FL MGUARD 1000
Web-based Management
mGuardNT 1.8.x

Anwenderhandbuch

UM DE MGUARD NT

INSPIRING INNOVATIONS

Anwenderhandbuch

FL MGUARD 1000 – Web-based Management – mGuardNT 1.8.x

UM DE MGUARD NT, Revision 12 2024-05-22

Dieses Handbuch ist gültig für:

Bezeichnung	Artikel-Nr.
FL MGUARD 1102	1153079
FL MGUARD 1105	1153078

Firmware-Version: mGuardNT 1.8.x

Siehe auch *mGuardNT 1.8.x Firmware – Release Notes* für weitere Informationen.

108420_de_12

PHOENIX CONTACT GmbH & Co. KG • Flachsmarktstraße 8 • 32825 Blomberg • Germany
phoenixcontact.com

Inhaltsverzeichnis

1 Zu Ihrer Sicherheit

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

1.1 Kennzeichnung der Warnhinweise

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

Hier finden Sie zusätzliche Informationen oder weiterführende Informationsquellen.

1.2 Über dieses Handbuch

Folgende Elemente werden in diesem Handbuch verwendet:

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

1.3 Qualifikation der Benutzer

Der in diesem Handbuch beschriebene Produktgebrauch richtet sich ausschließlich an

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

1.4 Bestimmungsgemäße Verwendung

– Die Geräte der Serie FL MGUARD 1000 sind industrietaugliche Security-Router mit integrierter Stateful-Packet-Inspection-Firewall. Sie eignen sich für die dezentrale Absicherung von Produktionszellen oder einzelner Maschinen gegen Manipulationen.
– Das Gerät ist für die Installation im Schaltschrank vorgesehen.

1.5 Veränderung des Produkts

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

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

1.6 IT-Sicherheit

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

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

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

Weiterführende Informationen zu den im Folgenden genannten Maßnahmen erhalten Sie auf den folgenden Webseiten (letzter Zugriff am 15.04.2024):

– bsi.bund.de/it-sik.html
– ics-cert.us-cert.gov/content/recommended-practices

Verwenden Sie die jeweils aktuelle Firmware-Version

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

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

Verwenden Sie aktuelle Sicherheits-Software

- Um Sicherheitsrisiken wie Viren, Trojaner und andere Schad-Software zu erkennen und auszuschalten, installieren Sie auf allen PCs eine Sicherheits-Software.
- Stellen Sie sicher, dass die Sicherheits-Software immer auf dem aktuellen Stand ist und die neuesten Datenbanken nutzt.
- Nutzen Sie Whitelist-Tools zur Überwachung des Gerätekontexts.
- Um die Kommunikation Ihrer Anlage zu prüfen, nutzen Sie ein Intrusion-Detection-System.

Führen Sie regelmäßige Bedrohungsanalysen durch

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

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

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

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

Deaktivieren Sie nicht benötigte Kommunikationskanäle

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

Binden Sie Komponenten und Systeme nicht in öffentliche Netzwerke ein

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

Beschränken Sie die Zugangsberechtigung zum Gerät

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

Sichern Sie den Zugriff ab

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

Verwenden Sie bei Fernzugriff sichere Zugriffswege

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

Verwenden Sie eine Firewall

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

Aktivieren Sie eine sicherheitsrelevante Ereignisprotokollierung (Logging)

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

Schützen Sie den Zugriff auf die SD-Karte

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

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

1.7 Aktuelle Sicherheitshinweise zu Ihrem Produkt

Product Security Incident Response Team (PSIRT)

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

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

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

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

1.8 Support

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

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

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

Die Verwendung von Snapshots wird in diesem Anwenderhandbuch beschrieben.

2 Grundlagen mGuardNT

2.1 Geräteeigenschaften und Funktionsumfang

Tabelle 2-1 Geräteeigenschaften und Funktionsumfang

Geräteeigenschaften	FL MGUARD	
	1102	1105
HARDWARE		
2 Netzzonen (Netzwerkinterfaces)	x	x
Ethernet über RJ45-Anschlüsse (Übertragungsrate: 10/100/1000 MBit/s)	2	5
4-Port Unmanaged Switch (RJ45) (*Bridge Mode*)	-	x
Service Ein- und Ausgänge (IOs)	x	x
SD-Kartenhalter	x	x
NETZWERK		
Stealth-Modus	x	x
Router-Modus	x	x
Paketweiterleitung (Router-Modus)		
Security-Router	x	x
IP-Masquerading (NAT)	x	x
Port-Weiterleitung	x	x
1:1-NAT	x	x
Zusätzliche statische Routen	x	x
Netzwerkdienste (Client/Server)		
DHCP	x	x
DNS	x	x
NTP	x	x
SNMP (nur Server)	x	x
HTTPS – WBM/*Config API* – (nur Server)	x	x
FIREWALL		
Stateful-Packet-Inspection Firewall	x	x
Firewall (für durchgehenden Datenverkehr)	x	x
Gerätezugriff (für eingehenden Datenverkehr)	x	x
Integritätsprüfung von Datenpaketen zur Erhöhung der Netzwerksicherheit	x	x
Easy Protect Mode Automatischer Schutz der angeschlossenen Netzwerk-Clients ohne Konfigurationsaufwand direkt nach Anschluss des Geräts.	x	x

Tabelle 2-1 Geräteeigenschaften und Funktionsumfang

Geräteeigenschaften	FL MGUARD	
	1102	1105
Firewall Assistant Analyse des Datenverkehrs zur automatischen Erstellung von Firewall-Regeln.	x	x
Firewall-Test-Mode Analyse des Datenverkehrs zur automatisierten Erweiterung bestehender Firewall-Regeln.	x	x
MANAGEMENT		
Administration über Web-based Management (WBM)	x	x
Administration über RESTful Configuration API (*Config API*)	x	x
Lesen-Zugriff auf wichtige Geräteparameter über SNMP	x	x
Firmware-Update über WBM, *Config API* und Smart-Mode	x	x
Rollenbasierte Benutzerverwaltung (WBM und *Config API*)	x	x
Benutzer-Authentisierung über LDAP-Server	x	x
Smart-Mode Der Zugriff auf bestimmte Management-Funktionen erfolgt über die Mode-Taste direkt am Gerät, ohne dass ein Zugriff auf ein Management-Interface besteht.	x	x
Sichern und Wiederherstellen von Konfiguration und Benutzerverwaltung via SD-Karte	x	x
Sichern und Wiederherstellen der Konfiguration via WBM	x	x
Support-Tools		
TCP-Dump (Paketdatenanalyse)	x	x
Ping (Netzwerkanalyse)	x	x
Log-Viewer (Auswertung von Log-Einträgen)	x	x
Remote-Logging (*Syslog*)	x	x
Support-Snapshot (Zustands- und Fehleranalyse)	x	x

2.2 Änderungen gegenüber der Vorversion

Für eine detaillierte Übersicht über alle Änderungen der jeweiligen Version siehe entsprechende *Release Notes*.

Die *Release Notes* der aktuellen Version sind im Download-Bereich der entsprechenden Produktseite im Web-Shop erhältlich, z. B. phoenixcontact.net/product/1153079.

2.2.1 Neu in mGuardNT 1.8

- Connection-Tracking-Helper (FTP)
- Zahlreiche Verbesserungen im Bereich Security.

2.2.2 Neu in mGuardNT 1.7

- Zahlreiche Verbesserungen im Bereich Security.

2.2.3 Neu in mGuardNT 1.6

- Zahlreiche Verbesserungen im Bereich Security (z. B.)
  - Über den PSIRT-Prozess gefundene Sicherheitslücken (CVEs) wurden behoben
  - Das Gesamtsystem wurde weiter gehärtet
- Zahlreiche Verbesserungen im Bereich Bedienbarkeit (z. B.)
  - Die Zuordnung von Log-Einträgen zu Kategorien/Komponenten wurde verbessert
  - Die Zeitangaben in Log-Einträgen entsprechen der eingestellten Zeitzone
  - Der Inhalt des Snapshot wurde erweitert
  - Doppelte Einträge in Firewall-Tabellen können einfach entfernt werden

2.2.4 Neu in mGuardNT 1.5

- IP-Masquerading (NAT) in beide Richtungen (Netzzone 1 ← → Netzzone 2)
- Benutzersperrung (automatisch/manuell)
- Konfiguration sichern und wiederherstellen (Download/Upload via WBM)
- Konfigurierbarer Hostname
- Neustart des Geräts via WBM und *Config API*
- Zahlreiche Verbesserungen in den Bereichen Performance und Security
- Zahlreiche Verbesserungen im Bereich Bedienbarkeit

2.2.5 Neu in mGuardNT 1.4

- Benutzer- und Rollenverwaltung
- LDAP-Authentifizierung (LDAP-Client)
- SNMP-Server
- Port-Bereiche in Firewall-Regeln
- NAT-Funktionalität für Netzwerke
- Remote-Logging (*Syslog*)
- Externer Konfigurationsspeicher (auf SD-Karte)
- Konfigurierbarer *Session Timeout*

2.2.6 Neu in mGuardNT 1.3

- Erweiterte Firewall-Funktionalität:
  - Easy Protect Mode
  - Firewall Assistant
  - Firewall-Test-Mode

2.2.7 Neu in mGuardNT 1.2

- Erweiterte Netzwerk-Funktionalität
  - Stealth-Mode

2.2.8 Neu in mGuardNT 1.1

- Router- und Firewall-Funktionalitäten hinzugefügt

2.3 Verwendete Verschlüsselungsalgorithmen

Manche Funktionen des Geräts bieten die Möglichkeit der verschlüsselten Kommunikation. Das Gerät verwendet in diesem Fall grundsätzlich das Verschlüsselungsprotokoll “TLS“ (*Transport Layer Security*). Einstellungen siehe Tabelle 2-2 und 2-3.

Aus Sicherheitsgründen sollten alle beteiligten Clients und Server bei der verschlüsselten Kommunikation immer eine aktuelle TLS-Einstellung verwenden.

TLS-Einstellungen, die vom Gerät verwendet werden:

Tabelle 2-2 TLS-Einstellungen: HTTPS-Interface (WBM/Config API)

Einstellung	Wert
Protocols	TLS 1.2 / TLS 1.3
Cipher suites (TLS 1.3)	TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256
Cipher suites (TLS 1.2)	ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-CHACHA20-POLY1305
Certificate type	ECDSA (P-256)
TLS curves (TLS 1.3)	X25519 prime256v1 secp384r1
TLS curves (TLS 1.2)	secp384r1
Cipher preference	client chooses

Tabelle 2-3 TLS-Einstellungen: Remote-Logging / LDAP-Authentifizierung

Einstellung	Wert
Protocols	TLS 1.2 / TLS 1.3
Cipher suites (TLS 1.3)	TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256
Cipher suites (TLS 1.2) **(Remote-Logging)**	ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-CHACHA20-POLY1305 DHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES256-GCM-SHA384
Cipher suites (TLS 1.2) **(LDAP-Authentifizierung)**	ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-CHACHA20-POLY1305
TLS curves (TLS 1.2 / TLS 1.3)	X25519 prime256v1 secp384r1

2.4 Netzwerk

Als Router bzw. Gateway verbindet das Gerät Subnetze bzw. Netzzonen. Für jede Netzzone ist eine eigene IP-Adresse konfiguriert, über die das Gerät im Netzwerk erreichbar ist (siehe Kapitel 6.1, „Interfaces“).

Über die NAT-Funktionen (IP-Masquerading, 1:1-NAT, Port-Weiterleitung) können einzelne Maschinen (SPS) oder mehrere Subnetze mit gleicher IP-Konfiguration leicht in ein bestehendes Netzwerk eingebunden werden, ohne dass die IP-Konfiguration der Maschine bzw. der Subnetze geändert werden muss.

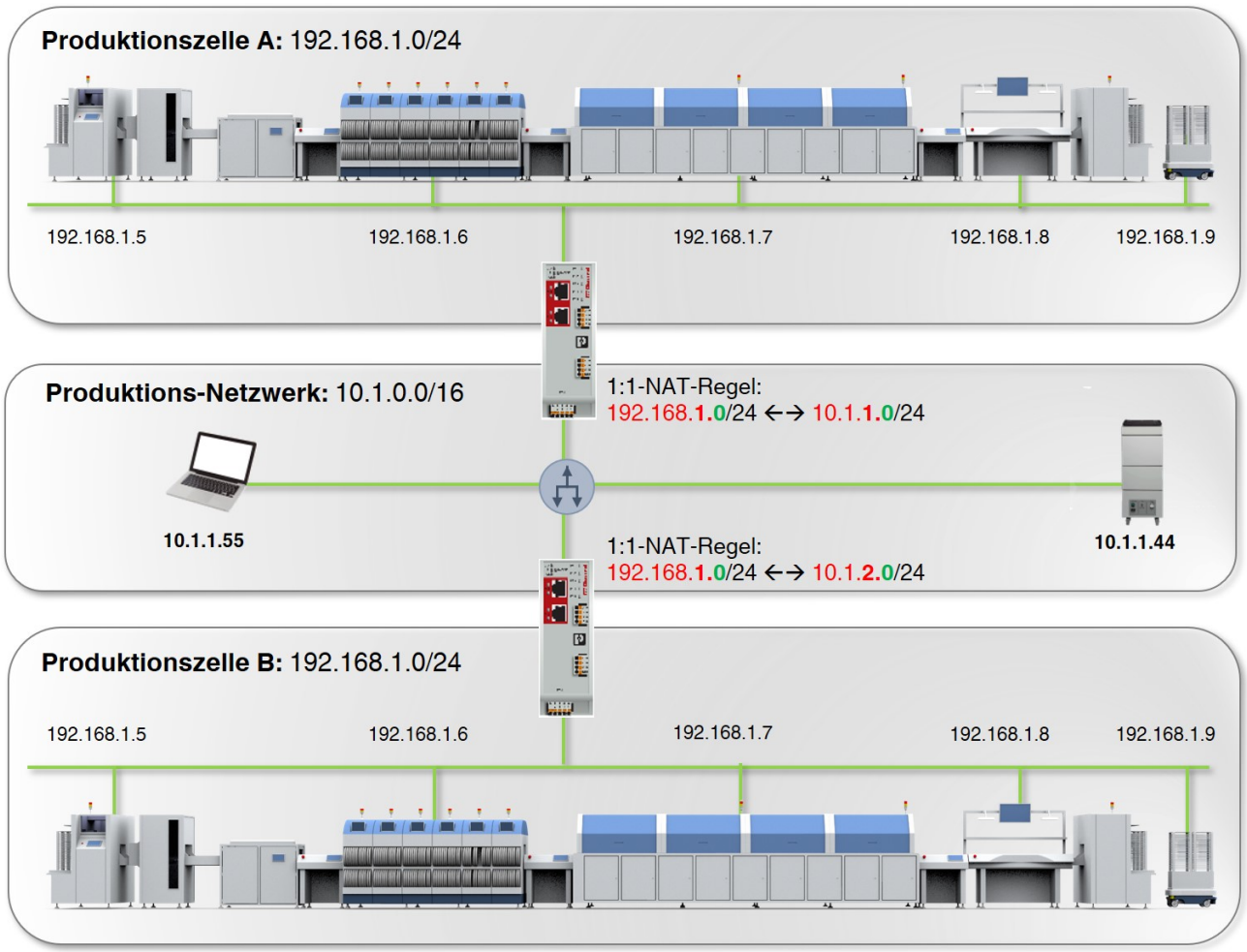


Bild 2-1 Das Gerät als NAT-Router einsetzen (Beispiel: 1:1-NAT)

2.5 Firewall

Die Firewall des Geräts ist genau genommen ein Paketfilter, der Datenpakete, die durch das Gerät durchgeleitet (*geroutet*) werden, analysiert und entsprechend der konfigurierten Firewall-Regeln weiterleitet oder blockiert (siehe Kapitel 7, „Menü: Netzwerksicherheit“).

Stateful-Packet-Inspection-Firewall

Der Paketfilter von mGuardNT funktioniert als *Stateful-Packet-Inspection*-Firewall. Das heißt, Antwortpakete passieren die Firewall automatisch, wenn sie einer zugehörigen und bereits akzeptierten Anfrage zweifelsfrei zugeordnet werden können. Firewall-Regeln werden deshalb grundsätzlich nicht auf Antwortpakete angewendet.

Firewall-Funktionen

Die Firewall kann auf unterschiedliche Arten genutzt und konfiguriert werden.

Tabelle 2-4 Nutzungsmöglichkeiten der mGuard-Firewall

Keine Konfiguration erforderlich	
Easy Protect Mode (siehe Kapitel 2.6)	Netzwerk-Clients werden direkt nach dem Anschließen des Geräts vor externen Zugriffen geschützt, ohne dass Firewall-Regeln selbst erstellt werden müssen.
Konfiguration über Web-based Management (WBM) oder Config API erforderlich	
Firewall (Paketfilter) (siehe Kapitel 7.1)	Firewall-Regeln werden manuell erstellt und erweitert. Die Regeln werden in eine Firewall-Tabelle des Geräts eingetragen und dort konfiguriert.
Firewall Assistant (siehe Kapitel 7.3)	Der Firewall Assistant analysiert und erfasst während eines beliebigen Zeitraums den Datenverkehr, der durch das Gerät durchgeleitet (*geroutet*) wird (**Netzzone 1 ←→ Netzzone 2**). Aus den erfassten Paketdaten werden Firewall-Regeln abgeleitet, die beim Beenden des Firewall Assistant automatisch in die Firewall-Tabellen des Geräts eingetragen werden.
Firewall-Test-Mode (siehe Kapitel 7.1, „Firewall-Test-Mode“)	Ungewollt durch die Firewall abgelehnter Datenverkehr kann einfach identifiziert und durch die automatisierte Erstellung entsprechender Firewall-Regeln erlaubt werden. Der Benutzer wird durch eine Alarmierung von dem Ereignis (Datenverkehr, der nicht über eine bestehende Firewall-Regel erfasst wird) in Kenntnis gesetzt.

2.6 Easy Protect Mode

Wird das Gerät im *Easy Protect Mode* gestartet, schützt es **automatisch** alle an Netzzone 2 (XF2–XF5) angeschlossenen Netzwerk-Clients vor externen Zugriffen (z. B. einzelne Maschinen oder über einen Switch angeschlossene Produktionszellen).

Für weitere Informationen siehe auch Anwenderhandbuch „*FL MGUARD 1000 – Installation und Inbetriebnahme*“, erhältlich unter phoenixcontact.net/product/1153079.

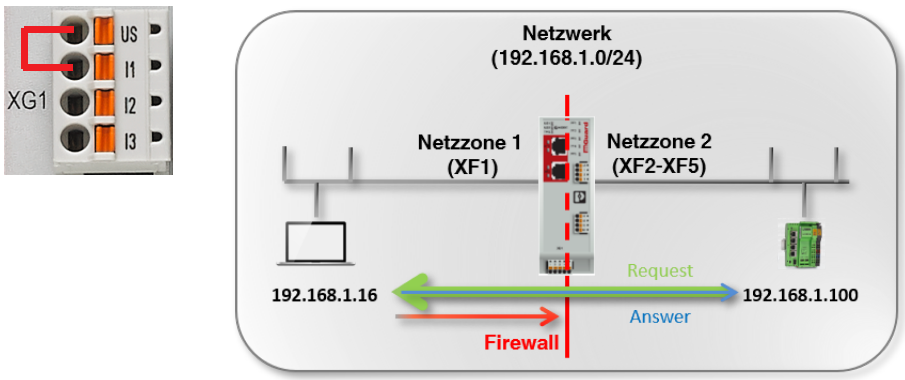


Bild 2-2 Aktivierter *Easy Protect Mode* (mittels Kabelbrücke)

Der *Easy Protect Mode* wird mittels einer Kabelbrücke aktiviert (siehe Bild 2-2)

Das Gerät wird über seine Netzzonen 1 und 2 bzw. XF1 und (XF2–XF5) in das bestehende Netzwerk eingefügt, ohne dass die bestehende Netzwerkkonfiguration der angeschlossenen Geräte geändert werden muss. Die Geräte in Netzzone 2 sind automatisch geschützt.

Eine Konfiguration des mGuard-Geräts ist grundsätzlich nicht notwendig und aufgrund der fehlenden Zugriffsmöglichkeit über das Web-based Management (HTTPS) auch nicht möglich.

Im *Easy Protect Mode* können Firmware-Updates über die Smart-Mode-Funktion „Update von SD-Karte“ durchgeführt werden (siehe Kapitel A 2, „Smart-Mode verwenden“).

3 Web-based Management verwenden

3.1 Netzwerkverbindung zum Gerät herstellen

Stellen Sie eine Verbindung zwischen dem Konfigurations-Rechner und dem Netzwerkinterface (XF2 / Netzzone 2) des Geräts her.

Werkseitige Voreinstellung (Netzwerkinterface: XF2)

– IP-Adresse: 192.168.1.1
– Subnetzmaske: 24 (255.255.255.0)
– Der DHCP-Server des Geräts ist aktiviert und über XF2 / Netzzone 2 erreichbar.

Für weitere Informationen siehe auch Anwenderhandbuch „*FL MGUARD 1000 – Installation und Inbetriebnahme*“, erhältlich unter phoenixcontact.net/product/1153079.

3.2 Benutzer anmelden

Vermeiden Sie konkurrierende Sitzungen
Die konkurrierende Anmeldung von Benutzern von unterschiedlichen Instanzen aus kann zu einem Datenverlust oder zu Problemen bei der Benutzerverwaltung führen.

Benutzersperrung
Ein Benutzer kann aufgrund mehrerer erfolgloser Anmeldeversuche oder durch einen Administrator gesperrt werden. Gesperrte Benutzer können sich nicht am Gerät anmelden. Kontaktieren Sie in diesem Fall einen Administrator mit entsprechender Berechtigung.

Hinweis: Wurde ein Benutzer automatisch gesperrt, kann die temporäre Sperre durch einen Administrator mit der Rolle „*Super Admin*“ oder durch einen Neustart des Geräts vorzeitig aufgehoben werden.

• Geben Sie z. B. folgende Web-Adresse in einen Webbrowser ein, um das WBM zu starten: **https://192.168.1.1** (werkseitige Voreinstellung für „XF2“)

⇒ Die Anmeldeseite wird geöffnet.

In der werkseitigen Voreinstellung kann sich folgender Benutzer am Gerät anmelden:

– Benutzername: *admin;* Passwort: *private*

Ändern Sie bei der Erstinbetriebnahme des Geräts umgehend das voreingestellte Administrator-Passwort (siehe Kapitel 5.1).

⇒ Nach erfolgreicher Anmeldung erscheint die folgende Startseite.

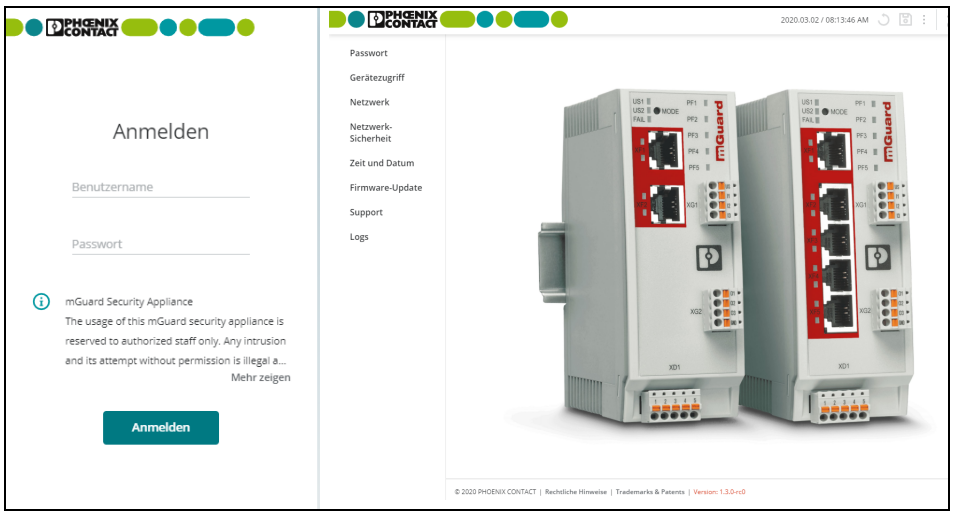


Bild 3-1 Web-based Management: Anmeldeseite (links) und Startseite (rechts)

3.2.1 Das Benutzerpasswort ist nicht mehr bekannt

Was ist zu tun, wenn Passwörter nicht mehr bekannt sind?

Sollten die Passwörter sämtlicher Benutzer nicht mehr bekannt und damit eine Anmeldung am Gerät nicht mehr möglich sein, muss das Gerät gegebenenfalls in die werkseitige Voreinstellung zurückgesetzt werden.

ACHTUNG: Datenverlust
Die gesamte Konfiguration, alle Einstellungen und Benutzer sowie deren Passwörter werden damit unwiderruflich gelöscht.

Führen Sie hierzu die Smart-Mode-Funktion „*Wiederherstellung der Werkseinstellung*“ aus (siehe Kapitel A 2).

3.3 Benutzer abmelden

Bild 3-2 Benutzer abmelden

Um den aktuellen Benutzer vom Gerät abzumelden, gehen Sie wie folgt vor:

- Klicken Sie auf das Icon .

⇒ Der Benutzer wird abgemeldet.

⇒ Alle Informationen der aktuellen Sitzung werden gelöscht.

⇒ Der Benutzer wird auf die Anmeldeseite weitergeleitet.

3.3.1 Automatische Abmeldung

Eine automatische Abmeldung erfolgt unter folgenden Bedingungen:

– Die Sitzung ist abgelaufen (*Session timeout*).

– Das Gerät wird neu gestartet.

– Der Benutzer wird aus der Benutzerverwaltung entfernt.

3.3.2 Ablauf der Sitzung (Timeout)

Die Sitzung eines Benutzers wird durch einen *Session timeout* zeitlich begrenzt. Die konfigurierbare Zeitspanne des *Session timeouts* liegt zwischen 5 Minuten und 8 Stunden. Nach Ablauf der Sitzung wird der Benutzer automatisch abgemeldet.

Der *Session timeout* startet mit der Anmeldung des Benutzers (werkseitige Voreinstellung: 30 Minuten). Führt der Benutzer während einer laufenden Sitzung eine Aktion durch, wird der *Session timeout* jeweils auf den konfigurierten Ausgangswert zurückgesetzt (siehe Kapitel 4.5).

3.4 Automatische Benutzersperre

Ein Benutzer wird nach einer konfigurierbaren Anzahl (2 – 200) erfolgloser Anmeldeversuche automatisch für bis zu 8 Stunden gesperrt.

Die Sperre ist konfigurierbar (siehe Kapitel 4.5) und kann durch einem Administrator mit der Rolle „*Super Admin*“ vorzeitig aufgehoben werden (siehe Kapitel 5.1).

Eine automatische Sperre wird ebenfalls durch einen Neustart des Geräts aufgehoben.

3.5 Benutzer-Passwort ändern

Bild 3-3 Passwort des angemeldeten Benutzers ändern

Das Passwort eines lokal angemeldeten Benutzers kann von diesem selbstständig geändert werden.

Sollte Ihnen das eigene Passwort nicht mehr bekannt sein, kann es von einem anderen Benutzer mit entsprechender Berechtigung geändert und neu zugewiesen werden (siehe Kapitel 5.1).

Gehen Sie wie folgt vor:

- Klicken Sie auf das Icon (Benutzereinstellungen) am oberen rechten Bildschirmrand.

⇒ Das Dialogfenster zum Ändern des Passworts wird geöffnet.

- Füllen Sie die drei Pflichtfelder aus.

Aktuelles Passwort	Das bestehende Passwort des angemeldeten Benutzers, das geändert werden soll.
Neues Passwort	Das neue Passwort für den angemeldeten Benutzer. **Eingabeformat:** Um die Sicherheit zu erhöhen, sollte das Passwort Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen enthalten. Erlaubte Zeichen (min. 6, max. 64): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
Neues Passwort bestätigen	Wiederholte Eingabe des neuen Passworts.

- Übernehmen Sie die Passwortänderung durch einen Klick auf die Schaltfläche **Passwort ändern.**

⇒ Das Passwort wird geändert und muss bei einer erneuten Anmeldung angegeben werden.

ACHTUNG: Ändern Sie das Administrator-Passwort bei der Erstanmeldung
Ändern Sie bei der ersten Anmeldung umgehend das werkseitig voreingestellte Administrator-Passwort des Benutzers „*admin*“ (Passwort = *private*).

3.6 Hilfe zur Konfiguration

3.6.1 Seitenaufbau und Funktion

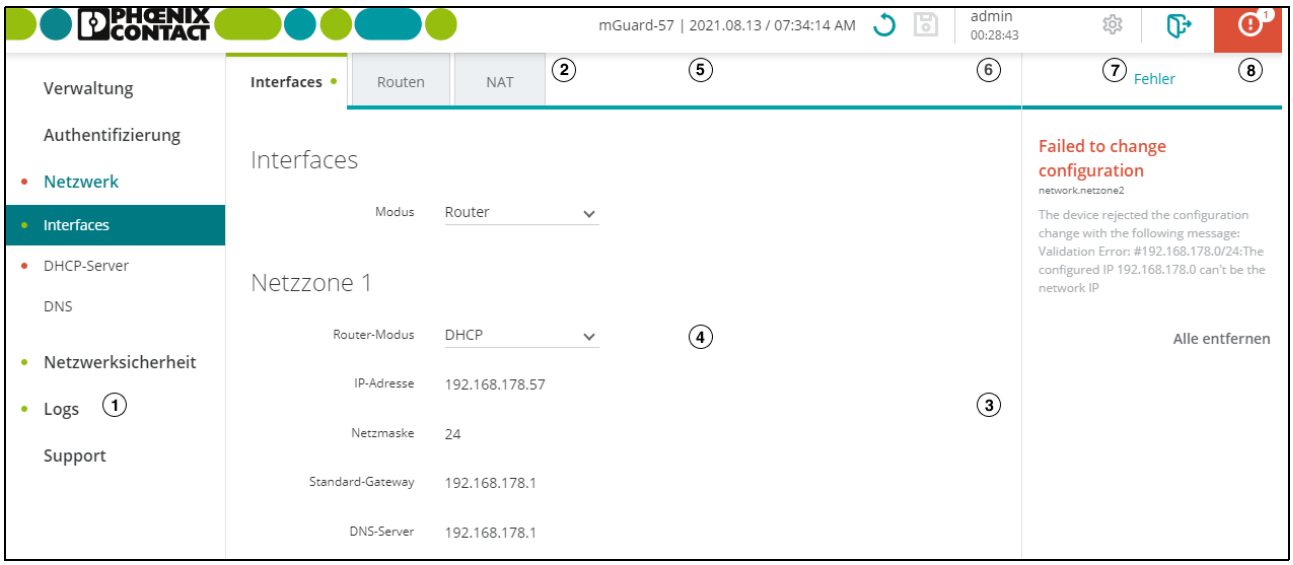


Bild 3-4 Web-based Management: Menüstruktur und Seitenelemente

Menüstruktur ①

Über die Haupt- und Untermenüstruktur können die einzelnen Konfigurationsseiten aufgerufen werden. Konfigurationsseiten unterteilen sich häufig in mehrere Unterseiten, die über Registerkarten (*Tabs*) aufgerufen werden können.

