HIRSCHMANN
A BELDEN BRAND

Referenz-Handbuch

Grafische Benutzeroberfläche (GUI)
Industrial Ethernet Firewall
EAGLE One

Die Nennung von geschützten Warenzeichen in diesem Handbuch berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

© 2013 Hirschmann Automation and Control GmbH

Handbücher sowie Software sind urheberrechtlich geschützt. Alle Rechte bleiben vorbehalten. Das Kopieren, Vervielfältigen, Übersetzen, Umsetzen in irgendein elektronisches Medium oder maschinell lesbare Form im Ganzen oder in Teilen ist nicht gestattet. Eine Ausnahme gilt für die Anfertigungen einer Sicherungskopie der Software für den eigenen Gebrauch zu Sicherungszwecken. Bei Geräten mit eingebetteter Software gilt die Endnutzer-Lizenzvereinbarung auf der mitgelieferten CD/DVD.

Die beschriebenen Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart wurden. Diese Druckschrift wurde von Hirschmann Automation and Control GmbH nach bestem Wissen erstellt. Hirschmann behält sich das Recht vor, den Inhalt dieser Druckschrift ohne Ankündigung zu ändern. Hirschmann gibt keine Garantie oder Gewährleistung hinsichtlich der Richtigkeit oder Genauigkeit der Angaben in dieser Druckschrift.

Hirschmann haftet in keinem Fall für irgendwelche Schäden, die in irgendeinem Zusammenhang mit der Nutzung der Netzkomponenten oder ihrer Betriebssoftware entstehen. Im Übrigen verweisen wir auf die im Lizenzvertrag genannten Nutzungsbedingungen.

Die jeweils neueste Version dieses Handbuches finden Sie im Internet auf den Hirschmann-Produktseiten (www.hirschmann.com).

Gedruckt in Deutschland
Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Deutschland
Tel.: +49 1805 141538

Inhalt

Über dieses Handbuch

Das Dokument „Referenz-Handbuch Grafische Benutzeroberfläche (GUI)“ enthält detaillierte Information zur Bedienung der einzelnen Funktionen des Gerätes über die grafische Benutzeroberfläche.

Das Dokument „Referenz-Handbuch Command Line Interface“ enthält detaillierte Information zur Bedienung der einzelnen Funktionen des Gerätes über das Command Line Interface.

Das Dokument „Anwender-Handbuch Installation“ enthält eine Gerätebeschreibung, Sicherheitshinweise, Anzeigebeschreibung und weitere Informationen, die Sie zur Installation des Gerätes benötigen, bevor Sie mit der Konfiguration des Gerätes beginnen.

Das Dokument „Anwender-Handbuch Konfiguration“ enthält die Informationen, die Sie zur Inbetriebnahme des Gerätes benötigen. Es leitet Sie Schritt für Schritt von der ersten Inbetriebnahme bis zu den grundlegenden Einstellungen für einen Ihrer Umgebung angepassten Betrieb.

Die Netzmanagement-Software Industrial HiVision bietet Ihnen weitere Möglichkeiten zur komfortablen Konfiguration und Überwachung:

- Gleichzeitige Konfiguration mehrerer Geräte
- Grafische Benutzeroberfläche mit Netz-Layout
- Autotopologie-Erkennung
- Ereignislogbuch
- Ereignisbehandlung
- Client/Server-Struktur
- Browser-Interface
- ActiveX-Control für SCADA-Integration
- SNMP/OPC-Gateway.

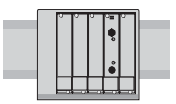
Legende

Die in diesem Handbuch verwendeten Auszeichnungen haben folgende Bedeutungen:

▶	Aufzählung
☐	Arbeitsschritt
■	Zwischenüberschrift
Link	Querverweis mit Verknüpfung
Anmerkung:	Eine Anmerkung betont eine wichtige Tatsache oder lenkt Ihre Aufmerksamkeit auf eine Abhängigkeit.
`Courier`	ASCII-Darstellung in der grafischen Benutzeroberfläche

Verwendete Symbole:

	WLAN-Access-Point
	Router mit Firewall
	Switch mit Firewall
	Router
	Switch
	Bridge

	Hub
	Beliebiger Computer
	Konfigurations-Computer
	Server
	SPS - Speicherprogrammier-bare Steuerung
	I/O - Roboter

Grafische Benutzeroberfläche

Systemvoraussetzungen

Verwenden Sie zum Öffnen der grafischen Benutzeroberfläche HiView. Diese Applikation bietet Ihnen die Möglichkeit, frei von weiteren Anwendungen wie einem Web-Browser oder einer installierten Java-Laufzeitumgebung (JRE), die grafische Benutzeroberfläche zu bedienen.

Alternativ haben Sie die Möglichkeit, die grafische Benutzeroberfläche im Web-Browser zu öffnen, z. B. im Mozilla Firefox ab Version 3.5 oder im Microsoft Internet Explorer ab Version 6. Installieren Sie hierzu auch die Java-Laufzeitumgebung (JRE) in der zuletzt freigegebenen Version. Installationspakete für Ihr Betriebssystem finden Sie unter http://java.com.

Grafische Benutzeroberfläche starten

Voraussetzung für das Starten der grafischen Benutzeroberfläche ist, dass die IP-Parameter im Gerät konfiguriert sind. Das Anwender-Handbuch „Grundkonfiguration“ enthält ausführliche Informationen, die Sie zum Festlegen der IP-Parameter im Gerät benötigen.

Grafische Benutzeroberfläche in HiView starten:

☐ Starten Sie HiView.

☐ Geben Sie in das URL-Feld des Startfensters die IP-Adresse Ihres Gerätes ein.

☐ Klicken Sie „Öffnen“.

HiView stellt die Verbindung zum Gerät her und zeigt das Login-Fenster.

Grafische Benutzeroberfläche im Web-Browser starten:

– Voraussetzung ist, dass Java in den Sicherheitseinstellungen Ihres Web-Browsers aktiviert ist.

☐ Starten Sie Ihren Web-Browser.

☐ Schreiben Sie die IP-Adresse des Gerätes in das Adressfeld des Web-Browsers. Verwenden Sie die folgende Form: `https://xxx.xxx.xxx.xxx`

Der Web-Browser stellt die Verbindung zum Gerät her und zeigt das Login-Fenster.

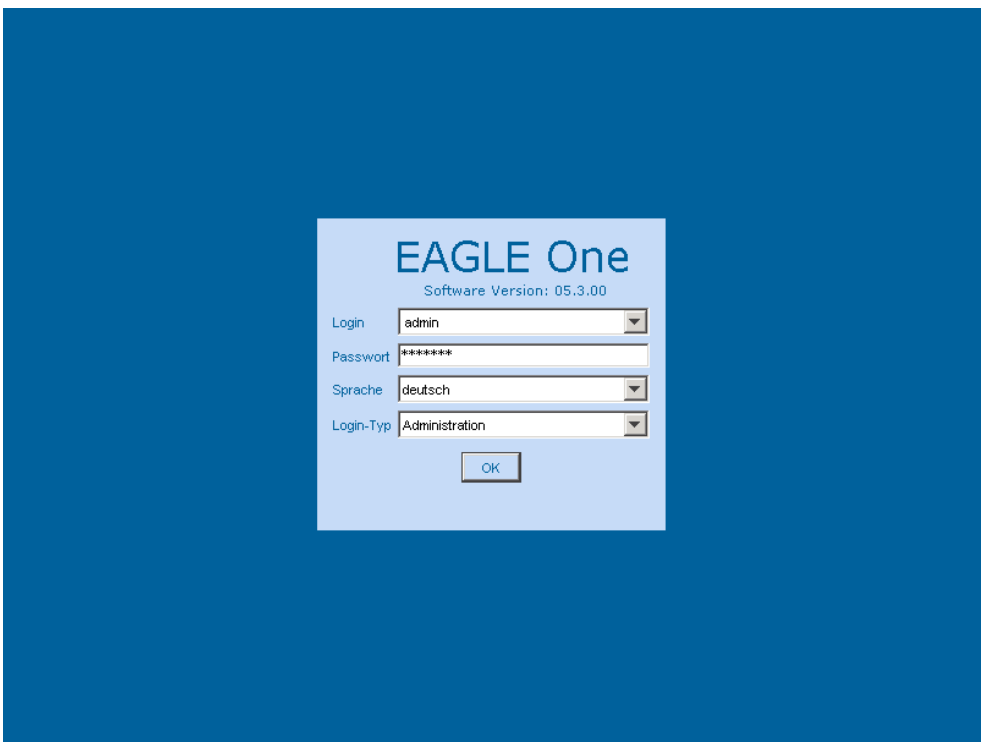


Abb. 1: Login-Fenster

☐ Wählen Sie die gewünschte Sprache aus.
☐ Wählen Sie im Ausklappmenü `Login`
  – `user`, um mit Leserecht oder
  – `admin`, um mit Schreib- und Leserecht

auf das Gerät zuzugreifen.

- ☐ Im Kennwort-Feld ist das Passwort "public", mit dem Sie über Leserechte verfügen, vorgegeben. Wollen Sie mit Schreibrechten auf das Gerät zugreifen, dann markieren Sie den Inhalt des Passwortfeldes und überschreiben ihn mit dem Passwort "private" (Lieferzustand).
- ☐ Wählen Sie im Ausklappmenü `Login-Typ`
  - – Administration, wenn Sie das Gerät verwalten wollen oder
  - – Benutzer-Firewall, wenn Sie sich für die Benutzer-Firewall-Funktion anmelden wollen (Voraussetzung: der im Ausklappmenü `Login` gewählte Benutzer ist in der Benutzer-Firewall bereits angelegt).
- ☐ Klicken Sie „OK“.

Der Bildschirm zeigt die grafische Benutzeroberfläche des Gerätes.

Anmerkung: Änderungen, die Sie an den Dialogen vornehmen, übernimmt das Gerät in den flüchtigen Speicher (RAM), wenn Sie auf „Schreiben“ klicken. Klicken Sie auf „Laden“, um die Anzeige zu aktualisieren.
Um jegliche durchgeführten Änderungen so zu speichern, dass sie nach einem Wiedereinschalten oder Neustart des Gerätes erhalten bleiben, benutzen Sie „Sichern“ im Dialog „Laden/Speichern“ (siehe auf Seite 42 „Konfiguration im nicht-flüchtigen Speicher (NVM)“).

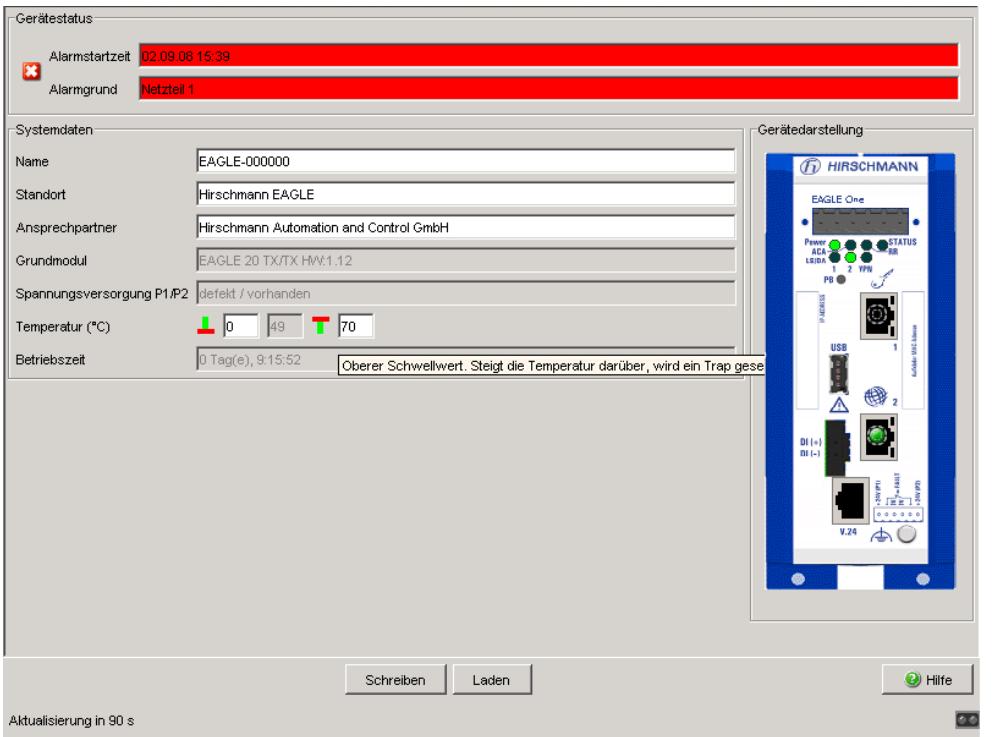
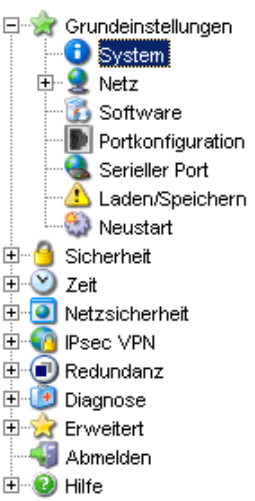


Abb. 2: Grafische Benutzeroberfläche des Gerätes

Menüleiste

Der Menüteil zeigt die Menüpunkte. Durch Platzieren des Mauszeigers im Menüteil und Drücken der rechten Maustaste können Sie mit „Zurück“ auf einen beliebigen, bereits schon vorher ausgewählten Menüpunkt zurückspringen und mit „Vor“ wieder auf einen beliebigen bereits schon vorher ausgewählten Menüpunkt vorspringen.



1 Grundeinstellungen

Das Grundeinstellungen-Menü enthält die Dialoge, Anzeigen und Tabellen zur Grundkonfiguration:

- System
- Netz
- Software
- Portkonfiguration
- Serieller Port
- Laden/Speichern
- Neustart

1.1 System

Das Untermenü „System“ im Grundeinstellungsmenü ist untergliedert in:

- Gerätestatus
- Systemdaten
- Gerätedarstellung
- Aktualisierung

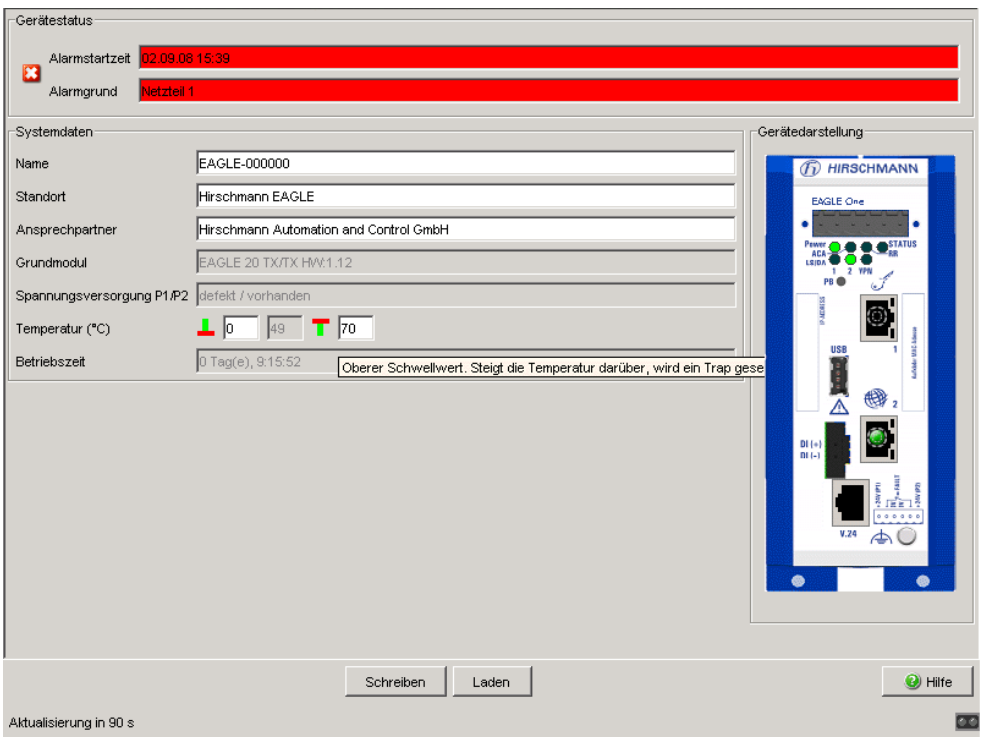


Abb. 3: Untermenü „System“

Gerätestatus

Dieser Bereich der grafischen Benutzeroberfläche gibt Auskunft über den Gerätestatus und Alarmzustand, den das Gerät erkannt hat.

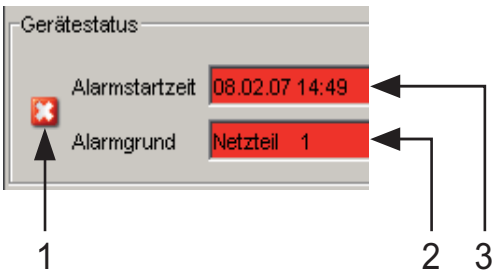


Abb. 4: Gerätestatus- und Alarm-Anzeige
1 - Das Symbol zeigt den Gerätestatus an
2 - Ursache des ältesten, bestehenden Alarms
3 - Beginn des ältesten, bestehenden Alarms

Systemdaten

Die Felder in diesem Rahmen zeigen Betriebsdaten sowie Informationen zum Standort des Gerätes.
- den Systemnamen,
- die Standortbezeichnung,
- den Namen des Ansprechpartners für dieses Gerät
- die Temperaturschwellen.

Bezeichnung	Bedeutung
Name	Systemname dieses Gerätes
Standort	Standort dieses Gerätes
Ansprechpartner	Ansprechpartner für dieses Gerät
Grundmodul	Hardware-Version des Geräts
Spannungsversorgung (P1/P2)	Status der Netzteile (P1/P2)
Temperatur	Temperatur im Gerät. Untere/obere Temperaturschwelle, bei deren Unter-/Überschreiten das Gerät einen Alarm generiert.
Betriebszeit	Zeit, die seit dem letzten Neustart dieses Gerätes vergangen ist.

Tab. 1: Systemdaten

Gerätedarstellung

Die Gerätedarstellung zeigt das Gerät. Symbole auf den Ports stellen den Status der einzelnen Ports dar.

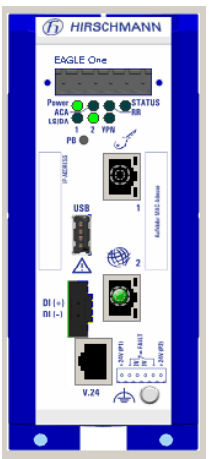


Abb. 5: Gerätedarstellung

Bedeutung der Symbole:

Der Port (10, 100 MBit/s) ist freigegeben und die Verbindung ist in Ordnung.

Der Port ist vom Management gesperrt und hat eine Verbindung.

Der Port ist vom Management gesperrt und hat keine Verbindung.

Der Port ist im Autonegotiation-Modus.

Der Port ist im HDX-Modus.

Aktualisierung

Dieser Bereich der Benutzeroberfläche (Web-based Interface) links unten zeigt an, nach welcher Zeit das Applet die aktuellen Daten dieses Dialogs wieder abruft. Das Klicken auf die „Laden“-Taste bewirkt ein sofortiges Abrufen der aktuellen Daten des Dialogs. Das Applet ruft automatisch alle 100 Sekunden die aktuellen Daten des Gerätes ab.

Abb. 6: Zeit bis zur Aktualisierung

1.2 Netz

Das Untermenü „Netz“ im Grundeinstellungsmenü bietet Ihnen die Möglichkeit, den Netzmodus zu konfigurieren und auszuwählen sowie statische Routen anzulegen:

- Global
- Transparent-Modus
- Router-Modus
- PPoE-Modus
- Routen

1.2.1 Global

Dieser Dialog bietet Ihnen die Möglichkeit, den Netzmodus auszuwählen und Einstellungen für die Weiterleitung von Paketen vorzunehmen.

Bezeichnung	Bedeutung
Modus	Wählen Sie den Modus, in dem Sie das Gerät betreiben möchten: ▶ `transparent`, um den Transparent-Modus, ▶ `router`, um den Router-Modus, oder ▶ `pppoe`, um den PPPoE-Modus einzustellen. Voreinstellung: `transparent`. **Anmerkung:** Die Details für die jeweiligen Netzmodi konfigurieren Sie in den Dialogen „Transparent-Modus“, „Router-Modus“ und „PPPoE-Modus“.
IP-Fragmente weiterleiten	Stellt ein, ob das Gerät IP-Fragmente vermittelt. Voreinstellung: `an`.
Net-Directed Broadcasts weiterleiten	Stellt ein, ob das Gerät Net-Directed Broadcasts vermittelt. Voreinstellung: `aus`.
ICMP-Redirects versenden	Gibt an, ob das Gerät zusätzlich einen ICMP-Redirect sendet, wenn das Gerät ein empfangenes Paket am Empfangs- Interface wieder in das selbe Subnetz routet. Voreinstellung: `an`.

Tab. 2: Netzkonfiguration global, Modus und Weiterleitungs-Einstellungen

Anmerkung:

▶ Die Einstellung für:
  – „IP-Fragmente weiterleiten“

beachtet das Gerät im Transparent-, Router- und PPPoE-Modus.

▶ Die Einstellungen für:
  – „Net-Directed Broadcasts weiterleiten“ und
  – „ICMP-Redirects versenden“

beachtet das Gerät ausschließlich im Router- und PPPoE-Modus.

Anmerkung: Vergewissern Sie sich vor einem Wechsel in einen anderen Modus, dass das Gerät mit der Konfiguration des anderen Modus weiterhin erreichbar ist.

1.2.2 Transparent-Modus

Dieser Dialog bietet Ihnen die Möglichkeit, den Transparent-Modus zu konfigurieren.
Im Transparent-Modus verhält sich das Gerät wie ein Switch und vermittelt auf Schicht 2 des ISO/OSI-Schichtenmodells.

Bezeichnung	Bedeutung
Protokoll	DHCP-Protokoll ein-/ausschalten. Schalten Sie das DHCP-Protokoll ein, wenn das Gerät seine IP-Parameter von einem DHCP-Server auf der Basis der MAC-Adresse oder des Namens des Gerätes beziehen soll. **Anmerkung:** Das EAGLE One-Gerät unterstützt ausschließlich Standard-DHCP. Wenn Sie einen Hirschmann-DHCP-Server verwenden, deaktivieren Sie daher in dessen Pool-Eintrag für das EAGLE One-Gerät die Einstellung „Hirschmann-Gerät“.

Tab. 3: Netz: Protokoll im Transparent-Modus

Bezeichnung	Bedeutung
IP-Adresse	Eingeben der IP-Adresse, über die Sie das Gerät erreichen können.
MAC-Adresse	Anzeige der MAC-Adresse.
Gateway-Adresse	Eingeben der Gateway-Adresse.
Netzmaske	Eingeben der Netzmaske.
VLAN-Tag verwenden	Durch Ankreuzen legen Sie fest, dass das Gerät das VLAN-Tag der Datenpakete auswertet, die an das Gerät (Management) adressiert sind. Damit ist das Management des Gerätes ausschließlich aus dem VLAN mit der Management VLAN-ID erreichbar.
VLAN-ID	Eingeben der VLAN-ID (1-4.094) des VLANs. **Anmerkung:** Das Gerät verwendet die in diesem Feld eingegebene VLAN-ID ausschließlich dann, wenn „VLAN-Tag verwenden“ angekreuzt ist.

Tab. 4: Netz: Lokal im Transparent-Modus

Bezeichnung	Bedeutung
Funktion	Ein-/Ausschalten des HiDiscovery-Protokolls. Das HiDiscovery-Protokoll ermöglicht Ihnen, dem Gerät an Hand seiner MAC-Adresse eine IP-Adresse zuzuweisen. Aktivieren Sie das HiDiscovery-Protokoll, wenn Sie von Ihrem PC aus mit der mitgelieferten HiDiscovery-Software dem Gerät eine IP-Adresse zuweisen wollen (Lieferzustand: „Funktion“ `an`, „Zugriff“ `read-write`).
Zugriff	lesen und schreiben: IP-Adressen lesen und zuweisen read-only: IP-Adressen lesen

Tab. 5: Netz: HiDiscovery-Protokoll im Transparent-Modus

Bezeichnung	Bedeutung
Relay	Durch Ankreuzen legen Sie fest, dass das Gerät das HiDiscovery-Protokoll weiterleitet (Lieferzustand: deaktiviert).

Tab. 6: Netz: HiDiscovery-Relay im Transparent-Modus

Anmerkung: Den momentan aktiven Netzmodus zeigt das Gerät im Netz-Submenü „Global“ an.

Anmerkung: Der Dialog `Erweitert:Paketweiterleitung` (siehe auf Seite 212) ermöglicht Ihnen, die Weiterleitung von STP-, GMRP- und DHCP-Datenpaketen ein- und auszuschalten. Voreinstellung: keine Weiterleitung dieser Pakete.

Anmerkung: Das Gerät bietet Ihnen ausschließlich im und für den Transparent-Modus die Konfiguration mit HiDiscovery an. Der Transparent-Modus ist im Lieferzustand eingeschaltet.

1.2.3 Router-Modus

Dieser Dialog bietet Ihnen die Möglichkeit den Router-Modus zu konfigurieren.
Im Router-Modus verhält sich das Gerät wie ein Router und vermittelt auf Schicht 3 des ISO/OSI-Schichtenmodells.

Internes Interface (Port 1)

Bezeichnung	Bedeutung
Protokoll	DHCP-Protokoll ein-/ausschalten. Schalten Sie das DHCP-Protokoll ein, wenn das Gerät seine IP-Parameter von einem DHCP-Server auf der Basis der MAC-Adresse oder des Namens des Gerätes beziehen soll. **Anmerkung:** Das EAGLE One-Gerät unterstützt ausschließlich Standard-DHCP. Wenn Sie einen Hirschmann-DHCP-Server verwenden, deaktivieren Sie daher in dessen Pool-Eintrag für das EAGLE One-Gerät die Einstellung „Hirschmann-Gerät“.

Tab. 7: Netz: Protokoll im Router-Modus am internen Interface

Bezeichnung	Bedeutung
IP-Adresse	Eingeben der IP-Adresse, über die Sie das Gerät erreichen können.
Netzmaske	Eingeben der Netzmaske.
VLAN-Tag verwenden	Bei eingeschalteter Funktion akzeptiert das Gerät ausschließlich Datenpakete mit der im Feld VLAN-ID eingegebenen VLAN-ID. Die NAT-Funktionen sind dabei außer Kraft gesetzt.
VLAN-ID	Eingeben der VLAN-ID (1-4.094) des VLANs. **Anmerkung:** Das Gerät verwendet die in diesem Feld eingegebene VLAN-ID ausschließlich dann, wenn „VLAN-Tag verwenden“ angekreuzt ist.

Tab. 8: Netz: Lokal im Router-Modus am internen Interface

Externes Interface (Port 2)

Bezeichnung	Bedeutung
Protokoll	DHCP-Protokoll ein-/ausschalten. Schalten Sie das DHCP-Protokoll ein, wenn das Gerät seine IP-Parameter von einem DHCP-Server auf der Basis der MAC-Adresse oder des Namens des Gerätes beziehen soll. **Anmerkung:** Das EAGLE One-Gerät unterstützt ausschließlich Standard-DHCP. Wenn Sie einen Hirschmann-DHCP-Server verwenden, deaktivieren Sie daher in dessen Pool-Eintrag für das EAGLE One-Gerät die Einstellung „Hirschmann-Gerät“.

Tab. 9: Netz: Protokoll im Router-Modus am externen Interface

Bezeichnung	Bedeutung
IP-Adresse	Eingeben der IP-Adresse, über die Sie das Gerät erreichen können.
Netzmaske	Eingeben der Netzmaske.
VLAN-Tag verwenden	Bei eingeschalteter Funktion akzeptiert das Gerät ausschließlich Datenpakete mit der im Feld VLAN-ID eingegebenen VLAN-ID. Die NAT-Funktionen sind dabei außer Kraft gesetzt.
VLAN-ID	Eingeben der VLAN-ID (1-4.094) des VLANs. **Anmerkung:** Das Gerät verwendet die in diesem Feld eingegebene VLAN-ID ausschließlich dann, wenn „VLAN-Tag verwenden“ angekreuzt ist.
Default Gateway	Eingabe des Standard-Gateways. Es ist unerheblich, ob das Subnetz, in dem das Gateway liegt, dem internen oder externen Interface zugeordnet ist. Zweck eines Gateways ist, Netzknoten zu erreichen, die außerhalb der Subnetze liegen, die direkt einem Interface zugeordnet sind. Das Gerät sendet Pakete, deren Zieladresse außerhalb der den Interfaces zugeordneten Subnetze liegen, an dieses Gateway. Die IP-Adresse des Gateways muss in einem der Subnetze liegen, die zu einem Interface gehören.

Tab. 10: Netz: Lokal im Router-Modus am externen Interface

Weitere IP-Interfaces

Dieser Teil des Dialoges bietet Ihnen die Möglichkeit, mehrere Subnetze an ein Router-Interface anzuschließen (Multinetting) und VLAN-Interfaces auf einem Router-Interface zu erzeugen. Das bietet Ihnen die Möglichkeit, zwischen VLANs zu routen.

☐ Klicken Sie auf „Erzeugen“, um ein Fenster für die Eingabe einer neuen Zeile in der Tabelle zu öffnen.
Wählen Sie „Internes Interface“ oder „Externes Interface“.
Nach der Eingabe
– der IP-Adresse,
– der Netzmaske,
– von VLAN-Tag verwenden und
– der VLAN-ID
klicken Sie auf „Schreiben“, um die Eingabe in die Tabelle zu übertragen.

☐ Klicken Sie auf „Zurück", um zur Tabelle zurückzukehren.

☐ Erzeugen Sie bei Bedarf zusätzliche Einträge in der Tabelle durch Klicken auf „Erzeugen...“.

Die Spalte „Aktiv" bietet Ihnen die Möglichkeit, die einzelnen Einträge in der Tabelle zu aktivieren/deaktivieren.

Sie können die Einträge direkt in der Tabelle ändern.

Um eine Zeile zu löschen, wählen Sie die Zeile aus und klicken Sie auf „Eintrag löschen".

Bezeichnung	Bedeutung
IP-Adresse	Eingeben der IP-Adresse
Netzmaske	Eingeben der Netzmaske
VLAN-Tag verwenden	Bei eingeschalteter Funktion akzeptiert das Gerät ausschließlich Datenpakete mit der im Feld VLAN-ID eingegebenen VLAN-ID. Die NAT-Funktionen sind dabei außer Kraft gesetzt.
VLAN-ID	Eingeben der VLAN-ID (1-4.094) des VLANs. **Anmerkung:** Das Gerät verwendet die in diesem Feld eingegebene VLAN-ID ausschließlich dann, wenn „VLAN-Tag verwenden“ angekreuzt ist.

Tab. 11: Netz: Tabelle für weitere IP-Adress-Einträge

Anmerkung: Den momentan aktiven Netzmodus zeigt das Gerät im Netz-Submenü „Global“ an.

1.2.4 PPPoE-Modus

Dieser Dialog bietet Ihnen die Möglichkeit den PPPoE- (Point to Point Protocoll over Ethernet-) Modus zu konfigurieren.
Im PPPoE-Netzmodus stellt das Gerät eine Punkt-zu-Punkt-Verbindung zu einem Einwahlknoten her.

Anmerkung: Benutzen Sie im PPPoE-Modus die NAT-Funktion, wenn Sie im internen Netz private IP-Adressen verwenden und ins öffentliche Netz kommunizieren wollen. Das Gerät vermittelt im Lieferzustand vom internen in das externe Netz, auch wenn NAT ausgeschaltet ist. Das Anlegen eines Paketfilters hilft Ihnen, dies zu verhindern.

Internes Interface (Port 1)

Bezeichnung	Bedeutung
Protokoll	DHCP-Protokoll ein-/ausschalten. Schalten Sie das DHCP-Protokoll ein, wenn das Gerät seine IP-Parameter von einem DHCP-Server auf der Basis der MAC-Adresse oder des Namens des Gerätes beziehen soll. **Anmerkung:** Das EAGLE One-Gerät unterstützt ausschließlich Standard-DHCP. Wenn Sie einen Hirschmann-DHCP-Server verwenden, deaktivieren Sie daher in dessen Pool-Eintrag für das EAGLE One-Gerät die Einstellung „Hirschmann-Gerät“.

Tab. 12: Netz: Protokoll im PPPoE-Modus am internen Interface

Bezeichnung	Bedeutung
IP-Adresse	Eingeben der IP-Adresse, über die Sie das Gerät erreichen können.
Netzmaske	Eingeben der Netzmaske.
VLAN-Tag verwenden	Bei eingeschalteter Funktion akzeptiert das Gerät ausschließlich Datenpakete mit der im Feld VLAN-ID eingegebenen VLAN-ID. Die NAT-Funktionen sind dabei außer Kraft gesetzt.
VLAN-ID	Eingeben der VLAN-ID (1-4.094) des VLANs. **Anmerkung:** Das Gerät verwendet die in diesem Feld eingegebene VLAN-ID ausschließlich dann, wenn „VLAN-Tag verwenden“ angekreuzt ist.

Tab. 13: Netz: Lokal im PPPoE-Modus am internen Interface

Externes Interface (Port 2)

Bezeichnung	Bedeutung
Benutzername	Eingeben des vom Provider zugewiesenen Benutzernamens.
Passwort	Eingeben des vom Provider zugewiesenen Kennworts.
Interface-MTU	Eingabe der vom Provider zugewiesenen maximalen Paketgröße, bei der die Datenpakete noch nicht fragmentiert werden (Maximum Transmission Unit). Zulässige Werte: 60-1.500 Bytes, Voreinstellung: 1.492 Bytes.

Tab. 14: Netz: Benutzer-Identifikation und MTU im PPPoE-Modus am externen Interface

Bezeichnung	Bedeutung
Automatisches Trennen einschalten	Durch Ankreuzen legen Sie fest, dass das Gerät die PPPoE-Verbindung täglich um die angegebene Uhrzeit automatisch trennt. Bevor Sie diese Funktion aktivieren, prüfen Sie, ob die Systemzeit Ihres EAGLE One-Gerätes korrekt eingestellt ist.
Uhrzeit (Stunde) zum Trennen	Eingeben der Uhrzeit (Stunde), zu der das Gerät die PPPoE-Verbindung täglich automatisch trennt. Wertebereich: 0 bis 23.

Tab. 15: Netz: Automatisches Trennen der PPPoE-Verbindung

Bezeichnung	Bedeutung
IP-Adresse	Anzeige der vom Provider zugewiesenen IP-Adresse
Netzmaske	Anzeige der vom Provider zugewiesenen Netzmaske
Gateway	Anzeige der vom Provider zugewiesenen Gateways
Status	Anzeige des Verbindungsstatus

Tab. 16: Netz: Lokale Parameter im PPPoE-Modus am externen Interface

Weitere IP-Adressen anlegen

Einträge für weitere IP-Adressen bietet Ihnen die Möglichkeit, mehrere Subnetze an ein Routerinterface anzuschließen (Multinetting).

☐ Klicken Sie auf „Erzeugen...“, um ein Fenster für die Eingabe einer neuen Zeile in der Tabelle zu öffnen.
Geben Sie ein:
– IP-Adresse,
– Netzmaske,
– VLAN-Tag verwenden,
– VLAN-ID
und klicken Sie auf „Schreiben“, um die Eingabe in die Tabelle zu übertragen.

☐ Klicken Sie auf „Zurück", um zur Tabelle zurückzukehren.

☐ Erzeugen Sie bei Bedarf zusätzliche Einträge in der Tabelle durch Klicken auf „Erzeugen...“.

Die Spalte „Aktiv" bietet Ihnen die Möglichkeit, die einzelnen Einträge in der Tabelle zu aktivieren/deaktivieren.

Sie können die Einträge direkt in der Tabelle ändern.

Um eine Zeile zu löschen, wählen Sie die Zeile aus und klicken Sie auf „Eintrag löschen".

Bezeichnung	Bedeutung
IP-Adresse	Eingeben der IP-Adresse
Netzmaske	Eingeben der Netzmaske
VLAN-Tag verwenden	Bei eingeschalteter Funktion akzeptiert das Gerät ausschließlich Datenpakete mit der im Feld VLAN-ID eingegebenen VLAN-ID. Die NAT-Funktionen sind dabei außer Kraft gesetzt.
VLAN-ID	Eingeben der VLAN-ID (1-4.094) des VLANs. **Anmerkung:** Das Gerät verwendet die in diesem Feld eingegebene VLAN-ID ausschließlich dann, wenn „VLAN-Tag verwenden“ angekreuzt ist.

Tab. 17: Netz: Tabelle für weitere IP-Adress-Einträge

Anmerkung: Den momentan aktiven Netzmodus zeigt das Gerät im Netz-Submenü „Global“ an.

1.2.5 Routen

Die Routen-Tabelle bietet Ihnen die Möglichkeit, statische Routen einzutragen.

Routen-Eintrag in Tabelle erzeugen

☐ Klicken Sie auf „Erzeugen...“, um ein Fenster für die Eingabe einer neuen Zeile in der Tabelle zu öffnen.
Wählen Sie „Internes Interface“ oder „Externes Interface“.
Nach der Eingabe
– des Zielnetzes,
– der Zielnetzmaske und
– des Next Hop
klicken Sie auf „Schreiben“, um die Eingabe in die Tabelle zu übertragen.

☐ Klicken Sie auf „Zurück", um zur Tabelle zurückzukehren.

☐ Erzeugen Sie bei Bedarf zusätzliche Einträge in der Tabelle durch Klicken auf „Erzeugen...“.

Die Spalte „Aktiv" bietet Ihnen die Möglichkeit, die einzelnen Einträge in der Tabelle zu aktivieren/deaktivieren.

Sie können die Einträge direkt in der Tabelle ändern.

Um eine Zeile zu löschen, wählen Sie die Zeile aus und klicken Sie auf „Eintrag löschen".

Bezeichnung	Bedeutung
Zielnetz	Erste IP-Adresse des Ziel-Subnetzes
Zielnetzmaske	Netzmaske des Ziel-Subnetzes
Next Hop	Gateway IP-Adresse

Tab. 18: Tabelle für Routen

1.3 Software

Der Dialog Software bietet Ihnen die Möglichkeit, die im Gerät vorhandenen Software-Versionen anzuzeigen und ein Software-Update des Gerätes via Datei-Auswahl durchzuführen.

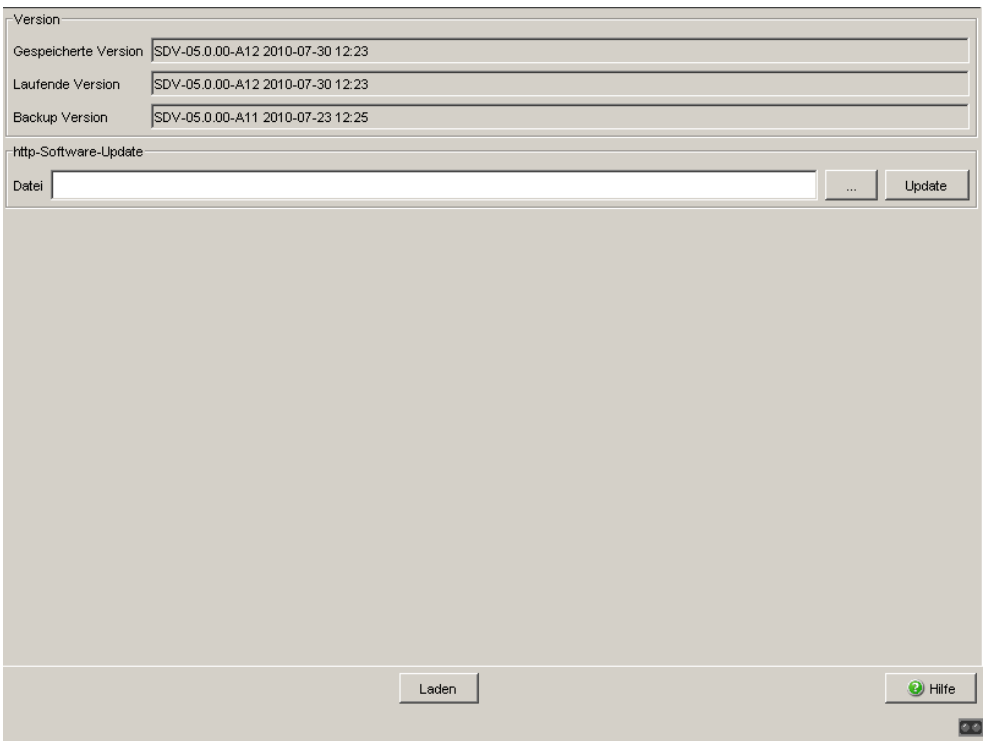


Abb. 7: Dialog Software

Für ein HTTPS-Software-Update (über ein Datei-Auswahl-Fenster) benötigen Sie die Geräte-Software auf einem Datenträger, den Sie von Ihrer Workstation aus erreichen.

