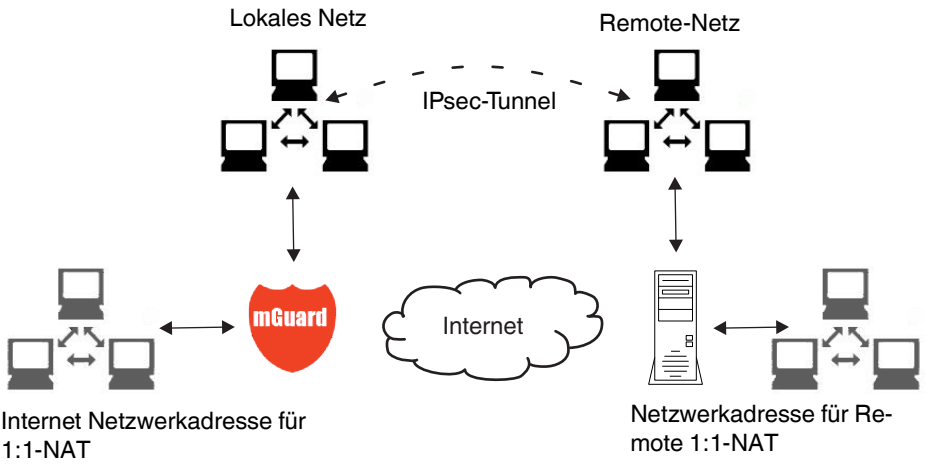
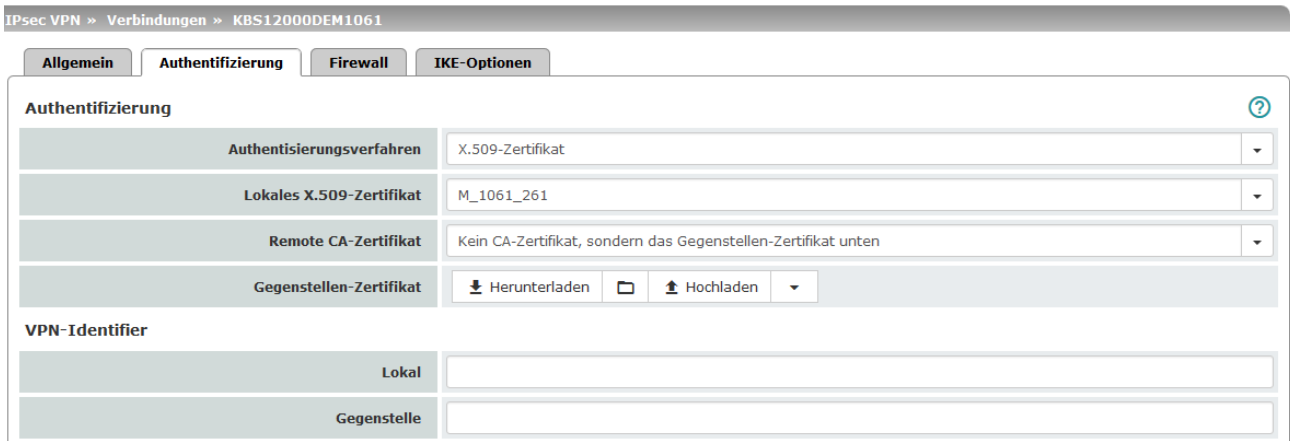


Bild 10-3 1:1-NAT

10.2.3 Authentifizierung



IPsec VPN >> Verbindungen >> Editieren >> Authentifizierung

Authentifizierung

Authentisierungs-verfahren

Es gibt 2 Möglichkeiten:

– X.509-Zertifikat (werkseitige Voreinstellung)

– 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.)

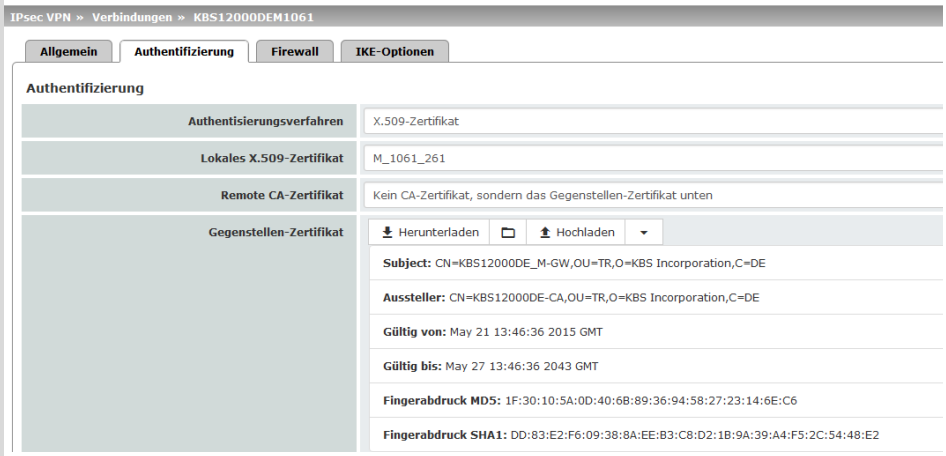
Es muss Folgendes festgelegt werden:

– 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 selbst signiertes 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 265).

Zum Verständnis der nachfolgenden Tabelle siehe Kapitel „Authentifizierung >> Zertifikate“ auf Seite 254.

Authentifizierung bei VPN

Die Gegenstelle zeigt vor:	Maschinenzertifikat von **CA signiert**	Maschinenzertifikat **selbst signiert**
Der mGuard authentifiziert die Gegenstelle anhand von...	⇕	⇕
	Gegenstellen-Zertifikat oder, allen CA-Zertifikaten, die mit dem von der Gegenstelle vorgezeigten Zertifikat die Kette bis zum Root-CA-Zertifikat bilden	Gegenstellen-Zertifikat

Nach dieser Tabelle sind dem mGuard die Zertifikate zur Verfügung zu stellen, die er zur Authentifizierung der jeweiligen VPN-Gegenstelle heranziehen muss.

Voraussetzung

Die nachfolgenden Anleitungen gehen davon aus, dass die Zertifikate bereits ordnungsgemäß im mGuard installiert sind (siehe *„Authentifizierung >> Zertifikate“ auf Seite 254*; 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

Selbst signiertes Maschinenzertifikat

Wenn sich die VPN-Gegenstelle mit einem **selbst signierten** Maschinenzertifikat authentisiert:

- Wählen Sie aus der Auswahlliste folgenden Eintrag:
  „Kein CA-Zertifikat, sondern das Gegenstellen-Zertifikat unten“
- Installieren Sie unter *Gegenstellen-Zertifikat* das Gegenstellen-Zertifikat (siehe „Gegenstellen-Zertifikat installieren“ auf Seite 362).

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 362).

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 Name*s, wenn die im Zertifikat aufgelistet sind. Wenn das Zertifikat *Subject Alternative Name*s enthält, werden diese unter „Gültige Werte sind:“ mit angegeben. Es können IP-Adressen, Hostnamen mit vorangestelltem @-Zeichen oder E-Mail-Adressen sein.

Gegenstelle

Legt fest, was im Maschinenzertifikat der VPN-Gegenstelle als Subject eingetragen sein muss, damit der mGuard diese VPN-Gegenstelle als Kommunikationspartner akzeptiert.

Durch eine entsprechende Festlegung ist es möglich, VPN-Gegenstellen, die der mGuard auf Grundlage von Zertifikatsprüfungen im Prinzip akzeptieren würde, wie folgt zu beschränken bzw. freizugeben:

- Beschränkung auf bestimmte *Subjects* (d. h. Maschinen) und/oder auf *Subjects*, die bestimmte Merkmale (Attribute) haben, oder
- Freigabe für alle *Subjects*

(Siehe „Subject, Zertifikat“ auf Seite 471.)

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.

Achten Sie auf Groß- und Kleinschreibung.

Beachten Sie folgendes, wenn Sie einen Subject-Filter setzen.

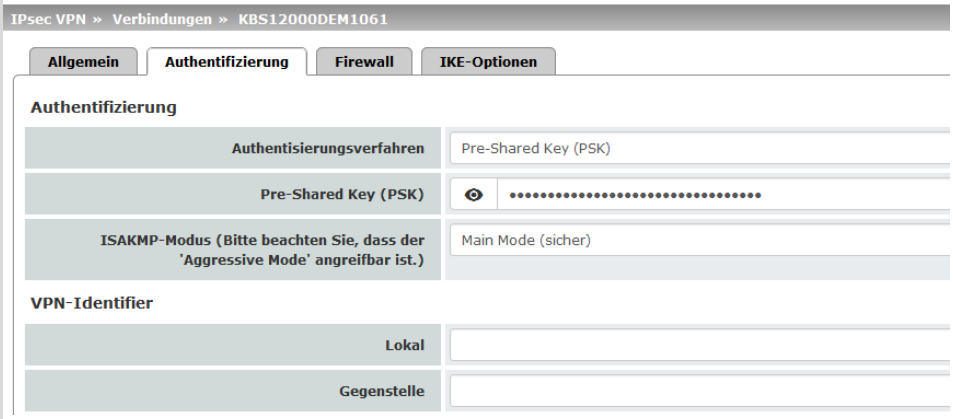
Bei den Attributen müssen Anzahl und Reihenfolge mit denen in den Zertifikaten übereinstimmen, auf die der Filter angewendet wird.

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.

Achten Sie auf Groß- und Kleinschreibung.

Um eine mit 3DES vergleichbare Sicherheit zu erzielen, sollte die Zeichenfolge aus ca. 30 nach dem Zufallsprinzip ausgewählten Klein- und Groß-Buchstaben, Ziffern und Sonderzeichen

Achten Sie auf Groß- und Kleinschreibung.

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.

Achten Sie auf Groß- und Kleinschreibung.

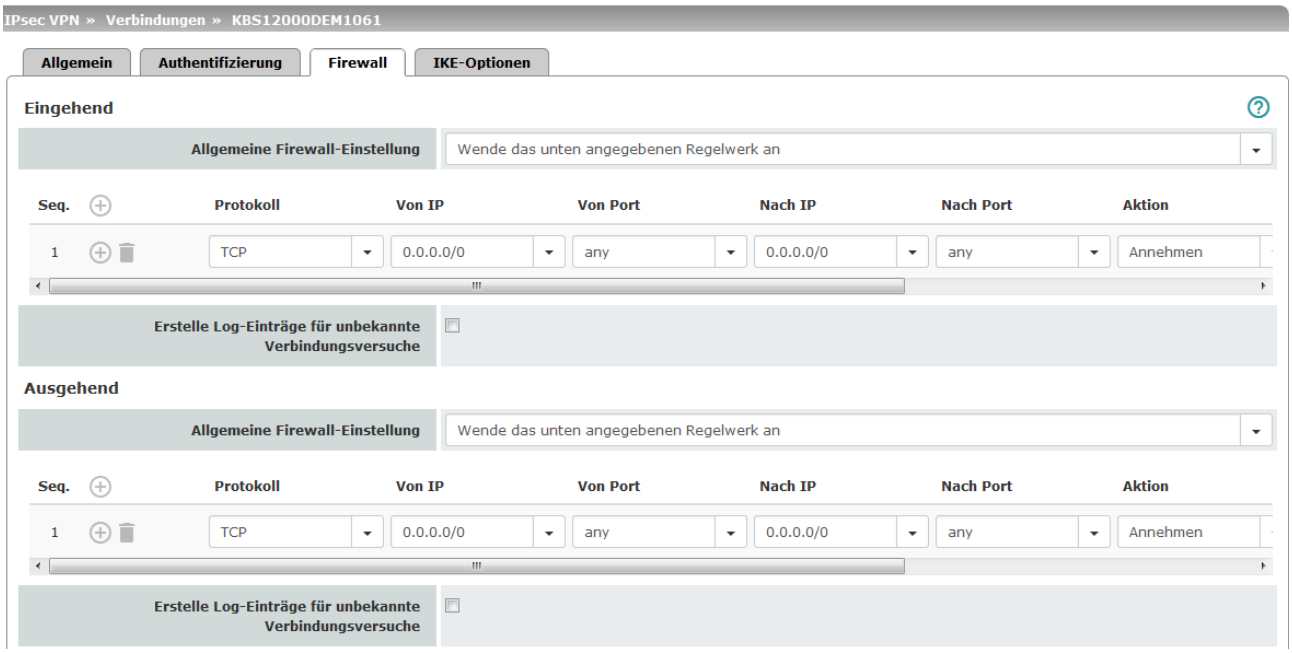
Wenn PSK mit der Einstellung „Aggressive Mode (unsicher)“ genutzt wird, dann sollten beim Responder der Verbindung unter IKE-Optionen alle Diffie-Hellmann-Algorithmen ausgewählt werden.

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“)	

10.2.4 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 271), 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 271, „Netzwerksicherheit >> Paketfilter“ auf Seite 271, „Erweitert“ auf Seite 292).

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 (z. B. durch das Erlauben einer SEC-Stick Hub & Spoke-Verbindung), dann werden vorhandene VPN-Firewall-Regeln nicht angewendet. Das bedeutet, dass zum Beispiel die Pakete einer SSH-Verbindung durch einen VPN-Tunnel geschickt werden, obwohl dessen Firewall-Regel dies verbietet.

IPsec VPN >> Verbindungen >> Editieren >> Firewall		
Eingehend	**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 26).

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 289).

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 mGuard-Geräten der RS2000-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.

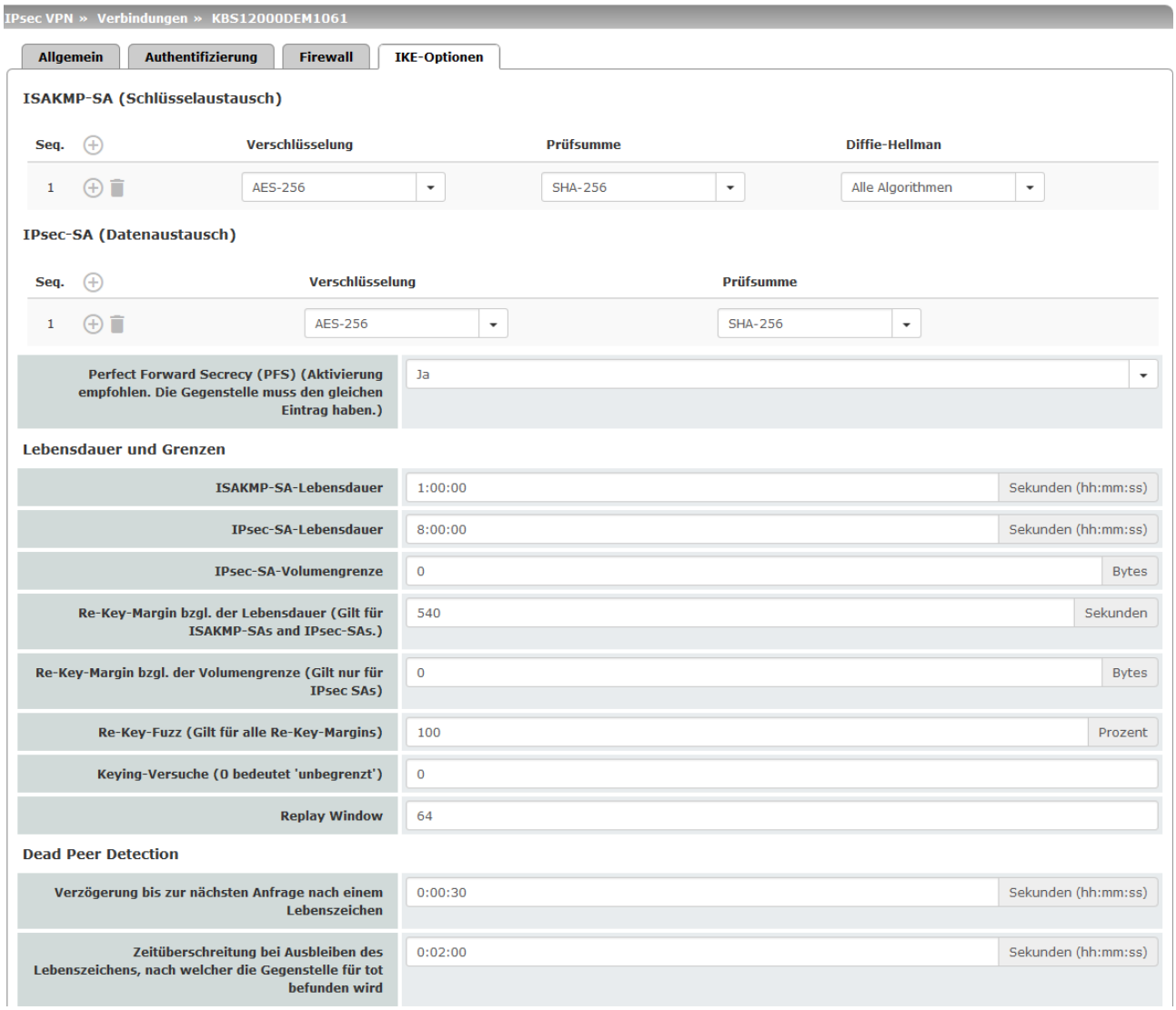
startport:endport (z. B. 110:120) bezeichnet einen Portbereich.

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 289).

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 mGuard-Geräten der RS2000-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 „Modbus TCP“ auf Seite 298).
	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 (werkseitige Voreinstellung).
	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“.	

10.2.5 IKE-Optionen



IPsec VPN >> Verbindungen >> Editieren >> IKE-Optionen

ISAKMP-SA (Schlüsselaustausch)

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 im mGuard ausgewählt und verwendet werden

Siehe „Verwendung sicherer Verschlüsselungs- und Hash-Algorithmen“ auf Seite 19.

Vereinbaren Sie mit dem Administrator der Gegenstelle, welches Verschlüsselungsverfahren verwendet werden soll.

Verschlüsselung

DES, 3DES, AES-128, AES-192, AES-256 (Standard)

Werkseitige Voreinstellung in mGuard Firmwareversion 8.5.0 geändert in AES-256.

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 im mGuard ausgewählt und verwendet werden.

Siehe „Verwendung sicherer Verschlüsselungs- und Hash-Algorithmen“ auf Seite 19.

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.

Der zur Auswahl stehende mit „Null“ bezeichnete Algorithmus beinhaltet keinerlei Verschlüsselung.

IPsec VPN >> Verbindungen >> Editieren >> IKE-Optionen

	Prüfsumme	**MD5, SHA1, SHA-256 (Standard), SHA-512** Werkseitige Voreinstellung in mGuard Firmwareversion 8.6.0 geändert in SHA-256. 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 im mGuard ausgewählt und verwendet werden. Siehe „Verwendung sicherer Verschlüsselungs- und Hash-Algorithmen“ auf Seite 19.
	Diffie-Hellman	Das Schlüsselaustausch-Verfahren Diffie-Hellmann ist nicht für alle Algorithmen verfügbar. Sie können hier die Bit-Tiefe der Verschlüsselung einstellen.
IPsec-SA (Datenaustausch)	Im Unterschied zu *ISAKMP-SA (Schlüsselaustausch)* (s. o.) wird hier das Verfahren für den Datenaustausch festgelegt. Es kann sich von denen des Schlüsselaustausches unterscheiden, muss aber nicht.	
	Algorithmen	Siehe oben: ISAKMP-SA (Schlüsselaustausch). Werkseitige Voreinstellungen in mGuard Firmwareversion 8.6.0 geändert.
	Perfect Forward Secrecy (PFS)	Verfahren zur zusätzlichen Steigerung der Sicherheit bei der Datenübertragung. Bei IPsec werden in bestimmten Intervallen die Schlüssel für den Datenaustausch erneuert. Mit PFS werden dabei mit der Gegenstelle neue Zufallszahlen ausgehandelt, anstatt sie aus zuvor verabredeten Zufallszahlen abzuleiten. Die Gegenstelle muss den gleichen Eintrag haben. Wir empfehlen aus Sicherheitsgründen die Aktivierung. Wenn die Gegenstelle PFS unterstützt, wählen Sie **Ja**. Ist die Gegenstelle ein IPsec/L2TP-Client, dann setzen Sie *Perfect Forward Secrecy (PFS)* auf **Nein**.
Lebensdauer und Grenzen	Die Schlüssel einer IPsec-Verbindung werden in bestimmten Abständen erneuert, um die Kosten eines Angriffs auf eine IPsec-Verbindung zu erhöhen.	

IPsec VPN >> Verbindungen >> Editieren >> IKE-Optionen		
	ISAKMP-SA-Lebensdauer	Lebensdauer der für die ISAKMP-SA vereinbarten Schlüssel in Sekunden (hh:mm:ss). Werkseinstellung: 3600 Sekunden (1 Stunde). Das erlaubte Maximum sind 86400 Sekunden (24 Stunden).
	IPsec-SA-Lebensdauer	Lebensdauer der für die IPsec-SA vereinbarten Schlüssel in Sekunden (hh:mm:ss). Werkseinstellung: 28800 Sekunden (8 Stunden). Das erlaubte Maximum sind 86400 Sekunden (24 Stunden).
	IPsec-SA-Volumengrenze	0 bis 2147483647 Bytes Der Wert 0 bedeutet, dass es keine Volumengrenze für die IPsec-SAs dieser VPN-Verbindung gibt. Alle anderen Werte geben die Anzahl an Bytes an, die maximal von IPsec-SA für diese VPN-Verbindung verschlüsselt werden (Hard Limit).
	Re-Key-Margin bzgl. der Lebensdauer	Gilt für ISAKMP-SAs und IPsec-SAs Minimale Zeitspanne vor Ablauf der alten Schlüssel, innerhalb der ein neuer Schlüssel erzeugt werden soll. Werkseinstellung: 540 Sekunden (9 Minuten).
	Re-Key-Margin bzgl. der Volumengrenze	Gilt nur für IPsec-SAs Der Wert 0 bedeutet, dass die Volumengrenze nicht angewendet wird. Sie müssen 0 einstellen, wenn der unter *IPsec-SA-Volumengrenze* eingestellte Wert 0 ist. Wenn ein Wert über 0 eintragen wird, dann wird eine neue Grenze aus zwei Werten errechnet. Und zwar wird von dem unter *IPsec-SA-Volumengrenze* angegebenen Wert (dem *Hard Limit*) die hier angegebene Byteanzahl abgezogen. Der so errechnete Wert wird als *Soft Limit* bezeichnet. Er gibt die Anzahl an Bytes an, die verschlüsselt worden sein müssen, damit ein neuer Schlüssel für die IPsec SA ausgehandelt wird. Wenn außerdem ein Re-Key-Fuzz (s. u.) über 0 eingetragen ist, wird ein zusätzlicher Betrag abgezogen. Dieser Betrag ist ein Prozentsatz des Re-Key-Margins. Die Höhe dieses Prozentsatzes wird unter Re-Key-Fuzz angegeben. Der Re-Key-Margin-Wert muss unter dem des *Hard Limits* liegen. Er muss sogar deutlich darunter liegen, wenn zusätzlich ein *Re-Key-Fuzz* addiert wird. Wenn die *IPsec-SA-Lebensdauer* vorher erreicht wird, dann wird das *Soft Limit* ignoriert.
	Re-Key-Fuzz	Maximum in Prozent, um das *Re-Key-Margin* zufällig vergrößert werden soll. Dies dient dazu, den Schlüsselaustausch auf Maschinen mit vielen VPN-Verbindungen zeitversetzt stattfinden zu lassen. Werkseinstellung: 100 Prozent.

IPsec VPN >> Verbindungen >> Editieren >> IKE-Optionen		
	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. Werkseinstellung: 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**).

10.3 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.