Registerkarten ②

Registerkarten (*Tabs*) können über die Registerkarten-Leiste am oberen Bildschirmrand ausgewählt werden.

Konfigurationsseite ③

In dem Hauptfenster einer Konfigurationsseite können die Parameter der einzelnen Variablen geändert werden.

Variablen ④

Variablenwerte können über ein Drop-down-Menü oder eine Checkbox ausgewählt oder manuell eingetragen werden.

Abhängig von der Variablen können Buchstaben, Ziffern und/oder bestimmte Sonderzeichen verwendet werden. Einige Variablen werden in Tabellen eingetragen (z. B. Firewall- und 1:1-NAT-Regeln).

Hostname / Systemzeit ⑤

Der konfigurierte Hostname (links) und die aktuelle Systemzeit (rechts) werden angezeigt.

Ablauf der Sitzung (Timeout) ⑥

Ein angemeldeter Benutzer wird nach Ablauf der Sitzung (*Session Timeout*) automatisch abgemeldet (siehe Kapitel 3.3).

Benutzer-Einstellungen ⑦

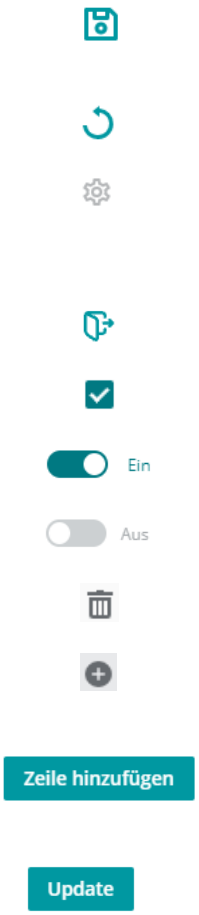
Die Einstellungen des aktuell angemeldeten Benutzers, z. B. dessen Passwort, können geändert werden.

Fehlermeldung (Server) ⑧

Fehlermeldungen, die nicht bereits bei der Eingabe festgestellt werden können, werden als Server-Antwort am rechten Bildschirmrand angezeigt (siehe Kapitel 3.6.3).

3.6.2 Icons und Schaltflächen

Folgende Beispiele zeigen Icons und Schaltflächen, die im WBM zur Verfügung stehen.



- Klicken Sie auf das **Icon „Speichern“**, um alle Änderungen, die Sie auf einer Konfigurationsseite oder in unterschiedlichen Menüpunkten vorgenommen haben, zu übernehmen.
- Klicken Sie auf das **Icon „Änderungen verwerfen“**, um alle nicht gespeicherten Änderungen zu verwerfen.
- Klicken Sie auf das **Icon „Einstellungen“**, um die Einstellungen des aktuelle angemeldeten Benutzers zu ändern.
- Das Passwort des aktuell angemeldeten Benutzers kann an dieser Stelle geändert werden.
- Klicken Sie auf das **Icon „Abmelden“**, um den aktuellen Benutzer vom Gerät abzumelden und die Sitzung zu beenden.
- Setzen Sie das Häkchen der **Checkbox**, um eine Funktion zu aktivieren.
- Schieben Sie den **Umschalter** in die Position **Ein**, um eine Funktion zu aktivieren.
- Schieben Sie den **Umschalter** in die Position **Aus**, um eine Funktion zu deaktivieren.
- Klicken Sie auf das **Icon „Mülleimer“**, um die ausgewählte Tabellenzeile zu löschen.
- Klicken Sie auf das **Icon „Plus“**, um die ausgewählte Tabellenzeile (*Test-Mode-Alarme*) als neue Firewall-Regel in die zugehörige Firewall-Tabelle zu übertragen.
- Klicken Sie auf die Schaltfläche **Zeile hinzufügen**, um eine neue Tabellenzeile unter der untersten bestehenden Zeile einzufügen.
- Klicken Sie auf die **Schaltfläche „Update“**, um ein Update-File auszuwählen und unmittelbar anzuwenden.

3.6.3 Fehlermeldungen

Kann ein Fehler nicht bereits bei der Eingabe, sondern erst bei einem Speicherversuch festgestellt werden, wird die Übernahme aller geänderten Werte abgebrochen.

Das Icon am oberen rechten Bildschirmrand zeigt Ihnen an, dass ein oder mehrere Konfigurationsfehler vorliegen. Klicken Sie auf das Icon , um sich die entsprechenden Fehlermeldungen in der rechten Seitenspalte anzeigen zu lassen (siehe Bild 3-4).

Korrigieren Sie die Eingaben und übernehmen Sie die geänderten Werte mit einem Klick auf das Icon .

3.6.4 Werte eingeben und ändern

Ändern von Werten

Um den Wert einer Variablen zu ändern und abzuspeichern, müssen Sie die Änderung mit einem Klick auf das Icon übernehmen.

Es ist möglich, auf einer Konfigurationsseite zunächst mehrere Werte zu ändern und diese dann mit einem Klick auf das Icon gemeinsam zu übernehmen.

Anzeige von geänderten Werten

Geänderte Werte, die noch nicht übernommen wurden, werden in der Oberfläche durch einen grünen Punkt markiert angezeigt. Die Markierung erscheint an entsprechender Stelle im Hauptmenü, Untermenü und auf der zugehörigen Registerkarte (siehe Bild 3-4).

Eingabe unzulässiger Werte

Die Übernahme unzulässiger Variablenwerte ist nicht möglich. Eine entsprechende Fehlermeldung wird in der Regel schon bei der Eingabe angezeigt.

Zusätzlich werden unzulässige Eingaben in der Oberfläche durch einen roten Punkt markiert angezeigt. Die Markierung erscheint an entsprechender Stelle im Hauptmenü, Untermenü und auf der zugehörigen Registerkarte (siehe Bild 3-4).

Korrigieren Sie die Eingaben und übernehmen Sie die geänderten Werte mit einem Klick auf das Icon.

Bereiche eingeben

Manche Werte können als Bereich angegeben werden. Die Eingabe eines Bereichs erfolgt, indem der Anfang und das Ende des Bereichs durch einen Doppelpunkt getrennt angegeben werden (Start:Ende).

Beispiel (Port-Bereich): startport:endport -->110:220

3.6.5 Änderungen verwerfen

Änderungen vor dem Übernehmen verwerfen
Werte, die an beliebiger Stelle neu eingegeben oder geändert, aber noch nicht übernommen wurden, können mit einem Klick auf das **Icon „Änderungen verwerfen“** verworfen werden.

3.6.6 Gerätekonfiguration vollständig und sicher löschen

Gerät auf Werkseinstellungen zurücksetzen
Damit keine geschützten Daten bei der Außerbetriebnahme auf dem Gerät verbleiben und von unbefugten Dritten eingesehen werden können, müssen alle Daten sicher und unwiderruflich gelöscht werden.

Führen Sie den Smart-Mode „Wiederherstellen der Werkseinstellung“ aus, um alle Daten auf dem Gerät sicher und unwiderruflich zu löschen (siehe Kapitel A 2, „Smart-Mode verwenden“).

3.6.7 Mit Tabellen arbeiten

Einige Einstellungen von mGuardNT werden als Datensatz gespeichert. Die Parameter und deren Werte werden im WBM in diesem Fall in Tabellenzeilen eingetragen.

Beachten Sie unbedingt die Reihenfolge der Tabellenzeilen
Bei der Anwendung von Firewall-Regeln ist die Reihenfolge der Tabellenzeilen entscheidend:
Die Firewall-Regeln in der Tabelle werden immer in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Nachfolgende Regeln werden dann nicht mehr berücksichtigt (siehe „Verhalten und Auswirkung von Firewall-Regeln“).

Einfügen einer Tabellenzeile (am Ende der Tabelle)

- Klicken Sie auf die Schaltfläche **Zeile hinzufügen**.

⇒ Eine neue Zeile wird unter der untersten bestehenden Zeile eingefügt.

- Klicken Sie auf das Icon , um die Änderung zu übernehmen.

Einfügen einer Tabellenzeile (unter einer bestehenden Tabellenzeile)

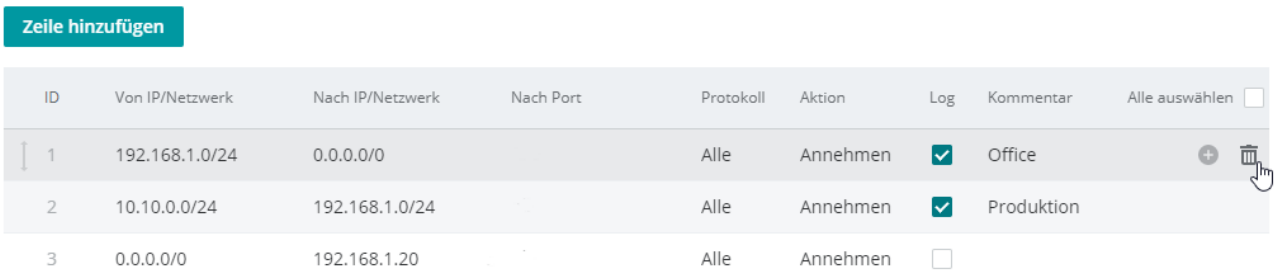
- Bewegen Sie den Mauszeiger über die Tabellenzeile, unter der Sie eine neue Zeile einfügen möchten.
- Klicken Sie auf das Icon .

⇒ Eine neue Zeile wird unter der bestehenden Zeile eingefügt.

- Klicken Sie auf das Icon , um die Änderung zu übernehmen.

Löschen einer Tabellenzeile

- Bewegen Sie den Mauszeiger über die Tabellenzeile, die Sie löschen möchten.
- Klicken Sie auf das Icon .



⇒ Die Zeile wird entfernt.

- Klicken Sie auf das Icon , um die Änderung zu übernehmen.

⇒ Die Tabellenzeile und der Datensatz wurden gelöscht.

Löschen mehrerer Tabellenzeilen

Durch das Drücken der *Strg*-Taste bzw. der *Shift*-Taste (Umschalttaste) und dem gleichzeitigen Klicken auf die ID-Nummern von Firewall-Regeln können mehrere Regeln bzw. ein Bereich von Regeln ausgewählt werden.

⇒ Die ausgewählten Regeln sind grün hinterlegt.

⇒ Die Anzahl der ausgewählten Regeln wird angezeigt.

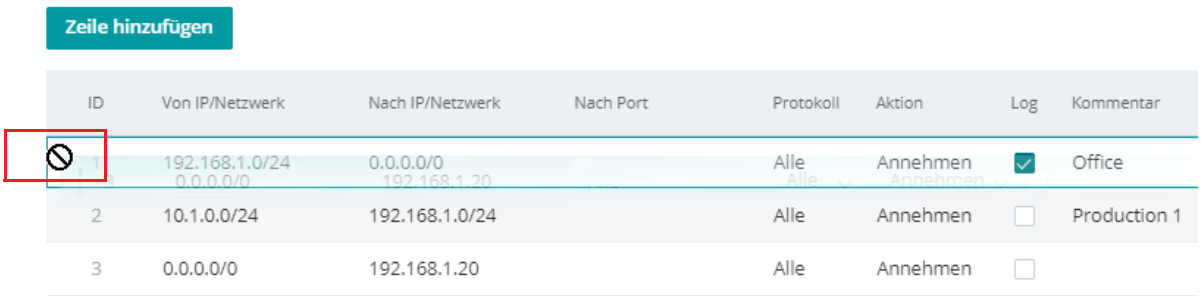
- Klicken Sie auf **Löschen**, um die ausgewählten Regeln zu löschen.
- Klicken Sie auf das Icon , um die Änderung zu übernehmen.

⇒ Die ausgewählten Tabellenzeilen und die zugehörigen Datensätze wurden gelöscht.

Verschieben einer Tabellenzeilen

- Bewegen Sie den Mauszeiger an die linke Seite der Tabellenzeile, die Sie verschieben möchten, bis der Zeiger zu einem Hand-Symbol wird.

- Klicken Sie in die Zeile und verschieben die Zeile bei gedrückter Maustaste an die gewünschte Position.



- Lassen Sie die Maustaste los.

⇒ Die Zeile wurde an eine neue Position verschoben.

- Klicken Sie auf das Icon , um die Änderung zu übernehmen.

3.6.8 Eingabe und Schreibweise: Netzmaske und Netzwerk

Netzmaske

Die Netzmaske kann wahlweise in einer der folgenden Schreibweisen angeben werden:

– numerisch (z. B. 24)
– dezimal (z. B. 255.255.255.0)

Im Web-based Management wird die dezimale Schreibweise bei einer Eingabe automatisch in die numerische Schreibweise umgewandelt (z. B. 255.255.0.0 --> 16).

Netzwerk

Ein Netzwerk muss in der CIDR-Schreibweise angegeben werden, z. B. 192.168.1.0/24, (siehe Kapitel 3.6.9).

Wird ein Netzwerk in einer der in Tabelle 3-1 dargestellten Schreibweisen im Web-based Management eingegeben, wird die Eingabe automatisch entsprechend umgewandelt.

Tabelle 3-1 Beispiele für die Umwandlung der Schreibweise von Netzwerken im WBM

Eingegebene Schreibweise	Umgewandelte Schreibweise
10.1.1.1/32	10.1.1.1
10.1.1.1/24	10.1.1.0/24
10.1.1.1/16	10.1.0.0/16
10.1.1.1/8	10.0.0.0/8
10.1.1.1/0	0.0.0.0/0

Hinweis: In der Config API darf die Netzmaske **/32** nicht verwendet werden. Die IP-Adresse muss stattdessen ohne Netzmaske angegeben werden.

3.6.9 CIDR (Classless Inter-Domain Routing)

IP-Netzmasken und CIDR fassen mehrere IP-Adressen zu einem Adressraum zusammen. Dabei wird ein Bereich von aufeinanderfolgenden Adressen als ein Netzwerk behandelt. Um einen Bereich von IP-Adressen anzugeben, müssen Sie den Adressraum in der CIDR-Schreibweise angeben (z. B. bei der Konfiguration der Firewall).

Tabelle 3-2 CIDR, Classless Inter-Domain Routing

IP-Netzmaske[1]	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
0.0.0.0	00000000	00000000	00000000	00000000	0

[1] Beispiel: 192.168.1.0 / 255.255.255.0 entspricht im CIDR: 192.168.1.0/24

4 Menü: Verwaltung

4.1 Gerätezugriff

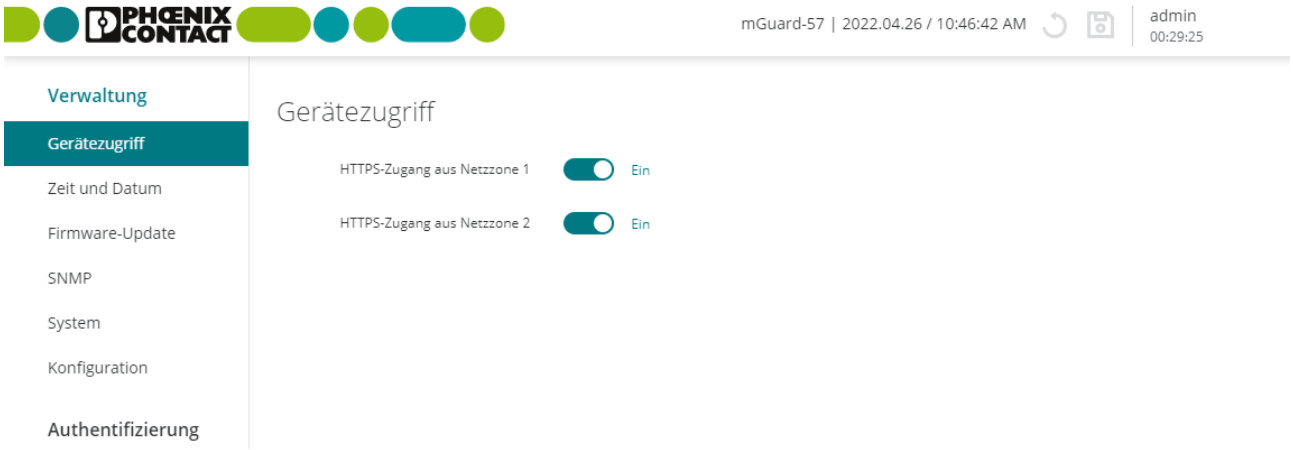


Bild 4-1 Verwaltung >> Gerätezugriff

Menü: Verwaltung >> Gerätezugriff	
Gerätezugriff	Der Zugriff auf den Web-Server des Geräts (Web-based Management oder *Config API*) kann mittels Zugriffsregeln auf eine der verfügbaren Netzzonen beschränkt werden. **Zugriff auf weitere aktive Dienste** Der Zugriff auf weitere vom Gerät bereitgestellte Dienste wird auf den entsprechenden Konfigurationsseiten aktiviert oder deaktiviert. – SNMP-Server (siehe Kapitel 4.4): werkseitig aktiviert für Netzzone 2 – DNS-Server (siehe Kapitel 6.3): werkseitig aktiviert für Netzzone 2 – NTP-Server (siehe Kapitel 4.2): werkseitig aktiviert für Netzzone 2 **ACHTUNG: Zugriff aus dem Internet** Der Server ist möglicherweise aus dem Internet erreichbar, wenn das Gerät über die aktivierte Netzzone mit dem Internet verbunden ist.
HTTPS-Zugang aus Netzzone 1	Bei aktivierter Funktion wird der Zugriff auf den HTTPS-Server des Geräts aus der ausgewählten Netzzone erlaubt (TCP-Port 443). **Voreinstellung:** deaktiviert
HTTPS-Zugang aus Netzzone 2	Bei aktivierter Funktion wird der Zugriff auf den HTTPS-Server des Geräts aus der ausgewählten Netzzone erlaubt (TCP-Port 443). **Voreinstellung:** aktiviert

4.2 Zeit und Datum

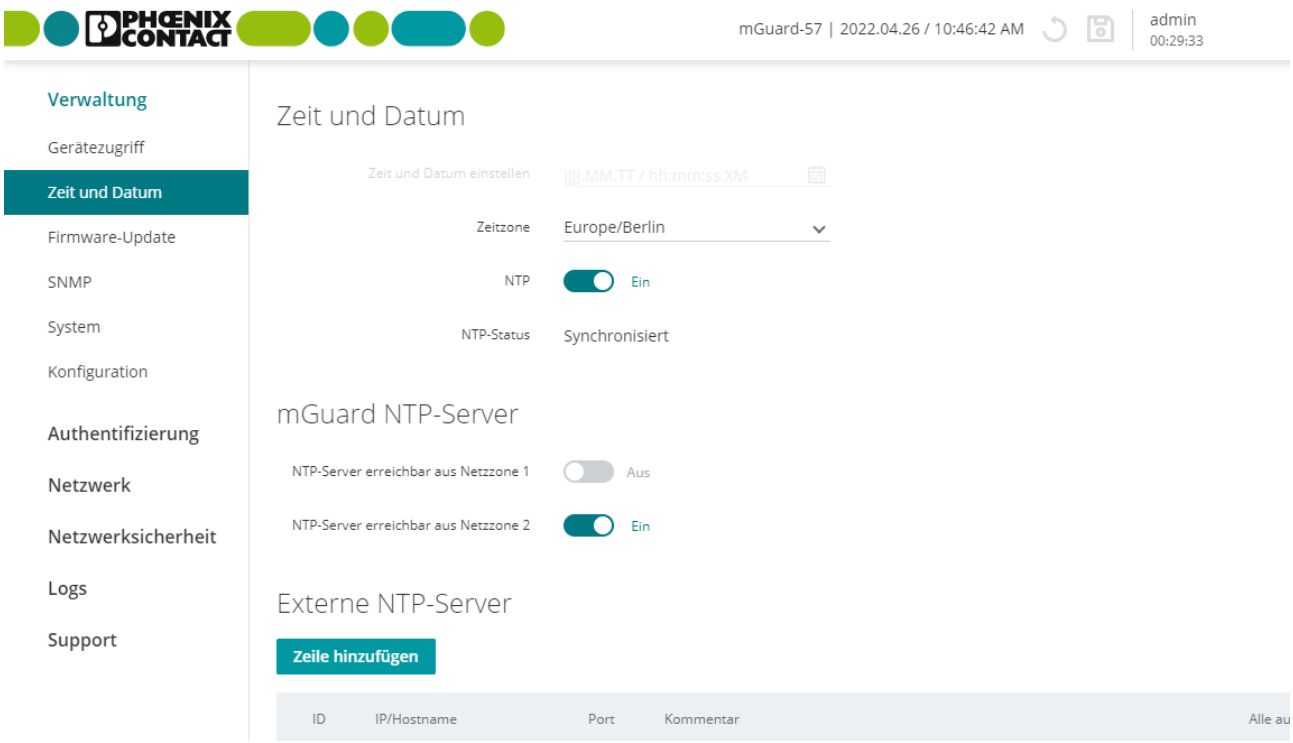


Bild 4-2 Verwaltung >> Zeit und Datum

Menü: Verwaltung >> Zeit und Datum	
Zeit und Datum	Sie können die Systemzeit des Geräts manuell einstellen oder die Synchronisation der Systemzeit mittels frei wählbarer NTP-Server vornehmen. Stellen Sie Zeit und Datum korrekt ein, da sonst das Gerät bestimmte zeitabhängige Aktivitäten nicht korrekt ausführen kann. Wird das Gerät kurzzeitig von der Spannungsversorgung getrennt, sorgt die gepufferte *Real-Time-Clock* (RTC) dafür, dass Zeit und Datum erhalten bleiben und nach einer kurzzeitigen Unterbrechung korrekt und der aktuellen Zeit entsprechend zur Verfügung stehen.

Menü: Verwaltung >> Zeit und Datum		
	Zeit und Datum einstellen (Nur konfigurierbar, wenn „NTP“ deaktiviert ist.)	Die Systemzeit des Geräts wird konfiguriert und in der *Real-Time-Clock* (RTC) abgespeichert. **Eingabeformat:** YYYY.MM.DD / hh:mm:ss XM Erlaubter Bereich: >= 2018-01-01_00:00:00 <= 2069-01-01_00:00:00 Die Systemzeit wird der konfigurierten Zeitzone entsprechend angezeigt und verwendet (z. B. in Log-Einträgen).
	Zeitzone	Die manuell eingestellte oder per NTP bezogene Systemzeit wird der konfigurierten Zeitzone entsprechend angezeigt und verwendet (z. B. in Log-Einträgen).
	NTP	Mit dieser Funktion kann der NTP-Client und der NTP-Server des Geräts aktiviert werden. Der NTP-Server des Geräts wird nur dann aktiviert, wenn der Zugriff auf den NTP-Server über mindestens eine Netzzone erlaubt ist (siehe unten). **NTP-Client** Bei aktivierter Funktion bezieht das Gerät seine Systemzeit (Uhrzeit und Datum) von einem oder mehreren NTP-Servern und synchronisiert sich fortlaufend mit ihnen. Der Status der Synchronisation wird angezeigt (siehe „NTP-Status“). Der NTP-Server überträgt die *Koordinierte Weltzeit* (UTC). Die Zeit auf dem Gerät (Systemzeit) wird der konfigurierten Zeitzone entsprechend angezeigt und verwendet (z. B. in Log-Einträgen). Die *Real-Time-Clock* (RTC) des Geräts wird automatisch mit den erhaltenen Zeitangaben der NTP-Server synchronisiert. **NTP-Server** Bei aktivierter Funktion können verbundene Netzwerk-Clients ihre Systemzeit über den NTP-Server des Geräts (*mGuard*) synchronisieren. Der NTP-Server überträgt die *Koordinierte Weltzeit* (UTC). Der Zugriff auf den NTP-Server kann für jede Netzzone aktiviert oder deaktiviert werden (siehe unten). **Voreinstellung:** aktiviert

Menü: Verwaltung >> Zeit und Datum		
	NTP-Status	Der NTP-Status gibt an, ob sich der NTP-Client des Geräts bereits mit den konfigurierten NTP-Servern synchronisiert hat. – Synchronisiert – Noch nicht synchronisiert – Deaktiviert Die initiale Zeitsynchronisation kann bis zu 15 Minuten oder länger dauern. Während dieser Zeitspanne vollzieht das Gerät immer wieder Vergleiche zwischen den Zeitangaben der externen NTP-Server und der eigenen Systemzeit, um diese so präzise wie möglich abzustimmen.
mGuard NTP-Server	**NTP-Server erreichbar aus Netzzone 1** (Nur konfigurierbar, wenn NTP aktiviert ist.)	Bei aktivierter Funktion wird der Zugriff auf den NTP-Server des Geräts aus der ausgewählten Netzzone erlaubt (UDP-Port 123). Der NTP-Server des Geräts wird erst aktiviert, wenn der Zugriff aus mindestens einer Netzzone erlaubt ist. **ACHTUNG: Zugriff aus dem Internet** Der Server ist möglicherweise aus dem Internet erreichbar, wenn das Gerät über die aktivierte Netzzone mit dem Internet verbunden ist. **Voreinstellung:** deaktiviert
	NTP-Server erreichbar aus Netzzone 2 (Nur konfigurierbar, wenn NTP aktiviert ist.)	Bei aktivierter Funktion wird der Zugriff auf den NTP-Server des Geräts aus der ausgewählten Netzzone erlaubt (UDP-Port 123). Der NTP-Server des Geräts wird erst aktiviert, wenn der Zugriff aus mindestens einer Netzzone erlaubt ist. **ACHTUNG: Zugriff aus dem Internet** Der Server ist möglicherweise aus dem Internet erreichbar, wenn das Gerät über die aktivierte Netzzone mit dem Internet verbunden ist. **Voreinstellung:** aktiviert
Externe NTP-Server	**IP/Hostname**	IP-Adresse oder Hostname des externen NTP-Servers (Zeit-Server), an den das Gerät NTP-Anfragen senden soll, um die aktuelle Zeit (Uhrzeit und Datum) zu beziehen. Sind mehrere NTP-Server angegeben, verbindet sich das Gerät automatisch mit allen Servern, um aus allen erhaltenen Werten die aktuelle Zeit zu berechnen. **Eingabeformat:** IPv4-Adresse oder Hostname **Voreinstellung:** – 0.pool.ntp.org | Port:123 – 1.pool.ntp.org | Port:123 – 2.pool.ntp.org | Port:123 – 3.pool.ntp.org | Port:123

Menü: Verwaltung >> Zeit und Datum		
	Port	Port, auf dem der externe NTP-Server NTP-Anfragen entgegennimmt. Die Angabe eines Ports ist optional. **Voreinstellung:** 123
	Kommentar	Frei wählbarer Kommentar. Erlaubte Zeichen: max. 128

4.3 Firmware-Update

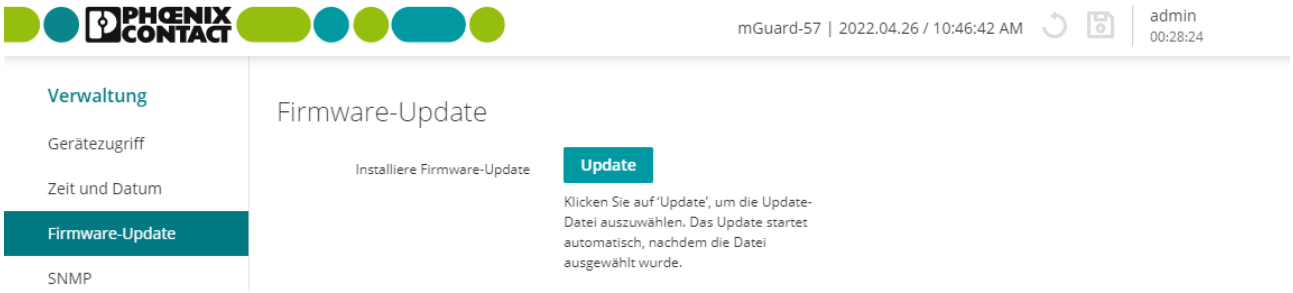


Bild 4-3 Verwaltung >> Firmware-Update

Tabelle 4-1 Unterscheidung von Update-Typen

Update-Typ	Eigenschaft	Auswirkung auf die bestehende Konfiguration
Beachten Sie vor jedem Update immer die aktuellen Release-Notes. Download unter phoenixcontact.net/product/1153079. Hinweise zu den Versionen, von denen Updates durchgeführt werden können, sind in Kapitel A 6 beschrieben.		
Patch-Release **Patch-Update**	Behebt Fehler aus den Vorversionen. Die Versionsnummer ändert sich an der dritten Stelle: – Die Version 1.6.**2** ist z. B. ein Patch-Release zu den Versionen 1.6.**1** oder 1.6.**0**.	Die bestehende Konfiguration wird in der Regel unverändert beibehalten. Neue Funktionen werden in der Regel nicht hinzugefügt.
Minor-Release **Minor-Update**	Ergänzt das Gerät zusätzlich um neue Eigenschaften und Funktionen. Die Versionsnummer ändert sich an der zweiten Stelle: – Die Version 1.**7**.0 ist z. B. ein Minor-Release zu den Versionen 1.**6**.2 oder 1.**5**.2.	1. Befindet sich das Gerät in der Werkseinstellung, gilt: – Das Gerät wird nach dem Update mit der werkseitigen Voreinstellung der **neuen** Firmware-Version konfiguriert. – Es ist möglich, dass sich Standardwerte der bestehenden Firmware-Version ändern oder Eigenschaften und Variablen hinzugefügt oder entfernt werden. 2. Wurden bereits Änderungen an der bestehenden Konfiguration des Geräts vorgenommen, gilt: – Die bestehende Konfiguration wird unverändert übernommen. – Neue Eigenschaften und Variablen aus der **neuen** Firmware-Version werden zur bestehenden Konfiguration hinzugefügt (in der Werkseinstellung). Damit das Update ausgeführt werden kann, müssen vor dem Update gegebenenfalls Anpassungen an der bestehenden Konfiguration vorgenommen werden (siehe auch Kapitel A 6). Sollte das Update aufgrund einer nicht kompatiblen Konfiguration fehlschlagen, wird der Benutzer über eine Fehlermeldung und/oder einen Log-Eintrag über den Grund des Fehlers informiert.
Major-Release **Major-Update**	Fügt dem Gerät zusätzlich grundlegende neue Eigenschaften und Funktionen hinzu. Die Versionsnummer ändert sich an der ersten Stelle: – Die Version **2**.0.0 ist z. B. ein Major-Release zu den Versionen **1**.5.0 oder **1**.4.2.	