Bezeichnung	Bedeutung
Rahmen „Version“	
Gespeicherte Version	Zeigt die Version der im Flash gespeicherten Software an.
Laufende Version	Zeigt die Version der auf dem Gerät laufenden Software an.
Backup-Version	Zeigt die Version der im Flash gespeicherten Backup-Software an.
Rahmen „https-Software-Update“	
Eingabezeile „Datei“	Anzeige der ausgewählten Geräte-Software (*.bin).
Taste „...“	Öffnen eines Dateiauswahlfensters
Taste „Update“	Übertragen der ausgewählten Geräte-Software auf das Gerät.

Tab. 19: Software-Versionsanzeige und -Update

Das Ende der Update-Aktion wird durch eine der folgenden Meldungen angezeigt:

- Update erfolgreich beendet.
- Update fehlgeschlagen, Ursache: siehe Textstring der Meldung.

☐ Nach erfolgreichem Laden aktivieren Sie die neue Software:
Wählen Sie den Dialog `Grundeinstellungen: Neustart` und führen Sie einen Kaltstart durch.
Bei einem Kaltstart lädt das Gerät die Software neu aus dem nichtflüchtigen Speicher, startet neu und führt einen Selbsttest durch.

☐ Klicken Sie in Ihrem Browser auf „Neu laden“, um nach dem Booten des Gerätes wieder auf das Gerät zugreifen zu können.

1.4 Portkonfiguration

Diese Konfigurationstabelle bietet Ihnen die Möglichkeit, jeden Port des Gerätes zu konfigurieren.

Variable	Bedeutung	Mögliche Werte	Lieferzustand
Port	Bezeichnung des Ports (int: 1, ext: 2)	-	–
Name	Für jeden Port einen beliebigen Namen eintragen.	ASCII-Zeichen, maximal 64 Zeichen	–
Port an	Den Port durch Ankreuzen einschalten.		
Verbindungs-fehler weiter-melden	Durch Ankreuzen festlegen, dass ein erkannter Verbindungsfehler an diesem Port an den Gerätestatus und den Meldekontakt weitergemeldet wird.	ein/aus	ein
Automatische Konfiguration	Aktivieren der automatischen Auswahl der Betriebsart eines Ports durch Ankreuzen des zugehörige Feldes. Nach dem Einschalten der automatischen Konfiguration vergehen einige Sekunden, bis die Betriebsart eingestellt ist.	ein/aus	ein
Manuelle Konfiguration	Einstellen der Betriebsart an diesem Port	– 10 Mbit/s Halbduplex (HDX)[a] – 10 Mbit/s Vollduplex (FDX)[a] – 100 Mbit/s Halbduplex (HDX) – 100 Mbit/s Vollduplex (FDX) [a] Nur für TX-Ports	100 Mbit/s Vollduplex (FDX)
Link/Aktuelle Betriebsart	Anzeige der aktuellen Betriebsart und damit Anzeige einer bestehenden Verbindung.		

Tab. 20: Einstellmöglichkeiten pro Port

Anmerkung: Die aktive automatische Konfiguration hat Vorrang vor der manuellen Konfiguration.

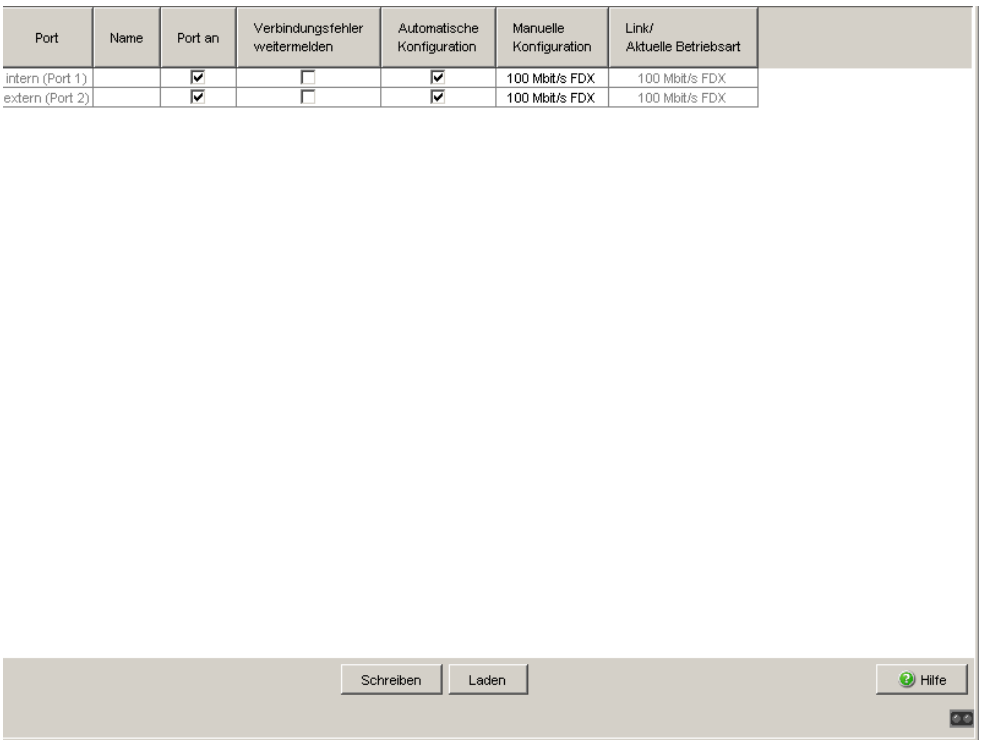


Abb. 8: Dialog Port-Konfigurationstabelle

1.5 Serieller Port

Dieser Dialog bietet Ihnen die Möglichkeit, den seriellen Port des Gerätes

- als Terminal- /CLI-Schnittstelle (Voreinstellung) oder
- als Modem-Schnittstelle

zu konfigurieren.

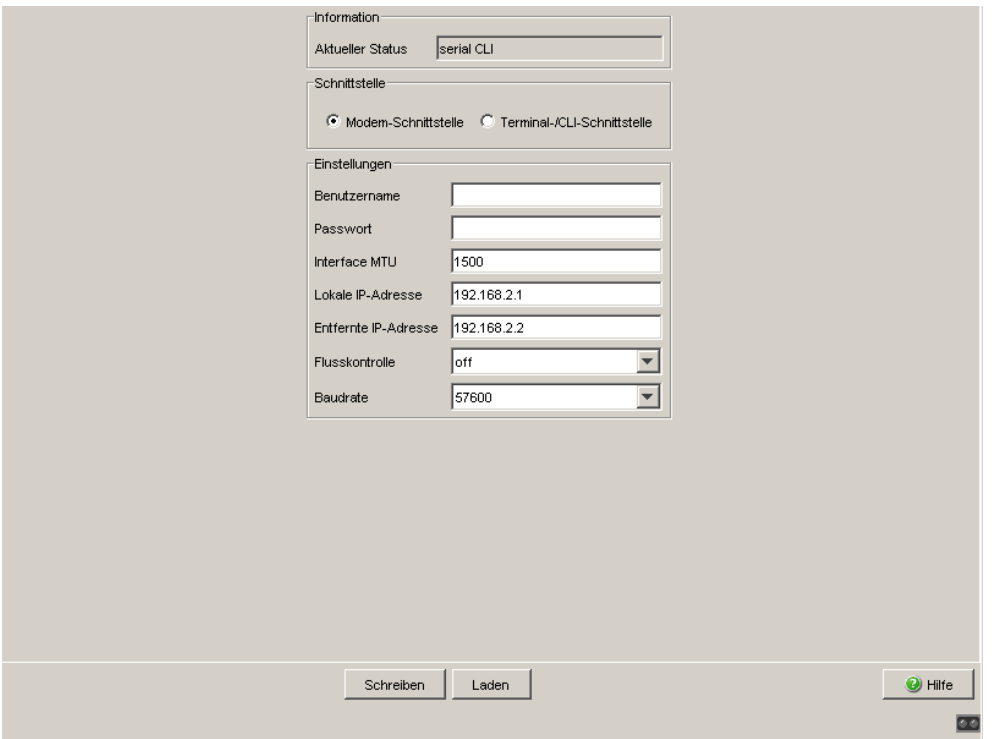


Abb. 9: Dialog Serieller Port

1.5.1 Konfiguration als Terminal/CLI-Schnittstelle

☐ Wählen Sie im Rahmen „Schnittstelle" `Terminal-/CLI-Schnittstelle`.

Im Modus Terminal-/CLI-Schnittstelle ist die Schnittstelle fest auf die folgenden Parameter eingestellt:

- 9.600 Bits/s,
- 8 Datenbits,
- keine Parität,
- 1 Stoppbit,
- keine Flusskontrolle.

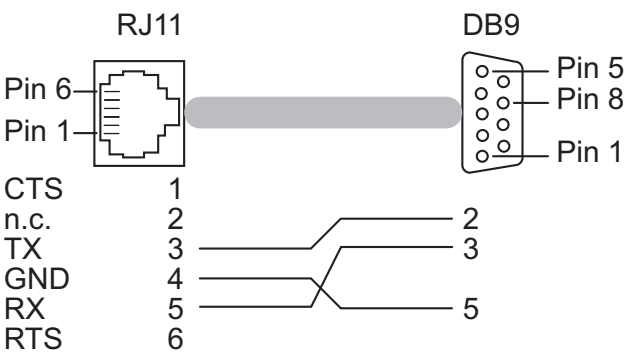


Abb. 10: Pin-Belegung des Terminalkabels

1.5.2 Konfiguration als Modem-Schnittstelle

☐ Wählen Sie im Rahmen „Schnittstelle" `Modem-Schnittstelle`.
Das Gerät zeigt den Rahmen „Einstellungen“ an.

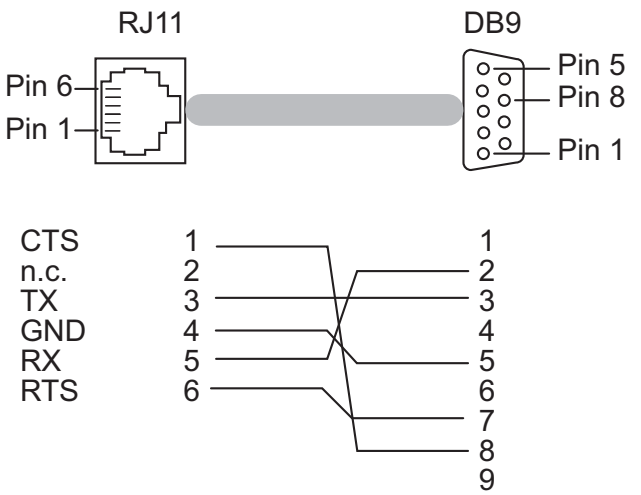


Abb. 11: Pin-Belegung des Modemkabels

Bezeichnung	Bedeutung
Benutzername	Eingeben des PPP-Benutzernamen für den Zugriff eines entfernten Geräts auf das EAGLE One-Gerät (PAP, CHAP).
Passwort	Eingeben des PPP-Kennworts für den Zugriff eines entfernten Geräts auf das EAGLE One-Gerät (PAP, CHAP).
Interface-MTU	Eingabe der maximalen Paketgröße für die PPP-Verbindung (Maximum Transmission Unit). Das Gerät fragmentiert Datenpakete, wenn sie größer als der eingegebene Wert sind. Zulässige Werte: 60-1.500 Bytes. Voreinstellung: 1.500 Bytes. Wählen Sie einen kleineren Wert, wenn Sie wissen, dass Ihr Internet-Service-Provider einen kleineren Wert verwendet oder wenn keine Verbindung zustande kommt.
Lokale IP-Adresse	Eingeben der IP-Adresse des seriellen Ports. Wählen Sie für den seriellen Port eine IP-Adresse, die zu einem anderen Subnetz gehört, als die unter „Transparent-Modus“, „Router-Modus“ und „PPPoE-Modus“ vergebenen IP-Adressen.
Entfernte IP-Adresse	Eingeben der IP-Adresse des entfernten Gerätes. Wählen Sie für den seriellen Port eine IP-Adresse, die zu einem anderen Subnetz gehört, als die unter „Transparent-Modus“, „Router-Modus“ und „PPPoE-Modus“ vergebenen IP-Adressen.
Flusskontrolle	Flusskontrolle ein-/ausschalten.
Baudrate	Wahl der Baudrate. Wählen Sie an Ihrem Modem und dem seriellem Port des EAGLE One dieselbe Baudrate (typisch: 57.600 Baud).
Status	Status der seriellen Schnittstelle im Modembetrieb. Mögliche Meldungen: „not connected“ oder „peer connected“. Im Terminal-/CLI-Modus lautet die Meldung „serial CLI mode“

Tab. 21: Einstellungen für Modem-Betrieb

Anmerkung: Wenn Sie den Modus `Terminal-/CLI-Schnittstelle` wählen, reduziert das Gerät die einstellbaren Parameter auf die der Terminal-/CLI-Schnittstelle.

Anmerkung: Konfigurieren Sie die Filterregeln im Dialog „Eingehende PPP-Pakete“ im Menü `Netzwerksicherheit:Paketfilter` so, dass die Firewall den Datenverkehr zwischen entfernter und lokaler IP-Adresse ermöglicht.

1.6 Laden/Speichern

Dieser Dialog bietet Ihnen die Möglichkeit,

- eine Konfiguration zu laden,
- eine Konfiguration zu speichern,
- eine Konfiguration anzuzeigen,
- eine Konfiguration zu löschen,
- eine Konfiguration zu aktivieren,
- eine Konfiguration zu erzeugen,
- den ACA zur Konfiguration zu verwenden,
- eine Konfigurationsänderung zu widerrufen.

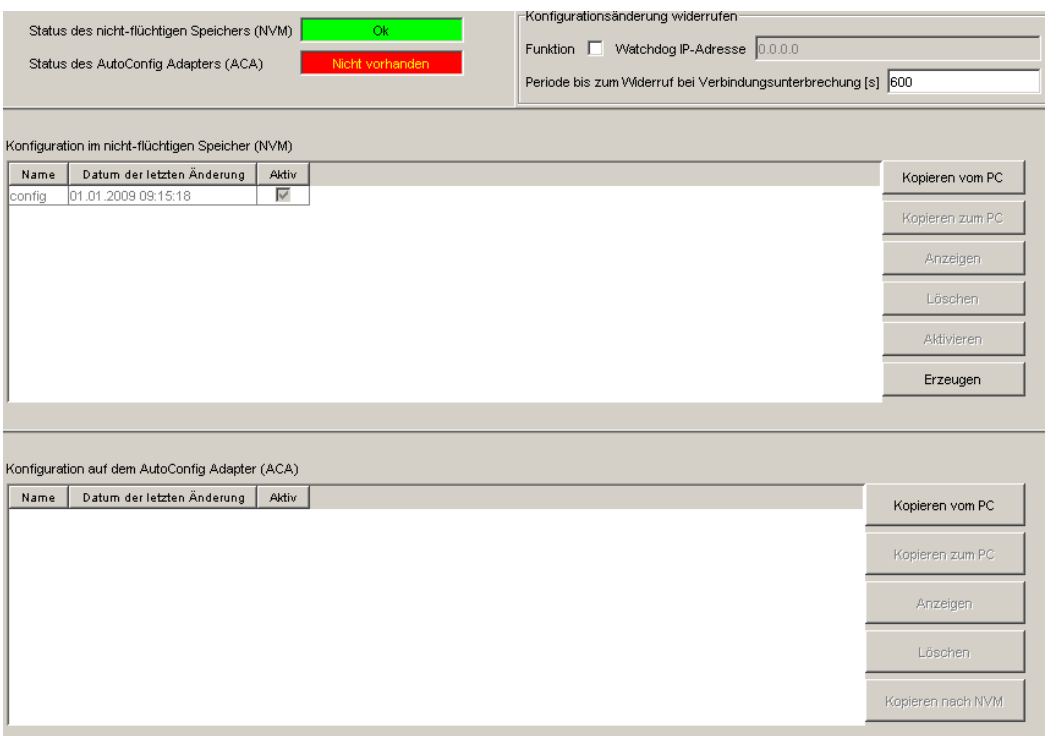


Abb. 12: Dialog Laden/Speichern

1.6.1 Statusanzeigen

Bezeichnung	Bedeutung
Ok	Konfigurationsdaten von NVM und Gerät stimmen überein.
Nicht synchronisiert	Konfigurationsdaten von NVM und Gerät stimmen nicht überein.

Tab. 22: Status des nicht-flüchtigen Speichers (NVM)

Bezeichnung	Bedeutung
Ok	AutoConfiguration Adapter angeschlossen. Konfigurationsdaten von ACA und Gerät stimmen überein.
Nicht synchronisiert	Die Konfigurationsdaten der aktiven Konfiguration stimmen auf ACA und NVM nicht überein.
Nicht vorhanden	Kein AutoConfiguration Adapter angeschlossen..

Tab. 23: Status des AutoConfiguration Adapters (ACA)

1.6.2 Konfiguration im nicht-flüchtigen Speicher (NVM)

In der Tabelle sind die einzelnen Konfigurationsdateien des nicht-flüchtigen Speichers aufgelistet.

Bezeichnung	Bedeutung
Name	Name der Konfigurationsdatei
Datum der letzten Änderung	Speicherdatum DD.MM.JJJJ HH:MM:SS
Aktiv	Anzeige der aktiven Konfiguration

Tab. 24: Konfiguration im nicht-flüchtigen Speicher (NVM)

Anmerkung: Der Name einer Konfigurationsdatei darf bis zu 32 Zeichen lang sein. Erlaubt sind alphanumerische Zeichen („A“ bis „Z“, „a“ bis „z“, „0“ bis „9“) sowie der Unterstrich „_“ und der Bindestrich „-“.

Bezeichnung	Bedeutung
Kopieren vom PC	Laden einer Konfigurationsdatei von einem PC auf das Gerät. Die Konfigurationsdatei erscheint in einem neuen Tabelleneintrag.
Kopieren zum PC	Speichern einer Konfigurationsdatei vom Gerät auf einen PC.
Anzeigen	Anzeigen einer Konfigurationsdatei.
Löschen	Löschen einer Konfigurationsdatei.
Aktivieren	Aktivieren einer Konfigurationsdatei. In der Spalte „Aktiv“ zeigt Ihnen das Gerät die aktive Konfiguration an.
Erzeugen	Speichern der aktuellen Konfiguration in einer Konfigurationsdatei auf das Gerät (und den ACA).

Tab. 25: Bearbeiten der Tabelleneinträge

Wenn Sie die laufende Konfiguration verändern (z. B. einen Port ausschalten), ändert die grafische Benutzeroberfläche das „Laden/Speichern“-Symbol im Navigationsbaum von einem Diskettensymbol in ein gelbes Dreieck. Nach dem Speichern der Konfiguration zeigt die grafische Benutzeroberfläche das „Laden/Speichern“-Symbol wieder als Diskette an.

Anmerkung: Den Lieferzustand erhalten Sie mit `Neustart: Lieferzustand herstellen` (siehe Seite 47). Beachten Sie, dass das Gerät alle Tabellen, Einstellungen und Dateien auf dem Gerät und auf einem angeschlossenen ACA löscht.

1.6.3 Konfiguration auf dem AutoConfiguration Adapter (ACA)

Ein ACA ist ein Hilfsmittel zum Speichern der Konfigurationsdaten eines Gerätes. Ein ACA ermöglicht bei einem erkannten Ausfall eine einfache Konfigurationsdatenübernahme durch ein Ersatzgerät des gleichen Typs.

In der Tabelle sind die einzelnen Konfigurationsdateien eines AutoConfiguration Adapters (ACA) aufgelistet.

Bezeichnung	Bedeutung
Name	Name der Konfigurationsdatei
Datum der letzten Änderung	Speicherdatum DD.MM.JJJJ HH:MM:SS
Aktiv	Anzeige der aktiven Konfiguration

Tab. 26: Konfiguration auf dem AutoConfiguration Adapter (ACA)

Bezeichnung	Bedeutung
Kopieren vom PC	Laden einer Konfigurationsdatei von einem PC auf den ACA. Die Konfigurationsdatei erscheint in einem neuen Tabelleneintrag.
Kopieren zum PC	Speichern einer Konfigurationsdatei vom ACA auf einen PC.
Anzeigen	Anzeigen einer Konfigurationsdatei.
Löschen	Löschen einer Konfigurationsdatei.
Kopieren nach NVM	Speichern einer Konfigurationsdatei vom ACA auf das Gerät.

Tab. 27: Bearbeiten der Tabelleneinträge

Wenn Sie die laufende Konfiguration verändern (z. B. einen Port ausschalten), ändert die grafische Benutzeroberfläche das „Laden/Speichern“-Symbol im Navigationsbaum von einem Diskettensymbol in ein gelbes Dreieck. Nach dem Speichern der Konfiguration zeigt die grafische Benutzeroberfläche das „Laden/Speichern“-Symbol wieder als Diskette an.

Anmerkung: Den Lieferzustand erhalten Sie mit `Neustart: Lieferzustand herstellen` (siehe Seite 47). Beachten Sie, dass das Gerät alle Tabellen, Einstellungen und Dateien auf dem Gerät und auf einem angeschlossenen ACA löscht.

1.6.4 Konfiguration speichern und laden

Bezeichnung	Bedeutung
Schreiben	Schreiben der Einstellung, welche Konfiguration als aktiv markiert ist, in den nicht-flüchtigen Speicher und auf den ACA.
Laden	Aktualisieren der Tabellenanzeige, falls sie durch einen anderen SNMP-Zugriff verändert wurde.
Speichern in NVM und ACA	Ersetzen der aktiven Konfiguration durch die laufende Konfiguration im nicht-flüchtigen Speicher und auf dem ACA
Laden vom NVM	Laden der aktiven Konfiguration aus dem nicht-flüchtigen Speicher.

Tab. 28: Speichern und Laden

1.6.5 Konfigurationsänderung widerrufen

Funktion

Ist die Funktion an und die Verbindung zum Gerät länger als die im Feld „Periode bis zum Widerruf bei Verbindungsunterbrechung [s]“ angegebene Zeit unterbrochen, dann lädt das Gerät die zuletzt gespeicherte Konfiguration.

☐ Schalten Sie die Funktion ein, bevor Sie das Gerät konfigurieren, damit Sie nach einer Fehlkonfiguration, die Ihre Verbindung zum Gerät unterbrochen hat, wieder Verbindung zum Gerät erhalten.

☐ Geben Sie die „Periode bis zum Widerruf bei Verbindungsunterbrechung [s]“ in Sekunden ein.
Mögliche Werte: 10-600 Sekunden.
Voreinstellung: 600 Sekunden.

Anmerkung: Schalten Sie die Funktion nach erfolgreicher Abspeicherung der Konfiguration aus. Das hilft Ihnen zu vermeiden, dass das Gerät die Konfiguration erneut lädt, nachdem Sie das Web-Interface schließen.

Anmerkung: Beachten Sie beim Zugriff auf das Gerät über ssh zusätzlich die TCP-Verbindungstimeouts für den Konfigurationswiderruf.

Watchdog IP-Adresse

„Watchdog IP-Adresse“ zeigt Ihnen die IP-Adresse des PCs an, von dem Sie die Funktion (Watchdog) aktiviert haben. Das Gerät überwacht die Verbindung zu dem PC mit dieser IP-Adresse auf Verbindungsunterbrechung.

1.7 Neustart

Dieser Dialog bietet Ihnen die Möglichkeit,

- einen Kaltstart des Gerätes auszulösen,
- die MAC-Adresstabelle zurückzusetzen,
- die ARP-Tabelle zurückzusetzen,
- die Firewall- und NAT-Verbindungen zurückzusetzen,
- die Portzähler zurückzusetzen,
- die Logdatei zu löschen,
- das Gerät in den Lieferzustand zurückzusetzen.

Name	Bedeutung
Kaltstart ...	Das Gerät lädt die Software neu aus dem nichtflüchtigen Speicher, startet neu und führt einen Selbsttest durch.
MAC-Adresstabelle zurücksetzen	Das Gerät setzt die Einträge mit dem Status „learned“ aus der Filtertabelle zurück.
ARP-Tabelle zurücksetzen	Das Gerät leert die ARP-Tabelle.
Firewall- und NAT-Verbindungen zurücksetzen	Das Gerät setzt die Zustandstabellen (siehe auf Seite 87 „Netzsicherheit“) zurück.
Portzähler zurücksetzen	Das Gerät setzt die Portzähler zurück.
Logdatei löschen	Das Gerät löscht die interne Logdatei (nicht persistente Logs).
Lieferzustand wiederherstellen	Das Gerät setzt alle Tabellen, Einstellungen und Dateien auf dem Gerät (und einem angeschlossenen ACA) in den Lieferzustand zurück.

Tab. 29: Neustart

Anmerkung: Während des Neustarts überträgt das Gerät kurzfristig keine Daten und ist nicht durch die grafische Benutzeroberfläche oder andere Management-Systeme wie z. B. Industrial HiVision erreichbar.

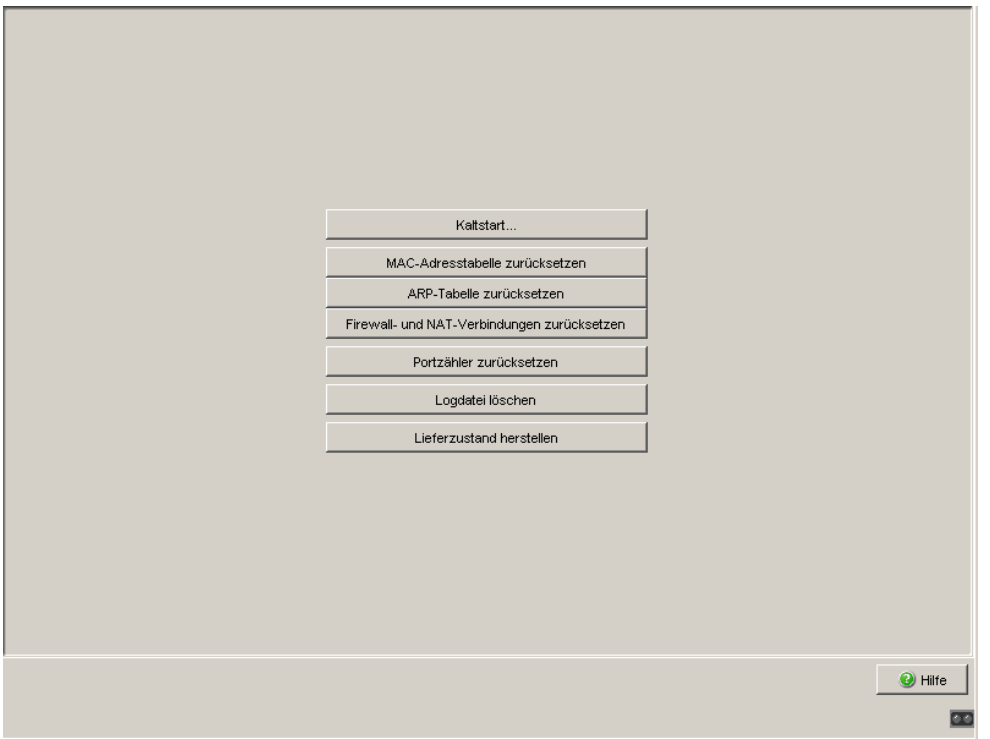


Abb. 13: Dialog Neustart

2 Sicherheit

Das Sicherheit-Menü enthält die Dialoge, Anzeigen und Tabellen zur Konfiguration der Sicherheitseinstellungen:

- Passwort
- SNMP-Zugriff
- Web-Zugriff
- SSH-Zugriff
- Externe Authentifizierung
- Login-Banner

2.1 Passwort

Dieser Dialog bietet Ihnen die Möglichkeit, das Lese- und das Schreib/Lese-Passwort für den Zugriff mit der grafischen Benutzeroberfläche (GUI), über das CLI und per SNMPv3 (SNMP-Version 3) auf dem Gerät zu ändern. Stellen Sie für das Lesepasswort und das Schreib-/Lesepasswort unterschiedliche Passwörter ein, damit ein Benutzer, der nur Lesezugriff hat (Benutzername „user“), das Passwort für den Schreib-/Lesezugriff (Benutzername „admin“) nicht kennen oder erraten kann.

Die grafische Benutzeroberfläche (GUI) kommuniziert über SNMPv3, das User Interface (CLI) über SSH.

Anmerkung: Passwörter unterscheiden Groß- und Kleinschreibung.

Anmerkung: Ändern Sie aus Sicherheitsgründen das Passwort des Lieferzustandes. Das hilft Ihnen, einen Zugriff auf das Gerät mit diesem Passwort zu verhindern. Ist das Passwort im Lieferzustand, dann zeigt das Gerät in allen Dialogen in der Kopfzeile „Standardpasswort“ an.

☐ Wählen Sie „Lesepasswort ändern (user)“, um das Lesepasswort einzugeben.
☐ Geben Sie das neue Lesepasswort in der Zeile „Neues Passwort“ ein und wiederholen Sie die Eingabe in der Zeile „Bitte nochmals eingeben“.
☐ Wählen Sie „Schreib-/Lesepasswort ändern (admin)“, um das Schreib-/Lesepasswort einzugeben.
☐ Geben Sie das Schreib-/Lesepasswort ein und wiederholen Sie die Eingabe.

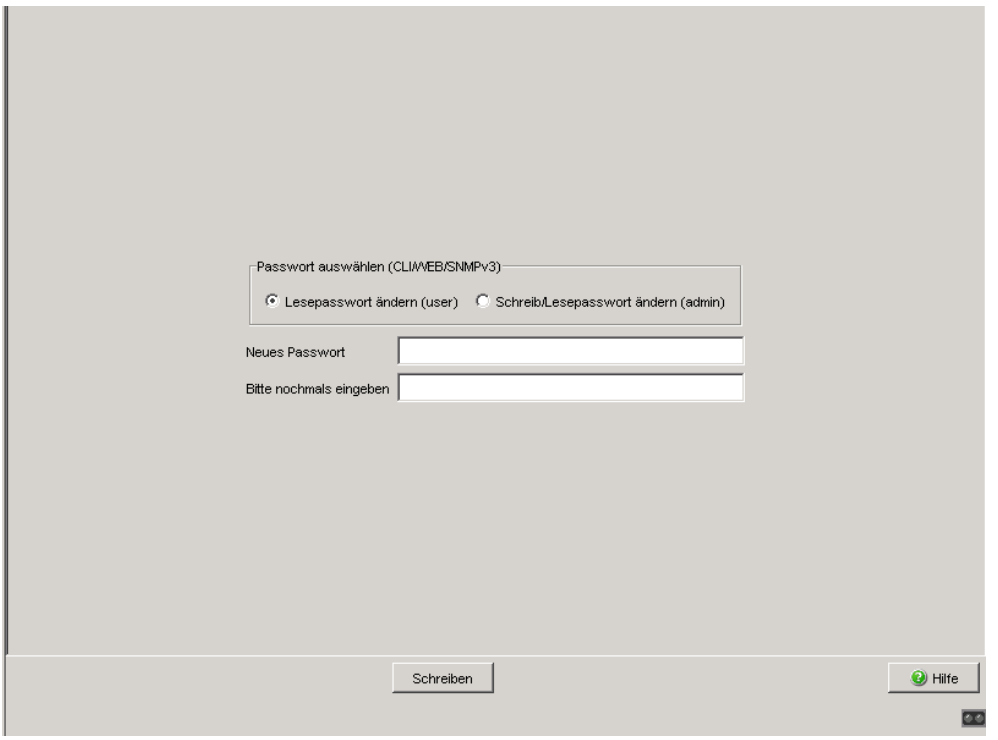


Abb. 14: Dialog Passwort

Anmerkung: Wenn Sie kein Passwort mit der Berechtigung „schreiben/lesen“ kennen, haben Sie keine Möglichkeit, auf das Gerät schreibend zuzugreifen.

Anmerkung: Aus Sicherheitsgründen zeigt der Dialog die Passwörter in Form von Sternen an. Notieren Sie sich jede Änderung. Ohne gültiges Passwort können Sie nicht auf das Gerät zugreifen.

Anmerkung: Verwenden Sie bei SNMP Version 3 für das Passwort 5 bis 32 Zeichen, da viele Anwendungen keine kürzeren Passwörter akzeptieren.

Die Sperre des Zugriffs über einen Web-Browser erfolgt in einem eigenen Dialog (siehe auf Seite 58 „Web-Zugriff“).

2.2 SNMP-Zugriff

Dieser Dialog bietet Ihnen die Möglichkeit,

- einen SNMP-Port einzugeben. Im Lieferzustand ist der Port 161 eingetragen.
  Tragen Sie eine andere UDP-Portnummer ein, wenn Sie zur Administration des Gerätes oder aus Sicherheitsgründen eine andere Portnummer verwenden möchten. Die grafische Benutzeroberfläche verwendet nach einem Neustart automatisch die neue Portnummer.
- Einträge für den Zugriff über SNMP auf das Gerät zu verwalten, zu erzeugen und zu löschen. Klicken Sie auf „↑“ oder „↓“, um einen selektierten Eintrag nach oben oder unten zu verschieben.
- die SNMP-Zugriffe der grafischen Benutzeroberfläche auf das Gerät durch HTTPS zu tunneln. Damit sind ausschließlich HTTPS-Verbindungen zum Gerät notwendig. Sie können mit dieser Funktion auch eine RADIUS-Authentifizierung für SNMP-Benutzer durchführen.
  Im Lieferzustand ist die Funktion SNMP über HTTPS (Tunnel) inaktiv.

Anmerkung: Der Browser übernimmt eine Änderung der Einstellung SNMP über HTTPS (Tunnel) erst nach dem Neuladen der grafischen Benutzeroberfläche. Der Zugriff über SNMP bleibt weiterhin möglich.

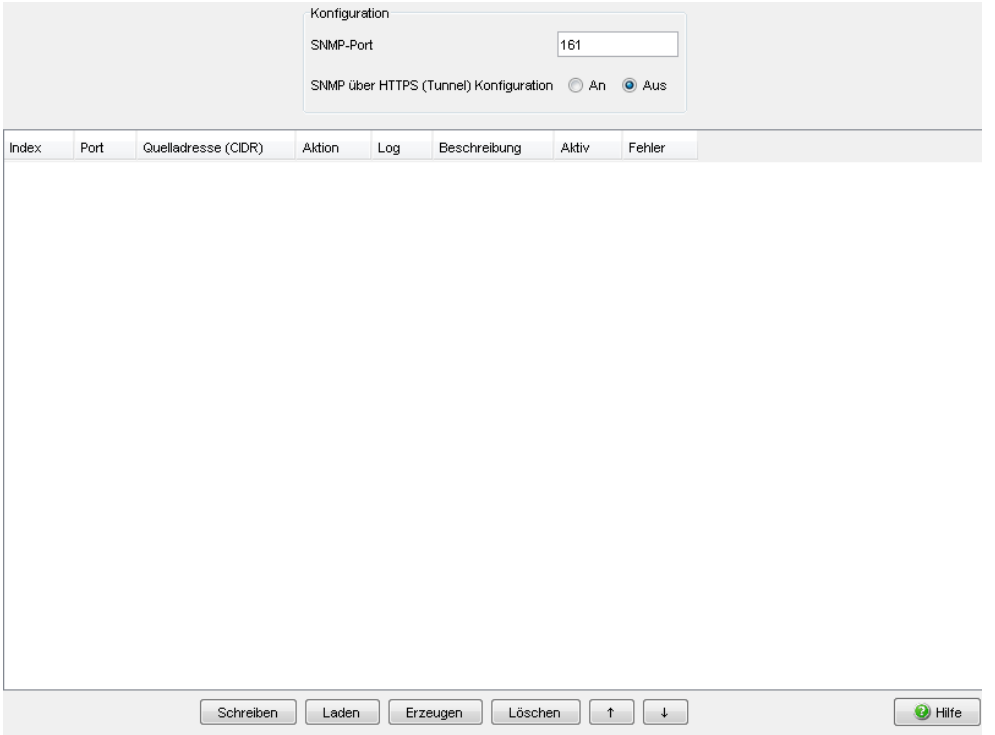


Abb. 15: Dialog SNMP-Zugriff

Parameter	Bedeutung	Mögliche Werte
Index	Laufende Nummer, auf die sich die Zugriffsbeschränkung bezieht	(Automatisch erzeugt, ab 1)
Port	Port auswählen.	`int` - Einstellungen beziehen sich auf den internen Port `ext` - Einstellungen beziehen sich auf den externen Port `ppp` - Einstellungen beziehen sich auf den als Modem konfigurierten V.24-Port.
Quelladresse (CIDR)	Eintragen einer IP-Adresse oder einer Gruppe von IP-Adressen in Maskenschreibweise, die Zugriff auf das Gerät haben oder von „any“. Beim Eintragen einer IP-Adresse ohne Maske ändert das Gerät die Schreibweise der IP-Adresse in die Maskenschreibweise mit 32 Bit langer Netzmaske (x.x.x.x in x.x.x.x/32).	Beliebige IP-Adresse in Maskenschreibweise. Dies ist die IP-Adresse oder die Gruppe von IP-Adressen, die auf das Gerät zugreifen darf. any - Der Zugriff von Rechnern mit beliebigen IP-Adressen auf dieses Gerät ist erlaubt.
Aktion	Aktion des Gerätes auswählen, wenn von (einer) der unter „Quelladresse (CIDR)“ angegebenen IP-Adresse auf das Gerät zugegriffen wird.	accept - Zugriff erlaubt drop - Zugriff nicht erlaubt, keine Mitteilung an den Absender reject - Zugriff nicht erlaubt, Mitteilung an den Absender
Log	Wenn die Regeln eines Tabelleneintrages vom Gerät angewendet wurden, schreibt das Gerät dies als Ereignis in den Ereignis-Log (siehe auf Seite 170 „Ereignis-Log“). **Anmerkung:** Die Einstellung `logAndTrap` kann große Mengen an Trap-Datenverkehr erzeugen. Dies gilt besonders dann, wenn das Senden des Traps wieder einen Match der Firewall-Regel auslöst (z.B. wenn der Trap-Host ist nicht erreichbar ist und ein Router mit einer ICMP-Nachricht antwortet).	enable, disable, logAndTrap
Beschreibung	Frei wählbare Beschreibung dieses Eintrags eingeben, z.B. Name oder Standort des PCs, der die eingetragene IP-Adresse hat.	Maximal 128 Zeichen
Aktiv	Tabelleneintrag aktivieren/deaktivieren	ein/aus
Fehler	Zeigt den letzten erkannten Fehler bei einem Versuch, den Tabelleneintrag zu aktivieren (typischerweise ein erkannter Syntaxfehler).	-

Tab. 30: Zugriffstabelle SNMP

- Mit „Erzeugen“ erzeugen Sie eine neue Zeile in der Tabelle.

- Mit „Löschen“ löschen Sie die ausgewählten Zeilen aus der Tabelle.

Anmerkung: Ist keine Zeile angekreuzt, dann gibt es
– am internen Port keine Zugriffsbeschränkungen
– am externen Port keine Zugriffsmöglichkeit über SNMP.

Anmerkung: Im Lieferzustand erlaubt die Firewall am internen Port den ausgehenden IP-Verkehr sowie den Management-Zugriff (SNMP, HTTPS und SSH) auf das Gerät. Wenn Sie den Management-Zugriff deaktivieren möchten, haben Sie folgende Möglichkeiten:

- Definieren Sie explizite `drop`-Regeln für den Management-Zugriff.
- Ändern Sie die entsprechenden Firewall-Regeln für den ausgehenden IP-Verkehr.

Anmerkung: Die Firewall unterstützt bis zu 1024 IP-Regeln.
Im Dialog `Diagnose:IP-Firewall-Liste` finden Sie die Zusammenfassung der aktiven Regeln.

2.3 SNMPv1/v2

Dieser Dialog bietet Ihnen die Möglichkeit,

- den Zugriff über SNMPv1 oder SNMPv2 auszuwählen. Im Lieferzustand sind beide Protokolle deaktiviert, der SNMP-Zugriff ist aus Sicherheitsgründen damit ausschließlich über SNMPv3 möglich.
- das Lese- und das Schreib/Lese-Passwort für den Zugriff mit SNMPv1/v2 auf dem Gerät zu ändern. Beachten Sie die Groß-/Kleinschreibung. Wählen Sie aus Sicherheitsgründen unterschiedliche Passwörter für den Lese- und Schreib-/Lesezugriff.

Anmerkung: Im Lieferzustand ist der SNMPv1- und der SNMPv2-Zugriff ausgeschaltet. Da SNMPv1 und SNMPv2 die Daten unverschlüsselt übertragen, stellt die Verwendung von SNMPv1 und SNMPv2 ein potentielles Sicherheitsrisiko dar. Lassen Sie den SNMPv1- oder SNMPv2-Zugriff ausschließlich dann zu, wenn Sie eine Anwendung, die dies erfordert, einsetzen wollen.