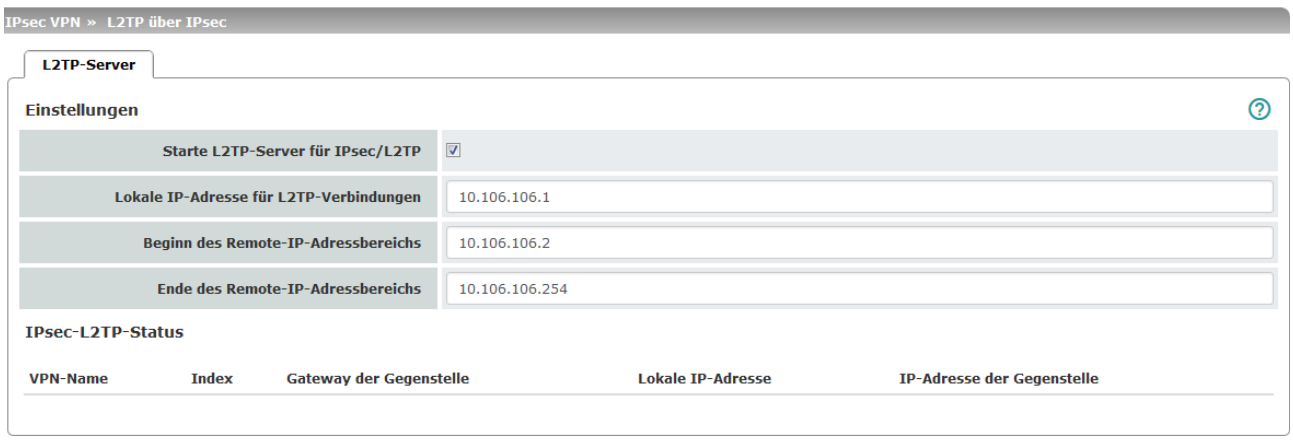
Um IPsec/L2TP zu nutzen muss der L2TP-Server aktiviert werden sowie eine oder mehrere IPsec-Verbindungen mit den folgenden Eigenschaften eingerichtet werden:

– **Typ**: Transport
– **Protokoll**: UDP
– **Lokal:** %all
– **Gegenstelle:** %all
– **PFS**: Nein

Siehe

– IPsec VPN >> Verbindungen >> Editieren >> Allgemein auf Seite 340
– IPsec VPN >> Verbindungen >> Editieren >> IKE-Optionen, Perfect Forward Secrecy (PFS) auf Seite 373

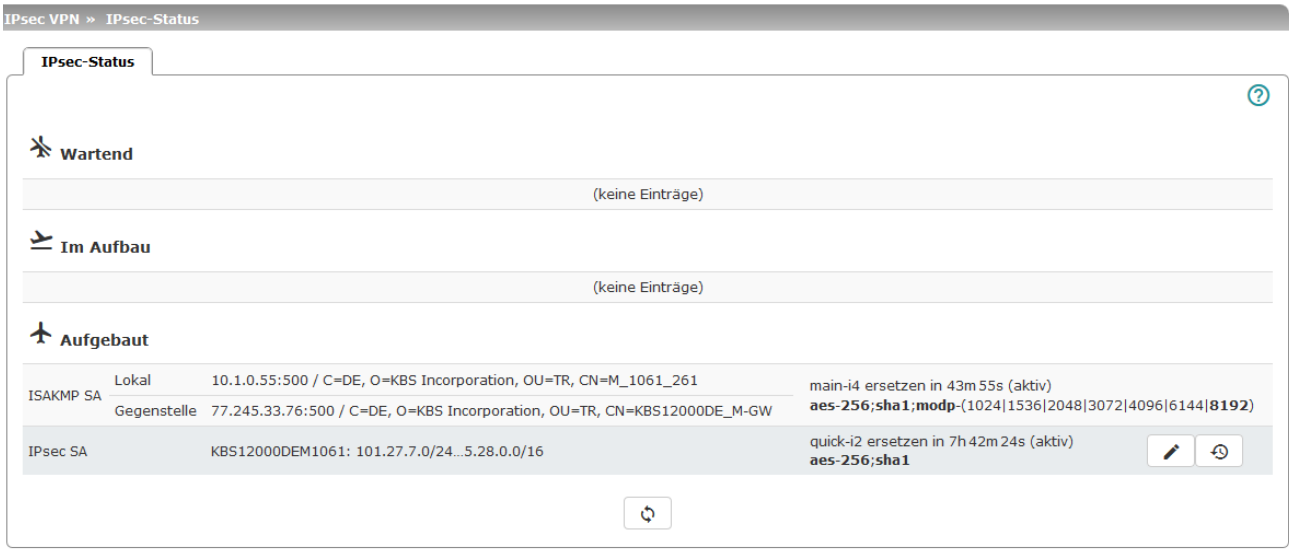
10.3.1 L2TP-Server



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.
	Lokale IP-Adresse für L2TP-Verbindungen	Nach dem obigen Screenshot teilt der mGuard der Gegenstelle mit, er habe die Adresse 10.106.106.1.

IPsec VPN >> L2TP über IPsec >> L2TP-Server		
	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.

10.4 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 auf den aktuellen Stand zu bringen, klicken Sie auf das Icon **Aktualisieren**.

Neustart

Wollen Sie eine Verbindung trennen und dann neu starten, auf die entsprechende **Neustart**-Schaltfläche klicken.

Editieren

Wollen Sie eine Verbindung neu konfigurieren, klicken Sie auf das entsprechende Icon **Zeile bearbeiten**.

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.

11 Menü OpenVPN-Client

Dieses Menü steht nicht auf dem FL MGUARD BLADE-Controller zur Verfügung.

11.1 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.

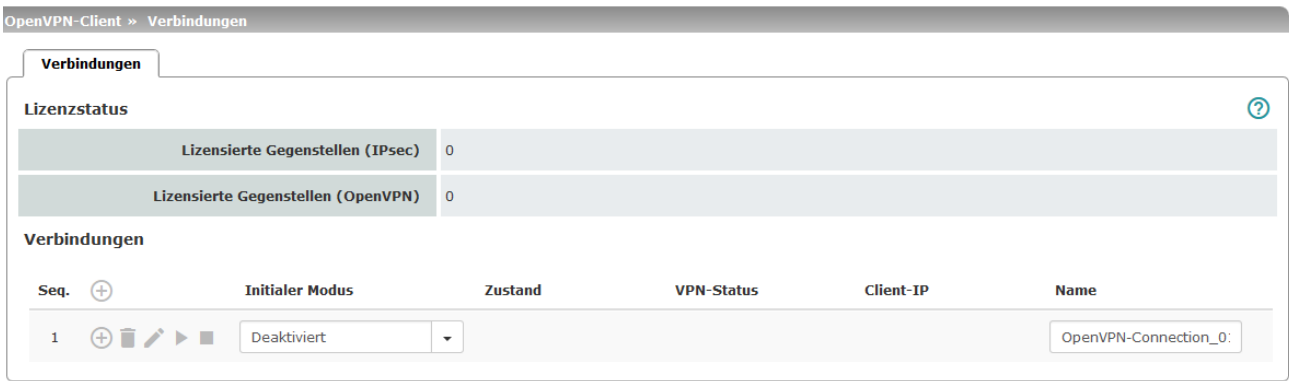
Der OpenVPN-Client unterstützt folgende TLS-Versionen: TLS 1.0, TLS 1.1, TLS 1.2

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 154). 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.

11.1.1 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

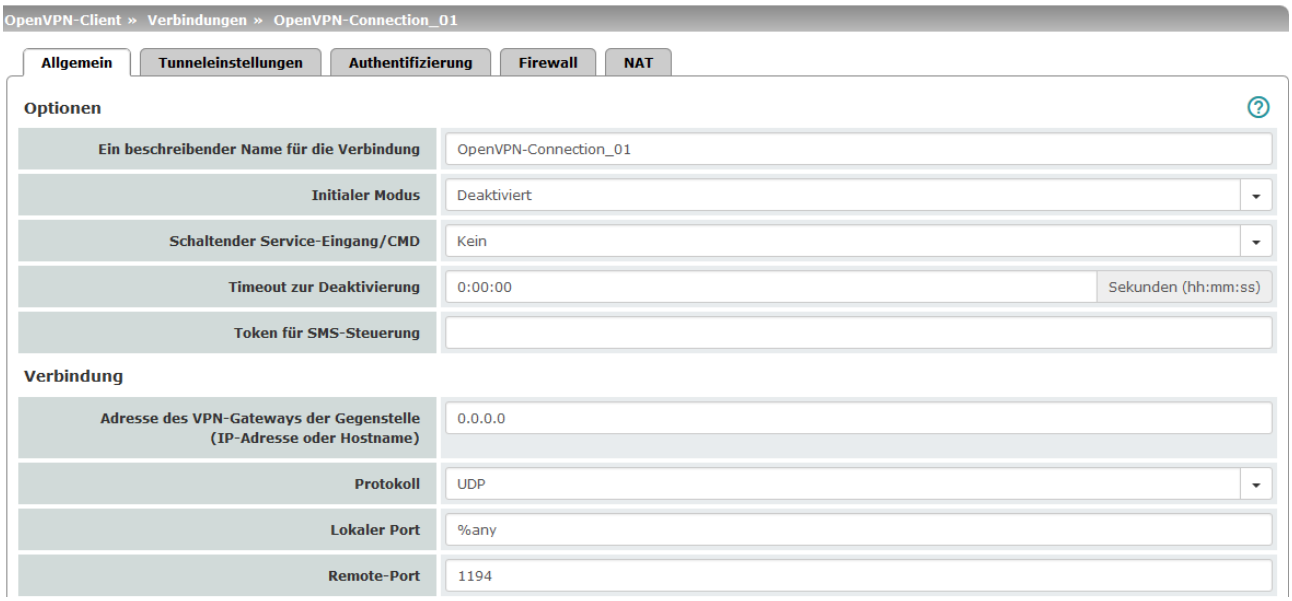
VPN-Verbindung neu definieren

- 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.

11.1.2 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.

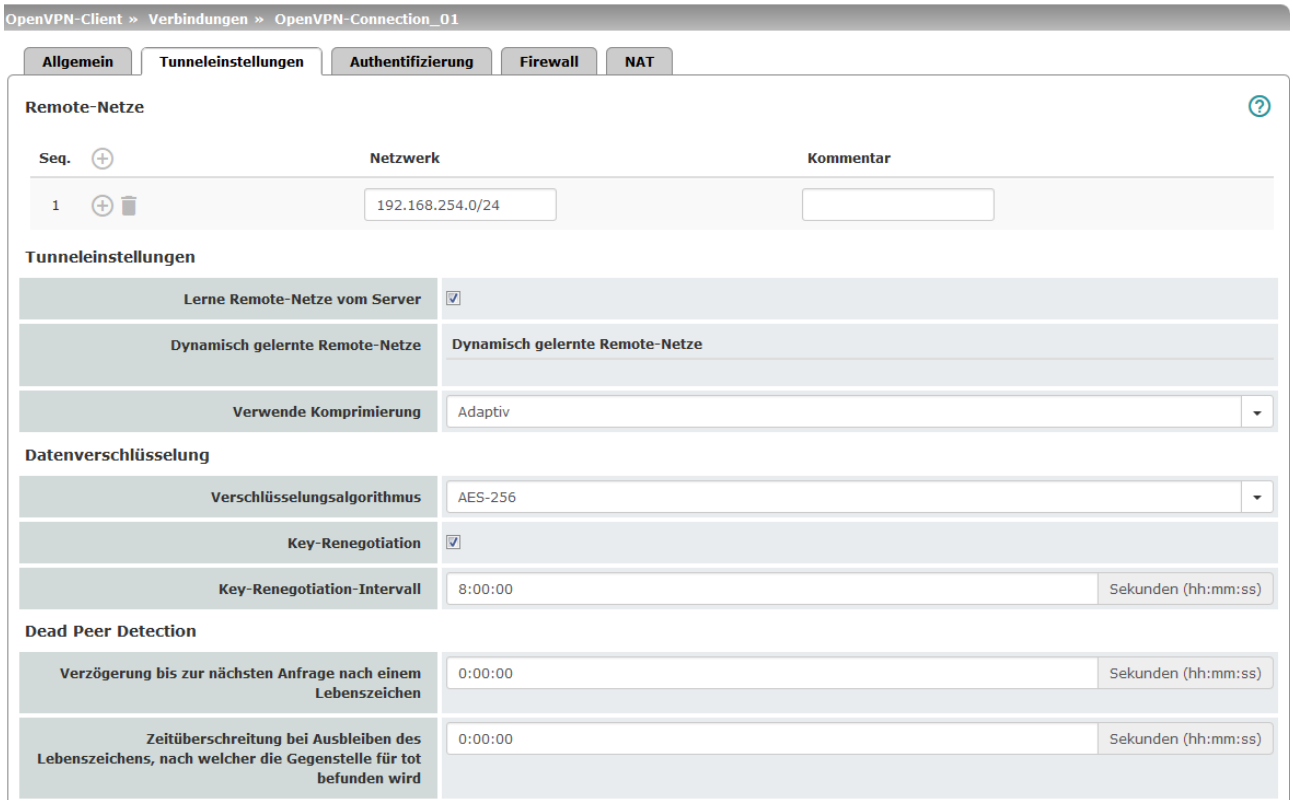
Die Einstellungen „**Gestartet**“ und „**Gestoppt**“ bestimmen den Status der VPN-Verbindung nach einem Neustart/Booten des mGuards (z. B. nach einer Unterbrechung der Stromversorgung).

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 (Nur verfügbar beim TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS4000/RS2000, FL MGUARD RS4004/RS2005, FL MGUARD RS, FL MGUARD GT/GT.)	**Kein / Service-Eingang CMD 1-3** Die VPN-Verbindung kann über einen angeschlossenen Taster/Schalter geschaltet werden. Der Taster/Schalter muss an einen der Servicekontakte (CMD 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 per SMS 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 SMS, 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.
	Token für SMS-Steuerung (Nur verfügbar beim TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G.)	Eingehende SMS können dazu benutzt werden, VPN-Verbindungen zu initiieren (start) oder zu beenden (stop). Die SMS muss das Kommando „*openvpn/start*“ bzw. „*openvpn/stop*“ gefolgt von dem Token enthalten.
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

11.1.3 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**

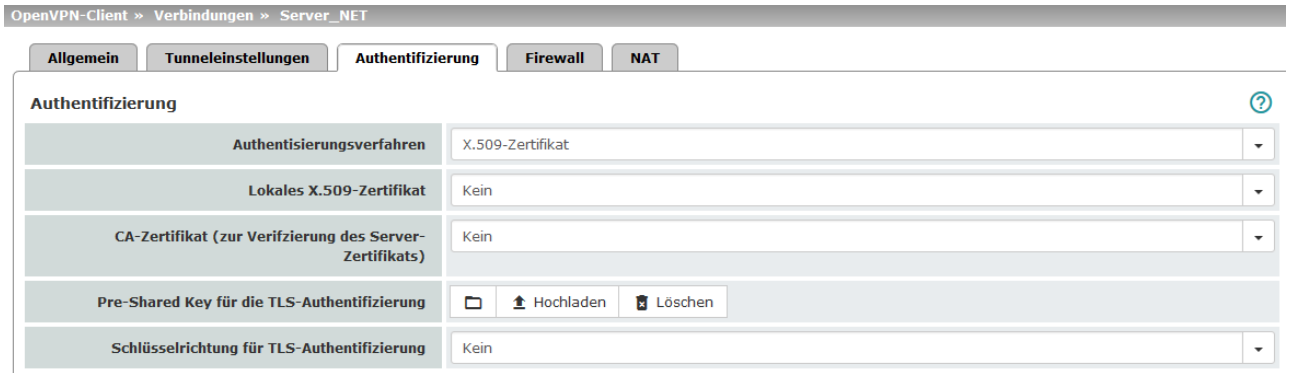
Sie können auswählen, ob eine Komprimierung immer, nie oder adaptiv (je nach Art des Traffics angepasst) angewendet wird.

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**	**Blowfish** / **AES-128** / **AES-192** / **AES-256 (Standard)** Vereinbaren Sie mit dem Administrator der Gegenstelle, welcher Verschlüsselungsalgorithmus verwendet werden soll. **Geänderte werkseitige Voreinstellung in mGuard-Firmwareversion 8.6.0** Aus Sicherheitsgründen wird in der werkseitigen Voreinstellung nicht mehr der häufig verwendete Verschlüsselungsalgorithmus **Blowfish**, sondern der sicherere Algorithmus **AES-256** verwendet. **Verwenden Sie sicherer Algorithmen** Aus Sicherheitsgründen sollte nach Möglichkeit der Verschlüsselungsalgorithmus **AES** verwendet werden (siehe „Verwendung sicherer Verschlüsselungs- und Hash-Algorithmen“ auf Seite 19). 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.
	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)

11.1.4 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 254.

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.

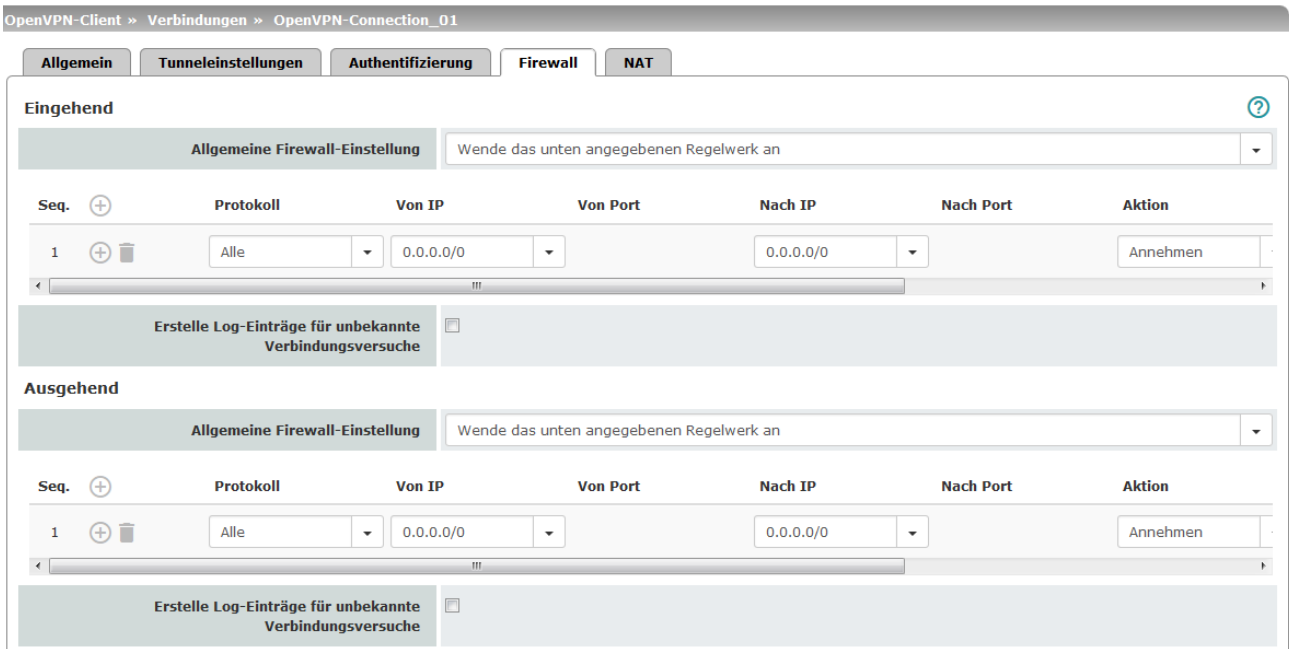
Die Auswahlliste stellt alle CA-Zertifikate zur Wahl, die unter Menüpunkt Authentifizierung >> Zertifikate in den mGuard importiert wurden.

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.

11.1.5 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 271), 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 271, „Netzwerksicherheit >> Paketfilter“ auf Seite 271, „Erweitert“ auf Seite 292).

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 26).

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 289).

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 mGuard-Geräten der RS2000-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.

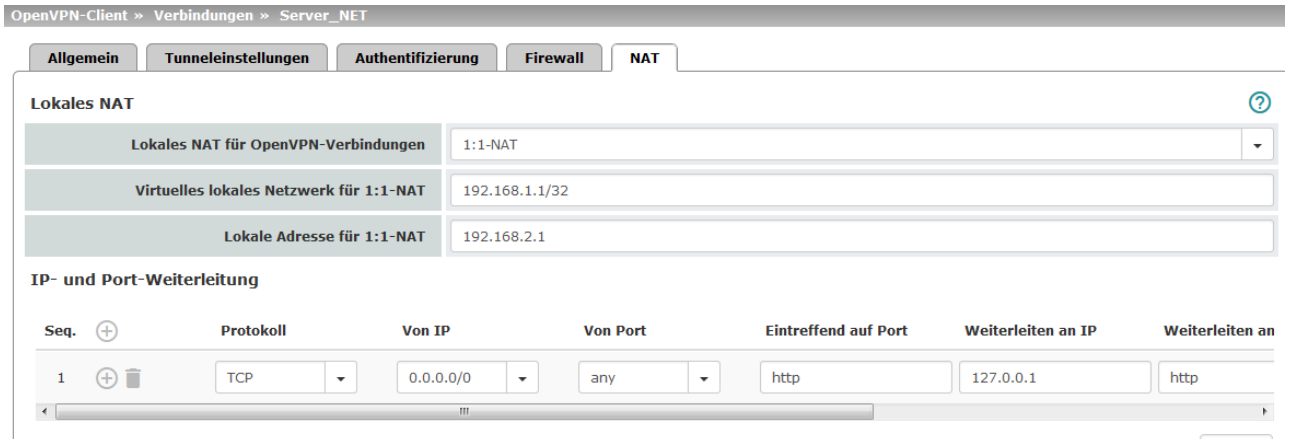
startport:endport (z. B. 110:120) bezeichnet einen Portbereich.

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 289).

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 mGuard-Geräten der RS2000-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 „Modbus TCP“ auf Seite 298).
	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 (werkseitige Voreinstellung).
	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“.	

11.1.6 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 26). Die Maskierung von Remote-Netzen kann unter *Netzwerk >> NAT >> Maskierung* (siehe „Maskierung“ auf Seite 209) 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 26).

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 289).

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 289).

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 (werkseitige Voreinstellung).

12 Menü SEC-Stick

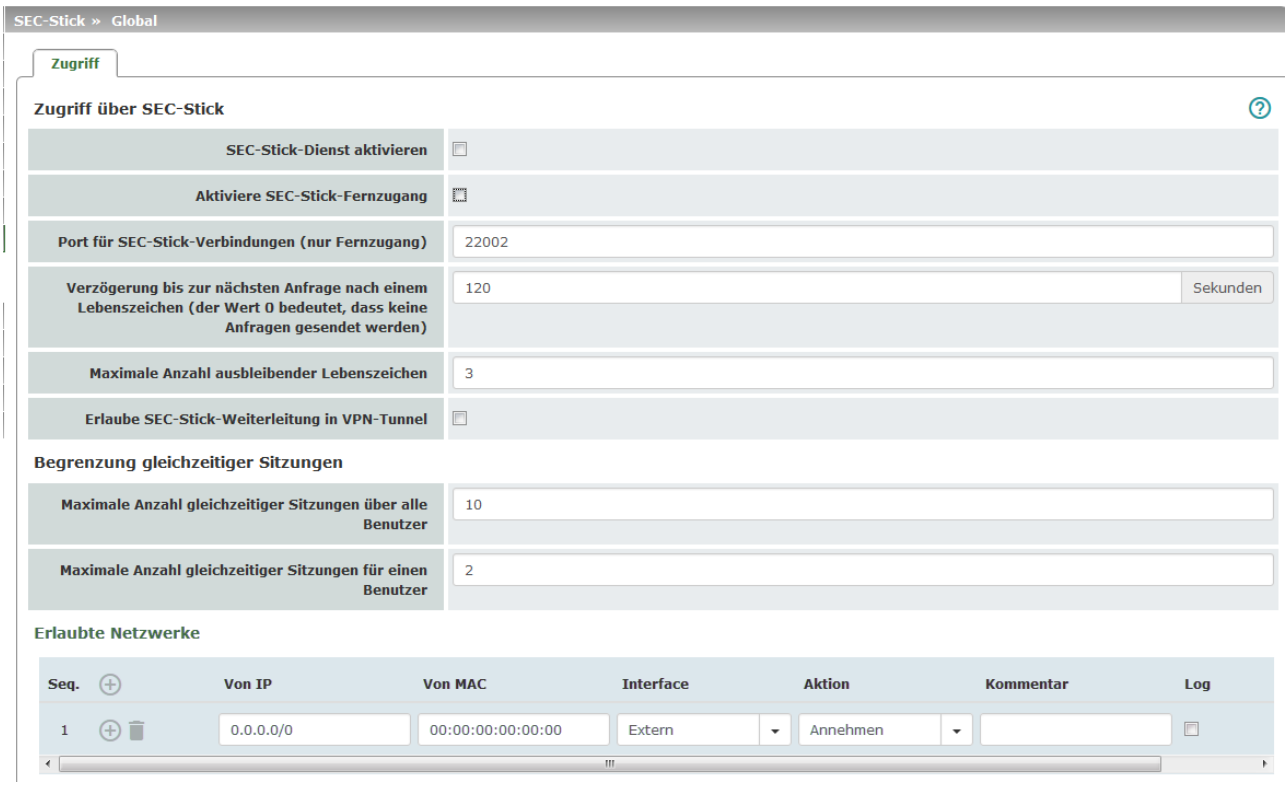
Der mGuard unterstützt die Nutzung eines SEC-Sticks, ein Zugriffsschutz für IT-Systeme. Der SEC-Stick ist ein Produkt der Firma team2work: www.team2work.de.