Menü: Verwaltung >> Firmware-Update	
Firmware-Update	Eine von Phoenix Contact bereitgestellte signierte Update-Datei wird von einem Konfigurations-Rechner auf das Gerät hochgeladen und dort automatisch installiert (z. B. *mguard-image-1.8.0.mguard3.update.signed*) . Alle aktuellen Einstellungen, Passwörter und Zertifikate bleiben auf dem Gerät erhalten. Ein Downgrade von einer höheren auf eine niedrigere Firmware-Version ist nicht möglich. **Verwenden Sie die jeweils aktuelle Firmware-Version** Da mit jeder neuen Firmware-Version sicherheitsrelevante Verbesserungen in das Produkt eingefügt werden, sollte grundsätzlich immer auf die neueste Firmware-Version aktualisiert werden. Phoenix Contact stellt regelmäßig Firmware-Updates zur Verfügung. Diese finden Sie auf der Produktseite des jeweiligen Geräts (z. B. phoenixcontact.net/product/1153079). • Stellen Sie sicher, dass die Firmware aller verwendeten Geräte immer auf dem aktuellen Stand ist. • Beachten Sie die Change Notes / Release Notes zur jeweiligen Firmware-Version. • Beachten Sie die Webseite des Product Security Incident Response Teams (PSIRT) von Phoenix Contact für Sicherheitshinweise zu veröffentlichten Sicherheitslücken. **Vorgehen** **ACHTUNG: Unterbrechen Sie während des Updates nicht die Spannungsversorgung zum Gerät.** • Öffnen Sie das Menü **Verwaltung >> Firmware-Update**. • Klicken Sie auf die Schaltfläche **Update**. • Wählen Sie die Update-Datei für das Firmware-Update aus. • Öffnen Sie die Datei. ⇒ Das Öffnen der Datei startet automatisch den Update-Prozess. ⇒ Nach erfolgreicher Installation des Firmware-Updates startet das Gerät nach einigen Sekunden automatisch neu. • Warten Sie, bis das Gerät vollständig gestartet wurde.
Update-Status	Zeigt aktuelle Meldungen und Informationen zum Status des Firmware-Updates an.

4.4 SNMP

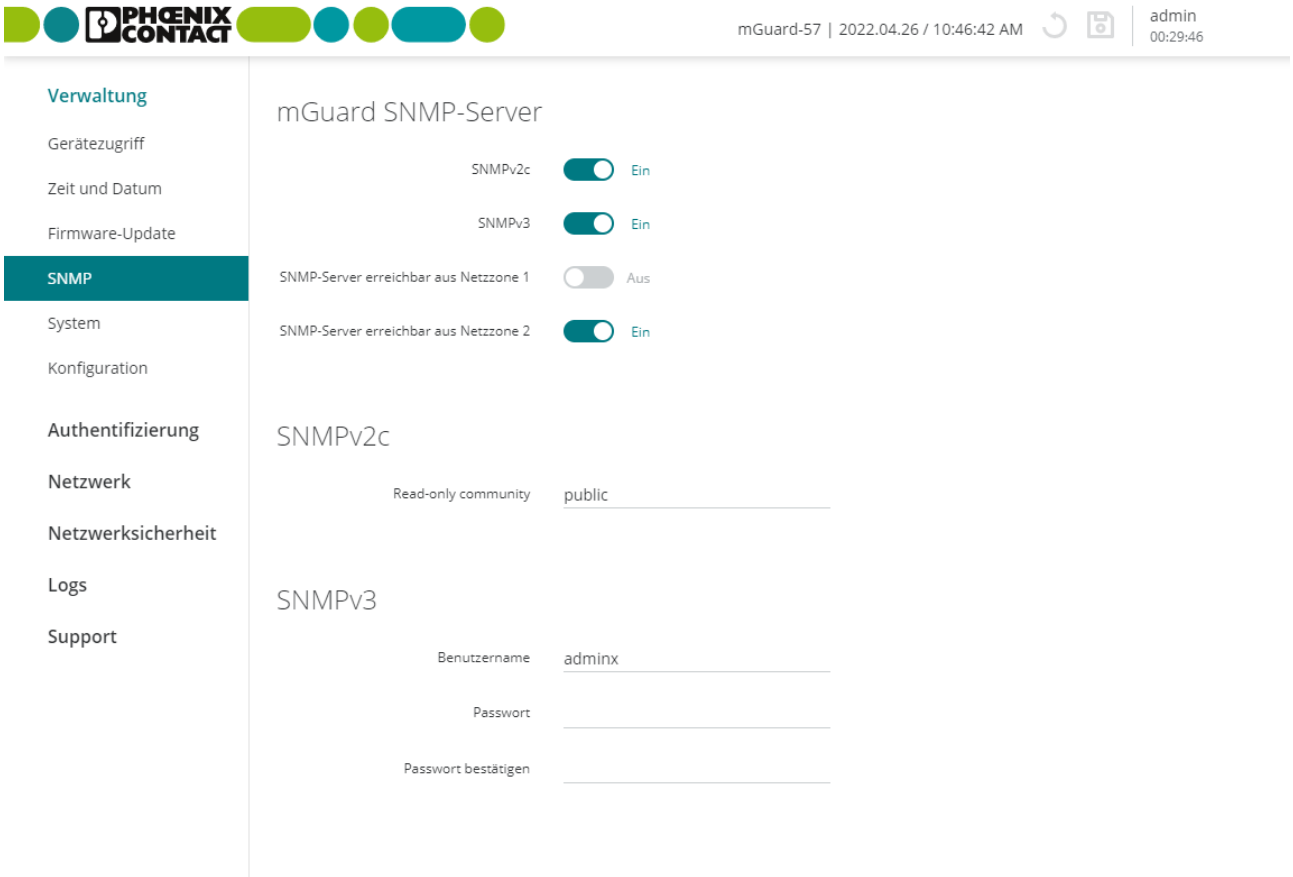


Bild 4-4 Verwaltung >> SNMP

Menü: Verwaltung >> SNMP	
SNMP	SNMP (*Simple Network Management Protocol*) wird vorzugsweise in komplexeren Netzwerken verwendet, um den Zustand und den Betrieb von Geräten zu überwachen. Das Gerät fungiert als SNMP-Server und unterstützt unterschiedliche Versionen des SNMP-Protokolls: SNMPv1/SNMPv2c und SNMPv3. Eine Konfiguration des Geräts über das SNMP-Protokoll ist aktuell ausgeschlossen. Die gleichzeitige Aktivierung verschiedener SNMP-Protokolle ist möglich.

Menü: Verwaltung >> SNMP		
mGuard SNMP-Server	**SNMPv2c**	Bei aktivierter Funktion kann das Gerät über das Protokoll SNMPv2c überwacht werden (Lesezugriff). **ACHTUNG: Unsicheres SNMPv1/v2-Protokoll** Im Gegensatz zum Protokoll SNMPv3 unterstützen die älteren Versionen SNMPv1/SNMPv2c keine Authentifizierung und keine Verschlüsselung und gelten daher als nicht sicher. Das SNMPv1/2-Protokoll sollte nur in einer sicheren Netzwerkumgebung verwendet werden, die gänzlich unter Kontrolle des Betreibers steht. Bei der Aktivierung von SNMPv2c wird das Protokoll SNMPv1 ebenfalls unterstützt. Der SNMP-Server wird erst aktiviert, wenn der Zugriff aus mindestens einer Netzzone erlaubt ist (siehe unten). **Voreinstellung:** deaktiviert
	SNMPv3	Bei aktivierter Funktion kann das Gerät über das Protokoll SNMPv3 überwacht werden (Lesezugriff). Der SNMP-Server wird erst aktiviert, wenn der Zugriff aus mindestens einer Netzzone erlaubt ist (siehe unten). **Voreinstellung:** deaktiviert
	SNMP-Server erreichbar aus Netzzone 1 (Nur konfigurierbar, wenn SNMP aktiviert ist.)	Bei aktivierter Funktion wird der Zugriff auf den SNMP-Server des Geräts aus der ausgewählten Netzzone erlaubt (UDP-Port 161). **ACHTUNG: Zugriff aus dem Internet** Der Server ist möglicherweise aus dem Internet erreichbar, wenn das Gerät über die aktivierte Netzzone mit dem Internet verbunden ist. **Voreinstellung:** deaktiviert
	SNMP-Server erreichbar aus Netzzone 2 (Nur konfigurierbar, wenn SNMP aktiviert ist.)	Bei aktivierter Funktion wird der Zugriff auf den SNMP-Server des Geräts aus der ausgewählten Netzzone erlaubt (UDP-Port 161). **ACHTUNG: Zugriff aus dem Internet** Der Server ist möglicherweise aus dem Internet erreichbar, wenn das Gerät über die aktivierte Netzzone mit dem Internet verbunden ist. **Voreinstellung:** deaktiviert
SNMPv2c (Nur konfigurierbar, wenn SNMPv2c aktiviert ist.)	Bei aktivierter Funktion werden die Protokolle SNMPv1und SNMPv2c unterstützt. **ACHTUNG: Unsicheres SNMPv1/v2-Protokoll** Im Gegensatz zum Protokoll SNMPv3 unterstützen die älteren Versionen SNMPv1/SNMPv2c keine Authentifizierung und keine Verschlüsselung und gelten daher als nicht sicher.	

Menü: Verwaltung >> SNMP		
	Read-only community	SNMP kodiert bei der Version SNMPv1/SNMPv2c die Zugangsdaten als Teil einer sogenannten *community*. Der *Read-only community* string wird dabei wie ein Passwort oder Zugangsschlüssel verwendet. Die Authentifizierung mittels *Read-only community* string ermöglicht einen beschränkten SNMP-Lesezugriff. **Eingabeformat:** Der String muss mit einem Buchstaben beginnen. Erlaubte Zeichen (min. 6, max. 255): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789_- **Voreinstellung:** public
SNMPv3 (Nur konfigurierbar, wenn SNMPv3 aktiviert ist.)	Im Gegensatz zu den Protokollen SNMPv1/v2c gilt das SNMPv3-Protokoll als sicher, da es die Möglichkeit zur Benutzerauthentifizierung und zur Verschlüsselung bietet. Verwendete Verschlüsselungs- und Hash-Algorithmen: – AES-128 – SHA-2 (SHA-256) mit SNMPv3 USM	
	Benutzername	Benutzername des SNMPv3-Benutzers, der über das SNMPv3-Protokoll auf den SNMP-Server des Geräts zugreifen möchte. Das Hinzufügen weiterer SNMPv3-Benutzer wird nicht unterstützt. **Eingabeformat:** Erlaubte Zeichen (min. 1, max. 200): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789_.-
	Passwort	Passwort des SNMPv3-Benutzers. **Eingabeformat:** Um die Sicherheit zu erhöhen, sollte das Passwort Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen enthalten. Erlaubte Zeichen (min. 8, max. 200): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
	Passwort bestätigen	Wiederholte Eingabe des Passworts.

4.5 System

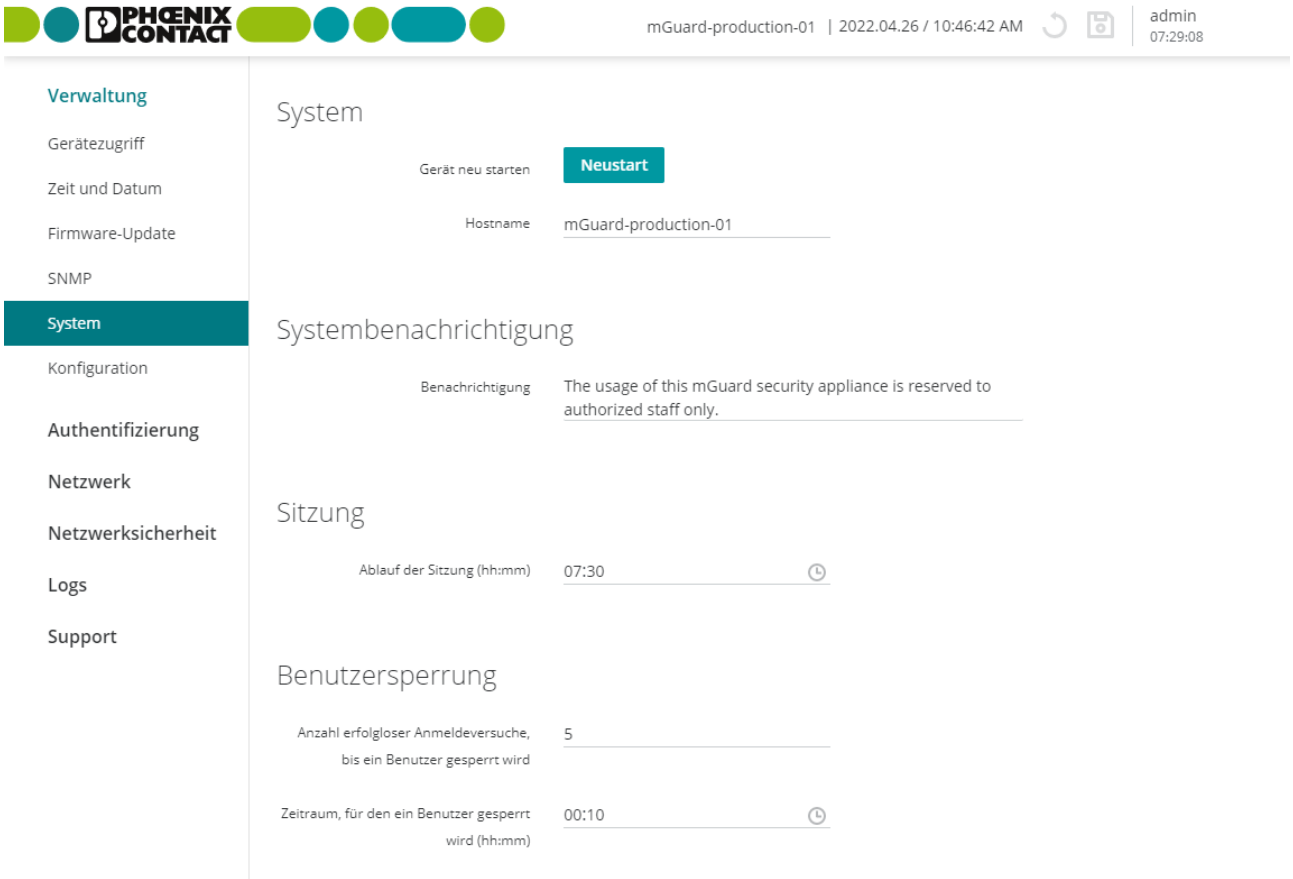


Bild 4-5 Verwaltung >> System

Menü: Verwaltung >> System		
System	**Gerät neu starten**	Das Gerät wird neu gestartet. **Schaltfläche** • Klicken Sie auf die Schaltfläche **Neustart**, um das Gerät neu zu starten. **Hinweis:** Alle nicht gespeicherten Änderungen gehen verloren.

Menü: Verwaltung >> System		
	Hostname	Name, unter dem das Gerät im Netzwerk grundsätzlich sichtbar und erreichbar ist. Wird der Hostname über das *Domain Name System* (DNS) aufgelöst, können Netzwerkteilnehmer das Gerät direkt über seinen Hostnamen ansprechen. **Eingabeformat:** Der Name muss mit einem Buchstaben oder einer Ziffer beginnen und enden. Erlaubte Zeichen (min. 1, max. 63): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789-
Systembenachrichtigung	**Benachrichtigung**	Frei wählbarer Text für eine Systembenachrichtigung, die vor einer Anmeldung am Gerät angezeigt wird (maximal 512 Zeichen). Wird angezeigt bei: – Anmeldung über das Web-based Management (WBM) **Eingabeformat:** frei wählbarer Text **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*.
Sitzung	**Ablauf der Sitzung (hh:mm)**	Länge des *Session Timeouts* (Zeitspanne). Die Sitzung eines Benutzers wird durch einen *Session timeout* zeitlich begrenzt. Die konfigurierbare Zeitspanne des *Session Timeouts* liegt zwischen 5 Minuten und 8 Stunden. Nach Ablauf der Sitzung wird der Benutzer automatisch abgemeldet. Der *Session timeout* startet mit der Anmeldung des Benutzers (werkseitige Voreinstellung: 30 Minuten). Führt der Benutzer während einer laufenden Sitzung eine Aktion durch, wird der *Session timeout* jeweils auf den konfigurierten Ausgangswert zurückgesetzt. **Eingabeformat:** Stunden:Minuten (min. 00:05, max. 08:00) **Voreinstellung:** 00:30

Menü: Verwaltung >> System		
Benutzersperre	**Anzahl erfolgloser Anmeldeversuche, bis ein Benutzer gesperrt wird**	Anzahl erfolgloser Anmeldeversuche, bis ein Benutzer gesperrt wird. Ein Benutzer wird nach der konfigurierten Anzahl erfolgloser Anmeldeversuche (falsche Passworteingabe) automatisch für bis zu 8 Stunden gesperrt (siehe unten). **Hinweis:** Diese Sperre kann durch einem Administrator mit der Rolle „*Super Admin*“ vorzeitig aufgehoben werden (siehe Kapitel 5.1). **Hinweis:** Eine automatische Sperre wird ebenfalls durch einen Neustart des Geräts aufgehoben. **Eingabeformat:** Zahl (min. 1, max. 200) **Voreinstellung:** 5
	Zeitraum, für den ein Benutzer gesperrt wird (hh:mm)	Zeitraum, für den ein Benutzer nach erfolglosen Anmeldeversuchen gesperrt wird. Ein Benutzer wird nach einer konfigurierbaren Anzahl erfolgloser Anmeldeversuche (falsche Passworteingabe) automatisch für den konfigurierten Zeitraum gesperrt (siehe oben). **Hinweis:** Diese Sperre kann durch einem Administrator mit der Rolle „*Super Admin*“ vorzeitig aufgehoben werden (siehe Kapitel 5.1). **Hinweis:** Eine automatische Sperre wird ebenfalls durch einen Neustart des Geräts aufgehoben. **Eingabeformat:** Stunden:Minuten (min. 00:01, max. 08:00) **Voreinstellung:** 00:10

4.6 Konfiguration sichern

Bild 4-6 Verwaltung >> Konfiguration sichern

Menü: Verwaltung >> Konfiguration sichern	
Konfiguration sichern und wiederherstellen	Die aktuell auf dem Gerät gespeicherte Konfiguration kann als JSON-Datei exportiert und auf den Konfigurations-Rechner heruntergeladen werden. **Sicherheitsrelevante Informationen und Informationen zur Benutzerverwaltung werden nicht exportiert.** Das betrifft: – alle Informationen zur Benutzerverwaltung (lokale Benutzer, Benutzerpasswörter und Einstellungen zum LDAP-Server, siehe Kapitel 5), – das SNMP-Passwort, – private kryptografische Schlüssel (z. B. Remote-Logging). Damit ist es möglich, einen beliebigen Zustand der Konfiguration zu archivieren. Die gespeicherte Konfiguration kann zu einem späteren Zeitpunkt auf dem selben oder einem anderen Gerät wiederhergestellt werden. Die Variablen-Werte der heruntergeladene Konfiguration können vor dem Import mit einem Text-Editor editiert werden. **Voraussetzung für den Import** Die Konfiguration darf nicht mit einer Minor-Version erstellt worden sein, die höher ist als die, die bereits auf dem Gerät installiert ist (siehe auch Kapitel 4.3). Damit der Import ausgeführt werden kann, müssen vor dem Import gegebenenfalls Anpassungen an der gespeicherten Konfiguration vorgenommen werden (siehe auch Kapitel A 6). Wird auf einem Gerät mit installierter Firmware-Version x.y.z (z. B. 1.7.1) eine Konfiguration wiederhergestellt, die mit einer älteren Minor-Version „y“ erstellt wurde (z. B. 1.5.1), werden die bereits konfigurierten Variablen-Werte, die in der älteren Version noch nicht vorhanden waren, beibehalten.

Menü: Verwaltung >> Konfiguration sichern

Konfiguration heruntergeladen

Die aktuell auf dem Gerät gespeicherte Konfiguration wird im JSON-Format exportiert und auf den Konfigurations-Rechner heruntergeladen.

Schaltfläche

- Klicken Sie auf die Schaltfläche **Herunterladen**, um die Konfiguration auf dem Konfigurations-Rechner zu speichern.

Dateiname: *mGuard-configuration.json*

Hinweis: Sie können die Datei beliebig umbenennen und unter dem neuen Dateinamen importieren.

Hinweis: Sie können die Variablen-Werte mit einem Text-Editor ändern und anschließend erneut importieren.

Konfiguration hochladen

Eine auf dem Konfigurations-Rechner gespeicherte Konfiguration wird in das Gerät importiert.

Die Konfiguration darf nicht mit einer Minor-Version erstellt worden sein, die höher ist als die, die bereits auf dem Gerät installiert ist.

Beispiel:

OK: Import einer mit Version 1.6.1 erstellten Konfiguration auf ein Gerät mit installierter Version 1.7.0.

FEHLER: Import einer mit Version 1.8.1 erstellten Konfiguration auf ein Gerät mit installierter Version 1.7.0.

Wird auf einem Gerät mit installierter Firmware-Version x.y.z (z. B. 1.6.1) eine Konfiguration wiederhergestellt, die mit einer älteren Minor-Version „y“ erstellt wurde (z. B. 1.5.1), werden die bereits konfigurierten Variablen-Werte, die in der älteren Version noch nicht vorhanden waren, beibehalten.

Damit der Import ausgeführt werden kann, müssen vor dem Import gegebenenfalls Anpassungen an der gespeicherten Konfiguration vorgenommen werden (siehe auch Kapitel A 6).

Schaltfläche

- Klicken Sie auf die Schaltfläche **Hochladen**, um die gespeicherte Konfiguration in das Gerät zu importieren.

⇒ Eine gültige Konfiguration wird angezeigt, aber noch nicht aktiviert.

⇒ Ungültige Variablenwerte werden gegebenenfalls wie in Kapitel 3.6.4 beschrieben mit einem roten Punkt markiert und angezeigt und müssen geändert werden.

- Klicken Sie auf das Icon , um die Konfiguration zu speichern und anzuwenden.

Menü: Verwaltung >> Konfiguration sichern

Externer Konfigurationsspeicher (ECS)

Die aktuell auf dem Gerät gespeicherte Konfiguration/Benutzerverwaltung kann automatisch oder manuell auf einen externen Konfigurationsspeicher (ECS) exportiert werden. Als Speichermedium fungiert eine SD-Karte.

ACHTUNG: Sicherheitsrelevante Informationen
Die gespeicherte Konfiguration enthält sicherheitsrelevante Informationen, wie z. B. lokale Benutzer, Berechtigungen, Passwörter (hashed) und Zertifikate (öffentliche Schlüssel). Das Passwort für den LDAP-Server ist im Klartext enthalten.
Ausnahme: Private Schlüssel sind in der Konfiguration nicht enthalten.

ACHTUNG: Sicherheitsrelevante Informationen
Stellen Sie sicher, dass nur befugte Personen auf die SD-Karte zugreifen können.

Von der SD-Karte kann die Konfiguration in FL MGUARD 1000-Geräte importiert und dort angewendet werden. Neue Geräte können so leicht auf der Basis einer bereits bestehenden Konfiguration in Betrieb genommen werden.

Voraussetzungen:

- Die Geräte befinden sich in Werkseinstellungen.
- Firmware-Version „SD-Karte“ ist kleiner/gleich Firmware-Version „Gerät“.
- Technische Voraussetzung SD-Karte:
  - SD- und SDHC-Karten bis max. 8 GB
  - VFAT-kompatibles Dateisystem

Beachten Sie, dass die Funktionalität der SD-Karte und des Produktes nur bei Einsatz einer Phoenix Contact SD-Karte (z. B. SD FLASH 2GB - 2988162) sichergestellt werden kann. Beim Einsatz von SD-Karten anderer Anbieter wird empfohlen, die Kompatibilität der Karte sicherzustellen.

Aktuelle Konfiguration auf SD-Karte speichern

Die aktuell auf dem Gerät gespeicherte Konfiguration wird auf die eingesetzte SD-Karte geschrieben.

Stellen Sie sicher, dass nur befugte Personen auf die SD-Karte zugreifen können.

Gespeicherte Konfiguration via SD-Karte erneut in ein Gerät importieren:

Für alle **neuen Geräte** oder Geräte, die mittels Smart-Mode auf Werkseinstellungen zurückgesetzt wurden (siehe Kapitel 3.6.6), gilt:

Eine auf der eingesetzten SD-Karte gespeicherte Konfiguration/Benutzerverwaltung wird beim Start bzw. der Inbetriebnahme des Geräts automatisch in das Gerät importiert und dort angewendet.

Voraussetzung:

- Firmware-Version „SD-Karte“ ist in der Minor-Version kleiner/gleich Firmware-Version „Gerät“.
- Die drei Dateien sind auf der SD-Karte enthalten (einzeln oder in gepackter Form als *mGuard.tar.gz:* Die Einzeldateien werden prioritär verwendet!).

Tritt während des Imports ein Fehler auf, startet das Gerät in der werkseitigen Voreinstellung. Die LEDs FAIL und PF1 leuchten zusätzlich rot.

Menü: Verwaltung >> Konfiguration sichern

Schaltfläche

- Klicken Sie auf die Schaltfläche **Speichern**, um die Konfiguration auf die SD-Karte zu schreiben.

Es werden drei Dateien gespeichert:

– *users_pass.json*
– *snmp-pass.conf*
– *configuration.json*

Hinweis: Entnehmen Sie die SD-Karte erst, wenn der Schreibvorgang abgeschlossen ist.

Konfiguration automatisch auf SD-Karte speichern

Bei aktivierter Funktion wird jede Konfigurationsänderung, die im WBM durch einen Klick auf das Icon gespeichert wird, automatisch auf die eingesetzte SD-Karte geschrieben.

Stellen Sie sicher, dass nur befugte Personen auf die SD-Karte zugreifen können.

Es werden drei Dateien gespeichert:

– *users_pass.json*
– *snmp-pass.conf*
– *configuration.json*

Gespeicherte Konfiguration via SD-Karte erneut in ein Gerät importieren:

Für alle **neuen Geräte** oder Geräte, die mittels Smart-Mode auf Werkseinstellungen zurückgesetzt wurden (siehe Kapitel 3.6.6), gilt:

Eine auf der eingesetzten SD-Karte gespeicherte Konfiguration/Benutzerverwaltung wird beim Start bzw. der Inbetriebnahme des Geräts automatisch in das Gerät importiert und dort angewendet.

Voraussetzung:

– Firmware-Version „SD-Karte“ ist kleiner/gleich Firmware-Version „Gerät“.
– Die drei Dateien sind auf der SD-Karte enthalten (einzeln oder in gepackter Form als *mGuard.tar.gz:* Die Einzeldateien werden prioritär verwendet!).

Tritt während des Imports ein Fehler auf, startet das Gerät in der werkseitigen Voreinstellung. Die LEDs FAIL und PF1 leuchten zusätzlich rot.

5 Menü: Authentifizierung

Nur sichtbar und konfigurierbar für Benutzer mit der Benutzerrolle *Super Admin*.

5.1 Benutzerverwaltung

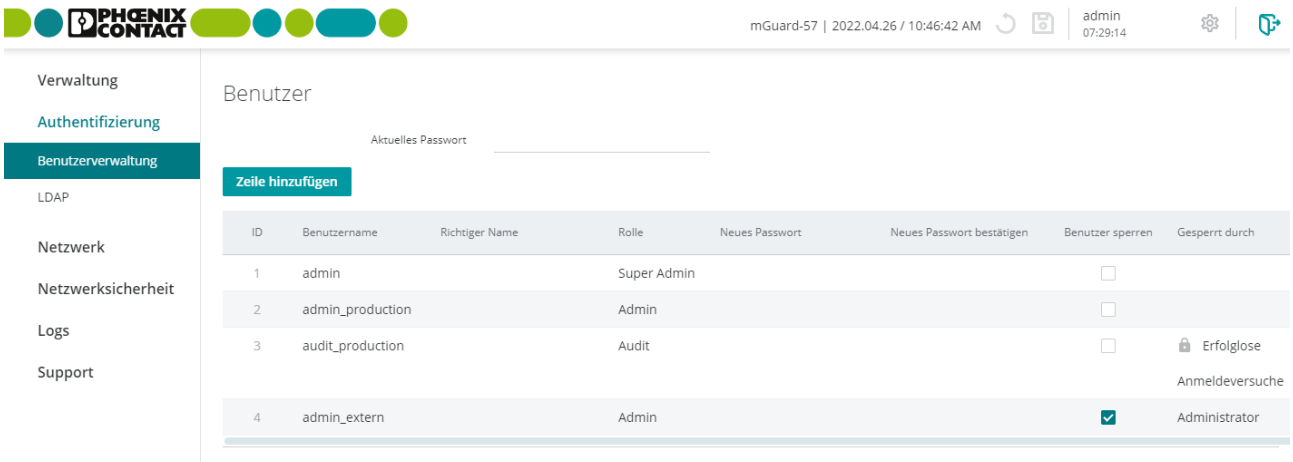


Bild 5-1 Authentifizierung >> Benutzerverwaltung

Menü: Authentifizierung >> Benutzerverwaltung	
Benutzer	Benutzer können sich mit ihrem Passwort beim Web-based Management (WBM) oder der *Config API* anmelden. Über Benutzerrollen werden Benutzern bestimmte Berechtigungen zugewiesen (siehe „Benutzerrollen und Berechtigungen“). In der werkseitigen Voreinstellung existiert lediglich der Benutzer „*admin*“ mit der Benutzerrolle „*Super Admin*“ und dem Passwort „*private*“. **ACHTUNG: Ändern Sie das Administrator-Passwort bei der Erstanmeldung** Ändern Sie bei der ersten Anmeldung umgehend das werkseitig voreingestellte Administrator-Passwort des Benutzers „*admin*“ (Passwort = *private*). Ein angemeldeter Benutzer kann sich nicht selber löschen.

Menü: Authentifizierung >> Benutzerverwaltung

Benutzerrollen und Berechtigungen

Berechtigung / Rolle	Super Admin	Admin	Audit
Benutzer verwalten	X		
LDAP konfigurieren	X		
Konfiguration ändern	X	X	
Aktionen durchführen	X	X	
Firmware-Updates installieren	X	X	
Konfiguration prüfen	X	X	X
Eigenes Passwort ändern	X	X	X
Gerätestatus abfragen	X	X	X
Log-Einträge lesen	X	X	X´

Was ist zu tun, wenn Passwörter nicht mehr bekannt sind?

Sollten die Passwörter sämtlicher Benutzer nicht mehr bekannt und damit eine Anmeldung am Gerät nicht mehr möglich sein, muss das Gerät gegebenenfalls in die werkseitige Voreinstellung zurückgesetzt werden.

ACHTUNG: Datenverlust
Die gesamte Konfiguration, alle Einstellungen und Benutzer sowie deren Passwörter werden damit unwiderruflich gelöscht.

Führen Sie hierzu die Smart-Mode-Funktion „*Wiederherstellung der Werkseinstellung*“ aus (siehe Kapitel A 2).

Logging

Die Aktivitäten der Benutzer werden in entsprechenden Log-Einträgen gespeichert. Das betrifft z. B. die An- und Abmeldung von Benutzern oder von Benutzern durchgeführte Konfigurationsänderungen.

Aktuelles Passwort — Das Passwort des angemeldeten Benutzers muss angegeben werden, wenn Änderungen in der Benutzerverwaltung vorgenommen werden.

ID — Identifikationsnummer des Benutzers (vom System generiert).