Anmerkung: Ändern Sie aus Sicherheitsgründen das Passwort des Lieferzustandes. Das hilft Ihnen, einen Zugriff auf das Gerät mit diesem Passwort zu verhindern. Ist das Passwort im Lieferzustand, dann zeigt das Gerät in allen Dialogen in der Kopfzeile „Standardpasswort“ an.

☐ Wählen Sie „Lesepasswort ändern (user)“, um das Lesepasswort einzugeben.
☐ Geben Sie das neue Lesepasswort in der Zeile „Neues Passwort“ ein und wiederholen Sie die Eingabe in der Zeile „Bitte nochmals eingeben“.
☐ Wählen Sie „Schreib-/Lesepasswort ändern (admin)“, um das Schreib-/Lesepasswort einzugeben.
☐ Geben Sie das Schreib-/Lesepasswort ein und wiederholen Sie die Eingabe.

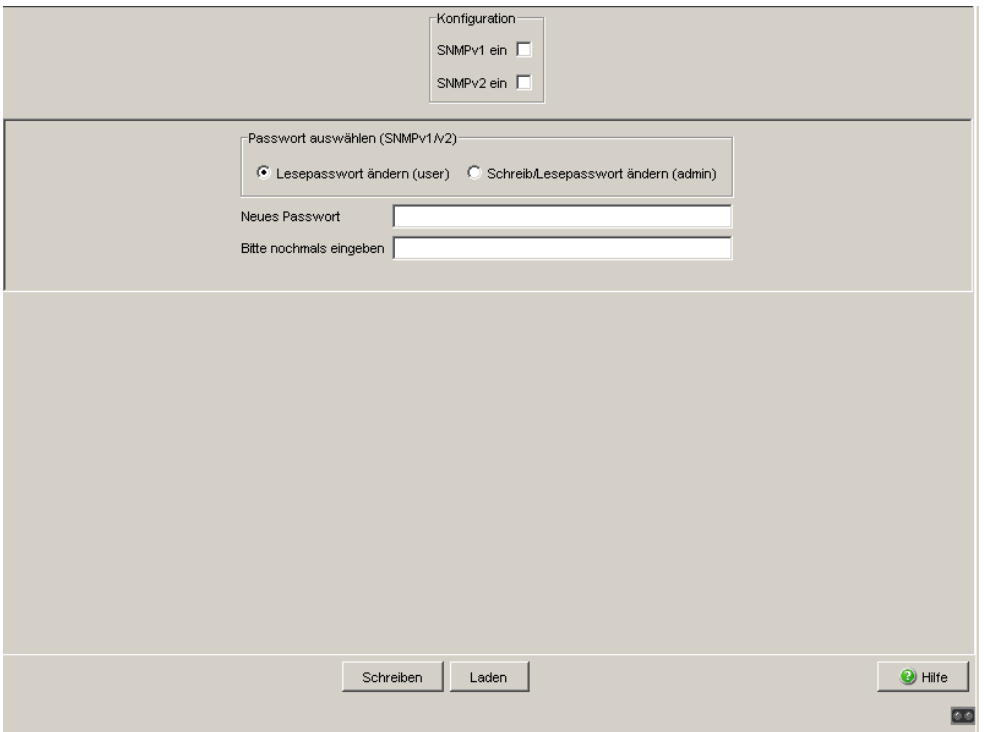


Abb. 16: Dialog SNMPv1/v2

Anmerkung: Aus Sicherheitsgründen zeigt der Dialog die Passwörter in Form von Sternen an. Notieren Sie sich jede Änderung. Ohne gültiges Passwort können Sie nicht auf das Gerät zugreifen.

Die Sperre des Zugriffs über einen Web-Browser erfolgt in einem eigenen Dialog (siehe auf Seite 58 „Web-Zugriff“).

2.4 Web-Zugriff

Dieser Dialog bietet Ihnen die Möglichkeit,

- den Web-Server auf dem Gerät ein-/auszuschalten. Im Lieferzustand ist der Web-Server auf dem internen Port eingeschaltet.
  Der Web-Server des Gerätes bietet Ihnen die Möglichkeit, das Gerät mit Hilfe der grafischen Benutzeroberfläche zu konfigurieren. Das Deaktivieren des Web-Servers hilft Ihnen, einen Web-Zugriff auf das Gerät zu verhindern.
- einen HTTPS-Port (TCP-Port-Nummer, die das Gerät für den Web-Server verwendet) einzugeben.
  Mögliche Werte: 1 - 65.535. Voreinstellung: Well Known Port 443 = HTTPS. Mit einem Neustart des Gerätes ist die Portänderung wirksam. Ergänzen Sie bei einer Portänderung für einen Zugriff auf das Gerät den URL um die Portnummer , z. B. https://192.168.1.1:444.
- Einträge für den Zugriff über der grafischen Benutzeroberfläche auf das Gerät zu verwalten, zu erzeugen und zu löschen,
- Zertifikate auf das Gerät zu laden.
  Im Lieferzustand bietet Ihnen das Gerät ein Zertifikat.

Nach dem Abschalten des Web-Servers ist ein erneutes Anmelden über einen Web-Browser nicht mehr möglich. Die Anmeldung im offenen Browserfenster bleibt aktiv.

Anmerkung: Die grafische Benutzeroberfläche kommuniziert über SNMP mit dem Gerät. Wenn Sie über den externen Port auf die grafische Benutzeroberfläche zugreifen wollen und SNMP über HTTPS (Tunnel) inaktiv ist, dann erstellen Sie eine SNMP-Zugriffsregel (siehe auf Seite 52 „SNMP-Zugriff“).

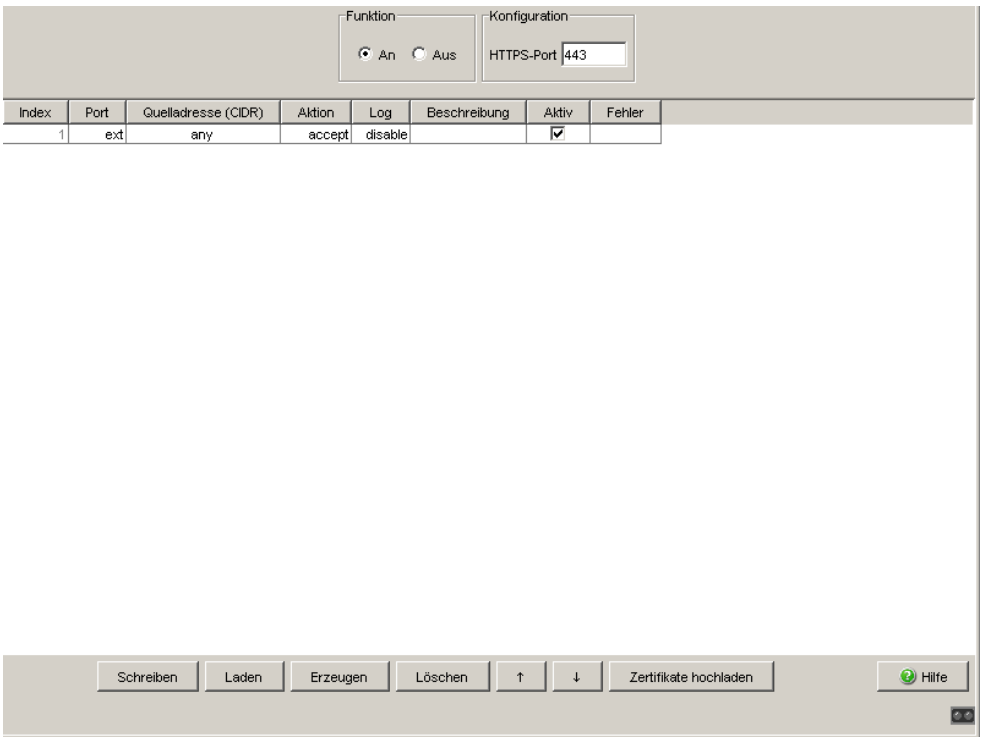


Abb. 17: Dialog Web-Zugriff

Parameter	Bedeutung	Mögliche Werte
Index	Laufende Nummer, auf die sich die Zugriffsbeschränkung bezieht	(Automatisch erzeugt, ab 1)
Port	Port auswählen.	`int` - Einstellungen beziehen sich auf den internen Port `ext` - Einstellungen beziehen sich auf den externen Port `ppp` - Einstellungen beziehen sich auf den als Modem konfigurierten V.24-Port.
Quelladresse (CIDR)	Eintragen einer IP-Adresse oder einer Gruppe von IP-Adressen in Maskenschreibweise, die Zugriff auf das Gerät haben oder von „any“. Beim Eintragen einer IP-Adresse ohne Maske ändert das Gerät die Schreibweise der IP-Adresse in die Maskenschreibweise mit 32 Bit langer Netzmaske (x.x.x.x in x.x.x.x/32).	Beliebige IP-Adresse in Maskenschreibweise. Dies ist die IP-Adresse oder die Gruppe von IP-Adressen, die auf das Gerät zugreifen darf. any - Der Zugriff von Rechnern mit beliebigen IP-Adressen auf dieses Gerät ist erlaubt.
Aktion	Aktion des Gerätes auswählen, wenn von (einer) der unter „Quelladresse (CIDR)“ angegebenen IP-Adresse auf das Gerät zugegriffen wird.	accept - Zugriff erlaubt drop - Zugriff nicht erlaubt, keine Mitteilung an den Absender reject - Zugriff nicht erlaubt, Mitteilung an den Absender
Log	Wenn die Regeln eines Tabelleneintrages vom Gerät angewendet wurden, schreibt das Gerät dies als Ereignis in den Ereignis-Log (siehe auf Seite 170 „Ereignis-Log“). **Anmerkung:** Die Einstellung `logAndTrap` kann große Mengen an Trap-Datenverkehr erzeugen. Dies gilt besonders dann, wenn das Senden des Traps wieder einen Match der Firewall-Regel auslöst (z.B. wenn der Trap-Host ist nicht erreichbar ist und ein Router mit einer ICMP-Nachricht antwortet).	enable, disable, logAndTrap
Beschreibung	Frei wählbare Beschreibung dieses Eintrags eingeben, z.B. Name oder Standort des PCs, der die eingetragene IP-Adresse hat.	Maximal 128 Zeichen
Aktiv	Tabelleneintrag aktivieren/deaktivieren	ein/aus
Fehler	Zeigt den letzten erkannten Fehler bei einem Versuch, den Tabelleneintrag zu aktivieren (typischerweise ein erkannter Syntaxfehler).	-

Tab. 31: Zugriffstabelle Web

▶ Mit „Eintrag erzeugen“ erzeugen Sie eine neue Zeile in der Tabelle. Das

Gerät zeigt einen Dialog an, um Sie zu erinnern, gegebenenfalls eine zusätzliche SNMP-Regel anzulegen, wenn Sie die grafische Benutzeroberfläche verwenden möchten.

- Mit „Eintrag löschen“ löschen Sie die ausgewählten Zeilen aus der Tabelle.
- Mit „↑“ oder „↓“, verschieben Sie einen selektierten Eintrag nach oben oder unten.

Für das Hochladen eines Zertifikates muss sich die Datei auf einem Laufwerk befinden, das Sie über Ihren PC erreichen.

☐ Klicken Sie auf „Zertifikate“.
☐ Klicken Sie im Datei-Auswahl-Rahmen auf „...“.
☐ Wählen Sie im Datei-Auswahl-Fenster die Zertifikatdatei (z.B. zertifikat.p12) aus und klicken Sie auf „Öffnen“.
☐ Klicken Sie auf „Kopieren vom PC“, um die Datei auf das Gerät zu übertragen.

Das Ende der Upload-Aktion wird durch eine der folgenden Meldungen angezeigt:

- Upload erfolgreich beendet.
- Upload fehlgeschlagen, Ursache: Kopieren fehlgeschlagen.

Anmerkung: Im Lieferzustand erlaubt die Firewall am internen Port den ausgehenden IP-Verkehr sowie den Management-Zugriff (SNMP, HTTPS und SSH) auf das Gerät. Wenn Sie den Management-Zugriff deaktivieren möchten, haben Sie folgende Möglichkeiten:

- Definieren Sie explizite `drop`-Regeln für den Management-Zugriff.
- Ändern Sie die entsprechenden Firewall-Regeln für den ausgehenden IP-Verkehr.

Anmerkung: Das Gerät akzeptiert HTTPS-Server-Zertifikate mit einer Schlüssellänge zwischen 512 und 2048 Bits (RSA-Schlüssel im PEM-Format mit nicht-verschlüsseltem privatem Schlüssel).
Vom Server unterstützte Verschlüsselungs-Algorithmen:

- SSLv3: AES128-SHA
- TLSv1: AES256-SHA AES128-SHA DES-CBC3-SHA

Anmerkung: Die Firewall unterstützt bis zu 1024 IP-Regeln.
Im Dialog `Diagnose:IP-Firewall-Liste` finden Sie die Zusammenfassung der aktiven Regeln.

2.5 SSH-Zugriff

Dieser Dialog bietet Ihnen die Möglichkeit,

- den SSH-Server auf dem Gerät ein-/auszuschalten. Im Lieferzustand ist der SSH-Server auf dem internen Port eingeschaltet.
  Der SSH-Server des Gerätes bietet Ihnen die Möglichkeit, das Gerät mit Hilfe des Command Line Interfaces (in-band) zu konfigurieren. Das Deaktivieren des SSH-Servers hilft Ihnen, einen SSH-Zugriff auf das Gerät zu verhindern.
- einen SSH-Port einzugeben. Mögliche Werte sind 1 - 65.535. Im Lieferzustand ist der Port 22 eingestellt.
- den DSA- und RSA-Fingerprint einzusehen. Die Fingerprints dienen zur Identifizierung des bei der Anmeldung verwendeten Schlüssels.
- Einträge für den Zugriff über SSH auf das Gerät zu verwalten, zu erzeugen und zu löschen.

Nach dem Abschalten des SSH-Servers ist ein erneuter Zugriff auf das Gerät über eine neue SSH-Verbindung nicht mehr möglich. Eine bestehende SSH-Verbindung bleibt erhalten.

Anmerkung: Das Command Line Interface (out-of-band) und der Dialog `Sicherheit:Web-Zugriff` in der grafischen Benutzeroberfläche (oder ein anderes SNMP-Administrierungswerkzeug) bietet Ihnen die Möglichkeit, den SSH-Server wieder zu aktivieren.

Anmerkung: Das Gerät bietet Ihnen die Möglichkeit, per SFTP auf Geräte-Dateien wie Konfigurationsdateien oder den ACA zuzugreifen, ein Firmware-Update oder VPN-Zertifikate auf das Gerät zu laden. Verwenden Sie dazu einen SFTP-Client, z. B. WinSCP. Für den SFTP-Zugriff ist der SSH-Zugriff auf das Gerät erforderlich.

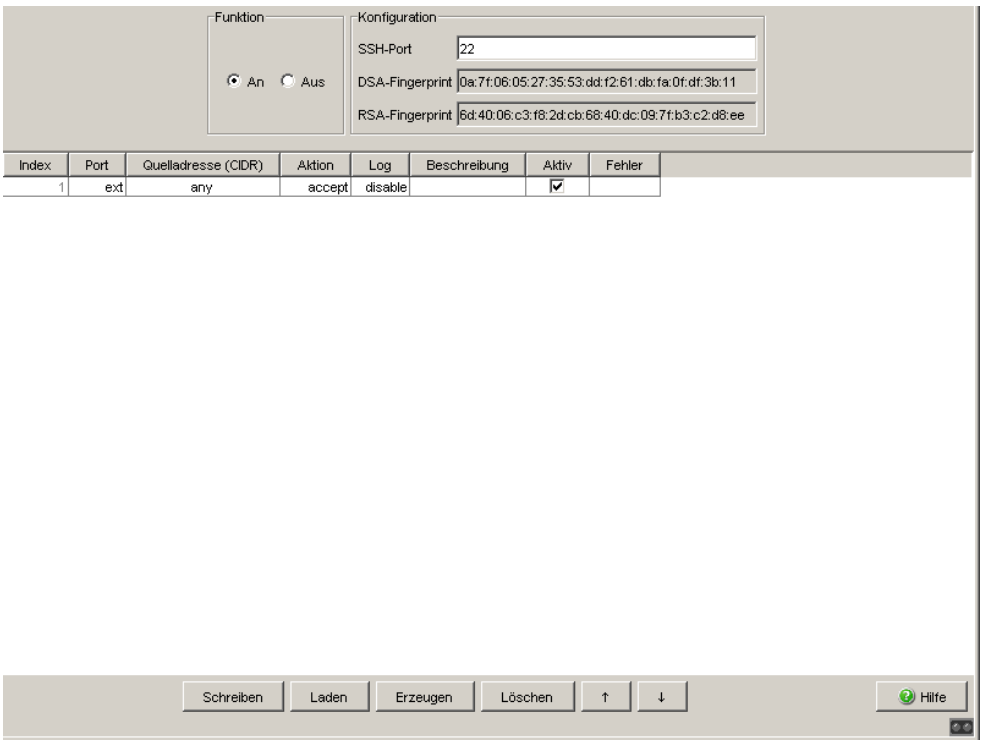


Abb. 18: Dialog SSH-Zugriff

Parameter	Bedeutung	Mögliche Werte
Index	Laufende Nummer, auf die sich die Zugriffs-beschränkung bezieht	(Automatisch erzeugt, ab 1)
Port	Port auswählen.	`int` - Einstellungen beziehen sich auf den internen Port `ext` - Einstellungen beziehen sich auf den externen Port `ppp` - Einstellungen beziehen sich auf den als Modem konfi-gurierten V.24-Port.
Quelladresse (CIDR)	Eintragen einer IP-Adresse oder einer Gruppe von IP-Adressen in Maskenschreib-weise, die Zugriff auf das Gerät haben oder von „any“. Beim Eintragen einer IP-Adresse ohne Maske ändert das Gerät die Schreibweise der IP-Adresse in die Maskenschreibweise mit 32 Bit langer Netzmaske (x.x.x.x in x.x.x.x/32).	Beliebige IP-Adresse in Maskenschreibweise. Dies ist die IP-Adresse oder die Gruppe von IP-Adressen, die auf das Gerät zugreifen darf. any - Der Zugriff von Rechnern mit beliebigen IP-Adressen auf dieses Gerät ist erlaubt.
Aktion	Aktion des Gerätes auswählen, wenn von (einer) der unter „Quelladresse (CIDR)“ angegebenen IP-Adresse auf das Gerät zugegriffen wird.	accept - Zugriff erlaubt drop - Zugriff nicht erlaubt, keine Mitteilung an den Absender reject - Zugriff nicht erlaubt, Mitteilung an den Absender
Log	Wenn die Regeln eines Tabelleneintrages vom Gerät angewendet wurden, schreibt das Gerät dies als Ereignis in den Ereignis-Log (siehe auf Seite 170 „Ereignis-Log“). **Anmerkung:** Die Einstellung `logAndTrap` kann große Mengen an Trap-Datenverkehr erzeugen. Dies gilt besonders dann, wenn das Senden des Traps wieder einen Match der Firewall-Regel auslöst (z.B. wenn der Trap-Host ist nicht erreichbar ist und ein Router mit einer ICMP-Nachricht antwortet).	enable, disable, logAndTrap
Beschreibung	Frei wählbare Beschreibung dieses Eintrags eingeben, z.B. Name oder Standort des PCs, der die eingetragene IP-Adresse hat.	Maximal 128 Zeichen
Aktiv	Tabelleneintrag aktivieren/deaktivieren	ein/aus
Fehler	Zeigt den letzten erkannten Fehler bei einem Versuch, den Tabelleneintrag zu aktivieren (typischerweise ein erkannter Syntaxfehler).	-

Tab. 32: Zugriffstabelle SSH

▶ Mit „Erzeugen“ erzeugen Sie eine neue Zeile in der Tabelle.

- Mit „Löschen“ löschen Sie die ausgewählten Zeilen aus der Tabelle.

Anmerkung: Im Lieferzustand erlaubt die Firewall am internen Port den ausgehenden IP-Verkehr sowie den Management-Zugriff (SNMP, HTTPS und SSH) auf das Gerät. Wenn Sie den Management-Zugriff deaktivieren möchten, haben Sie folgende Möglichkeiten:

- Definieren Sie explizite `drop`-Regeln für den Management-Zugriff.
- Ändern Sie die entsprechenden Firewall-Regeln für den ausgehenden IP-Verkehr.

Anmerkung: Das Deaktivieren eines Eintrags hilft Ihnen, das erneute Anmelden über SSH zu verhindern. Eine bereits bestehende SSH-Verbindung, auf die die Kriterien der Deaktivierung zutreffen, bleibt jedoch bis zur Abmeldung bestehen.

Anmerkung: Die Firewall unterstützt bis zu 1024 IP-Regeln.
Im Dialog `Diagnose:IP-Firewall-Liste` finden Sie die Zusammenfassung der aktiven Regeln.

2.6 Externe Authentifizierung

Dieser Dialog bietet Ihnen die Möglichkeit, bis zu 5 Benutzer-Firewall-Konten anzulegen.
Mit dem Kontonamen und dem zugehörigen Passwort kann sich ein Benutzer im Anmeldefenster unter dem Login-Typ „Benutzer-Firewall“ auf dem Gerät anmelden (siehe auf Seite 11 „Grafische Benutzeroberfläche“).
Für jedes Benutzer-Firewall-Konto ist in einer Authentifizierungsliste hinterlegt, nach welchen Methoden das Gerät das Konto bei der Anmeldung authentifiziert.
Ein Benutzer-Firewall-Konto ist Voraussetzung, um im Dialog `Netzsicherheit:Benutzer-Firewall-Einträge` (siehe Seite 136) einen Eintrag anlegen zu können.

2.6.1 Benutzer-Firewall-Konten

Dieser Dialog bietet Ihnen die Möglichkeit, Benutzer, die sich unter dem Login-Typ „Benutzer-Firewall“ (siehe Seite 11) auf dem Gerät anmelden können, neu anzulegen, zu konfigurieren und zu löschen.

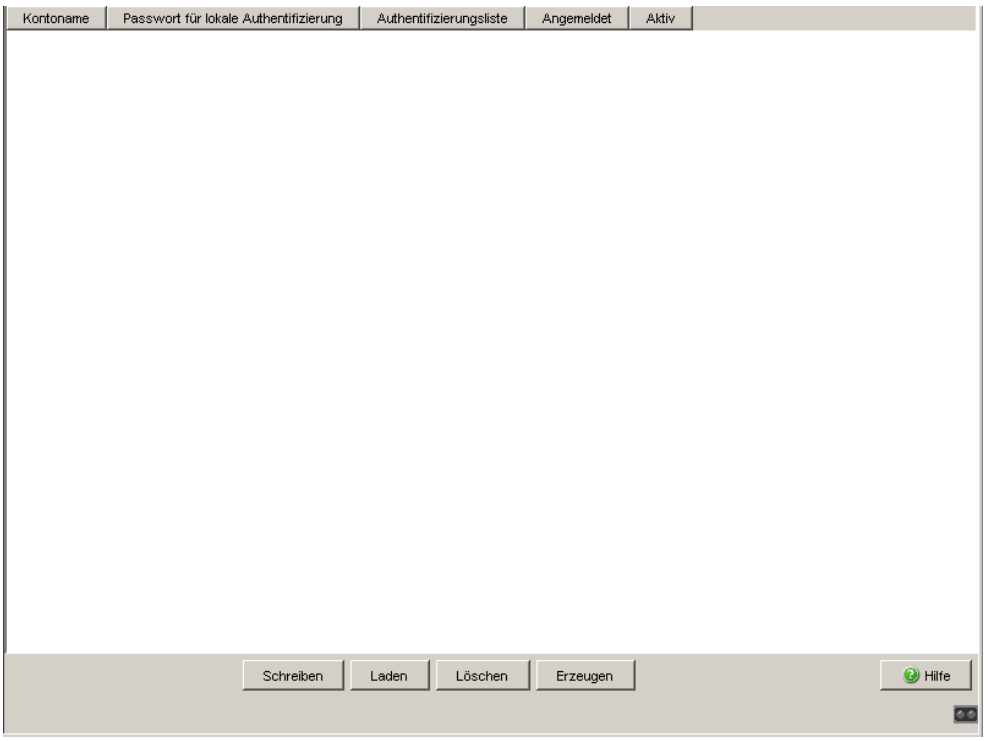


Abb. 19: Dialog Benutzer-Firewall-Konten

Parameter	Bedeutung	Mögliche Werte
Kontoname	Eingeben des Namens eines Benutzers (Kontoname), der sich im Anmeldefenster unter dem Login-Typ „Benutzer-Firewall“ anmelden kann.	1-128 ASCII-Zeichen
Passwort für lokale Authentifizierung	Eingeben des Passworts dieses Benutzers .	Maximal 5-32 Zeichen
Authentifizierungsliste	Auswählen einer Authentifizierungsliste (siehe auf Seite 69 „Authentifizierungslisten“)	- userFirewallLoginDefaultList, - systemLoginDefaultList , - Listen, die Sie unter `Sicherheit:Externe Authentifizierung:Authentifizierungslisten` (siehe Seite 69) angelegt haben.
Angemeldet	Anzeige, ob dieser Benutzer an der Benutzer-Firewall angemeldet ist. Ist dieser Benutzer angemeldet, dann hat der Administrator durch Klicken auf den Haken und auf „Schreiben“ die Möglichkeit, ihn von der Benutzer-Firewall abzumelden.	ein/aus
Aktiv	Tabelleneintrag aktivieren/deaktivieren	ein/aus

Tab. 33: Zugriffstabelle Benutzer

- Mit „Erzeugen“ erzeugen Sie eine neue Zeile in der Tabelle.
- Mit „Löschen“ löschen Sie die ausgewählten Zeilen aus der Tabelle.

2.6.2 Authentifizierungslisten

Dieser Dialog bietet Ihnen die Möglichkeit, Authentifizierungslisten neu anzulegen, zu konfigurieren und zu löschen.
In einer Authentifizierungsliste legen Sie fest,

- welche Authentifizierungsmethoden das Gerät beim Anmelden eines Benutzers, dem diese Authentifizierungsliste zugeordnet ist, anwendet.
- in welcher Reihenfolge das Gerät diese Authentifizierungsmethoden nacheinander anwendet.

Im Lieferzustand bietet Ihnen dieser Dialog bereits die Authentifzierungslisten „userFirewallLoginDefaultList“ und „systemLoginDefaultList“ zur Erleichterung der Konfiguration.

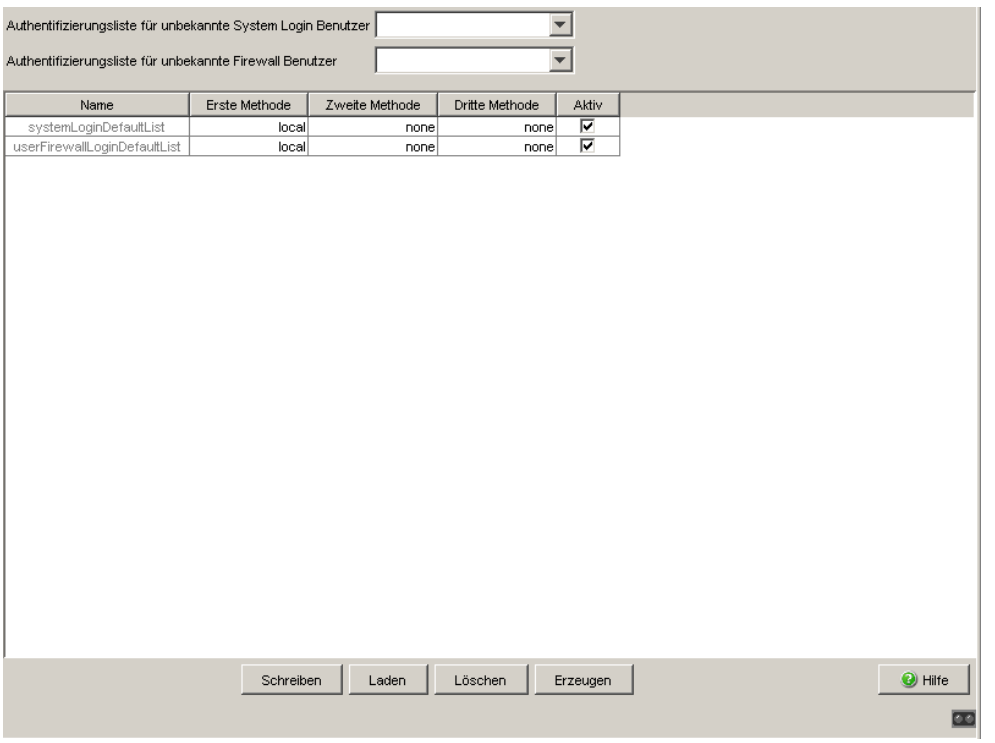


Abb. 20: Authentifizierungslisten

Bei „Authentifizierungsliste für unbekannte System-Login-Benutzer“ wählen Sie bei Bedarf eine der Authentifizierungslisten aus, die das Gerät beim Administrations-Zugriff eines unbekannten Benutzers anwenden soll. Keine Auswahl hat zur Folge, dass ein unbekannter Benutzer keinen Administrations-Zugriff auf das Gerät hat.

Bei „Authentifizierungsliste für unbekannte Firewall-Benutzer“ wählen Sie bei Bedarf eine der Authentifizierungslisten aus, die das Gerät beim Benutzer-Firewall-Zugriff eines unbekannten Benutzers anwenden soll. Keine Auswahl hat zur Folge, dass ein unbekannter Benutzer keinen Benutzer-Firewall-Zugriff auf das Gerät hat.

Parameter	Bedeutung	Mögliche Werte
Name	Name der Authentifzierungsliste. „userFirewallLoginDefaultList“ und „systemLoginDefaultList“ sind im Liefer-zustand bereits angelegt.	Beliebige ASCII-Zeichen
Erste Methode	Festlegen der Authentifizierungsmethode, die das Gerät zuerst anwendet.	`none` - Zugriff auf das Gerät ohne Authentifizierung `local` - Authentifizierung von Benutzer und Password durch das Gerät `radius` - Authentifizierung von Benutzer und Passwort durch RADIUS-Server `deny` - Authentifizierung ablehnen
Zweite Methode	Festlegen der Authentifizierungsmethode, die das Gerät anwendet, wenn die erste Authentifizierungsmethode nicht zum Erfolg führte.	`none` - Zugriff auf das Gerät ohne Authentifizierung `local` - Authentifizierung von Benutzer und Password durch das Gerät `radius` - Authentifizierung von Benutzer und Passwort durch RADIUS-Server `deny` - Authentifizierung ablehnen
Dritte Methode	Festlegen der Authentifizierungsmethode, die das Gerät anwendet, wenn die erste und zweite Authentifizierungsmethode nicht zum Erfolg führte.	`none` - Zugriff auf das Gerät ohne Authentifizierung `local` - Authentifizierung von Benutzer und Password durch das Gerät `radius` - Authentifizierung von Benutzer und Passwort durch RADIUS-Server `deny` - Authentifizierung ablehnen
Aktiv	Tabelleneintrag aktivieren/deaktivieren	ein/aus

Tab. 34: Authentifzierungslisten

- Mit „Erzeugen“ erzeugen Sie eine neue Zeile in der Tabelle.
- Mit „Löschen“ löschen Sie die ausgewählten Zeilen aus der Tabelle.

2.6.3 RADIUS-Server

RADIUS (Remote Authentication Dial-In User Service) ist ein Client-Server-Protokoll für die zentrale Authentifizierung von Benutzern und Endgeräten (AAA-System).

Dieser Dialog bietet Ihnen die Möglichkeit, die Daten für 1 bis 3 RADIUS-Server einzugeben.
Ist in `Externe Authentifizierung:Authentifizierungslisten` „radius“ als Authentifizierungsmethode gewählt, kontaktiert das Gerät bei Authentifizierungsanfragen nacheinander die eingetragenen RADIUS-Server.

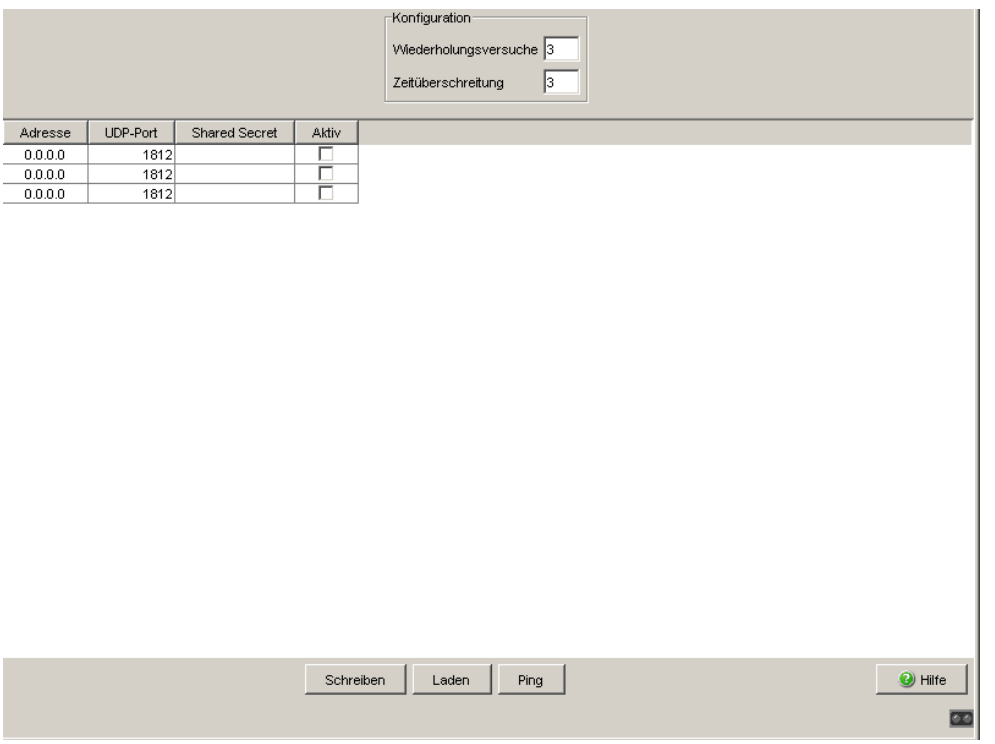


Abb. 21: Dialog RADIUS-Server

Parameter	Bedeutung	Mögliche Werte
Wiederholungs-versuche	Eingeben, wie oft das Gerät eine unbeant-wortete Anforderung an den RADIUS-Server wiederholt, bevor das Gerät die Anforderung an einen anderen RADIUS-Server schickt.	1 bis 15
Zeitüberschrei-tung	Eingeben, wie lange (in Sekunden) das Gerät nach einer Anforderung an den RADIUS-Server auf eine Antwort wartet, bevor es die Anforderung erneut schickt.	1-30
Tabelle		
Adresse	Eingeben der IP-Adresse eines RADIUS-Servers	
UDP-Port	Eingeben des UDP-Ports des RADIUS-Servers.	1-65.535 (Voreinstellung 1.812)
Shared Secret	Eingeben der Zeichenfolge, die Sie vom Administrator Ihres RADIUS-Servers als Schlüssel erhalten.	Maximal 20 Zeichen
Aktiv	Tabelleneintrag aktivieren/deaktivieren	ein/aus

Tab. 35: RADIUS-Server

2.7 Login-Banner

Dieser Dialog bietet Ihnen die Möglichkeit, ein Login-Banner einzugeben. Das Gerät gibt das Login-Banner aus, wenn sich ein Benutzer in die Benutzerschnittstelle (grafische Benutzeroberfläche oder CLI) einloggt. Das Login-Banner kann bis zu 255 Zeichen lang sein. Erlaubt sind die Zeichen im Bereich ASCII-Code 0x20 (Leerzeichen, „ “) bis ASCII-Code 0x7E (Tilde, „~“) mit Ausnahme des Prozent-Zeichens (%, 0x25).

3 Zeit

3.1 Grundeinstellungen

Dieser Dialog bietet Ihnen die Möglichkeit, allgemeine zeitbezogene Einstellungen vorzunehmen.

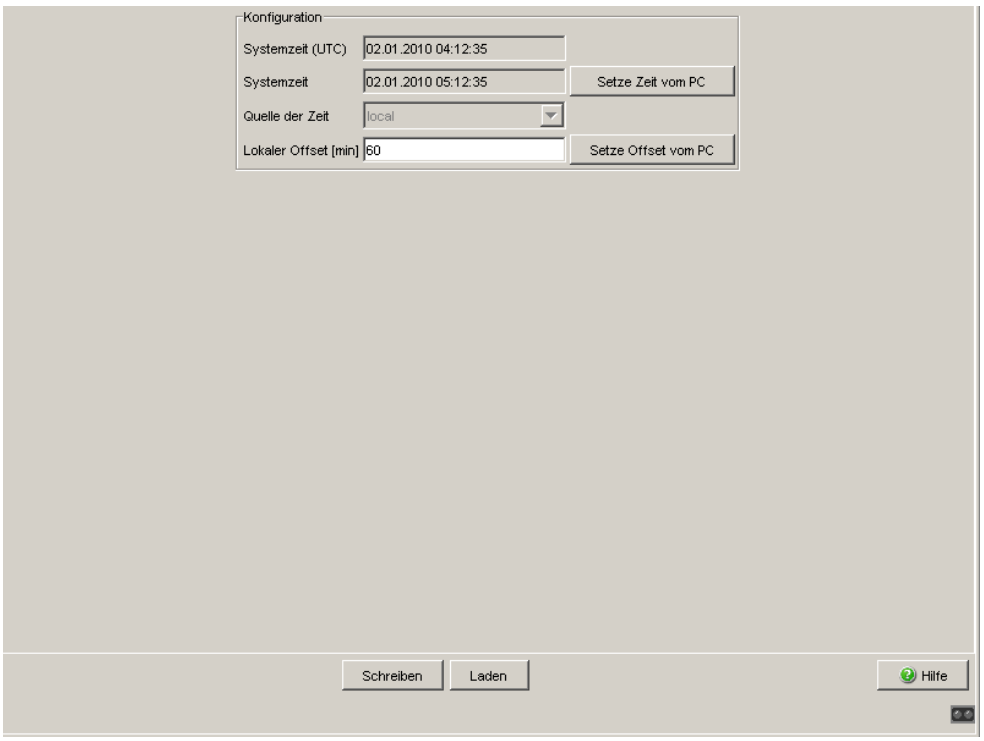


Abb. 22: Dialog Zeit:Grundeinstellungen

- Die „Systemzeit (UTC)" zeigt die Uhrzeit bezogen auf die koordinierte Weltzeitskala UTC (Universal Time Coordinated) an.
  Die Anzeige ist weltweit gleich. Lokale Zeitverschiebungen bleiben unberücksichtigt.
  Mögliche Quellen der Systemzeit (UTC) sind: `local`, `sntp` und `ntp`, siehe „Quelle der Zeit“.

- Die „Systemzeit" berechnet das Gerät aus der „Systemzeit (UTC)" und dem „lokalen Offset“ (der lokalen Zeitdifferenz zur UTC).
  „Systemzeit" = „Systemzeit (UTC)" + „Lokaler Offset".

- „Quelle der Zeit“ zeigt den Ursprung der Systemzeit (UTC) an. Das Gerät wählt automatisch die verfügbare Quelle mit der höchsten Genauigkeit.
  Mögliche Quellen sind: `local`, `sntp` und `ntp`.
  - Die Quelle ist zunächst `local`. Dies ist die Systemuhr des Gerätes.
  - Haben Sie den SNTP-Client aktiviert und empfängt das Gerät ein gültiges SNTP-Paket, setzt es seine Zeit-Quelle auf `sntp`.
  - Haben Sie den NTP-Client aktiviert und hat sich dieser synchronisiert, setzt es seine Zeit-Quelle auf `ntp`.

☐ Mit der Schaltfläche „Setze Zeit vom PC“ übernimmt das Gerät die lokale Zeit von der Workstation, auf der Sie die grafische Benutzeroberfläche ausführen. Es berechnet mit der lokalen Zeitdifferenz die Systemzeit (UTC).
„Systemzeit (UTC)" = „Systemzeit" - „Lokaler Offset"

▶ „Lokaler Offset" dient zur Anzeige/Eingabe der Zeitdifferenz zwischen der lokalen Zeit und der „Systemzeit (UTC)".

☐ Mit der Schaltfläche „Setze Offset vom PC" ermittelt das Gerät die Zeitzone auf Ihrem PC, berechnet daraus die lokale Zeitdifferenz und übernimmt sie.

Anmerkung: Passen Sie in Zeitzonen mit Sommer-/Winterzeit den lokalen Offset bei der Zeitumstellung an, falls erforderlich.
Der SNTP-Client kann die SNTP-Server-IP-Adressen und den lokalen Offset auch von einem DHCP-Server beziehen.
Der NTP-Client bezieht seine NTP-Server-IP-Adressen ausschließlich aus der Konfiguration, die Sie einstellen.