Der SEC-Stick ist praktisch ein Schlüssel. Der Benutzer steckt ihn in den USB-Port eines Rechners mit Internetanbindung, und kann dann eine verschlüsselte Verbindung zum mGuard aufbauen, um sicher auf definierte Dienste im Netzwerk des Büros oder daheim zuzugreifen. Zum Beispiel kann das Remote Desktop Protokoll innerhalb der verschlüsselten und sicheren SEC-Stick-Verbindung benutzt werden, um den PC im Büro oder zu Hause fernzusteuern als säße man direkt davor.

Damit das funktioniert, ist der Zugang zum Geschäfts-PC durch den mGuard geschützt, und der mGuard muss für den SEC-Stick konfiguriert sein, damit dieser den Zugang öffnen kann. Denn der Benutzer des entfernten Rechners, in den der SEC-Stick eingesteckt ist, authentisiert sich beim mGuard mit den Daten und der Software, die auf seinem SEC-Stick gespeichert sind.

Der SEC-Stick stellt eine SSH-Verbindung zum mGuard her. In diese können weitere Tunnel eingebettet sein, z. B. TCP/IP-Verbindungen.

12.1 Global



SEC-Stick >> Global >> Zugriff

Achten Sie auf Groß- und Kleinschreibung.

Zugriff über SEC-Stick

(Dieser Menüpunkt gehört nicht zum Funktionsumfang von TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005, FL MGUARD RS2000.)

Der Zugriff über SEC-Stick ist eine lizenzpflichtige Funktion. Sie kann nur benutzt werden, wenn die entsprechende Lizenz erworben und installiert ist.

SEC-Stick-Dienst aktivieren	Bei aktivierter Funktion wird festgelegt, dass der an einem entfernten Standort eingesetzte SEC-Stick bzw. dessen Besitzer sich einloggen kann. In diesem Fall muss zusätzlich der SEC-Stick-Fernzugang aktiviert werden (nächster Schalter).
Aktiviere SEC-Stick-Fernzugang	Bei aktivierter Funktion wird der SEC-Stick-Fernzugang aktiviert.
Port für SEC-Stick-Verbindungen (nur Fernzugang)	Standard: 22002 Wird diese Port-Nummer geändert, gilt die geänderte Port-Nummer nur für Zugriffe über das Interface *Extern, Extern 2*, DMZ, GRE oder *VPN*. Für internen Zugriff gilt weiterhin 22002
Verzögerung bis zur Anfrage nach einem Lebenszeichen	Default: 120 Sekunden Einstellbar sind Werte von 0 bis 3600 Sekunden. Positive Werte bedeuten, dass der mGuard innerhalb der verschlüsselten SSH-Verbindung eine Anfrage an die Gegenstelle sendet, ob sie noch erreichbar ist. Die Anfrage wird gesendet, wenn für die angegebene Anzahl von Sekunden keine Aktivität von der Gegenstelle bemerkt wurde (zum Beispiel durch Netzwerkverkehr innerhalb der verschlüsselten Verbindung). Der hier eingetragene Wert bezieht sich auf die Funktionsfähigkeit der verschlüsselten SSH-Verbindung. Solange diese gegeben ist, wird die SSH-Verbindung vom mGuard wegen dieser Einstellungen nicht beendet, selbst wenn der Benutzer während dieser Zeit keine Aktion ausführt. Da die Anzahl der gleichzeitig geöffneten Sitzungen begrenzt ist (siehe *Maximale Zahl gleichzeitiger Sitzungen über alle Benutzer*), ist es wichtig, abgelaufene Sitzungen zu beenden. Deshalb wird ab Version 7.4.0 die Anfrage nach einem Lebenszeichen auf 120 Sekunden voreingestellt. Bei maximal drei Anfragen nach einem Lebenszeichen, wird eine abgelaufende Sitzung nach sechs Minuten entdeckt und entfernt. In vorherigen Versionen war die Voreinstellung „0“. Das bedeutet, dass keine Anfragen nach einem Lebenszeichen gesendet werden. Beachten Sie, dass durch die Lebenszeichen-Anfragen zusätzlicher Traffic erzeugt wird.
Maximale Anzahl ausbleibender Lebenszeichen	Gibt an, wie oft Antworten auf Anfragen nach Lebenszeichen der Gegenstelle ausbleiben dürfen. Wenn z. B. alle 15 Sekunden nach einem Lebenszeichen gefragt werden soll und dieser Wert auf 3 eingestellt ist, dann wird die Verbindung des SEC-Stick-Clients gelöscht, wenn nach circa 45 Sekunden immer noch kein Lebenszeichen gegeben wurde.

SEC-Stick >> Global >> Zugriff [...]

Erlaube SEC-Stick-Weiterleitung in VPN-Tunnel
Ermöglicht die Weiterleitung von SSH-Verbindungen in einen VPN-Tunnel (Hub & Spoke).

Begrenzung gleichzeitiger Sitzungen

Für SEC-Stick-Verbindungen gibt eine Begrenzung der Anzahl von gleichzeitigen Sitzungen. Pro Sitzung wird etwa 0,5 MB Speicherplatz benötigt, um das maximale Sicherheitslevel zu gewährleisten.

Die Einschränkung hat keine Auswirkung auf bereits bestehende Sitzungen, sondern nur auf neu aufgebaute Verbindungen.

Maximale Zahl gleichzeitiger Sitzungen über alle Benutzer
0 bis 2147483647

Gibt die Anzahl der Verbindungen an, die von allen Benutzern gleichzeitig erlaubt sind. Bei "0" ist keine Sitzung erlaubt.

Maximale Zahl gleichzeitiger Sitzungen für einen Benutzer
0 bis 2147483647

Gibt die Anzahl der Verbindungen an, die von einem Benutzer gleichzeitig erlaubt sind. Bei "0" ist keine Sitzung erlaubt.

Erlaubte Netzwerke

Listet die eingerichteten Firewall-Regeln für den SEC-Stick-Fernzugriff auf.

Wenn mehrere Firewall-Regeln gesetzt sind, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Falls in der Regelliste weitere passende Regeln vorhanden sind, werden diese ignoriert.
Die hier angegebenen Regeln treten nur in Kraft, wenn die Funktion **Aktiviere SEC-Stick-Fernzugang** aktiviert wurde. Weil Zugriffe von *Intern* auch möglich sind, wenn diese Funktion deaktiviert ist, tritt für diesen Fall eine Firewall-Regel, die den Zugriff von *Intern* verwehren würde, nicht in Kraft.

Sie können mehrere Regeln festlegen.

Von IP
Geben Sie hier die Adresse des Rechners/Netzes an, von dem der Zugriff 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 26).

Interface
Intern / Extern / Extern 2 / DMZ / VPN / GRE / Einwahl[1]

Gibt an, für welches Interface die Regel gelten soll.

Wenn keine Regeln gesetzt sind oder keine Regel greift, gelten folgende Standardeinstellungen:

- SEC-Stick-Fernzugang ist erlaubt über *Intern, DMZ, VPN* und *Einwahl*.
- Zugriffe über *Extern*, *Extern 2* und *GRE* werden verwehrt.

Legen Sie die Zugriffsmöglichkeiten nach Bedarf fest.

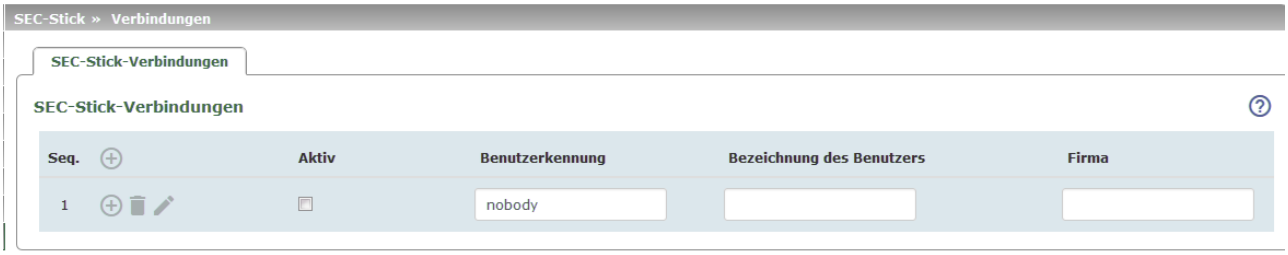
Wenn Sie Zugriffe über *Intern, DMZ, VPN* oder *Einwahl* verwehren wollen, müssen Sie das explizit durch entsprechende Firewall-Regeln bewirken, in der Sie als Aktion z. B. *Verwerfen* festlegen.

SEC-Stick >> Global >> Zugriff [...]

Aktion	**Annehmen** bedeutet, die Datenpakete dürfen passieren. **Abweisen** bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat *Abweisen* dieselbe Wirkung wie *Verwerfen*.) **Verwerfen** bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information über deren Verbleib erhält. **Namen von Regelsätzen**, sofern definiert. Bei Angabe eines Namens für Regelsätze treten die Firewall-Regeln in Kraft, die unter diesem Namen gespeichert sind (siehe Registerkarte Regelsätze). Regelsätze, die IP-Gruppen mit Hostnamen enthalten, sollten aus Sicherheitsgründen nicht in Firewall-Regeln verwendet werden, die als Aktion „Verwerfen“ oder „Abweisen“ ausführen.
Kommentar	Ein frei wählbarer Kommentar für diese Regel.
Log	Für jede einzelne Firewall-Regel können Sie festlegen, ob beim Greifen der Regel – das Ereignis protokolliert werden soll – *Log* auf **Ja** setzen – oder das Ereignis nicht protokolliert werden soll – *Log* auf **Nein** setzen (werkseitige Voreinstellung).

[1] *Extern 2* und *Einwahl* nur bei Geräten mit serieller Schnittstelle (siehe „Netzwerk >> Interfaces“ auf Seite 135).

12.2 Verbindungen



SEC-Stick >> Verbindungen >> SEC-Stick-Verbindungen

SEC-Stick-Verbindungen

Liste der definierten SEC-Stick-Verbindungen.

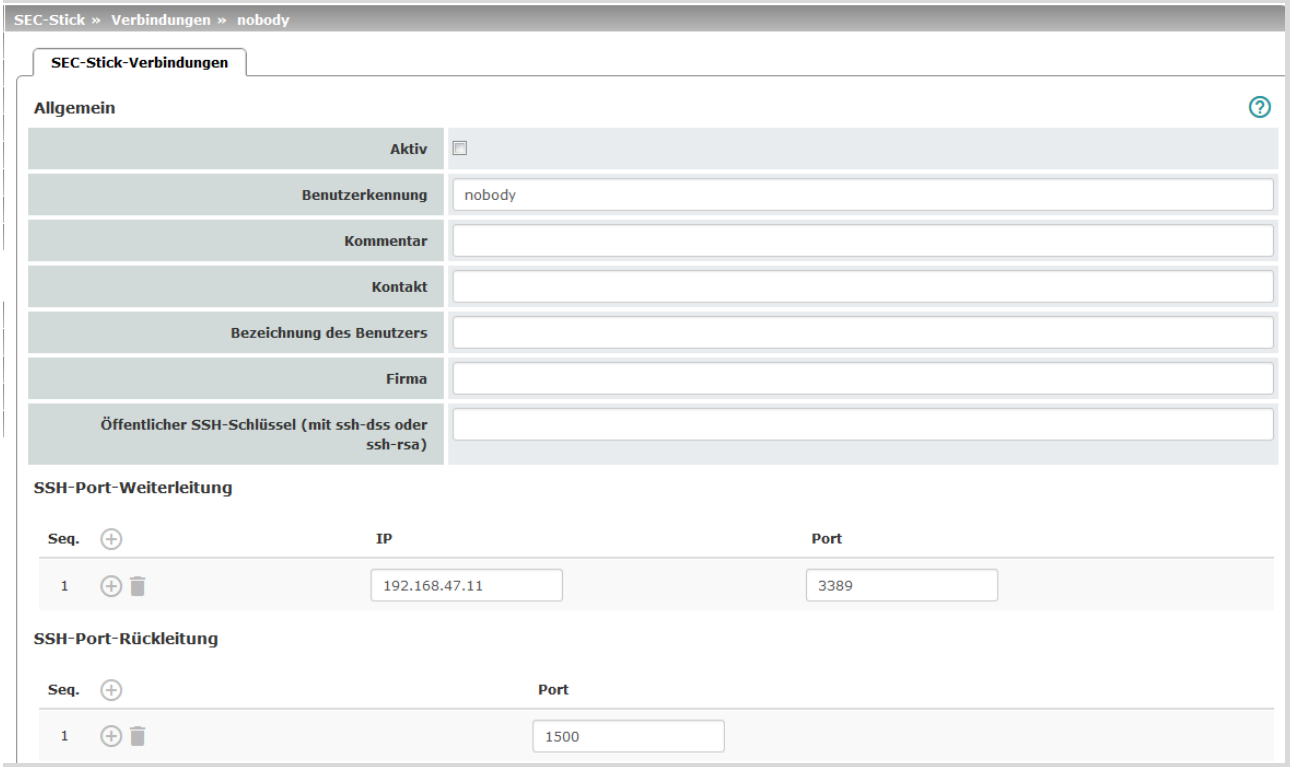
Achten Sie auf Groß- und Kleinschreibung.

Nicht alle Funktionen des SEC-Sticks können über die Web-Benutzeroberfläche des mGuards konfiguriert werden.

Aktiv	Um eine definierte SEC-Stick-Verbindung nutzen zu können, muss der Schalter **Aktiv** auf aktiviert werden.
Benutzerkennung	Für jeden zugriffsberechtigten Inhaber eines SEC-Sticks, muss eine SEC-Stick-Verbindung mit einem eindeutig zugeordneten Benutzernamen definiert werden. Anhand dieses Benutzernamens werden die definierten Verbindungen eindeutig identifiziert.
Bezeichnung des Benutzers	Name der Person.
Firma	Angabe der Firma.

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

SEC-Stick >> Verbindungen >> SEC-Stick-Verbindungen [...]



Allgemein	**Aktiv**	Wie oben
	Benutzerkennung	Wie oben
	Kommentar	Optional: kommentierender Text.
	Kontakt	Optional: kommentierender Text.
	Bezeichnung des Benutzers	Optional: Name der Person. (Wiederholt)
	Firma	Optional: Wie oben
	Öffentlicher SSH-Schlüssel (mit ssh-dss oder ssh-rsa)	Hier muss der öffentliche SSH-Schlüssel, der zum SEC-Stick gehört, im ASCII-Format eingetragen werden. Das geheime Gegenstück ist auf dem SEC-Stick gespeichert.
SSH-Port-Weiterleitung	Liste der erlaubten Zugriffe und SSH-Port-Weiterleitungen bezogen auf den SEC-Stick des entsprechenden Benutzers.	
	IP	IP-Adresse des Rechners, auf den der Zugriff ermöglicht wird.
	Port	Port-Nummer, die beim Zugriff auf den Rechner benutzt werden soll.
SSH-Remote-Port-Weiterleitung	**Port**	Port, der für die SSH-Remote-Port-Weiterleitung verwendet wird.

13 Menü QoS

Dieses Menü steht **nicht** auf dem **FL MGUARD RS2000, TC MGUARD RS2000 3G**, **TC MGUARD RS2000 4G** und **FL MGUARD RS2005** zur Verfügung.

QoS (Quality of Service) bezeichnet die Dienstgüte einzelner Übertragungskanäle in IP-Netzwerken. Dabei geht es um die Zuteilung bestimmter Ressourcen an bestimmte Dienste (Services) bzw. Kommunikationsarten, damit diese reibungslos funktionieren. So muss z. B. für die Übertragung von Audio- oder Videodaten in Realzeit die notwendige Bandbreite bereitgestellt werden, um eine zufriedenstellende Kommunikation zu erreichen, während ein eventuell langsamerer Datentransfer per FTP oder E-Mail unkritisch für den gewünschten Gesamterfolg (Übertragung der gewünschten Datei oder E-Mail) ist.

13.1 Ingress-Filter

Ein Ingress-Filter bewirkt, dass bestimmte Datenpakete vor Eintreten in den Verarbeitungsmechanismus des mGuards ausgefiltert und verworfen werden, so dass eine Verarbeitung nicht stattfindet. Der mGuard kann Ingress-Filter benutzen, um die vorhandene Verarbeitungsleistung nach Möglichkeit nicht mit solchen Datenpaketen zu belasten, die im Netzwerk nicht gebraucht werden. Das hat den Effekt, dass die anderen, d. h. die gebrauchten Datenpakete schneller verarbeitet werden.

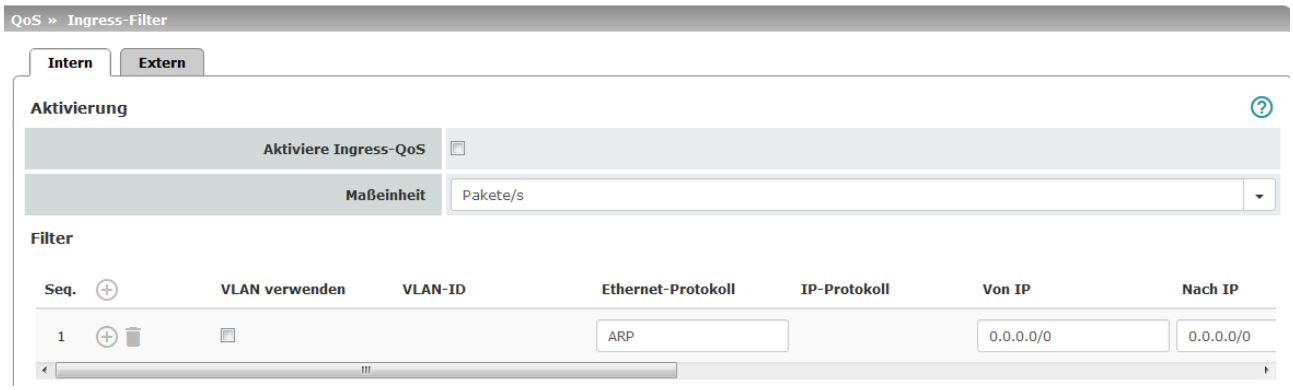
Durch geeignete Filterregeln kann z. B. sichergestellt werden, dass der administrative Zugang zum mGuard immer mit hoher Wahrscheinlichkeit erfolgen kann.

Die Paketverarbeitung auf dem mGuard ist im Wesentlichen durch das Handling des einzelnen Datenpakets geprägt, so dass die Verarbeitungsleistung nicht von der Bandbreite sondern von der Zahl der zu verarbeitenden Pakete abhängt.

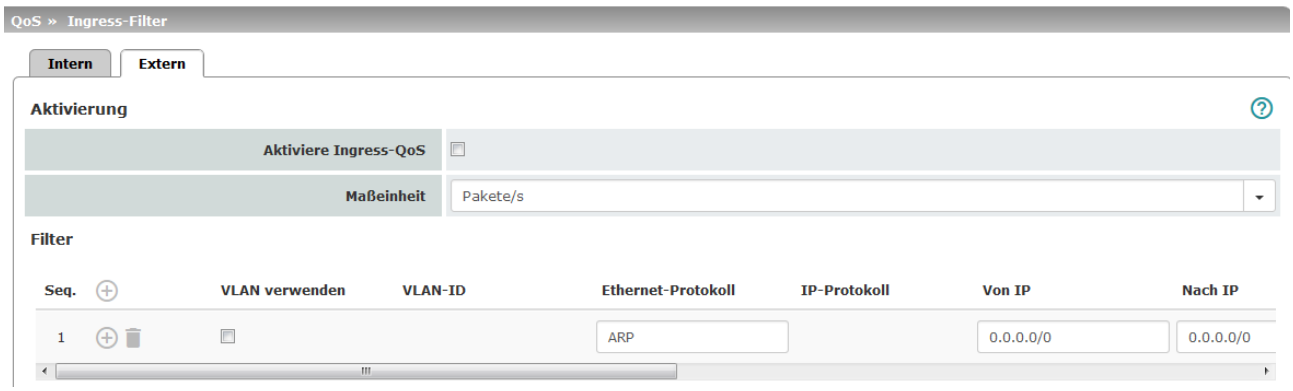
Gefiltert wird ausschließlich nach Merkmalen, die jedes einzelne Datenpaket aufweist oder aufweisen kann: die im Header angegebene IP-Adresse von Sender und Empfänger, das angegebene Ethernet-Protokoll, das angegebene IP-Protokoll, der angegebene TOS/DSCP-Wert und/oder die VLAN-ID, wenn VLANs eingerichtet sind. Da durch die gesetzten Filterregeln bei jedem einzelnen Datenpaket geprüft wird, ob es unter die Filterregeln fällt, sollte die Liste der Filterregeln kurz sein. Sonst könnte die Zeit, die zum Ausfiltern gebraucht wird, länger sein, als der durch das Ausfiltern erzielte Zeitgewinn.

Es ist zu beachten, dass nicht alle angebbaren Filterkriterien sinnvoll kombiniert werden können. Zum Beispiel macht es keinen Sinn, bei Angabe des Ethernet-Protokolls ARP im selben Regelsatz zusätzlich ein IP-Protokoll anzugeben. Oder bei Angabe des Ethernet-Protokolls IPX (hexadezimal anzugeben) die IP-Adressen von Sender oder Empfänger vorzugeben.

13.1.1 Intern / Extern



Intern: Einstellung für Ingress Filter an der LAN-Schnittstelle



Extern: Einstellung für Ingress Filter an der WAN-Schnittstelle

Menü QoS >> Ingress-Filter >> Intern/Extern		
Aktivierung	**Aktiviere Ingress-QoS**	**Deaktiviert** (Standard): Das Feature ist ausgeschaltet. Falls Filterregeln definiert sind, werden sie ignoriert. **Aktiviert**: Das Feature ist eingeschaltet. Datenpakete dürfen nur dann passieren und werden der Weitervermittlung und -verarbeitung des mGuards zugeführt, wenn sie den nachfolgend festgelegten Filterregeln entsprechen. Filter können für den LAN-Port (Registerkarte **Intern**) und den WAN-Port (Registerkarte **Extern**) gesetzt werden.
	Maßeinheit	**kbit/s / Pakete/s** Legt fest, in welcher Maßeinheit die weiter unten unter **Garantiert** und **Obergrenze** anzugebenden Zahlenwerte zu verstehen sind.