Benutzername — Eindeutiger Benutzername, mit dem sich der Benutzer beim Gerät anmeldet.

Eingabeformat: Der Name muss mit einem Buchstaben oder einer Ziffer beginnen. Er darf nicht mit einem Punkt enden.

Erlaubte Zeichen (min. 2, max. 200):

ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz
0123456789_.-

Menü: Authentifizierung >> Benutzerverwaltung

Richtiger Name	Frei zu vergebender Name zur Vereinfachung der Administration.
Rolle	**Super Admin, Admin, Audit** Mit der Auswahl einer Benutzerrolle werden dem Benutzer bestimmte Berechtigungen zugewiesen (siehe „Benutzerrollen und Berechtigungen“). Der Standard-Benutzer in der werkseitigen Voreinstellung „admin“ besitzt die Rolle „*Super Admin*“.
Neues Passwort	Das neue Passwort des zugehörigen Benutzers. **Eingabeformat:** Um die Sicherheit zu erhöhen, sollte das Passwort Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen enthalten. Erlaubte Zeichen (min. 6, max. 64): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
Neues Passwort bestätigen	Wiederholte Eingabe des neuen Passworts.
Benutzer sperren	Bei aktivierter Funktion ist der zugehörige Benutzer gesperrt und kann sich nicht erneut am Gerät anmelden. Eine angemeldeter Benutzer kann sich nicht selber sperren. Ein angemeldeter Benutzer bleibt innerhalb seiner laufenden Sitzung auch dann angemeldet, wenn er von einer anderen Instanz aus gesperrt wird. Benutzer, die über einen LDAP-Server authentisiert werden, können nur über die Benutzerverwaltung des LDAP-Servers gesperrt werden. **Voreinstellung:** deaktiviert
Gesperrt durch	Angabe des Grundes für die Benutzersperre: a) Erfolglose Anmeldeversuche (siehe Kapitel 4.5) b) Administrator (siehe oben „Benutzer sperren“) Wurde ein Benutzer automatisch gesperrt, kann die Sperre durch einen Klick auf das Icon vor der Meldung „*Erfolglose Anmeldeversuche*“ vorzeitig aufgehoben werden. Eine automatische Sperre wird ebenfalls durch einen Neustart des Geräts aufgehoben.

5.2 LDAP

Sicherheitshinweis
Aus Sicherheitsgründen sollte immer eine verschlüsselte TLS-Verbindung zwischen dem Gerät (mGuard) und dem LDAP-Server verwendet werden.

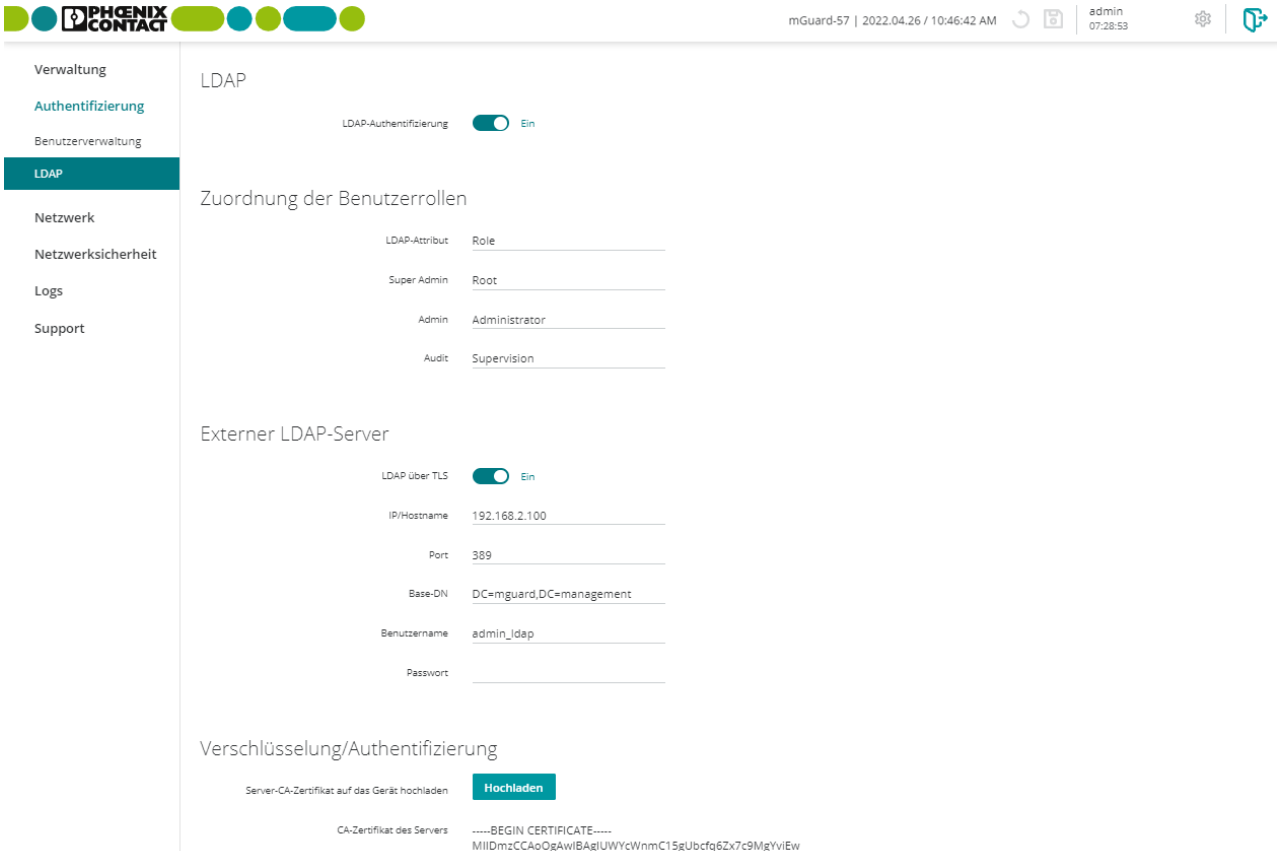


Bild 5-2 Authentifizierung >> LDAP

Menü: Authentifizierung >> LDAP	
LDAP	LDAP (*Lightweight Directory Access Protocol*) ist ein Client/Server-Protokoll, mit dem Daten eines entfernten Verzeichnisdienstes über das IP-Netzwerk abgefragt und verwaltet werden können. Das mGuard-Gerät fungiert dabei als LDAP-Client. Durch die Verwendung von LDAP kann die Benutzerverwaltung des Geräts in eine zentrale Datenbank auf einem LDAP-Server ausgelagert werden, der die Benutzerauthentifizierung übernimmt. Die Konfiguration von lokalen Benutzern auf dem Gerät ist weiterhin möglich, grundsätzlich aber nicht mehr nötig (Ausnahme: ein lokaler Benutzer mit der Rolle „*Super Admin*“ muss vorhanden sein). Auf dem LDAP-Server verwaltete Benutzer können sich am mGuard-Gerät anmelden, indem sie ihre zentral verwalteten Zugangsdaten (Benutzername und Passwort) eingeben.

Menü: Authentifizierung >> LDAP		
	LDAP-Authentifizierung	Bei aktivierter Funktion kann das Gerät über das LDAP-Protokoll auf einen konfigurierten LDAP-Server zugreifen. Auf dem LDAP-Server verwaltete Benutzer können bei der Anmeldung am Gerät über das LDAP-Protokoll und die Eingabe ihrer LDAP-Zugangsdaten authentisiert werden. Bei der Anmeldung eines Benutzers (Login) prüft das Gerät als Erstes, ob der Benutzer als **lokaler Benutzer** auf dem Gerät vorhanden ist. Ist dies der Fall, kann der lokale Benutzer nur mit dem **lokal konfigurierten Benutzer-Passwort** angemeldet werden. Eine Abfrage beim LDAP-Server findet in diesem Fall nicht mehr statt. Die Rolle, die einem über LDAP angemeldeten Benutzer auf dem LDAP-Server zugewiesen wurde, muss ebenfalls auf dem mGuard-Gerät existieren (siehe Kapitel 5.1). Ein über LDAP angemeldeter Benutzer wird automatisch abgemeldet, wenn die Funktion während der laufenden Sitzung deaktiviert wird. **Voreinstellung:** deaktiviert
Zuordnung der Benutzerrollen	**LDAP-Attribut**	Name des Attributs, in dem die Rollen/Benutzerklassen für jeden LDAP-Benutzer festgelegt werden. Damit die Zuordnung der Rollen stattfinden kann, müssen diese sowohl auf dem LDAP-Server als auch auf dem Gerät dem gleichen LDAP-Attribut zugeordnet werden. **Beispielkonfiguration:** Konfiguration auf dem LDAP-Server**:** – **Role***: Role_1* – **Role***: Role_2* – **Role***: Role_3* LDAP-Attribut auf dem mGuard-Gerät**:** – **Role** Erlaubte Zeichen (min. 1, max. 200): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789_.-

Menü: Authentifizierung >> LDAP		
	Super Admin **Admin** **Audit**	Bei einer Anmeldung über LDAP muss die dem LDAP-Benutzer auf dem LDAP-Server zugewiesene Benutzerrolle (oder Benutzerrollen) mindestens einer der drei verfügbaren Benutzerrollen auf dem Gerät zugeordnet werden (siehe auch Kapitel 5.1). Kann die Benutzerrolle des LDAP-Benutzers nicht zugeordnet werden, ist eine Anmeldung nicht möglich. **Beispiel:** **Gerät <-> LDAP-Server** Super Admin <-> Role_1 Admin <-> Role_2 Audit <-> Role_3 Sind einem LDAP-Benutzer mehrere Benutzerrollen zugeordnet, wird er bei der Anmeldung mit der Rolle mit den weitestgehenden Berechtigungen angemeldet. Erlaubte Zeichen (min. 1, max. 200): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789_.-
Externer LDAP-Server	**LDAP über TLS**	Bei aktivierter Funktion werden die Daten verschlüsselt über eine TCP-Verbindung übertragen. **Hinweis:** Aus Sicherheitsgründen sollte immer eine verschlüsselte TLS-Verbindung zwischen dem Gerät (mGuard) und dem LDAP-Server verwendet werden. (Siehe auch „Verwendete Verschlüsselungsalgorithmen“ auf Seite 15.) **Voraussetzung:** Um die Integrität und Authentizität der verschlüsselten TCP-Verbindung sicherzustellen, muss das Server-Zertifikat (CA-Zertifikat) des Remote-Servers auf dem Gerät installiert werden (siehe unten).
	IP/Hostname	IP-Adresse oder Hostname des externen LDAP-Servers, an den das Gerät Anfragen zur Benutzer-Authentisierung senden soll. **Eingabeformat:** IPv4-Adresse oder Hostname
	Port	Port, auf dem der LDAP-Server Anfragen entgegennimmt. **Voreinstellung:** 389

Menü: Authentifizierung >> LDAP		
	Base-DN	Basisadresse im Verzeichnis auf dem LDAP-Server. Die Suche nach den gewünschten Objekten (z. B. Benutzerdaten) wird auf einen kleineren Bereich im Verzeichnisbaum des LDAP-Servers eingeschränkt. Sie erfolgt ausschließlich unterhalb der angegebenen Basisadresse (Knotenpunkt). **Eingabeformat:** Verzeichnispfad (*DC=x,DC=y,DC=z*) Erlaubte Zeichen (min. 1, max. 1024): Die Eingabe muss mit einem der folgenden Zeichen beginnen: ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789._ Diese Zeichen können jeweils durch eines der folgenden vier Zeichen verbunden werden: -_=, Beispiel: *DC=mguard,DC=management,DC=user*
	Benutzername	Benutzername, mit dem sich das Gerät beim LDAP-Server anmeldet und authentifiziert. Erlaubte Zeichen (min. 1, max. 200): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789_.-
	Passwort	Passwort, mit dem sich das Gerät beim LDAP-Server anmeldet und authentifiziert. **Eingabeformat:** Um die Sicherheit zu erhöhen, sollte das Passwort Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen enthalten. Erlaubte Zeichen (min. 6, max. 200): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789!#$%&()*+,-./:;<=>?[]^_`{|}~@
Verschlüsselung/ Authentifizierung	**Verwendung von Zertifikaten** 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 (siehe auch Kapitel B 3, „Erklärung der Fachwörter“ unter „X.509-Zertifikat“). **Zertifikat** Ein Zertifikat dient dem Zertifikatsinhaber als Bescheinigung dafür, dass er der ist, für den er sich ausgibt. Die bescheinigende, beglaubigende Instanz dafür ist die CA (*Certificate Authority*). Von ihr stammt die Signatur (= elektronische Unterschrift) auf dem Zertifikat, mit der die CA bescheinigt, dass der rechtmäßige Inhaber des Zertifikats einen privaten Schlüssel besitzt, der zum öffentlichen Schlüssel im Zertifikat passt. Der Name des Ausstellers eines Zertifikats wird im Zertifikat als Aussteller aufgeführt, der Name des Inhabers eines Zertifikats als Subject.	

Menü: Authentifizierung >> LDAP		
Server-Zertifikat	**Server-CA-Zertifikat auf das Gerät hochladen**	CA-Zertifikat, mit dem der Remote-Server (LDAP-Server) gegenüber dem Gerät authentifiziert wird. Das CA-Zertifikat wird vom Betreiber des Remote-Servers bereitgestellt und muss auf das Gerät hochgeladen werden (X.509-Zertifikat mit öffentlichem Schlüssel). Eine verschlüsselte TCP-Verbindung zum Remote-Server kann nur dann erfolgreich aufgebaut werden, wenn dieser seinerseits ein vom CA-Zertifikat ausgestelltes Zertifikat (mit dem *geheimen* Schlüssel) oder eine gültige Zertifikatskette, mit dem CA-Zertifikat als oberste Instanz, vorzeigt. **Schaltfläche** • Klicken Sie auf die Schaltfläche **Hochladen**, um das CA-Zertifikat des Remote-Servers (LDAP-Servers) von einem Konfigurationsrechner auf das Gerät hochzuladen. **Format:** Die maximal erlaubte Dateigröße beträgt 1 MB. **Hinweis:** Ein bereits hochgeladenes CA-Zertifikat wird in diesem Fall gelöscht und ersetzt.
	CA-Zertifikat des Servers	Zeigt das hochgeladene CA-Zertifikat an.

6 Menü: Netzwerk

6.1 Interfaces

6.1.1 Interfaces

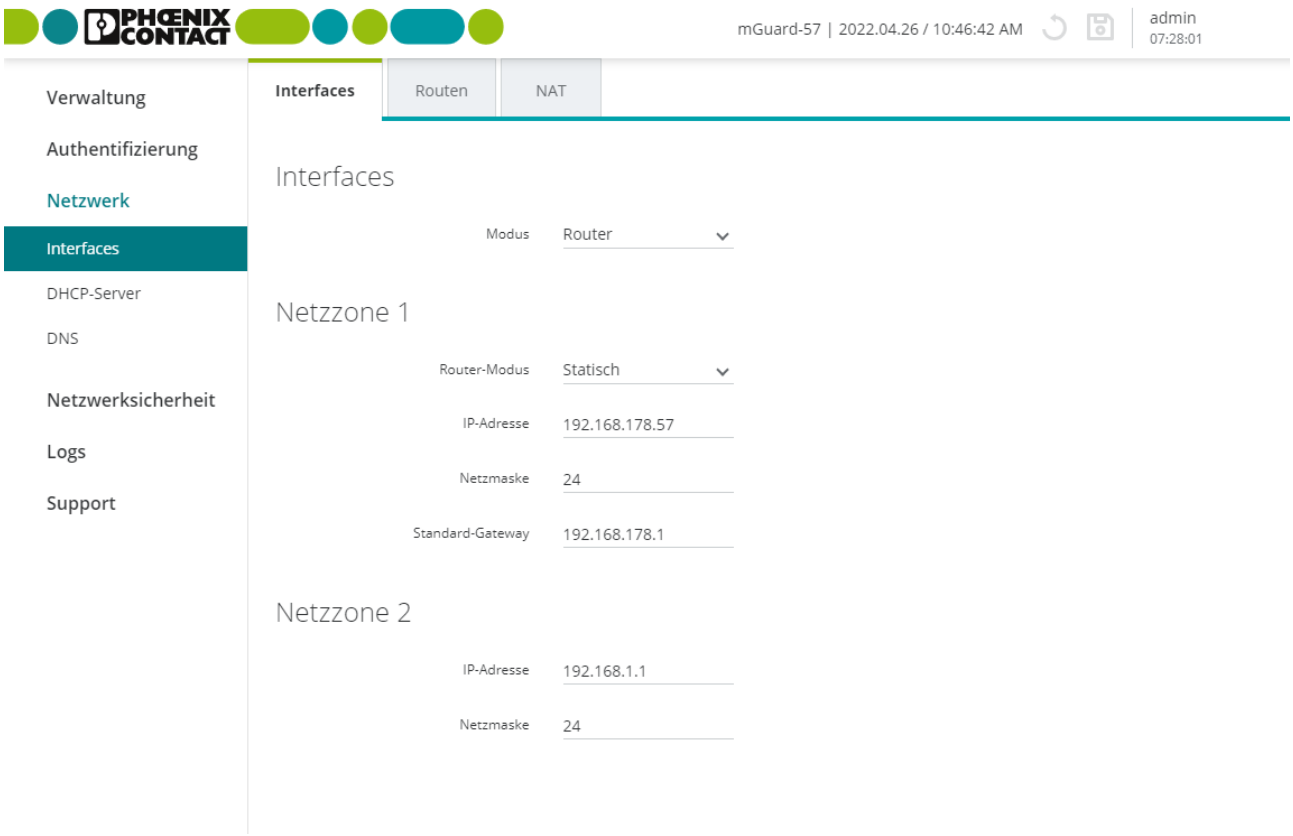


Bild 6-1 Netzwerk >> Interfaces >> Interfaces: Netzzone 1/2 konfigurieren

Menü: Netzwerk >> Interfaces >> Interfaces		
	Modus	Das Gerät kann in zwei Netzwerk-Modi betrieben werden (*Router-Modus* und *Stealth-Modus*). **Router** Siehe „Router-Modus“ auf Seite 58 **Stealth** Siehe „Stealth-Modus“ auf Seite 61

Menü: Netzwerk >> Interfaces >> Interfaces

Router-Modus

Befindet sich das Gerät im Router-Modus, arbeitet es als Gateway zwischen verschiedenen Subnetzen. Der Datenverkehr wird dabei zwischen den beiden Netzwerkinterfaces (Netzzonen) des Geräts weitergeleitet (*geroutet*).

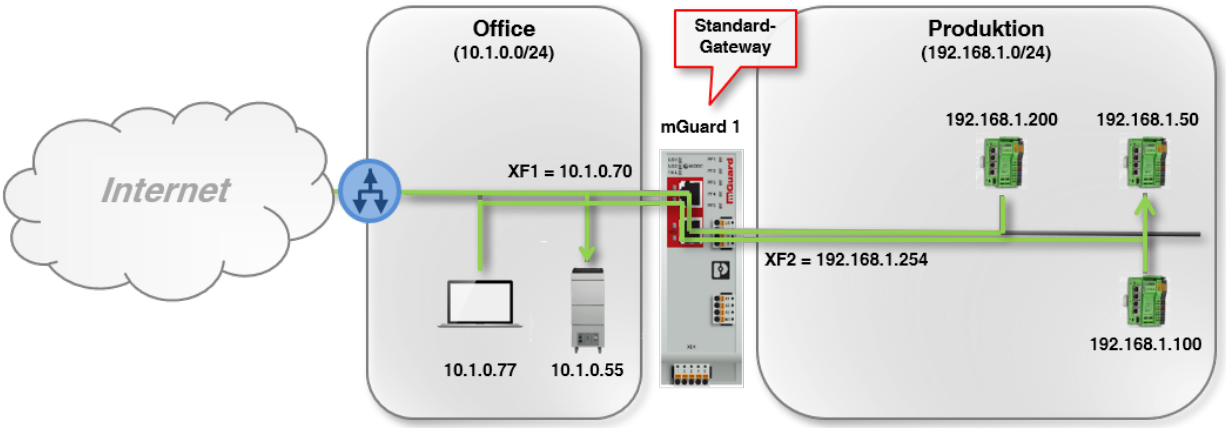


Bild 6-2 Beispiel: Router-Modus

Clients im Subnetz der einen Netzzone (z. B. *Office*) können mit Clients im Subnetz der anderen Netzzone (z. B. *Produktion*) kommunizieren und Daten austauschen.

Die Netzwerkkonfiguration der Netzzone 1 (XF1) des Geräts kann statisch eingetragen oder von einem DHCP-Server bezogen werden. In der Netzzone 2 (XF2–XF5) kann das Gerät selbst als DHCP-Server fungieren.

Die Sicherheits- und Firewall-Funktionen des Geräts werden auf eingehenden und durchgeleiteten (*gerouteten*) Datenverkehr angewendet.

Netzzone 1 (XF1)

(Nur konfigurierbar im Modus „*Router*“)

Die Netzwerkinterfaces des Geräts sind zwei unterschiedlichen Netzzonen zugeordnet, die jeweils über eine eigene Netzwerkkonfiguration (IPv4-Adresse und Netzmaske) verfügen.

Die über DHCP oder statisch konfigurierten Netzwerke der beiden Netzzonen dürfen sich nicht überlappen.

Über Netzzone 1 (XF1) wird in der Regel der Zugang zu externen Netzwerken oder zum Internet hergestellt.

Verbundene Netzwerk-Clients in der gleichen Netzzone (Subnetz) können das Gerät über die konfigurierte IP-Adresse erreichen.

Die Netzwerkadresse der Netzzone 1 (XF1) kann auf dem Gerät statisch konfiguriert oder per DHCP zugewiesen werden.

Damit das Gerät von angeschlossenen Clients als direktes Gateway verwendet werden kann, muss bei diesen die IP-Adresse der entsprechenden Netzzone des Geräts als Standard-Gateway angegeben werden.

Damit Geräte einer Netzzone mit Geräten anderer Netzzonen oder dem Internet kommunizieren können, muss auf dem Gerät gegebenenfalls NAT/IP-Masquerading aktiviert werden (siehe „NAT“ auf Seite 64).

Menü: Netzwerk >> Interfaces >> Interfaces

Router-Modus

(Nur konfigurierbar im Modus „*Router*“)

Modus, mit dem festgelegt wird, wie der Netzzone eine Netzwerkkonfiguration zugewiesen wird.

DHCP

Der Netzzone wird eine Netzwerkkonfiguration (IP-Adresse, Subnetzmaske und optional ein Standard-Gateway und DNS-Server) automatisch von einem DHCP-Server zugewiesen, wenn ein DHCP-Server im Netzwerk vorhanden ist.

Statisch

Der Netzzone muss eine statische Netzwerkkonfiguration vom Benutzer manuell zugewiesen werden (IP-Adresse, Subnetzmaske und optional ein Standard-Gateway).

Voreinstellung: DHCP

IP-Adresse

(Nur konfigurierbar im Router-Modus „*Statisch*“)

(Statusinformation im Router-Modus „*DHCP*“)

IP-Adresse des Netzwerkinterface XF1 (Netzzone 1).

Hinweis: Das Ändern der IP-Adresse, über die Sie aktuell auf das Gerät zugreifen, führt dazu, dass das Gerät nach dem Speichern der Konfiguration unter dieser Adresse nicht mehr erreichbar ist. Melden Sie sich über die geänderte IP-Adresse erneut an.

Eingabeformat: IPv4-Adresse

Netzmaske

(Nur konfigurierbar im Router-Modus „*Statisch*“)

(Statusinformation im Router-Modus „*DHCP*“)

Subnetzmaske, die definiert, in welchem Subnetz sich das Gerät befindet.

Eingabeformat: CIDR- oder Dezimal-Schreibweise, z. B. 24 (= 255.255.255.0)

Standard-Gateway

(Nur konfigurierbar im Router-Modus „*Statisch*“)

(Statusinformation im Router-Modus „*DHCP*“)

IP-Adresse des Standard-Gateways, an das das Gerät Verbindungsanfragen sendet, um unbekannte Subnetze oder das Internet zu erreichen.

Als Standard-Gateway kann sowohl ein Gerät im Subnetz der Netzzone 1 (XF1) als auch im Subnetz der Netzzone 2 (XF2–XF5) angegeben werden.

Ein leeres Feld ohne Eintrag bedeutet, dass kein Standard-Gateway auf dem Gerät konfiguriert ist.

Eingabeformat: IPv4-Adresse

DNS-Server

(Statusinformation im Router-Modus „*DHCP*“)

Vom DHCP-Server zugewiesene IP-Adressen eines oder mehrerer DNS-Server.

Ein DNS-Server (DNS = *Domain Name System*) ermöglicht es Clients, Hostnamen in IP-Adressen aufzulösen.

Hinweis: Wird die Netzwerkkonfiguration vom DHCP-Server zugewiesen, ist die Auswahl der voreingestellten DNS-Root-Server oder die Konfiguration benutzerdefinierter DNS-Server nicht möglich (siehe „Externer DNS-Server“ auf Seite 78).

Das gilt auch, wenn der DHCP-Server keinen DNS-Server zuweist.

Menü: Netzwerk >> Interfaces >> Interfaces

Netzzone 2 (XF2–XF5)

(Nur konfigurierbar im Modus „*Router*“)

Die Netzwerkinterfaces des Geräts sind zwei unterschiedlichen Netzzonen zugeordnet, die jeweils über eine eigene Netzwerkkonfiguration (IPv4-Adresse/Netzmaske) verfügen.

Die über DHCP oder statisch konfigurierten Netzwerke der beiden Netzzonen dürfen sich nicht überlappen.

Über Netzzone 2 (XF2–XF5) wird in der Regel der Zugang zum lokalen (geschützten) Netzwerk hergestellt.

Verbundene Netzwerk-Clients in der gleichen Netzzone (Subnetz) können das Gerät über die konfigurierte IP-Adresse erreichen.

Die Netzwerkadresse der Netzzone 2 (XF2–XF5) muss statisch konfiguriert werden. Sie kann im Unterschied zur Netzzone 1 (XF1) nicht per DHCP zugewiesen werden.

Damit das Gerät von angeschlossenen Clients als direktes Gateway verwendet werden kann, muss bei diesen die IP-Adresse der entsprechenden Netzzone des Geräts als Standard-Gateway angegeben werden.

Damit Geräte einer Netzzone mit Geräten anderer Netzzonen oder dem Internet kommunizieren können, muss auf dem Gerät gegebenenfalls NAT/IP-Masquerading aktiviert werden (siehe „NAT“ auf Seite 64).

IP-Adresse

IP-Adresse des Netzwerkinterface XF2–XF5 (Netzzone 2).

Hinweis: Das Ändern der IP-Adresse, über die Sie aktuell auf das Gerät zugreifen, führt dazu, dass das Gerät nach dem Speichern der Konfiguration unter dieser Adresse nicht mehr erreichbar ist. Melden Sie sich über die geänderte IP-Adresse erneut an.

Eingabeformat: IPv4-Adresse

Voreinstellung: 192.168.1.1

Netzmaske

Subnetzmaske, die definiert, in welchem Subnetz sich das Gerät befindet.

Eingabeformat: CIDR- oder Dezimal-Schreibweise, z. B. 24 (= 255.255.255.0)

Voreinstellung: 24

Menü: Netzwerk >> Interfaces >> Interfaces

Stealth-Modus

Der Stealth-Modus wird dazu verwendet, einen einzelnen oder mehrere lokale Clients in einem bestehenden Subnetz (z. B. die Maschinensteuerungen in einem Produktions-Netzwerk) vor unerwünschten Netzwerkzugriffen zu schützen, ohne dass deren IP-Einstellungen geändert werden müssen.

Das Gerät wird dazu über seine beiden Netzwerkinterfaces (Netzzonen) zwischen den Clients und dem umgebenden Subnetz eingefügt, sodass der gesamte Datenverkehr von und zu den Clients durch das Gerät geleitet wird.

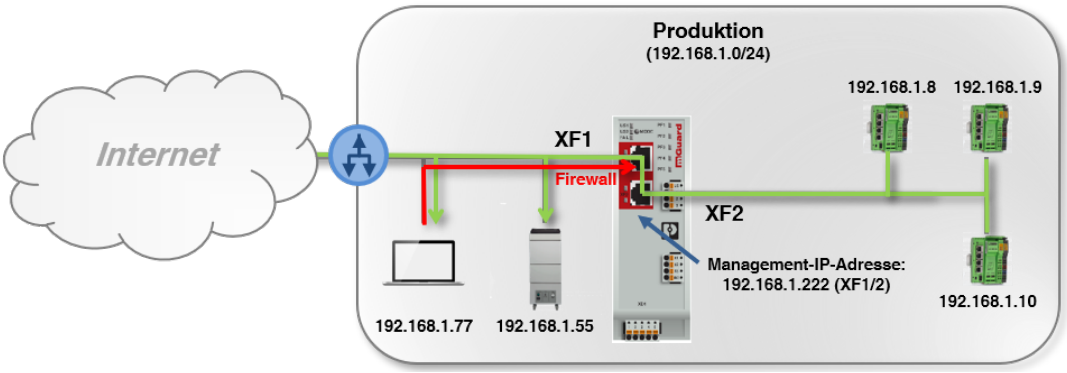


Bild 6-3 Beispiel: Stealth-Modus (mit aktivierter Firewall XF1 --> XF2)

Die Netzwerkkonfiguration der angeschlossenen Clients muss nicht geändert werden.

Die Serverdienste DHCP-, NTP-, SNMP- und DNS-Server sind auf dem Gerät deaktiviert. Sicherheits- und Firewall-Funktionen des Geräts werden grundsätzlich auf eingehenden und durchgeleiteten Datenverkehr angewendet.

(Stealth-Modus)
(Nur konfigurierbar im Modus „*Stealth*“)

Management-IP-Adresse

IP-Adresse, über die das Gerät im Stealth-Modus erreichbar ist und administriert werden kann. Die Management-IP-Adresse ist auf allen Netzwerkinterfaces (Netzzonen) verfügbar.

Die Konfiguration des Geräts erfolgt über das WBM oder die *Config API*.

Hinweis: Das Ändern der IP-Adresse, über die Sie aktuell auf das Gerät zugreifen, führt dazu, dass das Gerät nach dem Speichern der Konfiguration unter dieser Adresse nicht mehr erreichbar ist. Melden Sie sich über die geänderte IP-Adresse erneut an.

Eingabeformat: IPv4-Adresse

Voreinstellung: 192.168.1.1

Netzmaske

Subnetzmaske, die definiert, in welchem Subnetz das Gerät im Stealth-Modus über die Management-IP-Adresse erreichbar ist.