3.2 SNTP-Konfiguration

Das Simple Network Time Protocol (SNTP) bietet Ihnen die Möglichkeit, die Systemzeit in Ihrem Netz zu synchronisieren.
Das Gerät unterstützt die SNTP-Client- und die SNTP-Server-Funktion.

Der SNTP-Server stellt die UTC (Universal Time Coordinated) zur Verfügung. Die UTC ist die auf die koordinierte Weltzeitmessung bezogene Uhrzeit. Die Anzeige ist weltweit gleich. Lokale Zeitverschiebungen bleiben unberücksichtigt.

SNTP verwendet dasselbe Paketformat wie NTP, daher kann ein SNTP-Client seine Zeit sowohl von einem SNTP-Server als auch von einem NTP-Server beziehen.

Anmerkung: Für eine genaue Systemzeitverteilung mit kaskadierten SNTP-Servern und -Clients verwenden Sie im Signalpfad zwischen SNTP-Servern und SNTP-Clients ausschließlich Netzkomponenten (Router, Switches, Hubs), die SNTP-Pakete mit möglichst kleiner Verzögerung weiterleiten.

▶ Funktion
☐ In diesem Rahmen schalten Sie die SNTP-Funktion global ein/aus.

Anmerkung: Wenn Sie SNTP einschalten, während NTP auf dem Gerät schon aktiv ist, meldet das Gerät einen erkannten Fehler.
Um SNTP einzuschalten, deaktivieren Sie zuerst NTP.
Im Lieferzustand ist NTP ausgeschaltet.

▶ SNTP-Status

☐ Die „Statusmeldung“ zeigt Zustände des SNTP-Clients als eine oder mehrere Textmeldungen an, z.B. `Server 1 antwortet nicht`.

▶ Konfiguration SNTP-Client

☐ In „Externe Server-Adresse“ geben Sie die IP-Adresse des SNTP-Servers ein, von dem das Gerät zyklisch die Systemzeit anfordert.

☐ In „Redundante Server-Adresse“ geben Sie die IP-Adresse eines weiteren SNTP-Servers ein. Von diesem fordert das Gerät die Systemzeit an, wenn es 1 Sekunde nach einer Anforderung an die „Externe Server-Adresse“ keine Antwort von dieser erhält.

Anmerkung: Wenn Sie von einer externen/redundanten Server-Adresse die Systemzeit beziehen, dann akzeptieren Sie keine SNTP-Broadcast-Pakete (siehe unten). Das hilft Ihnen sicherzustellen, dass das Gerät die Zeit des eingetragenen Servers verwendet.

☐ In „Server-Anforderungsintervall“ geben Sie den Zeitabstand ein, in dem das Gerät SNTP-Pakete anfordert (gültige Werte: 1 s bis 3.600 s, Lieferzustand: 30 s).

☐ Mit „SNTP-Broadcasts akzeptieren“ übernimmt das Gerät die Systemzeit aus SNTP-Broadcast-/Multicast-Paketen, die es empfängt.

▶ Konfiguration SNTP-Server

☐ In „Anycast-Zieladresse“ geben Sie die IP-Adresse an, an die der SNTP-Server des Gerätes seine SNTP-Pakete schickt (siehe Tab. 36).

☐ In „Anycast-Sendeintervall“ geben Sie den Zeitabstand an, in dem das Gerät SNTP-Pakete verschickt (gültige Werte: 1 s bis 3.600 s, Lieferzustand: 120 s).

☐ Mit „Server deaktivieren bei lokaler Zeitquelle“ schaltet das Gerät die SNTP-Server-Funktion aus, wenn die Quelle der Zeit `local` ist (siehe Dialog `Zeit:Grundeinstellungen`).

IP-Zieladresse	SNTP-Paket versenden an
0.0.0.0	Niemand
Unicast-Adresse (0.0.0.1 - 223.255.255.254)	Unicast-Adresse
Multicast-Adresse (224.0.0.0 - 239.255.255.254), insbesondere 224.0.1.1 (NTP-Adresse)	Multicast-Adresse
255.255.255.255	Broadcast-Adresse

Tab. 36: Zieladressklassen für SNTP- und NTP-Pakete

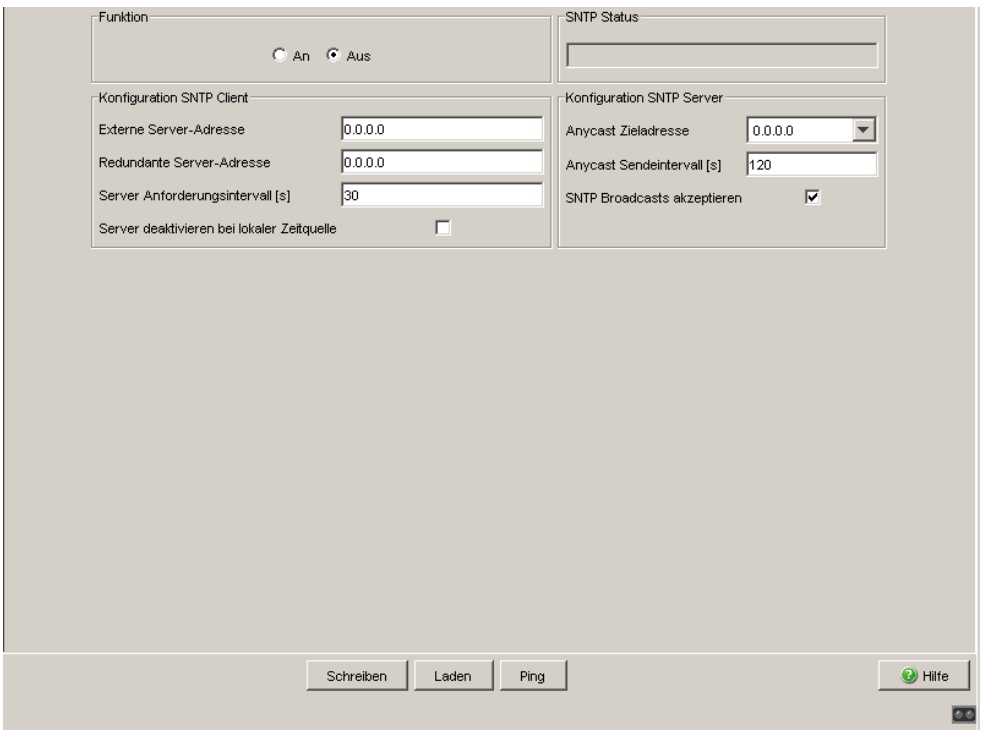


Abb. 23: Dialog SNTP

3.3 NTP-Konfiguration

Das Network Time Protocol (NTP) bietet Ihnen die Möglichkeit, die Systemzeit in Ihrem Netz zu synchronisieren. Das Gerät unterstützt die NTP-Client- und die NTP-Server-Funktion.

Das Gerät kann mit Hilfe von NTP die Zeit genauer bestimmen als mit SNTP. Somit kann es als NTP-Server auch eine genauere Uhrzeit anbieten.

Das Paketformat von NTP und SNTP ist identisch.
Der NTP-Client verwendet im Gegensatz zum SNTP-Client mehrere NTP-Server und einen aufwändigeren Algorithmus zur Synchronisation. Damit kann er die Zeit genauer bestimmen. Die Synchronisation des NTP-Clients kann daher länger dauern als bei einem SNTP-Client.
Verwenden Sie NTP ausschließlich dann, wenn Sie eine höhere Genauigkeit benötigen.

Der NTP-Server stellt die UTC (Universal Time Coordinated) zur Verfügung. Die UTC ist die auf die koordinierte Weltzeitmessung bezogene Uhrzeit. Die Anzeige ist weltweit gleich. Lokale Zeitverschiebungen bleiben unberücksichtigt.
Der NTP-Client bezieht die UTC von einem oder mehreren externen NTP-Servern.

Anmerkung: Für eine möglichst genaue Systemzeitverteilung verwenden Sie für einen NTP-Client mehrere NTP-Server.

- ▶ Funktion
  - ☐ In diesem Rahmen wählen Sie den NTP-Funktionsmodus global aus. Mögliche Werte sind:
    - `off`:
    NTP-Client und NTP-Server sind ausgeschaltet (Voreinstellung)
    - `symmetric-active`:
    NTP-Client und NTP-Server sind aktiv, der Assoziations-Modus ist „Symmectric Active“ (Modus 1)
    - `symmectric-passive`:
    NTP-Client und NTP-Server sind aktiv, der Assoziations-Modus ist

„Symmetric Passive“ (Modus 2)
- `client`:
ausschließlich der NTP-Client ist aktiv, der Assoziations-Modus ist „Client“ (Modus 3)
- `server`:
ausschließlich der NTP-Server ist aktiv, der Assoziations-Modus ist „Server“ (Modus 4).
- `client-server`:
NTP-Client und NTP-Server sind aktiv. Der Assoziations-Modus des Clients ist „Client“ (Modus 3, sendet Anfrage-Pakete mit Modus 4). Der Assoziations-Modus des Servers ist „Server“ (Modus 4, sendet Antwort-Pakete mit Modus 3)
- `broadcast-client`:
ausschließlich der NTP-Client ist aktiv und akzeptiert NTP-Broadcast-Pakete (Modus 5)

Anmerkung: Wenn Sie NTP einschalten (einen anderen Wert als `off` einstellen), während SNTP auf dem Gerät schon aktiv ist, meldet das Gerät einen erkannten Fehler.
Um NTP einzuschalten, deaktivieren Sie zuerst SNTP.
Im Lieferzustand ist SNTP ausgeschaltet.

- NTP-Status
  - ☐ Die „Statusmeldung“ zeigt Zustände des NTP-Clients als eine oder mehrere Textmeldungen an, z.B.`Server 1 antwortet nicht`.

- Konfiguration NTP-Client
  - ☐ In „Externe Server-Adresse“ geben Sie die IP-Adresse des ersten NTP-Servers ein, von dem das Gerät die Systemzeit bezieht.
  - ☐ In „Redundante Server-Adresse“ geben Sie die IP-Adresse eines weiteren NTP-Servers ein, von dem das Gerät die Systemzeit bezieht.
  - ☐ In „Server-Anforderungsintervall“ geben Sie den Zeitabstand ein, in dem das Gerät NTP-Pakete anfordert (gültige Werte: 1 s bis 3.600 s, Lieferzustand: 64 s).

- Konfiguration NTP-Server
  - ☐ In „Anycast-Zieladresse“ geben Sie die IP-Adresse an, an die der NTP-Server des Gerätes seine NTP-Pakete schickt (siehe Tab. 36).
  - ☐ In „Anycast-Sendeintervall“ geben Sie den Zeitabstand an, in dem das Gerät NTP-Pakete verschickt (gültige Werte: 1 s bis 3.600 s, Lieferzustand: 128 s).

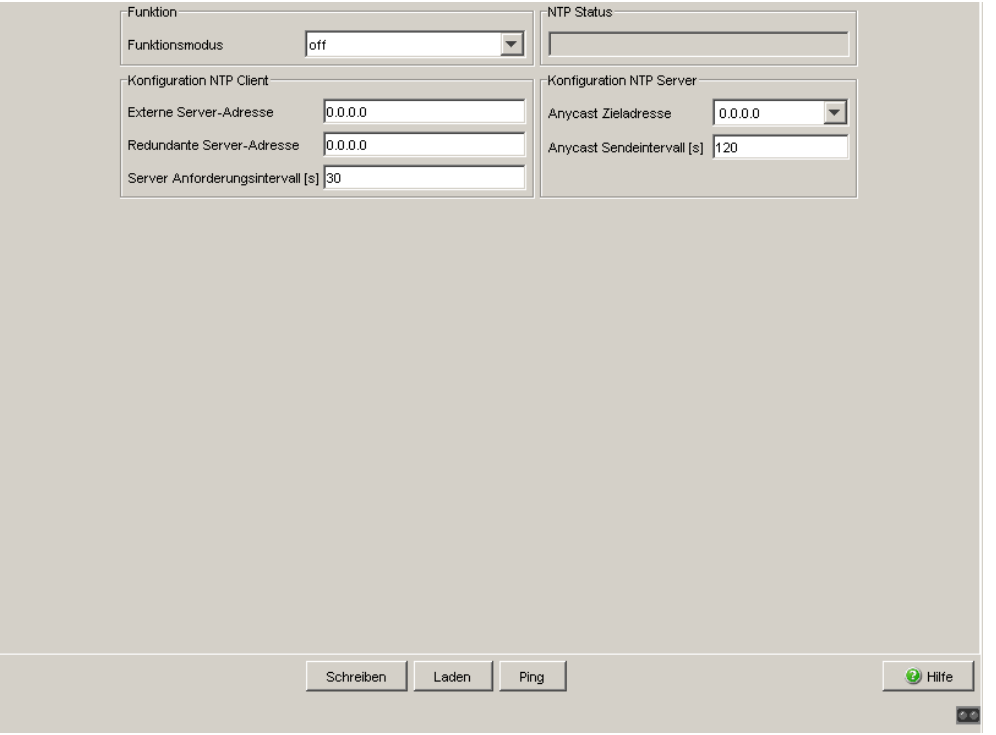


Abb. 24: Dialog NTP

Anmerkung: Wenn Sie einen Parameter für NTP ändern, wird der NTP-Dienst neu gestartet.

4 Netzsicherheit

Um Sie bei der Herstellung der Netzsicherheit zu unterstützen, bietet Ihnen die Firewall:

- Paketfilter mit Adressvorlagen und Firewall-Lern-Modus
- NAT - Network Address Translation
- DoS - Unterstützung beim Schutz vor Denial of Service (DoS)
- Benutzer-Firewall

Die Firewall beobachtet und überwacht den Datenverkehr. Aus den Ergebnissen der Beobachtung und Überwachung zusammen mit den Regeln für die Netzsicherheit erstellt die Firewall sogenannte Zustandstabellen. Nach diesen Zustandstabellen entscheidet die Firewall, ob sie Daten vermittelt, verwirft oder zurückweist.

Mit Hilfe von Adressvorlagen können Sie IP-Paketfilter-Einträge einfacher und schneller erstellen und anpassen.

Als Besonderheit verfügt die Firewall über einen innovativen Einrichtungsassistenten, den Firewall-Lern-Modus. Er unterstützt sie bei der Analyse des Verkehrs und der Erstellung passender Regeln zum Erlauben von erwünschtem Verkehr.

4.1 Paketfilter

Im Untermenü Paketfilter haben Sie die Möglichkeit, Regeln zu erstellen, nach denen die Firewall empfangene Datenpakete behandelt. Die Firewall kann Datenpakete akzeptieren, d. h. weiterleiten, verwerfen oder zurückweisen.

Sie haben die Möglichkeit:
- Regeln selbst zu erstellen,
- Adressvorlagen zu definieren und in Ihren Regeln zu verwenden,
- den Verkehr durch die Firewall mit Hilfe eines innovativen Assistenten für den Firewall-Lern-Modus (FLM) zu analysieren und die vorgeschlagenen Regeln zu übernehmen und bei Bedarf anzupassen.

Die Firewall bietet Ihnen die Möglichkeit, Regeln für folgende Gruppen zu erstellen:
- eingehende IP-Pakete (am externen Port empfangen)
- ausgehende IP-Pakete (am internen Port empfangen)
- eingehende MAC-Pakete (am externen Port empfangen)
- ausgehende MAC-Pakete (am internen Port empfangen)
- eingehende PPP-Pakete (am seriellen Port empfangen)

Die Firewall prüft jedes Datenpaket zunächst nach der 1. Regel in der Tabelle. Treffen die Bedingungen dieser Regel zu, führt die Firewall die zugehörige Aktion aus (akzeptieren, zurückweisen, verwerfen). Trifft die 1. Regel nicht zu, prüft die Firewall die Datenpakete nach der 2. Regel in der Tabelle, usw. bis zur letzten Regel der Tabelle.
Die letzte Default-Regel des Geräts lautet „alles verwerfen“. Diese Regel ist in den Tabellen unsichtbar und kann nicht gelöscht werden.

Sie haben bei IP- und PPP-Paketen die Möglichkeit, einen Log-Eintrag zu erzeugen, wenn keine der Regeln zutrifft.

Sie können Regeln erstellen, löschen, bearbeiten und ihre Reihenfolge verändern. Markieren Sie zum Verschieben eine oder mehrere zusammenhängende Zeilen und verschieben Sie die Selektion mit den Schaltflächen „↑“ oder „↓“. Außerdem können Sie eine Regel duplizieren (klonen) und sie gleich darauf bearbeiten.

Einstellungen im Lieferzustand:

- Im Lieferzustand sind keine Adressvorlagen definiert.
- Der Assistent für den Firewall-Lern-Modus ist ausgeschaltet.
- Die Firewall ist asymmetrisch. Das bedeutet:
  - Sie vermittelt die Datenpakete vom internen Netz in das externe Netz. Die Tabelle für das interne Interface enthält dazu eine sichtbare Regel „alles akzeptieren“.
  - Die Firewall vermittelt Datenpakete vom externen Netz in das interne Netz ausschließlich dann, wenn zuvor ein Teilnehmer des internen Netzes diese Datenpakete angefordert hat.
    Dieses Verhalten entspricht der Stateful Packet Inspection (SPI), einer dynamischen Paketfiltertechnik, die jedes Datenpaket einer bestimmten aktiven Kommunikationsverbindung zuordnet.
    Die anderen Datenpakete verwirft die Firewall.
    Die Tabelle für das externe Interface enthält dazu eine Regel „alles verwerfen“.
- Für IP- oder PPP-Pakete erzeugt die Firewall keinen Log-Eintrag, falls keine Regel zutrifft.

Anmerkung: Firewall-Regeln können sich auch auf die CPU des Geräts selbst beziehen. Sie können dabei die IP-Zieladresse des Geräts mit dem symbolischen Eintrag `me` angeben.
Damit im Lieferzustand die CPU des Geräts erreichbar ist, verwendet es Default-Regeln, die SSH-, SNMP- und HTTPS-Verkehr akzeptieren. Diese sind in den Tabellen unsichtbar und können nicht gelöscht werden.

4.1.1 Adressvorlagen

Dieser Dialog bietet Ihnen die Möglichkeit, Adressvorlagen zu erzeugen, mit deren Hilfe Sie IP-Paketfilter-Einträge einfacher und schneller erstellen und anpassen können. Eine Adressvorlage besteht aus 1 oder mehreren Adress-Einträgen mit dem selben Namen.

Das Gerät erzeugt aus einem Paketfilter-Eintrag mit Variablen automatisch die passenden Paketfilter-Einträge. Wenn Sie die Adressvorlage für eine Variable ändern, passt das Gerät automatisch die erzeugten Paketfilter-Einträge an.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Listen-Name	Name eines Eintrags einer Adressvorlage. **Anmerkung:** Die aktiven Einträge mit dem selben Namen bilden zusammen eine Adressvorlage.	1-19 ASCII-Zeichen, empfohlen: im Bereich 0x21 („!“) bis 0x7e („~“)	
Index	Fortlaufender Zeilenindex.		-
IP-Adresse (CIDR)	IP-Adressbereich des Eintrags in CIDR-Notation. Das Gerät fügt an einen Eintrag für eine Host-Adresse automatisch die Netzmaske /32 an. Um einen bestehenden Adresseintrag zu editieren, klicken Sie in die Tabellenzelle.	Gültiger IPv4-Adressbereich	
Aktiv	Aktiviert oder deaktiviert einen einzelnen Eintrag einer Adressvorlage.	`An`, `Aus`	`An`
Taste „Erzeugen“	Öffnet einen Subdialog mit den Eingabe-Feldern „Listen-Name“ und „IP-Adresse (CIDR)“ zum Erzeugen eines neuen Eintrags für eine Adressvorlage. **Anmerkung:** Wenn Sie zu einer bestehenden Adressvorlage einen Adresseintrag hinzufügen möchten, wählen Sie im Subdialog für das Feld „Listen-Name“ den bestehenden Namen aus.	-	-
Taste „Löschen“	Löscht die selektierten Einträge einer oder mehrerer Adressvorlagen.	-	-

Tab. 37: Beschreibung des Dialogs Adressvorlagen

Anmerkung: Sortieren Sie nach dem Hinzufügen von Einträgen die Liste neu nach der Spalte „Listen-Name“. Das bietet Ihnen die Möglichkeit, dass die grafische Benutzeroberfläche die Einträge, die zu ein und derselben Adressvorlage gehören, untereinander anzeigt.

Anmerkung: Die maximale Anzahl aktiver Einträge in den Adressvorlagen ist durch die maximale Anzahl der IP-Paketfilter-Einträge beschränkt (siehe auf Seite 112 „Ein- und ausgehende IP-Pakete“).

4.1.2 Firewall-Lern-Modus (FLM)

Der Firewall-Lern-Modus ist ein innovativer Einrichtungsassistent. Er unterstützt sie bei der Analyse des Verkehrs und der Erstellung passender Regeln zum Erlauben von erwünschtem Verkehr.

Der Assistent für den Firewall-Lern-Modus bietet Ihnen die Möglichkeit:

- auf einfache Weise automatisch den Verkehr zu ermitteln, den Ihre vorhandenen Regeln noch nicht erlauben (eigentlicher Lern-Modus),
- diesen Verkehr nach verschiedenen Kriterien zu analysieren,
- aus dem erwünschten Verkehr automatisch neue Regelvorschläge zu erstellen,
- diese Regeln bei Bedarf zu modifizieren und deren Verkehrsabdeckung automatisch zu visualisieren, und
- die neuen Regeln auf die gewünschte Abdeckung zu testen.

Anmerkung: Der Assistent für den Firewall-Lern-Modus erfordert dennoch Fachkenntnisse über Datennetze, da der Bediener für die erstellten Regeln verantworlich ist.

Der FLM bezieht sich ausschließlich auf Pakete, die das Gerät (die Firewall) durchqueren möchten. Pakete, die an das Gerät selbst gerichtet sind und solche, die das Gerät selbst erzeugt, sind davon ausgenommen.

Führen Sie zur FLM-unterstützten Regel-Erstellung folgende Schritte aus:

- ☐ Setzen Sie die Firewall an der vorgesehenen Stelle in Ihr Netz ein.
- ☐ Aktivieren Sie den FLM-Assistenten an den gewünschten Interfaces der Firewall (typischerweise an beiden Interface).
- ☐ Starten Sie den eigentlichen Lern-Modus.
- ☐ Betreiben Sie die Geräte in Ihrem Netz eine Zeitlang, so dass die Firewall den erwünschten Verkehr lernt.
- ☐ Stoppen Sie den Lern-Modus.
- ☐ Lassen Sie sich den gelernten Verkehr auf dem ausgewählten Interface anzeigen:
  - ▶ Hat die Firewall zu wenig Verkehr gelernt, setzen Sie den Lern-Modus fort, um mehr Verkehr zu lernen.
  - ▶ Hat die Firewall genügend Verkehr gelernt, inspizieren Sie die erfassten Daten.
- ☐ Wählen Sie erwünschte Einträge aus den erfassten Daten aus und fügen Sie sie dem temporären Regelsatz hinzu.
- ☐ Modifizieren Sie gegebenenfalls die hinzugefügten Regeln.
- ☐ Ignorieren Sie unerwünschte Einträge in den erfassten Daten, d. h., legen Sie dafür keine Regeln an. Die Firewall sperrt so nach dem Beenden des Lern- und Test-Modus diesen Verkehr.
- ☐ Geben Sie die gewünschten Regeln zum Test frei.
- ☐ Starten Sie den Testmodus:
  - ▶ Arbeiten die Geräte in Ihrem Netz wie gewünscht, schreiben Sie die temporären Regeln in Ihre Regelbasis.
  - ▶ Arbeiten die Geräte in Ihrem Netz anders als gewünscht, modifizieren Sie die zum Test freigegebenen Regeln. Alternativ starten Sie den Lern-Modus erneut, um mehr Verkehr zu lernen.
- ☐ Beenden Sie den Assistenten für den Firewall-Lern-Modus.
- ☐ Speichern Sie die Regeln in der Konfiguration.

Anmerkung: Während des Lernens beobachtet und lernt die Firewall ausschließlich den Verkehr, den sie durch die bestehenden Regeln bisher nicht erlaubt hat. Dazu deaktiviert die Firewall am externen Interface den Paketfilter-Eintrag „alles verwerfen“. Dies kann dazu führen, dass die Firewall während des Lern-Modus auch unerwünschten Verkehr akzeptiert. Erzeugen Sie während des Lernens ausschließlich erwünschten Verkehr über die Firewall. Finden Sie bei der Auswertung des gelernten Verkehrs dennoch unerwünschte Einträge, legen Sie für diese keine Regel an und löschen Sie ggf. bereits angelegte Regeln.

Akzeptieren Sie nach dem Abschluss der Lern- und Test-Phase die aus den gelernten Daten abgeleiteten, temporären Regeln, verhält sich die Firewall in der Regel nicht mehr asymmetrisch.

Anmerkung:

- Wenn Sie das Gerät während des Lernens zwischen dem Router- und Transparent-Modus umschalten, kann dies zu unvorhersehbaren Ergebnissen führen.
- Wenn Sie während des Lernens manuell Paketfilter-Einträge hinzufügen, löschen oder ändern, kann dies die Effizienz der Regeln beeinträchtigen, die Sie von den gelernten Daten ableiten.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Rahmen „Funktion“	Schaltet den Assistenten für den Firewall-Lern-Modus an oder aus.	`An`, `Aus`	`Aus`
Rahmen „Konfiguration“			
Lernen an Interfaces	Wählt die Interfaces der Firewall aus, auf denen die Firewall Verkehr lernen soll.	`Beide`, `Internes`, `Externes`	`Beide`
Anpassung der „alles erlauben“-Regel	▶ `Automatisch`: Die Firewall deaktiviert vor dem Lernen und Testen auf den Interfaces automatisch die Regeln „alles erlauben“. Ist eine solche Regel während des Lernens oder Testens aktiv, trifft sie auf den Verkehr zu dem betroffenen Interface zu. Diese Situation unterbindet das Lernen von neuem Verkehr . Die automatische Deaktivierung dieser Regeln während dem Lernen und Testen ermöglicht das einfache Lernen von neuem Verkehr. Während der Verkehrs-Analyse und der Regel-Erstellung aktiviert die Firewall diese Regeln wieder bzw. fügt eine solche ein. Dies unterstützt Sie bei der Sicherung Ihrer Produktiv-Umgebung. Übernehmen Sie die neu erstellten, temporären Regeln, deaktiviert das Gerät die „alles erlauben“-Regeln auf den betroffenen Interfaces. ▶ `Manuell`: Deaktivieren Sie vor dem Lernen und Testen auf den betroffenen Interfaces manuell die Regeln „alles erlauben“. Aktivieren Sie diese während der Verkehrs-Analyse und der Regel-Erstellung wieder. Übernehmen Sie die neu erstellten, temporären Regeln, deaktivieren Sie die „alles erlauben“-Regeln auf den betroffenen Interfaces.	`Automatisch`, `Manuell`	`Automatisch`

Tab. 38: Firewall-Lern-Modus, Karteikarte „FLM-Steuerung“, Rahmen Funktion und Konfiguration

Parameter	Bedeutung	Wertebereich	Voreinstellung
Tasten			
Taste „Starte Lernmodus“/ „Stoppe Lernmodus“/ „Setze Lernmodus fort“	▶ `Starte Lernmodus`: startet das Lernen von Verkehrsdaten, wenn noch keine Daten vorhanden sind. ▶ `Stoppe Lernmodus`: unterbricht das Lernen von Verkehrsdaten. ▶ `Setze Lernmodus fort`: setzt das Lernen von Verkehrsdaten fort, wenn schon Daten vorhanden sind.	`Starte Lernmodus`, `Stoppe Lernmodus`, `Setze Lernmodus fort`	`Starte Lernmodus` (deaktiviert)
Taste „Starte Testmodus“/ „Stoppe Testmodus“	▶ `Starte Testmodus`: übernimmt die zum Test freigegebenen Regeln des jeweiligen Interface vorübergehend in den Regelsatz. ▶ `Stoppe Testmodus`: beendet den Testmodus.	`Starte Testmodus`, `Stoppe Testmodus`	`Starte Testmodus` (deaktiviert)
Taste „Daten löschen“	Bricht das Lernen ab und löscht die gelernten Verkehrs-Daten. Sie haben die Möglichkeit, das Lernen wieder neu zu starten.		

Tab. 39: Firewall-Lern-Modus, Karteikarte „FLM-Steuerung“, Bedientasten

Anmerkung: Der Dialog bietet ausschließlich die Karteikarten an, die Sie im aktuellen Zustand des Lern- oder Test-Modus bedienen können. Ist eine Bedienung nicht möglich, stellen die Dialog-Karteikartenreiter „Internes Interface“ oder „Externes Interface“ ihren Text deaktiviert (ausgegraut) dar. Die Tasten des Dialogs können verschiedene Beschriftungen anzeigen. Sie bieten ausschließlich die Aktionen an, die Sie im aktuellen Zustand des FLM-Assistenten ausführen können. Ist keine Aktion möglich, stellt eine Taste ihren Text deaktiviert (ausgegraut) dar.

Parameter	Bedeutung	Werte-bereich	Voreinstellung
Rahmen „Information“			
Status	▶ `Aus`: Das Lernen ist nicht aktiv. ▶ `Keine Daten. Modus wählen und Lernen starten`: Das Lernen ist inaktiv und die Firewall hat noch keine Daten gelernt. ▶ `Angehalten. Interface-Daten prüfen und freigeben`: Sie haben das Lernen unterbrochen. Sie haben nun die Möglichkeit, in den Dialog-Reitern „Internes Interface“ oder „Externes Interface“ die gelernten Daten zu prüfen, Regeln davon abzuleiten, diese zu modifizieren und zum Testen freizugeben. ▶ `Am Lernen`: Sie haben das Lernen gestartet. Das Gerät sammelt Verkehrs-Daten. ▶ `Am Testen`: Sie haben den Test-Modus gestartet. ▶ `Gerade beschäftigt. Bitte warten`: Das Gerät ist gerade mit der Verarbeitung von Daten beschäftigt oder die grafische Benutzeroberfläche tauscht Daten mit dem Gerät aus.		
Weitere Informationen	▶ (Keine Anzeige): Das Lernen ist nicht aktiv. ▶ `Normale Funktion`: Das Lernen ist aktiv. Das Gerät hat noch genügend Speicher für Verkehrs-Daten. ▶ `Gestoppt! Kein freier Speicher`: Der verfügbare Speicher zum Lernen von Verbindungen ist erschöpft. Die Firewall hat das Erfassen von Verkehrs-Daten angehalten. ▶ `Einige Verbindungen wurden nicht erfasst`: Bei der internen Verarbeitung der zu lernenden Verbindungen hat die Firewall zu viele Hash-Kollisionen festgestellt. Dies bedeutet, dass die Firewall einige Verbindungen nicht erfasst hat. Möglicherweise sind die dadurch ermittelten Regeln unvollständig und erlauben nicht den gewünschten Verkehr. Testen Sie die aus diesem Lernvorgang erstellten Regeln gründlich.		

Tab. 40: Firewall-Lern-Modus, Karteikarte „FLM-Steuerung“, Rahmen „Information“

Parameter	Bedeutung	Werte-bereich	Voreinstellung
IP-Einträge	Anzahl der bisher gelernten Layer 3-Verbindungen, die an den gewählten Interfaces eingegangen sind. Bei TCP-Paketen zählt die Firewall nur den Verbindungsaufbau. Bei anderen Layer 4-Protokollen zählt sie nur das 1. Paket einer Verbindung. Eine Verbindung ist eine eindeutige Kombination aus Quell- und Ziel-Adressen, Quell- und Ziel-Ports und der Layer 4-Protokoll-Nr. des IP-Headers. Um die Anzeige bei laufendem Lernen zu aktualisieren, drücken Sie die Taste „Laden“.		
Freier Speicher für Lerndaten [%]	Zeigt den noch verbleibenden Speicher für zu lernende Verbindungen an. Die Firewall kann bis zu 65.536 verschiedene Verbindungen lernen. In ICMP-Paketen ignoriert die Firewall dabei die Codes. ICMP-Pakete, die sich nur im Code unterscheiden, ordnet die Firewall einer einzigen Verbindung zu. Um die Anzeige bei laufendem Lernen zu aktualisieren, drücken Sie die Taste „Laden“.		

Tab. 40: Firewall-Lern-Modus, Karteikarte „FLM-Steuerung“, Rahmen „Information“

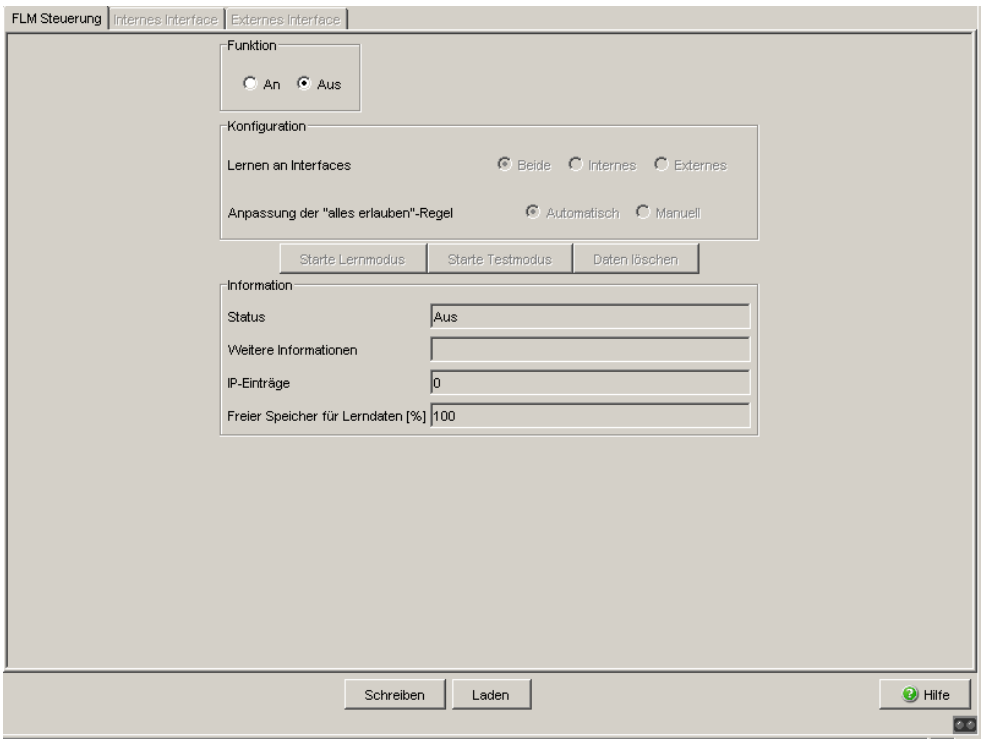


Abb. 25: Dialog Firewall-Lern-Modus, Karteikarte „FLM-Steuerung“

Parameter	Bedeutung	Wertebereich	Voreinstellung
Rahmen „Erfasste Daten“			
Index	Fortlaufender Zeilenindex.		-
Quelladresse	Gelernte IP-Quelladresse	IPv4-Adresse	
Quellport	Gelernter UDP- oder TCP-Quellport	0-65.535	
Zieladresse	Gelernte IP-Zieladresse	IPv4-Adresse	
Zielport	Gelernter UDP- oder TCP-Zielport (ICMP 0).	0-65.535	
Protokoll	Gelernte Layer 4-Protokoll-Nr. aus dem IP-Header. Bekannte Protokoll-Nummern zeigt das Gerät mit ihren Namen an.	0-255, `icmp`, `tcp`, `udp`	
Taste „Zum Regelsatz hinzufügen“	Fügt die ausgewählten Zeilen der gelernten Daten dem temporären Regelsatz hinzu. Haben Sie mehrere Zeilen ausgewäht, übernimmt das Gerät die erste Zeile als Regel. Danach haben Sie die Möglichkeit, die Regel zu editieren. **Anmerkung:** Die gelernten Einträge, die durch den gesamten temporären Regel-Satz abgedeckt sind, markiert das Gerät hellgrün. Die Einträge, die durch die aktuell selektierten Regeln abgedeckt sind, markiert das Gerät dunkelgrün. Wenn Sie eine Regel ändern, z. B. eine Netzmaske verkürzen, passt das Gerät automatisch die dunkelgrüne Markierung an. So haben Sie die Möglichkeit, schnell und einfach zu erkennen, wie eine geänderte Regel die gelernten Einträge abdeckt. **Anmerkung:** Erstellen Sie eine Regel aus einem ICMP-Eintrag, ordnet das Gerät der Regel den Zielport `any` zu.		