Menü QoS >> Ingress-Filter >> Intern/Extern [...]		
Filter	**VLAN verwenden**	Ist ein VLAN eingerichtet, kann die betreffende VLAN-ID angegeben werden, damit die betreffenden Datenpakete passieren dürfen. **VLAN verwenden** darf nicht aktiviert werden, wenn VLAN bereits in den Interface-Einstellungen des entsprechenden Interfaces (Intern oder Extern) aktiviert ist.
	VLAN-ID (Wenn **VLAN verwenden** aktiviert ist)	Legt fest, dass die Datenpakete des VLANs, das diese VLAN-ID hat, passieren dürfen.
	Ethernet-Protokoll	Legt fest, dass nur Datenpakete des angegebenen Ethernet-Protokolls passieren dürfen. Mögliche Einträge: **ARP**, **IPV4**, **%any**. Andere Angaben müssen hexadezimal (bis zu 4 Ziffern) eingetragen werden. (Bei den Angaben handelt es sich um die Kennung des betreffenden Protokolls, die im Ethernet-Header steht. Das kann in den Veröffentlichungen des betreffenden Standards nachgeschlagen werden.)
	IP-Protokoll	**Alle / TCP / UDP / ICMP / ESP** Legt fest, dass nur Datenpakete des ausgewählten IP-Protokolls passieren dürfen. Mit **Alle** findet keine Filterung nach IP-Protokoll statt.
	Von IP	Legt fest, dass nur Datenpakete passieren dürfen, die von der angegebenen IP-Adresse kommen. Die Angabe **0.0.0.0/0** steht für alle Adressen, d. h. in diesem Fall findet keine Filterung nach IP-Adresse des Absenders statt. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise (siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 26).
	Nach IP	Legt fest, dass nur solche Datenpakete passieren dürfen, die zur angegebenen IP-Adresse weitergeleitet werden sollen. Angabe entsprechend wie oben unter *Von IP*. Die Angabe **0.0.0.0/0** steht für alle Adressen, d. h. in diesem Fall findet keine Filterung nach IP-Adresse des Absenders statt.
	Aktueller TOS/DSCP-Wert	Jedes Datenpaket enthält ein TOS bzw. DSCP-Feld. (TOS steht für Type Of Service, DSCP für Differentiated Services Code Point.) Hier wird angegeben, zu welcher Art von Traffic das Datenpaket gehört. So wird z. B. ein IP-Telefon in dieses Feld der von ihm ausgehenden Datenpakete etwas anderes hineinschreiben als ein FTP-Programm. Wenn Sie hier einen Wert auswählen, dürfen nur die Datenpakete passieren, die in ihrem TOS-bzw. DSCP-Feld diesen Wert haben. Mit **Alle** findet keine Filterung nach TOS/DSCP Wert statt.

Menü QoS >> Ingress-Filter >> Intern/Extern [...]		
	Garantiert	Die anzugebende Zahl legt fest, wie viele Datenpakete/s bzw. kbit/s - je nach eingestellter **Maßeinheit** (s. o.) - auf jeden Fall passieren dürfen. Das gilt für den Datenstrom, der den links angegebenen Kriterien dieses Regelsatzes entspricht, also passieren darf. Liefert dieser Datenstrom mehr Datenpakete pro Sekunde, dann **darf** der mGuard bei Kapazitätsengpässen die überzählige Anzahl an Datenpaketen verwerfen.
	Obergrenze	Die anzugebende Zahl legt fest, wie viele Datenpakete/s bzw. kbit/s - je nach eingestellter **Maßeinheit** (s. o.) - maximal passieren dürfen. Das gilt für den Datenstrom, der den links angegebenen Kriterien dieses Regelsatzes entspricht, also passieren darf. Liefert dieser Datenstrom mehr Datenpakete pro Sekunde, dann verwirft der mGuard die überzählige Anzahl an Datenpaketen.
	Kommentar	Optional: kommentierender Text.

13.2 Egress-Queues

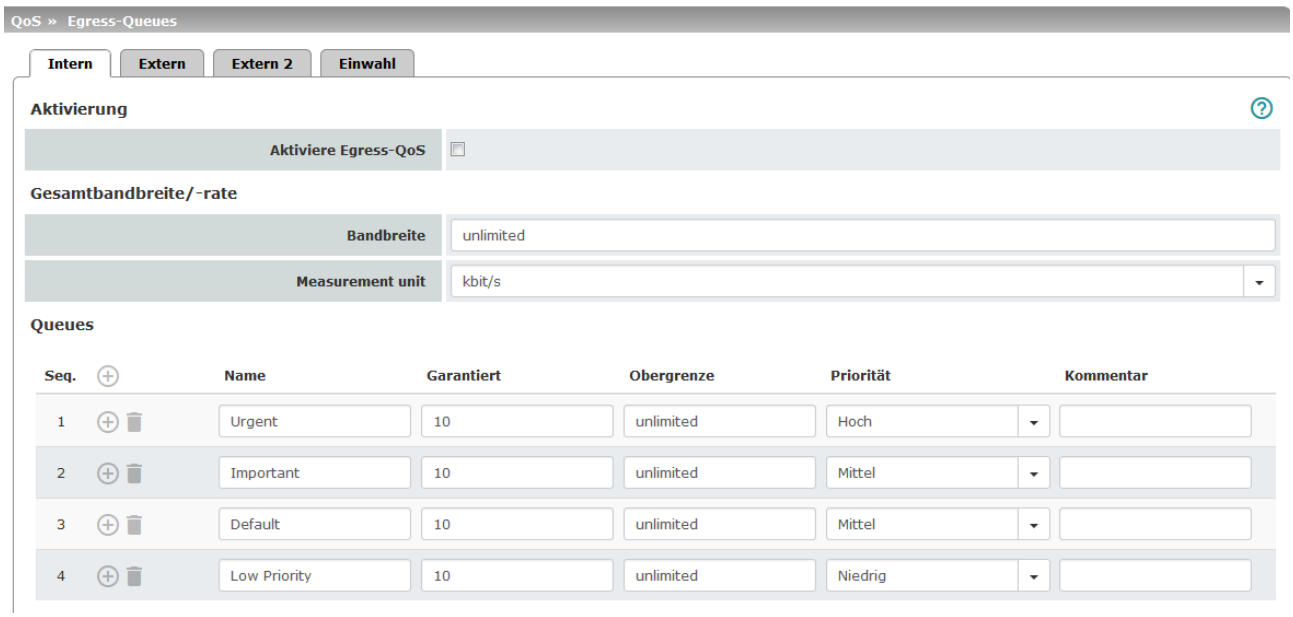
Den Diensten werden entsprechende Prioritätsstufen zugeordnet. Bei Verbindungsengpässen werden dann je nach zugeordneter Prioritätsstufe die ausgehenden Datenpakete in Egress-Queues (= Warteschlangen für anstehende Pakete) gestellt, die mit entsprechender Priorität abgearbeitet werden. Die Zuordnung von Prioritätsstufe und Bandbreite sollte im Idealfall so erfolgen, dass für Datenpakete von in Realzeit zu vollziehenden Übertragungen immer genügend Bandbreite zur Verfügung steht, während Pakete von anderen wie z. B. FTP-Downloads im Ernstfall vorübergehend auf Warten gesetzt werden.

Die Hauptanwendung von Egress-QoS ist die optimale Ausnutzung der zur Verfügung stehenden Bandbreite am jeweiligen Anschluss. In einigen Fällen kann auch eine Begrenzung der Paketrate nützlich sein, z. B. um einen langsamen Rechner im geschützten Netz vor Überlast zu schützen.

Die Funktion *Egress-Queues* kann für alle Schnittstellen eingesetzt werden. Bis zur mGuard-Firmwareversion 8.6.x kann die Funktion ebenfalls für VPN-Verbindungen verwendet werden. In Firmwareversion 8.7.0 ist eine Verwendung in VPN-Verbindungen nicht mehr möglich.

13.2.1 Intern / Extern / Extern 2 / Einwahl

Intern: Einstellung für Egress-Queues an der LAN-Schnittstelle



Extern / Extern 2 / Einwahl:

Die Registerkarten für Egress-Queues an der WAN-Schnittstelle (Extern), der sekundären externen Schnittstelle (Extern 2) und für Pakete für ppp-Wählverbindung (Einwahl) bieten die gleichen Einstellmöglichkeiten wie die Registerkarte für die LAN-Schnittstelle (Intern).

In allen Fällen beziehen sich die Einstellungen auf die Daten, die von der jeweiligen Schnittstelle gesehen vom mGuard nach außen ins Netz gehen.

Menü QoS >> Egress-Queues >> Intern / Extern / Extern 2 / Einwahl		
Aktivierung	**Aktiviere Egress-QoS**	**Deaktiviert** (Standard): Das Feature ist ausgeschaltet. **Aktiviert**: Das Feature ist eingeschaltet. Empfiehlt sich dann, wenn die Schnittstelle an ein Netz mit geringer Bandbreite angeschlossen ist, so dass eine Beeinflussung der Bandbreitenzuordnung zugunsten besonders wichtiger Daten gewünscht wird.
Gesamtbandbreite/-rate	**Bandbreite**	Bandbreite, die insgesamt maximal physikalisch zur Verfügung steht - anzugeben in kBit/s oder Pakete/s (s. u. **Maßeinheit**). Die hier angegebene Gesamtbandbreite sollte etwas geringer angegeben werden als tatsächlich vorhanden, damit die Priorisierung optimal arbeitet. Damit wird verhindert, dass Puffer von weitervermittelnden Geräten überlaufen können und dadurch einen unerwünschten Effekt erzeugen.
	Maßeinheit	**kbit/s / Pakete/s** Legt fest, in welcher Maßeinheit die Zahlenwerte zu verstehen sind (s. o. **Bandbreite**).
Queues	**Name**	Sie können die voreingestellten Namen für die Egress-Queues übernehmen oder andere vergeben. Die Namen legen nicht die Prioritätsstufe fest.
	Garantiert	Bandbreite, die der betreffenden Queue auf jeden Fall zur Verfügung stehen soll. Je nachdem, ob oben unter **Maßeinheit** diese in **kbit/s** oder in **Pakete/s** angegeben ist, verwenden Sie auch hier die selbe Maßeinheit, ohne diese explizit anzugeben. Die Summe aller garantierten Bandbreiten muss in Bezug zur Gesamtbandbreite kleiner oder gleich sein.
	Obergrenze	Bandbreite, die der betreffenden Queue vom System maximal zur Verfügung gestellt werden darf. Je nachdem, ob oben unter **Maßeinheit** diese in **kbit/s** oder in **Pakete/s** angegeben ist, verwenden Sie auch hier die selbe Maßeinheit, ohne diese explizit anzugeben. Der Wert muss größer sein als die garantierte Bandbreite oder dieser gleich sein. Es kann auch der Wert **unlimited** angegeben werden, der keine weitere Beschränkung bewirkt.
	Priorität	**Niedrig / Mittel / Hoch** Legt fest, mit welcher Priorität die betreffende Warteschlange, sofern vorhanden, abgearbeitet werden muss, falls die zur Verfügung stehende Gesamtbandbreite aktuell nicht ausgeschöpft ist.
	Kommentar	Optional: kommentierender Text.

13.3 Egress-Queues (VPN)

Die Funktion *Egress-Queues (VPN)* steht in mGuard-Firmwareversion **8.7.0** nicht mehr zur Verfügung.

Ein Update auf mGuard-Firmwareversion 8.7.0 von einer älteren Firmwareversion mit aktivierter *Egress-Queues (VPN)*-Funktion ist nicht möglich.

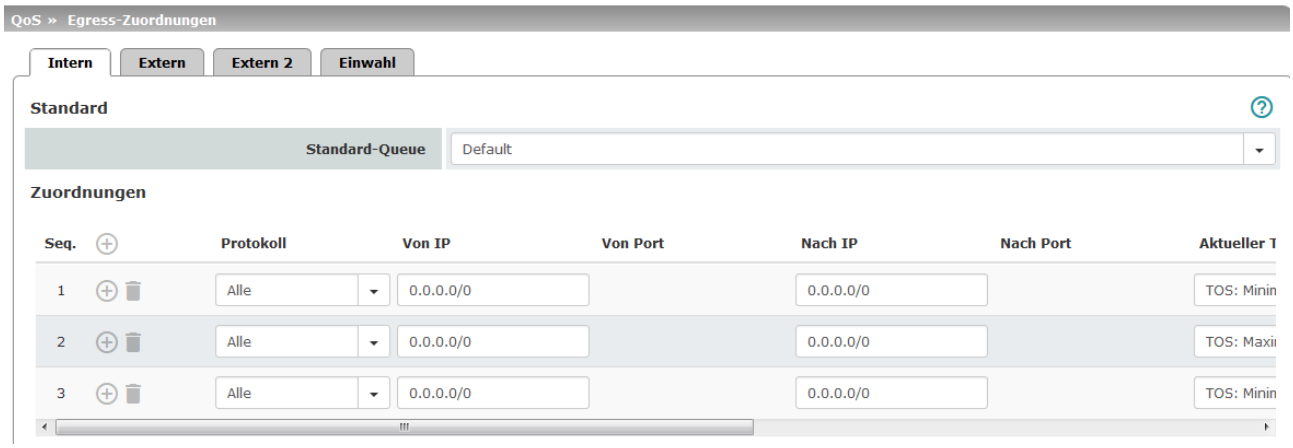
13.4 Egress-Zuordnungen

Welche Daten werden den definierten Egress-Queues (= Warteschlangen) (s. o.) zugeordnet, damit sie mit der Priorität übertragen werden, die der jeweiligen Queue zugeteilt ist?

Die Zuordnungen können bezüglich aller Schnittstellen sowie für VPN-Verbindungen separat festgelegt werden.

13.4.1 Intern / Extern / Extern2 / Einwahl

Intern: Einstellung für Egress-Queue-Zuordnungen



Extern / Extern 2 / Einwahl:

Die Registerkarten für Egress-Queue-Zuordnungen an der WAN-Schnittstelle (Extern), der sekundären externen Schnittstelle (Extern 2) und für Pakete für ppp-Wählverbindung (Einwahl) bieten die gleichen Einstellmöglichkeiten wie die Registerkarte für die LAN-Schnittstelle (Intern).

Menü QoS >> Egress-Zuordnungen >> Intern / Extern / Extern 2 / Einwahl		
Standard	**Standard-Queue**	*Name der Egress-Queues* (benutzerdefiniert) Angezeigt werden die Namen der Queues, wie sie unter *Egress-Queues* auf den Registerkarten *Intern* / *Extern* / *VPN via Extern* angezeigt oder festgelegt sind. Standardmäßig sind das folgende Namen: Default / Urgent / Important / Low Priority Traffic, der **nicht** nachfolgend unter *Zuordnungen* einer bestimmten Egress-Queue zugeordnet wird, bleibt der *Standard-Queue* zugeordnet. Über diese Auswahlliste legen Sie fest, welche Egress-Queue als *Standard-Queue* gelten soll.
Zuordnungen	Die Zuordnung bestimmten Daten-Traffics zu einer Egress-Queue erfolgt über eine Liste von Kriterien. Treffen die Kriterien einer Zeile auf ein Datenpaket zu, wird es in die dort benannte Egress-Queue eingeordnet. **Beispiel**: Sie haben für zu übertragende Audio-Daten unter Egress-Queues (siehe Seite 409) unter dem Namen *Urgent* eine Queue mit garantierter Bandbreite und Priorität definiert. Dann legen Sie hier fest, nach welchen Regeln Audio-Daten erkannt werden, und dass diese Daten zur Queue *Urgent* gehören sollen.	

Menü QoS >> Egress-Zuordnungen >> Intern / Extern / Extern 2 / Einwahl		
	Protokoll	**Alle / TCP / UDP / ICMP /ESP** Protokoll(e), auf das/die sich die Zuordnung bezieht.
	Von IP	IP-Adresse des Netzes/Geräts, von wo die Daten kommen. **0.0.0.0/0** bedeutet alle IP-Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise (siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 26). Den Traffic von dieser Quelle ordnen Sie weiter hinten in dieser Zeile der Queue zu, die Sie unter *Queue-Name* auswählen.
	Von Port (Nur bei den Protokollen TCP und UDP)	Benutzter Port bei der Quelle, von wo die Daten kommen. **any** bezeichnet jeden beliebigen Port. **startport:endport** (z. B. 110:120) bezeichnet einen Portbereich. Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben: (z. B. 110 für pop3 oder pop3 für 110).
	Nach IP	IP-Adresse des Netzes/Geräts, wohin die Daten gehen. Angabe entsprechend wie oben unter *Von IP*.
	Nach Port (Nur bei den Protokollen TCP und UDP)	Benutzter Port bei der Quelle, wohin die Daten gehen. Angabe entsprechend wie oben unter *Von Port.*
	Aktueller TOS/DSCP-Wert	Jedes Datenpaket enthält ein TOS bzw. DSCP Feld. (TOS steht für Type Of Service, DSCP für Differentiated Services Code Point.) Hier wird angegeben, zu welcher Art von Traffic das Datenpaket gehört. So wird z. B. ein IP-Telefon in dieses Feld der von ihm ausgehenden Datenpakete etwas anderes hineinschreiben als ein FTP-Programm, das Datenpakete auf einen Server hochlädt. Wenn Sie hier einen Wert auswählen, werden nur die Datenpakete genommen, die in ihrem TOS-bzw. DSCP-Feld diesen Wert haben, um sie - je nach Eintrag im Feld **Neuer TOS/DSCP-Wert** - auf einen anderen Wert zu setzen.

Menü QoS >> Egress-Zuordnungen >> Intern / Extern / Extern 2 / Einwahl		
	Neuer TOS/DSCP-Wert	Wenn Sie den TOS/DSCP-Wert der Datenpakete ändern wollen, die anhand der gegebenen Regeln selektiert sind, wählen Sie hier aus, was ins TOS- bzw. DSCP-Feld geschrieben werden soll. Weitere Erläuterungen zu **Aktueller TOS/DSCP-Wert** und **Neuer TOS/DSCP-Wert** finden Sie in folgenden RFC-Dokumenten – RFC 3260 „New Terminology and Clarifications for Diffserv“ – RFC 3168 „The Addition of Explicit Congestion Notification (ECN) to IP“ – RFC 2474 „Definition of the Differentiated Services Field (DS Field)“ – RFC 1349 „Type of Service in the Internet Protocol Suite“
	Queue-Name	Name der Egress-Queue, welcher der Traffic zugeordnet werden soll.
	Kommentar	Optional: kommentierender Text.

13.5 Egress-Zuordnungen (VPN)

Die Funktion *Egress-Zuordnungen (VPN)* steht ab mGuard-Firmwareversion **8.7.0** nicht mehr zur Verfügung.

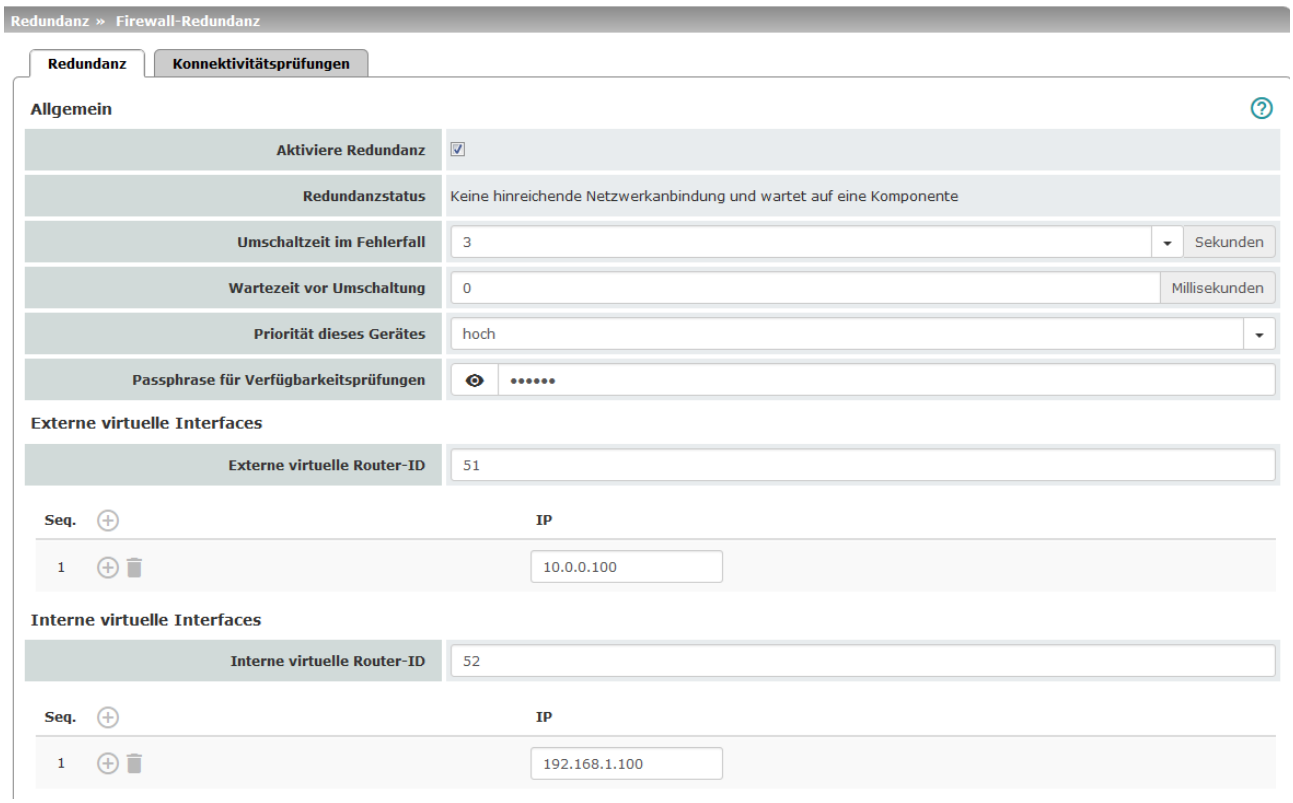
Ein Update auf mGuard-Firmwareversion 8.7.0 von einer älteren Firmwareversion mit aktivierter *Egress-Zuordnungen (VPN)*-Funktion ist nicht möglich.

14 Menü Redundanz

Eine ausführliche Darstellung zum Thema Redundanz finden Sie in Kapitel 17, „Redundanz“.

Um die Redundanzfunktion zu nutzen, müssen beide mGuards die gleiche Firmware haben.

Bei aktivierter Redundanzfunktion kann VLAN im Stealth-Modus nicht verwendet werden.



14.1 Redundanz >> Firewall-Redundanz

Dieses Menü steht **nicht** auf dem **FL MGUARD RS2000, FL MGUARD RS2005, TC MGUARD RS2000 3G** und **TC MGUARD RS2000 4G** zur Verfügung.

14.1.1 Redundanz

Redundanz >> Firewall-Redundanz >> Redundanz		
	Aktiviere Redundanz	**Deaktiviert** (Standard): Die Firewall-Redundanz ist ausgeschaltet. **Aktiviert**: Die Firewall-Redundanz ist aktiviert. Sie können diese Funktion nur aktivieren, wenn ein passender Lizenzschlüssel installiert ist. Wenn Sie gleichzeitig die VPN-Redundanz aktivieren wollen, gelten weitere Bedingungen, siehe „VPN-Redundanz“ auf Seite 455.
Allgemein	**Redundanzstatus**	Zeigt den aktuellen Status an.
	Umschaltzeit im Fehlerfall	Zeit, die im Fehlerfall maximal verstreichen darf, bevor auf den anderen mGuard gewechselt wird.
	Wartezeit vor Umschaltung	**0 ... 10 000 Millisekunden, Standard: 0** Zeitdauer, in der ein Fehler vom Redundanz-System ignoriert wird. Ein Fehler wird von der Konnektivitäts- und der Verfügbarkeitsprüfung ignoriert, bis er länger als die hier eingestellte Zeit andauert.
	Priorität dieses Gerätes	**hoch/niedrig** Definiert die Priorität, die mit den Anwesenheitsnachrichten (CARP) verbunden ist. Setzen Sie bei dem mGuard, der aktiv sein soll, die Priorität **hoch**. Der mGuard in Bereitschaft bekommt die Priorität **niedrig**. Beide mGuards eines Redundanzpaares dürfen entweder eine unterschiedliche Priorität oder die Priorität **hoch** haben. Setzen Sie niemals **beide** mGuards eines Redundanzpaares auf die Priorität **niedrig**.