Eingabeformat: CIDR- oder Dezimal-Schreibweise, z. B. 24 (= 255.255.255.0)

Voreinstellung: 24

Menü: Netzwerk >> Interfaces >> Interfaces		
	Standard-Gateway	IP-Adresse des Standard-Gateways, an das das Gerät Verbindungsanfragen sendet, um unbekannte Subnetze oder das Internet zu erreichen. Im Stealth-Modus ist es dem Gerät damit möglich, als Client z. B. Anfragen an einen NTP- oder DNS-Server zu senden. Wird eine Management-IP-Adresse vergeben, muss das Standard-Gateway des Netzes, in dem sich das Gerät befindet, angegeben werden. Das Standard-Gateway kann sowohl über Netzzone 1 (XF1) als auch über Netzzone 2 (XF2–XF5) erreichbar sein. **Eingabeformat:** IPv4-Adresse **Voreinstellung:** 192.168.1.254

6.1.2 Routen

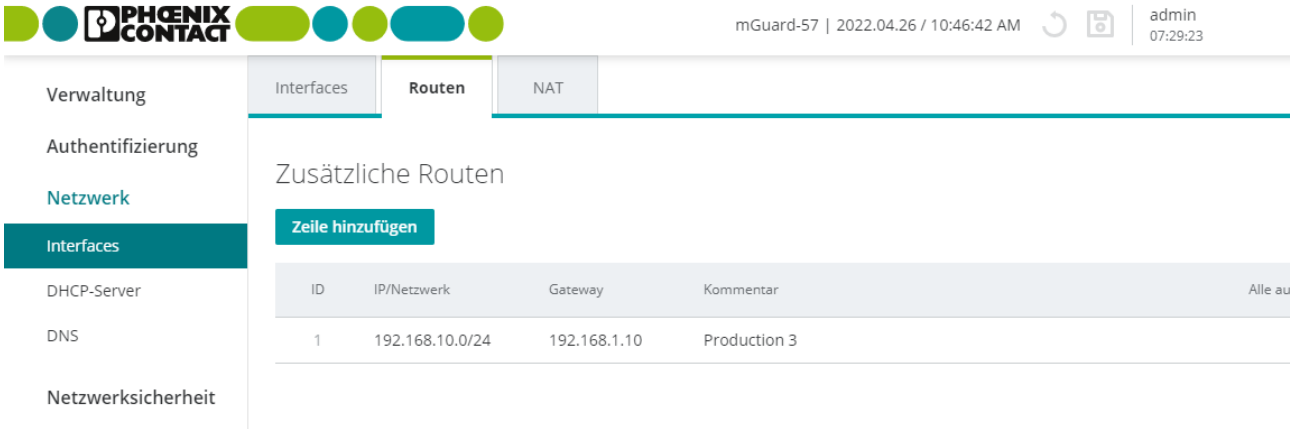


Bild 6-4 Netzwerk >> Interfaces >> Routen: Statische Routen konfigurieren

Menü: Netzwerk >> Interfaces >> Routen

Routen

(Nur konfigurierbar im Modus „*Router*“)

Über statisch eingetragene Routen kann das Gerät Netzwerkziele erreichen, die seinem Standard-Gateway nicht bekannt sind.

Diese Ziele können ebenfalls von angeschlossenen Netzwerk-Clients erreicht werden, die ihrerseits das Gerät als Gateway verwenden.

Datenpakete an Ziele, die über die statische Route erreicht werden können, werden vom Gerät direkt an das in der statischen Route angegebene Gateway weitergeleitet.

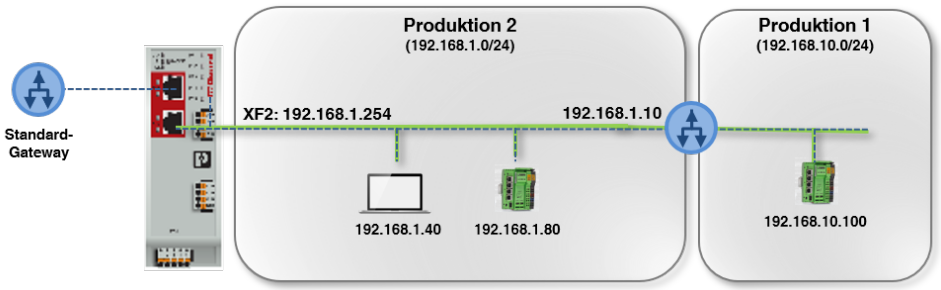


Bild 6-5 Beispiel: Zusätzliche statische Routen

Anfragen von Clients in *Produktion 2*, die Ziele im Subnetz 192.168.10.0/24 erreichen wollen, werden vom Gerät über die statische Route 192.168.1.10 weitergeleitet.

IP/Netzwerk

Ziel (Netzwerk oder IP-Adresse), das über eine zusätzliche Route erreicht werden soll.

Eingabeformat: IPv4-Adresse, IPv4-Netzwerk (CIDR-Notation)

Gateway

IP-Adresse des Gateways, über das das Ziel über die zusätzliche Route erreichbar ist.

Eingabeformat: IPv4-Adresse

Kommentar

Frei wählbarer Kommentar.

Erlaubte Zeichen: max. 128

6.1.3 NAT

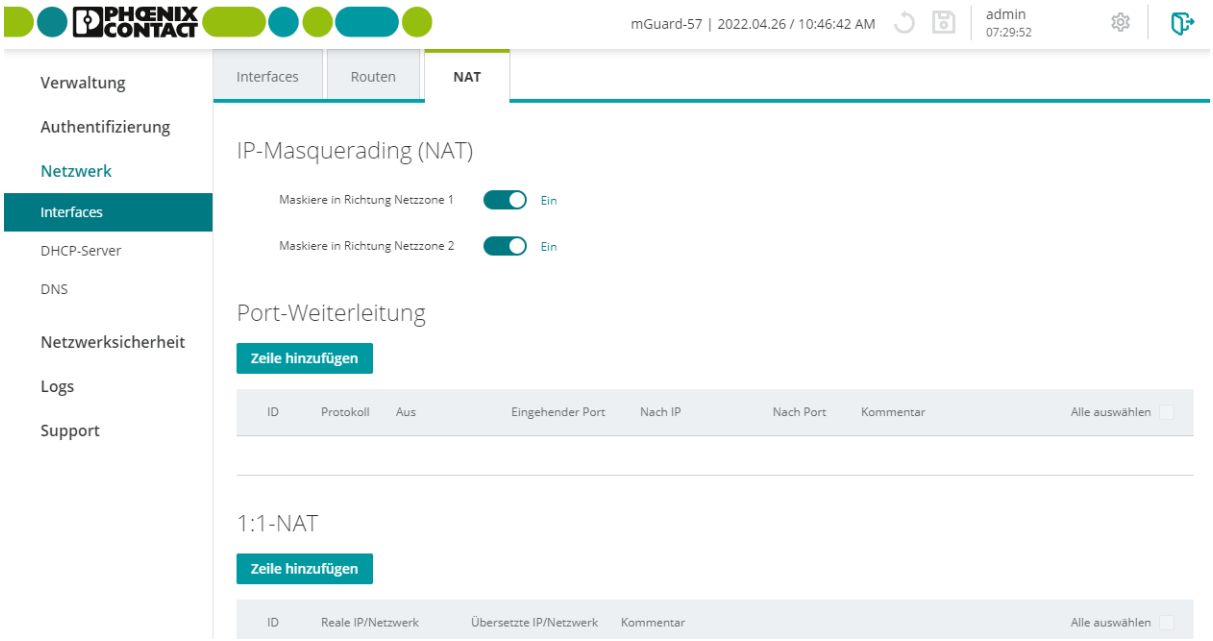


Bild 6-6 Netzwerk >> Interfaces >> NAT: IP-Masquerading, Port-Weiterleitung und 1:1-NAT konfigurieren

Menü: Netzwerk >> Interfaces >> NAT	
Network Address Translation (NAT) (Nur konfigurierbar im Modus „*Router*“)	**IP-Masquerading und 1:1-NAT** *Network Address Translation* (NAT) wird verwendet, um die reale IP-Adresse von angeschlossenen Netzwerk-Clients vor externen Netzwerkteilnehmern zu verbergen. Das Gerät ersetzt dazu, in seiner Funktion als NAT-Router, die im IP-Header angegebene Absenderadresse eines anfragenden Clients durch – seine eigene IP-Adresse (**„IP-Masquerading (NAT)“**) oder – eine übersetzte (virtuelle) IP-Adresse (**„1:1-NAT“**). Mit dieser (übersetzten) IP-Adresse als Absenderadresse leitet das Gerät Anfragen an externe Netzwerkteilnehmer weiter. Diese senden ihre Antwortpakete an die (übersetzte) Absenderadresse, die vom Gerät wiederum in die reale IP-Adresse des anfragenden Clients umgeschrieben wird. Im Falle von 1:1-NAT können Netzwerkteilnehmer auch eigenen Anfragen an die übersetzte IP-Adresse senden. Somit kann z. B. ein ganzes („privates“) Netzwerk hinter dem Gerät versteckt werden. Die realen IP-Adressen der Clients im „privaten“ Netz bleiben bei der Kommunikation mit dem anderen Netzwerk verborgen. Siehe **„IP-Masquerading (NAT)“ auf Seite 65** und **„1:1-NAT“ auf Seite 70**. **Port-Weiterleitung** Port-Weiterleitung bewirkt, dass Datenpakete, die (von außen) an einen bestimmten Port des Geräts gesendet werden, an eine definierte Ziel-IP-Adresse und einen definierten Ziel-Port im (lokalen) Subnetz des Geräts weitergeleitet werden. Siehe **„Port-Weiterleitung“ auf Seite 67**.

Menü: Netzwerk >> Interfaces >> NAT

IP-Masquerading (NAT)

(Nur konfigurierbar im Modus „*Router*“)

Beim **IP-Masquerading** maskiert das Gerät Absender-IP-Adressen von Netzwerk-Clients mit seiner eigenen IP-Adresse, um z. B. Netzwerkstrukturen zu verbergen:

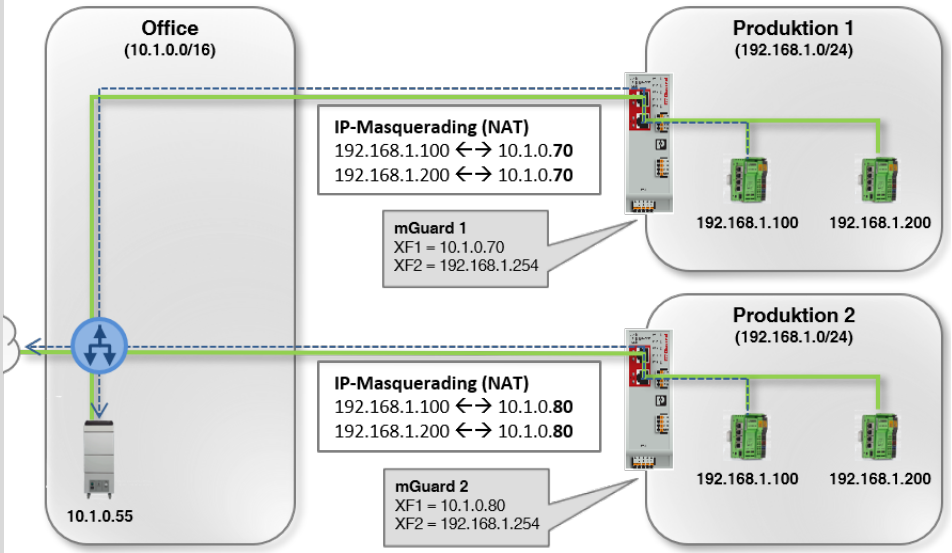
Senden Netzwerk-Clients Daten durch das Gerät, ersetzt dieses deren Quell-IP-Adressen (*src_ip*) durch seine eigene IP-Adresse (des ausgehenden Interfaces).

Den Empfängern der Daten wird als Quell-IP-Adresse immer die IP-Adresse des mGuard-Geräts mitgeteilt. Sie senden ihre Antwortpakete folglich an das mGuard-Gerät zurück, das diese wiederum an den ursprünglichen Absender (Netzwerk-Client) weiterleitet.

Die IP-Adressen der anfragenden Clients und die dazugehörige Netzwerkstruktur wird maskiert und bleibt den externen Netzwerkteilnehmern verborgen.

Die Verbindungsdaten in den Datenpaketen der Anfragen werden in einer *Connection Tracking*-Tabelle gespeichert und mit den Verbindungsdaten der Antworten verglichen.

Soll ein Zugriff auf die maskierten Clients von außen erfolgen, kann die IP-Adresse des Geräts dazu **nicht** verwendet werden. Bei Anfragen von außen müssen die maskierten Clients unter ihrer realen IP-Adresse kontaktiert werden. (Das Netzwerk und die generellen Routing-Einstellungen müssen dazu entsprechend konfiguriert sein.)



Anfragen der **SPS (Produktion)** werden an die IP-Adresse des **Office-Servers (10.1.0.55)** gesendet und mit der IP-Adresse des **mGuard-Geräts (10.1.0.70** bzw. **10.1.0.80)** als Absender-Adresse maskiert.

Bild 6-7 Beispiel: IP-Masquerading in Richtung Netzzone 1

Beispiel

IP-Masquerading wird häufig verwendet, wenn die „privaten“ IP-Adressen extern nicht geroutet werden können oder sollen, z. B. weil ein privater Adressbereich wie 192.168.1.x oder die interne Netzstruktur eines Produktions-Netzwerks verborgen werden sollen.

Mehrere Produktionszellen mit identischer IP-Einstellung können so leicht in die Netzwerk-Infrastruktur integriert werden.

Menü: Netzwerk >> Interfaces >> NAT		
	Maskiere in Richtung Netzzone 1	Bei aktivierter Funktion wird die NAT-Masquerading-Regel auf Datenpakete (Anfragen) angewendet, die das Gerät auf dem ausgewählten Netzwerkinterface (XF1 / Netzzone 1) verlassen. Die IP-Adresse des Absenders wird im Datenpaket auf die IP-Adresse des Netzwerkinterface (XF1 / Netzzone 1) umgeschrieben. **Voreinstellung:** aktiviert
	Maskiere in Richtung Netzzone 2	Bei aktivierter Funktion wird die NAT-Masquerading-Regel auf Datenpakete (Anfragen) angewendet, die das Gerät auf dem ausgewählten Netzwerkinterface (XF2–XF5 / Netzzone 2) verlassen. Die IP-Adresse des Absenders wird im Datenpaket auf die IP-Adresse des Netzwerkinterface (XF2–XF5 / Netzzone 2) umgeschrieben. **Voreinstellung:** deaktiviert

Menü: Netzwerk >> Interfaces >> NAT

Port-Weiterleitung

(Nur konfigurierbar im Modus „*Router*“)

Port-Weiterleitung bewirkt, dass Datenpakete, die an die IP-Adresse und einen bestimmten Port des Geräts gesendet werden, an eine andere Ziel-IP-Adresse und einen anderen Ziel-Port im Netzwerk weitergeleitet werden.

Die ursprüngliche Ziel-IP-Adresse und der ursprüngliche Ziel-Port im Header des eingehenden Datenpakets werden dabei der Port-Weiterleitungs-Regel entsprechend umgeschrieben.

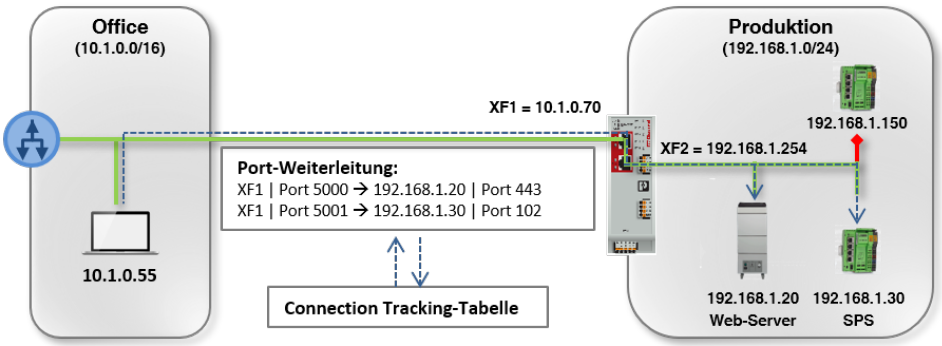
Port-Weiterleitung

Zeile hinzufügen

ID	Protokoll	Aus	Eingehender Port	Nach IP	Nach Port	Kommentar
1	TCP	Netzzone 1	5000	0.0.0.0	443	
2	UDP	Netzzone 1	5001	0.0.0.0	102	

Das Umschreiben des Headers wird in die *Connection Tracking*-Tabelle des Geräts eingetragen. Antwortpakete werden mit diesen Einträgen verglichen und die Header-Daten wieder auf die ursprünglichen Werte umgeschrieben.

Die Firewall erlaubt automatisch den in einer Port-Weiterleitungsregel definierten Datenverkehr von und zu den definierten IP-Adressen und Ports.



Anfragen an den **Web-Server** (**Port 443**) sendet der Office-Client (10.1.0.55) an die IP-Adresse **10.1.0.70** (Port **5000**)
Anfragen an die **SPS** (**Port 102**) sendet der Office-Client (10.1.0.55) an die IP-Adresse **10.1.0.70 (**Port **5001**)

Bild 6-8 Beispiel: Port-Weiterleitung

Beispiel

Port-Weiterleitung wird häufig dazu verwendet, einzelne Geräte bzw. Serverdienste in einem lokalen Netzwerk (z. B. Web-Server) aus dem externen Netzwerk oder dem Internet gezielt erreichbar zu machen (siehe Abbildung):

– Der **Web-Server (192.168.1.20 / Port 443)** im Produktions-Netzwerk ist aus dem Office-Netzwerk über die IP-Adresse des Geräts (**XF1 = 10.1.0.70**) und Port **5000** erreichbar.
– Die **SPS (192.168.1.30 / Port 102)** im Produktions-Netzwerk ist aus dem Office-Netzwerk über die IP-Adresse des Geräts (**XF1 = 10.1.0.70**) und Port **5001** erreichbar.

Alle anderen Geräte im Produktions-Netzwerk (z. B. SPS 192.168.1.150) sollen von außen nicht erreichbar sein. Sie sind durch die Firewall geschützt.

Menü: Netzwerk >> Interfaces >> NAT

Port-Weiterleitungs-Regeln werden vor Firewall-Regeln angewendet

Die Regeln zur Port-Weiterleitung werden angewendet, bevor die konfigurierten Firewall-Regeln für durchgehenden/gerouteten Datenverkehr angewendet werden (siehe Kapitel 7).

Das heißt, eine Firewall-Regel, die allen eingehenden Datenverkehr blockiert, würde beim Zutreffen einer Port-Weiterleitungs-Regel nicht angewendet.

ID	Identifikationsnummer der Regel (vom System generiert) Die ID bestimmt die Reihenfolge, in der die Regeln angewendet werden, beginnend mit der niedrigsten ID.
Protokoll	**TCP, UDP** Netzwerkprotokoll, das für die Übertragung der Datenpakete verwendet werden muss, damit die Regel angewendet wird. **Voreinstellung:** TCP
Aus	**Netzzone 1, Netzzone 2** Netzzone, aus der Datenpakete an das Gerät gesendet werden müssen, damit die Regel angewendet wird. **Voreinstellung:** Netzzone 2
Eingehender Port	Netzwerk-Port des Geräts, an den Datenpakete gesendet werden müssen, damit die Regel angewendet wird. Datenpakete, die an diesen Port gesendet werden, werden an die in der Regel festgelegte Ziel-IP-Adresse (*Nach IP*) und den definierten Ziel-Port (*Nach Port*) weitergeleitet: – Die Ziel-IP-Adresse im Header des Datenpakets wird auf die in der Regel definierte Ziel-IP-Adresse (*Nach IP*) umgeschrieben. – Der Ziel-Port im Header des Datenpakets wird auf den in der Regel definierten Ziel-Port (*Nach Port*) umgeschrieben. **Eingabeformat:** 1 – 65535, unter Ausschluss folgender Ports, da sie von Diensten des Geräts verwendet werden: DNS (53), HTTPS (443), NTP (123), SNMP (161), DHCP (67, 68) **Voreinstellung:** 1
Nach IP	IP-Adresse des Ziel-Clients, an die eingehende Datenpakete weitergeleitet werden, wenn die Regel angewendet wird. Die Original-Ziel-Adresse im Header des Datenpakets wird auf diese IP-Adresse umgeschrieben. **Eingabeformat:** IPv4-Adresse **Voreinstellung:** 0.0.0.0

Menü: Netzwerk >> Interfaces >> NAT		
	Nach Port	Netzwerk-Port, an den eingehende Datenpakete weitergeleitet werden, wenn die Regel angewendet wird. Der Original-Ziel-Port im Header des Datenpakets (siehe „Eingehender Port“) wird auf diesen Port umgeschrieben. **Eingabeformat:** 1 – 65535 **Voreinstellung:** 1
	Kommentar	Frei wählbarer Kommentar. Erlaubte Zeichen: max. 128

Menü: Netzwerk >> Interfaces >> NAT

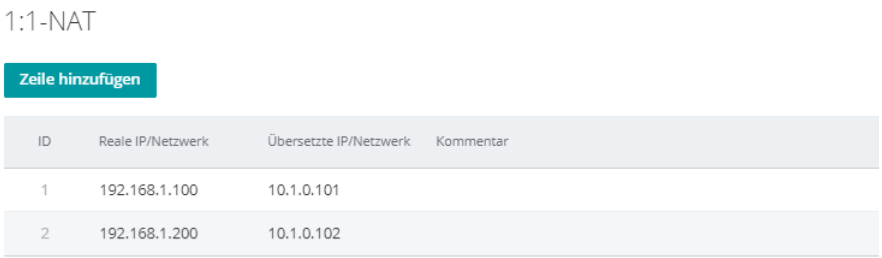
1:1-NAT

(Nur konfigurierbar im Modus „*Router*“)

Ein **reales Netzwerk** wird in einem **übersetzten (virtuellen) Netzwerk** abgebildet.

Die IP-Adressen der Clients im realen Netzwerk werden entsprechend der 1:1-NAT-Regel so umgeschrieben, dass die Kommunikation mit Clients im anderen (übersetzten) Netzwerk nicht über die realen, sondern über die übersetzten IP-Adressen stattfindet.

Das reale Netzwerk (zumeist privat) bleibt damit vor den Netzwerkteilnehmern im anderen Netzwerk (zumeist öffentlich) verborgen.



Beispiel 1

Maschinensteuerungen (SPS) im Produktions-Netzwerk sind mit ihren realen IP-Adressen vor Netzwerkteilnehmern im Office-Netzwerk verborgen. Sie kommunizieren mit dem Office-Netzwerk über ihre übersetzten IP-Adressen (z. B. 192.168.1.100 <--> 10.1.0.100).

Für Anfragen aus dem Office-Netzwerk, sind sie über ihre übersetzten IP-Adressen erreichbar. ARP-Anfragen aus dem Office-Netzwerk werden stellvertretend vom mGuard-Gerät beantwortet.

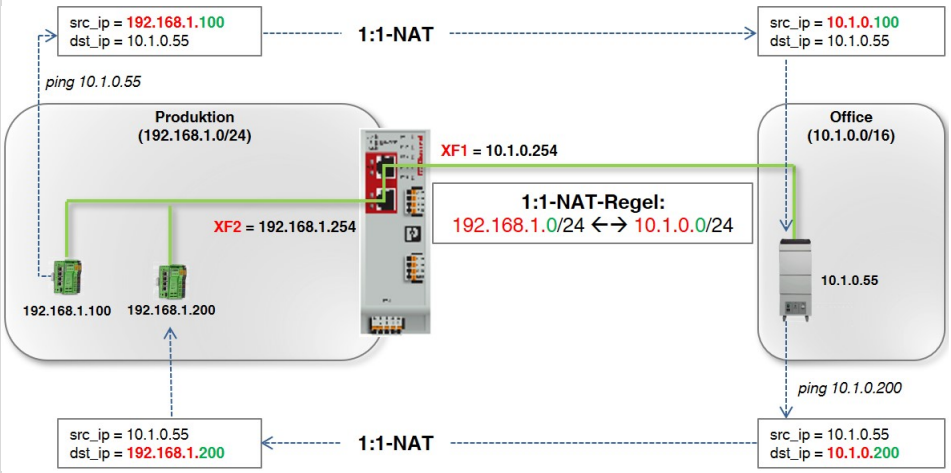


Bild 6-9 Beispiel: 1:1-NAT (zwei Netzwerke)

Menü: Netzwerk >> Interfaces >> NAT

Beispiel 2

In der Praxis wird in unterschiedlichen Produktionszellen häufig eine identische IP-Konfiguration für angebundene Maschinen verwendet. Das würde zu Adresskonflikten führen.

Um das Problem mittels 1:1-NAT zu lösen, ersetzt das Gerät den Netzwerkteil der realen IP-Adressen der Clients in den Produktions-Netzwerken jeweils durch den Netzwerkteil eines Subnetzes im Office-Netzwerk: z. B. 192.168.1.0/24 <--> 10.1.1.0/24.

Clients im Office- und in den Produktions-Netzwerken können nun in beide Richtungen miteinander kommunizieren.

ARP-Anfragen aus dem Office-Netzwerk werden automatisch und stellvertretend vom mGuard-Gerät beantwortet.

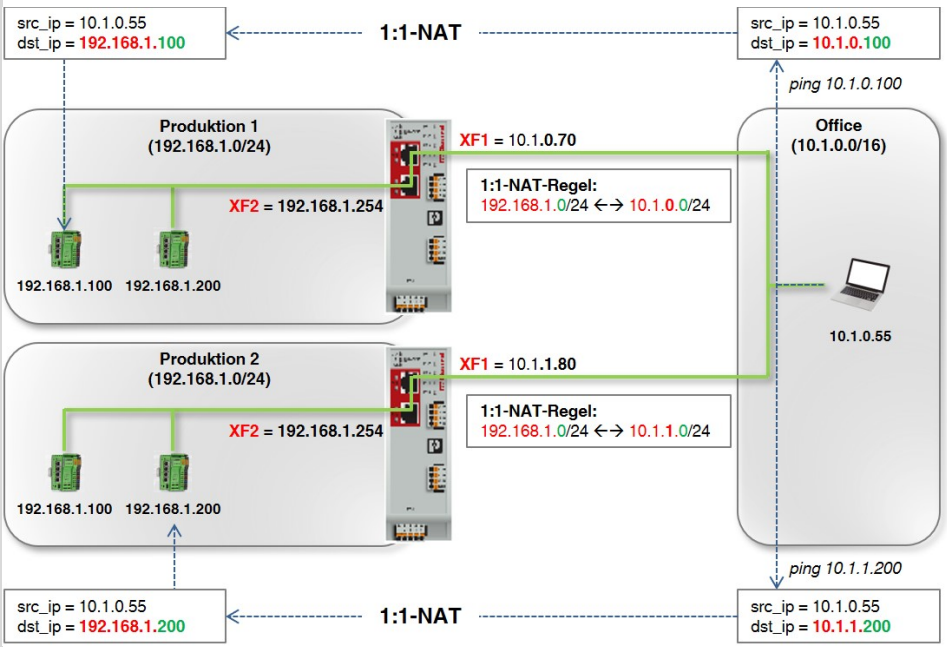


Bild 6-10 Beispiel: 1:1-NAT (identische Netze)

ID Identifikationsnummer der Regel (vom System generiert)

Die ID bestimmt die Reihenfolge, in der die Regeln angewendet werden, beginnend mit der niedrigsten ID.

Menü: Netzwerk >> Interfaces >> NAT

Reale IP/Netzwerk

Der Datenverkehr, der von oder an Netzwerk-Clients des realen Netzwerks gesendet wird, unterliegt der 1:1-NAT-Regel.

1:1-NAT

Beim 1:1-NAT wird der Netzwerkteil (rot) der IP-Adressen von Clients im realen Netzwerk auf den Netzwerkteil eines anderen (übersetzten) Netzwerks umgeschrieben (siehe Beispiel).

Der den Clients zugeordnete Hostteil (grün) der IP-Adressen wird unverändert beibehalten.

Beispiel (Bild 6-9 und 6-10)

1:1-NAT-Regel: 192.168.1.0/**24** <-> 10.1.0.0/**24**

⇒ **Übersetzung:** 192.168.1.100 <-> 10.1.0.100

⇒ **Übersetzung:** 192.168.1.200 <-> 10.1.0.200

Der Netzwerk- und der Hostteil einer IP-Adresse werden durch die Subnetzmaske definiert (z. B. 192.168.70.80/**16** oder 10.1.1.30/**24**).

Reale IP

Ist die Netzmaske 32, werden einzelne IP-Adressen und keine Netzwerke durch die 1:1-NAT-Regel übersetzt:

Hinweis: Die Netzmaske **/32** darf in der Konfiguration in der Config API nicht verwendet werden. Die IP-Adresse muss stattdessen ohne Netzmaske angegeben werden.

1:1-NAT-Regel: 192.168.1.40 <-> 10.1.5.40

⇒ **Übersetzung:** 192.168.1.40 <-> 10.1.5.40

Praxis

Clients in beiden Netzwerken können in beide Richtungen miteinandern kommunizieren. Dabei ist das reale (zumeist private) Netzwerk im anderen (zumeist öffentlichen) Netzwerk nicht sichtbar:

– Als Absenderadresse der Clients im realen Netzwerk erscheint den Netzwerkteilnehmern im anderen Netzwerk jeweils deren übersetzte IP-Adresse.
– Um Clients im realen Netzwerk aus dem anderen Netzwerk zu erreichen, muss deren übersetzte IP-Adresse verwendet werden.
– ARP-Anfragen an die übersetzten IP-Adressen der Clients im realen Netzwerk werden automatisch und stellvertretend vom Gerät beantwortet.

Voraussetzung

– Das reale und das übersetzte Netzwerk müssen die gleiche Subnetzmaske verwenden.
– Die übersetzten IP-Adressen der Clients im realen Netzwerk dürfen im anderen (übersetzten) Netzwerk noch nicht vergeben sein.
– Firewall-Regeln werden grundsätzlich auch auf übersetzte IP-Adressen angewendet.