Tab. 41: Firewall-Lern-Modus, Karteikarte „Internes Interface“ und „Externes Interface“, Rahmen „Erfasste Daten“

Parameter	Bedeutung	Wertebereich	Voreinstellung
Ausblenden von Verbindungen, die vom gelernten Regelsatz abgedeckt sind	Aktivieren Sie diese Funktion, dann blendet das Gerät die gelernten Einträge aus, die von einer der Regel abgedeckt sind, statt diese grün zu markieren. Aktivieren Sie diese Funktion, wenn Sie ausschließlich die noch nicht von Regeln abgedeckten Einträge anzeigen möchten.		
Vom Regelsatz erfasste Verbindungen	Zeigt die Anzahl der gelernten Verbindungen an, die der gesamte temporäre Regelsatz abdeckt. Zusätzlich zeigt das Gerät nach dem Schrägstrich die Gesamtzahl aller gelernten Verbindungen an.	Format: abgedeckt / gesamt	-
Von aktueller Auswahl erfasste Verbindungen	Zeigt die Anzahl der gelernten Verbindungen an, die die aktuelle Auswahl des temporären Regelsatzes abdeckt Zusätzlich zeigt das Gerät nach dem Schrägstrich die Gesamtzahl der gelernten Verbindungen an.	Format: abgedeckt / gesamt	-

Tab. 41: Firewall-Lern-Modus, Karteikarte „Internes Interface“ und „Externes Interface“, Rahmen „Erfasste Daten“

Protokoll	Port-Nr.
FTP (data, control)	20, 21
SSH	22
Telnet	23
SMTP	25
DHCP/BOOTP (Server, Client)	67, 68
TFTP	69
HTTP (www)	80
POP3	110
NTP	123
NetBIOS (Name, Datagram, Session Service)	137, 138, 139
SNMP, SNMP Trap	161, 162
HTTPS	443
EtherNet/IP I/O	2222
EtherNet/IP Messaging	44818
Foundation Fieldbus Annunciation	1089
Foundation Fieldbus Message Specification	1090
Foundation Fieldbus System Management	1091
Foundation Fieldbus LAN Redundancy Port	3622
LonWorks	2540
LonWorks2	2541
Modbus/TCP	502
Profinet RT Unicast	34962
Profinet RT Multicast	34963
Profinet Context Manager	34964
IEC 60870-5-104	2404
DNP	20000
Ethercat	34980

Tab. 42: Beispiele für registrierte Portnummern

Anmerkung: Unter http://www.iana.org/assignments/port-numbers finden Sie eine Liste mit den registrierten Portnummern.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Rahmen „Regeln“	**Anmerkung:** Die meisten Spalten in dieser Tabelle sind mit denen in den Dialogen `Eingehende IP-Pakete` und `Ausgehende IP-Pakete` identisch.		
Index	Fortlaufender Zeilenindex.		-
Beschreibung	Beliebige Beschreibung dieses Eintrags. Hat die Firewall den Eintrag aus den gelernten Daten des Firewall-Lern-Modus (FLM) erstellt, trägt das Gerät den Text „learned by FLM“ ein.	0-128 ASCII-Zeichen	
Aktiv	Aktivieren/Deaktivieren der Regel. **Anmerkung:** Haben Sie die Regel im Firewall-Lern-Modus erstellt, ist die Regel aktiv. Diese Einstellung ist innerhalb des FLM-Dialogs unveränderlich. Sie können die Regel später im Dialog `Eingehende IP-Pakete` oder `Ausgehende IP-Pakete` modifizieren.	`An`	`An`
Quelladresse (CIDR)	IP-Adresse mit Netzmaske (CIDR) der eigentlichen Quelle des Datenpaketes **Anmerkung:** Wenn Sie eine Adressvorlage einsetzen möchten, geben Sie den Namen der Adressvorlage ein. Stellen Sie dem Namen ein Dollar-Zeichen („$“) voran, um ihn als Variablennamen zu kennzeichnen. **Anmerkung:** Wenn Sie in den Regeln, die Sie von den gelernten Daten abgeleitet haben, Adressvorlagen verwenden, funktionieren diese Regeln anschließend korrekt. Das Gerät ignoriert diese Regeln jedoch beim Markieren und Ausblenden der gelernten Daten.	IP-Adresse mit Netzmaske, any = alle, me = eigene IP-Adresse, $<Adressvorlage> = Adressvorlage	any

Tab. 43: Firewall-Lern-Modus, Karteikarte „Internes Interface“ und „Externes Interface“, Rahmen „Regeln“

Parameter	Bedeutung	Wertebereich	Voreinstellung
Quellport	Logischer Quellport des Datenpaketes Zur Auswahl mehrerer Ports können Sie auch Operatoren (op) verwenden: = gleich != ungleich < kleiner <= kleiner gleich > größer >= größer gleich >< innerhalb <> außerhalb Verwenden Sie für die Portbezeichnung Dezimalzahlen. Folgende bekannte Ports können Sie auch als ASCII-Zeichen eingeben: 7 tcp/udp: echo 9 tcp/udp: discard 20 tcp :ftp-data 21 tcp :ftp 22 tcp/udp: ssh 23 tcp :telnet 53 tcp/udp: domain 67 tcp/udp: bootps 68 tcp/udp: bootpc 69 udp : tftp 80 tcp/udp: www, http 88 tcp/udp: kerberos 115 tcp : sftp 123 tcp : ntp 161 udp : snmp 162 udp : snmp-trap 179 tcp/udp: bgp 389 tcp/udp: ldap 443 tcp/udp: https	any = alle op port or port 1 op port 2	any

Tab. 43: Firewall-Lern-Modus, Karteikarte „Internes Interface“ und „Externes Interface“, Rahmen „Regeln“

Parameter	Bedeutung	Wertebereich	Voreinstellung

Quellport (Fortsetzung)	Um eingehende IP-Pakete selektiv auf bestimmte ICMP-Traffic-Kriterien zu prüfen, verwenden Sie:
	- für den Parameter „Protokoll" die Angabe `icmp`
	- für den Parameter „Quellport" die folgende Definition für ICMP-Typ und -Code:
	`type <t> [code <c>]`
	<...> Angabe eines Parameters
	[...] Optionale Angabe
	t Dezimalwert, 1- bis 3-stellig
	c Dezimalwert, 1- bis 3-stellig
	Beispiele: `type 0 code 0`
	`type 10`
	Mögliche Werte für ICMP-Typ und -Code entnehmen Sie der folgenden Tabelle (Tab. 46).
		`type <t> [code <c>]`	any

Zieladresse (CIDR)	IP-Adresse mit Netzmaske (CIDR) des eigentlichen Ziels des Datenpaketes **Anmerkung:** Wenn Sie eine Adressvorlage einsetzen möchten, geben Sie den Namen der Adressvorlage ein. Stellen Sie dem Namen ein Dollar-Zeichen („$") voran, um ihn als Variablennamen zu kennzeichnen. **Anmerkung:** Wenn Sie in den Regeln, die Sie von den gelernten Daten abgeleitet haben, Adressvorlagen verwenden, funktionieren diese Regeln anschließend korrekt. Das Gerät ignoriert diese Regeln jedoch beim Markieren und Ausblenden der gelernten Daten.	IP-Adresse mit Netzmaske, any = alle, me = eigene IP-Adresse, $<Adressvorlage> = Adressvorlage	
Zielport	Logischer Zielport des Datenpaketes Zur Auswahl mehrerer Ports können Sie die gleichen Operatoren wie beim Quellport verwenden: Verwenden Sie für die Portbezeichnung Dezimalzahlen. Die gleichen bekannten Ports wie beim Quellport können Sie auch als ASCII-Zeichen eingeben.	any = alle op port port 1 op port 2	any

Tab. 43: Firewall-Lern-Modus, Karteikarte „Internes Interface" und „Externes Interface", Rahmen „Regeln"

Parameter	Bedeutung	Wertebereich	Voreinstellung
Protokoll	Folgende Protokolle können Sie als ASCII-Zeichen eingeben: ▶ `any` Beliebiges Layer 4-Protokoll ▶ `tcp` Transmission Control Protocol (RFC 793) ▶ `udp` User Datagram Protocol (RFC 768) ▶ `icmp` Internet Control Message Protocol (RFC 792) ▶ `igmp` Internet Group Management Protocol (RFCs 1112 (v1), 2236 (v2), 3376 (v3)) ▶ `ipip` IP in IP Tunneling (RFC 1853) ▶ `esp` IPsec Encapsulated Security Payload (RFC 2406) ▶ `ah` IPsec Authentication Header (RFC 2402) ▶ `ipv6-icmp` Internet Control Message Protocol for IPv6 (RFC 4443) ▶ `<0 - 255>` Nr. des Layer 4-Protokolls im IP-Header **Anmerkung:** Bei den Protokollen udp und tcp haben Sie die Möglichkeit, in den Spalten „Quellport“ und „Zielport“ die Protokoll-Ports anzugeben. Für andere Protokollen tragen Sie bei „Quellport“ und „Zielport“ `any` ein. **Anmerkung:** Die stateful Firewall unterstützt die Protokolle tcp, udp und icmp.	`any` = alle, `tcp`, `udp`, `icmp`, (außerdem: `igmp`, `ipip`, `esp`, `ah`, `ipv6-icmp`, `<0 - 255>`) **Anmerkung:** Sie können die Protokolle `any`, `tcp`, `udp` und `icmp` aus der Liste auswählen. Geben Sie die Protokolle `igmp`, `ipip`, `esp`, `ah`, `ipv6-icmp` und `<0 - 255>` von Hand ein.	any

Tab. 43: Firewall-Lern-Modus, Karteikarte „Internes Interface“ und „Externes Interface“, Rahmen „Regeln“

Parameter	Bedeutung	Wertebereich	Voreinstellung
Aktion	Aktion, die die Firewall durchführt, wenn die Regel zutrifft. **Anmerkung:** Haben Sie die Regel im Firewall-Lern-Modus erstellt, ist die Aktion `accept`. Diese Einstellung ist innerhalb des FLM-Dialogs unveränderlich. Sie können die Regel später im Dialog `Eingehende IP-Pakete` oder `Ausgehende IP-Pakete` modifizieren.	`accept`	`accept`
Log	Eintrag in die Ereignis-Liste, wenn die Firewall die Regel anwendet. Ggf. sendet das Gerät zusätzlich einen Trap. **Anmerkung:** Die Einstellung `logAndTrap` kann große Mengen an Trap-Datenverkehr erzeugen. Dies gilt besonders dann, wenn das Senden des Traps wieder einen Match der Firewall-Regel auslöst (z.B. wenn der Trap-Host ist nicht erreichbar ist und ein Router mit einer ICMP-Nachricht antwortet).	`enable`, `disable`, `logAndTrap`	`disable`
Fehler	Zeigt die letzte Meldung bei einem erfolglosen Versuch, den Tabelleneintrag zu aktivieren (typischerweise ein erkannter Syntaxfehler).		

Tab. 43: Firewall-Lern-Modus, Karteikarte „Internes Interface“ und „Externes Interface“, Rahmen „Regeln“

Parameter	Bedeutung	Werte-bereich	Voreinstellung
Taste „Zum Test freigeben“/ „Freigabe aufheben“	▶ **Zum Test freigeben:** Fügt die Regeln des temporären Regel-Satzes zum Test in die vorläufig Produktiv-Regelbasis ein. Das Gerät sperrt dabei die freigegebenen Regeln gegen Veränderungen in der Produktiv-Regelbasis. ▶ **Freigabe aufheben:** Entfernt die Regeln des temporären Regel-Satzes wieder aus der Produktiv-Regelbasis. Das Gerät gibt die Regeln wieder zum Editieren im Firewall-Lern-Modus frei.		
Taste „Regel löschen“	Löscht die selektierten Regeln aus dem temporären Regel-Satz.		

Tab. 44: Firewall-Lern-Modus, Karteikarte „Internes Interface“ und „Externes Interface“, Bedientasten

Anmerkung: Die Tasten des Dialogs können verschiedene Beschriftungen anzeigen. Eine Taste bietet die Aktion an, die im aktuellen Zustand möglich ist.

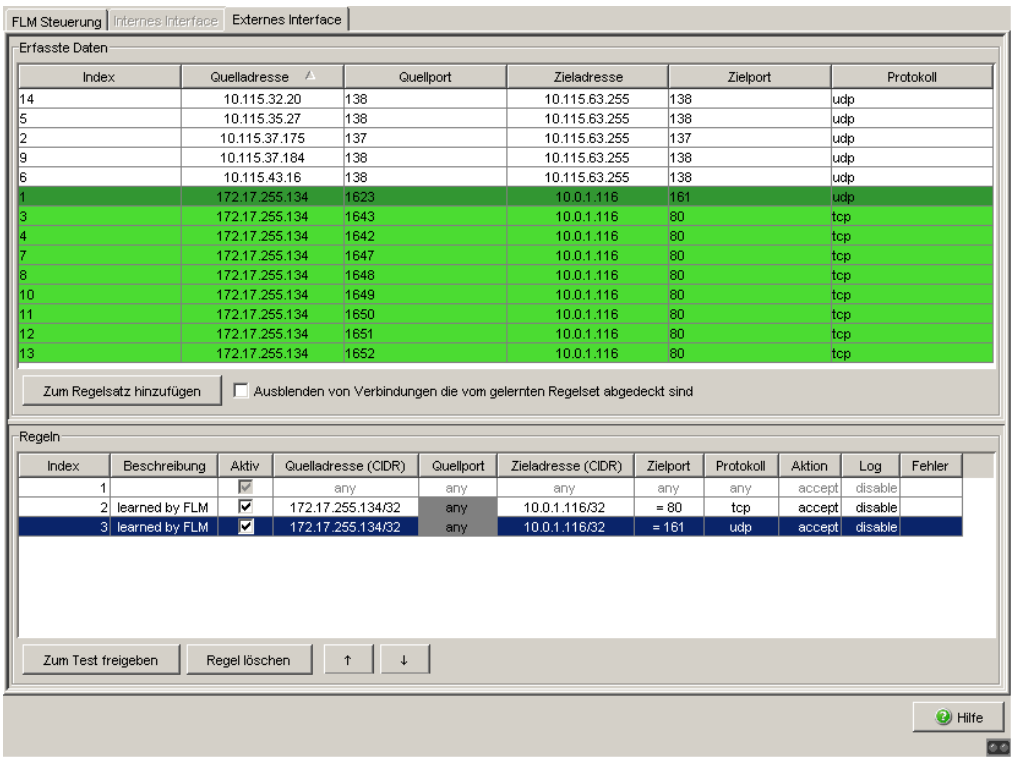


Abb. 26: Dialog Firewall-Lern-Modus, Karteikarte „Externes Interface“

Details des Beispiel-Screen-Shots

Die Abb. 26 zeigt die Dialog-Karteikarte „Externes Interface“ nach den folgenden Schritten: Der Benutzer hat:

- ☐ den Lern-Modus gestartet,
- ☐ von einer Workstation aus auf die grafische Benutzeroberfläche eines Switch im internen Netz zugegriffen (die grafische Benutzeroberfläche geladen und Dialoge geöffnet),
- ☐ den Lern-Modus wieder unterbrochen,
- ☐ die Dialog-Karteikarte „Externes Interface gewählt“,
- ☐ die erfassten Daten nach IP-Quelladresse aufsteigend sortiert
- ☐ 2 Regeln aus dem gewünschten Verkehr abgeleitet und diese modifiziert.

Die Abb. 26 zeigt folgende Details:

- Die weißen Zeilen der erfassten Daten zeigen, dass die Firewall am externen Interface NetBIOS-Verkehr von verschiedenen Hosts an die Netzwerk-Broadcast-Adresse 10.115.63.255 gelernt hat. Dieser Verkehr ist unerwünscht, deshalb hat der Benutzer dafür keine Regeln angelegt.
- Die grünen Zeilen zeigen, dass die Firewall außerdem SNMP- und HTTP-Verkehr von der Workstation 172.17.255.134 zum Switch 10.0.1.116 gelernt hat. Dieser Verkehr ist erwünscht, deshalb hat der Benutzer dafür Regeln angelegt.
- Der Benutzer hat aus dem Datum mit dem Index 3 eine Regel dem temporären Regel-Satz hinzugefügt (die Regel mit dem Index 2), um den HTTP-Verkehr zwischen Workstation und Switch zu erlauben.
  - Die Firewall hat zunächst den TCP-Quellport 1643 in die Regel übernommen.
  - Der Benutzer hat den Quellport der Regel auf `any` geändert (dunkelgraue Markierung), damit die zufällig gewählten Quellports bei HTTP-Verkehr erlaubt sind.
- Der Benutzer hat danach aus dem Datum mit dem Index 1 eine Regel dem temporären Regel-Satz hinzugefügt (die Regel mit dem Index 3), um den SNMP-Verkehr zwischen Workstation und Switch zu erlauben.
  - Die Firewall hat zunächst den UDP-Quellport 1623 in die Regel übernommen.
  - Der Benutzer hat den Quellport der Regel auf `any` geändert, damit die zufällig gewählten Quellports bei SNMP-Verkehr erlaubt sind.
- Die grünen Zeilen in den erfassten Daten zeigen an, dass nun der ausgehende HTTP- und SNMP-Verkehr von der Workstation zum Switch von den Regeln erlaubt würde.
- Die dunkelgrüne Zeile zeigt den erlaubten Verkehr an, der durch die Regel 3 erlaubt ist. Diese Regel ist gerade selektiert.
- Die hellgrünen Zeilen der erfassten Daten zeigen den erlaubten Verkehr an, der durch die anderen Regeln des temporären Regel-Satzes (hier nur die Regel 2) erlaubt ist. Diese Regeln sind deselektiert.

Der Benutzer kann nun:

- ☐ die Regeln 2 und 3 selektieren und mit der Taste „Zum Test freigeben“ dem zu testenden Regelsatz hinzufügen,
- ☐ in der Dialog-Karteikarte „FLM-Steuerung“ die Taste „Starte Testmodus“ klicken,
- ☐ weiteren Netz-Verkehr erzeugen.

Die Firewall wird nun:

- Den SNMP- und HTTP-Verkehr von der Workstation zum Switch erlauben. Diesen Verkehr übergeht die Firewall nun beim Lernen.
- Nur den noch nicht erlaubten Verkehr lernen. So hilft sie dem Benutzer, ggf. weiteren erwünschten Verkehr zu entdecken und zu analysieren. Somit unterstützt Sie den Benutzer, seine Regeln zu verfeinern.

4.1.3 Ein- und ausgehende IP-Pakete

Die Firewall bietet Ihnen die Möglichkeit, am externen und internen Port eingehende IP-Pakete zu prüfen auf:

- den logischen Port
- die Quell-IP-Adresse
- den logischen Zielport
- die Ziel-IP-Adresse
- das Übertragungsprotokoll

Sie haben die Möglichkeit, bei jedem Paket, das mit keiner der Regeln der Tabelle übereinstimmt, sondern nur mit der unsichtbaren Default-Regel „alles verwerfen“, einen Log-Eintrag zu erzeugen. Aktivieren Sie dazu die Einstellung „Log bei Nichtübereinstimmung“.

Sie können Regeln erstellen, löschen, bearbeiten und ihre Reihenfolge verändern. Markieren Sie zum Verschieben eine oder mehrere zusammenhängende Zeilen und verschieben Sie die Selektion mit den Schaltflächen „↑“ oder „↓“. Außerdem können Sie eine Regel duplizieren (klonen) und sie gleich darauf bearbeiten.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Index	Fortlaufender Zeilenindex.		-
Beschreibung	Beliebige Beschreibung dieses Eintrags. Hat die Firewall den Eintrag aus den gelernten Daten des Firewall-Lern-Modus (FLM) erstellt, trägt das Gerät den Text „learned by FLM“ ein.	0-128 ASCII-Zeichen	
Aktiv	Aktivieren/Deaktivieren der Regel	ein/aus	aus
Quelladresse (CIDR)	IP-Adresse mit Netzmaske (CIDR) der eigentlichen Quelle des Datenpaketes **Anmerkung:** Wenn Sie eine Adressvorlage einsetzen möchten, geben Sie den Namen der Adressvorlage ein. Stellen Sie dem Namen ein Dollar-Zeichen („$“) voran, um ihn als Variablennamen zu kennzeichnen.	IP-Adresse mit Netzmaske, any = alle, me = eigene IP-Adresse, $<Adressvorlage> = Adressvorlage	any

Tab. 45: Am externen/internen Port eingehende/ausgehende IP-Pakete

Parameter	Bedeutung	Wertebereich	Voreinstellung
Quellport	Logischer Quellport des Datenpaketes Zur Auswahl mehrerer Ports können Sie auch Operatoren (op) verwenden: = gleich != ungleich < kleiner <= kleiner gleich > größer >= größer gleich >< innerhalb <> außerhalb Verwenden Sie für die Portbezeichnung Dezimalzahlen. Folgende bekannte Ports können Sie auch als ASCII-Zeichen eingeben: 7 tcp/udp: echo 9 tcp/udp: discard 20 tcp :ftp-data 21 tcp :ftp 22 tcp/udp: ssh 23 tcp :telnet 53 tcp/udp: domain 67 tcp/udp: bootps 68 tcp/udp: bootpc 69 udp : tftp 80 tcp/udp: www, http 88 tcp/udp: kerberos 115 tcp : sftp 123 tcp : ntp 161 udp : snmp 162 udp : snmp-trap 179 tcp/udp: bgp 389 tcp/udp: ldap 443 tcp/udp: https	any = alle op port or port 1 op port 2	any

Tab. 45: Am externen/internen Port eingehende/ausgehende IP-Pakete

Parameter	Bedeutung	Wertebereich	Voreinstellung

Quellport (Fortsetzung)	Um eingehende IP-Pakete selektiv auf bestimmte ICMP-Traffic-Kriterien zu prüfen, verwenden Sie:
	- für den Parameter „Protokoll" die Angabe `icmp`
	- für den Parameter „Quellport" die folgende Definition für ICMP-Typ und -Code:
	`type <t> [code <c>]`
	<...> Angabe eines Parameters
	[...] Optionale Angabe
	t Dezimalwert, 1- bis 3-stellig
	c Dezimalwert, 1- bis 3-stellig
	Beispiele: `type 0 code 0`
	`type 10`
	Mögliche Werte für ICMP-Typ und -Code entnehmen Sie der folgenden Tabelle (Tab. 46).
		`type <t> [code <c>]`	any

Zieladresse (CIDR)	IP-Adresse mit Netzmaske (CIDR) des eigentlichen Ziels des Datenpaketes **Anmerkung:** Wenn Sie eine Adressvorlage einsetzen möchten, geben Sie den Namen der Adressvorlage ein. Stellen Sie dem Namen ein Dollar-Zeichen („$") voran, um ihn als Variablennamen zu kennzeichnen.	IP-Adresse mit Netzmaske, any = alle, me = eigene IP-Adresse, $<Adressvorlage> = Adressvorlage	
Zielport	Logischer Zielport des Datenpaketes Zur Auswahl mehrerer Ports können Sie die gleichen Operatoren wie beim Quellport verwenden: Verwenden Sie für die Portbezeichnung Dezimalzahlen. Die gleichen bekannten Ports wie beim Quellport können Sie auch als ASCII-Zeichen eingeben.	any = alle op port port 1 op port 2	any

Tab. 45: Am externen/internen Port eingehende/ausgehende IP-Pakete

Parameter	Bedeutung	Wertebereich	Voreinstellung
Protokoll	Folgende Protokolle können Sie als ASCII-Zeichen eingeben: ▶ `any` Beliebiges Layer 4-Protokoll ▶ `tcp` Transmission Control Protocol (RFC 793) ▶ `udp` User Datagram Protocol (RFC 768) ▶ `icmp` Internet Control Message Protocol (RFC 792) ▶ `igmp` Internet Group Management Protocol (RFCs 1112 (v1), 2236 (v2), 3376 (v3)) ▶ `ipip` IP in IP Tunneling (RFC 1853) ▶ `esp` IPsec Encapsulated Security Payload (RFC 2406) ▶ `ah` IPsec Authentication Header (RFC 2402) ▶ `ipv6-icmp` Internet Control Message Protocol for IPv6 (RFC 4443) ▶ `<0 - 255>` Nr. des Layer 4-Protokolls im IP-Header **Anmerkung:** Bei den Protokollen udp und tcp haben Sie die Möglichkeit, in den Spalten „Quellport“ und „Zielport“ die Protokoll-Ports anzugeben. Für andere Protokollen tragen Sie bei „Quellport“ und „Zielport“ `any` ein. **Anmerkung:** Die stateful Firewall unterstützt die Protokolle tcp, udp und icmp.	`any` = alle, `tcp`, `udp`, `icmp`, (außerdem: `igmp`, `ipip`, `esp`, `ah`, `ipv6-icmp`, `<0 - 255>`) **Anmerkung:** Sie können die Protokolle `any`, `tcp`, `udp` und `icmp` aus der Liste auswählen. Geben Sie die Protokolle `igmp`, `ipip`, `esp`, `ah`, `ipv6-icmp` und `<0 - 255>` von Hand ein.	any
Aktion	Aktion, die die Firewall durchführt, wenn die Regel zutrifft.	accept, drop, reject	drop (eingehend) accept (ausgehend)

Tab. 45: Am externen/internen Port eingehende/ausgehende IP-Pakete

Parameter	Bedeutung	Wertebereich	Voreinstellung
Log	Eintrag in die Ereignis-Liste, wenn die Firewall die Regel anwendet. Ggf. sendet das Gerät zusätzlich einen Trap. **Anmerkung:** Die Einstellung `logAndTrap` kann große Mengen an Trap-Datenverkehr erzeugen. Dies gilt besonders dann, wenn das Senden des Traps wieder einen Match der Firewall-Regel auslöst (z.B. wenn der Trap-Host ist nicht erreichbar ist und ein Router mit einer ICMP-Nachricht antwortet).	`enable`, `disable`, `logAndTrap`	`disable`
Fehler	Zeigt die letzte Meldung bei einem erfolglosen Versuch, den Tabelleneintrag zu aktivieren (typischerweise ein erkannter Syntaxfehler).		

Tab. 45: Am externen/internen Port eingehende/ausgehende IP-Pakete

ICMP Typ	Name	ICMP Code	Name	Referenz
0	Echo Reply			RFC792
		0	No Code	RFC792
3	Destination Unreachable			RFC792
		0	Net Unreachable	RFC792
		1	Host Unreachable	RFC792
		2	Protocol Unreachable	RFC792
		3	Port Unreachable	RFC792
		4	Fragmentation Needed and Don't Fragment was Set	RFC792
		5	Source Route Failed	RFC792
		6	Destination Network Unknown	RFC1122
		7	Destination Host Unknown	RFC1122
		8	Source Host Isolated	RFC1122
		9	Communication with Destination Network is Administratively Prohibited	RFC1122
		10	Communication with Destination Host is Administratively Prohibited	RFC1122
5	Redirect			RFC792
		0	Redirect Datagram for the Network (or subnet)	RFC792
		1	Redirect Datagram for the Host	RFC792
		2	Redirect Datagram for the Type of Service and Network	RFC792
		3	Redirect Datagram for the Type of Service and Host	RFC792
8	Echo			RFC792
		0	No Code	RFC792
9	Router Advertisement			RFC1256
		0	Normal router advertisement	RFC3344
		16	Does not route common traffic	RFC3344
10	Router Solicitation			RFC1256
		0	No Code	RFC1256
11	Time Exceeded			RFC792
		0	Time to Live exceeded in Transit	RFC792
		1	Fragment Reassembly Time Exceeded	RFC792

Tab. 46: ICMP-Typen und -Codes

Anmerkung: Die Firewall unterstützt bis zu 1024 IP-Regeln. Im Dialog `Diagnose:IP-Firewall-Liste` finden Sie die Zusammenfassung der aktiven Regeln.

4.1.4 Ein- und ausgehende MAC-Pakete

Die Firewall bietet Ihnen die Möglichkeit, am externen und internen Port eingehende MAC-Pakete zu prüfen auf:

- die Quell-MAC-Adresse
- die Ziel-MAC-Adresse
- das Typ-Feld des MAC-Datenpaketes

Transparent-Modus
Im Transparent-Modus haben folgende Einstellungen Vorrang vor den Einträgen in den MAC-Paketfiltern.

- „HiDiscovery-Relay“ im Dialog `Grundeinstellungen:Netz:Transparent-Modus`.
- „RSTP“ im Dialog `Erweitert:Paketweiterleitung`.
- „GMRP“ im Dialog `Erweitert:Paketweiterleitung`.
- „DHCP“ im Dialog `Erweitert:Paketweiterleitung`.

Diese Eigenschaft erspart Ihnen das Anlegen von speziellen MAC-Paket-Filterregeln für diese Anwendungsfälle.

Router-Modus
Im Router-Modus vermittelt die Firewall ausschließlich IP-Pakete. Andere Pakete werden verworfen, mit Ausnahme von Broadcast- und Multicast-Paketen. Die Regeln für MAC-Pakete greifen dennoch, wenn ein IP-Paket an ein Interface der Firewall adressiert ist.
Für eine bessere Vermittlungsleistung der Firewall können Sie im Router-Modus die Regeln für MAC-Pakete deaktivieren.

Sie können Regeln erstellen, löschen, bearbeiten und ihre Reihenfolge verändern. Markieren Sie zum Verschieben eine oder mehrere zusammenhängende Zeilen und verschieben Sie die Selektion mit den Schaltflächen „↑“ oder „↓“. Außerdem können Sie eine Regel duplizieren (klonen) und sie gleich darauf bearbeiten.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Index	Fortlaufender Zeilenindex.		-
Beschreibung	Beliebige Beschreibung dieses Eintrags	0-127 ASCII-Zeichen	
Aktiv	Aktivieren/Deaktivieren der Regel	ein/aus	aus
Quelladresse	MAC-Adresse der eigentlichen Quelle des Datenpaketes. Eingabeformat: `11:22:33:44:55:66` Die Eingabe von „?“ ermöglicht den Einsatz von Wildcards. Beispiel: `1?:22:??:44:55:6?`.		
Zieladresse	MAC-Adresse des eigentlichen Zieles des Datenpaketes.Eingabeformat: `11:22:33:44:55:66` Die Eingabe von „?“ ermöglicht den Einsatz von Wildcards. Beispiel: `1?:22:??:44:55:6?`.		
Protokoll	Protokoll im Typ-Feld des MAC-Datenpaketes		any
Aktion	Aktion, die die Firewall durchführt, wenn die Regel zutrifft.	accept, drop	drop (eingehend) accept (ausgehend)
Log	Eintrag in die Ereignis-Liste, wenn die Firewall die Regel anwendet. Ggf. sendet das Gerät zusätzlich einen Trap. **Anmerkung:** Die Einstellung `logAndTrap` kann große Mengen an Trap-Datenverkehr erzeugen. Dies gilt besonders dann, wenn das Senden des Traps wieder einen Match der Firewall-Regel auslöst (z.B. wenn der Trap-Host ist nicht erreichbar ist und ein Router mit einer ICMP-Nachricht antwortet).	`enable`, `disable`, `logAndTrap`	`disable`
Fehler	Zeigt die letzte Meldung bei einem erfolglosen Versuch, den Tabelleneintrag zu aktivieren (typischerweise ein erkannter Syntax-fehler).		

Tab. 47: Am externen/internen Port eingehende/ausgehende MAC-Pakete

Anmerkung: Die Firewall unterstützt bis zu 256 MAC-Regeln. Im Dialog `Diagnose:MAC-Firewall-Liste` finden Sie die Zusammenfassung der aktiven Regeln.

4.1.5 Eingehende PPP-Pakete

Die Firewall bietet Ihnen die Möglichkeit, am externen Port eingehende PPP-Pakete zu prüfen auf:

- den logischen Port
- die Quell-IP-Adresse
- den logischen Zielport
- die Ziel-IP-Adresse
- das Übertragungsprotokoll

Sie haben die Möglichkeit, bei jedem Paket, das mit keiner der Regeln der Tabelle übereinstimmt, sondern nur mit der unsichtbaren Default-Regel „alles verwerfen“, einen Log-Eintrag zu erzeugen. Aktivieren Sie dazu die Einstellung „Log bei Nichtübereinstimmung“.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Index	Fortlaufender Zeilenindex.		-
Beschreibung	Beliebige Beschreibung dieses Eintrags	0-127 ASCII-Zeichen	
Aktiv	Aktivieren/Deaktivieren der Regel	ein/aus	aus
Quelladresse (CIDR)	IP-Adresse mit Netzmaske (CIDR) der eigentlichen Quelle des Datenpaketes	IP-Adresse mit Netzmaske, any = alle, me = eigene IP-Adresse	any
Quellport	Logischer Quellport des Datenpaketes Zur Auswahl mehrerer Ports können Sie auch Operatoren (op) verwenden: = gleich != ungleich < kleiner <= kleiner gleich > größer >= größer gleich >< innerhalb <> außerhalb Verwenden Sie für die Portbezeichnung Dezimalzahlen. Folgende bekannte Ports können Sie auch als ASCII-Zeichen eingeben: 7 tcp/udp: echo 9 tcp/udp: discard 20 tcp :ftp-data 21 tcp :ftp 22 tcp/udp: ssh 23 tcp :telnet 53 tcp/udp: domain 67 tcp/udp: bootps 68 tcp/udp: bootpc 69 udp : tftp 80 tcp/udp: www, http 88 tcp/udp: kerberos 115 tcp : sftp 123 tcp : ntp 161 udp : snmp 162 udp : snmp-trap 179 tcp/udp: bgp 389 tcp/udp: ldap 443 tcp/udp: https	any = alle op port or port 1 op port 2	any

Tab. 48: Am externen Port eingehende PPP-Pakete

Parameter	Bedeutung	Wertebereich	Voreinstellung
Zieladresse (CIDR)	IP-Adresse mit Netzmaske (CIDR) des eigentlichen Ziels des Datenpaketes	IP-Adresse mit Netzmaske, any = alle, me = eigene IP-Adresse	
Zielport	Logischer Zielport des Datenpaketes Zur Auswahl mehrerer Ports können Sie die gleichen Operatoren wie beim Quellport verwenden: Verwenden Sie für die Portbezeichnung Dezimalzahlen. Die gleichen bekannten Ports wie beim Quellport können Sie auch als ASCII-Zeichen eingeben.	any = alle op port port 1 op port 2	any

Tab. 48: Am externen Port eingehende PPP-Pakete

Parameter	Bedeutung	Wertebereich	Voreinstellung
Protokoll	Folgende Protokolle können Sie als ASCII-Zeichen eingeben: ▶ `any` Beliebiges Layer 4-Protokoll ▶ `tcp` Transmission Control Protocol (RFC 793) ▶ `udp` User Datagram Protocol (RFC 768) ▶ `icmp` Internet Control Message Protocol (RFC 792) ▶ `igmp` Internet Group Management Protocol (RFCs 1112 (v1), 2236 (v2), 3376 (v3)) ▶ `ipip` IP in IP Tunneling (RFC 1853) ▶ `esp` IPsec Encapsulated Security Payload (RFC 2406) ▶ `ah` IPsec Authentication Header (RFC 2402) ▶ `ipv6-icmp` Internet Control Message Protocol for IPv6 (RFC 4443) ▶ `<0 - 255>` Nr. des Layer 4-Protokolls im IP-Header **Anmerkung:** Bei den Protokollen udp und tcp haben Sie die Möglichkeit, in den Spalten „Quellport“ und „Zielport“ die Protokoll-Ports anzugeben. Für andere Protokollen tragen Sie bei „Quellport“ und „Zielport“ `any` ein. **Anmerkung:** Die stateful Firewall unterstützt die Protokolle tcp, udp und icmp.	`any` = alle, `tcp`, `udp`, `icmp`, (außerdem: `igmp`, `ipip`, `esp`, `ah`, `ipv6-icmp`, `<0 - 255>`) **Anmerkung:** Sie können die Protokolle `any`, `tcp`, `udp` und `icmp` aus der Liste auswählen. Geben Sie die Protokolle `igmp`, `ipip`, `esp`, `ah`, `ipv6-icmp` und `<0 - 255>` von Hand ein.	any
Aktion	Aktion, die die Firewall durchführt, wenn die Regel zutrifft.	`accept`, `drop`, `reject`	accept

Tab. 48: Am externen Port eingehende PPP-Pakete

Parameter	Bedeutung	Wertebereich	Voreinstellung
Log	Eintrag in die Ereignis-Liste, wenn die Firewall die Regel anwendet. Ggf. sendet das Gerät zusätzlich einen Trap. **Anmerkung:** Die Einstellung `logAndTrap` kann große Mengen an Trap-Datenverkehr erzeugen. Dies gilt besonders dann, wenn das Senden des Traps wieder einen Match der Firewall-Regel auslöst (z.B. wenn der Trap-Host ist nicht erreichbar ist und ein Router mit einer ICMP-Nachricht antwortet).	`enable`, `disable`, `logAndTrap`	`disable`
Fehler	Zeigt die letzte Meldung bei einem erfolglosen Versuch, den Tabelleneintrag zu aktivieren (typischerweise ein erkannter Syntax-fehler).		

Tab. 48: Am externen Port eingehende PPP-Pakete

Anmerkung: Die Firewall unterstützt bis zu 1024 IP-Regeln. Im Dialog `Diagnose:IP-Firewall-Liste` finden Sie die Zusammenfassung der aktiven Regeln.

4.2 NAT – Network Address Translation

Die Firewall bietet Ihnen folgende Funktionen des Network Address Translation Protokolls:

- IP-Masquerading
- 1:1-NAT
- Portweiterleitung

Das 1:1-NAT bietet Ihnen die Möglichkeit, Kommunikations-Verbindungen in beide Richtungen aufzubauen.

4.2.1 Allgemeine NAT-Einstellungen

Die Einstellungen in diesem Dialog gelten für alle NAT-Verfahren gemeinsam.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Maximale Anzahl zugeordneter Verbindungen	Summe der zugeordneten Verbindungen aller NAT-Verfahren, die die Firewall maximal zulässt.	0-4.096	1.024
Zeitbegrenzung für bestehende TCP-Verbindungen	Zeitdauer in Sekunden, wie lange eine aktive TCP-Verbindung bestehen darf, bevor die Firewall die TCP-Verbindung unterbricht.	0-2.147.483.647	3.600
Paketversand am Empfangs-Interface erlauben	Aktivieren Sie diese Einstellung, wenn Sie der Firewall erlauben möchten, ein empfangenes Paket nach der NAT-Bearbeitung am selben Interface wieder auszusenden. Diese Einstellung ist ausschließlich in speziellen Sonderfällen nötig.	ein/aus	aus

Tab. 49: Allgemeine NAT-Einstellungen

4.2.2 IP-Masquerading

Dieser Dialog bietet Ihnen die Möglichkeit, bis zu 128 interne Netze in die Network-Address-Translation mit einzubeziehen.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Index	Fortlaufender Zeilenindex.		-
Beschreibung	Beliebige Beschreibung dieses Eintrags	0-127 ASCII-Zeichen	
Aktiv	Aktivieren/Deaktivieren der Regel	ein/aus	aus
Internes Netz (CIDR)	IP-Adresse mit Netzmaske (CIDR) des Internen Netzes, z.B. 10.1.2.0/24	IP-Adresse mit Netzmaske	192.168.1.0/24
FTP	Aktives FTP aus dem internen Netz zulassen	ein/aus	aus
Fehler	Zeigt die letzte Meldung bei einem erfolglosen Versuch, den Tabelleneintrag zu aktivieren (typischerweise ein erkannter Syntax-fehler).		

Tab. 50: IP-Masquerading

4.2.3 1:1-NAT

Dieser Dialog bietet Ihnen die Möglichkeit, bis zu 128 Einträge für eine 1:1-Adressenübersetzung einzutragen, zu bearbeiten oder zu löschen. Sie können Einträge für einzelne Endgeräte mit einer 32 Bit langen Netzmaske und Einträge für ganze Netzbereiche mit einer entsprechend kürzeren Netzmaske erstellen.

Bei 1:1-NAT arbeitet das Gerät als Router und ordnet für ein Endgerät im internen Netz eine weitere IP-Adresse im externen Netz zu. Dazu beantwortet das Gerät als Proxy die ARP-Anfragen für die zusätzliche IP-Adresse im externen Netz. Bei ausgehenden Datenpaketen ersetzt das Gerät die interne Quell-IP-Adresse des Endgerätes durch dessen externe IP-Adresse. Bei eingehenden Paketen ersetzt es die externe Ziel-IP-Adresse durch die interne IP-Adresse.

Anmerkung: Bevor Sie 1:1-NAT einrichten, stellen Sie sicher, dass die IP-Adresse im externen (mit Richtungsumkehr: im internen) Netz unbenutzt ist.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Index	Fortlaufender Zeilenindex.		-
Beschreibung	Beliebige Beschreibung dieses Eintrags	0-127 ASCII-Zeichen	
Aktiv	Aktivieren/Deaktivieren der Regel	ein/aus	aus
Internes Netz	IP-Adresse des internen Netzes bzw. die kleinste IP-Adresse des Netzbereiches des inneren Netzes	IP-Adresse	192.168.1.1
Externes Netz	IP-Adresse des externen Netzes bzw. die kleinste IP-Adresse des Netzbereiches des externen Netzes	IP-Adresse	10.0.1.1
Netzmaske	Netzmaske für den zu übersetzenden Bereich	1-32	32
FTP	Aktives FTP aus dem internen Netz zulassen	ein/aus	aus
Richtungsumkehr	Zuordnung einer zusätzlichen IP-Adresse (per Proxy-ARP) für ein externes Endgerät am internen Interface statt für ein internes Endgerät am externen Interface. Dadurch können Endgeräte im internen Netz ohne Gateway-Einträge mit externen Endgeräten kommunizieren. **Anmerkung:** Bevor Sie inverses 1:1-NAT einrichten, stellen Sie sicher, dass die IP-Adresse im internen Netz unbenutzt ist.	ein/aus	aus
Double-NAT	Bei Double-NAT ersetzt das Gerät bei umgesetzter Quelladresse in den Paketen zusätzlich auch die Zieladresse, wenn eine entsprechende Regel vorhanden ist. Dadurch können Endgeräte sowohl im internen als auch im externen Netz ohne Gateway-Einträge mit Endgeräten im anderen Netz kommunizieren. **Anmerkung:** Tragen Sie für die Ersetzung der Ziel-Adresse eine weitere Regel für die Adressübersetzung des externen Endgerätes ein. Aktivieren Sie „Output“ (Double-NAT). Aktivieren Sie außerdem für diese zweite Regel die Invertierung.	ein/aus	aus
Fehler	Zeigt die letzte Meldung bei einem erfolglosen Versuch, den Tabelleneintrag zu aktivieren (typischerweise ein erkannter Syntaxfehler).		

Tab. 51: 1:1-NAT

Das Gerät bietet Ihnen die Möglichkeit, 1:1-NAT mit der Router-Redundanz zu kombinieren (siehe auf Seite 165 „Router-Redundanz“).

4.2.4 Port-Weiterleitung

Ein Gerät kann aus dem externen Netz eine Kommunikation zu einem Gerät im internen Netz aufbauen, wenn Sie zuvor in der Tabelle die Weiterleitungsbedingungen eingetragen haben.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Index	Fortlaufender Zeilenindex.		-
Quelladresse (CIDR)	IP-Adresse mit Netzmaske (CIDR) der eigentlichen Quelle des Datenpaketes	IP-Adresse mit Netzmaske, `any` = alle	`any`

Quellport	Logischer Quellport des Datenpaketes
	Sie können optional den Operator „=“ verwenden:
	`=` gleich
	Verwenden Sie für die Portbezeichnung Dezimalzahlen. Folgende bekannte Ports können Sie auch als ASCII-Zeichen eingeben:
	`7 tcp/udp: echo`
	`9 tcp/udp: discard`
	`20 tcp : ftp-data`
	`21 tcp : ftp`
	`22 tcp/udp: ssh`
	`23 tcp : telnet`
	`53 tcp/udp: domain`
	`67 tcp/udp: bootps`
	`68 tcp/udp: bootpc`
	`69 udp : tftp`
	`80 tcp/udp: www, http`
	`88 tcp/udp: kerberos`
	`115 tcp : sftp`
	`123 tcp : ntp`
	`161 udp : snmp`
	`162 udp : snmp-trap`
	`179 tcp/udp: bgp`
	`389 tcp/udp: ldap`
	`443 tcp/udp: https`
		0..65.535
		Syntax:
		`= port-nr.`
		or
		`= port-id`
		e. g.: `= http`
			`any`

Eingangsadresse	Ziel-Adresse des Datenpakets, das am externen Port zur Weiterleitung ankommt. `%extern` kennzeichnet die IP-Adresse des externen Ports	`%extern` oder IP-Adresse	`%extern`

Tab. 52: Portweiterleitung

Parameter	Bedeutung	Wertebereich	Voreinstellung

Eingangsport	Logischer Ziel-Port des Datenpakets, das am externen physischen Port zur Weiterleitung ankommt.
	Verwenden Sie für die Portbezeichnung Dezimalzahlen. Folgende bekannte Ports können Sie auch als ASCII-Zeichen eingeben:
	`7 tcp/udp: echo`
	`9 tcp/udp: discard`
	`20 tcp :ftp-data`
	`21 tcp :ftp`
	`22 tcp/udp: ssh`
	`23 tcp :telnet`
	`53 tcp/udp: domain`
	`67 tcp/udp: bootps`
	`68 tcp/udp: bootpc`
	`69 udp : tftp`
	`80 tcp/udp: www, http`
	`88 tcp/udp: kerberos`
	`115 tcp : sftp`
	`123 tcp : ntp`
	`161 udp : snmp`
	`162 udp : snmp-trap`
	`179 tcp/udp: bgp`
	`389 tcp/udp: ldap`
	`443 tcp/udp: https`
		0..65.535	`80`

Weiterleitungs-adresse	IP-Adresse des Gerätes im internen Netz, für das das Datenpaket bestimmt ist.		127.0.0.1
Weiterleitungsport	Logischer Port des Gerätes im internen Netz, für das das Datenpaket bestimmt ist. Die gleichen bekannten Ports wie beim Eingangsport können Sie auch als ASCII-Zeichen eingeben.	0..65.535	80
Protokoll	`tcp` Transmission Control Protocol (RFC 793) `udp` User Datagram Protocol (RFC 768) `icmp` Internet Control Message Protocol (RFC 792)	tcp, udp, icmp	tcp
Log	Eintrag in die Ereignis-Liste, wenn die Firewall die Regel anwendet.	ja, nein	nein
Beschreibung	Beliebige Beschreibung dieses Eintrags	0-127 ASCII-Zeichen	

Tab. 52: Portweiterleitung

Parameter	Bedeutung	Wertebereich	Voreinstellung
Aktiv	Aktivieren/Deaktivieren der Regel	ein/aus	aus
Fehler	Zeigt die letzte Meldung bei einem erfolglosen Versuch, den Tabelleneintrag zu aktivieren (typischerweise ein erkannter Syntax-fehler).		