Redundanz >> Firewall-Redundanz >> Redundanz

Passphrase für Verfügbarkeitstest

Bei einem mGuard, der Teil eines Redundanzpaares ist, wird kontinuierlich geprüft, ob ein aktiver mGuard vorhanden ist und ob dieser aktiv bleiben soll. Dafür wird eine Variante des CARP (Common Address Redundancy Protocol) verwendet.

CARP nutzt die SHA-1 HMAC-Verschlüsselung in Verbindung mit einem Passwort. Dieses Passwort muss für beide mGuards gleich eingestellt sein. Er wird niemals im Klartext übertragen, sondern zur Verschlüsselung genutzt.

Das Passwort ist wichtig für die Sicherheit, da der mGuard an dieser Stelle angreifbar ist. Wir empfehlen, ein Passwort mit mindestens 20 Zeichen und vielen Sonderzeichen zu verwenden (druckbare UTF-8-Zeichen). Es muss regelmäßig erneuert werden.

Gehen Sie so vor, um das Passwort zu ändern:

Stellen Sie das neue Passwort an beiden mGuards ein. Die Reihenfolge ist egal, aber das Passwort muss bei beiden gleich sein. Wenn Sie versehentlich ein abweichendes Passwort eingetragen haben, folgen Sie den Anweisungen unter „Vorgehensweise bei einem falschem Passwort“ auf Seite 420.

Sobald ein Redundanzpaar ein neues Passwort erhalten hat, handelt es selbst aus, wann es unterbrechungsfrei zum neuen Passwort wechseln kann.

Wenn ein mGuard während des Passwort-Wechsels ausfällt, gibt es diese Fälle:

- Die Passwort-Erneuerung wurde an allen mGuards gestartet und dann unterbrochen, z. B. durch einen Netzwerk-Fehler. Dieser Fall wird automatisch behoben.
- Die Passwort-Erneuerung wurde an allen mGuards gestartet. Aber dann fällt ein mGuard aus und muss ausgetauscht werden.
- Die Passwort-Erneuerung wurde gestartet, aber nicht an allen mGuards, weil diese ausgefallen sind. Sobald ein fehlerhafter mGuard wieder online ist, muss die Passwort-Erneuerung gestartet werden. Bei einem ausgetauschten mGuard muss dieser zunächst mit dem alten Passwort konfiguriert werden, bevor er angeschlossen wird.

Redundanz >> Firewall-Redundanz >> Redundanz

Vorgehensweise bei einem falschem Passwort

Wenn Sie versehentlich bei einem mGuard 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 den mGuard, bei dem das falsche Passwort eingetragen wurde, noch einmal mit dem alten Passwort.
- Warten Sie bis der mGuard anzeigt, dass das alte Passwort benutzt wird.
- Tragen Sie dann das richtige Passwort ein.

Wenn Sie das alte Passwort nicht mehr kennen, gehen Sie so vor:

- Prüfen Sie, ob Sie das alte Passwort beim anderen mGuard auslesen können.
- Wenn der andere mGuard ausgeschaltet ist oder fehlt, dann können Sie bei dem aktiven mGuard, dem sie versehentlich das falsche Passwort eingestellt haben, einfach das korrekte neue Passwort eintragen. Sorgen Sie dafür, dass der andere mGuard das gleiche Passwort erhält, bevor er wieder in Betrieb geht.
- Wenn der andere mGuard das neue Passwort bereits verwendet, dann müssen Sie sicherstellen, dass der mGuard mit dem falschen Passwort nicht aktiv ist oder wird, z. B. durch das Herausziehen des Kabels an der LAN- oder WAN-Schnittstelle.

  Bei einem Fernzugriff können Sie für die Konnektivitätsprüfung ein Ziel eintragen, das nicht reagieren wird. Bevor Sie einen solchen Fehler provozieren, prüfen Sie, dass bei keinem der mGuards ein Fehler bei der Redundanz vorliegt. Ein mGuard muss aktiv und der andere in Bereitschaft sein. Gegebenenfalls müssen Sie angezeigte Fehler beheben und dann erst die Methode verwenden. Dann führen Sie die folgenden Schritte aus:
  - Ersetzen Sie das falsche Passwort durch ein anderes.
  - Geben Sie dieses Passwort auch beim aktiven mGuard ein.
  - Nehmen Sie den nicht aktiven mGuard wieder in Betrieb. Stecken Sie zum Beispiel das Ethernet-Kabel wieder ein oder stellen Sie die alten Einstellungen für die Konnektivitätsprüfung wieder her.

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 mGuards gleich sein. Sie ist notwendig, um das Redundanzpaar von anderen Redundanzpaaren zu unterscheiden, die über ihr externes Interface mit demselben Ethernet-Segment verbunden sind.

Beachten Sie dabei, dass CARP dasselbe Protokoll und denselben Port wie 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	Default: 10.0.0.100 Nur im Netzwerk-Modus Router IP-Adressen, die von beiden mGuards als virtuelle IP-Adresse des externen Interfaces geteilt wird. Diese IP-Adressen müssen für beide mGuards gleich sein. Diese Adressen werden als Gateway für explizite statische Routen von Geräten genutzt, die sich im selben Ethernet-Segment wie das externe Netzwerk-Interface des mGuards befinden. Der aktive mGuard kann auf dieser IP-Adresse ICMP-Anfragen erhalten. Er reagiert auf diese ICMP-Anfragen wie es im Menü unter *Netzwerksicherheit >> Paketfilter >> Erweitert* eingestellt ist. Für die virtuelle IP-Adressen werden keine Netzwerkmaske oder VLAN ID eingerichtet, da diese Attribute von der realen externen IP-Adresse bestimmt werden. Zu jeder virtuellen IP-Adresse muss eine reale IP-Adresse konfiguriert sein, in deren IP-Netz die virtuelle Adresse passt. Der mGuard überträgt die Netzwerkmaske und die VLAN-Einstellung von der realen externen IP-Adresse auf die entsprechende virtuelle IP-Adresse. Die übernommenen VLAN-Einstellungen bestimmen, ob Standard-MTU-Einstellungen oder VLAN-MTU-Einstellungen für die virtuelle IP-Adresse genutzt werden. Wenn keine reale IP-Adresse und Netzwerkmaske vorhanden sind, kann die Firewall-Redundanz nicht richtig arbeiten.
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 mGuards gleich eingestellt sein. Sie ist notwendig, um das Redundanzpaares von anderen Ethernet-Teilnehmern zu unterscheiden, die über ihr externes/internes Interface mit demselben Ethernet-Segment verbunden sind. Beachten Sie dabei, dass CARP dasselbe Protokoll und denselben Port wie VRRR (Virtuell Router Redundancy Protokoll) nutzt. Die hier eingestellte ID muss sich unterscheiden von den IDs der Geräte, die VRRR oder CARP nutzen und sich im selben Ethernet-Segment befinden.

Redundanz >> Firewall-Redundanz >> Redundanz

Interne virtuelle IP-Adressen

Wie unter *Externe virtuelle IP-Adressen* beschrieben, aber mit zwei Ausnahmen

Unter **Interne virtuelle IP-Adresse** werden IP-Adressen definiert für Geräte, die zum internen Ethernet-Segment gehören. Diese Geräte müssen die IP-Adresse als ihr Standard-Gateway nutzen. Sie können diese Adresse als DNS- oder NTP-Server nutzen, wenn der mGuard als Server für die Protokolle konfiguiert ist.

Zu jeder virtuellen IP-Adresse muss eine reale IP-Adresse konfiguriert sein, in deren IP-Netz die virtuelle Adresse passt.

Die Reaktion auf ICMP-Anfragen bei internen virtuellen IP-Adressen ist unabhängig von den Einstellungen unter *Netzwerksicherheit >> Paketfilter >> Erweitert.*

Verschlüsselter Zustandsabgleich

(Nicht mehr verfügbar)

Ab mGuard Firmwareversion 8.8.0 ist ein verschlüsselter Zustandsabgleich nicht mehr möglich.

Ein Update auf Firmware-Version 8.8.0 ist nur möglich, wenn die Funktion zuvor deaktiviert wurde.

Interface für den Zustandsabgleich

(Nur bei mGuard centerport (Innominate), FL MGUARD CENTERPORT)

Interface, das zum Zustandsabgleich verwendet wird

Internes Interface/Dediziertes Interface

Der *mGuard centerport (Innominate), FL MGUARD CENTERPORT* unterstützt ein **dediziertes Interface**. Das ist eine reservierte direkte Ethernet-Schnittstelle oder ein dediziertes LAN-Segment, über das der Zustandsabgleich gesendet wird.

Das Redundanzpaar kann über ein zusätzliches dediziertes Ethernet-Interface verbunden sein oder über einen dazwischen geschalteten Switch.

Bei **Dediziertes Interface** wird an dem dritten Ethernet-Interface ebenfalls auf Anwesenheitsnachrichten (CARP) gelauscht. Wenn der mGuard aktiv ist, werden auch Anwesenheitsnachrichten (CARP) gesendet.

Für dieses Interface wird aber kein zusätzliches Routing unterstützt.

Aus Sicherheitsgründen werden Frames, die an dieser Schnittstelle empfangen werden, nicht weitergeleitet.

Über das SNMP kann der Verbindungsstatus des dritten Ethernet-Interface abgefragt werden.

Redundanz >> Firewall-Redundanz >> Redundanz		
	IP des dedizierten Interfaces (Nur wenn **Dediziertes Interface** ausgewählt ist)	**IP** IP-Adresse, die der *mGuard centerport (Innominate), FL MGUARD CENTERPORT* an seinem dritten Netzwerk-Interface für den Zustandsabgleich mit dem anderen mGuard nutzt. Default: 192.168.68.29 **Netzmaske** Netzwerkmaske, die der *mGuard centerport (Innominate), FL MGUARD CENTERPORT* an seinem dritten Netzwerk-Interface für den Zustandsabgleich mit dem anderen mGuard nutzt. Default: 255.255.255.0 **Verwendete VLAN** Bei **Ja** wird eine VLAN-ID für das dritte Netzwerk-Interface genutzt. **VLAN-ID** 1, 2, 3, ... 4094 (Standard: 1) VLAN-ID, wenn diese Einstellung aktiviert ist.
	Unterlasse die Verfügbarkeitsprüfung der externen Schnittstelle (Nur wenn **Dediziertes Interface** ausgewählt ist)	Bei **aktivierter Funktion** werden an dem externen Interface keine Anwesenheitsnachrichten (CARP) gesendet und empfangen. Das macht für einige Szenarien Sinn, um Angreifer von außen abzuwehren.

14.1.2 Konnektivitätsprüfung

Bei der Konnektivitätsprüfung können Ziele für das interne und externe Interface konfiguriert werden. Es ist wichtig, dass diese Ziele tatsächlich an dem angegebenen Interface angeschlossen sind. Ein ICMP-Echo-Reply kann nicht von einem externen Interface empfangen werden, wenn das zugehörige Ziel am internen Interface angeschlossen ist (und umgekehrt). Bei einem Wechsel der statischen Routen kann es leicht passieren, dass die Ziele nicht entsprechend überprüft werden.

Redundanz >> Firewall-Redundanz >> Konnektivitätsprüfung		
Externes Interface	**Art der Prüfung**	Legt fest, ob und wie bei dem externen Interface eine Konnektivitätsprüfung durchgeführt wird. 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.
	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.

Redundanz >> Firewall-Redundanz >> Konnektivitätsprüfung		
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. Betroffen sind: TC MGUARD RS4000/RS2000 4G, TC MGUARD RS4000/RS2000 3G und FL MGUARD RS4004/RS2005. 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).
	Status der Konnektivitätsprüfung des internen Interface	Zeigt den Status der Konnektivitätsprüfung an.

Redundanz >> Firewall-Redundanz >> Konnektivitätsprüfung	
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

14.2 Ring-/Netzkopplung

Die Funktion Ring-/Netzkopplung wird **nicht** unterstützt vom *mGuard centerport (Innominate)*.

Ring-/Netzkopplung mit Einschränkung:

– mGuard delta (Innominate): hier lässt sich die interne Seite (Switch-Ports) nicht abschalten

– FL MGUARD PCI 533/266: hier lässt sich im Treibermodus die interne Netzwerkschnittstelle nicht abschalten (wohl aber im Power-over-PCI-Modus).

14.2.1 Ring-/Netzkopplung

Redundanz >> Firewall-Redundanz >> Ring-/Netzkopplung		
Settings	**Aktiviere Ring-/Netzkopplung/Dual Homing**	Bei Aktivierung wird im Stealth-Modus der Status der Ethernetverbindung von einen Port auf den anderen übertragen, wodurch sich Unterbrechungen im Netzwerk leicht zurückverfolgen lassen.
	Redundanzport	**Intern / Extern** **Intern**: Wenn die Verbindung am LAN-Port wegfällt/kommt, wird auch der WAN-Port ausgeschaltet/eingeschaltet. **Extern**: Wenn die Verbindung am WAN-Port wegfällt/kommt, wird auch der LAN-Port ausgeschaltet/eingeschaltet.

15 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 431).

15.1 Logging >> Einstellungen

15.1.1 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	**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

Logging >> Einstellungen [...]

Achten Sie auf Groß- und Kleinschreibung.

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 354), gilt Folgendes:

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

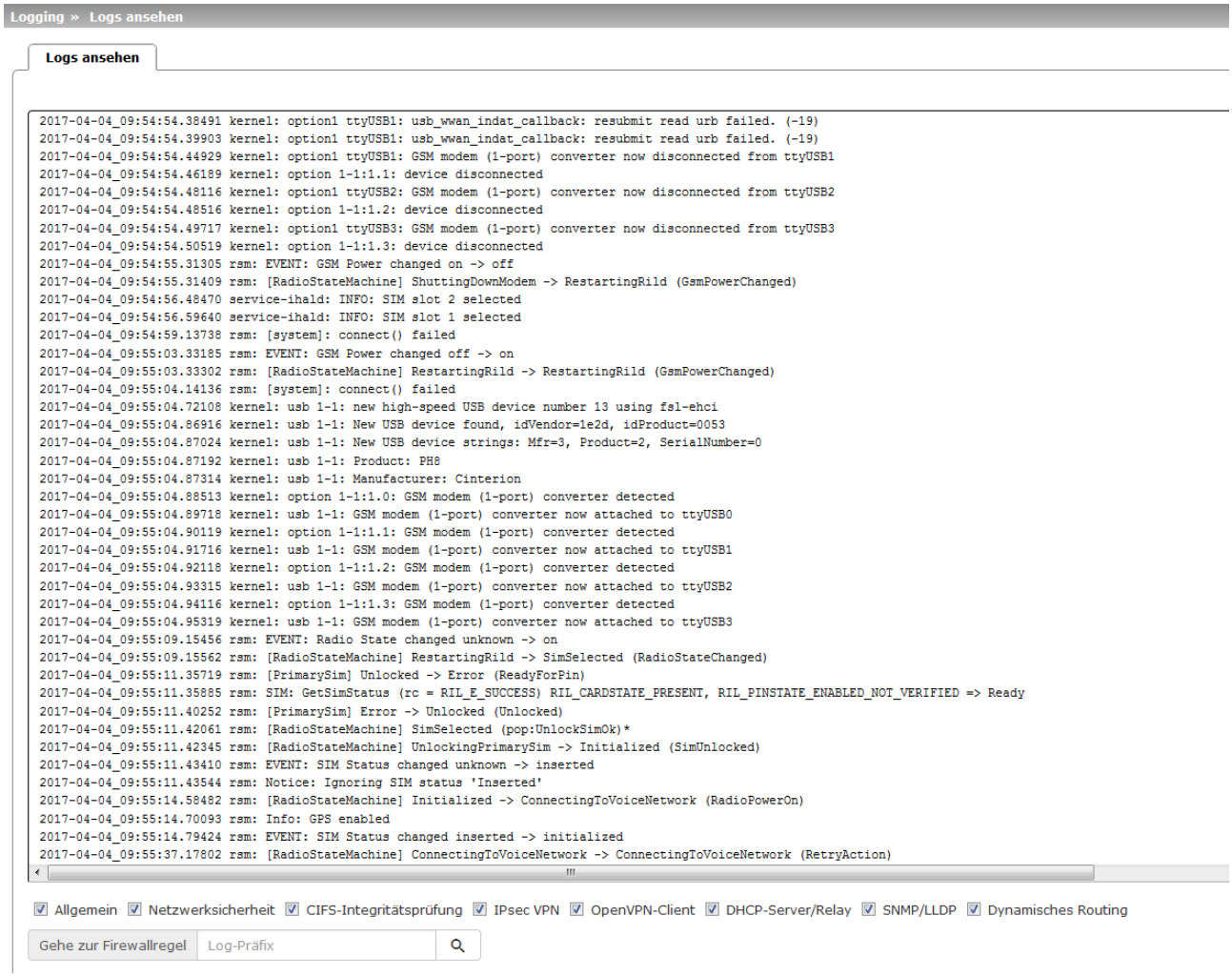
– Wenn dabei die Option IPsec VPN >> Verbindungen >> Editieren >> Allgemein, **Gegenstelle** auf **1:1-NAT** gestellt (siehe Seite 355), gilt Folgendes:

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

Ausführliches Logging

Ausführliches Modem-Logging	Nur verfügbar, wenn ein internes oder externes Modem vorhanden und eingeschaltet ist. – Internes Modem: TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS mit internem Analog-Modem oder ISDN-Modem – Externes Modem: FL MGUARD RS4000/RS2000, TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS4004/RS2005, mGuard centerport (Innominate), FL MGUARD CENTERPORT, FL MGUARD RS, FL MGUARD BLADE, mGuard delta (Innominate), FL MGUARD DELTA Ausführliches Logging
Ausführliches Mobilfunk-Logging	Nur verfügbar beim TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G Ausführliches Logging

15.2 Logging >> Logs ansehen



Je nachdem, welche Funktionen des mGuards aktiv gewesen sind, werden unterhalb der Log-Einträge entsprechende Kontrollkästchen zum Filtern der Einträge nach Kategorien angezeigt.

Damit eine oder mehrerer Kategorien angezeigt werden, aktivieren Sie das/die Kontrollkästchen der gewünschten Kategorie(n). Die Logeinträge 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 erfolgten.

Tabelle 15-1 Log-Einträge einsehen

mGuard	UDP	Web-Oberfläche (Web UI)
/var/log/cifsscand	socklog	CIFS-Integritätsprüfung
/var/log/dhclient	Nein	Allgemein
/var/log/dhcp-ext	Nein	DHCP Server/Relay
/var/log/dhcp-int	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/gsm	Nein	Allgemein
/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/login	Nein	Nein
/var/log/maid	Nein	Nein
/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

Tabelle 15-1 Log-Einträge einsehen

mGuard	UDP	Web-Oberfläche (Web UI)
/var/log/snmp	Nein	SNMP/LLDP
/var/log/tinydns	Nein	Allgemein
/var/log/userfwd	socklog	Netzwerksicherheit

15.2.1 Kategorien der Log-Einträge

Logging >> Logs ansehen >> Kategorien	
Allgemein	Log-Einträge, die den anderen Kategorien nicht zugeordnet werden können.
Netzwerksicherheit	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*** – 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***

Logging >> Logs ansehen >> Kategorien

– Firewall-Regeln für serielle Schnittstelle:
  Menü Netzwerk >> Interfaces >> Einwahl
  Eingangsregeln: Log-ID: ***fw-serial-incoming***
  Ausgangsregeln: Log-ID: ***fw-serial-outgoing***

Suche nach Firewall-Regel auf Grundlage eines Netzwerksicherheits-Logs

Ab mGuard-Firmwareversion 8.6.0 sind Firewall-Log-Einträge 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.

Bei der Verwendung von mGuard-Firmwareversionen < 8.6.0 gehen Sie wie folgt vor:

Ist das Kontrollkästchen **Netzwerksicherheit** aktiviert, sodass die betreffenden Log-Einträge angezeigt werden, wird unterhalb der Schaltfläche *Aktualisiere Logs* das Suchfeld **Gehe zur Firewallregel** angezeigt.

Gehen Sie wie folgt vor, wenn Sie die Firewall-Regel ausfindig machen wollen, auf die sich ein Log-Eintrag der Kategorie *Netzwerksicherheit* bezieht und die zum entsprechenden Ereignis geführt hat:

1. Beim betreffenden Log-Eintrag die Passage markieren, die die Log-ID und Nummer enthält, z. B.: **fw-https-access-1-1ec2c133-dca1-1231-bfa5-000cbe01010a**

2. Diese Passage über die Zwischenablage ins Feld **Gehe zur Firewallregel** kopieren.
3. Auf die Schaltfläche **Suchen** klicken.

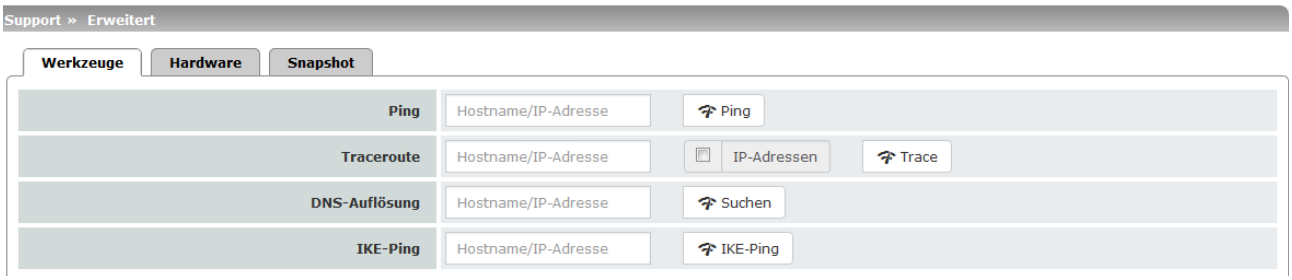
Es wird die Konfigurationsseite mit der Firewall-Regel angezeigt, auf die sich der Log-Eintrag bezieht.

Logging >> Logs ansehen >> Kategorien	
FL MGUARD BLADE	Auf dem FL MGUARD BLADE-Controller werden, neben Fehlermeldungen, die folgenden Meldungen ausgegeben: (Die mit < und > umklammerten Bereiche sind in den Log-Einträgen durch die jeweiligen Daten ersetzt.) **Allgemeine Meldungen:** blade daemon "<version>" starting ... Blade[<bladenr>] online Blade[<bladenr>] is mute Blade[<bladenr>] not running Reading timestamp from blade[<bladenr>] **Beim Aktivieren eines Konfigurationsprofils auf einem Blade:** Push configuration to blade[<bladenr>] reconfiguration of blade[<bladenr>] returned <returncode> blade[<bladenr>] # <text> **Beim Holen eines Konfigurationsprofils vom Blade:** Pull configuration from blade[<bladenr>] Pull configuration from blade[<bladenr>] returned <returncode>
CIFS-Integritätsprüfung	In diesem Log werden Meldungen über die Integritätsprüfung von Netzwerklaufwerken angezeigt. Zusätzlich sind Meldungen sichtbar, die beim Anbinden der Netzlaufwerke entstehen und die für die Integritätsprüfung benötigt werden.
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-Client	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.