Eingabeformat: IPv4-Adresse, IPv4-Netzwerk (CIDR-Notation)

Menü: Netzwerk >> Interfaces >> NAT		
	Übersetzte IP/Netzwerk	Das Netzwerk, auf das die realen IP-Adressen der Clients aus dem realen Netzwerk umgeschrieben werden sollen (siehe „Reale IP/Netzwerk“). **Voraussetzung** – Das reale und das übersetzte Netzwerk müssen die gleiche Subnetzmaske verwenden. – Die übersetzten IP-Adressen der Clients im realen Netzwerk dürfen im anderen (übersetzten) Netzwerk noch nicht vergeben sein. **Übersetzte IP** Ist die Netzmaske 32, werden einzelne IP-Adressen und keine Netzwerke durch die 1:1-NAT-Regel übersetzt. **Eingabeformat:** IPv4-Adresse, IPv4-Netzwerk (CIDR-Notation)
	Kommentar	Frei wählbarer Kommentar. Erlaubte Zeichen: max. 128

6.2 DHCP-Server

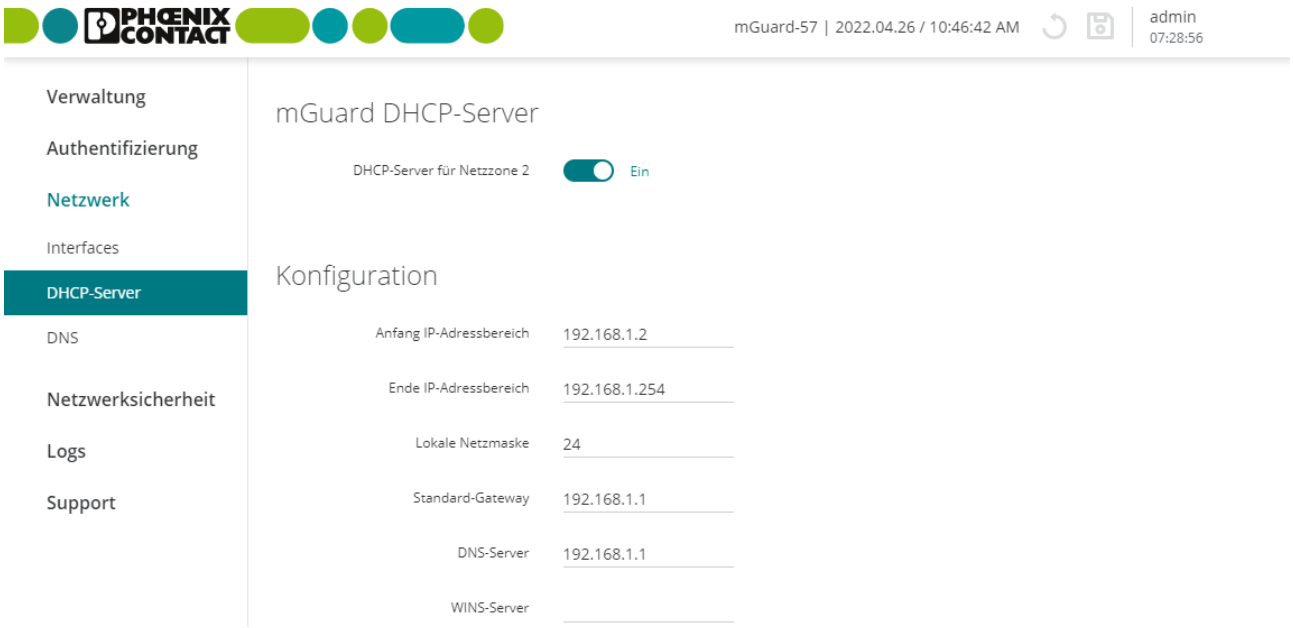


Bild 6-11 Netzwerk >> DHCP-Server: DHCP-Server konfigurieren

Menü: Netzwerk >> DHCP-Server		
mGuard DHCP-Server	Über das *Dynamic Host Configuration Protocol* (DHCP) wird anfragenden Netzwerk-Clients automatisch eine Netzwerkkonfiguration zugewiesen. Angeschlossene Clients müssen so konfiguriert sein, dass sie eine DHCP-Anfrage senden, um eine Netzwerkkonfiguration von einem DHCP-Server zu erhalten. Im anderen Fall muss die Konfiguration bei jedem Client einzeln statisch konfiguriert werden.	
	DHCP-Server für Netzzone 2	Bei aktivierter Funktion wird anfragenden Clients, die über Netzzone 2 mit dem Gerät verbunden sind, eine Netzwerkkonfiguration zugewiesen. **Hinweis:** Die Anfragen an den UDP-Port 67 werden unabhängig von den Einstellungen in den Firewall-Tabellen des Geräts immer angenommen, wenn der DHCP-Server aktiviert ist. Der Server weist den Clients dann IP-Adressen aus dem konfigurierten IP-Adressbereich zu. **Voreinstellung:** aktiviert
Konfiguration (Nur konfigurierbar, wenn der DHCP-Server für Netzzone 2 aktiviert ist.)	**Anfang IP-Adressbereich**	Anfang des IP-Adressbereichs, aus dem der DHCP-Server anfragenden Clients IP-Adressen zuweist. Der Bereich sollte so gewählt werden, dass die in ihm enthaltenen IP-Adressen in dem zugewiesenen Subnetz erreichbar sind (siehe unten „„Lokale Netzmaske““). **Eingabeformat:** IPv4-Adresse **Voreinstellung:** 192.168.1.2

Menü: Netzwerk >> DHCP-Server		
	Ende IP-Adressbereich	Ende des IP-Adressbereichs, aus dem der DHCP-Server anfragenden Clients IP-Adressen zuweist. Der Bereich sollte so gewählt werden, dass die in ihm enthaltenen IP-Adressen in dem zugewiesenen Subnetz erreichbar sind (siehe unten „Lokale Netzmaske“). **Eingabeformat:** IPv4-Adresse **Voreinstellung:** 192.168.1.254
	Lokale Netzmaske	Subnetzmaske, die der DHCP-Server anfragenden Clients zuweist. Der Bereich, aus dem Netzwerk-Clients IP-Adressen zugewiesen werden, sollte so gewählt werden, dass die IP-Adressen in dem zugewiesenen Subnetz erreichbar sind (siehe oben „Anfang“ bzw. „Ende IP-Adressbereich“). **Eingabeformat:** CIDR- oder Dezimal-Schreibweise, z. B. 24 (= 255.255.255.0) **Voreinstellung:** 24
	Standard-Gateway	IP-Adresse des Standard-Gateways, die der DHCP-Server anfragenden Clients zuweist. Dies ist in der Regel die interne IP-Adresse des Geräts. **Eingabeformat:** IPv4-Adresse **Voreinstellung:** 192.168.1.1
	DNS-Server	IP-Adresse eines DNS-Servers, die der DHCP-Server anfragenden Clients zuweist. Ein DNS-Server (DNS = *Domain Name System*) ermöglicht es Clients, Hostnamen in IP-Adressen aufzulösen. Wenn der DNS-Server des Geräts genutzt werden soll, muss die IP-Adresse der Netzzone angegeben werden, auf der dieser Dienst aktiv ist (werkseitige Voreinstellung: Netzzone 2 = 192.168.1.1). **Eingabeformat:** IPv4-Adresse **Voreinstellung:** 192.168.1.1
	WINS-Server	IP-Adresse eines WINS-Servers, die der DHCP-Server anfragenden Clients zuweist. Ein WINS-Server (*Windows Internet Naming Service*) ermöglicht es Clients, Hostnamen (*NetBIOS*-Namen) in IP-Adressen aufzulösen. **Eingabeformat:** IPv4-Adresse **Voreinstellung:** leer

6.3 DNS

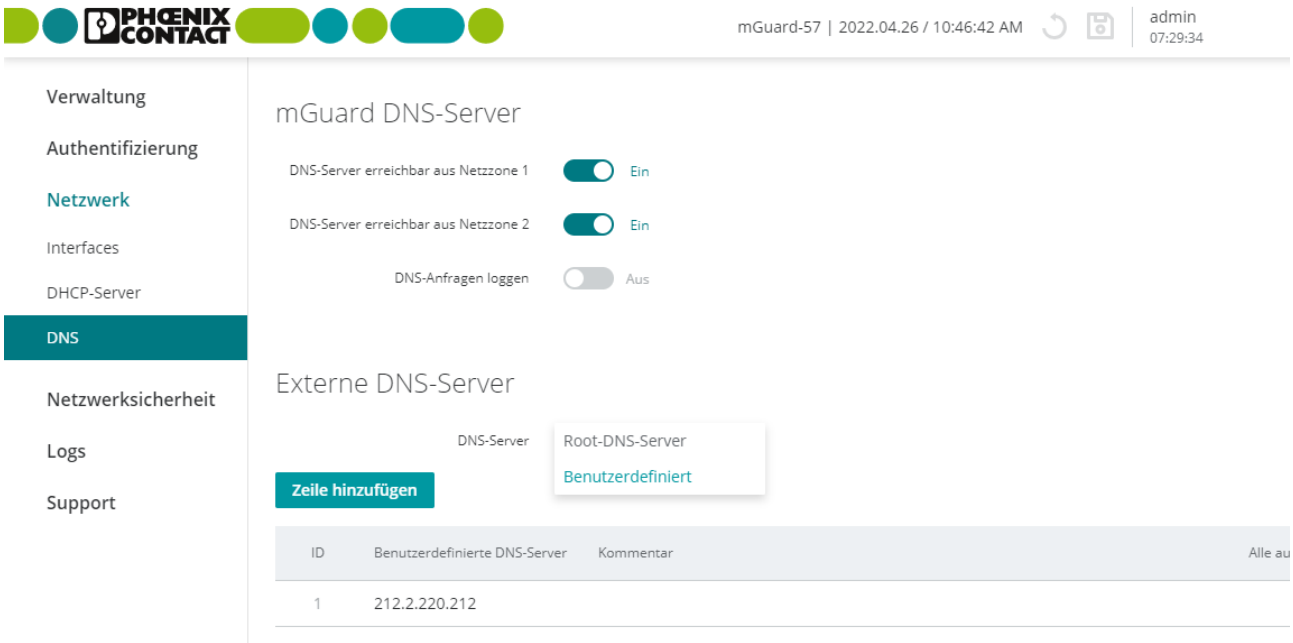


Bild 6-12 Netzwerk >> DNS: DNS-Server und DNS-Client konfigurieren

Menü: Netzwerk >> DNS	
mGuard DNS-Server	Soll das Gerät eine Verbindung zu einer Gegenstelle aufbauen (z. B. zu einem NTP-Server), deren Adresse in Form eines Hostnamens angegeben ist (z. B. *ntp-server.com*), dann muss das Gerät ermitteln, welche IP-Adresse sich hinter dem Hostnamen verbirgt. Dazu nimmt das Gerät als **DNS-Client** Verbindung zu einem **externen DNS-Server** auf, um dort die zugehörige IP-Adresse zu erfragen. Die vom DNS-Server zurückgegebene Information zu einer Anfrage, d. h. die Auflösung eines Hostnamens in eine IP-Adresse, wird im DNS-Cache des Geräts gespeichert. 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-Gerät nur vertrauenswürdige und abgesicherte DNS-Server aus Ihrem internen Firmennetzwerk, um entsprechende Angriffe zu vermeiden. Mit dem Gerät verbundene Netzwerk-Clients können das Gerät ihrerseits als **mGuard DNS-Server** verwenden und DNS-Anfragen an das Gerät senden. Beziehen die angeschlossenen Clients ihre Netzwerkkonfiguration per DHCP vom Gerät, wird ihnen das Gerät automatisch als DNS-Server zugewiesen.

Menü: Netzwerk >> DNS		
	DNS-Server erreichbar aus Netzzone 1	Bei aktivierter Funktion wird der Zugriff auf den DNS-Server des Geräts aus der ausgewählten Netzzone erlaubt (UDP/TCP-Port 53). **ACHTUNG: Zugriff aus dem Internet** Der Server ist möglicherweise aus dem Internet erreichbar, wenn das Gerät über die aktivierte Netzzone mit dem Internet verbunden ist. **Voreinstellung:** deaktiviert
	DNS-Server erreichbar aus Netzzone 2	Bei aktivierter Funktion wird der Zugriff auf den DNS-Server des Geräts aus der ausgewählten Netzzone erlaubt (UDP/TCP-Port 53). **ACHTUNG: Zugriff aus dem Internet** Der Server ist möglicherweise aus dem Internet erreichbar, wenn das Gerät über die aktivierte Netzzone mit dem Internet verbunden ist. **Voreinstellung:** aktiviert
	DNS-Anfragen loggen	Bei aktivierter Funktion wird für alle Anfragen an den DNS-Server des Geräts (UDP/TCP) ein Log-Eintrag erstellt. Log-Einträge können über das Menü **Logging** (siehe Kapitel 8) oder in der Datei *journal* analysiert werden, die über einen Snapshot erzeugt und heruntergeladen werden kann (siehe Kapitel 9.3). Log-Einträge können unterschiedliche Präfixe haben (siehe Kapitel 8). **Voreinstellung:** deaktiviert

Menü: Netzwerk >> DNS		
Externer DNS-Server (Nur konfigurierbar, wenn die Netzwerkkonfiguration des Geräts **nicht über DHCP** zugewiesen wird.)	**DNS-Server**	Der Benutzer kann auswählen, ob im Gerät voreingestellte „Root-DNS-Server“ oder „benutzerdefinierte DNS-Server“ zur Auflösung von Hostnamen verwendet werden. **Hinweis:** Diese Auswahlmöglichkeit besteht nur, wenn das Gerät seine Netzwerkkonfiguration **nicht von einem DHCP-Server** bezieht (siehe Kapitel 6.1.1). 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-Gerät nur vertrauenswürdige und abgesicherte DNS-Server – falls möglich aus Ihrem internen Firmennetzwerk –, um entsprechende Angriffe zu vermeiden. **Root-DNS-Server** **Nur** die im Gerät voreingestellten Root-DNS-Server werden zur Auflösung von Hostnamen verwendet (siehe Liste in Kapitel A 5, „Root-DNS-Server“). Der erste erreichbare Root-DNS-Server wird verwendet. **Benutzerdefiniert** **Nur** die benutzerdefinierten DNS-Server werden zur Auflösung von Hostnamen verwendet. Es können mehrere DNS-Server angegeben werden. Wird kein DNS-Server angegeben, werden Hostnamen nicht aufgelöst. **Voreinstellung:** Root-DNS-Server
	Benutzerdefinierte DNS-Server (Nur konfigurierbar, wenn „Benutzerdefiniert“ ausgewählt wurde.)	IP-Adresse eines oder mehrerer DNS-Server, die vom Gerät zur Auflösung von Hostnamen angefragt werden. **Eingabeformat:** IPv4-Adresse
	Kommentar	Frei wählbarer Kommentar. Erlaubte Zeichen: max. 128

7 Menü: Netzwerksicherheit

7.1 Firewall

Datenpakete, die durch das Gerät durchgeleitet (*geroutet*) werden, werden von dessen Firewall (Paketfilter) analysiert und entsprechend der konfigurierten Firewall-Regeln blockiert oder weitergeleitet.

Durchgehender (*gerouteter*) Datenverkehr bezeichnet Datenverbindungen, die nicht auf dem Gerät terminieren (wie z. B. Anfragen an den NTP-Server des Geräts), sondern vom Gerät geroutet (*Router-Modus*) oder weitergeleitet (*Stealth-Modus*) werden.

Dabei können die Verbindungen auch auf demselben Netzwerkinterface (Netzzone) empfangen und weitergeleitet werden.

Die Firewall-Regeln werden je nach Richtung des initialen Datenverkehrs in unterschiedlichen Tabellen konfiguriert (*Netzzone 1* → *Netzzone 2* und *Netzzone 2* → *Netzzone 1*).

Firewall-Logging
Log-Einträge werden nur für Pakete mit dem *Ether-Type IPv4* erstellt. Pakete mit anderen *Ether-Types* (z. B. *ARP, IPv6*) werden nicht in den Log-Dateien protokolliert. (Ausnahme: Einträge, die das Rate-Limit betreffen – *fw-input-rate-limit*)

Stateful-Packet-Inspection

Die Firewall des Geräts arbeitet nach dem Prinzip der *Stateful-Packet-Inspection-Firewall*: Das heißt, Antwortpakete zu Anfragen, die von der Firewall bereits in der Hinrichtung erlaubt worden sind, passieren die Firewall in der Rückrichtung automatisch, wenn sie der Anfrage zweifelsfrei zugeordnet werden können.

Dazu werden die Informationen jeder einzelnen Datenverbindung in einer *Connection Tracking*-Tabelle gespeichert und mit den Antwortpaketen verglichen, um diese den zugehörigen Anfragen eindeutig zuordnen zu können.

Firewall-Regeln werden grundsätzlich nicht auf Antwortpakete angewendet.

7.1.1 Einstellungen

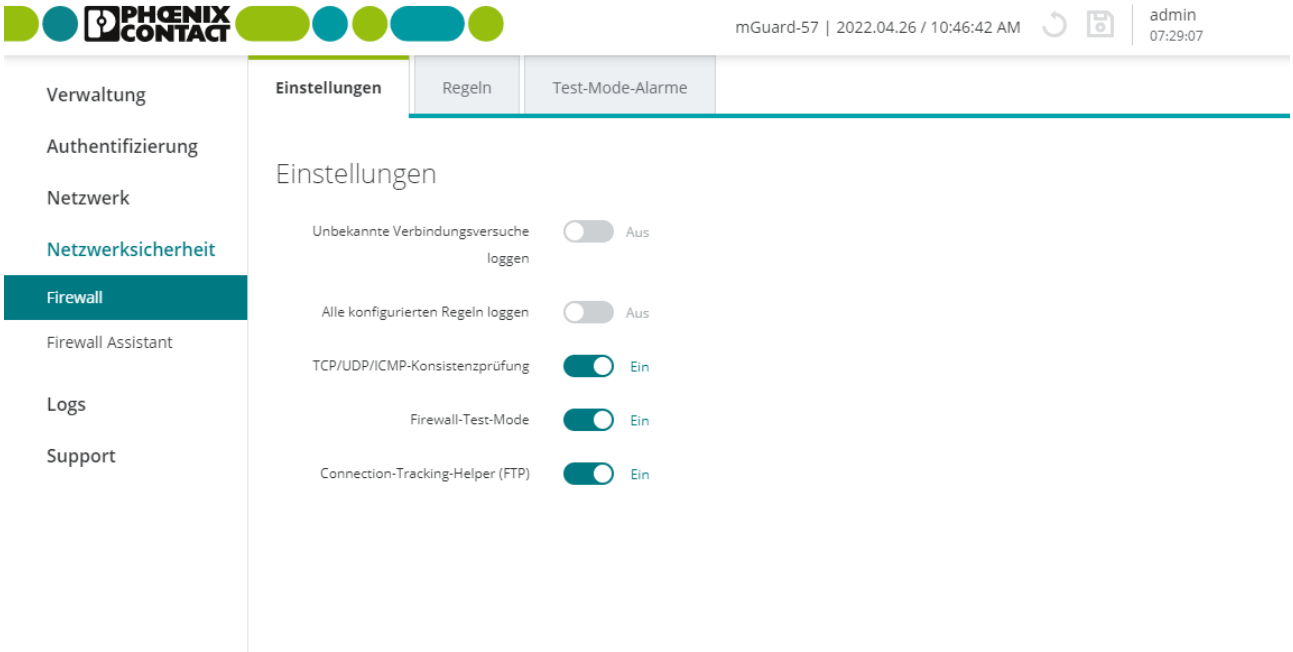


Bild 7-1 Netzwerksicherheit >> Firewall >> Einstellungen

Menü: Netzwerksicherheit >> Firewall >> Einstellungen		
Einstellungen	**Unbekannte Verbindungsversuche loggen**	Bei aktivierter Funktion wird für jede Datenverbindung, auf die keine konfigurierte Firewall-Regel zutrifft, ein entsprechender Log-Eintrag erstellt. Log-Einträge können über das Menü **Logging** (siehe Kapitel 8) oder in der Datei *journal* analysiert werden, die über einen Snapshot erzeugt und heruntergeladen werden kann (siehe Kapitel 9.3). Log-Präfix: *fw-forward-policy-* **Voreinstellung:** deaktiviert
	Alle konfigurierten Regeln loggen	Bei aktivierter Funktion wird für jede Datenverbindung, auf die eine beliebige Firewall-Regel zutrifft, ein entsprechender Log-Eintrag erstellt. Das gilt auch für die Regeln, in denen das Logging mittels der Funktion „*Log*“ deaktiviert ist. Log-Einträge können über das Menü **Logging** (siehe Kapitel 8) oder in der Datei *journal* analysiert werden, die über einen Snapshot erzeugt und heruntergeladen werden kann (siehe Kapitel 9.3). Log-Präfix: *fw-forward-* **Voreinstellung:** deaktiviert

Menü: Netzwerksicherheit >> Firewall >> Einstellungen		
	TCP/UDP/ICMP-Konsistenzprüfung	Die Konsistenzprüfung erhöht den Schutz von angeschlossenen Netzwerk-Clients vor *Denial of Service* (DoS)-Angriffen. Bei aktivierter Funktion werden Datenpakete, die durch das Gerät geroutet und an angebundene Netzwerk-Clients weitergeleitet werden, auf das Vorhandensein schadhafter Elemente geprüft: **ICMP-Pakete** Nur bekannter ICMP-Code wird verwendet. **UDP-Pakete** Zielport im UDP-Paket ist ungleich Null. **TCP-Pakete** Quell- und Zielport im TCP-Paket sind ungleich Null. **IPv4-Pakete** Protokoll ist nicht auf Null gesetzt. Datenpakete, die vorgegebenen Anforderungen nicht genügen, werden von der Firewall verworfen und nicht weitergeleitet. **Voreinstellung:** aktiviert
	Weiterleitung von DHCP-Paketen erlauben (Nur konfigurierbar im Modus „*Stealth*“)	**Im Stealth-Modus gilt:** Bei aktivierter Funktion können Clients in Netzzone 2 ihre IP-Konfiguration **automatisch und unabhängig von den Einstellungen in den Firewall-Tabellen** von einem DHCP-Server in Netzzone 1 beziehen. In den Firewall-Tabellen konfigurierte Firewall-Regeln, die diesen DHCP-Datenverkehr blockieren würden, werden nicht beachtet. Eine manuelle Konfiguration von Firewall-Regeln, um DHCP-Datenverkehr zu erlauben, ist nicht erforderlich. **Voreinstellung:** aktiviert

Menü: Netzwerksicherheit >> Firewall >> Einstellungen

Firewall-Test-Mode

Ungewollt durch die Firewall abgelehnter Datenverkehr kann einfach identifiziert und durch die automatisierte Erstellung entsprechender Firewall-Regeln erlaubt werden.

ACHTUNG: Firewall ist teilweise deaktiviert
Im Firewall-Test-Mode werden Datenpakete, die durch keine der bereits konfigurierten Firewall-Regeln erfasst werden, anders als üblich nicht verworfen, sondern weitergeleitet

Voraussetzung
Damit der Firewall-Test-Mode Einträge erzeugen kann, darf in der bestehenden Firewall-Tabelle keine abschließende Regel vorhanden sein, die jeglichen Datenverkehr ablehnt.

Funktionsweise

Bei aktivierter Funktion wird der durch das Gerät durchgeleitete (*geroutete*) Datenverkehr von der Firewall analysiert.

Trifft eine bereits konfigurierte Firewall-Regel auf ein Datenpaket zu, wird die Regel, **wie üblich**, auf das Datenpaket angewendet (*Annehmen*, *Abweisen* oder *Verwerfen*).

Trifft keine der konfigurierten Regeln auf ein Datenpaket zu, wird das Paket **anders als üblich** nicht verworfen, sondern weitergeleitet.

Gleichzeitig wird der Benutzer über das Ereignis informiert:

1. Die LED „PF2“ des Geräts leuchtet rot.
2. Der Schaltausgang „O1“ auf der COMBICON-Steckverbindung „XG2“ des Geräts nimmt *High-Pegel* ein.
   (Eine angeschlossene Signallampe würde in diesem Fall leuchten.)
3. In der Tabelle *Test-Mode-Alarme* wird ein Eintrag erstellt, der vom Benutzer analysiert werden kann.

Soll der Datenverkehr, der einen *Test-Mode-Alarm* ausgelöst hat, in Zukunft erlaubt werden, kann der Benutzer aus dem zugehörigen Eintrag in der Tabelle *Test-Mode-Alarme* automatisch eine entsprechende Firewall-Regel erstellen (siehe unten und Kapitel 7.1.3).

Erstellen von Firewall-Regeln aus Test-Mode-Alarmen

Einträge in der Tabelle *Test-Mode-Alarme* können ausgewählt und automatisch als neue Firewall-Regel am Ende der bestehenden Firewall-Tabellen eingefügt werden (siehe Kapitel 7.1.3).

Die neu eingefügten Regeln würden den entsprechenden Datenverkehr zukünftig erlauben (*Aktion = Annehmen*).

Firewall-Test-Mode deaktivieren

Wird der Firewall-Test-Mode deaktiviert, werden alle Einträge in der Tabelle *Test-Mode-Alarme* gelöscht und eine Signalisierung durch die LED „PF2“ und den Schaltausgang „O1“ beendet.

Voreinstellung: deaktiviert

Menü: Netzwerksicherheit >> Firewall >> Einstellungen

Connection-Tracking-Helper (FTP)

Die Aktivierung der Funktion hilft dabei, erwünschte, von der Firewall jedoch blockierte Datenverbindungen über das FTP-Protokoll, zu ermöglichen.

Wird eine Verbindung über das FTP-Protokoll hergestellt, kann die Datenübertragung auf zwei Wegen erfolgen:

1. Beim „aktiven FTP“ stellt der angerufene FTP-Server im Gegenzug eine zusätzliche Verbindung zum Anrufer (FTP-Client) her, um über diese Verbindung die Daten zu übertragen.
2. Beim „passiven FTP“ baut der Anrufer (FTP-Client) eine zusätzliche Verbindung zum Server auf, um die Daten zu übertragen.

Damit die zusätzliche Verbindung nicht von der Firewall blockiert wird, muss der Connection-Tracking-Helper für FTP in beiden Fällen aktiviert sein.

Die aktivierte Funktion wird auch auf Datenpakete angewendet, die mittels Port-Weiterleitung weitergeleitet werden.

ACHTUNG: Keine Verbindung im Stealth-Modus bei „aktivem FTP“.

Bei Verbindungen im Stealth-Modus mit „aktivem FTP“ wird auch mit aktiviertem Connection-Tracking-Helper keine Verbindung aufgebaut.

Verwenden Sie in diesem Fall entweder „passives FTP“ oder erstellen Sie eine zusätzliche Firewall-Regel, die eine Datenverbindung vom Server zum Client den Anforderungen entsprechend erlaubt (z. B. Erlauben: *Netzzone 1* → *Netzzone 2,* Protokoll: *TCP*, Von IP: *192.168.1.100*, Nach IP: *192.168.1.200*).

Voreinstellung: deaktiviert

7.1.2 Regeln

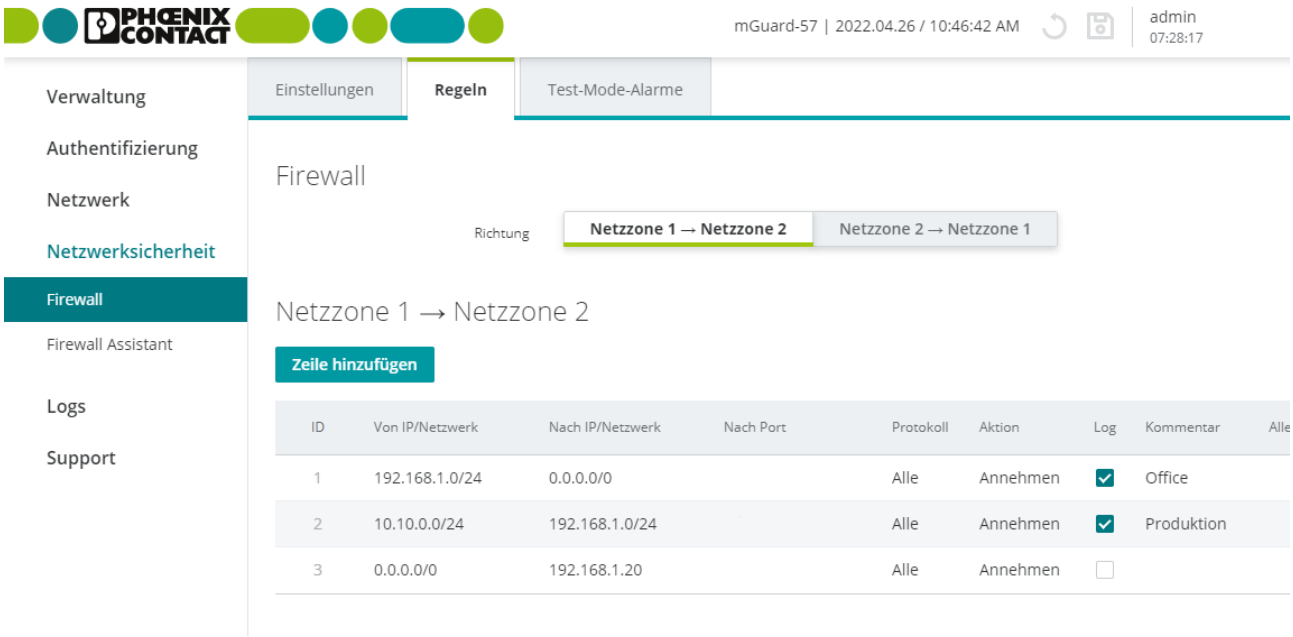


Bild 7-2 Netzwerksicherheit >> Firewall >> Regeln

Menü: Netzwerksicherheit >> Firewall >> Regeln	
Firewall	Die Firewall-Regeln werden je nach Richtung des initialen Datenverkehrs in zwei unterschiedlichen Tabellen konfiguriert: – *Netzzone 1 → Netzzone 2* – *Netzzone 2 → Netzzone 1* **ACHTUNG: Beachten Sie die Richtung des Datenverkehrs** Die Regeln in einer Firewall-Tabelle werden ausschließlich auf den Datenverkehr angewendet, der entsprechend der angegebenen Richtung von der einen in die andere Netzzone durch das Gerät durchgeleitet (*geroutet*) wird. **Netzzone 1 → Netzzone 2** Zeigt die Firewall-Tabelle, deren Regeln auf den Datenverkehr in der angegebenen Richtung (**Netzzone 1 → Netzzone 2**) angewendet werden. **Netzzone 2 → Netzzone 1** Zeigt die Firewall-Tabelle, deren Regeln auf den Datenverkehr in der angegebenen Richtung (**Netzzone 2 → Netzzone 1**) angewendet werden.

Menü: Netzwerksicherheit >> Firewall >> Regeln

Netzzone X → Netzzone Y

Verhalten und Auswirkung von Firewall-Regeln
Wie wirkt sich die Konfiguration von Firewall-Regeln auf den durchgeleiteten (*gerouteten*) Datenverkehr aus?

1. **Es ist keine Regel konfiguriert:** Alle Datenpakete werden verworfen**.**
2. **Keine der konfigurierten Regeln trifft zu:** Alle Datenpakete werden verworfen**.**
3. **Eine Regel ist konfiguriert und trifft zu:**
   Die Regel wird angewendet und die konfigurierte Aktion ausgeführt.
4. **Mehrere Regeln sind konfiguriert und treffen zu:**
   Die Regeln werden von oben nach unten abgefragt, bis eine Regel zutrifft. Diese wird angewendet und die konfigurierte Aktion ausgeführt.
   Alle nachfolgenden Regeln werden in diesem Fall nicht mehr berücksichtigt, auch wenn sie zutreffen würden.
   Die Erstellung einer abschließenden, alles verwerfenden Regel ist nicht erforderlich.

Im Firewall-Test-Mode können keine *Test-Mode-Alarme* erzeugt werden, wenn eine abschließende, alles verwerfende Regel existiert.

Wird eine Firewall-Regel umkonfiguriert, werden alle bestehenden Einträge in der Zustandstabelle (*connection tracking table*) gelöscht.