Tab. 52: Portweiterleitung

Anmerkung: Die Firewall unterstützt bis zu 1024 IP-Regeln. Im Dialog `Diagnose:IP-Firewall-Liste` finden Sie die Zusammenfassung der aktiven Regeln.

4.3 Unterstützung beim Schutz vor Denial of Service (DoS)

Diese Funktion unterstützt Sie beim Schutz Ihres Netzes und Ihres Servers vor einem unerlaubten Zugriff durch eine Überflutung mit TCP-Verbindungen, Ping-Paketen und ARP-Paketen.

Anmerkung: Passen Sie die in den Voreinstellungen festgelegten Werte den tatsächlich benötigten TCP-Verbindungen, Ping-Paketen und ARP-Paketen in Ihrem Netz an. Das Gerät bietet Ihnen außerdem die Möglichkeit, bei Überschreitung einer Grenze einen Log-Eintrag zu erzeugen. Dies können Sie für jede Grenze gesondert einstellen.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Max eingehende TCP-Verbindungen pro s	Maximale Anzahl neuer (SYN-Flag gesetzt) am externen Port eingehender TCP-Verbindungen pro Sekunde	1-999.999	25
Max. ausgehende TCP-Verbindungen pro s	Maximale Anzahl neuer (SYN-Flag gesetzt) am internen Port eingehender TCP-Verbindungen pro Sekunde	1-999.999	75
Max. eingehende Ping-Pakete pro s	Maximale Anzahl am externen Port eingehender Ping-Pakete pro Sekunde	1-999.999	3
Max. ausgehende Ping-Pakete pro s	Maximale Anzahl am internen Port eingehender Ping-Pakete pro Sekunde	1-999.999	5
Max. eingehende ARP-Pakete pro s	Maximale Anzahl am externen Port eingehender ARP-Pakete pro Sekunde	1-999.999	500
Max. ausgehende ARP-Pakete pro s	Maximale Anzahl am internen Port eingehender ARP-Pakete pro Sekunde	1-999.999	500

Tab. 53: Einstellungen zur Unterstützung beim Schutz vor Denial of Service

4.4 Benutzer-Firewall

Die Benutzer-Firewall bietet Ihnen die Möglichkeit, bis zu 32 Firewall-Benutzer-Einträge zu erzeugen. Jeder Benutzer-Firewall-Eintrag enthält:

- einen Regelsatz, der definiert, welche Datenpakete die Firewall vermitteln darf und welche nicht.
- eine Liste der Benutzer, auf die die Firewall diese Regeln anwenden soll.
- eine Zeitgrenze zur Begrenzung der Benutzungsdauer.

Im Rahmen „Konfiguration“ des Dialogs können Sie

- die Benutzer-Firewall global ein- oder ausschalten, und
- die Gruppen-Authentifizierung für Benutzer ein- oder ausschalten.

Gruppen-Authentifizierung:
Die Gruppen-Authentifizierung bietet Ihnen die Möglichkeit, mehrere Benutzer über einen RADIUS-Server in Gruppen zu organisieren.
Wenn sich bei aktiver Gruppen-Authentifizierung ein Unbekannter bei der Benutzer-Firewall anmeldet, dann prüft die Firewall die Authenzität über den RADIUS-Server (siehe auf Seite 69 „Authentifizierungslisten“).
Bei erfolgreicher Authentifizierng schickt der RADIUS-Server ein „Accept“-Datenpaket mit dem Attribut „Filter-ID=<groupname>“ an die Firewall.
Verfügt die Firewall über ein Benutzer-Firewall-Konto mit diesem Gruppennamen, dann gewährt die Firewall dem Benutzer den Zugang.

Voraussetzung für die Benutzung der Benutzer-Firewall ist der Eintrag eines Benutzers im Dialog `Sicherheit:Externe Authentifizierung:Benutzer-Firewall-Konten`.
Um eine klare Zuordnung „Benutzer zu Benutzer-Firewall-Eintrag“ zu gewährleisten, können Sie jedem Benutzer genau einen Eintrag zuordnen. Einem Firewall-Benutzer-Eintrag können Sie mehrere Benutzer zuordnen.

Sie können Regeln erstellen, löschen, bearbeiten und ihre Reihenfolge verändern. Markieren Sie zum Verschieben eine oder mehrere zusammenhängende Zeilen und verschieben Sie die Selektion mit den Schaltflächen „↑“ oder „↓“. Außerdem können Sie eine Regel duplizieren (klonen) und sie gleich darauf bearbeiten.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Name	Eindeutiger Name zur Identifikation dieses Eintrags	0-32 ASCII-Zeichen	
Zeitgrenzentyp	Bestimmt den Start für das Dekrementieren der Zeitgrenze: `static`: Mit der Anmeldung des Benutzers beginnt das Dekrementieren der Zeitgrenze. `dynamic`: Nach der Abmeldung beginnt das Dekrementieren der Zeitgrenze.	`static`, `dynamic`	static
Quelladresse (CIDR)	IP-Adresse mit Netzmaske (CIDR) des Benutzers (siehe Tab. 55).	Unicast-IP-Adresse	%authorized_ip
Beschreibung	Beliebige Beschreibung dieses Eintrags	0-127 ASCII-Zeichen	
Aktiv	Aktivieren/Deaktivieren der Regel	ein/aus	aus

Tab. 54: Benutzer-Firewall-Einträge

Bearbeiten eines Benutzer-Firewall-Eintrags

Die Karteikarte `Grundeinstellungen` bietet Ihnen die Möglichkeit, allgemeine Vorgaben für diesen Benutzer-Firewall-Eintrag zu treffen.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Name	Beliebiger Name für diesen Eintrag.	0-32 ASCII-Zeichen	
Zeitgrenze [s]	Maximale Zeit für die Dauer des Zugriffs des Benutzers.	1-604.800 (7 Tage)	28.800 (8 h)
Zeitgrenzentyp	Bestimmt den Start für das Dekrementieren der Zeitgrenze: `static`: Mit der Anmeldung des Benutzers beginnt das Dekrementieren der Zeitgrenze. `dynamic`: Nach der Abmeldung beginnt das Dekrementieren der Zeitgrenze.	`static`, `dynamic`	static
Quelladresse	IP-Adresse des Benutzers. Wenn der Benutzer keine feste IP-Adresse hat, dann bietet Ihnen der Ausdruck `%authorized_ip` die Möglichkeit, als Quelladresse die IP-Adresse aus der Benutzeranmeldung zu übernehmen.	IP-Adresse, %authorized_ip	%authorized_ip
Beschreibung	Beliebige Beschreibung dieses Eintrags	0-127 ASCII-Zeichen	

Tab. 55: Grundeinstellungen

Die Karteikarte `Konten` bietet Ihnen die Möglichkeit, den oder die Benutzer zu benennen, für den oder die dieser Benutzer-Firewall-Eintrag gilt. Die Benutzer definieren Sie zuvor im Dialog `Sicherheit:Externe Authentifizierung:User-Firewall Konten`.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Kontoname	Name eines Benutzers aus der Tabelle `Sicherheit:Externe Authentifizierung:Benutzer-Firewall Konten`		
Aktiv	Aktivieren/Deaktivieren der Regel	ein/aus	aus

Tab. 56: Konten

Die Karteikarte `Regeln` bietet Ihnen die Möglichkeit, Regeln für diesen Benutzer-Firewall-Eintrag zu erstellen.

Parameter	Bedeutung	Wertebereich	Voreinstellung

Quellport	Logischer Quellport des Datenpaketes
	Zur Auswahl mehrerer Ports können Sie auch Operatoren (op) verwenden:
	= gleich
	!= ungleich
	< kleiner
	<= kleiner gleich
	> größer
	>= größer gleich
	>< innerhalb
	<> außerhalb
	Verwenden Sie für die Portbezeichnung Dezimalzahlen. Folgende bekannte Ports können Sie auch als ASCII-Zeichen eingeben:
	7 tcp/udp: echo
	9 tcp/udp: discard
	20 tcp :ftp-data
	21 tcp :ftp
	22 tcp/udp: ssh
	23 tcp :telnet
	53 tcp/udp: domain
	67 tcp/udp: bootps
	68 tcp/udp: bootpc
	69 udp : tftp
	80 tcp/udp: www, http
	88 tcp/udp: kerberos
	115 tcp : sftp
	123 tcp : ntp
	161 udp : snmp
	162 udp : snmp-trap
	179 tcp/udp: bgp
	389 tcp/udp: ldap
	443 tcp/udp: https
		any = alle
		`op port`
		or
		`port 1 op port 2`
			`any`

Zielnetz	IP-Adresse mit Netzmaske (CIDR) des Zielnetzes. Z.B. 10.1.2.0/24	IP-Adresse mit Netzmaske, any = alle, me = eigene IP-Adresse	

Tab. 57: Regeln

Parameter	Bedeutung	Wertebereich	Voreinstellung
Zielport	Logischer Zielport des Datenpaketes Zur Auswahl mehrerer Ports können Sie die gleichen Operatoren wie beim Quellport verwenden: Verwenden Sie für die Portbezeichnung Dezimalzahlen. Die gleichen bekannten Ports wie beim Quellport können Sie auch als ASCII-Zeichen eingeben.	any = alle op port port 1 op port 2	any
Protokoll	Folgende bekannte Protokolle können Sie als ASCII-Zeichen eingeben: `tcp` Transmission Control Protocol (RFC 793) `udp` User Datagram Protocol (RFC 768) `icmp` Internet Control Message Protocol (RFC 792)	`any`, `tcp`, `udp`, `icmp`	tcp
Log	Eintrag in die Ereignis-Liste, wenn die Firewall die Regel anwendet.	ja, nein	nein
Beschreibung	Beliebige Beschreibung dieses Eintrags	0-127 ASCII-Zeichen	
Aktiv	Aktivieren/Deaktivieren der Regel	ein/aus	aus

Tab. 57: Regeln

Anmerkung: Die Firewall unterstützt bis zu 1024 IP-Regeln. Im Dialog `Diagnose:IP-Firewall-Liste` finden Sie die Zusammenfassung der aktiven Regeln.

5 VPN – Virtuelles privates Netz

Zum Einrichten einer VPN-Verbindungen bietet Ihnen das Gerät einen Assistenten.
Dieser Assistent führt Sie schrittweise durch die Konfiguration einer VPN-Verbindung. Der Assistent wählt für Sie den nächsten Schritt in Abhängigkeit Ihrer Einstellungen, die Sie bisher getätigt haben.
Nach wie vor bietet Ihnen das Gerät die Möglichkeit, die Einstellungen unabhängig vom Assistenten in den einzelnen Dialogen durchzuführen oder zu bearbeiten.

5.1 Verbindungen

Dieser Dialog bietet Ihnen die Möglichkeit,

- bis zu 256 VPN-Verbindungen am externen Port anzulegen und sie mit Namen zu bezeichnen. Jede Zeile (Eintrag) in der Liste stellt eine VPN-Verbindung dar. Bis zu 64 der konfigurierten Verbindungen können gleichzeitig aktiv und/oder im Zustand `up` sein.
- ein Passwort für das ferngesteuerte Aktivieren/Deaktivieren einer Verbindung einzugeben.
- das Gerät anzuweisen, empfangene und lokale Zertifikate vor ihrer Verwendung zu überprüfen (Lieferzustand: „Zertifikatsüberprüfung“ eingeschaltet).
- die LED „VPN“ des EAGLE One-Gerätes zur Anzeige von aktiven VPN-Verbindungen zu verwenden (Lieferzustand: „VPN-LED-Statusanzeige“ ausgeschaltet).
- einen IP-Adressbereich zu definieren, aus dem der EAGLE One eine Adresse an die Clients von VPN-Verbindungen vergibt, die eine Adresse anfordern.
- die Quelle für die Aktivierung des Service Mode festzulegen.

Einen markierten VPN-Eintrag können Sie:

- Löschen
- Bearbeiten

Zu einem markierten Eintrag können Sie:

- Informationen anzeigen
- eine PKCS#12-Datei vom PC laden.

Den Namen einer VPN-Verbindung benötigen Sie zusammen mit dem Passwort, um eine VPN-Verbindung ferngesteuert zu aktivieren oder zu deaktivieren. Greifen Sie dazu auf folgenden URL des Geräts zu:

```
https://vpn:<password>@<firewall_ip>/nph-vpn.cgi?
  name=<connection>&cmd={up|down}
```

Dabei bedeuten:

- `<password>` : das im Dialog angebene Passwort
- `<firewall_ip>` : die IP-Adresse oder den Host-Namen des EAGLE One-Gerätes
- `<connection>` : den Namen einer VPN-Verbindung in der Tabelle
- `{up|down}` : `up`: VPN-Verb. aufbauen, `down`: VPN-Verb. abbauen

Beispiele:

```
https://vpn:test@10.1.1.1/nph-vpn.cgi?name=test1&cmd=up
```

```
https://vpn:two@fw2.local/nph-vpn.cgi?name=two&cmd=down
```

Das Feld „VPN-LED-Statusanzeige“ bietet Ihnen die Möglichkeit, die LED „VPN“ des EAGLE One-Gerätes zur Anzeige von aktiven VPN-Verbindungen zu verwenden.
Die einstellbaren Werte haben folgende Bedeutung:

Einstellung	LED VPN	Bedeutung
`aus`	leuchtet nicht	
`ein`		LED „VPN” des EAGLE One-Gerätes zur Anzeige von aktiven VPN-Verbindungen verwenden.
	leuchtet nicht	Einer der folgenden Fälle trifft zu: ▶ Keine VPN-Verbindung ist aktiv. ▶ Keine aktive VPN-Verbindung ist im Zustand `up`.
	leuchtet grün	Die LED leuchtet grün, wenn eine oder mehrere VPN-Verbindungen aktiv und im Zustand `up` sind.

Tab. 58: Bedeutung der Werte im Feld „VPN-LED-Statusanzeige “

Das Eingabefeld „Client-IP-Adressvergabe“ bietet Ihnen die Möglichkeit, einen IP-Adressbereich zu definieren. Fordert ein Client einer VPN-Verbindung eine Adresse an, dann weist der EAGLE One dem Client dynamisch eine Adresse aus diesem Bereich zu.
Die einstellbaren Werte haben folgende Bedeutung:

Parameter	Bedeutung	Wertebereich	Voreinstellung
Client-IP-Adressvergabe	IPv4-Adressbereich in CIDR-Notation.	Gültiger IPv4-Adressbereich in CIDR-Notation.	-

Tab. 59: IP-Adressbereich für VPN-Clients (CIDR)

Anmerkung: Achten Sie bei der Definition des Adressbereichs darauf, dass die Adressen mit den Verkehrs-Selektoren derjenigen VPNs kompatibel sind, aus denen Clients Adressen anfordern. So helfen Sie sicherzustellen, dass ein Client, der eine solche Adresse erhält, auch über das VPN kommunizieren kann.

Das Eingabefeld „Quelle für Service Mode“ bietet Ihnen die Möglichkeit, die Quelle festzulegen, die den Service-Modus startet.
Die einstellbaren Werte haben folgende Bedeutung:

Parameter	Bedeutung	Wertebereich	Voreinstellung

Quelle für Service Mode	Auswahl der Quelle, die den Service-Modus startet.	`powersupply`
		Der Service-Modus startet, wenn
		▶ die redundante Stromversorgung des Gerätes außer Funktion ist.
		▶ Sie die redundante Stromversorgung des Gerätes zu diesem Zweck ausschalten.
		
		`digitalinput-low`
		Der Service-Modus startet, wenn am digitalen Eingang die Eingangsspannung Low-Pegel (Zustand „0“) anliegt.
		
		`digitalinput-high`
		Der Service-Modus startet, wenn am digitalen Eingang die Eingangsspannung High-Pegel (Zustand „1“) anliegt.
			`powersupply`

Tab. 60: Bedeutung der Werte im Feld „Quelle für Service Mode“

Parameter	Bedeutung	Wertebereich	Voreinstellung
Index	Zeilenindex zur eindeutigen Identifikation einer Verbindung.		
Name	Beliebiger Name für diese Verbindung. Diesen Namen verwenden Sie auch im URL für das ferngesteuerte Aktivieren/ Deaktivieren der Verbindung.	0-128 ASCII-Zeichen	
Starten als	Ausgangsrolle zur Aushandlung des Schlüssel-Austauschs	responder initiator	responder

Tab. 61: Verbindungen

Parameter	Bedeutung	Wertebereich	Voreinstellung
Service Mode	Aktivieren/Deaktivieren des Service-Modus. Im Service-Modus aktiviert das Gerät automatisch eine oder mehrere vorkonfigurierte VPN-Verbindungen. Die Quelle, die den Service-Modus startet, legen Sie im Dialog `Virtuelles privates Netz:Verbindungen` im Eingabefeld „Quelle für Service Mode“ fest (siehe Tabelle 60 auf Seite 144). - Service Mode ein: Kreuzen Sie das Feld „Service Mode” für eine oder mehrere VPN-Verbindungen an, um den Service-Modus des Gerätes für diese Verbindung(en) einzuschalten. Konfigurieren Sie zuerst die angekreuzte(n) VPN-Verbindung(en), wie im Kapitel „Bearbeiten einer Verbindung“ auf Seite 147ff beschrieben. Das Gerät meldet Ihnen den Eintritt in den Service-Modus wie folgt: - Das Gerät erzeugt einen Ereignis-Log Eintrag: „System service mode is active.” (siehe auf Seite 170 „Ereignis-Log“). - Das Feld „Status“ beinhaltet bei aktivem Service-Modus den Wert `servicemode-up`. - Falls Sie die Funktion „VPN-LED-Statusanzeige“ aktiviert haben, leuchtet die LED „VPN“ wie in Tab. 58 beschrieben, wenn das Gerät die VPN-Verbindung(en) aktiviert hat. Das Gerät meldet Ihnen das Verlassen des Service-Modus mit einem Ereignis-Log Eintrag: „System service mode is not active”. - Service Mode aus: Entfernen Sie den Haken im Feld Service Mode, um den Service-Modus des Gerätes auszuschalten.	Ein/Aus	Aus
Aktiv	Aktivieren/Deaktivieren der Verbindung	Ein/Aus	Aus

Tab. 61: Verbindungen

Parameter	Bedeutung	Wertebereich	Voreinstellung
Status	Zustand der Verbindung	up/ down/ negotiation/ constructing/ dormant/ servicemode-up	-
Exchange Mode	`mainaggressive`: das Gerät verwendet beim Verbindungsaufbau als Initiator den main-Modus, als Responder akzeptiert es sowohl den main-, als auch den aggressive-Modus. `main`: das Gerät verwendet beim Verbindungsaufbau als `initiator` und `responder` nur den main-Modus. `aggressive`: das Gerät verwendet beim Verbindungsaufbau als `initiator` und `responder` nur den aggressive-Modus.	mainaggres-sive/ main/ aggressive	mainaggressive

Tab. 61: Verbindungen

Bearbeiten einer Verbindung

Die Karteikarte `Grundeinstellungen` bietet Ihnen die Möglichkeit, der Verbindung einen beliebigen Namen zu geben.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Name	Beliebiger Name für diese Verbindung. Diesen Namen verwenden Sie auch im URL für das ferngesteuerte Aktivieren/ Deaktivieren der Verbindung.	0-128 ASCII-Zeichen	

Tab. 62: Grundeinstellungen

Die Karteikarte `Authentisierung` bietet Ihnen die Möglichkeit, die Parameter einzustellen, die das Gerät benötigt, um sich am anderen Ende der VPN-Verbindung zu authentisieren.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Rahmen Schlüssel-Informationen	Parameter zum anzuwendenden Schlüssel		
Methode	Methode zur Schlüsselauswahl und -Übertragung	`psk` `x509rsa`	`psk`
Pre-Shared-Key (PSK)	Schlüssel, den beide Enden einer VPN-Verbindung zum Aufbau der Verbindung und zur Datenübertragung benötigen. Wenn Sie Verbindung zum Bearbeiten öffnen, zeigt die Firewall den PSK in Form von acht Sternen an. **Anmerkung:** Das Web-Interface verwendet die Zeichencodierung UTF-8, um den PSK mit dem Gerät auszutauschen. Verwenden Sie für den PSK ausschließlich Zeichen und Zeichencodierungen, welche die beteiligten Geräte gleich interpretieren. Schränken Sie nötigenfalls die verwendete Zeichenmenge auf ASCII ein (Zeichencodes 32-127).	6-128 beliebige ASCII-Zeichen	
PKCS#12-Datei vom PC laden	Eine PKCS#12-Datei ist ein Dateicontainer, der das CA-Zertifikat, das lokale Zertifikat und den privaten Schlüssel enthält (PEM-Dateien) enthält.		
Rahmen Identitäten	Typ der Information, den ein Endpunkt der VPN-Verbindung zur Identifikation benutzt.		
Lokaler Typ	Auswahl des lokalen Identifikationstyps	`default` `ipaddr` `keyid` `fqdn` `email` `asn1dn`	`default`
Lokale ID	Identifikation für den Schlüsselaustausch mit der Gegenstelle entsprechend des oben augewählten lokalen Typs.		

Tab. 63: Authentisierung

Parameter	Bedeutung	Wertebereich	Voreinstellung

Entfernter Typ	Auswahl des entfernten Identifikations-typs	`any`
		`ipaddr`
		`keyid`
		`fqdn`
		`email`
		`asn1dn`
			any

Entfernte ID	Akzeptierte Identifikation für den Schlüsselaustausch von der Gegenstelle entsprechend des oben ausgewählten entfernten Typs.		

Tab. 63: Authentisierung

Die in den Feldern „Lokaler Typ“ und „Entfernter Typ“ auswählbaren Identitäts-Typen haben folgende Bedeutung:

Identitäts-Typ	Bedeutung
`default`	Voreinstellung (bei PSK: `ipaddr`, bei: x509rsa: `asn1dn`)
`any`	Eine der zur Verfügung stehenden Möglichkeiten
`psk`	Pre-Shared-Key
`x509rsa`	X.509 RSA-Zertifikat
`ipaddr`	IP-Adresse des anderen Endes der VPN-Verbindung
`keyid`	Schlüssel-Identifikation
`fqdn`	Vollqualifizierter Domänennamen (Fully Qualified Domain Name)
`email`	E-Mail-Adresse einer vertrauenswürdigen Person
`asn1dn`	X.500 Distinguished Name (DN). Ist das Feld „Lokale ID“ in diesem Fall leer, dann verwendet die Firewall den DN aus dem Zertifikat.

Tab. 64: Bedeutung der Identitäts-Typen bei der Authentisierung

Die Karteikarte `Zertifikate` bietet Ihnen die drei Möglichkeiten, Zertifikate, die Sie eventuell für die Authentisierung benötigen, einzugeben:

- PKCS#12-Datei laden
  Eine PKCS#12-Datei ist ein Datencontainer, der das CA-Zertifikat, das lokale Zertifikat und den privaten Schlüssel enthält.
- PEM-Dateien laden
  Ein Zertifikat besteht aus dem CA-Zertifikat, dem lokalen Zertifikat und dem privaten Schlüssel. Eine PEM-Datei enthält einen dieser Teile.
- Das CA-Zertifikat, das lokale Zertifikat und den privaten Schlüssel von Hand eingeben.

Parameter	Bedeutung
PKCS#12-Datei vom PC laden	Eine PKCS#12-Datei ist ein Datencontainer, der einzelne Zertifikatsanteile enthält. Alternativ zur PKCS#12-Datei können sie unten die einzelnen Zertifikatsanteile in Form von PEM-Dateien laden.
Lokal	Einträge für das lokale Zertifikat
Zertifikat	Das lokale Zertifikat zur Authentisierung am anderen Ende der VPN-Verbindung
Passwort	Das Passwort für den privaten Schlüssel, falls er in verschlüsselter Form vorliegt. Wenn Sie Verbindung zum Bearbeiten öffnen, zeigt die Firewall den PSK in Form von acht Sternen an.
Privater Schlüssel	Der dem Zertifikat zugeordnete private Schlüssel.
Zertifizierungs-stelle (CA)	Eintrag für das Zertifikat der Zertifizierungsstelle.
Zertifikat	Zertifikat der Zertifizierungsstelle.
Entfernt	Eintrag für das Zertifikat des anderen Endes der VPN-Verbindung.
Zertifikat (optional)	Zertifikat des anderen Endes der VPN-Verbindung (falls gewünscht). Bei einer Verbindung zu einem EAGLE One mGuard geben Sie das Zertifikat des EAGLE One mGuard ein.

Tab. 65: Zertifikate

Die Karteikarte `IKE - Schlüssel-Austausch` bietet Ihnen die Möglichkeit, die Parameter für den Schlüssel-Austausch einzustellen.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Modus			
Protokoll	Anzuwendende Protokollversion für den Schlüssel-Austausch	auto v1 v2	auto
Starten als	Ausgangsrolle zur Aushandlung des Schlüssel-Austauschs	responder initiator	responder
DPD-Zeitbegrenzung	Dead Peer Detection. Zeit, nach welcher die Verbindung ungültig wird, sobald das andere Ende der Verbindung kein Lebenszeichen sendet.	0-86.400 s (24 h), wobei der Wert „0“ DPD ausschaltet.	120 Sekunden
Lebenszeit	Verwendungsdauer der zur Unterstützung des Schutzes von IKE-Protokollnachrichten verwendeten Schlüssel und damit die maximale Lebenszeit der IKE-Sicherheitsbeziehung (IKE-SA) selbst. Wählen Sie die Lebenszeit des Initiators kleiner oder gleich der Lebenszeit des Responders.	1-86.400 Sekunden (= 24 h)	28.800 Sekunden (8 h)
Kompatibilitätsmodus	Für LANCOM Client und Hirschmann EAGLE One mGuard.		aus
Algorithmen	Auswahl der zur verwendenden Verschlüsselungs- und Hash-Algorithmen für den Schlüsselaustausch.		

Schlüssel-Vereinbarung	Algorithmus zur Schlüssel-Vereinbarung.
	Die Firewall bietet die Einstellung „any“ an, wenn sie die Ausgangsrolle „responder“ hat.
	Gruppenzuordnung:
	modp768: DH-Group 1
	modp1024: DH-Group 2
	modp1536: DH-Group 5
	modp2048: DH-Group 14
	modp3072: DH-Group 15
	modp4096: DH-Group 16
		`any`
		`modp768`
		`modp1024`
		`modp1536`
		`modp2048`
		`modp3072`
		`modp4096`
			`modp1024`

Hash	Hash-Agorithmus.
	Die Firewall bietet die Einstellung „any“ an, wenn sie die Ausgangsrolle „responder“ hat.
		`any`
		`md5`
		`sha1`
			`sha1`

Tab. 66: IKE-Schlüssel-Austausch

Parameter	Bedeutung	Wertebereich	Voreinstellung

Integrität	Authentisierungsalgorithmus für IKE-Protokollnachrichten.
	Die Firewall bietet die Einstellung „any“ an, wenn sie die Ausgangsrolle „responder“ hat.
		`any`
		`hmacmd5`
		`hmacsha1`
			hmacsha1

Verschlüsselung	Algorithmus zur Verschlüsselung von IKE-Protokollnachrichten.
	Die Firewall bietet die Einstellung „any“ an, wenn sie die Ausgangsrolle „responder“ hat.
		`any`
		`des`
		`des3`
		`aes128`
		`aes192`
		`aes256`
			aes128

Endpunkte (Peers)	IP-Adressen der beiden Endpunkte der VPN-Verbindung		
Lokale IP-Adresse	Hostname (FQDN) oder IP-Adresse des lokalen Sicherheit-Gateways. Beim Wert „any“ benutzt die Firewall die erste IP-Adresse des externen Interfaces. Wenn diese Adresszuweisung per DHCP erfolgt, verzögert sich der Aufbau der VPN-Verbindung, bis eine gültige IP-Adresse zugewiesen ist. Bei Verwendung eines Hostnamens verzögert sich der Aufbau der VPN-Verbindung, bis der Hostname aufgelöst ist.	IP-Adresse, `any any`	
Entfernte IP-Adresse	Hostname (FQDN) oder IP-Adresse des entfernten Sicherheit-Gateways. Beim Wert „any“ akzeptiert die Firewall jede IP-Adresse, beim Aufbau einer IKE-Sicherheitsbeziehung als „Responder“ (Antwortender). Ebenso akzeptiert die Firewall ein Netzwerk in CIDR-Notation beim Aufbau einer IKE-Sicherheitsbeziehung als „Responder“. Als Initiator akzeptiert die Firewall solche Werte nicht. Bei Verwendung eines Hostnamens verzögert sich der Aufbau der VPN-Verbindung, bis der Hostname aufgelöst ist.	IP-Adresse, `any any`	

Tab. 66: IKE-Schlüssel-Austausch

Die in den Feldern „Protokoll“, „Starten als“, „Schlüsselvereinbarung“, „Hash“, „Integrität“ und „Verschlüsselung“ auswählbaren Werte haben folgende Bedeutung:

Wert	Bedeutung
`auto`	Automatische Auswahl
`v1`	IKE-Protokoll Version 1
`v2`	IKE-Protokoll Version 2
`responder`	IKE-Antwortender
`initiator`	IKE-Initiator
`modp...`	Angabe der Modular Exponentiation Group, verwendetes Modul beim Diffie-Hellman-Schlüsselaustausch.
`md5`	Message-Digest Algorithm 5, kryptografische Hash-Funktion
`sha1`	Secure Hash Algorithm 1, kryptografische Hash-Funktion
`hmacmd5`	Hashed Message Authentication Code, basierend auf MD5
`hmacsha1`	Hashed Message Authentication Code, basierend auf SHA1
`des`	DES (Data Encryption Standard)-Verschlüsselungsstandard
`aes`	AES (Advanced Encryption Standard)-Verschlüsselungsstandard

Tab. 67: Bedeutung der Werte bei IKE-Schlüssel-Austausch

Die Karteikarte `IPsec - Daten-Austausch` bietet Ihnen die Möglichkeit, die Parameter für den Daten-Austausch einzustellen.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Modus			
Betriebsart (Encapsulation)	Wahl der VPN-Betriebsart	`transport` `tunnel`	`transport`
NAT-T erzwingen	Network Address Translation - Traversal: Befinden sich im Übertragungsweg NAT-Router, trifft IPsec entsprechende Vorkehrungen. In diesem Fall adressiert IPsec IKE- und IPsec-Datenpakete an den Port 4.500 gemäß RFC 3948. Ist NAT-T eingeschaltet, dann adressiert die Firewall auf alle Fälle an den Port 4.500.	ein/aus	aus
Lebenszeit	Verwendungsdauer der zur Unterstützung des Schutzes von Datenpaketen verwendeten Schlüssel und damit die maximale Lebenszeit der IPsec-Sicherheitsbeziehung (IPsec-SA) selbst	1-28.800 (8 h)	3.600 (1 h)
Algorithmen	Auswahl der zur verwendenden Verschlüsselungs- und Hash-Algorithmen für den Schlüsselaustausch.		

Schlüssel-Vereinbarung	Auswahl eines Algorithmus´ zur Schlüssel-Vereinbarung.
	Die Firewall bietet die Einstellung „any“ an, wenn sie die Ausgangsrolle „responder“ hat.
	Gruppenzuordnung:
	modp768 DH-Group 1
	modp1024 DH-Group 2
	modp1536 DH-Group 5
	modp2048 DH-Group 14
	modp3072 DH-Group 15
	modp4096 DH-Group 16
		`any`
		`modp768`
		`modp1024`
		`modp1536`
		`modp2048`
		`modp3072`
		`modp4096`
		`none`
			`modp1024`

Integrität	Auswahl eines Algorithmus zum Integritätsschutz	`any`
		`md5`
		`sha1`
			`hmacsha1`

Verschlüsselung	Auswahl eines Algorithmus zur Datenverschlüsselung	`any`
		`des`
		`des3`
		`aes128`
		`aes192`
		`aes256`
			aes128

Tab. 68: IPsec - Daten-Austausch

Die in den Feldern „Betriebsart Encapsulation“, „Schlüsselvereinbarung“, „Integrität“ und „Verschlüsselung“ auswählbaren Werte haben folgende Bedeutung:

Wertebereich	Bedeutung
`modp...`	Angabe der Modular Exponentiation Group, verwendetes Modul beim Diffie-Hellman-Schlüsselaustausch.
`hmacmd5`	Hash Message Authentication Code, basierend auf MD5
`hmacsha1`	Hash Message Authentication Code, basierend auf SHA1
`des`	DES (Data Encryption Standard)-Verschlüsselungsstandard
aes	AES (Advanced Encryption Standard)-Verschlüsselungsstandard

Tab. 69: Bedeutung der Werte bei IPsec - Daten-Austausch

Die Karteikarte `IP-Netze` bietet Ihnen die Möglichkeit, die Parameter für die IP-Netze am internen Port, deren Daten über die VPN-Verbindung übertragen werden sollen, einzustellen.
Die Firewall vermittelt und verschlüsselt ausschließlich die Daten durch den Tunnel, die einem Eintrag in dieser Tabelle entsprechen. Andere Daten routet die Firewall gemäß den vorhandenen Einträgen in den Paketfiltern.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Index	Fortlaufender Zeilenindex.		-
Quelladresse (CIDR)	IP-Adresse mit Netzmaske (CIDR) der eigentlichen Quelle des Datenpaketes **Anmerkung:** Wenn Sie 2 Geräte per VPN miteinander verbinden, werden als lokale Quelladressen auch Netzadressen akzeptiert, die nicht mit den auf der Gegenseite eingetragenen Zieladressen identisch sind, sondern eine Untermenge dieser Zieladressen sind. **Beispiel:** Eine gültige Konfiguration ist, wenn Sie im lokalen Gerät als Quelladresse 192.168.2.0/24 eintragen und auf der Gegenseite als Zieladresse 192.168.1.0/20.	IP-Adresse mit Netzmaske, any = alle	any

Tab. 70: IP-Netze am internen Port

Parameter	Bedeutung	Wertebereich	Voreinstellung
Quellport	Logischer Quellport des Datenpaketes. Verwenden Sie für die Portbezeichnung Dezimalzahlen. Folgende bekannte Ports können Sie auch als ASCII-Zeichen eingeben: 7 tcp/udp: echo 9 tcp/udp: discard, sink, null 20 tcp: ftp-data 21 tcp: ftp 22 tcp/udp: ssh 23 tcp: telnet 53 tcp/udp: dns 67 tcp/udp: bootps 68 tcp/udp: bootpc 69 udp: tftp 80 tcp/udp: www, http 88 tcp/udp: kerberos, krb5 115 tcp: sftp 123 tcp/udp: ntp 161 udp: snmp 162 udp: snmp-trap, snmptrap 179 tcp/udp: bgp 389 tcp/udp: ldap 443 tcp/udp: https	any = alle op port op port 1 op port 2	any
Zieladresse (CIDR)	IP-Adresse mit Netzmaske (CIDR) des eigentlichen Ziels des Datenpaketes	IP-Adresse mit Netzmaske, any = alle	
Zielport	Logischer Zielport des Datenpaketes. Verwenden Sie für die Portbezeichnung Dezimalzahlen. Die gleichen bekannten Ports wie beim Quellport können Sie auch als ASCII-Zeichen eingeben.	any = alle op port op port 1 op port 2	any

Tab. 70: IP-Netze am internen Port

Parameter	Bedeutung	Wertebereich	Voreinstellung
Policy	Das EAGLE One-Gerät wendet diese Sicherheitsvorgaben für den Verkehr durch eine VPN-Verbindung. Das EAGLE One-Gerät unterstützt folgende Sicherheitsvorgaben: – `require`: Zum Aufbau einer VPN-Verbindung benötigt das EAGLE One-Gerät die Verschlüsselung der Daten. – `use`: Zum Aufbau einer VPN-Verbindung verwendet das EAGLE One-Gerät die Verschlüsselung, falls Sie eine Verschlüsselung gewählt haben. Andernfalls leitet das EAGLE One-Gerät die Daten unverschlüsselt weiter.	`require`, `use`	require
Protokoll	`tcp` Transmission Control Protocol (RFC 793) `udp` User Datagram Protocol (RFC 768) `icmp` Internet Control Message Protocol (RFC 792) **Anmerkung:** Wenn Sie eine andere Protokoll-Einstellung als die Standard-Einstellung `any` verwenden und den EAGLE One mit einer Gegenstelle verbinden, die nur eine veraltete Implementierung von IKEv1 unterstützt, aktivieren Sie beim EAGLE One zusätzlich den `Kompatibilitäts-modus` im Karteikartenreiter `IKE-Schlüssel-Austausch`, damit die Geräte eine Verbindung aufbauen können. Die beim EAGLE One eingestellten Bedingungen für den Traffic-Selektor werden auch im Kompatibilitätsmodus eingehalten.	`any` = alle, `tcp`, `udp`, `icmp`	any
Beschreibung	Beliebige Beschreibung dieses Eintrags	0-127 ASCII-Zeichen	
Gemappte Quelladress (CIDR)	Das EAGLE One-Gerät ersetzt die IP-Quelladresse der in die VPN-Verbindung gesendeten Daten durch eine IP-Adresse aus diesem Adressbereich. Voraussetzung: Protokoll = `any`		

Tab. 70: IP-Netze am internen Port

Parameter	Bedeutung	Wertebereich	Voreinstellung
Gemappte Zieladress (CIDR)	Das EAGLE One-Gerät ersetzt die IP-Zieladresse der aus der VPN-Verbindung empfangenen Daten durch eine IP-Adresse aus diesem Adressbereich. Voraussetzung: Protokoll = `any`		
Aktiv	Aktivieren/Deaktivieren der Regel	ein/aus	aus

Tab. 70: IP-Netze am internen Port

Löschen einer Verbindung

Die Firewall unterstützt Sie beim Schutz einer aktiven Verbindung vor einem Löschvorgang. Markieren Sie den zu löschenden, deaktivierten Eintrag einer Verbindung.
Klicken Sie „Eintrag löschen“.

6 Redundanz

Die Redundanzfunktionen bieten Ihnen die Möglichkeit, redundante Wege über eine redundante Firewall bereitzustellen.
Stellt die Firewall, die momentan vermittelt, eine Kommunikationsunterbrechung fest (z. B. einen unterbrochenen Link), sendet sie die Information an ihre Partner-Firewall, die darauf die Vermittlung übernimmt.