16 Menü Support

16.1 Support >> Erweitert

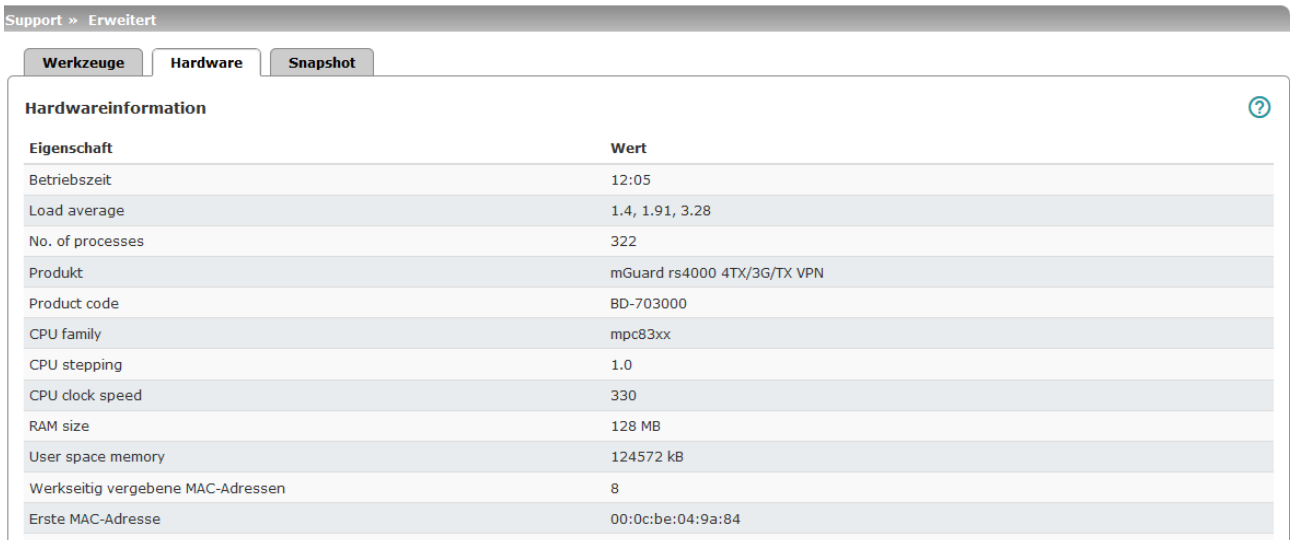
16.1.1 Werkzeuge



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.
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.

16.1.2 Hardware

Diese Seite listet verschiedene Hardware-Eigenschaften des mGuards auf.



Eigenschaft	Wert
Betriebszeit	12:05
Load average	1.4, 1.91, 3.28
No. of processes	322
Produkt	mGuard rs4000 4TX/3G/TX VPN
Product code	BD-703000
CPU family	mpc83xx
CPU stepping	1.0
CPU clock speed	330
RAM size	128 MB
User space memory	124572 kB
Werkseitig vergebene MAC-Adressen	8
Erste MAC-Adresse	00:0c:be:04:9a:84

MAC-Adressen

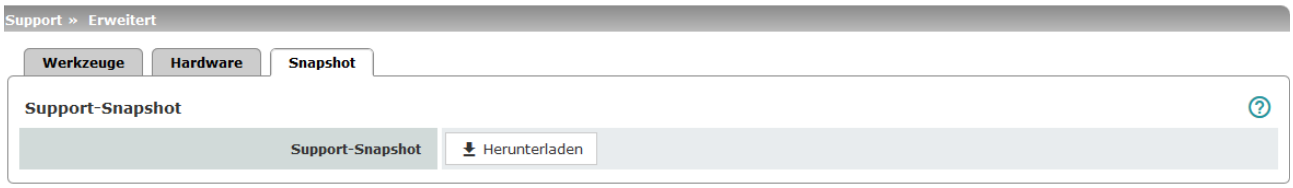
Die angegebene „Erste MAC-Adresse“ ist die MAC-Adresse des WAN-Interface. Die weiteren MAC-Adressen (LAN-DMZ [optional]) lassen sich wie folgt berechnen:

– **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 6 erhöht (**WAN + 6**).

Beispiel:

– WAN: 00:a0:45:eb:28:9d (Erste MAC-Adresse)
– LAN: 00:a0:45:eb:28:9e
– DMZ: 00:a0:45:eb:28:a3

16.1.3 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.

17 Redundanz

Die Firewall- und die VPN-Redundanz stehen **nicht** auf dem **FL MGUARD RS2000, FL MGUARD RS2005**, **TC MGUARD RS2000 3G** und **TC MGUARD RS2000 4G** zur Verfügung.

Es gibt verschiedene Möglichkeiten mit dem mGuard Fehler so zu kompensieren, dass eine bestehende Verbindung nicht unterbrochen wird.

- **Firewall-Redundanz:** Sie können zwei baugleiche mGuards zu einem Redundanzpaar zusammenzufassen, bei dem im Fehlerfall der eine die Funktion des anderen übernimmt.
- **VPN-Redundanz**: Basis hierfür ist eine bestehende Firewall-Redundanz. Zusätzlich dazu werden die VPN-Verbindungen so ausgelegt, das mindestens ein mGuard eines Redunanzpaares die VPN-Verbindungen betreibt.
- **Ring-/Netzkopplung:** Bei der Ring-/Netzkopplung wird ein anderer Ansatz gewählt. Hier werden Teile eines Netzes redundant ausgelegt. Im Fehlerfall wird dann der alternative Weg gewählt.

17.1 Firewall-Redundanz

Mit Hilfe der Firewall-Redundanz ist es möglich, zwei baugleiche mGuards zu einem Redundanzpaar (einem virtuellen Router) zusammenzufassen. Dabei übernimmt ein mGuard in einem Fehlerfall die Funktion des anderen. Beide mGuards laufen synchron, so dass bei einem Wechsel die bestehende Verbindung nicht unterbrochen wird.

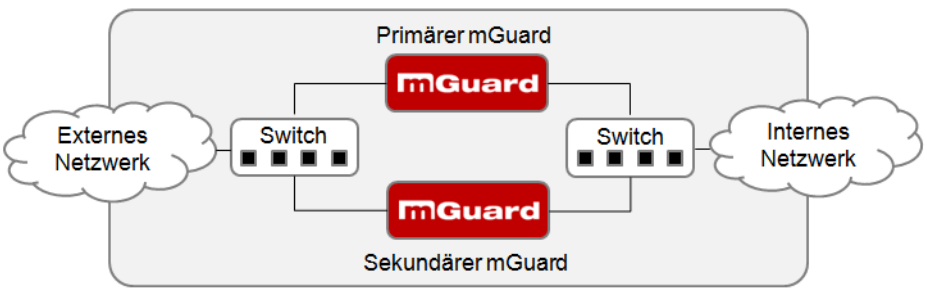


Bild 17-1 Firewall-Redundanz (Beispiel)

Grundbedingungen für die Firewall-Redundanz

Die Firewall-Redundanz ist eine lizenzpflichtige Funktion. Sie kann nur benutzt werden, wenn die entsprechende Lizenz erworben wurde und installiert ist.

- Nur baugleiche mGuards können ein Redundanzpaar bilden.
- Im Netzwerk-Modus Router wird die Firewall-Redundanz nur mit dem Router-Modus „Statisch“ unterstützt.
- Ab mGuard-Firmwareversion 7.5 wird die Firewall-Redundanz ebenfalls im Stealth-Modus, allerdings nur in der Stealth-Konfiguration „Mehrere Clients“, unterstützt.
- Weitere Einschränkungen siehe „Voraussetzungen für die Firewall-Redundanz“ auf Seite 444 und „Grenzen der Firewall-Redundanz“ auf Seite 454.

17.1.1 Komponenten der Firewall-Redundanz

Die Firewall-Redundanz besteht aus mehreren Komponenten:

- **Konnektivitätsprüfung**
  Prüft, ob die erforderlichen Netzwerkverbindungen bestehen.
- **Verfügbarkeitsprüfung**
  Prüft, ob ein aktiver mGuard vorhanden ist und ob dieser aktiv bleiben soll.
- **Zustandsabgleich der Firewall**
  Der mGuard in Bereitschaft erhält eine Kopie des aktuellen Zustands der Firewall-Datenbank.
- **Virtuelles Netzwerk-Interface**
  Stellt virtuelle IP-Adressen und MAC-Adressen bereit, die von anderen Geräten als Routen und Standard-Gateways genutzt werden können.
- **Statusüberwachung**
  Koordiniert alle Komponenten.
- **Statusanzeige**
  Zeigt dem Benutzer den Zustand des mGuards an.

Konnektivitätsprüfung

Bei jedem mGuard eines Redundanzpaares wird kontinuierlich geprüft, ob eine Verbindung besteht, über die Netzwerkpakete weitergleitet werden können.

Jeder mGuard prüft seine interne und externe Netzwerk-Schnittstelle unabhängig voneinander. Beide Schnittstellen werden auf eine durchgehende Verbindung getestet. Diese Verbindung muss bestehen, sonst wird die Konnektivitätsprüfung nicht bestanden.

Optional können ICMP-Echo-Requests gesendet werden. Sie können die ICMP-Echo-Requests über das Menü *Redundanz >> Firewall-Redundanz >> Konnektivitätsprüfung* einstellen.

Verfügbarkeitsprüfung

Bei jedem mGuard eines Redundanzpaares wird außerdem kontinuierlich geprüft, ob ein aktiver mGuard vorhanden ist und ob dieser aktiv bleiben soll. Dafür wird eine Variante des CARP (Common Address Redundancy Protocol) verwendet.

Der aktive mGuard sendet ständig Anwesenheitsnachrichten über sein internes und externes Netzwerk-Interface, während beide mGuards zuhören. Wenn ein dedizierter Ethernet-Link für den Zustandsabgleich der Firewall vorhanden ist, wird die Anwesenheitsnachricht auch über diesen gesendet. In diesem Fall kann die Anwesenheitsnachricht für die externe Netzwerk-Schnittstelle auch unterdrückt werden.

Die Verfügbarkeitsprüfung wird nicht bestanden, wenn ein mGuard in einer bestimmten Zeit keine Anwesenheitsnachricht erhält. Außerdem wird die Prüfung nicht bestanden, wenn ein mGuard Anwesenheitsnachrichten von niedrigerer Priorität erhält als die eigene.

Die Daten werden immer über das physikalische Netzwerk-Interface übertragen und niemals über das virtuelle Netzwerk-Interface.

Zustandsabgleich

Der mGuard, der sich im Zustand der Bereitschaft befindet, erhält eine Kopie des Zustandes des aktuell aktiven mGuards.

Dazu gehört eine Datenbank mit den weitergeleiteten Netzwerkverbindungen. Diese Datenbank wird laufend durch die weitergeleiteten Netzwerkpakete aufgebaut und erneuert. Sie ist gegen einen unberechtigen Zugriff geschützt. Die Daten werden über die physikalische LAN-Schnittstelle übertragen und niemals über das virtuelle Netzwerk-Interface gesendet.

Um den internen Datenverkehr gering zu halten, kann ein VLAN so konfiguiert werden, dass es die Abgleichsdaten in eine separate Multicast- und Broadcast-Domain verlagert.

Virtuelle IP-Adressen

Jeder mGuard wird mit virtuellen IP-Adressen konfiguriert. Deren Anzahl hängt von dem verwendeten Netzwerk-Modus ab. Bei einem Redundanzpaar müssen Sie beiden mGuards die gleichen virtuellen IP-Adressen zuweisen. Die virtuellen IP-Adressen werden vom mGuard benötigt, um virtuelle Netzwerk-Interfaces aufzubauen.

Für den Netzwerk-Modus Router sind zwei virtuelle IP-Adressen notwendig, weitere können angelegt werden. Eine virtuelle IP-Adresse wird für das externe Netzwerk-Interface und die andere für das interne Netzwerk-Interface benötigt.

Diese IP-Adressen werden als Gateway für das Routen von Geräten benutzt, die sich im externen oder internen LAN befinden. Auf diese Weise können die Geräte von der hohen Verfügbarkeit profitieren, die durch die beiden redundanten mGuards entsteht.

Das Redundanzpaar bestimmt automatisch MAC-Adressen für das virtuelle Netzwerk-Interface. Diese MAC-Adressen sind identisch für das Redundanzpaar. Im Netzwerk-Modus Router teilen sich beide mGuards je eine MAC-Adresse für das virtuelle Netzwerk-Interface, das mit dem externen und dem internen Ethernet-Segment verbunden ist.

Im Netzwerk-Modus Router unterstützen die mGuards eine Weiterleitung von speziellen UDP/TCP-Ports von einer virtuellen IP-Adresse zu anderen IP-Adressen, sofern letztere vom mGuard erreicht werden können. Zusätzlich maskiert der mGuard Daten mit virtuellen IP-Adressen, wenn Masquerading-Regeln eingerichtet sind.

Statusüberwachung

Die Statusüberwachung entscheidet darüber, ob der mGuard im Zustand aktiv, in Bereitschaft oder im Fehlerzustand ist. Jeder mGuard entscheidet autonom über seinen Zustand, basierend auf den Informationen, die von anderen Komponenten bereitgestellt werden. Die Statusüberwachung sorgt dafür, dass nicht zwei mGuards gleichzeitig aktiv sind.

Statusanzeige

Die Statusanzeige enthält detaillierte Informationen über den Status der Firewall-Redundanz. Eine Zusammenfassung des Status kann über das Menü *Redundanz >> Firewall-Redundanz >> Redundanz* oder *Redundanz >> Firewall-Redundanz >> Konnektivitätsprüfung* abgerufen werden.

17.1.2 Zusammenarbeit der Firewall-Redundanz-Komponenten

Während des Betriebes interagieren die Komponenten folgendermaßen: Beide mGuards führen fortlaufend für ihre beiden Netzwerk-Schnittstellen (internes und externes Interface) eine Konnektivitätsprüfung durch. Außerdem wird fortlaufend eine Verfügbarkeitsprüfung gemacht. Dazu lauscht jeder mGuard kontinuierlich auf Anwesenheitsnachrichten (CARP) und der aktive mGuard sendet diese zusätzlich.

Auf Grundlage der Informationen aus der Konnektivitäts- und - Verfügbarkeitsprüfung weiß die Statusüberwachung, in welchem Zustand sich die mGuards befinden. Die Statusüberwachung sorgt dafür, dass der aktive mGuard seine Daten auf den anderen mGuard spiegelt (Zustandsabgleich).

17.1.3 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.

17.1.4 Voraussetzungen für die Firewall-Redundanz

- Um die Redundanz-Funktion zu nutzen, müssen beide **mGuards** die gleiche Firmware haben.
- Die Firewall-Redundanz kann nur aktiviert werden, wenn ein gültiger Lizenzschlüssel installiert ist.

  (unter: *Redundanz >> Firewall-Redundanz >> Redundanz >> Aktiviere Redundanz)*
- *Redundanz >> Firewall-Redundanz >> Redundanz >> Interface, das zum Zustandsabgleich verwendet wird*

  Der Wert **Dediziertes Interface** wird nur auf **mGuards** akzeptiert, die mehr als zwei physikalische und getrennte Ethernet-Interfaces haben. Zur Zeit ist das der *mGuard centerport (Innominate)* / *FL MGUARD CENTERPORT*.
- Jeder Satz von Zielen für die Konnektivitätsprüfung kann mehr als zehn Ziele beinhalten. (Ohne eine Obergrenze kann eine Failover-Zeit nicht garantiert werden.)

  Redundanz >> Firewall-Redundanz >> Redundanz
  - *>> Externes Interface >> Primäre 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.

17.1.5 Umschaltzeit im Fehlerfall

Von der Variablen **Umschaltzeit im Fehlerfall** errechnet der mGuard automatisch die Zeitabstände für die Konnektivitäts- und Verfügbarkeitsprüfung.

Konnektivitätsprüfung

In der Tabelle 17-1 auf Seite 445 werden die Faktoren angegeben, die die Zeitabstände für die Konnektivitätsprüfung bestimmen.

Für die Konnektivitätsprüfung werden ICMP-Echo-Requests verschickt, die 64 kByte groß sind. Sie werden auf Layer 3 des Internet-Protokolls gesendet. Mit dem Ethernet auf Layer 2 kommen 18 Bytes für den MAC-Header und die Prüfsumme dazu, wenn kein VLAN verwendet wird. Der ICMP-Echo-Reply hat die gleiche Größe.

In Tabelle 17-1 wird außerdem die Bandbreite gezeigt. Sie berücksichtigt die genannten Werte für ein einzelnes Ziel und summiert die Bytes für ICMP-Echo-Request und Reply.

Der Timeout am mGuard nach dem Senden enthält Folgendes:

– Die Zeit, die der mGuard braucht, um den ICMP-Echo-Reply zu übertragen. Der Halb-Duplex-Modus ist hierfür nicht geeignet, wenn anderer Datenverkehr dazu kommt.
– Die Zeit, die für die Übertragung des ICMP-Echo-Requests zu einem Ziel erforderlich ist. Beachten Sie dabei die Latenzzeit bei einer hohen Auslastung. Die gilt besonders, wenn Router die Anfrage weiterleiten. Die 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 17-1 Frequenz der ICMP-Echo-Requests

Failover-Umschaltzeit	ICMP-Echo-Requests pro Ziel	Timeout am mGuard nach dem Senden	Bandbreite pro Ziel
1 s	10 pro Sekunde	100 ms	6560 Bit/s
3 s	$3,\overline{3}$ pro Sekunde	300 ms	2187 Bit/s
10 s	1 pro Sekunde	1 s	656 Bit/s

Wenn sekundäre Ziele konfiguriert sind, kann es gelegentlich passieren, dass zusätzliche ICMP-Echo-Requests zu diesen Zielen gesendet werden. Dies muss bei der Berechnung für die ICMP-Echo-Request-Rate berücksichtigt werden.

In der Tabelle 17-1 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.

Die Tabelle 17-2 zeigt die maximale Frequenz, mit der Anwesenheitsnachrichten (CARP) vom aktiven mGuard gesendet werden. Sie zeigt außerdem die Bandbreite, die dabei verbraucht wird. Die Frequenz hängt von der Priorität des mGuards und der *Umschaltzeit im Fehlerfall* ab.

Die Tabelle 17-2 zeigt außerdem die maximale Latenzzeit, die der mGuard für das Netzwerk toleriert, das die Anwesenheitsnachrichten (CARP) überträgt. Wenn diese Latenzzeit überschritten wird, kann das Redundanzpaar ein undefiniertes Verhalten zeigen.

Tabelle 17-2 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

17.1.6 Fehlerkompensation durch die Firewall-Redundanz

Die Firewall-Redundanz dient dazu, den Ausfall von Hardware auszugleichen.

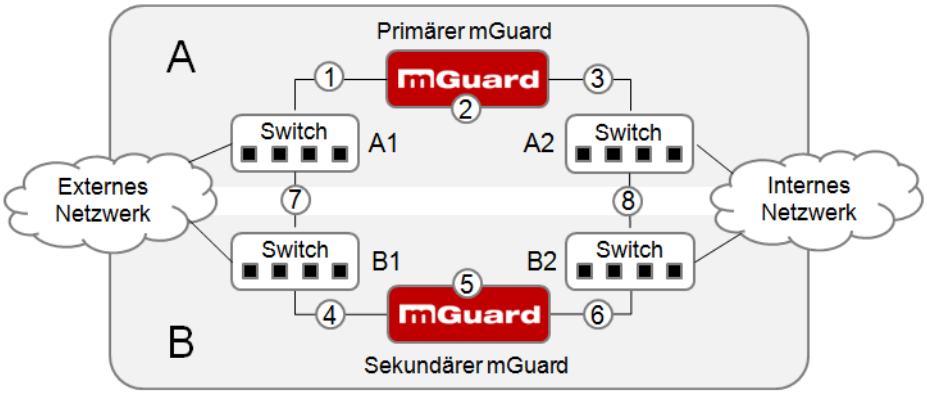


Bild 17-2 Mögliche Fehlerorte (1 ... 8)

In Bild 17-2 wird ein Aufbau gezeigt, der verschiedene Fehlerorte zeigt (unabhängig vom Netzwerk-Modus).

Jeder der beiden mGuards eines Redundanzpaares sitzt in einem unterschiedlichen Bereich (A und B). Der mGuard in Bereich A ist mit seinem externen Ethernet-Interface an Switch A1 und mit seinem internen Ethernet-Interface an Switch A2 angeschlossen. Der mGuard B ist entsprechend mit den Switchen B1 und B2 gekoppelt. Auf diese Weise verbinden die Switche und die mGuards ein externes mit einem internen Ethernet-Netzwerk. Sie stellen die Verbindung her, indem sie Netzwerk-Pakete (im Netzwerk-Modus Router) weiterleiten.

Die Firewall-Redundanz kompensiert die Fehler, die in Bild 17-2 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 17-2).

17.1.7 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 292), 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

17.1.8 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 424). 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 445 beschrieben.

Ausreichende Bandbreite

Der Datenverkehr, der durch die Konnektivitäts- und Verfügbarkeitsprüfung und den Zustandsabgleich entsteht, verbraucht Bandbreite im Netzwerk. Außerdem erzeugt die Konnektivitätsprüfung einen rechnerischen Aufwand. Es gibt mehrere Methoden, dies zu verringern oder ganz aufzuheben.

Wenn ein Einfluss auf andere Geräte nicht akzeptabel ist,

– dann muss die Konnektivitätsprüfung entweder deaktiviert werden oder sie darf sich nur auf die reale IP-Adresse des anderen **mGuards** beziehen.
– dann muss der Datenverkehr durch die Verfügbarkeitsprüfung und den Zustandsabgleich in ein separates VLAN verschoben werden.
– dann müssen Switche genutzt werden, die es erlauben, VLANs zu splitten.

Dediziertes Interface

Der *mGuard centerport (Innominate) /* FL MGUARD CENTERPORT unterstützt ein **dediziertes Interface**. Das ist eine reservierte direkte Ethernet-Schnittstelle oder ein dediziertes LAN-Segment, über das der Zustandsabgleich gesendet wird. Auf diese Weise ist die Last sogar physikalisch vom internen LAN-Segment getrennt.

17.1.9 Übertragungsleistung der Firewall-Redundanz

Die Werte gelten für den Netzwerk-Modus Router, wenn der Datenverkehr für den Zustandsabgleich unverschlüsselt übertragen wird. Wenn die hier beschriebene Übertragungsleistung überschritten wird, kann im Fehlerfall eine längere Umschaltzeiten entstehen, als eingestellt ist.

Plattform		Übertragungsleistung der Firewall-Redundanz
mGuard centerport (Innominate), FL MGUARD CENTERPORT		1500 MBit/s, bidirektional[1], nicht mehr als 400000 Frames/s
FL MGUARD RS FL MGUARD SMART 533/266 FL MGUARD BLADE mGuard delta (Innominate)	mit 533 MHz	150 MBit/s[1], bidirektional, nicht mehr als 12750 Frames/s
FL MGUARD RS FL MGUARD SMART 533/266 FL MGUARD BLADE mGuard delta (Innominate)	mit 266 MHz	62 MBit/s, bidirektional[1], nicht mehr als 5250 Frames/s
FL MGUARD RS4000 TC MGUARD RS4000 3G, TC MGUARD RS4000 4G FL MGUARD RS4004 FL MGUARD SMART2 FL MGUARD CORE TX FL MGUARD PCI(E)4000 FL MGUARD DELTA		62 MBit/s, bidirektional[1], nicht mehr als 5250 Frames/s

1 Bidirektional umfasst den Traffic in beide Richtungen. Zum Beispiel bedeutet 1500 MBit/s, dass in jede Richtung 750 MBit/s weitergeleitet werden.

Failover-Umschaltzeit

Sie können die Umschaltzeit im Fehlerfall auf 1, 3 oder 10 Sekunden einstellen.

Die Obergrenze von 1 Sekunde wird derzeit nur vom *mGuard centerport (Innominate),* FL MGUARD CENTERPORT auch unter hoher Auslastung eingehalten.