Sind identische Einträge in der Tabelle mehrfach vorhanden, wird dies im Tabellenkopf angezeigt. Identische Einträge können mit einem Klick auf die Schaltfläche **Duplikate löschen** gelöscht werden, wobei der jeweils erste Eintrag erhalten bleibt.

Aufbau von Firewall-Regeln

Eine Firewall-Regel setzt sich aus verschiedenen Parametern zusammen. Nur wenn alle konfigurierten Parameter einer Regel auf ein Paket zutreffen, trifft auch die gesamte Regel zu.

Manche Parameter einer Regel können so konfiguriert sein, dass sie immer zutreffen (z. B. *Alle* oder *0.0.0.0/0*).

ID

Identifikationsnummer der Regel (vom System generiert)

Die ID bestimmt die Reihenfolge, in der die Regeln abgefragt werden, beginnend mit der niedrigsten ID.

Von IP/Netzwerk

Quelle (Netzwerk oder IP-Adresse), von der aus Datenpakete gesendet werden müssen, damit die Regel in diesem Punkt zutrifft.

Hinweis: Wird als Subnetzmaske eine „0“ angegeben, trifft die Regel in diesem Punkt auf alle Quellen (alle IP-Adressen und Netzwerke) zu.

Eingabeformat: IPv4-Adresse, IPv4-Netzwerk (CIDR-Notation)

Voreinstellung:

- Netzzone 1 → Netzzone 2: Keine Regel
- Netzzone 2 → Netzzone 1: 0.0.0.0/0

Menü: Netzwerksicherheit >> Firewall >> Regeln		
	Nach IP/Netzwerk	Ziel (Netzwerk oder IP-Adresse), an das Datenpakete gesendet werden müssen, damit die Regel in diesem Punkt zutrifft. **Hinweis:** Wird als Subnetzmaske eine „0“ angegeben, trifft die Regel in diesem Punkt auf alle Ziele (alle IP-Adressen und Netzwerke) zu. **Eingabeformat:** IPv4-Adresse, IPv4-Netzwerk (CIDR-Notation) **Voreinstellung:** – Netzzone 1 → Netzzone 2: Keine Regel – Netzzone 2 → Netzzone 1: 0.0.0.0/0
	Nach Port (Nur konfigurierbar, wenn als „Protokoll“ *TCP* oder *UDP* ausgewählt ist.)	Ziel-Port oder Port-Bereich, an den Datenpakete gesendet werden müssen, damit die Regel in diesem Punkt zutrifft. **Eingabeformat:** 1 – 65535, startport:endport, Alle **Hinweis:** Alle = alle Ports; startport:endport = Port-Bereich **Voreinstellung:** – Netzzone 1 → Netzzone 2: Keine Regel – Netzzone 2 → Netzzone 1: Alle
	Protokoll	**TCP, UDP, ICMP, GRE, ESP, Alle** Netzwerkprotokoll, das für die Übertragung der Datenpakete verwendet werden muss, damit die Regel in diesem Punkt zutrifft. **Hinweis:** Alle = alle Protokolle **Voreinstellung:** – Netzzone 1 → Netzzone 2: Keine Regel – Netzzone 2 → Netzzone 1: Alle

Menü: Netzwerksicherheit >> Firewall >> Regeln		
	Aktion	**Annehmen, Abweisen, Verwerfen** Aktion, die ausgeführt wird, wenn alle in der Zugriffsregel konfigurierten Parameter auf ein Paket zutreffen. **Annehmen:** Die Datenpakete dürfen passieren. **Abweisen:** Die Datenpakete werden zurückgewiesen. Der Absender wird informiert. **Verwerfen:** Die Datenpakete werden verworfen. Der Absender wird nicht informiert. **Hinweis (Stealth-Modus):** Im *Stealth-Modus* führt die Auswahl der Aktion *Abweisen* zum gleichen Verhalten wie die Auswahl der Aktion *Verwerfen.* Da das Gerät im *Stealth-Modus* über keine eigene IP-Adresse verfügt, werden Datenpakete in beiden Fällen verworfen und der Absender nicht informiert. In den Log-Einträgen wird in diesen Fällen als Aktion „*drop*“ und nicht „*reject*“ protokolliert. **Voreinstellung:** – Netzzone 1 → Netzzone 2: Keine Regel – Netzzone 2 → Netzzone 1: Annehmen
	Log	Bei aktivierter Funktion wird für jede Datenverbindung, auf die die Regel zutrifft, ein Log-Eintrag erstellt. Für Regeln, in denen die Funktion deaktiviert ist, wird kein Log-Eintrag erstellt, es sei denn, die Funktion „„Alle konfigurierten Regeln loggen““ ist aktiviert. Log-Einträge können über das Menü **Logging** (siehe Kapitel 8) oder in der Datei *journal* analysiert werden, die über einen Snapshot erzeugt und heruntergeladen werden kann (siehe Kapitel 9.3). Log-Präfix: *fw-forward-* **Voreinstellung:** deaktiviert
	Kommentar	Frei wählbarer Kommentar. Erlaubte Zeichen: max. 128

7.1.3 Test-Mode-Alarme

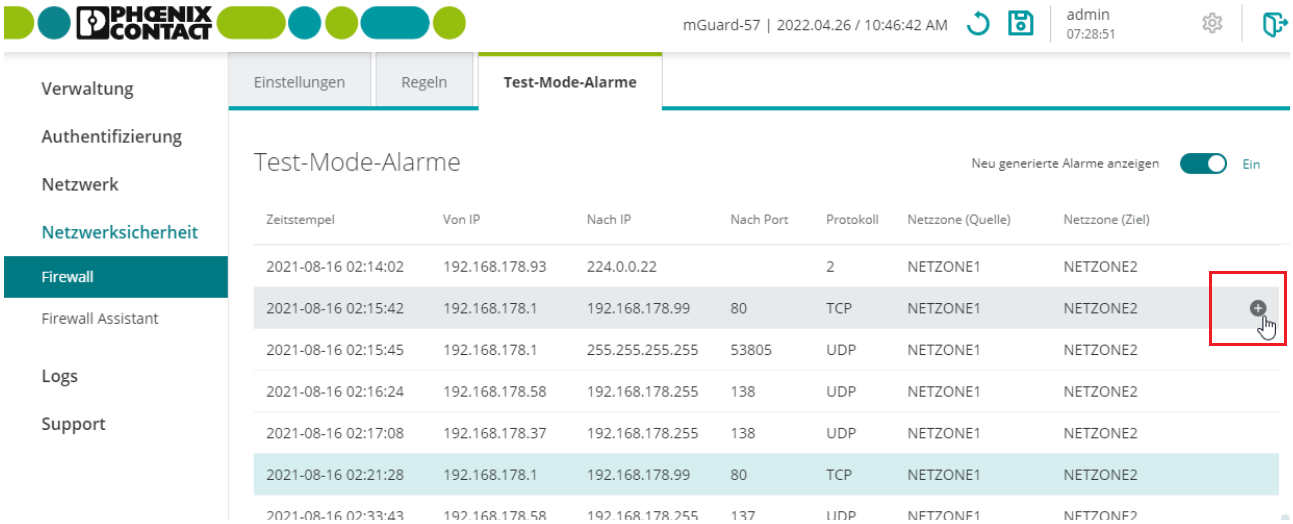


Bild 7-3 Netzwerksicherheit >> Firewall >> Test-Mode-Alarme

Menü: Netzwerksicherheit >> Firewall >> Test-Mode-Alarme

Test-Mode-Alarme

(Die Registerkarte „Test-Mode-Alarme“ ist nur sichtbar, wenn der „Firewall-Test-Mode“ aktiv ist.)

Im Firewall-Test-Mode wird der durch das Gerät durchgeleitete (*geroutete*) Datenverkehr analysiert und automatisch eine Tabelle mit Einträgen für die Datenpakete erstellt, die durch keine der bereits konfigurierten Firewall-Regeln erfasst werden.

In dieser Tabelle erfasste Einträge können anschließend ausgewählt und als Firewall-Regeln am Ende der entsprechenden Firewall-Tabellen des Geräts hinzugefügt werden (Menü: **Netzwerksicherheit >> Firewall >> Regeln**; siehe Kapitel 7.1.2).

Hinzugefügte Regeln erlauben den entsprechenden Datenverkehr (**Aktion = Annehmen**).

ACHTUNG: Automatisch erstellte Firewall-Regeln werden aktiviert.
Prüfen Sie umgehend die neu erstellten Firewall-Regeln und passen Sie diese Ihren Sicherheitsanforderungen entsprechend an.

ACHTUNG: Limit bei 2000 Test-Mode-Alarmen erreicht!
Ist das Limit erreicht, werden keine neue Einträge zur Tabelle hinzugefügt. Es ist dann davon auszugehen, dass die in der Tabelle erfassten Alarme unvollständig sind.

Um weitere Test-Mode-Alarme zu erzeugen, gehen Sie deshalb wie folgt vor:

- Fügen Sie die gewünschten Einträge in Ihr Firewall-Regelwerk ein (siehe unten).
- Beenden Sie anschließen den Firewall-Test-Mode.
- Starten Sie den Firewall-Test-Mode erneut, um neue Alarme zu erzeugen.

Menü: Netzwerksicherheit >> Firewall >> Test-Mode-Alarme

Test-Mode-Alarme in das Firewall-Regelwerk einfügen:

- Prüfen Sie die Tabelleneinträge.
- Identifizieren Sie die Einträge, die Sie unter Berücksichtigung Ihrer Sicherheitsanforderungen als neue Firewall-Regeln übernehmen möchten.
- Klicken Sie auf einen Eintrag, um eventuell vorhandene identischen Einträge, die zu unterschiedlichen Zeitpunkten erstellt wurden, in der Liste zu markieren.
- Bewegen Sie den Mauszeiger über einen Eintrag, den Sie als neue Firewall-Regel in die entsprechende Firewall-Tabelle übernehmen möchten.

⇒ Das Icon erscheint am Ende der Zeile.

- Klicken Sie auf , um die Regel in die zugehörige Firewall-Tabelle zu kopieren.

⇒ Die Firewall-Regel wird am Ende der zugehörigen Firewall-Tabelle eingefügt.

- Wechseln Sie in das Menü **Netzwerksicherheit >> Firewall >> Regeln.**
- Prüfen Sie die Regeln und passen Sie diese gegebenenfalls an.
- Klicken Sie auf das Icon , um die Änderungen zu übernehmen.

⇒ Die neu eingefügten Firewall-Regeln sind aktiv und erlauben umgehend den entsprechenden Datenverkehr.

Neu generierte Alarme anzeigen	Bei aktivierter Funktion liegt der Fokus der Anzeige immer auf den zuletzt hinzugefügten Alarmen der Tabelle. Das Gerät prüft laufend, ob neue Test-Mode-Alarme generiert werden und fügt diese am Ende der bestehenden Tabelle hinzu. Für eine Betrachtung der bereits hinzugefügten älteren Alarme sollte die Funktion deaktiviert werden. **Voreinstellung:** aktiviert
Zeitstempel	Zeitpunkt, an dem der Eintrag durch den entsprechenden Datenverkehr erzeugt wurde. **Hinweis:** Der Zeitpunkt wird entsprechend der eingestellten Zeitzone angezeigt. **Format:** YYYY-MM-DD hh:mm:ss
Von IP	Quelle (IP-Adresse) von der aus das Datenpaket gesendet wurde.
Nach IP	Ziel (IP-Adresse) an das das Datenpaket gesendet wurde.
Nach Port	Ziel-Port, an den das Datenpaket gesendet wurde. – Kein Eintrag bedeutet, dass im Datenpaket kein Ziel-Port angegeben wurde (z. B. ICMP-Datenpakete).
Protokoll	Netzwerkprotokoll, das für die Übertragung des Datenpakets verwendet wurde. Die Protokolle **TCP**, **UDP**, **ICMP**, **GRE** und **ESP** werden übernommen. Für alle anderen Protokolle wird der Wert **Alle** eingetragen.

Menü: Netzwerksicherheit >> Firewall >> Test-Mode-Alarme		
	Netzzone (Quelle)	Netzzone, in der die Datenverbindung initiiert wurde. Die Richtung der Datenverbindung entscheidet darüber, in welche Firewall-Tabelle die Daten gegebenenfalls eingetragen werden (siehe Kapitel 7.1.2).
	Netzzone (Ziel)	Netzzone, an die die Daten gesendet wurden. Die Richtung der Datenverbindung entscheidet darüber, in welche Firewall-Tabelle die Daten gegebenenfalls eingetragen werden (siehe Kapitel 7.1.2)

7.2 Firewall-Test-Mode

Siehe „Firewall-Test-Mode“ auf Seite 82.

7.3 Firewall Assistant

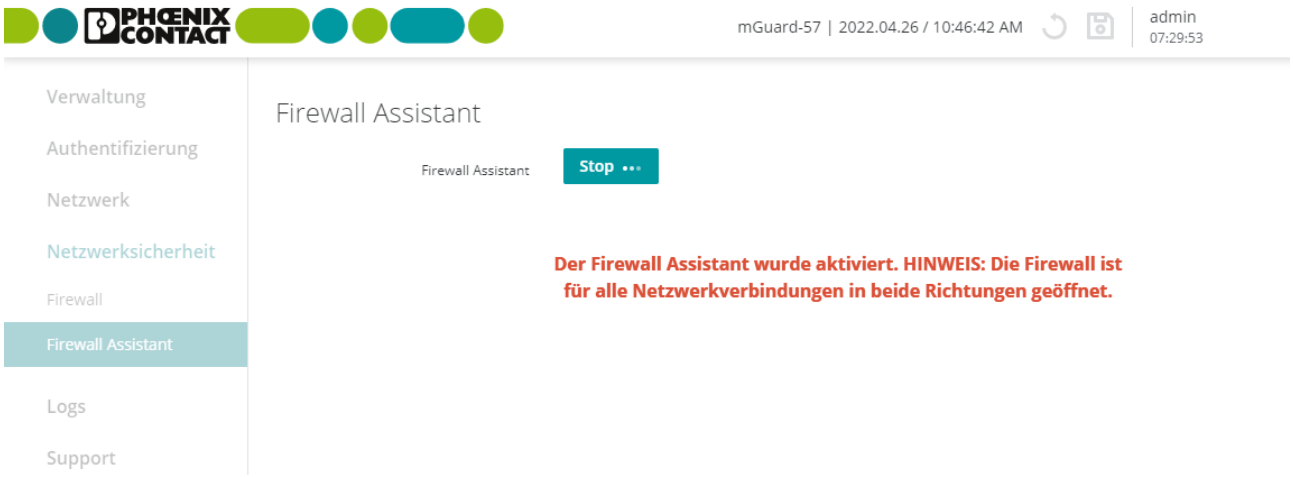


Bild 7-4 Netzwerksicherheit >> Firewall Assistant

Der Firewall Assistant analysiert und erfasst im aktivierten Zustand den Datenverkehr, der durch das Gerät durchgeleitet (*geroutet*) wird (**Netzzone 1 ←→ Netzzone 2**).

Die Firewall ist dabei in beide Richtungen geöffnet.

Aus den erfassten Paketdaten werden Firewall-Regeln abgeleitet, die beim Beenden des Firewall Assistant automatisch in die entsprechenden Firewall-Tabellen des Geräts eingetragen werden.

Der in diesen Firewall-Regeln definierte Datenverkehr wird künftig erlaubt (**Aktion = Annehmen**). Alle anderen Verbindungen werden verworfen.

Die mittels Firewall Assistant erstellten Firewall-Tabellen können beliebig angepasst und erweitert werden.

Tabelle 7-1 Firewall Assistant: Umwandlung von Paketdaten in Firewall-Regeln

Header-Eintrag	**Eintrag in Firewall-Regel**	**Beispiel**
Quell-IP-Adresse	**Von IP/Netzwerk**	*10.1.1.55*
Ziel-IP-Adresse	**Nach IP/Netzwerk**	*192.168.1.100*
Die jeweilige Netzmaske des Quell- und des Ziel-Netzwerks wird nicht erfasst. Es werden lediglich einzelne IP-Adressen erfasst und in die Firewall-Regel übernommen.		
Ziel-Port	**Nach Port**	*443*
Wird kein Ziel-Port übertragen (wie z. B. beim *ICMP*-Protokoll), wird in der Firewall-Regel kein Wert eingetragen.		
Protokoll	**Protokoll**	*TCP*
Folgende Protokolle können als Wert in die Firewall-Regel übernommen werden: – *TCP, UDP, ICMP, GRE, ESP* Für alle anderen Protokolle wird in der Firewall-Regel der Wert *„Alle“* eingetragen.		
—	**Aktion**	*Annehmen*
In alle mittels Firewall Assistant oder Firewall-Test-Mode erstellten Firewall-Regeln wird als Aktions-Wert grundsätzlich immer *„Annehmen“* eingetragen.		

Vorgehen

Den Firewall Assistant starten

ACHTUNG: Die Firewall wird deaktiviert
Wenn der Firewall Assistant aktiviert ist, werden angebundenen Netzwerk-Clients nicht mehr durch die Firewall geschützt.

Der Firewall Assistant kann nur gestartet werden, wenn vorher **alle Firewall-Regeln** in allen Firewall-Tabellen unter **Netzwerksicherheit >> Firewall >> Regeln** gelöscht wurden (siehe Kapitel 7.1.2).

Firewall-Regeln werden nur übernommen, wenn der Firewall Assistant über die Schaltfläche **Stop** beendet wird.

ACHTUNG: Limit für Paketdaten erreicht
Der Firewall Assistant wird automatisch beendet, wenn die maximal mögliche Anzahl von Paketdaten analysiert wurde. **In diesem Fall werden keine Regeln in die Firewall-Tabellen eingetragen!** Starten Sie den Firewall Assistant erneut mit einer kürzeren Laufzeit.

Gehen Sie wie folgt vor:

- Klicken Sie auf die Schaltfläche **Start**, um den Firewall Assistant zu aktivieren.

⇒ Der Datenverkehr wird analysiert und erfasst.

⇒ Die Firewall ist in beide Richtungen geöffnet.

Den Firewall Assistant stoppen und Firewall-Regeln erstellen

ACHTUNG: Die automatisch erstellten Firewall-Regeln sind ungeprüft aktiv.
Prüfen Sie umgehend die neu erstellten Firewall-Regeln und passen Sie diese Ihren Sicherheitsanforderungen entsprechend an.

Gehen Sie wie folgt vor:

- Klicken Sie auf die Schaltfläche **Stop**, um den Firewall Assistant zu deaktivieren.

⇒ Aus den erfassten Paketdaten werden automatisch Firewall-Regeln erstellt und in die entsprechenden Firewall-Tabellen eingetragen (Menü: **Netzwerksicherheit >> Firewall >> Regeln**, siehe Kapitel 7.1.2).

⇒ Die eingetragenen Regeln erlauben den entsprechenden Datenverkehr umgehend und permanent (**Aktion = Annehmen**) (siehe Tabelle 7-1).

Die mittels Firewall Assistant erstellten Firewall-Tabellen können beliebig angepasst und erweitert werden.

8 Menü: Logging

Unter Logging versteht man die Protokollierung der Meldungen zu stattgefundenen Ereignissen (z. B. Konfigurationsänderungen, angewendete Firewall-Regeln, Fehlermeldungen).

Log-Einträge werden temporär auf dem Gerät gespeichert und können zusätzlich, dem *Syslog*-Protokoll entsprechend, an einen Remote-Server übertragen werden.

Sensitive Daten und sicherheitsrelevante Informationen (z. B. Passwörter oder geheime kryptografische/gehashte Schlüssel) sind in den Log-Dateien nicht enthalten.

8.1 Log-Einträge

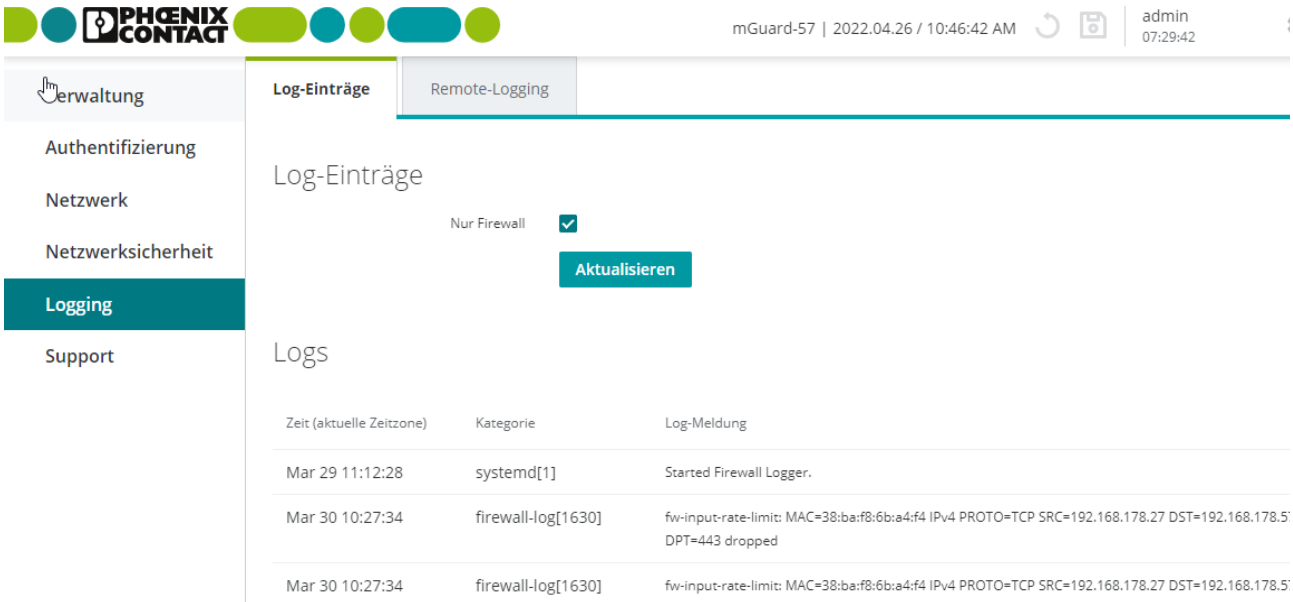


Bild 8-1 Logging >> Log-Einträge

Menü: Logging >> Log-Einträge	
Log-Einträge	Log-Einträge werden im Arbeitsspeicher des Geräts erfasst. Ist der Speicherplatz verbraucht, werden automatisch die ältesten Log-Einträge durch neue überschrieben. Wird das Gerät ausgeschaltet, werden alle Log-Einträge gelöscht. Um Log-Einträge längerfristig zu sichern, können diese, dem Syslog-Protokoll entsprechend, an einen Remote-Server übertragen werden (siehe Kapitel 8.2, „Remote-Logging“). In seltenen Fällen kann es bei der Generierung vieler Log-Einträge dazu kommen, dass ein Log-Eintrag nicht übertragen wird. Um dies nachprüfen zu können, wird jeder Log-Eintrag, wie im Syslog-Protokoll beschrieben, mit einer fortlaufenden Sequenz-ID versehen (z. B. meta sequenceId="728").

Menü: Logging >> Log-Einträge

Das Erstellen von Log-Einträgen zu bestimmten Ereignissen muss vom Benutzer gegebenenfalls zunächst aktiviert werden.

Firewall-Logging
Log-Einträge werden nur für Pakete mit dem *Ether-Type IPv4* erstellt. Pakete mit anderen *Ether-Types* (z. B. *ARP, IPv6*) werden nicht in den Log-Dateien protokolliert. (Ausnahme: Einträge, die das Rate-Limit betreffen – *fw-input-rate-limit*)

Bei Datenverbindungen (z. B. UDP, TCP oder ICMP) wird grundsätzlich nur das erste Paket der Verbindung geloggt (wenn Logging aktiviert ist), da die Verbindung dem *Connection Tracking* unterliegt.

Log-Präfixe

Log-Einträge sind verschiedenen Kategorien zugeordnet, die mit einem eigenen Präfix gekennzeichnet werden.

Log-Präfixe (Firewall-Logging)

forward = Betrifft die Firewall (Routing/Stealth) für durchgehenden Datenverkehr:

- **fw-forward** = Eine Firewall-Regel wurde auf ein Paket angewendet.
- **fw-forward-policy =** Ein Paket, **für das keine Regel definiert ist**, wurde verworfen.
- **fw-forward-testmode** = Betrifft Einträge (*„Test-Mode-Alarme“*), die über die Funktion *„Firewall-Test-Mode“* erzeugt wurden (wird nur angezeigt, wenn alle Log-Einträge angezeigt werden; siehe unten „Nur Firewall“).

input = Betrifft die *Eingangs-Firewall* für Zugriffe auf das Gerät:

- **fw-input** = Eine *Eingangs-Firewall*-Regel wurde auf ein Paket angewendet.
- **fw-input-policy** = Ein Paket, **für das keine Regel definiert ist**, wurde verworfen.
- **fw-input-dnscache** = Betrifft den Zugriff auf den DNS-Server des Geräts.
- **fw-input-rate-limit** = Aufgrund zu vieler Gerätezugriffe in einem definierten Zeitraum (z. B. per HTTPS), erfolgte eine Drosselung des Datenverkehrs.

Erklärung der Abkürzungen

- IPv4 PROTO = Netzwerkprotokoll
- SRC = Source IP address / Quell-IP-Adresse
- DST = Destination IP address / Ziel-IP-Adresse
- SPT = Source port / Quell-Port (TCP und UDP)
- DPT = Destination port / Ziel-Port (TCP und UDP)
- MAC = Source MAC address / MAC-Adresse der Quelle

Nur Firewall	Bei aktivierter Funktion werden nur die Log-Einträge zu Ereignissen, die die Firewall betreffen (*Firewall - Routing/Stealth* - und *Eingangs-Firewall*), angezeigt. Bei deaktivierter Funktion werden alle Log-Einträge angezeigt. **Voreinstellung:** aktiviert
Schaltfläche	**Aktualisieren** • Klicken Sie auf die Schaltfläche **Aktualisieren**, um die Anzeige der Log-Einträge zu aktualisieren.

Menü: Logging >> Log-Einträge		
Logs	**Zeit (aktuelle Zeitzone)**	Zeitpunkt, an dem der Log-Eintrag erstellt wurde. Im WBM wird der Zeitpunkt entsprechend der aktuell gespeicherten Zeitzone angezeigt. **Format:** Monat Tag Stunde:Minute:Sekunde **Hinweis:** Ein Zeitstempel innerhalb einer Log-Meldung wird nicht an die aktuelle Zeitzone angepasst.
	Kategorie	Kategorie (Komponente/Unit), der der Log-Eintrag zugeordnet ist.
	Log-Meldung	Die dem Log-Eintrag zugehörige Meldung. **Hinweis:** Ein Zeitstempel innerhalb einer Log-Meldung wird nicht an die aktuelle Zeitzone angepasst.

8.2 Remote-Logging

Sicherheitshinweis

Aus Sicherheitsgründen sollte immer eine verschlüsselte TLS-Verbindung zwischen dem Gerät (mGuard) und dem *Syslog*-Server verwendet werden.

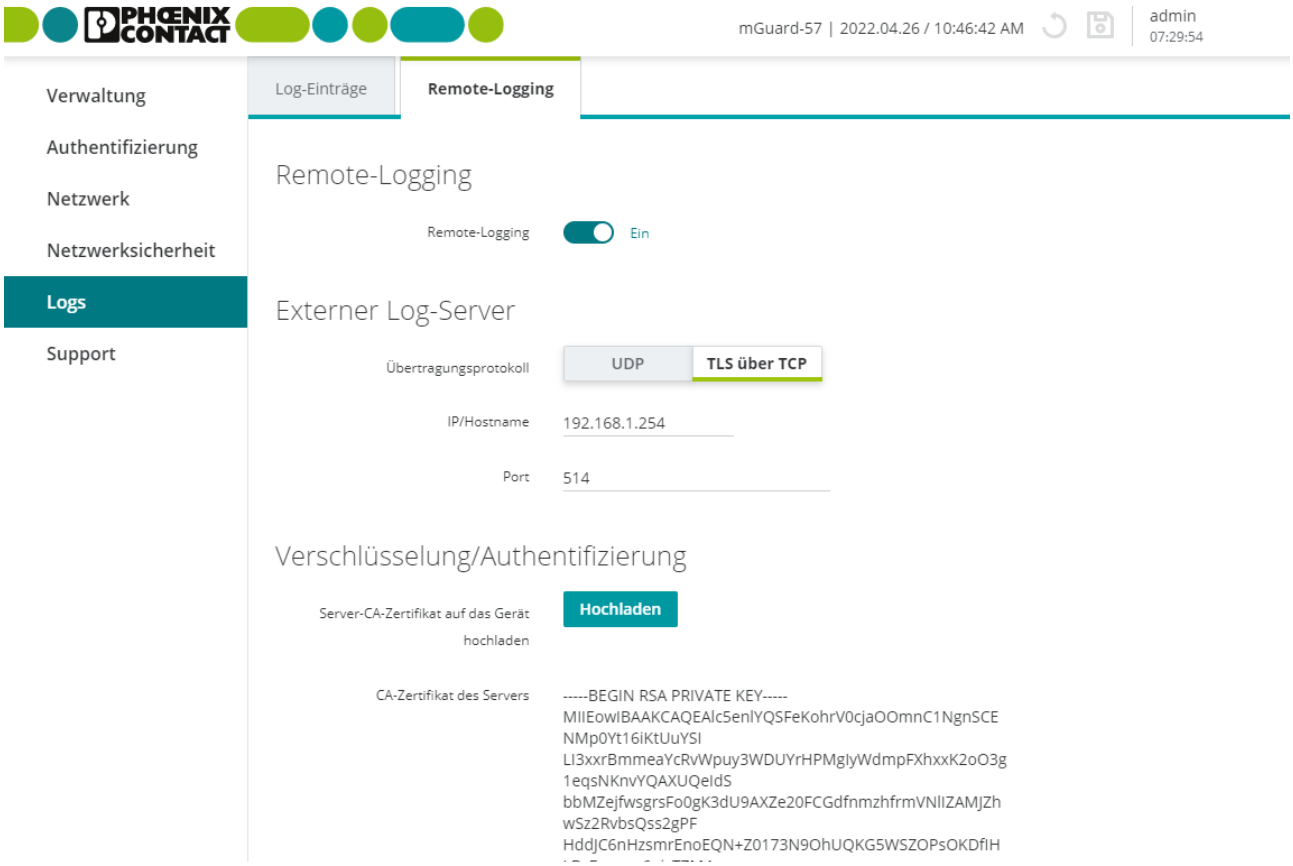


Bild 8-2 Logging >> Remote-Logging (Syslog)

Menü: Logging >> Remote-Logging		
Remote-Logging	**Remote-Logging**	Bei aktivierter Funktion werden alle Log-Einträge des Geräts, dem *Syslog*-Protokoll entsprechend (siehe RFC 5424), an einen entfernten Remote-Server übertragen (siehe unten). Die Übertragung erfolgt wahlweise über das unverschlüsselte UDP- oder verschlüsselt über das TCP-Protokoll. **Voreinstellung:** deaktiviert

Menü: Logging >> Remote-Logging		
Externer Log-Server	**Übertragungsprotokoll**	Netzwerkprotokoll, das für den Verbindungsaufbau zum Remote-Server (*Syslog*-Server) verwendet wird. **Hinweis:** Aus Sicherheitsgründen sollte immer eine verschlüsselte TLS-Verbindung zwischen dem Gerät (mGuard) und dem *Syslog*-Server genutzt werden. **UDP** Bei aktivierter Funktion werden die Daten unverschlüsselt über das UDP-Protokoll übertragen. Eine gegenseitige Authentifizierung von Gerät und Remote-Server findet nicht statt. **TLS über TCP** Bei aktivierter Funktion werden die Daten verschlüsselt über eine TCP-Verbindung übertragen. (Siehe auch „Verwendete Verschlüsselungsalgorithmen“ auf Seite 15.) Eine gegenseitige Authentifizierung von Gerät und Remote-Server erfolgt mittels X.509-Zertifikaten (siehe unten). **Voraussetzung:** Um die Integrität und Authentizität der verschlüsselten TCP-Verbindung sicherzustellen, muss 1. ein Server-Zertifikat (CA-Zertifikat) des Remote-Servers auf dem Gerät installiert werden (siehe unten), 2. ein Client-Zertifikat auf dem Gerät erzeugt, heruntergeladen und auf dem Remote-Server installiert werden (siehe unten). **Voreinstellung:** UDP
	IP/Hostname	IP-Adresse oder Hostname des Remote-Servers (*Syslog*-Server), an den Log-Einträge gesendet werden sollen. **Eingabeformat:** IPv4-Adresse oder Hostname **Voreinstellung:** 192.168.1.254
	Port	Netzwerk-Port, auf dem der Remote-Server Datenpakete annimmt (Standard-Port: *514/UDP*). **Eingabeformat:** 1 – 65535 **Voreinstellung:** 514
Verschlüsselung/ Authentifizierung (Nur konfigurierbar, wenn TLS über TCP aktiviert ist.)	**Verwendung von Zertifikaten** 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 (siehe auch Kapitel B 3, „Erklärung der Fachwörter“ unter „X.509-Zertifikat“).	