Abhängig von der Netz-Betriebsart-Einstellung bietet Ihnen die Firewall:
- Transparent-Redundanz
- Router-Redundanz

6.1 Transparent-Redundanz

Die Transparent-Redundanz-Funktion bietet Ihnen die Möglichkeit, die Firewall in den Pfad der redundanten Ring-/Netzkopplung einzubinden (siehe Anwender-Handbuch Redundanz-Konfiguration Ihres Hirschmann-Gerätes, das die redundante Kopplung unterstützt).
Die Transparent-Redundanz-Funktion können Sie einsetzen, wenn Sie die Firewall im Transparent-Modus betreiben.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Funktion			
	Die Transparent-Redundanz ein-/ausschalten. Voraussetzung: Im Dialog `Grundeinstellungen:Netz:Global` ist der Modus `transparent` ausgewählt.	An, Aus	Aus
Transparent-Modus			
Master- oder Slave-Port	Der Port des EAGLE One, der mit dem Master (über die Hauptleitung) oder mit dem Slave (über die redundante Leitung) der Ringkopplung verbunden ist. Der jeweils andere Port des EAGLE One ist mit dem entfernten Ring oder Netzwerk verbunden, in dem sich weder ein Ringkopplungs-Master noch ein -Slave befinden. Bei Einstellung external: Wenn die Verbindung am internen Port außer Funktion ist, dann schaltet die Firewall den externen Port ab. Bei Einstellung internal: Wenn die Verbindung am externen Port außer Funktion ist, dann schaltet die Firewall den internen Port ab.	internal, external	external
Firewall-Zustandstabellen-Synchronisation			

Tab. 71: Transparent-Redundanz

Parameter	Bedeutung	Wertebereich	Voreinstellung
IP-Adresse des Redundanzpartners	Die IP-Adresse identifiziert den Redundanzpartner, mit dem die Firewall ihre Zustandstabelle synchronisiert, damit dieser jederzeit alle Aufgaben übernehmen kann.	IPv4-Adresse	0.0.0.0
Kommunikation	Die Kommunikation zwischen den Redundanzpartnern ist aktiv/inaktiv. - Aktiv: Die Kommunikation zwischen Master und Slave ist aktiv. Der Master sendet Synchronisationspakete an den Slave und empfängt dessen Bestätigungspakete, wenn Datenverkehr über das Gerät geht. - Inaktiv: Es findet momentan keine Kommunikation statt. Stellen Sie sicher, dass keine Datenleitung oder Netzkomponente ausgefallen ist: Prüfen Sie den Layer 2-Redundanzstatus über die Switches im Pfad der redundanten Ring-/Netzkopplung, in den Sie die Firewall eingebunden haben (siehe Anwender-Handbuch Redundanz-Konfiguration Ihres Hirschmann-Gerätes, das die redundante Kopplung unterstützt).	Aktiv, Inaktiv	Inaktiv

Tab. 71: Transparent-Redundanz

Anmerkung: Die redundante Kopplung schaltet unmittelbar nach der Wiederherstellung der Hauptverbindung die Vermittlung von der redundanten Leitung zur Hauptleitung um. Waren zuvor beide Leitungen der Haupt-Firewall unterbrochen, dann konnten die beiden Firewalls ihre Zustandstabellen nicht synchronisieren.

Anmerkung: Wenn vom anderen System keine Pakete empfangen werden, kann dies verschiedene Ursachen haben:
☐ Zu diesem Zeitpunkt findet kein Datentransfer über das Gerät statt.
☐ Eine Datenleitung oder Netzkomponente ist außer Funktion.
Den tatsächlichen Zustand der Layer-2-Redundanz können Sie ausschließlich auf den Switches ermitteln.

6.2 Router-Redundanz

Die Router-Redundanz-Funktion bietet Ihnen die Möglichkeit, für die Firewall selbst eine redundante Firewall im Netz bereitzustellen. In diesem Fall fasst die Firewall-Router-Redundanz-Funktion zwei Firewalls zu einer virtuellen Firewall zusammen. Beide Firewalls besitzen ein gemeinsames virtuelles Interface, welches die jeweils aktive Firewall verwendet. Im Falle eines erkannten Fehlers übernimmt die redundante Firewall die Funktionen der ersten Firewall.

Voraussetzungen für den Einsatz der Router-Redundanz-Funktion:

- Der Router-Modus ist aktiv.
- Die Paketfilter- und NAT-Einstellungen der Firewall und der redundanten Firewall sind identisch.
- Die Router-Redundanz-Konfiguration der Firewall und der redundanten Firewall entsprechen sich.
- Die Einträge für die Ziele der ICMP-Host-Check-Funktion sind identisch und haben die gleiche Reihenfolge.
- Alle VPN-Verbindungen sind ausgeschaltet.
- Alle Geräte, die die Firewall als Gateway eingetragen haben, benutzen die virtuelle IP-Adresse der Firewall-Redundanz-Funktion.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Konfiguration			
Funktion An/Aus	Die Router-Redundanz ein-/ ausschalten. Voraussetzung: Im Dialog `Grundeinstel-lungen:Netz:Global` ist im Rahmen „Konfiguration“ der Modus `router` ausgewählt.	An, Aus	Aus
Priorität	Die Priorität dient der Bestimmung, welches Gerät die Redundanzfunktion übernimmt. Das Gerät mit der niedrigeren Priorität (kleinere Zahl) übernimmt die Redundanzfunktion. Bei gleicher Priorität regeln die Geräte automatisch, welches die Redundanzfunktion übernimmt.	1-255	100
Status	Anzeige des Redundanz-Zustandes.		
Internes Interface (Port 1)			
IP-Adresse	Anzeige der IP-Adresse des internen Interfaces (Port 1).		192.168.3.1
Virtuelle IP-Adresse	IP-Adresse des virtuellen Routers am internen Interface.	IP-Adresse	192.168.3.100
VRID	Die VRID (virtueller Router Identifikation) zur eindeutigen Kennzeichnung eines virtuellen Routers. Wählen Sie unterschiedliche VRIDs für das interne und das externe Interface.	1-255	1
IP-Adresse des Redundanzpartners	IP-Adresse des physikalischen Redundanzpartners, der Teil des virtuellen Routers ist.	IP-Adresse	192.168.3.153
Externes Interface (Port 2)			
IP-Adresse	Anzeige der IP-Adresse des externen Interfaces (Port 2).		10.0.0.10
Virtuelle IP-Adresse	IP-Adresse des virtuellen Routers am externen Interface.	IP-Adresse	10.0.0.100
VRID	Die VRID (virtueller Router Identifikation) zur eindeutigen Kennzeichnung eines virtuellen Routers. Wählen Sie unterschiedliche VRIDs für das interne und das externe Interface.	1-255	2
IP-Adresse des Redundanzpartners	Physikalische IP-Adresse des Redundanzpartners, der Teil des virtuellen Routers ist.	IP-Adresse	10.0.0.153

Tab. 72: Grundeinstellungen

Das Gerät bietet Ihnen die Möglichkeit, die Router-Redundanz mit 1:1-NAT zu kombinieren (siehe auf Seite 128 „1:1-NAT“).
Die ICMP-Host-Check-Funktion bietet Ihnen die Möglichkeit, die Erreichbarkeit von Geräten bei einzelnen Verbindungsunterbrechungen im Netz von der Firewall prüfen zu lassen. Die Firewalls entscheiden an Hand dieser Prüfung, welche Firewall die aktive Vermittlungsfunktion übernimmt.
Sie nutzen diese Funktion optimal, wenn Sie an jedem Port beider Firewalls mindestens einen Host zur Prüfung konfigurieren.

Arbeitsweise des ICMP-Host-Checks:
Stellt das Router-Redundanz-Protokoll der Firewalls fest, dass diese sich gegenseitig nicht mehr auf allen Interfaces erreichen können, beginnen die Firewalls mit dem ICMP-Host-Check. Dabei gehen die Firewalls für das betroffenen Interface die Host-Liste in aufsteigender Reihenfolge der Host-Indices solange durch, bis sie bei einem Host einen Unterschied in der Erreichbarkeit feststellen. Kann der momentane Router-Master einen bestimmten Host nicht erreichen, obwohl er vom Backup-Router aus erreichbar ist, tauschen die Firewalls ihre Redundanz-Rollen. Der momentane Backup-Router übernimmt dabei die Master-Rolle und der momentane Master-Router wird zum Backup-Router.

Voraussetzungen für den Einsatz der ICMP-Host-Check-Funktion:
- Verbinden Sie mit jedem Interface der Firewalls mindestens einen Host, der im Normalfall von beiden Firewalls aus erreichbar ist.
- Diese Hosts sind bei beiden Firewalls in der Liste eingetragen und die Host-Listen der Firewalls sind identisch.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Funktion An/Aus	Den ICMP-Host-Check ein-/ausschalten.	`An`, `Aus`	`Aus`
Status	Zustandsanzeige der Überprüfung der Erreichbarkeit der in der Tabelle eingetragenen Ping-Geräte.	`out of service`, `service enabled`, `host check running`	-
Index	Fortlaufender Zeilenindex.		-
Port	Port, an dem die Firewall die Ping-Abfrage zur Prüfung der Erreichbarkeit verschickt.	`internal`, `external`	`internal`
IP-Adresse	IP-Adresse des Gerätes, an welches die Firewall die Ping-Abfrage für die Prüfung der Erreichbarkeit verschickt.	Gültige IPv4-Host-Adresse	-
Aktiv	Aktivieren/Deaktivieren des Eintrags.	`Ein`, `Aus`	`Ein`

Tab. 73: ICMP Host Check

Die Werte der Status-Anzeige haben folgende Bedeutung:

- `out of service`: die ICMP-Host-Check-Funktion ist abgeschaltet.
- `not in router mode`: die Firewall befindet sich nicht im Router-Modus.
- `service enabled`: die Funktion ist eingeschaltet und wird momentan nicht gebraucht, da die Router-Redundanz kein Problem festgestellt hat.
- `host check running`: die Funktion ist eingeschaltet und die Firewall geht momentan die Host-Liste durch, da die Router-Redundanz ein Problem festgestellt hat.

7 Diagnose

Das Diagnose-Menü enthält folgende Tabellen und Dialoge:

- Ereignisse
  - Ereignis-Log
  - Syslog-Server
  - Ereignis-Einstellungen
  - Erweiterte Einstellungen
- Ports
  - Netzlast
  - Statistiktabelle
  - ARP-Einträge
- Topologie-Erkennung
- Gerätestatus
- Meldekontakt
- Alarme (Traps)
- Bericht
  - System-Information
- MAC-Firewall-Liste
- IP-Firewall-Liste
- Konfigurations-Check
- Erreichbarkeits-Test (Ping)

Diese Tabellen und Dialoge geben im Service-Fall dem Techniker die notwendigen Informationen zur Diagnose.

7.1 Ereignisse

Die Dialoge bieten Ihnen folgende Möglichkeiten:

- Ereignis-Log:
  Auswählen der zu loggenden Ereignisse, Anzeigen und Speichern der Ereignis-Log-Datei.

- Syslog-Server:
  Konfiguration der Syslog-Server-Einstellungen, um Ereignismeldungen auf einen Syslog-Server zu übertragen.

- Ereignis-Einstellungen:
  Auswählen, ab welchem Mindest-Schweregrad das Gerät Ereignisse in die Ereignis-Log-Datei übernimmt und welche davon es auf einen angeschlossenen ACA schreibt.

- Erweiterte Einstellungen:
  – SNMP-Anfragen als Ereignisse mitzuloggen
  – Konfiguration für persistente Log-Dateien

7.1.1 Ereignis-Log

Diese Funktion bietet Ihnen die Möglichkeit, die Anzeige des Ereignis-Logs zu filtern, damit diese nur die für Sie relevanten Ereignisse enthält.
Im Dialog `Ereignis-Log` legen Sie fest, welche Kategorien von Ereignissen im Log das Gerät in der Anzeige auflisten soll. Ereignisse anderer bekannter Kategorieren zeigt das Gerät dann nicht an. Der Ereignis-Log selbst wird durch die Filterung nicht verändert.
Welche Ereignisse das Gerät in den Ereignis-Log schreibt, legen sie in den Ereignis-Einstellungen (siehe auf Seite 173 „Ereignis-Einstellungen“) fest.

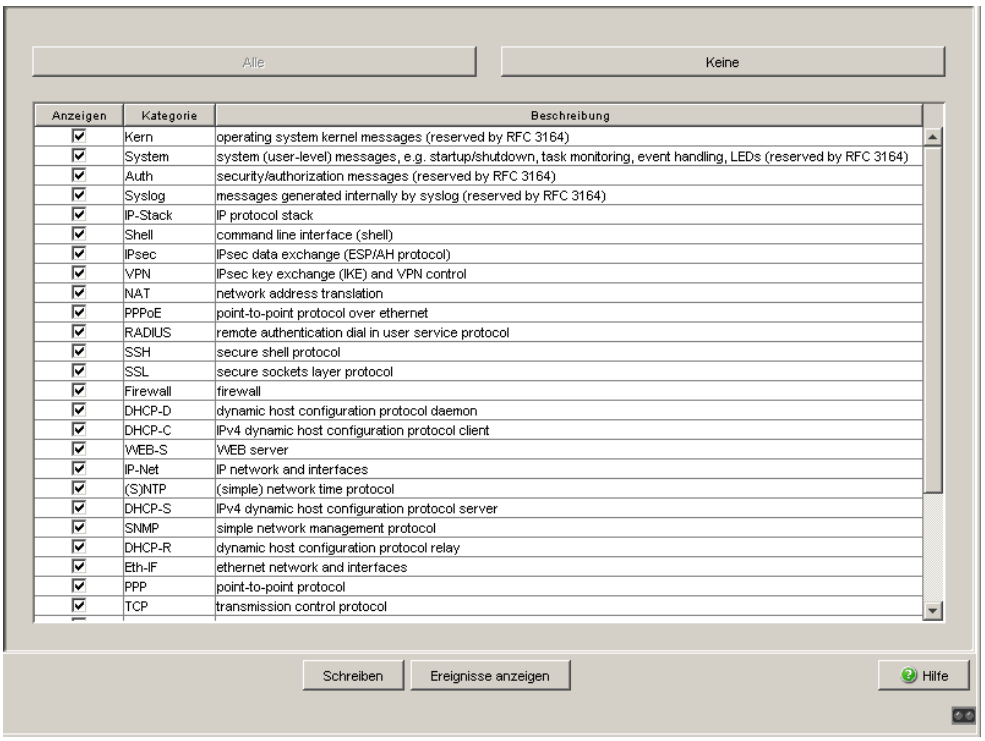


Abb. 27: Dialog Ereignis-Log

☐ Wählen Sie die Ereignis-Kategorien aus, die das Gerät in der Anzeige auflisten soll. Die Bedeutung der Kategorien entnehmen Sie dem Dialog Ereignis-Einstellungen (siehe Abb. 29).

☐ Klicken Sie auf „Schreiben“, um die ausgewählten Kategorien auf Ihrer Workstation (nicht auf dem Gerät selbst!) zu speichern. Sie werden in einer Datei im Home-Verzeichnis des aktuellen Benutzers gespeichert. Von dort werden sie beim ersten Öffnen des Dialogs automatisch geladen

☐ Klicken Sie auf „Ereignisse anzeigen“, um die Ereignis-Log-Datei als HTML-Datei anzuzeigen.

☐ Klicken Sie auf

- „Zurück“,um zum Ereignis-Log-Fenster zurückzukehren.
- „Laden“, um die Anzeige zu aktualisieren.
- „Speichern...“, wenn Sie die Ereignis-Log-Datei weiter benötigen. Wählen Sie danach im Datei-Auswahl-Fenster das gewünschte Verzeichnis aus, geben Sie einen Namen für die Datei ein und klicken Sie auf „Speichern“.
- „Suchen...“, um die Ereignis-Log-Datei nach einem Schlüsselwort oder einem regulären Ausdruck zu durchsuchen.

Anmerkung: Die Log-Datei hat folgende Eigenschaften:
– Die maximale Anzahl der Einträge in der Log-Datei ist 4.143.
– Ist die maximale Anzahl der Einträge erreicht, werden die ältesten Einträge durch die neuen überschrieben.
– Gleiche Einträge, die sich zusammenhängend wiederholen, werden zusammengefasst.
– Wenn Ereignisse, die sich zusammenhängend wiederholen, zusammengefasst werden, kann die Aktualisierung der Log-Datei bis zu 20 s nach dem letzten geloggten Ereignis dauern.

7.1.2 Syslog-Server

Dieser Dialog bietet Ihnen die Möglichkeit, einen Syslog-Server einzutragen. Ist ein Syslog-Server eingetragen, übermittelt das Gerät jeweils beim Eintreten eines Ereignisses eine Ereignismeldung über das Syslog-Protokoll zu diesem Server, der z.B. die Ereignismeldungen anzeigt oder bei bestimmten Ereignismeldungen einen Alarm auslöst.
Wenn Sie das Versenden von Ereignismeldungen über das Syslog-Protokoll deaktivieren möchten, tragen Sie die IP-Adresse 0.0.0.0 ein.

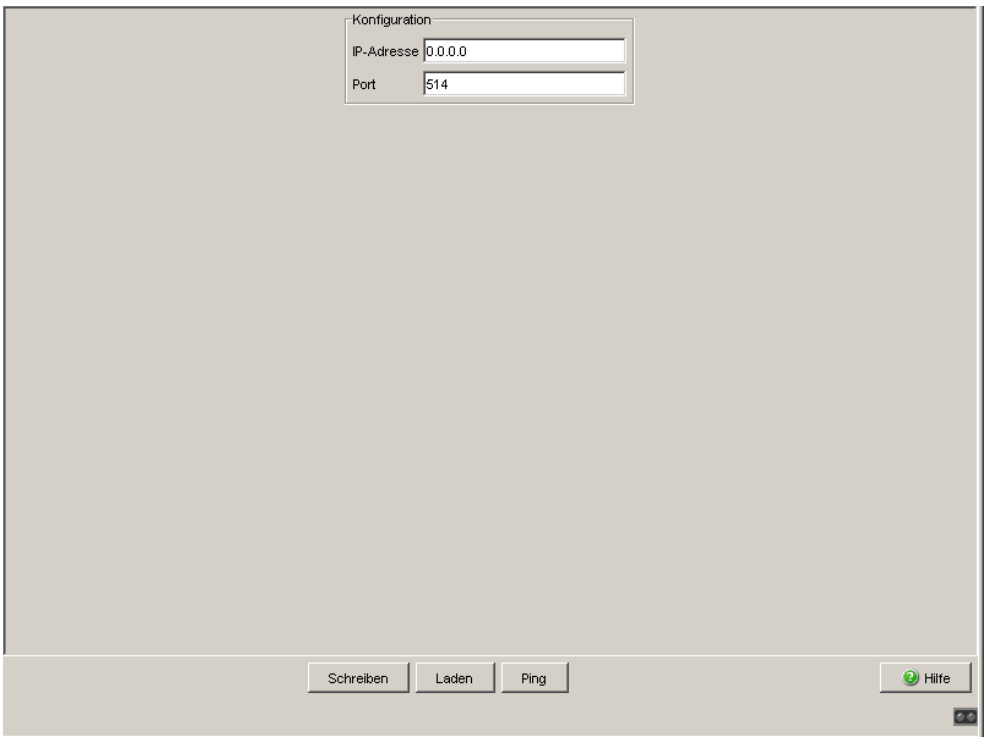


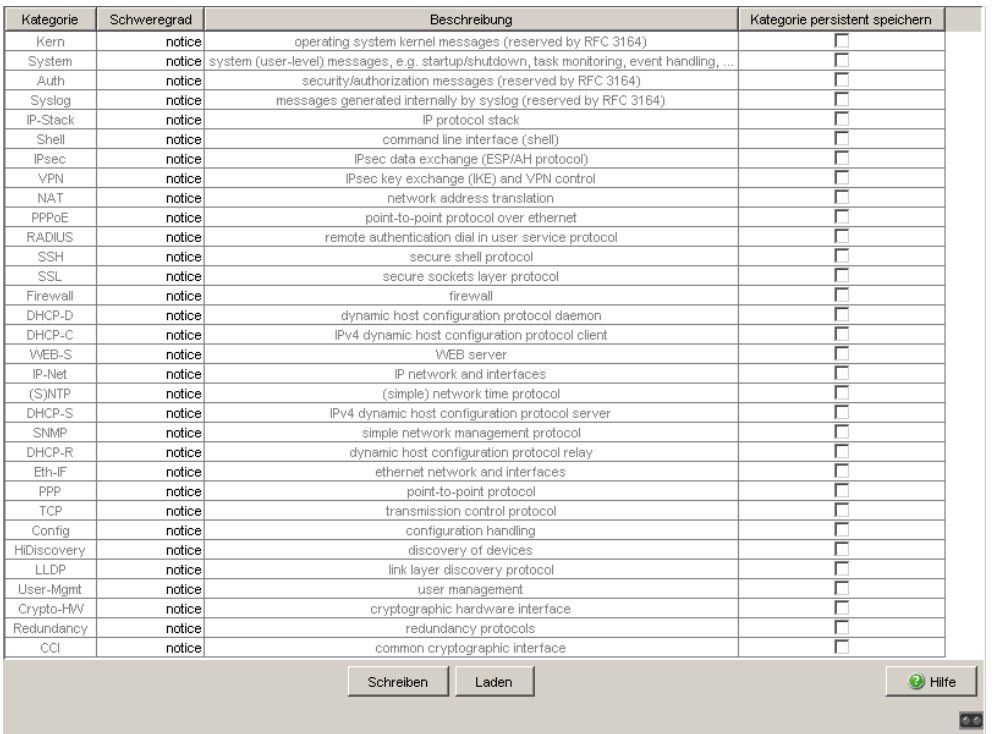
Abb. 28: Dialog Syslog-Server

☐ In „IP-Adresse“ geben Sie die IP-Adresse des Syslog-Servers ein.
☐ In „Port“ geben Sie die Portnummer ein. Voreinstellung: 514 (Syslog-Protokoll). Geben Sie auf dem Gerät und dem Syslog-Server die gleiche Portnummer ein.

7.1.3 Ereignis-Einstellungen

Dieser Dialog bietet Ihnen die Möglichkeit, für jede Ereignis-Kategorie einen minimalen Schweregrad für die Protokollierung zu wählen. Das Gerät protokolliert Ereignisse mit dem gewählten oder einem höheren Schweregrad.

Außerdem haben Sie die Möglichkeit, für jede Ereignis-Kategorie gesondert auszuwählen, ob das Gerät diese Ereignisse in den persistenten Log-Speicher auf dem ACA schreibt.



Kategorie	Schweregrad	Beschreibung	Kategorie persistent speichern
Kern	notice	operating system kernel messages (reserved by RFC 3164)	☐
System	notice	system (user-level) messages, e.g. startup/shutdown, task monitoring, event handling, ...	☐
Auth	notice	security/authorization messages (reserved by RFC 3164)	☐
Syslog	notice	messages generated internally by syslog (reserved by RFC 3164)	☐
IP-Stack	notice	IP protocol stack	☐
Shell	notice	command line interface (shell)	☐
IPsec	notice	IPsec data exchange (ESP/AH protocol)	☐
VPN	notice	IPsec key exchange (IKE) and VPN control	☐
NAT	notice	network address translation	☐
PPPoE	notice	point-to-point protocol over ethernet	☐
RADIUS	notice	remote authentication dial in user service protocol	☐
SSH	notice	secure shell protocol	☐
SSL	notice	secure sockets layer protocol	☐
Firewall	notice	firewall	☐
DHCP-D	notice	dynamic host configuration protocol daemon	☐
DHCP-C	notice	IPv4 dynamic host configuration protocol client	☐
WEB-S	notice	WEB server	☐
IP-Net	notice	IP network and interfaces	☐
(S)NTP	notice	(simple) network time protocol	☐
DHCP-S	notice	IPv4 dynamic host configuration protocol server	☐
SNMP	notice	simple network management protocol	☐
DHCP-R	notice	dynamic host configuration protocol relay	☐
Eth-IF	notice	ethernet network and interfaces	☐
PPP	notice	point-to-point protocol	☐
TCP	notice	transmission control protocol	☐
Config	notice	configuration handling	☐
HiDiscovery	notice	discovery of devices	☐
LLDP	notice	link layer discovery protocol	☐
User-Mgmt	notice	user management	☐
Crypto-HW	notice	cryptographic hardware interface	☐
Redundancy	notice	redundancy protocols	☐
CCI	notice	common cryptographic interface	☐

Schreiben Laden Hilfe

Abb. 29: Dialog Ereignis-Einstellungen

☐ Wählen Sie für jede Kategorie unter „Schweregrad“ das gewünschte Ereignisattribut (siehe Tab. 74), ab der das Gerät die Ereignisse protokolliert.
Sie haben durch Mehrfachselektion die Möglichkeit, mehreren Kategorien in einem Schritt den selben Schweregrad zuzuweisen.

☐ Markieren Sie für jede Kategorie, deren Ereignisse das Gerät in die Log-Datei auf dem ACA schreiben soll, das Kästchen in der Spalte „In persistente Log-Datei schreiben“.

Name	Bedeutung
emergency	Die Funktion steht nicht mehr zur Verfügung. Dies hat Einfluss auf andere Funktionen. Das Gerät führt in der Regel einen Neustart durch.
alert	Die Funktion steht nicht mehr zur Verfügung. Dies kann Einfluss auf andere Funktionen haben. Finden Sie die Ursache des erkannten Fehlers heraus und beseitigen Sie den erkannten Fehler.
critical	Die Funktion stand temporär nicht zur Verfügung. Dies kann Einfluss auf andere Funktionen gehabt haben Finden Sie die Ursache des erkannten Fehlers heraus und beseitigen Sie den erkannten Fehler.
error	Bei dieser Funktion wurde ein Fehler erkannt. Dies hat keinen Einfluss auf andere Funktionen gehabt. Der erkannte Fehler wurde vom Gerät behandelt. Finden Sie heraus, ob der erkannte Fehler durch eine Fehlkonfiguration entstanden ist oder durch ein kurzeitiges Ereignis (z. B. Überlast) im Netzwerk.
warning	Der Verdacht auf einen erkannten Fehler bei dieser Funktion ist aufgetreten. Dies hat keinen Einfluss auf diese und andere Funktionen. Finden Sie heraus, ob die Mitteilung durch eine Fehlkonfiguration entstanden ist oder durch ein kurzzeitiges Ereignis (z. B. Überlast) im Netzwerk.
notice	Die Funktion steht zur Verfügung. Die Meldung ist ausschließlich informativ (z. B. Reboot, bestimmte Konfigurationsänderungen).
info	Die Funktion steht zur Verfügung. Die Meldung bedeutet Normalbetrieb und kann für Reports oder Messungen verwendet werden. Es ist keine Aktion erforderlich.
debug	Die Funktion steht zur Verfügung. Die Meldung ist für die Suche nach einem erkannten Fehler nützlich, jedoch nicht für den Normalbetrieb.

Tab. 74: Bedeutung der Ereignisattribute

Anmerkung: Die Schweregrade `info` und `debug` sind für die Verwendung in einer zukünftigen Software-Version vorbereitet, sie können in der derzeitigen Software-Version zwar selektiert, aber nicht gespeichert werden.

7.1.4 Erweiterte Einstellungen

SNMP-Logging

Das Gerät bietet Ihnen im Rahmen „SNMP-Logging“ die Möglichkeit, die SNMP-Anfragen an das Gerät als Ereignisse zu behandeln. Dabei haben Sie die Möglichkeit, GET- und SET-Anfragen getrennt zu behandeln und den erzeugten Ereignis-Log-Einträgen einen Schweregrad zuzuweisen.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Rahmen „SNMP-Logging“	Einstellungen, um SNMP-Anfragen an das Gerät als Ereignisse zu behandeln.		
Log SNMP-Get-Requests.	Erzeugt bei SNMP-Get-Anfragen Ereignisse mit dem vorgegebenen Schweregrad.	`Aktiv`, `inaktiv`	`inaktiv`
Schweregrad (für Logs von SNMP-Get-Requests)	Gibt den Schweregrad vor, mit dem das Gerät das Ereignis „SNMP-Get-Request erhalten“ erzeugt.	`notice`, `warning`, `error`, `critical`, `alert`, `emergency`	`notice`
Log SNMP-Set-Requests.	Erzeugt bei SNMP-Set-Anfragen Ereignisse mit dem vorgegebenen Schweregrad.	`Aktiv`, `inaktiv`	`inaktiv`
Schweregrad (für Logs von SNMP-Set-Requests)	Gibt den Schweregrad vor, mit dem das Gerät das Ereignis „SNMP-Set-Request erhalten“ erzeugt.	`notice`, `warning`, `error`, `critical`, `alert`, `emergency`	`notice`

Tab. 75: SNMP-Logging-Einstellungen

In persistente Log-Datei schreiben

Im Rahmen „In persistente Log-Datei schreiben“ haben Sie die Möglichkeit, die maximale Größe und die maximale Anzahl der persistenten Log-Dateien zu konfigurieren. Zusätzlich können Sie die aktuelle Log-Datei anhalten. Dies bietet Ihnen die Möglichkeit, den ACA im laufenden Betrieb zu tauschen, so dass die persistenten Log-Dateien konsistent bleiben.

Das Gerät schreibt die persistenten Log-Dateien in das Verzeichnis „/log“ des ACA. Die aktuelle Log-Datei hat den Dateinamen „messages“, ältere Log-Dateien im Archiv haben die Namen „messages.0“ bis „messages.97“. Erreicht die aktuelle Log-Datei ihre Maximalgröße, benennt das Gerät sie in die Archiv-Datei „messages.0“ um und öffnet eine neue aktuelle Log-Datei. Das Gerät benennt dabei die vorherige Archiv-Datei „messages.0“ in „messages.1“ um, „messages.1“ in „messages.2“ usw. Ist die maximale Anzahl für persistente Log-Dateien überschritten, löscht das Gerät die älteste.

Um den ACA während des laufenden Betriebs zu wechseln, bietet das Gerät Ihnen die Möglichkeit, die laufende Log-Datei zu sperren und anzuhalten. Das Gerät schließt danach die laufende Log-Datei.
Sie können nun den ACA entfernen, die Log-Dateien auf dem ACA bleiben dabei konsistent.
Schließen Sie einen anderen ACA an und heben Sie die Sperre auf. Das Gerät legt eine neue laufende Log-Datei auf dem ACA an und schreibt die neuen Ereignisse in diese Datei.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Rahmen „In persistente Log-Datei schreiben“	Einstellungen für persistente Log-Dateien		
Maximale Größe der einer Datei in KBytes	Gibt die maximale Größe einer Log-Datei in KBytes an. Eine Maximalgröße von 0 schließt die aktuelle Log-Datei, archiviert sie und beendet das Schreiben von persistenten Log-Dateien.	`0 - 4.096 KByte`	`0 KByte`
Maximale Anzahl Dateien	Bestimmt die maximale Anzahl der Log-Dateien auf dem ACA. Ein Anzahl von 0 löscht die bereits vorhandenen Log-Dateien und beendet das Schreiben von persistenten Log-Dateien.	`0 - 99`	`0`
Persistentes Loging anhalten	Sperren und Anhalten der aktuellen persistenten Log-Datei. Aktivieren Sie die Sperre, um den ACA auszutauschen und deaktivieren Sie die Sperre danach wieder.	`Aktiv`, `inaktiv`	`inaktiv`

Tab. 76: Einstellungen für persistente Log-Dateien

Anmerkung: Um persistente Log-Dateien zu aktivieren, setzen Sie sowohl die maximale Größe als auch die maximale Anzahl der der Log-Dateien auf Werte > 0.

Anmerkung: Wählen Sie nur die für Sie notwendigen Ereignisse zum Schreiben in die persistente Log-Datei aus, da die Daten-Schreibrate des ACA begrenzt ist.

Anmerkung: Um den ACA im laufenden Betrieb auszutauschen, halten Sie zuerst das Logging in die persistente Log-Datei an und klicken auf „Schreiben“. Tauschen Sie nun den ACA aus. Danach heben Sie die Sperre der Log-Datei auf und klicken erneut auf „Schreiben“.

Anmerkung: Log-Ereignisse, die im angehaltenen Zustand der persistenten Log-Datei eintreten, schreibt das Gerät ausschließlich in den normalen Ereignis-Log.

7.2 Ports

Das Port-Menü enthält Anzeigen und Tabellen zu den einzelnen Ports:
- Netzlast
- Statistiktabelle
- ARP-Einträge

7.2.1 Netzlast

Diese Tabelle zeigt Ihnen die Netzlast an den einzelnen Ports an.

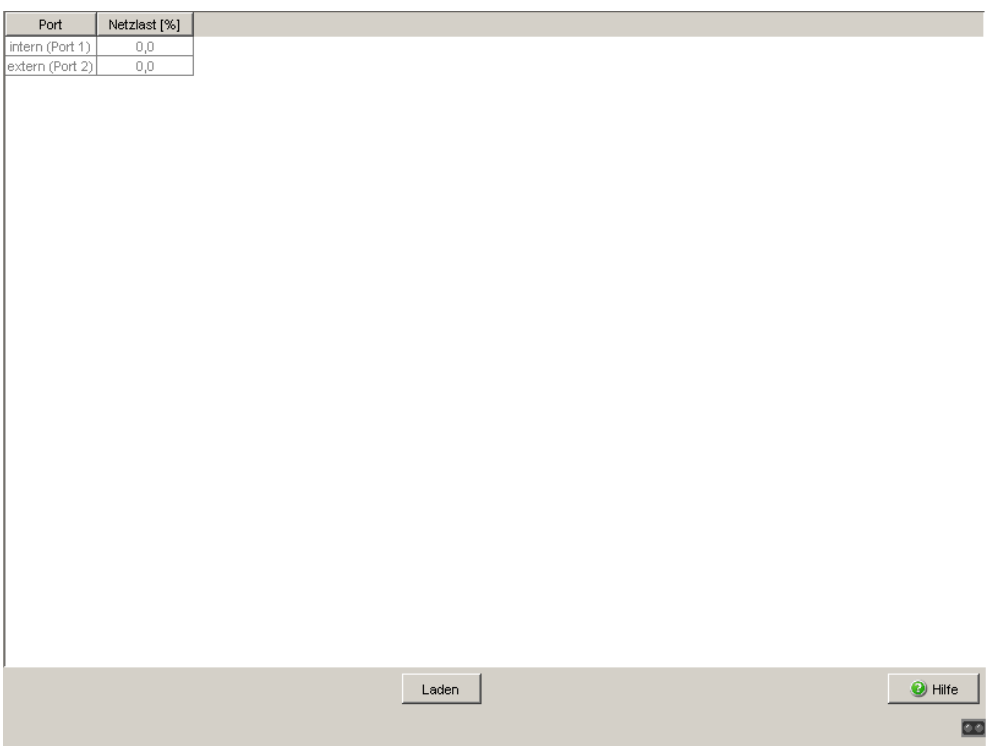


Abb. 30: Dialog Netzlast

7.2.2 Portstatistiken

Diese Tabelle zeigt Ihnen die Inhalte verschiedener Port-Ereigniszähler an. Im Menüpunkt `Grundeinstellungen:Neustart` bietet das Gerät Ihnen die Möglichkeit, mit „Kaltstart“ oder „Port-Zähler zurücksetzen“ die Ereigniszähler auf 0 zurücksetzen.

Parameter	MIB-Variable
Port	ifIndex
Empfangene Pakete	Summe aus ifInUcastPkts, ifInMulticastPkts und ifInBroadcastPkts
Empfangene Unicast-Pakete	ifInUcastPkts
Empfangene Multicast-Pakete	ifInMulticastPkts.
Empfangene Broadcast-Pakete	ifInBroadcastPkts.
Empfangene Oktetts	ifInOctets
Empfangsseitig verworfene Pakete	ifInDiscards
Empfangene Pakete mit erkannten Fehlern	ifInErrors
Empfangene unbekannte Protokolle	ifInUnknownProtos
Gesendete Unicast-Pakete	ifOutUcastPkts
Gesendete Multicast-Pakete	ifOutMulticastPkts
Gesendete Broadcast-Pakete	ifOutBroadcastPkts
Gesendete Oktetts	ifOutOctets.
Sendeseitig verworfene Pakete	ifOutDiscards
Gesendete Pakete mit erkannten Fehlern	ifOutError

Tab. 77: MIB-Variablen in der Statistiktabelle

Anmerkung: Im PPPoE-Modus werden beim externen Interface nicht alle PPPoE - Pakete in den Statistiken aufgeführt.

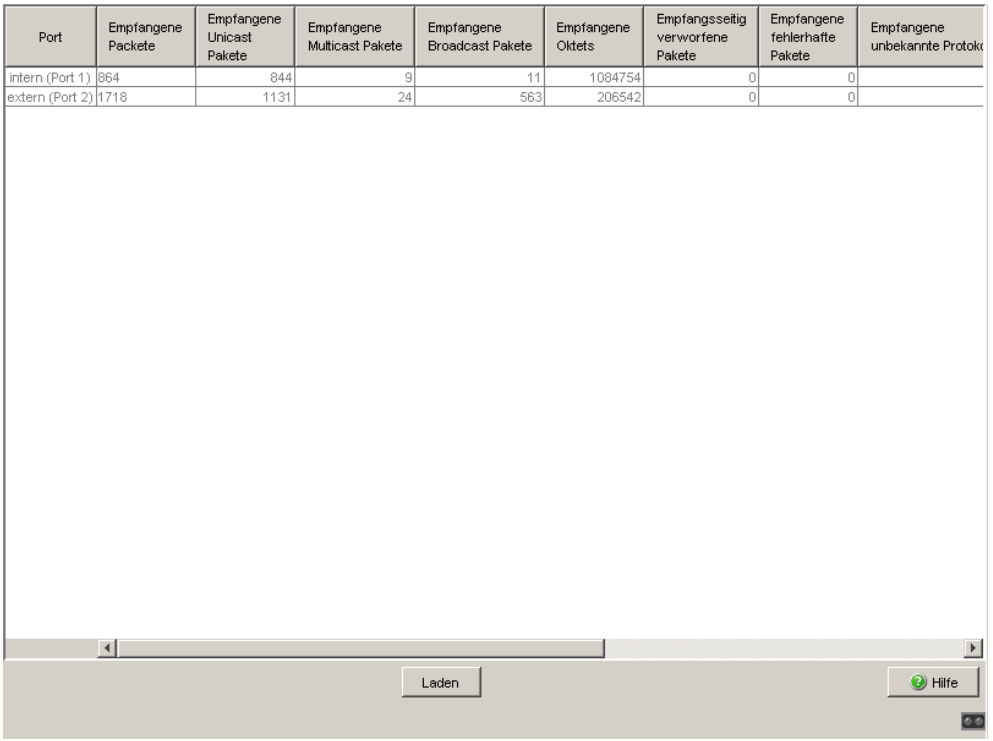


Abb. 31: Beispiel für Portstatistiktabelle

7.2.3 ARP

Diese Tabelle zeigt Ihnen die ARP-Einträge je Port an.
Das Gerät ermittelt mit Hilfe des Address Resolution Protocols (ARP) zur IPAdresse eines Gerätes die zugehörige MAC-Adresse und speichert diese Zuordnung in der ARP-Tabelle ab.

Parameter	Bedeutung
Port	Anzeige des Ports, für den dieser Eintrag gilt.
IP-Adresse	Anzeige der IP-Adresse eines Gerätes, das auf eine ARP-Anfrage an diesem Port geantwortet hat.
MAC-Adresse	Anzeige der MAC-Adresse eines Gerätes, das auf eine ARP-Anfrage an diesem Port geantwortet hat.
Letztes Update	Anzeige der Zeit der letzten Aktualisierung des ARP-Eintrages als System-Uptime (Angabe in Tagen, Stunden, Minuten und Sekunden).
Typ	Anzeige der Art des Eintrags: – static: statischer ARP-Eintrag, der auch nach dem Löschen der ARP-Tabelle erhalten bleibt. – dynamic: dynamischer Eintrag. Wenn das Gerät während der „Aging Time“ keine Daten empfängt, löscht es den Eintrag nach Ablauf der Zeit aus der Tabelle. – local: IP- und MAC-Adresse des eigenen Ports
Aktiv	Anzeige des Status des Eintrages: – Angekreuzt: ARP aktiv – Nicht angekreuzt: ARP inaktiv

Tab. 78: ARP-Tabelle

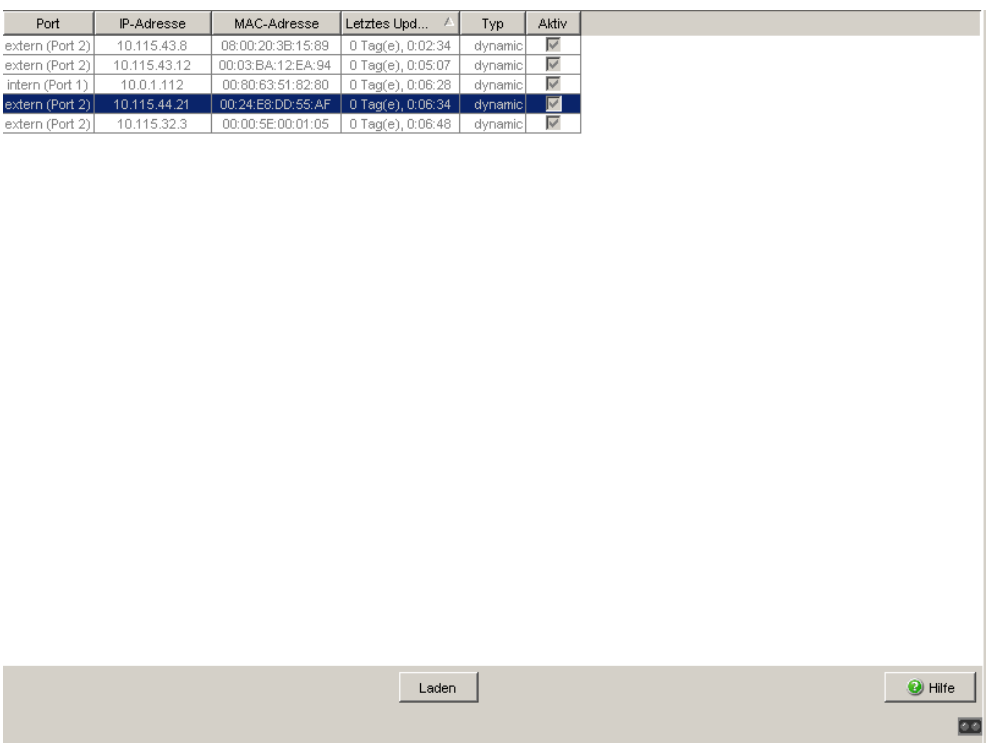


Abb. 32: Beispiel für ARP-Einträge

7.3 Topologie-Erkennung

Dieser Dialog bietet Ihnen die Möglichkeit, die Funktion zur Topologie-Erkennung (Link Layer Discovery Protocol, LLDP) ein/auszuschalten. Die Topologie-Tabelle zeigt Ihnen die gesammelten Informationen zu Nachbargeräten an. Mit diesen Informationen ist eine Netzmanagement-station in der Lage, die Struktur Ihres Netzes darzustellen.