17.1.10 Grenzen der Firewall-Redundanz

- Im **Netzwerk-Modus Router** wird die Firewall-Redundanz nur mit dem Modus „statisch“ unterstützt.
- Ein Zugang zum mGuard über die **Management-Protokolle** HTTPS, SNMP und SSH ist nur mit einer realen IP-Adresse eines jeden mGuards möglich. Zugriffe auf virtuelle Adressen werden zurückgewiesen.
- Die folgenden **Features** können mit der Firewall-Redundanz **nicht benutzt** werden.
  - ein sekundäres externes Ethernet-Interface,
  - ein DHCP-Server,
  - ein DHCP-Relay,
  - ein SEC-Stick-Server,
  - eine Benutzer-Firewall und
  - das CIFS-Integrity-Monitoring.
- Das **Redundanzpaar muss identisch konfiguriert** werden. Beachten Sie dies bei der Einstellung von:
  - NAT-Einstellungen (Masquerading, Port-Weiterleitung und 1:1-NAT)
  - Flood-Protection
  - Paketfilter (Firewall-Regeln, MAC-Filter, Erweiterte Einstellungen)
  - den Queues und den Regeln für die QoS
- Nach einer **Netzwerk-Lobotomie** sind möglicherweise einige Netzwerkverbindungen unterbrochen. (Siehe „Wiederherstellung bei einer Netzwerk-Lobotomie“ auf Seite 448).
- Nach einem Failover können s**emi-unidirektionale oder komplexe Verbindungen** unterbrochen sein, die genau in der Sekunde vor dem Failover aufgebaut worden sind. (Siehe „Failover beim Aufbau von komplexen Verbindungen“ auf Seite 448 und „Failover beim Aufbau von semi-unidirektionalen Verbindungen“ auf Seite 448.)
- Die Firewall-Redundanz unterstützt nicht den **FL MGUARD PCI 533/266 im Treiber-Modus**.
- Der Zustandsabgleich repliziert keine Connection-Tracking-Einträge für **ICMP-Echo-Requests**, die vom mGuard weitergeleitet werden. Deshalb können ICMP-Echo-Replies entsprechend der Firewall-Regeln fallen gelassen werden, wenn sie den mGuard erst erreichen, wenn der Failover abgeschlossen ist. Beachten Sie, dass ICMP-Echo-Replies nicht dazu geeignet sind, die Failover-Umschaltzeit zu messen.
- **Masquerading** wird dadurch ausgeführt, dass der Sender hinter der ersten virtuellen IP-Adresse bzw. der ersten internen IP-Adresse verborgen wird. Das unterscheidet sich von dem Masquerading des mGuards ohne Firewall-Redundanz. Ohne aktivierte Firewall-Redundanz wird in einer Routing-Tabelle festgelegt, hinter welcher externen bzw. internen IP-Adresse der Sender verborgen wird.

17.2 VPN-Redundanz

Die VPN-Redundanz kann nur zusammen mit der Firewall-Redundanz genutzt werden.

Das Konzept ist genauso wie bei der Firewall-Redundanz. Um einen Fehler im Umfeld aufzufangen, wird die Aktivität von dem aktiven mGuard auf einen mGuard in Bereitschaft übertragen.

Zu jedem Zeitpunkt betreibt mindestens ein mGuard des Redundanzpaares die VPN-Verbindung, außer wenn eine Netzwerk-Lobotomie vorliegt.

Grundbedingungen für die VPN-Redundanz

Für die VPN-Redundanz gibt es keine eigenen Variablen. Es gibt gegenwärtig kein eigenes Menü in der Benutzeroberfläche, sondern sie wird mit der Firewall-Redundanz zusammen aktiviert.

Voraussetzung für die VPN-Redundanz ist eine entsprechende Lizenz, die Sie auf dem mGuard installieren müssen.

Da für die VPN-Redundanz der Aufbau von VPN-Verbindungen notwendig ist, brauchen Sie zusätzlich eine entsprechende VPN-Lizenz.

Wenn Sie nur die Lizenz für die Firewall-Redundanz haben und VPN-Verbindungen installiert sind, können Sie keine VPN-Redundanz aktivieren. Sie erhalten eine Fehlermeldung, sobald Sie die Firewall-Redundanz nutzen wollen.

Nur baugleiche mGuards können ein Redundanzpaar bilden.

17.2.1 Komponenten der VPN-Redundanz

Die Komponenten der VPN-Redundanz sind die gleichen, die bei der Firewall-Redundanz beschrieben worden sind. Zusätzlich gibt es noch eine weitere Komponente: der VPN-Zustandsabgleich. Einige wenige Komponenten sind für die VPN-Redundanz leicht erweitert. Aber die Konnektivitäts- und Verfügbarkeitsprüfung und der Zustandsabgleich von der Firewall funktionieren auf die gleiche Weise.

VPN-Zustandsabgleich

Der mGuard unterstützt die Konfiguration von Firewall-Regeln für die VPN-Verbindung.

Der VPN-Zustandsabgleich verfolgt den Zustand der verschiedenen VPN-Verbindungen am aktiven mGuard. Er sorgt dafür, dass der mGuard in Bereitschaft eine zur Zeit gültige Kopie der VPN-Zustand-Datenbank erhält.

Wie bei dem Zustandsabgleich der Firewall sendet er Updates vom aktiven mGuard zum mGuard in Bereitschaft. Auf Anfrage vom mGuard in Bereitschaft versendet der aktive mGuard einen kompletten Satz aller Zustandsinformationen.

Dediziertes Interface (mGuard centerport (Innominate), FL MGUARD CENTERPORT)

Beim *mGuard centerport (Innominate), FL MGUARD CENTERPORT* können Sie das dritte Ethernet-Interface für den VPN-Zustandsabgleich fest zuordnen.

Wie bei dem Zustandsabgleich der Firewall wird der Datenverkehr für den VPN-Zustandsabgleich für das dedizierte Interface übertragen, wenn eine Variable gesetzt wird. Stellen Sie unter *Redundanz >> Firewall-Redundanz >> Redundanz* das *Interface, das zum Zustandsabgleich verwendet wird* auf **Dediziertes Interface**.

Aufbau von VPN-Verbindungen

Mit der VPN-Redundanz wird das virtuelle Netzwerk-Interface für einen zusätzlichen Zweck genutzt: Es wird verwendet, um VPN-Verbindungen aufzubauen, zu akzeptieren und zu betreiben. Der mGuard lauscht nur auf der ersten virtuellen IP-Adresse.

Im Netzwerk-Modus Router hört er an der ersten externen und internen virtuellen IP-Adresse zu.

Statusüberwachung

Die Statusüberwachung überwacht den VPN-Zustandsabgleich genauso wie den der Firewall.

17.2.2 Zusammenarbeit der VPN-Redundanz Komponenten

Die einzelnen Komponenten arbeiten auf die gleiche Weise zusammen, wie bei der Firewall-Redundanz. Der VPN-Zustandsabgleich wird ebenfalls durch die Statusüberwachung gesteuert, der Status wird festgehalten und es werden Updates gesendet.

Damit die Zustände eintreten, müssen bestimmte Bedingungen erfüllt werden. Der VPN-Zustandsabgleich wird damit mit berücksichtigt.

17.2.3 Fehlerkompensation durch die VPN-Redundanz

Die VPN-Redundanz kompensiert genau die gleichen Fehler wie die Firewall-Redundanz (siehe „Fehlerkompensation durch die Firewall-Redundanz“ auf Seite 447).

Allerdings kann bei einer Netzwerk-Lobotomie der VPN-Teil die anderen VPN-Gateways stören. Die von einander unabhängigen mGuards haben dann die gleiche virtuelle IP-Adresse um mit den VPN-Partnern zu kommunizieren. Das kann dazu führen, dass die VPN-Verbindungen in schneller Folge auf- und abgebaut werden.

17.2.4 Variablen für die VPN-Redundanz erstellen

Bei passenden Lizenzschlüsseln wird die VPN-Redundanz automatisch aktiviert, wenn Sie die Firewall-Redundanz aktivieren. Dies geschieht, sobald Sie im Menü *Redundanz >> Firewall-Redundanz >> Redundanz* den Punkt *Aktiviere Redundanz* auf **Ja** stellen.

Es gibt kein eigenes Menü für die VPN-Redundanz. Die vorhandenen Firewall-Redundanz-Variablen werden erweitert.

Tabelle 17-3 Erweiterte Funktionen bei aktivierter VPN-Redundanz

Redundanz >> Firewall-Redundanz >> Redundanz		
Allgemein	**Aktiviere Redundanz**	Die Firewall-Redundanz und die VPN-Redundanz werden aktiviert oder deaktiviert.
Virtuelle Interfaces	**Externe virtuelle IP-Adressen**	Nur im Netzwerk-Modus Router Der mGuard nutzt die erste externe virtuelle IP-Adresse als Adresse von der er IKE-Nachrichten sendet und erhält. Die externe virtuelle IP-Adresse wird anstelle der realen primäre IP-Adresse des externen Netzwerk-Interfaces genutzt. Der mGuard verwendet die reale IP-Adresse nicht länger, um IKE-Nachrichten zu senden oder zu beantworten. Der ESP-Datenverkehr wird ähnlich gehandhabt, allerdings wird er ebenfalls von der realen IP-Adresse akzeptiert und bearbeitet.
	Interne virtuelle IP-Adressen	Wie unter *Externe virtuelle IP-Adressen* beschrieben, aber für die internen virtuellen IP-Adressen.

17.2.5 Voraussetzungen für die VPN-Redundanz

– Die VPN-Redundanz kann nur aktiviert werden, wenn ein **Lizenzschlüssel** für die VPN-Redundanz installiert ist und eine VPN-Verbindung aktiviert ist.

– **Nur bei TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4004, FL MGUARD RS4000, FL MGUARD GT/GT und FL MGUARD RS**

  Wenn eine VPN-Verbindung über einen **VPN-Schalter** gesteuert wird, dann kann die VPN-Redundanz nicht aktiviert werden.

  (unter: *IPsec VPN* >> *Global* >> *Optionen* >> *VPN-Schalter*)

Beim VPN-Zustandsabgleich wird kontinuierlich der Zustand der VPN-Verbindung vom aktiven auf den mGuard in Bereitschaft übertragen, damit dieser im Fehlerfall eine tatsächliche Kopie hat. Die einzige Ausnahme dazu ist der Status des IPsec Replay Windows. Änderungen dort werden nur von Zeit zur Zeit übertragen.

Der Umfang des Datenverkehrs für den Zustandsabgleich hängt nicht von dem Datenverkehr ab, der über die VPN-Tunnel geleitet wird. Das Datenvolumen für den Zustandsabgleich wird durch verschiedene Parameter bestimmt, die für ISAKMP SAs und IPsec SAs vergeben werden.

17.2.6 Umgang der VPN-Redundanz mit extremen Situationen

Die Bedingungen, die unter „Umgang der Firewall-Redundanz mit extremen Situationen“ auf Seite 448 aufgeführt sind, gelten auch für die VPN-Redundanz. Sie gelten auch dann, wenn der mGuard ausschließlich dafür genutzt wird, VPN-Verbindungen weiterzuleiten. Der mGuard leitet die Datenströme über die VPN-Tunnel weiter und sortiert fehlerhafte Pakete aus, unabhängig davon, ob für die VPN-Verbindungen Firewall-Regeln definiert sind oder nicht.

Ein Fehler unterbricht den laufenden Datenverkehr

Wenn ein Fehler den Datenverkehr unterbricht, der über die VPN-Tunnel läuft, ist das eine extreme Situation. In diesem Fall ist der IPsec-Datenverkehr für kurze Zeit für Replay-Attacken anfällig. (Eine Replay-Attacke ist die Wiederholung bereits gesendeter verschlüsselter Datenpakete mit Hilfe von Kopien, die ein Angreifer aufbewahrt hat.) Der Datenverkehr wird mit Hilfe von Sequenznummern geschützt. Für jede Richtung eines IPsec-Tunnels werden unabhängige Sequenznummern verwendet. Der mGuard lässt ESP-Pakete fallen, die die gleiche Sequenznummer haben, wie ein Paket, das der mGuard für einen bestimmten IPsec-Tunnel bereits entschlüsselt hat. Dieser Mechanismus wird **IPsec-Replay-Window** genannt.

Das IPsec-Relay-Window wird beim Zustandsabgleich nur von Zeit zur Zeit repliziert, da es zu viele Ressourcen bindet. So kann es vorkommen, dass nach einem Failover der aktive mGuard ein veraltetes IPsec-Replay-Window hat. Auf diese Weise ist ein Angriff möglich, bis der echte VPN-Partner das nächste ESP-Paket für die entsprechenden IPsec SA sendet oder bis der IPsec SA erneuert wird.

Um eine zu geringe Sequenznummer bei dem ausgehenden IPsec SA zu verhindern, addiert die VPN-Redundanz zu jeder ausgehenden IPsec SA einen konstanten Wert zur Sequenznummer dazu, bevor der mGuard aktiv wird. Dieser Wert ist so berechnet, dass er zu der maximalen Anzahl an Datenpaketen passt, die durch den VPN-Tunnel während der maximalen Failover-Umschaltzeit gesendet werden können. Im schlimmsten Fall (bei einem Gigabit-Ethernet und einer Umschaltzeit von 10 Sekunden) sind das 0,5 % einer IPsec Sequenz. Im besten Fall ist es nur ein Promille.

Das Addieren des konstanten Wertes zur Sequenznummer verhindert, dass eine Sequenznummer versehentlich wiederverwendet wird, die bereits vom anderen mGuard verwendet wurde, kurz bevor dieser ausgefallen ist. Ein weiterer Effekt ist, dass die ESP-Pakete, die vom vorher aktiven mGuard gesendet wurden, vom VPN-Partner fallengelassen werden, wenn neue ESP-Pakete vom nun aktiven mGuard früher ankommen. Dafür ist es aber notwendig, dass die Latenzzeit im Netzwerk sich von der Failover-Umschaltzeit unterscheidet.

Ein Fehler unterbricht den ersten Aufbau von ISAKMP SA oder IPsec SA

Wenn ein Fehler den ersten Aufbau von ISAKMP SA oder IPsec SA unterbricht, dann kann der mGuard in Bereitschaft den Aufbau nahtlos fortsetzen, da der Status der SA synchron repliziert wird. Der Response auf eine IKE-Nachricht wird nur vom aktiven mGuard gesendet, nachdem der mGuard in Bereitschaft den Empfang des entsprechenden Updates des VPN-Zustandsabgleichs bestätigt hat.

Wenn ein mGuard aktiv wird, wiederholt er sofort die letzte IKE-Nachricht, die vom vorher aktiven mGuard hätte gesendet werden müssen. Damit wird der Fall kompensiert, dass der vorher aktive mGuard zwar den Zustandabgleich noch gesendet hat, aber ausgefallen ist, bevor er die entsprechende IKE-Nachricht senden konnte.

Auf diese Weise wird während eines Failovers der Aufbau von ISAKMP SA oder IPsec SA nur um die Zeit verzögert, die für die Umschaltung benötigt wird.

Ein Fehler unterbricht die Erneuerung einer ISAKMP SA

Wenn ein Fehler die Erneuerung einer ISAKMP SA unterbricht, wird das auf die gleiche Weise ausgeglichen, wie dem ersten Aufbau einer SA. Außerdem wird die alte ISAKMP SA für die Dead Peer Detection beibehalten, bis die Erneuerung der ISAKMP SA abgeschlossen ist.

Ein Fehler unterbricht die Erneuerung einer IPsec SA

Wenn ein Fehler die Erneuerung einer IPsec SA unterbricht, wird das auf die gleiche Weise ausgeglichen, wie dem ersten Aufbau einer SA. Solange die Erneuerung der ISAKMP SA noch nicht abgeschlossen ist, werden die alten ein- und ausgehende IPsec SAs beibehalten, bis der VPN-Partner den Wechsel bemerkt hat.

Der VPN-Zustandsabgleich sorgt dafür, dass die alten IPsec SA beibehalten werden, solange der mGuard in Bereitschaft ist. Wenn er dann aktiv wird, ist sichergestellt, dass er ohne weitere Aktionen mit der Ver- und Entschlüsselung des Datenverkehrs fortfahren kann.

Datenpaket-Verlust beim VPN-Zustandsabgleich

Der Zustandsabgleich ist gegen den Verlust von einem von zwei aufeinanderfolgenden Update-Paketen resistent. Wenn mehr Datenpakete verloren gehen, kann es zu einer längeren Umschaltzeit im Fehlerfall kommen.

Der mGuard in Bereitschaft hat ein veraltetes Maschinenzertifikat

Es kann vorkommen, dass X.509-Zertifikate und private Schlüssel geändert werden müssen, die von einem Redundanzpaar genutzt werden, um sich selbst als VPN-Partner zu authentifizieren. Die Kombination aus privatem Schlüssel und Zertifikat wird im Folgenden Maschinenzertifikat genannt.

Jeder mGuard eines Redundanzpaares muss neu konfiguriert werden, um das Maschinenzertifikat zu tauschen. Und beide mGuards benötigen das gleiche Zertifikat, um aus der Sicht ihrer VPN-Partner als die selbe virtuelle VPN-Appliance zu erscheinen.

Da jeder mGuard einzeln neu konfiguriert wird, kann es für eine kurze Zeit vorkommen, dass der mGuard in Bereitschaft ein veraltetes Maschinenzertifikat besitzt.

Wenn der mGuard in Bereitschaft genau in dem Augenblick aktiv wird, in dem ISAKMP SAs aufgebaut werden, kann es das mit einem veralteten Maschinenzertifikat nicht fortsetzen,

Als Gegenmaßnahme repliziert der VPN-Zustandsabgleich das Maschinenzertifikat vom aktiven mGuards zu dem mGuard in Bereitschaft. Bei einem Failover wird der mGuard in Bereitschaft dieses nur benutzen, um den bereits begonnenen Aufbau der ISAKMP SAs abzuschließen.

Wenn der mGuard in Bereitschaft nach einem Failover neue ISAKMP SAs aufbaut, wird er das noch konfigurierte Maschinenzertifikat nutzen.

Der VPN-Zustandsabgleich sorgt also für die Replizierung der Maschinenzertifikate, die gerade benutzt werden. Aber es repliziert nicht die Konfiguration selbst.

Der mGuard **in Bereitschaft hat einen veralteten Pre-Shared-Key (PSK)**

Ebenso müssen Preshared-Keys (PSK) zur Authentifizierung von VPN-Partnern manchmal erneuert werden. Für eine kurze Zeit können also die redundanten mGuards einen unterschiedlichen PSK haben. In diesem Fall kann nur einer der mGuards eine VPN-Verbindung aufbauen, da die meisten VPN-Partner nur einen PSK akzeptieren. Der mGuard hat hierfür keine Gegenmaßnahme.

Wir empfehlen daher, X.509-Zertifikate anstelle von PSKs zu benutzen.

Wenn der VPN-Zustandsabgleich die PSKs längere Zeit auf den mGuard in Bereitschaft repliziert, dann verdeckt dies eine fehlerhafte Konfiguration für eine längere Zeit und ist schwer zu entdecken.

17.2.7 Zusammenwirken mit anderen Geräten

Auflösen von Hostnamen

Wenn Hostnamen als VPN-Gateways konfiguriert sind, dann müssen die mGuards eines Redundanzpaares in der Lage sein, die Hostnamen zu selben IP-Adresse aufzulösen. Dies gilt besonders, wenn *DynDNS-Überwachung* (siehe *Seite 335*) aktiviert ist.

Wenn die Hostnamen von dem mGuard in Bereitschaft auf eine andere IP-Adresse aufgelöst werden, dann wird nach einem Failover die VPN-Verbindung zu diesem Host abgebrochen. Die VPN-Verbindung wird an einer anderen IP-Adresse wieder aufgebaut. Dies passiert direkt nach dem Failover. Es kann aber zu einer kurzen Verzögerung kommen, die u. a. davon abhängt, was unter *DynDNS-Überwachung* als Wert für das *Abfrageintervall* eingetragen ist.

Veraltetes IPsec-Replay-Window

Der IPsec-Datenverkehr ist gegen einen unauthorisierten Zugriff geschützt. Dazu wird jeder IPsec-Tunnel mit einer unanhängigen Sequenznummer versehen. Der mGuard lässt ESP-Pakete fallen, die die gleiche Sequenznummer haben, wie ein Paket, das der mGuard für einen bestimmten IPsec-Tunnel bereits entschlüsselt hat. Dieser Mechanismus wird **IPsec-Replay-Window** genannt. Es verhindert einen Replay-Angriff, bei dem der Angreifer zuvor aufgezeichnete Daten sendet, um etwa eine fremde Identität vorzutäuschen.

Das IPsec-Relay-Window wird beim Zustandsabgleich nur von Zeit zur Zeit repliziert, da es zu viele Ressourcen bindet. So kann es vorkommen, dass nach einem Failover der aktive mGuard ein veraltetes IPsec-Replay-Window hat. Auf diese Weise ist kurzzeitig eine Re-

play-Angriff möglich, bis der echte VPN-Partner das nächste ESP-Paket für die entsprechenden IPsec SA sendet oder bis der IPsec SA erneuert wird. Allerdings müsste ein vollständiger Traffic gekapert werden.

Dead Peer Detection

Sie müssen bei der Dead Peer Detection einen Punkt beachten.

Stellen Sie bei der Dead Peer Detection einen höheren Timeout ein als die obere Grenze der *Umschaltzeit im Fehlerfall* beim Redundanzpaar.

(unter: *IPsec VPN >> Verbindungen >> Editieren >> IKE-Optionen, Verzögerung bis zur nächsten Anfrage nach einem Lebenszeichen)*

Andernfalls könnten die VPN-Partner das Redundanzpaar für tot halten, obwohl sie nur mit dem Failover beschäftigt sind.

Datenverkehr

Eine hohe Latenzzeit im Netzwerk, das für die Updates des Zustandsabgleichs genutzt wird führt dazu, dass der mGuard in Bereitschaft in den „outdated“ Zustand geht. Das Gleiche geschieht bei einem ernsten Datenverlust in diesem Netzwerk.

Solange nicht mehr als zwei aufeinander folgende Updates verloren gehen, kommt es aber nicht dazu. Denn der mGuard in Bereitschaft fordert automatisch eine Wiederholung des Updates ein. Die Anforderungen an die Latenzzeit sind dieselben, wie unter „Umschaltzeit im Fehlerfall“ auf Seite 445 beschrieben.

Reale IP-Adressen

VPN-Partner dürfen keinen ESP-Traffic an die reale IP-Adresse des Redundanzpaares senden. VPN-Partner müssen immer die virtuelle IP-Adresse des Redundanzpaares nutzen, um dorthin IKE-Nachrichten oder ESP-Traffic zu senden.

17.2.8 Übertragungsleistung der VPN-Redundanz

Die Werte gelten für den Netzwerk-Modus Router, wenn der Datenverkehr für den Zustandsabgleich unverschlüsselt übertragen wird. Wenn die hier beschriebene Übertragungsleistung überschritten wird, kann im Fehlerfall eine längere Umschaltzeiten entstehen, als eingestellt ist.

Plattform		Übertragungsleistung der Firewall-Redundanz
mGuard centerport (Innominate), FL MGUARD CENTERPORT		220 MBit/s, bidirektional[1], nicht mehr als 60000 Frames/s
FL MGUARD RS FL MGUARD SMART 533/266 mGuard core (Innominate) FL MGUARD PCI 533/266 FL MGUARD BLADE mGuard delta (Innominate)	mit 533 MHz	50 MBit/s, bidirektional[1], nicht mehr als 5500 Frames/s
FL MGUARD RS FL MGUARD SMART 533/266 mGuard core (Innominate) FL MGUARD PCI 533/266 FL MGUARD BLADE mGuard delta (Innominate)	mit 266 MHz	17 MBit/s, bidirektional[1], nicht mehr als 2300 Frames/s
FL MGUARD RS4000 TC MGUARD RS4000 3G TC MGUARD RS4000 4G FL MGUARD RS4004 FL MGUARD SMART2 FL MGUARD CORE TX FL MGUARD PCI(E)4000 FL MGUARD DELTA		17 MBit/s, bidirektional[1], nicht mehr als 2300 Frames/s

[1] Bidirektional umfasst den Traffic in beide Richtungen. Zum Beispiel bedeutet 1500 MBit/s, dass in jede Richtung 750 MBit/s weitergeleitet werden.