Menü: Logging >> Remote-Logging		
	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.	
	Server-CA-Zertifikat auf das Gerät hochladen	Das CA-Zertifikat, mit dem der Remote-Server (*Syslog*-Server) authentifiziert wird, wird auf das Gerät hochgeladen. Das CA-Zertifikat wird vom Betreiber des Remote-Servers bereitgestellt und muss auf das Gerät hochgeladen werden (X.509-Zertifikat mit öffentlichem Schlüssel). Eine verschlüsselte TCP-Verbindung zum Remote-Server kann nur dann erfolgreich aufgebaut werden, wenn dieser seinerseits ein vom CA-Zertifikat ausgestelltes Zertifikat (mit dem *geheimen* Schlüssel) oder eine gültige Zertifikatskette, mit dem CA-Zertifikat als oberste Instanz, vorzeigt. **Schaltfläche** • Klicken Sie auf die Schaltfläche **Hochladen**, um das CA-Zertifikat des Remote-Servers (*Syslog*-Servers) von einem Konfigurationsrechner auf das Gerät hochzuladen. **Format:** Die maximal erlaubte Dateigröße beträgt 1 MB. **Hinweis:** Ein bereits hochgeladenes CA-Zertifikat wird in diesem Fall gelöscht und ersetzt.
	CA-Zertifikat des Servers	Zeigt das aktuell hochgeladene CA-Zertifikat an.
Client-Zertifikat	**Neues Client-Zertifikat auf dem Gerät erstellen**	Das selbstsignierte Client-Zertifikat, mit dem sich das Gerät gegenüber dem Remote-Server (*Syslog*-Server) authentifiziert, wird auf dem Gerät erzeugt und dort gespeichert. Es muss heruntergeladen und vom Betreiber des Remote-Servers auf den Remote-Server hochgeladen werden (X.509-Zertifikat mit *öffentlichem* Schlüssel). **ACHTUNG: Das aktuelle Zertifikat wird gelöscht** Wenn Sie ein neues Client-Zertifikat erzeugen, wird das aktuell auf dem Gerät gespeicherte Zertifikat unwiderruflich gelöscht. Das neu erzeugte Zertifikat muss erneut auf den Remote-Server hochgeladen werden. **Schaltfläche** • Klicken Sie auf die Schaltfläche **Erstellen**, um ein neues Client-Zertifikat auf dem Gerät zu erzeugen. **Hinweis:** Ein bereits erzeugtes Zertifikat wird in diesem Fall gelöscht und ersetzt.

Menü: Logging >> Remote-Logging		
	Client-Zertifikat herunterladen	Das erstellte Client-Zertifikat (siehe unten) wird auf den Konfigurationsrechner heruntergeladen. **Schaltfläche** • Klicken Sie auf die Schaltfläche **Herunterladen**, um das Client-Zertifikat (mit dem *öffentlichen* Schlüssel) herunterzuladen. Der geheime Schlüssel (*secret key*) des Zertifikats verbleibt grundsätzlich auf dem Gerät. Das heruntergeladene Client-Zertifikat kann anschließend auf den Remote-Server hochgeladen werden. Dateiname: *Client-Zertifikat.crt*
	Client-Zertifikat	Zeigt das aktuelle vom Gerät verwendete Client-Zertifikat an.

9 Menü: Support

9.1 Ping

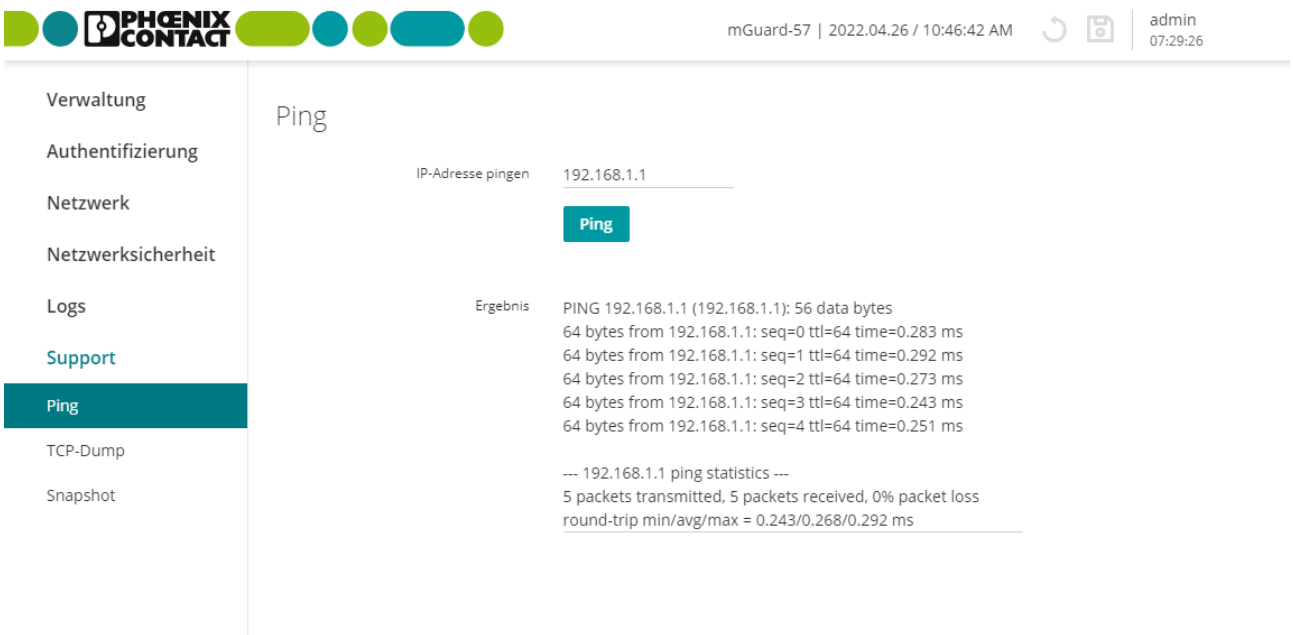


Bild 9-1 Support >> Ping

Menü: Support >> Ping	
Ping	Mithilfe einer Ping-Anfrage (*ICMP request*) kann geprüft werden, ob ein Netzwerk-Client über seine IP-Adresse mit einem Interface des Geräts verbunden und über das ICMP-Protokoll erreichbar ist.
	IP-Adresse Eine Ping-Anfrage (*ICMP request*) wird an die angegebene IP-Adresse eines Netzwerk-Clients gesendet. Ist der Client über eine beliebige Netzzone des Geräts über das *ICMP*-Protokoll erreichbar, sendet er eine Antwort an das Gerät zurück. **Vorgehen** • Öffnen Sie das Menü **Support >> Ping**. • Geben Sie die IP-Adresse des zu prüfenden Clients in das Feld ein. • Klicken Sie auf die Schaltfläche **Ping**. ⇒ Ist der Client über *ICMP* erreichbar, wird nach wenigen Sekunden die Antwort des Clients angezeigt: z. B. *5 packets transmitted, 5 packets received*. ⇒ Ist der Client nicht über *ICMP* erreichbar, wird eine entsprechende Meldung angezeigt: z. B. *100% packet loss*). **Eingabeformat:** IPv4-Adresse

9.2 TCP-Dump

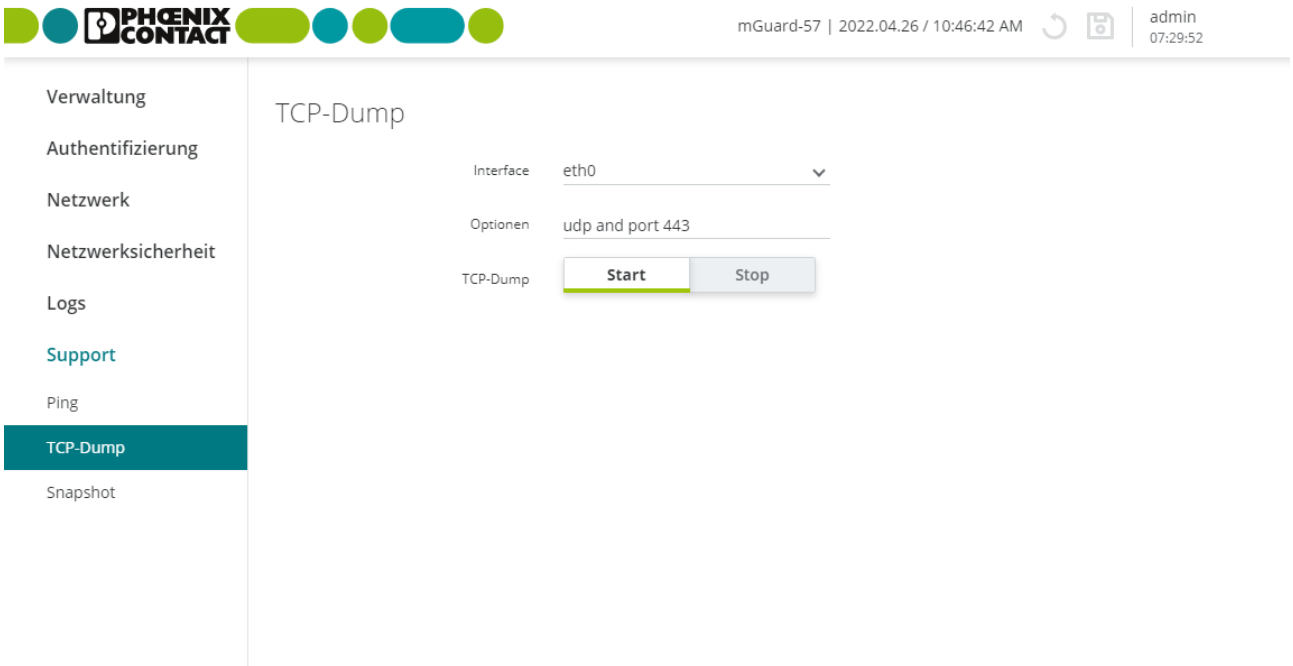


Bild 9-2 Support >> TCP-Dump

Menü: Support >> TCP-Dump	
TCP-Dump	Mithilfe einer Paketanalyse (*tcpdump*) kann der Inhalt von Netzwerkpaketen analysiert werden, die über ein ausgewähltes Netzwerkinterface gesendet oder empfangen werden. Welche Netzwerkpakete analysiert werden, wird über Filteroptionen bestimmt. Das Ergebnis der Analyse wird in einer Datei (**.pcap*) gespeichert, heruntergeladen und auf dem Gerät gelöscht. Wird das Gerät während einer laufenden Analyse neu gestartet, werden die bis dahin gesammelten Daten gelöscht. Wenn die Datei (**.pcap*) eine Größe von 50 MB überschreitet, wird die Analyse mit einem Fehler abgebrochen. Die bis dahin gesammelten Daten werden gelöscht. **Vorgehen** • Öffnen Sie das Menü **Support >> TCP-Dump**. • Wählen Sie das **Interface** aus, dessen Netzwerkpakete analysiert werden sollen. • Geben Sie die gewünschten **Optionen** ein, um die Analyse zu beschränken. • Um die Analyse zu starten, klicken Sie auf die Schaltfläche **Start**. • Um die Analyse zu beenden und herunterzuladen, klicken Sie auf die Schaltfläche **Stop**. ⇒ Das Ergebnis der Analyse wird in einer Datei (**.pcap*) gespeichert, heruntergeladen und auf dem Gerät gelöscht.

Menü: Support >> TCP-Dump

Interface	Nur Datenpakete, die über das ausgewählte Netzwerk-Interface gesendet oder empfangen werden, werden analysiert. Netzzone 1: – **eth0** Netzzone 2: – **lan0** – **lan1** – **lan2** – **lan3**
Optionen	Durch die Angabe von Optionen kann die Paketanalyse auf eine Auswahl der unten stehenden Elemente beschränkt werden. Optionen können über die logischen Verknüpfungen „*and*, *or*, *not*“ verknüpft werden. Beispiel: *tcp and net 192.168.1.0/24 and not port 443*
Zur Verfügung stehende Optionen:	
tcp	TCP-Protokoll
udp	UDP-Protokoll
arp	ARP-Protokoll
icmp	ICMP-Protokoll
esp	ESP-Protokoll
host <ip>	IPv4-Adresse
port <1-65535>	Netzwerkport (einzelne Portnummer)
net <nw_cidr>	Netzwerk (in CIDR-Schreibweise, z. B. 192.168.1.0/24)
and, or, not	Logische Verknüpfungen
TCP-Dump	**Start (Schaltfläche)** Klicken Sie auf die Schaltfläche **Start**, um eine Analyse zu starten. **Stop (Schaltfläche)** Klicken Sie auf die Schaltfläche **Stop**, um eine laufende Analyse zu stoppen. ⇒ Die erfassten Paketinhalte werden in einer Datei (*.*pcap*) zusammengefasst und automatisch vom Gerät heruntergeladen. Anschließend wird die Datei auf dem Gerät gelöscht. Der Zeitpunkt des Herunterladens der Datei wird im Dateinamen wie folgt angegeben: <YYYY-MM-DD_hh:mm:ss> Beispiel**:** *tcpdump_2019-10-09_22_00_00.pcap*

9.3 Snapshot

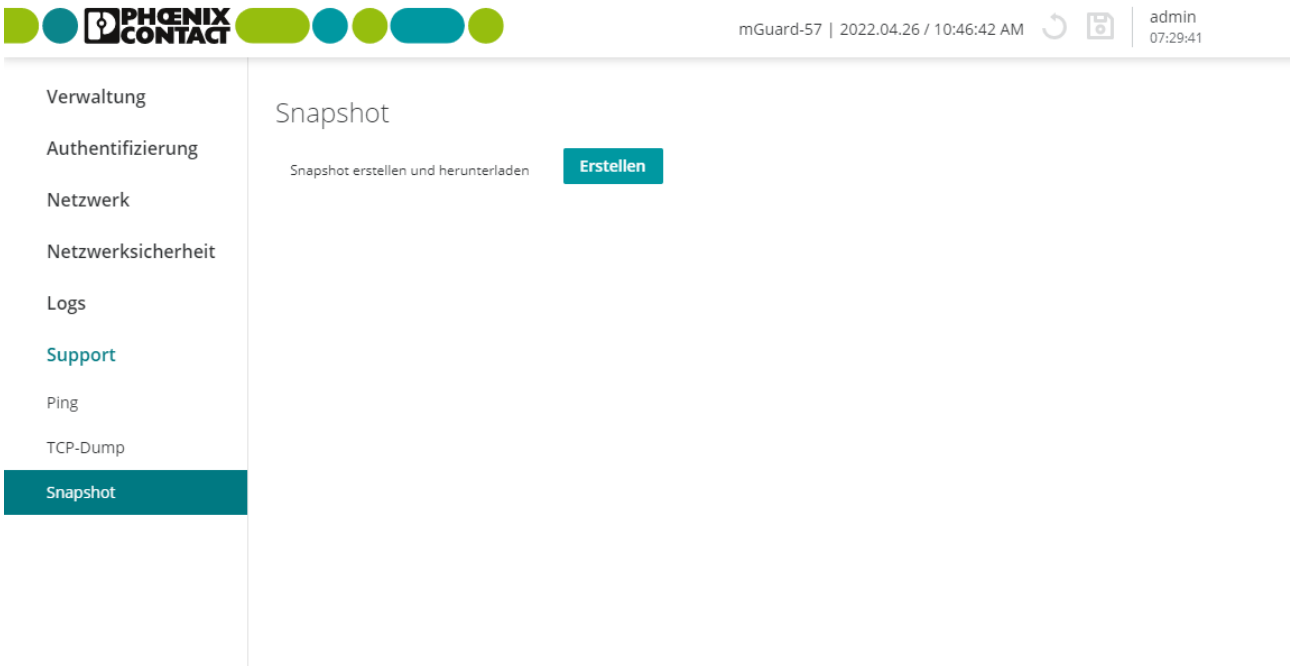


Bild 9-3 Support >> Snapshot

Menü: Support >> Snapshot	
Snapshot	Ein Snapshot kann zur Fehlerdiagnose und bei der Kommunikation mit dem Support verwendet werden. Der Snapshot wird in Form einer komprimierten Datei (im *tar.gz*-Format) erstellt und heruntergeladen. Der Snapshot enthält die aktuelle Konfiguration, Informationen zur Benutzerverwaltung und andere Systeminformationen des Geräts (siehe „Inhalt des Snapshots“ auf Seite 105). Sensitive Daten und sicherheitsrelevante Informationen (z. B. Passwörter oder geheime kryptografische/gehashte Schlüssel) sind im Snapshot nicht enthalten. **Snapshot erstellen und herunterladen** **Erstellen (Schaltfläche)** Klicken Sie auf die Schaltfläche **Erstellen**, um den Snapshot zu erstellen. Der erstellte Snapshot (**.tar.gz*) wird automatisch vom Gerät heruntergeladen. Der Zeitpunkt der Snapshot-Erstellung wird im Dateinamen wie folgt angegeben: <YYYY-MM-DD_hh:mm:ss> Beispiel: *snapshot_2021-10-09_22_00_00.tar.gz*

Inhalt des Snapshots

Tabelle 9-1 Inhalt eines Snapshots

Dateiname	Inhalt / Beschreibung
Dateiformat: *json*	
config.json	Zeigt die aktuelle Gerätekonfiguration.
serdata.json	Zeigt die Serialisierungsdaten, die bei der Herstellung mit dem Gerät verknüpft wurden.
ldap.json	Zeigt die aktuelle Konfiguration zur LDAP-Authentifizierung via LDAP-Server.
users.json	Zeigt aktuelle Informationen über die lokalen Benutzer auf dem Gerät.
Dateiformat: *txt*	
bootloader_version	Zeigt die Version des aktuell installierten Bootloaders.
conntrack	Zeigt den aktuellen Inhalt der Zustandstabelle (*connection tracking table*).
df	Zeigt die aktuelle Belegung des Dateisystems.
eds	Zeigt aktuelle dynamische Status-Informationen zu bestimmten Funktionen des Geräts.
ethtool_eth0	Zeigt Informationen über den Ethernet-Port *eth0* (XF1 / Netzzone 1).
ethtool_eth1	Zeigt Informationen über den Ethernet-Port *eth1* (XF2–5 / Netzzone 2).
ipset_list	Zeigt Informationen über das aktuell verwendete IP-Set.
ip_neight	Zeigt aktuelle Verbindungsinformationen zu angeschlossenen (*benachbarten)* Geräten.
ip_route	Zeigt die aktuelle Routing-Tabelle.
ip_link	Zeigt den aktuellen Verbindungsstatus der Netzwerkinterfaces.
ip_addr	Zeigt die aktuelle Netzwerkkonfiguration.
issue	Informationen zum Firmware-Image.
journal	Zeigt die aktuelle Log-Datei des Systems.
ls_mnt_hfs	Zeigt die aktuell im Dateisystem des Geräts (/mnt/hfs) vorhandenen Dateien und Verzeichnisse.
mount	Zeigt die eingehängten Dateisysteme.
nft_ruleset	Zeigt die aktuell konfigurierten Firewall-Regeln.
nft_tables	Zeigt die aktuell konfigurierten Firewall-Tabellen.
proc_net_dev	Zeigt aktuelle Informationen über den Netzwerkverkehr aller Netzwerk-Interfaces (Datei */proc/net/dev*).
proc_net_snmp	Zeigt Informationen über den Netzwerkverkehr über das SNMP-Protokoll (Datei */proc/net/snmp*).
pstree	Zeigt Informationen über aktuell laufende Prozesse.
services	Zeigt die aktuell auf dem System gestarteten Dienste (*systemd)*.
tpm2_fixed	Zeigt nicht veränderbare Informationen über den TPM-Chip.
tpm2_variable	Zeigt veränderbare Informationen des TPM-Chips.
uptime	Zeigt die aktuelle Betriebszeit und den Load Average des Systems.
userid	Zeigt die User-ID und die Gruppenmitgliedschaft.
version	Zeigt die aktuell installierte Firmware-Version.

A Anhang

A 1 RESTful Configuration API verwenden (Config API)

Neben der Konfiguration über das Web-based Management, kann das Gerät auch über die *RESTful Configuration API* (kurz: *Config API*) konfiguriert werden.

Die Verwendung der *Config API* sollte auf erfahrene Anwender beschränkt werden.

Als Maschine-zu-Maschine-Interface ermöglicht die *RESTful Configuration API* unter anderem eine automatisierte und dynamische Steuerung und Konfiguration des Geräts.

Siehe Anwenderhandbuch „*FL MGUARD 1000 – RESTful Configuration API* “, erhältlich unter phoenixcontact.net/product/1153079).

A 2 Smart-Mode verwenden

Die Verwendung des *Smart-Mode* wird im Anwenderhandbuch „*FL MGUARD 1000 – Installation und Inbetriebnahme“* beschrieben (UM DE FL MGUARD 1000). Erhältlich im Download-Bereich der entsprechenden Produktseite im Phoenix Contact Web-Shop, z. B. unter phoenixcontact.net/product/1153079.

Über den *Smart-Mode* können Gerätefunktionen aufgerufen werden, ohne Zugriff auf eines der Management-Interfaces des Geräts zu haben (WBM oder *Config API*).

Folgende Funktionen stehen zur Verfügung:

– Wiederherstellen des Konfigurationszugriffs
– Wiederherstellen der Werkseinstellung (Unwiderrufliches Löschen aller Daten)
– Update von SD-Karte

A 3 Rechtliche Hinweise (Software License Terms)

Über den Link **Rechtliche Hinweise** am unteren Bildschirmrand können die aktuell gültigen *Software License Terms* (SLT) für das Produkt heruntergeladen werden.

A 4 Drittanbieter-Lizenzen

Über den Link **Rechtliche Hinweise** am unteren Bildschirmrand können die auf dem Gerät verwendeten Software-Komponenten (Module) von Drittanbietern sowie die zugehörigen Lizenzinformationen angezeigt werden.

A 5 Root-DNS-Server

- nameserver 1.1.1.1
- nameserver 1.0.0.1
- nameserver 193.17.47.1
- nameserver 185.43.135.1
- nameserver 185.95.218.42
- nameserver 185.95.218.43
- nameserver 192.99.183.132
- nameserver 149.56.228.45
- nameserver 216.146.35.35
- nameserver 216.146.36.36
- nameserver 84.200.69.80
- nameserver 84.200.70.40
- nameserver 80.80.80.80
- nameserver 80.80.81.81
- nameserver 8.8.8.8
- nameserver 8.8.4.4
- nameserver 156.154.70.1
- nameserver 156.154.70.5
- nameserver 156.154.71.5
- nameserver 9.9.9.10
- nameserver 91.239.100.100
- nameserver 89.233.43.71
- nameserver 64.6.64.6
- nameserver 64.6.65.6
- nameserver 77.88.8.1
- nameserver 77.88.8.8

A 6 Update-Möglichkeiten

In Tabelle 9-2 sind die mGuardNT-Firmwareversionen aufgeführt, von denen ein Update auf die angegebenen Zielversionen durchgeführt werden kann.

Tabelle 9-2 Update-Möglichkeiten

Ausgangsversion	Zielversion	Anmerkungen
1.3.x	1.8.x	– Vor dem Update muss in der Konfiguration der Ausgangsversion sichergestellt werden, dass die Netzwerke der Netzzonen 1 und 2 sich nicht überlappen (siehe Kapitel 6.1.1).
1.4.x		
1.5.x		
1.6.x		
1.7.x		
1.8.y (bei y < x)		

B Verzeichnisanhang

B 1 Abbildungsverzeichnis

Kapitel 1

Kapitel 2

Kapitel 3

Kapitel 4

Kapitel 5

Kapitel 6

Kapitel 7

Kapitel 8

Kapitel 9

Anhang A

Anhang B

B 2 Tabellenverzeichnis

Kapitel 1

Kapitel 2

Kapitel 3

Kapitel 4

Kapitel 5

Kapitel 6

Kapitel 7

Kapitel 8

Kapitel 9

Anhang A

Anhang B

B 3 Erklärung der Fachwörter

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.

Asymmetrische Verschlüsselungsverfahren wie RSA sind jedoch langsam und anfällig für bestimmte Angriffe, weshalb sie oft mit einem symmetrischen Verfahren kombiniert werden (→„Symmetrische Verschlüsselung“ auf Seite 120).

CA-Zertifikat

Wie vertrauenswürdig sind ein Zertifikat und die CA (Certificate Authority), die es ausgestellt hat (→ „X.509-Zertifikat“ auf Seite 119)? Ein CA-Zertifikat kann herangezogen werden, um ein Zertifikat zu überprüfen, das die Signatur dieser CA trägt.

Diese Prüfung ergibt nur dann einen Sinn, wenn davon auszugehen ist, dass das CA-Zertifikat aus authentischer Quelle stammt, also selber echt ist. Wenn darüber Zweifel bestehen, kann das CA-Zertifikat selber überprüft werden.

Wenn es sich um ein Sub-CA-Zertifikat handelt, also ein CA-Zertifikat ausgestellt von einer Sub-CA (Sub Certificate Authority) - was normalerweise der Fall ist -, kann das CA-Zertifikat der übergeordneten CA benutzt werden, um das CA-Zertifikat der ihr untergeordneten Instanz zu überprüfen.

Und gibt es für diese übergeordnete CA eine weitere CA, die ihr wiederum übergeordnet ist, kann deren CA-Zertifikat benutzt werden, um das CA-Zertifikat der ihr untergeordneten Instanz zu prüfen, usw.

Diese Kette des Vertrauens setzt sich fort bis zur Wurzelinstanz, die Root-CA (Root Certificate Authority). Die CA-Datei der Root-CA ist zwangsläufig selbstsigniert. Denn diese Instanz ist die höchste, und der „Anker des Vertrauens“ liegt letztlich bei ihr. Es ist niemand mehr da, der dieser Instanz bescheinigen kann, dass sie die Instanz ist, für die sie sich ausgibt. Eine Root-CA ist daher eine staatliche oder staatlich kontrollierte Organisation.

Der mGuard kann die in ihn importierten CA-Zertifikate benutzen, um die von Gegenstellen „vorgezeigten“ Zertifikate auf Echtheit zu überprüfen.

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 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, der 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 (Quell-IP-Adresse / source IP-address)
– die IP-Adresse des Empfängers (Ziel-IP-Adresse / 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 wurde dessen interne IP-Adresse dem Betriebssystem als Standard-Gateway 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.

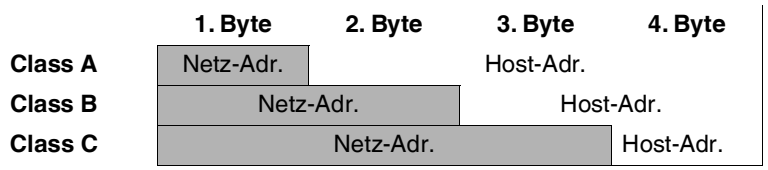
IP-Adresse

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.

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 119).

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 9-3 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

NAT (IP-Masquerading)

Bei *IP-Masquerading*, einer speziellen Variante des *Network Address Translation (NAT)*, 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 Netzwerkteilnehmer 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.

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 die 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.

X.509-Zertifikat

Ein X.509-Zertifikat ist eine Art „Siegel“, das die Echtheit eines öffentlichen Schlüssels (→ „Asymmetrische Verschlüsselung“ auf Seite 115) 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 (→ „CA-Zertifikat“ auf Seite 115).

Dies geschieht nach den Regeln der CA, indem der Aussteller des öffentlichen Schlüssels beispielsweise persönlich zu erscheinen hat. Nach erfolgreicher Überprüfung signiert die CA den öffentliche Schlüssel mit ihrer (digitalen) Unterschrift, ihrer Signatur. Es entsteht ein Zertifikat.

Ein X.509(v3) Zertifikat beinhaltet also einen öffentlichen Schlüssel, Informationen über den Schlüsseleigentümer (angegeben als Distinguised Name (DN)), erlaubte Verwendungszwecke usw. und die Signatur der CA. (→ „Subject, Zertifikat“ auf Seite 117).

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 für die Kommunikation die selben Regeln verwenden. Sie müssen die selbe „Sprache sprechen“. Solche Regeln und Standards bezeichnet man als Protokoll bzw. Übertragungsprotokoll. Oft benutze Protokolle sind z. B. IP, TCP, UDP, PPP, HTTP oder SMTP.

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 ist AES.

TCP/IP (Transmission Control Protocol/Internet Protocol)

Netzwerkprotokolle, die für die Verbindung zweier Rechner im Internet verwendet werden. IP ist hierbei 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 116)

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.

B 4 Stichwortverzeichnis

H

I

K

L

M

N

P

R

S

T

U

V

W

Z

Bitte beachten Sie folgende Hinweise

Allgemeine Nutzungsbedingungen für Technische Dokumentation

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

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

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

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

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

So erreichen Sie uns

Internet

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

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

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Phone: +49 5235 3-00
Fax: +49 5235 3-41200
E-mail: info@phoenixcontact.com
phoenixcontact.com

108420_de_12
Order No. —12

INSPIRING INNOVATIONS