Failover-Umschaltzeit

Sie können die Umschaltzeit im Fehlerfall auf 1, 3 oder 10 Sekunden einstellen.

Die Obergrenze von 1 Sekunde wird derzeit nur vom mGuard centerport (Innominate) / FL MGUARD CENTERPORT auch unter hoher Auslastung eingehalten.

17.2.9 Grenzen der VPN-Redundanz

Die Grenzen die für die Firewall-Redundanz dokumentiert sind, gelten auf für die VPN-Redundanz (siehe „Grenzen der Firewall-Redundanz“ auf Seite 454). Es gibt zusätzlich weitere Einschränkungen.

- Das Redundanzpaar muss bei diesen Punkten **identisch konfiguriert** sein:
  - bei den allgemeinen VPN-Einstellungen und
  - jeder einzelnen VPN-Verbindung.
- Der mGuard akzeptiert VPN-Verbindungen nur an der **ersten virtuellen IP-Adresse**.
  - Für den Netzwerk-Modus Router meint dies die erste interne und die erste externe IP-Adresse.
- Die folgenden **Features** können mit der VPN-Redundanz **nicht genutzt** werden:
  - Die dynamische Aktivierung der VPN-Verbindungen mit Hilfe eines VPN-Schalters oder über die Kommandos des CGI-Skriptes nph-vpn.cgi (nur beim TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4004 und FL MGUARD RS4000).
  - Das Archivieren von Diagnose-Meldungen für VPN-Verbindungen.
- VPN-Verbindungen werden nur im Tunnel-Modus unterstützt. VPN-Verbindungen im Transport-Modus werden nicht hinreichend berücksichtigt.
- Die obere Grenze der **Failover-Umschaltzeit** gilt nicht für Verbindungen, die mit **TCP gekapselt** sind. Solche Verbindungen werden bei einem Failover für eine längere Zeit unterbrochen. Nach jedem Failover müssen die gekapselten TPC-Verbindungen von der initiierenden Seite neu aufgebaut werden. Wenn der Failover auf der initiierenden Seite passiert ist, können sie sofort nach der Übernahme starten. Aber wenn der Failover auf der antwortenden Seite liegt, muss der Initiator erst die Unterbrechung entdecken und kann sie dann neu aufbauen.
- Die VPN-Redundanz unterstützt **Masquerading** auf die gleiche Weise, wie ohne VPN-Redundanz. Dies gilt, wenn ein Redundanzpaar durch ein NAT-Gateway mit einer dynamischen IP-Adresse maskiert wird.

  Zum Beispiel kann ein Redundanzpaar hinter einem DSL-Router versteckt werden, der das Redundanzpaar mit einer offiziellen IP-Adresse maskiert. Dieser DSL-Router leitet den IPsec-Datenverkehr (IKE und ESP, UDP-Ports 500 und 4500) zu den virtuellen IP-Adressen weiter. Wenn sich die dynamische IP-Adresse ändert, werden alle aktiven VPN-Verbindungen, die über das NAT-Gateway fließen, wieder aufgebaut.

  Für den Wiederaufbau sorgt die Dead Peer Detection (DPD) mit der dafür konfigurierten Zeit. Dieser Effekt liegt außerhalb des Einflussbereichs des mGuards.
- Die Redundanz-Funktion des mGuards unterstützt keine **Pfad-Redundanz**. Die Pfad-Redundanz kann über andere Maßnahmen erreicht werden, z. B. über ein Routerpaar. Dieses Routerpaar wird auf der einen virtuellen Seite von den mGuards gesehen, während auf der anderen Seite jeder der Router unterschiedliche Verbindungen hat.

  Eine Pfad-Redundanz darf keine NAT-Mechanismen wie Masquerading nutzen, um die virtuellen IP-Adressen der mGuards zu verbergen. Andernfalls wird eine Migration von einem Pfad zum anderen die IP-Adressen, mit denen das Redundanzpaar maskiert ist, ändern. Das würde dazu führen, dass alle VPN-Verbindungen (alle ISAKMP SAs und alle IPsec SAs) wieder aufgebaut werden müssen.

  Für den Wiederaufbau sorgt die Dead Peer Detection (DPD) mit der dafür konfigurierten Zeit. Dieser Effekt liegt außerhalb des Einflussbereichs des mGuards.
- Bei einer Pfad-Redundanz, die durch eine Netzwerk-Lobotomie ausgelöst wird, werden die VPN-Verbindungen nicht länger unterstützt. Eine Netzwerk-Lobotomie muss wenn möglich verhindert werden.

X.509-Zertifikate für die VPN-Authentification

Der mGuard unterstützt die Verwendung von X.509-Zertifikaten beim Aufbau von VPN-Verbindungen. Dies wird ausführlich unter „Authentifizierung“ auf Seite 359 beschrieben.

Es gib aber einige Besonderheiten, wenn X.509-Zertifikate zur Authentifizierung von VPN-Verbindungen in Kombination mit Firewall- und VPN-Redundanz genutzt werden.

Maschinen-Zertifikate wechseln

Ein Redundanzpaar kann so konfiguriert werden, dass es gemeinsam einen X.509-Zertifikat und einen entsprechenden privaten Schlüssel nutzt, um sich selbst als virtuelle einzelne VPN-Instanz bei einem entfernten VPN-Partner zu identifizieren.

Diese X.509-Zertifikate müssen regelmäßig erneuert werden. Wenn der VPN-Partner so eingestellt ist, dass er den Gültigkeitszeitraum der Zertifikate prüft, müssen diese erneuert werden, bevor ihre Gültigkeit erlischt (siehe „Zertifikatseinstellungen“ auf Seite 259).

Wenn ein Maschinenzertifikat ersetzt wird, werden alle VPN-Verbindung, die es nutzen, vom mGuard neu gestartet. Währenddessen kann der mGuard für eine bestimmte Zeit über die betroffenen VPN-Verbindungen keine Daten weiterleiten. Die Zeit hängt von der Anzahl der betroffenen VPN-Verbindungen, der Leistungsfähigkeit des mGuards und der VPN-Partner und der Latenzzeit der mGuards im Netzwerk ab.

Wenn dies für die Redundanz nicht tragbar sein sollte, müssten die VPN-Partner eines Redundanzpaares so konfiguriert werden, dass sie alle Zertifikate akzeptieren, deren Gültigkeit über einen Satz von bestimmten CA-Zertifikaten bestätigt wird (siehe „CA-Zertifikate“ auf Seite 263 und „Authentifizierung“ auf Seite 359).

Wählen Sie dazu unter *IPsec VPN* >> *Verbindungen* >> *Editieren* >> *Authentifizierung* bei dem Punkt *Remote CA-Zertifikat* die Einstellung **Alle bekannten CAs**.

Wenn das neue Maschinenzertifikat von einem anderen Sub-CA-Zertifikat herausgegeben wird, dann muss der VPN-Partner dieses kennen, bevor das Redundanzpaar das neue Maschinenzertifikat nutzt.

Das Maschinenzertifikat muss an beiden mGuards eines Redundanzpaars getauscht weden. Aber manchmal ist das nicht möglich, wenn einer nicht erreichbar ist. Dies kann zum Beispiel bei einem Netzwerkausfall geschehen. So kann der mGuard in Bereitschaft ein veraltetes Maschinenzertifikat haben, wenn er aktiv wird. Das ist ein weiterer Grund dafür, dass die VPN-Partner so eingestellt sein müssen, dass sie beide Maschinenzertifikate nutzen.

Normalerweise wird von dem VPN-Zustandsabgleich auch das Maschinenzertifikat mit dem passenden Schlüssel repliziert. Bei einem Failover kann der andere mGuard übernehmen und sogar den Aufbau unvollständiger ISAKMP SAs fortsetzen.

Remote-Zertifikate für eine VPN-Verbindung wechseln

Der mGuard kann so eingestellt werden, dass er VPN-Partner direkt über die X.509-Zertifikate authentifiziert, die diese vorweisen. Dafür muss dieses X.509-Zertifikat beim mGuard eingestellt sein. Es wird *Remote CA-Zertifikat* genannt.

Wenn ein Remote-Zertifikat erneuert wird, hat kurzfristig nur einer der mGuards ein neues Zertifikat. Wir empfehlen deshalb bei der VPN-Redundanz die VPN-Partner über CA-Zertifikate statt über Remote-Zertifikate zu authentifizieren.

Neues CA-Zertifikat hinzufügen, um VPN-Partner zu identifizieren

Der mGuard kann so eingestellt werden, das er VPN-Partner über CA-Zertifikate authentifiziert (siehe „CA-Zertifikate“ auf Seite 263 und „Authentifizierung“ auf Seite 359).

Wählen Sie dazu unter *IPsec VPN* >> *Verbindungen* >> *Editieren* >> *Authentifizierung* bei dem Punkt *Remote CA-Zertifikat* die Einstellung **Alle bekannten CAs**.

Bei dieser Einstellung kann ein neues CA-Zertifikat hinzugefügt werden, ohne die aufgebauten VPN-Verbindungen zu beeinflussen. Aber die neuen CA-Zertifikate werden sofort genutzt. Das X.509-Zertifikat, das der VPN-Partner nutzt, um sich beim mGuard zu authentifizieren kann dann mit einer minimalen Unterbrechung ausgetauscht werden. Es muss nur sichergestellt werden, dass das neue CA-Zertifikat zuerst verfügbar ist.

Der mGuard kann so eingestellt werden, dass er den Gültigkeitszeitraum der Zertifikate prüft, die vom VPN-Partner bereitgestellt werden (siehe „Zertifikatseinstellungen“ auf Seite 259). In diesem Fall ist es notwendig, dass neue vertrauenswürdige CA-Zertifikate zur Konfiguration des mGuards hinzugefügt werden. Diese Zertifikate sollten ebenfalls einen Gültigkeitszeitraum haben.

Wenn die CRL-Prüfung eingeschaltet ist (unter *Authentifizierung* >> *Zertifikate* >> *Zertifikatseinstellungen),* dann muss eine URL pro CA-Zertifikat vorgehalten werden, an der die entsprechende CRL verfügbar ist. Die URL und CRL müssen veröffentlicht werden, bevor der mGuard die CA-Zertifikate nutzt, um die Gültigkeit der von den VPN-Partnern vorgezeigten Zertifikate zu bestätigen.

Einsatz von X.509-Zertifikaten mit einem beschränkten Gültigkeitszeitraum und CRL-Prüfung

Der Einsatz von X.509-Zertifikaten wird unter „Zertifikatseinstellungen“ auf Seite 259 beschrieben (Menü *„Authentifizierung* >> *Zertifikate* >> *Zertifikatseinstellungen“*).

Wenn Sie X.509-Zertifikate einsetzen und dort **Beachte den Gültigkeitszeitraum von Zertifikaten und CRLs** eingestellt haben, dann muss die Systemzeit stimmen. Wir empfehlen, die Systemzeit mit einem vertrauenswürdigen **NTP-Server** zu synchronisieren. Jeder mGuard eines Redundanzpaars kann den anderen als NTP-Server nutzen, aber nicht als einzigen NTP-Server.

18 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 474). 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 19.

Der von IBM stammende und von der NSA überprüfte symmetrische Verschlüsselungsalgorithmus (→ „Symmetrische Verschlüsselung“ auf Seite 474) 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 473) Ein CA-Zertifikat kann herangezogen werden, um ein Zertifikat zu überprüfen, das die Signatur dieser CA trägt. Diese Prüfung macht nur dann Sinn, wenn davon auszugehen ist, dass das CA-Zertifikat aus authentischer Quelle stammt, also selber echt ist. Wenn darüber Zweifel bestehen, kann das CA-Zertifikat selber überprüft werden. Wenn es sich um ein Sub-CA-Zertifikat handelt, also ein CA-Zertifikat ausgestellt von einer Sub-CA (Sub Certificate Authority) - was normalerweise der Fall ist -, kann das CA-Zertifikat der übergeordneten CA benutzt werden, um das CA-Zertifikat der ihr untergeordneten Instanz zu überprüfen. Und gibt es für diese übergeordnete CA eine weitere CA, die ihr wiederum übergeordnet ist, kann deren CA-Zertifikat benutzt werden, um das CA-Zertifikat der ihr untergeordneten Instanz zu prüfen, usw. Diese Kette des Vertrauens setzt sich fort bis zur Wurzelinstanz, die Root-CA (Root Certificate Authority). Die CA-Datei der Root-CA ist zwangsläufig selbst signiert. Denn diese Instanz ist die höchste, und der „Anker des Vertrauens“ liegt letztlich bei ihr. Es ist niemand mehr da, der dieser Instanz bescheinigen kann, dass sie die Instanz ist, für die sie sich ausgibt. Eine Root-CA ist daher eine staatliche oder staatlich kontrollierte Organisation.

Der mGuard kann die in ihn importierten CA-Zertifikate benutzen, um die von Gegenstellen „vorgezeigten“ Zertifikate auf Echtheit zu überprüfen. Bei VPN-Verbindungen z. B. kann die Authentifizierung der Gegenstelle ausschließlich durch CA-Zertifikate erfolgen. Dann müssen im mGuard alle CA-Zertifikate installiert sein, um mit dem von der Gegenstelle vorgezeigten Zertifikat eine Kette zu bilden: neben dem CA-Zertifikat der CA, deren Signatur im zu überprüfenden vorgezeigten Zertifikat des VPN-Partners steht, auch das CA-Zertifikat der ihr übergeordneten CA usw. bis hin zum Root-Zertifikat. Denn je lückenloser diese „Kette des Vertrauens“ überprüft wird, um eine Gegenstelle als authentisch zu akzeptieren, desto höher ist die Sicherheitsstufe.

Client / Server

In einer Client-Server-Umgebung ist ein Server ein Programm oder Rechner, das vom Client-Programm oder Client-Rechner Anfragen entgegennimmt und beantwortet.

Bei Datenkommunikation bezeichnet man auch den Rechner als Client, der eine Verbindung zu einem Server (oder Host) herstellt. 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.

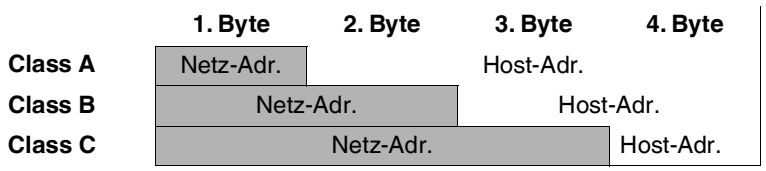
IP-Adresse

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 468) 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 473).

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 18-1 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 Ausstellers mit seinem Schlüssel übernimmt eine zertifizierende Stelle (*Certification Authority - CA*). Dies ge-

schieht 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 468)

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.

19 Anhang

19.1 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.net/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*** funktioniert nur im Zusammenspiel mit mGuard-Firmwareversionen < 8.4.0. Ab mGuard-Firmwareversion 8.4.0 kann das Kommandozeilen-Tool ***curl*** verwendet werden (Parameter und Optionen abweichend!).

Beispiel:

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

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

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

Tabelle 19-1 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

19.2 Kommandozeilen-Tool „mg“

Die folgenden Befehle können durch die Benutzer **root** und **admin** auf der Kommandozeile des mGuards ausgeführt werden.

Tabelle 19-2 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 94). **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/netmask	**Netzmaske der externen IP-Adresse.**

19.3 LED-Statusanzeige und Blinkverhalten

Das beschriebene Blinkverhalten bezieht sich auf Geräte der Gerätefamilie FL MGUARD RS 200x / FL MGUARD RS 400x und TC MGUARD RS 200x / TC MGUARD RS 400x.

19.3.1 Beschreibung der LEDs

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

Die Zustände werden durch permanentes oder temporäres Leuchten bzw. Blinken der LEDs angezeigt. Das angezeigte LED-Muster kann auch eine Kombination verschiedener Systemzustände darstellen.

ACHTUNG: Da mehrere Systemzustände nicht eindeutig, nur temporär oder in Kombination mit anderen Zuständen durch die LEDs angezeigt werden, müssen zusätzlich die Log-Dateien des mGuard-Geräts überprüft werden!

LED-Dioden der FL/TC MGUARD (RS200x/RS400x)-Geräte:

P1	Stat	Mod	Info2 (Sig)
●	●	●	●
●	●	●	●
P2	Err	Fault	Info1

P1 / P2

Die LEDs *P1* und *P2* zeigen an, welche der beiden Stromversorgungen angeschlossen ist (Geräte der FL/TC MGUARD RS2000-Serie: nur *P1* ist verfügbar).

Info2 / Info1 (die LED Sig wird nicht verwendet)

Über die LEDs *Info2* und *Info1* können aktive VPN-Verbindungen oder (ab Version 8.1) aktive Firewall-Regelsätze angezeigt werden. Die Aktivierung der LEDs durch eine bestimmte VPN-Verbindung oder einen bestimmten Firewall-Regelsatz wird auf der mGuard-Oberfläche im Menüpunkt **Verwaltung >> Servicekontakte** konfiguriert.

Die folgenden Zustände werden angezeigt:.

ON	Die VPN-Verbindung ist aufgebaut / der Firewall-Regelsatz ist geschaltet.
Blink	Die VPN-Verbindung wird auf- bzw. abgebaut oder wurde von der Gegenstellen gestoppt/deaktiviert.
OFF	Die VPN-Verbindung ist auf beiden Gegenstellen gestoppt/deaktiviert.

Stat / Mod / Err / Fault

Die LEDs *Stat*, *Mod*, *Err* und *Fault* zeigen Systemzustände (Status-, Alarm- oder Fehlermeldungen) an (siehe Tabelle 19-5).

Eine leuchtende **LED Fault** zeigt neben den Alarmmeldungen generell auch an, dass das Gerät aktuell nicht betriebsbereit ist.

LAN / WAN

Die LAN/WAN LEDs befinden sich in den LAN/WAN-Buchsen (10/100 und Duplex-Anzeige).

Die LEDs zeigen den Ethernet-Status des LAN- bzw. WAN-Interface. Sobald das Gerät am entsprechenden Netzwerk angeschlossen ist, zeigt ein kontinuierliches Leuchten an, dass eine Verbindung zum Netzwerkpartner im LAN bzw. WAN besteht. Beim Übertragen von Datenpaketen erlischt kurzzeitig die LED.

Wenn alle LAN-/WAN-LEDs leuchten, bootet das System.

Bargraph und SIM 1/2 (Mobilfunk)

Tabelle 19-3 Anzeigen des TC MGUARD RS4000 3G und TC MGUARD RS2000 3G

LED	**Zustand und Bedeutung**					
Bar-graph	LED 3	Oben	Aus	Aus	Aus	Grün
	LED 2	Mitte	Aus	Aus	Grün	Grün
	LED 1	Unten	Aus	Gelb	Gelb	Gelb
	Signalstärke (dBm)		–113 ... 111	–109 ... 89	–87 ... 67	–65 ... 51
	Netzempfang		Sehr schlecht bis kein	Ausreichend	Gut	Sehr gut
SIM 1	Grün	ON Blink	SIM-Karte 1 aktiv Keine oder falsche PIN eingegeben			
SIM 2	Grün	ON Blink	SIM-Karte 2 aktiv Keine oder falsche PIN eingegeben			

19.3.2 Leucht- und Blinkverhalten der LEDs.

Tabelle 19-4 Beschreibung des Leucht- und Blinkverhaltens der LED-Dioden

Heartbeat	Das Blinkverhalten ähnelt eine Herzschlag, bei dem zwei Schläge kurz hintereinander ausgeführt werden, gefolgt von einer kurzen Pause.
Running light	Drei Lichter bilden ein sich kontinuierlich wiederholendes Lauflicht von links nach rechts und wieder zurück.
Blink 50/1500	Blitzen mit 1500 ms Pause (50 ms an, dann 1500 ms aus)
Blink 50/800	Blitzen mit 800 ms Pause (50 ms an, dann 800 ms aus)
Blink 50/100	Blitzen mit 100 ms Pause (50 ms an, dann 100 ms aus)
Blink 500/500	Gleichmäßiges Blinken (500 ms an / 500 ms aus)
Morse code (. . . – – – . . .)	Das Blinkverhalten zeigt den *Morse-Code 'SOS'*, bei dem sich das Blinkverhalten "3x kurz, 3x lang, 3x kurz" fortlaufend wiederholt.
ON	Die Diode leuchtet permanent.
ON (n sec)	Die Diode leuchtet permanent für die angegeben Zeit (in Sekunden *n*)

19.3.3 Darstellung der Systemzustände

Die Systemzustände (Status-, Alarm- oder Fehlermeldungen), die über das Leucht- bzw. Blinkverhalten der LED-Dioden angezeigt werden, entnehmen Sie bitte Tabelle 19-5.

Tabelle 19-5 Durch das Leucht- und Blinkverhalten der LEDs dargestellte Systemzustände

STAT	MOD	Info 2 (Sig)	ERR	FAULT	Beschreibung des Systemzustands
Heart-beat					Der Systemstatus ist OK.
			ON		Ein schwerer Fehler ist aufgetreten.
ON (12 sec)	ON (3 sec)		ON (12 sec)	ON (12 sec)	Das System bootet.
Morse code					Die Lizenz zur Verwendung der Firmware fehlt.
Morse code			**Morse code**		Der Austausch des Bootloaders ist aufgrund eines Hardwaredefekts fehlgeschlagen.
				ON	Ein Fehler bei der Stromversorgung wurde festgestellt.
				ON	Keine Konnektivität auf der WAN-Schnittstelle (Linküberwachung am Gerät konfigurierbar)
				ON	Keine Konnektivität auf der LAN-Schnittstelle (Linküberwachung am Gerät konfigurierbar)
				ON	Keine Konnektivität auf der LAN(1-4)-Schnittstelle (Linküberwachung am Gerät konfigurierbar)
				ON	Keine Konnektivität auf der DMZ-Schnittstelle (Linküberwachung am Gerät konfigurierbar)
				ON	Spannungsversorgung 1 oder 2 ausgefallen (Alarm am Gerät konfigurierbar)
				ON	Temperatur zu hoch / zu niedrig (Alarm am Gerät konfigurierbar)
				ON	(Redundanz) Verbindungsprüfung fehlgeschlagen (Alarm am Gerät konfigurierbar)
				ON	(Modem) Verbindungsprüfung fehlgeschlagen (Alarm am Gerät konfigurierbar)
			ON (3 sec)		ECS: Das ECS ist inkompatibel.
			ON (3 sec)		ECS: Die Kapazität des ECS ist erschöpft.
			ON (3 sec)		ECS: Das Root-Passwort aus dem ECS stimmt nicht überein.
			ON (3 sec)		ECS: Die Konfiguration konnte nicht aus dem ECS geladen werden.
			ON (3 sec)		ECS: Die Konfiguration konnte nicht im ECS gespeichert werden.
	ON				PPPD: Das interne Modem hat eine Verbindung aufgebaut (eingestellt durch pppd).
	Blink 50/1500				PPPD: Das interne Modem ist aktiviert und erwartet eine Einwahl.
	Blink 500/500				PPPD: Das interne Modem wählt.
			ON (2 sec)		RECOVERY: Das Wiederherstellungsverfahren ist fehlgeschlagen.
ON (2 sec)					RECOVERY: Das Wiederherstellungsverfahren war erfolgreich.
ON				ON	FLASH-PROZEDUR: Die Flash-Prozedur wurde gestartet. Bitte warten.

Tabelle 19-5 Durch das Leucht- und Blinkverhalten der LEDs dargestellte Systemzustände

STAT	MOD	Info 2 (Sig)	ERR	FAULT	Beschreibung des Systemzustands
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		ON		FLASH-PROZEDUR: Die Flash-Prozedur / der Produktionsvorgang 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: Die Flash-Prozedur 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.