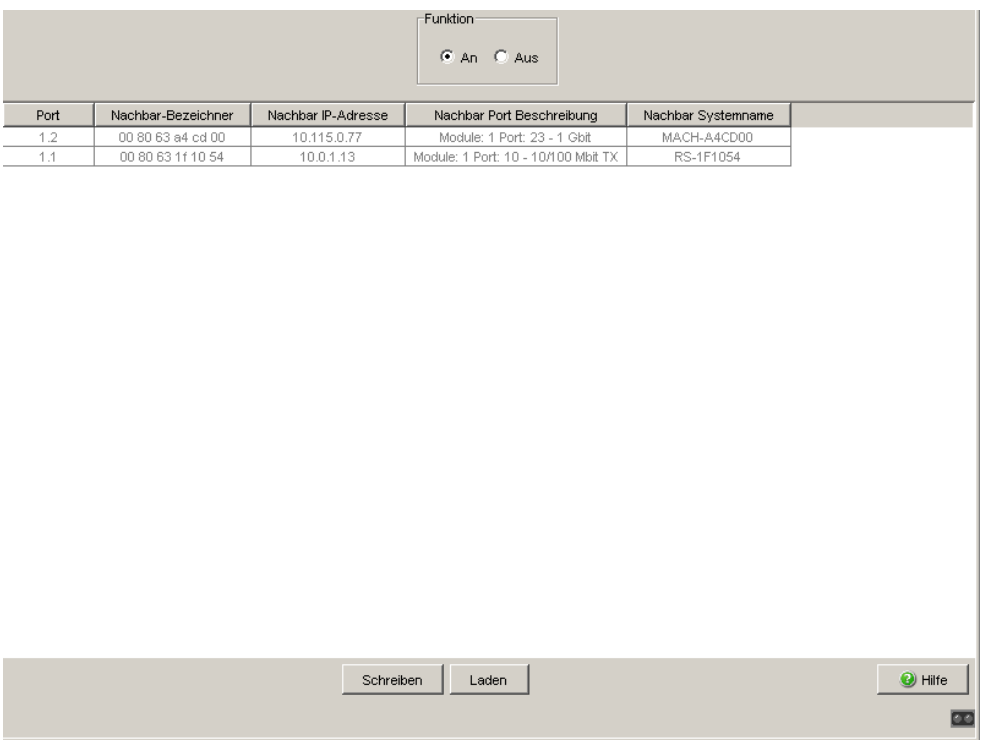


Abb. 33: Dialog Topologie-Erkennung

Sind an einem Port, z. B. über einen Hub, mehrere Geräte angeschlossen, dann zeigt die Tabelle pro angeschlossenem Gerät eine Zeile an.

Wenn an einem Port sowohl Geräte mit als auch ohne aktive Topologie-Erkennungs-Funktion angeschlossen sind, dann blendet die Topologie-Tabelle die Geräte ohne aktive Topologie-Erkennung aus.

Wenn nur Geräte ohne aktive Topologie-Erkennung an einem Port angeschlossen sind, dann enthält die Tabelle stellvertretend für alle Geräte eine Zeile für diesen Port. Diese Zeile enthält die Anzahl der angeschlossenen Geräte.

7.4 Gerätestatus

Der Gerätestatus gibt einen Überblick über den Gesamtzustand des Gerätes. Viele Prozessvisualisierungssysteme erfassen den Gerätestatus eines Gerätes, um seinen Zustand grafisch darzustellen.

Das Gerät zeigt seinen aktuellen Status als „Fehler“ oder „Ok“ im Rahmen „Gerätestatus“ an. Das Gerät bestimmt diesen Status aus den einzelnen Überwachungsergebnissen.

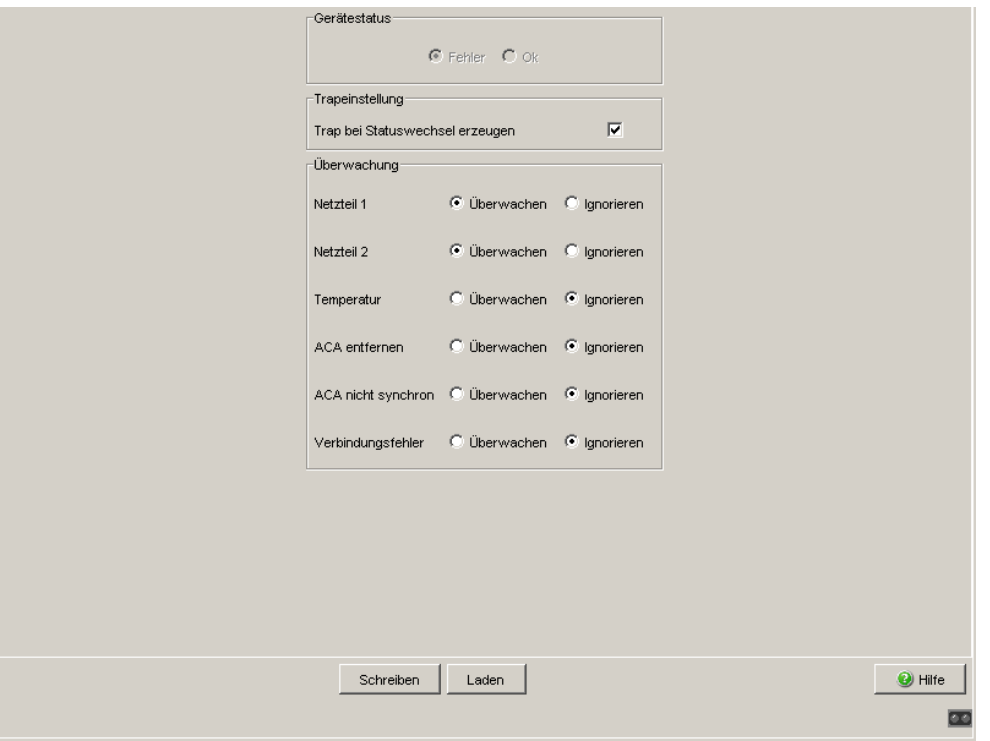


Abb. 34: Dialog Gerätestatus

Die auswählbaren Ereignisse haben folgende Bedeutung:

Name	Bedeutung
Netzteil ...	Versorgungsspannung(en) überwachen/ignorieren
Temperatur	Eingestellte Temperaturschwelle (siehe auf Seite 16 „System“) auf Über- und Unterschreiten überwachen/ignorieren
ACA entfernen	Entfernen des ACA überwachen/ignorieren.
ACA nicht synchron	Nichtübereinstimmung der Konfiguration im Gerät und auf dem ACA[1] überwachen/ignorieren.
Verbindungsfehler	Den Linkstatus mindestens eines Ports überwachen/ignorieren. Die Meldung des Linkstatus kann pro Port über das Management maskiert werden (siehe auf Seite 34 „Portkonfiguration“). Zur Verbindungsfehlerüberwachung markieren Sie im Dialog `Grundeinstellungen:Portkonfiguration` in der Tabellenspalte „Verbindungsfehler weitermelden“ das Kästchen für jeden gewünschten Port. Im Lieferzustand erfolgt keine Verbindungsüberwachung.

Tab. 79: Gerätestatus

1. Die Konfigurationen stimmen dann nicht überein, wenn nur eine Datei existiert oder die 2 Dateien nicht den gleichen Inhalt haben.

☐ Wählen Sie im Feld „Trapeinstellung“ „Trap bei Statuswechsel erzeugen“, um das Versenden eines Traps zu aktivieren, wenn sich der Gerätestatus ändert.

Anmerkung: Bei nicht redundanter Zuführung der Versorgungsspannung meldet das Gerät das Fehlen einer Versorgungsspannung. Sie können diese Meldung verhindern, indem Sie die Versorgungsspannung über beide Eingänge zuführen oder die Überwachung ausschalten (siehe auf Seite 187 „Meldekontakt“).

7.5 Meldekontakt

Die Meldekontakte dienen
- der Funktionsüberwachung des Geräts,
- der Steuerung externer Geräte durch die manuelle Einstellung der Meldekontakte,
- der Signalisierung des Gerätestatus des Geräts (Lieferzustand).

7.5.1 Funktionsüberwachung

☐ Wählen Sie im Feld „Modus Meldekontakt“ den Modus „Funktionsüberwachung“. Die Meldekontakte dienen in diesem Modus der Funktionsüberwachung des Gerätes und ermöglichen damit eine Ferndiagnose.

Das Gerät meldet über die potentialfreien Meldekontakte (Relaiskontakt, Ruhestromschaltung) durch eine Kontaktunterbrechung:

- den erkannten Ausfall des Netzteils 1/2 oder eine erkannte dauerhafte Störung im Gerät (interne Spannung). Wählen Sie Netzteil 1/2 „überwachen“, wenn der Meldekontakt den erkannten Ausfall eines Netzteils oder der internen 3,3 V-Spannung melden soll.
- das Über- oder Unterschreiten der eingestellten Temperaturschwellen (siehe auf Seite 17 „Systemdaten“). Wählen Sie Temperatur „überwachen“, wenn der Meldekontakt eine unzulässige Temperatur melden soll.
- das Entfernen des ACA. Wählen Sie ACA entfernen „überwachen“, wenn der Meldekontakt das Entfernen des ACA melden soll.

- das Nichtübereinstimmen der aktuellen Konfiguration auf dem Gerät und dem ACA. Wählen Sie ACA nicht synchron „überwachen“, wenn der Meldekontakt diese Nichtübereinstimmung melden soll.
- die unterbrochene Verbindung zu mindestens einem Port. Im Lieferzustand ignoriert das das Gerät den Linkstatus. Zur Überwachung erkannter Verbindungsfehler markieren Sie außerdem im Dialog `Grundeinstellungen:Portkonfiguration` in der Tabellenspalte `Verbindungsfehler weitermelden` das Kästchen für jeden gewünschten Port.

7.5.2 Manuelle Einstellung

☐ Wählen Sie im Feld „Modus Meldekontakt“ den Modus „Manuelle Einstellung“. Dieser Modus bietet Ihnen die Möglichkeit, diesen Meldekontakt fernzubedienen.
☐ Wählen Sie „Offen“ im Feld „Manuelle Einstellung“, um den Kontakt zu öffnen.
☐ Wählen Sie „Geschlossen“ im Feld „Manuelle Einstellung“, um den Kontakt zu schließen.

Anwendungsmöglichkeiten:

- Simulation eines erkannten Fehlers bei einer SPS-Fehlerüberwachung.
- Fernbedienung eines Gerätes über SNMP, wie z. B. das Einschalten einer Kamera.

7.5.3 Gerätestatus

☐ Wählen Sie im Feld „Modus Meldekontakt“ den Modus „Gerätestatus“. Der Meldekontakt dient in diesem Modus der Überwachung des Gerätestatus des Gerätes (siehe auf Seite 185 „Gerätestatus“) und ermöglicht damit eine Ferndiagnose.
Über den potentialfreien Meldekontakt (Relaiskontakt, Ruhestromschaltung) meldet das Gerät durch Kontaktunterbrechung den Gerätestatus „Fehler“ (siehe auf Seite 185 „Gerätestatus“).

7.5.4 Trapeinstellung

☐ Wählen Sie `Trap bei Statuswechsel erzeugen`, damit das Gerät ein Trap erzeugt, sobald sich bei aktiver Funktionsüberwachung die Stellung eines Meldekontaktes ändert.

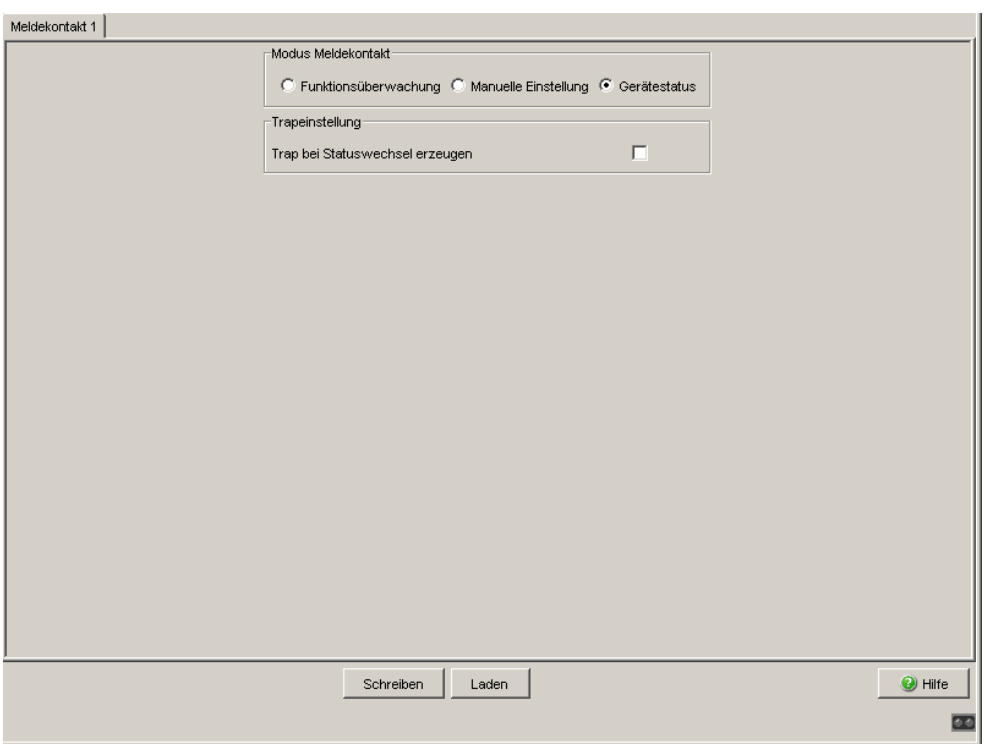


Abb. 35: Dialog Meldekontakt

7.6 Alarme (Traps)

Dieser Dialog bietet Ihnen die Möglichkeit festzulegen, welche Ereignisse einen Alarm (Trap) auslösen und an wen diese Alarme gesendet werden sollen.

- ☐ Klicken Sie auf „Eintrag erzeugen“, um das Dialogfenster zur Eingabe eines Namens und der IP-Adresse des Empfängers anzugeben, an den die Traps geschickt werden sollen.
- ☐ Bestätigen Sie die Eingaben mit „OK“. Damit erzeugen Sie eine neue Zeile in der Tabelle für diesen Empfänger.
- ☐ In der Spalte „Aktiv“ kreuzen Sie die Einträge an, die das Gerät beim Versenden von Traps berücksichtigen sollen. Voreinstellung: inaktiv.
- ☐ Im Rahmen „Konfiguration“ wählen Sie die Trap-Kategorien aus, von denen Sie Traps versenden wollen. Voreinstellung: alle Trap-Kategorien sind aktiv.

Die auswählbaren Ereignisse haben folgende Bedeutung:

Name	Bedeutung
Login	Ein Zugriff oder Zugriffsversuch auf das Gerät über die serielle Schnittstelle oder über das Netzwerk (SSH) ist erfolgt.
Authentifizierung	Das Gerät hat einen unerlaubten Zugriff zurückgewiesen, siehe Dialog „SNMP-Zugriff“ auf Seite 52.
Chassis	Fasst die folgenden Ereignisse zusammen: – Der Status einer Versorgungsspannung hat sich geändert (siehe auf Seite 16 „System“). – Der Status des Meldekontakts (siehe auf Seite 187 „Meldekontakt“) hat sich geändert. Um dieses Ereignis zu berücksichtigen, aktivieren Sie „Trap bei Statuswechsel erzeugen“ im Dialog `Diagnose:Meldekontakt` (siehe auf Seite 187 „Meldekontakt“). – Der Gerätestatus hat sich geändert. Um dieses Ereignis zu berücksichtigen, aktivieren Sie "Trap bei Statuswechsel erzeugen" im Dialog „Gerätestatus“. – Bei eingeschalteter SNTP-Funktion: die Synchronisierung mit dem SNTP-Server (siehe auf Seite 79 „SNTP-Konfiguration“) wurde hergestellt oder unterbrochen. – Bei eingeschalteter NTP-Funktion: die Synchronisierung mit dem NTP-Server (siehe auf Seite 82 „NTP-Konfiguration“) wurde hergestellt oder unterbrochen. – Der AutoConfiguration Adapter ACA wurde hinzugefügt oder entfernt. – Die Temperaturschwelle wurde unter-/überschritten.
Kaltstart	Das Gerät wurde eingeschaltet und ist managebar.
Verbindungs-status	An einem Port des Gerätes wurde eine Verbindung mit einem dort angeschlossenen Gerät hergestellt/unterbrochen.
Redundanz	Bei aktiver Router-Redundanz: der Router-Redundanz-Status (Master-Router/Backup-Router) (siehe auf Seite 165 „Router-Redundanz“) des Gerätes hat sich geändert.
Firewall	Ein Benutzer (siehe auf Seite 67 „Benutzer-Firewall-Konten“) der Firewall (siehe auf Seite 136 „Benutzer-Firewall“) hat sich angemeldet, abgemeldet oder die Anmeldung war erfolglos.
VPN	Eine VPN-Verbindung wurde hergestellt oder unterbrochen.

Tab. 80: Trap-Kategorien

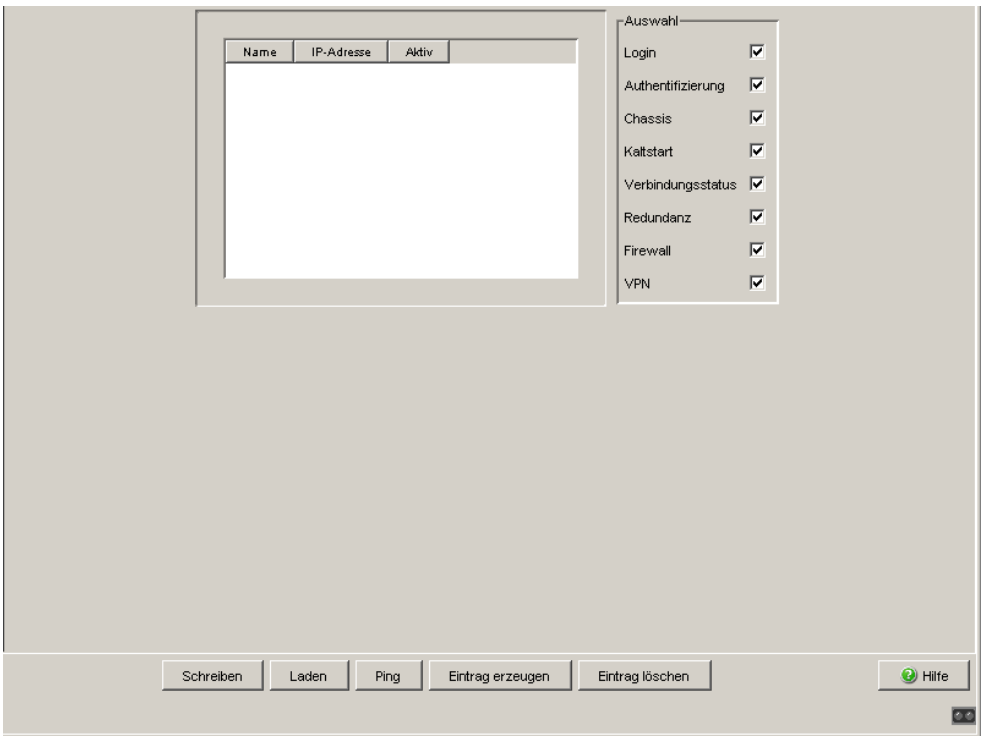


Abb. 36: Dialog Alarme (Traps)

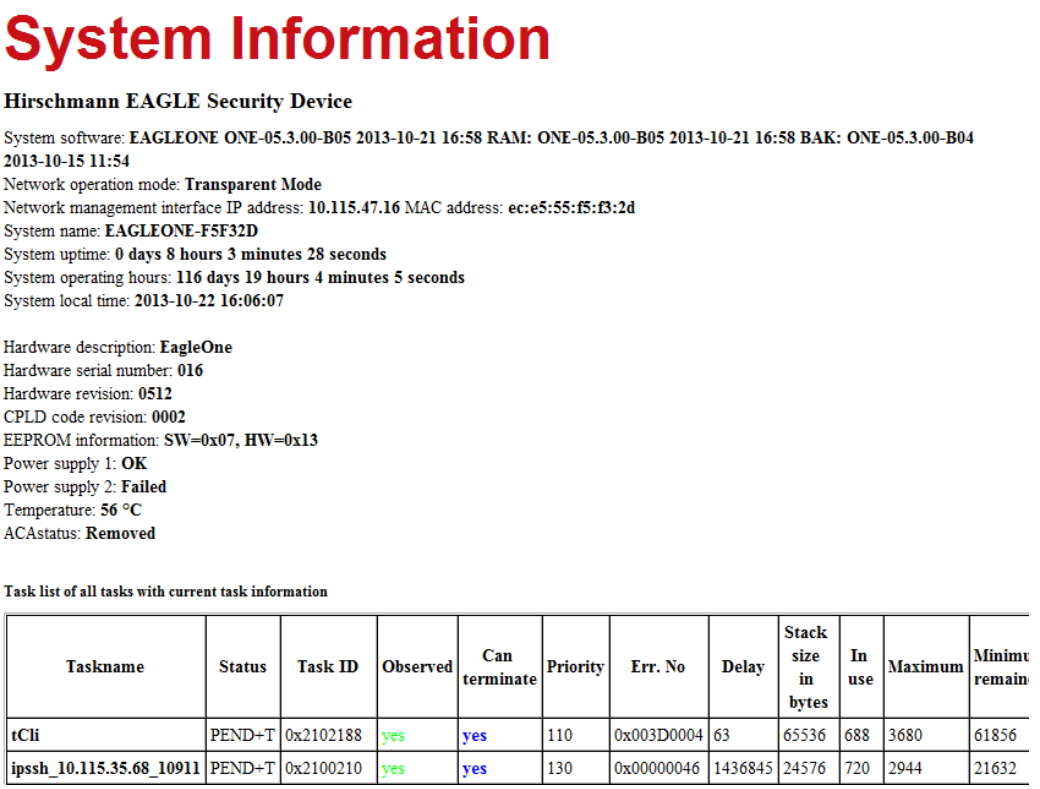
7.7 Bericht

Folgende Berichte stehen zur Diagnose zur Verfügung:

- System-Information

7.7.1 System-Information

Die Systeminformation ist eine HTML-Datei, die alle systemrelevanten Daten enthält.



System Information

Hirschmann EAGLE Security Device

System software: **EAGLEONE ONE-05.3.00-B05 2013-10-21 16:58 RAM: ONE-05.3.00-B05 2013-10-21 16:58 BAK: ONE-05.3.00-B04 2013-10-15 11:54**
Network operation mode: **Transparent Mode**
Network management interface IP address: **10.115.47.16** MAC address: **ec:e5:55:f5:f3:2d**
System name: **EAGLEONE-F5F32D**
System uptime: **0 days 8 hours 3 minutes 28 seconds**
System operating hours: **116 days 19 hours 4 minutes 5 seconds**
System local time: **2013-10-22 16:06:07**

Hardware description: **EagleOne**
Hardware serial number: **016**
Hardware revision: **0512**
CPLD code revision: **0002**
EEPROM information: **SW=0x07, HW=0x13**
Power supply 1: **OK**
Power supply 2: **Failed**
Temperature: **56 °C**
ACAstatus: **Removed**

Task list of all tasks with current task information

Taskname	Status	Task ID	Observed	Can terminate	Priority	Err. No	Delay	Stack size in bytes	In use	Maximum	Minimu remain
tCli	PEND+T	0x2102188	yes	yes	110	0x003D0004	63	65536	688	3680	61856
ipssh_10.115.35.68_10911	PEND+T	0x2100210	yes	yes	130	0x00000046	1436845	24576	720	2944	21632

Abb. 37: Dialog System-Information

☐ Klicken Sie auf „System-Informationen anzeigen“. Das Gerät zeigt die System-Informationen in einer HTML-Datei an.
☐ Klicken Sie auf
- „Zurück“, um zum Systeminformations-Fenster zurückzukehren.
- „Laden“, um die Anzeige zu aktualisieren.
- „Suchen...“, um die Systeminformations-Datei nach einem Schlüsselwort oder einem regulären Ausdruck zu durchsuchen.
- „Speichern,,,“, wenn Sie die Systeminformations-Datei weiter benötigen. Wählen Sie dazu im Datei-Auswahl-Fenster das gewünschte Verzeichnis aus, geben Sie einen Namen für die Datei ein und klicken Sie auf „Speichern“.

7.8 MAC-Firewall-Liste

Die MAC-Firewall-Liste zeigt die vom Benutzer angelegten Regeln zuzüglich die durch das System eingetragenen impliziten Regeln der Layer 2- (MAC-) Firewall.
Diese Liste kann Ihnen helfen, Ereignis-Log-Einträge zu verstehen und trägt zur Übersicht der Firewall-Konfiguration bei.

Parameter	Bedeutung	Mögliche Werte
Index	Fortlaufender Zeilenindex	
Regelgruppe	Interne Klassifizierung der Regel	- Default Rules - Miscellaneous - Rate-Limits (DoS) - Special Traffic
Referenz	Interne Information für den Service-Techniker.	
Interface	Interface, für das diese Regel gilt.	- any = alle - egress = geräteeigene Daten - external = externer Port - internal = interner Port - mirror = Bridge-Schnittstelle im Transparent-Modus.

Quelladresse	MAC-Adresse der eigentlichen Quelle des Datenpaketes.
	Eingabeformat:
	`11:22:33:44:55:66`
	Die Eingabe von „?“ ermöglicht den Einsatz von Wildcards. Beispiel:
	`1?:22:??:44:55:6?.`	

Zieladresse	MAC-Adresse des eigentlichen Zieles des Datenpaketes.Eingabeformat:
	`11:22:33:44:55:66`
	Die Eingabe von „?“ ermöglicht den Einsatz von Wildcards. Beispiel:
	`1?:22:??:44:55:6?.`	

Protokoll	Protokoll im Typ-Feld des MAC-Daten-paketes	
Aktion	Aktion, die die Firewall durchführt, wenn die Regel zutrifft.	accept, drop

Tab. 81: MAC-Firewall-Liste

Parameter	Bedeutung	Mögliche Werte
Log	Eintrag in die Ereignis-Liste, wenn die Regel zutrifft.	ja, nein
Übereinstim-mungen	Zähler, der festhält, wie oft die Regel bereits zugetroffen hat	0 - 4.294.967.295 (2^{32} - 1)

Tab. 81: MAC-Firewall-Liste

7.9 IP-Firewall-Liste

Die IP-Firewall-Liste zeigt die vom Benutzer angelegten Regeln zuzüglich die durch das System eingetragenen impliziten Regeln der Layer 3- (IP-) Firewall.
Diese Liste kann Ihnen helfen, Ereignis-Log-Einträge zu verstehen und trägt zur Übersicht der Firewall-Konfiguration bei.

Parameter	Bedeutung	Mögliche Werte
Index	Fortlaufender Zeilenindex	
Regelgruppe	Interne Klassifizierung der Regel	- Special Traffic - Miscellaneous - Rate-Limits - VPN - HTTPS Access - SSH Access - SNMP Access - PPP Packet Filterr - Packet Filter IP Outgoing - Packet Filter IP Incoming - Default Rules
Referenz	Interne Information für den Service-Techniker.	
Interface	Interface, für das diese Regel gilt.	- any = alle - egress = geräteeigene Daten - external = externer Port - internal = interner Port - mirror = Bridge-Schnittstelle im Transparent-Modus. - loopback - ppp (serial) = V.24-Port
Quellnetz	IP-Adresse mit Netzmaske (CIDR) der eigentlichen Quelle des Datenpaketes	IP-Adresse mit Netzmaske, any = alle, me = eigene IP-Adresse
Quellport	Logischer Quellport des Datenpaketes.	any = alle op port port 1 op port 2
Zielnetz	IP-Adresse mit Netzmaske (CIDR) des eigentlichen Ziels des Datenpaketes	IP-Adresse mit Netzmaske, any = alle, me = eigene IP-Adresse

Tab. 82: IP-Firewall-Liste

Parameter	Bedeutung	Mögliche Werte
Zielport	Logischer Zielport des Datenpaketes	any = alle op port port 1 op port 2
Protokoll	IP-Protokoll	any = alle, tcp, udp, icmp
Aktion	Aktion, die die Firewall durchführt, wenn die Regel zutrifft.	accept, drop, reject
Log	Eintrag in die Ereignis-Liste, wenn die Regel zutrifft.	ja, nein
Übereinstim-mungen	Zähler, der festhält, wie oft die Regel bereits zugetroffen hat	0 - 4.294.967.295 (2^{32} - 1)

Tab. 82: IP-Firewall-Liste

7.10 Konfigurations-Check

Das Gerät bietet Ihnen die Möglichkeit, seine Konfiguration mit denen seiner Nachbar-Geräte zu vergleichen.
Dazu verwendet es die Daten, die es mittels Topologie-Erkennung (LLDP) von seinen Nachbargeräten empfangen hat.
Der Dialog listet die erkannten Abweichungen auf, die die Leistungsfähigkeit der Kommunikation zwischen dem Gerät und den erkannten Nachbargeräten beeinflussen.

☐ Mit der „Laden“-Bedientaste aktualisieren Sie den Inhalt der Tabelle. Bleibt die Tabelle leer, war der Konfigurations-Check erfolgreich und die Konfiguration des Gerätes ist kompatibel zu den erkannten Nachbargeräten.

Anmerkung: Ein Nachbargerät ohne LLDP-Unterstützung, das LLDP-Pakete weiterleitet, kann im Dialog mehrdeutige Meldungen verursachen. Dies tritt auf, wenn das Nachbargerät ein Hub oder ein Switch ohne Management ist, der die Norm IEEE 802.1D-2004 ignoriert.
Der Dialog stellt in dem Fall die am Nachbargerät angeschlossenen und erkannten Geräte als direkt mit dem Switch-Port verbunden dar, obwohl diese am Nachbargerät angeschlossen sind.

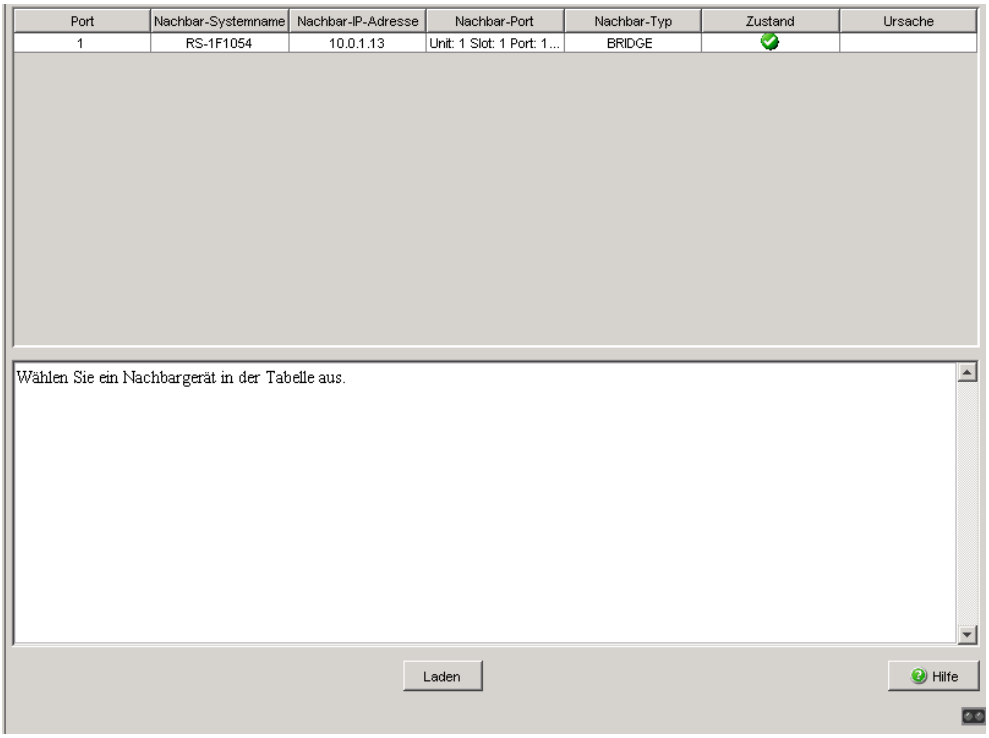


Abb. 38: Konfigurations-Check

Parameter	Bedeutung
Port	Port, für den dieser Eintrag gilt.
Nachbar-Systemname	Systemname des Nachbargerätes (siehe auf Seite 17 „Systemdaten“)
Nachbar-IP-Adresse	IP-Adresse des Nachbargerätes mit LLDP-Funktion (siehe auf Seite 20 „Netz“)
Nachbar-Port	Zeigt Informationen zu dem Nachbargerät an.
Nachbar-Typ	Zeigt den Typ des Nachbargerätes an. Schreibweise in – Großbuchstaben: das Gerät verfügt über diese Funktion und diese Funktion ist aktiviert. – Kleinbuchstaben: das Gerät verfügt über diese Funktion und diese Funktion ist deaktiviert.
Zustand	Zeigt den Konfigurations-Zustand an – Grüner Kreis mit Haken: Die Konfiguration dieses Gerätes und die Konfiguration des Nachbargerätes sind kompatibel. Die Kommunikation zwischen den beiden Geräten ist in Ordnung. – Gelbes Dreieck: Die Konfiguration dieses Gerätes und die Konfiguration des Nachbargerätes stimmen nicht überein. Die Leistungsfähigkeit der Kommunikation zwischen den beiden Geräten kann gefährdet sein. Wählen Sie diese Zeile aus, um im Fenster darunter weitere Informationen zu erhalten. – Rotes Quadrat mit Kreuz: Die Konfiguration dieses Gerätes und die Konfiguration des Nachbargerätes sind nicht kompatibel. Die Kommunikation zwischen den beiden Geräten ist gefährdet. Wählen Sie diese Zeile aus, um im Fenster darunter weitere Informationen zu erhalten. – Blauer Kreis mit Fragezeichen: Konfigurationsdaten des Nachbargerätes liegen nicht vor, Wählen Sie diese Zeile aus, um im Fenster darunter weitere Informationen zu erhalten.
Ursache	Ist in einer Zeile eine Ursache eingetragen, zeigt die Auswahl dieser Zeile im Fenster darunter nähere Informationen zu dieser Ursache an.

Tab. 83: Konfigurations-Check Tabelle

7.11 Erreichbarkeits-Test (Ping)

Dieser Dialog bietet Ihnen die Möglichkeit, einen Erreichbarkeits-Test (Ping) für eine beliebige IP-Adresse direkt vom Gerät aus durchzuführen.
Für spezielle Fälle wie z.B. einem Erreichbarkeits-Test durch einen VPN-Tunnel, haben Sie die Möglichkeit, die Quelladresse der Pings manuell vorzugeben.

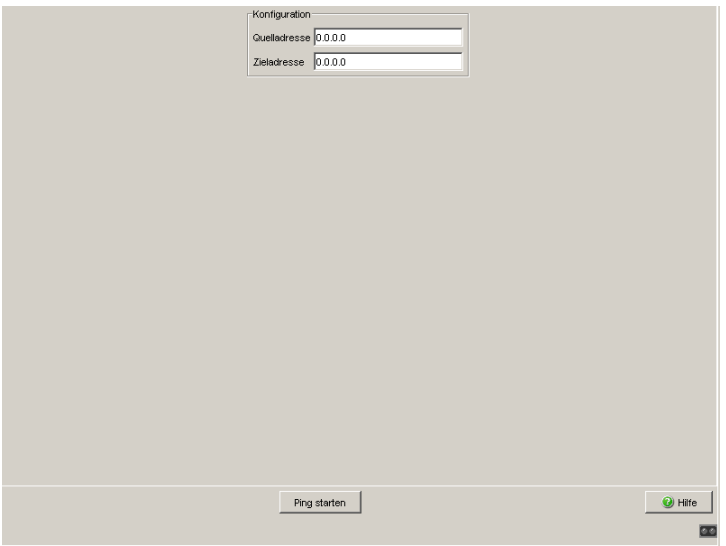


Abb. 39: Ping-Dialog (Erreichbarkeits-Test)

Parameter	Bedeutung	Mögliche Werte
Quelladresse	Absendeadresse für die ICMP-Echo-Anforderungen (Pings), im Normalfall 0.0.0.0. Bei 0.0.0.0 als Quelladresse verwendet die Firewall die IP-Adresse des Interface, an dem die Pings ausgesandt werden. Die Firewall bestimmt das Interface aus der Zieladresse und der Routing-Tabelle. Stellen Sie für besondere Fälle (z.B. um zu erreichen, dass der Erreichbarkeits-Test einen bestimmten VPN-Tunnel benutzt) eine andere IP-Adresse ein. Lieferzustand: 0.0.0.0	IPv4-Adresse, normalerweise 0.0.0.0
Zieladresse	Zieladresse der ICMP-Echo-Anforderungen (Pings). Lieferzustand: 0.0.0.0	Beliebige, zu testende IPv4-Adresse, nicht 0.0.0.0
Ping starten	Klicken Sie auf „Ping starten“, um den Erreichbarkeits-test zu starten. Das Gerät stellt nach wenigen Sekunden das Ergebnis in Textform in einem neuen Dialogfenster dar.	-

Tab. 84: Tabelle Ping-Dialog

8 Erweitert

Das Erweitert-Menü enthält die Dialoge:

- DNS
- Paketweiterleitung
- DHCP-Relay-Agent
- DHCP-Server

8.1 DNS

Das Domain-Name-System (DNS) ermöglicht die Verwendung von Namen (z.B. www.example.com) statt IP-Adressen im Internet. Bei der Eingabe von Host-Namen, z.B. zur Herstellung einer Verbindung mit einer Gegenstelle, startet ein Gerät (z.B. ein PC) eine DNS-Anfrage auf einem oder mehreren DNS-Servern nach der zugehörigen IP-Adresse (Namensauflösung). Der DNS-Server, der die angefragte Namensauflösung kennt, teilt dem anfragenden Gerät (DNS-Client) die zugehörige IP-Adresse mit. Die DNS-Server können über den Internet-Service-Provider erreicht werden oder auch im lokalen Netz installiert sein.
Das EAGLE One-Gerät bietet Ihnen die Funktion eines DNS-Cache. Er speichert das Ergebnis der Namensauflösung für eine bestimmte Zeit, maximal bis zum Neustart, im flüchtigen Speicher (Cache). Weitere DNS-Anfragen, deren Ergebnis bereits im Cache gespeichert sind, kann das EAGLE One-Gerät somit sofort beantworteten, ohne dass eine erneute DNS-Anfrage bei einem DNS-Server notwendig ist. Das entlastet den zuständigen DNS-Server und Sie erhalten die Antwort schneller.

Ein DynDNS-Service ermöglicht Ihnen, dort einen Namen (DynDNS-Hostnamen) registrieren zu lassen, über den ein Gerät (z.B. PC zur Administrierung der Firewall) auch dynamisch vergebene IP-Adressen ermitteln kann.

8.1.1 DNS-Server

Dieser Dialog bietet Ihnen die Möglichkeit, einen oder mehrere DNS-Server anzugeben, auf denen das Gerät nach einer Namensauflösung sucht. Damit kann das Gerät, wenn es eine Verbindung zu einer Gegenstelle über einen Hostnamen aufbaut (z.B. VPN-Gateway), als DNS-Client die zugehörige IP-Adresse zu diesem Hostnamen ermitteln.

Wählen Sie im Feld „DNS-Client-Konfiguration“ die DNS-Server, auf die das Gerät für eine Namensauflösung zugreift.

- Provider: Der DNS-Client des Gerätes richtet DNS-Anfragen an die DNS-Server, die dem Gerät von dem Internet-Service-Providers zugewiesen wurden (z.B. über DHCP-Client oder PPPoE).
- Benutzer: Der DNS-Client des Gerätes richtet DNS-Anfragen an die vom Benutzer in den vier Feldern eingetragenen DNS- (Root-) Server in der Reihenfolge der Einträge. Sollte ein DNS- (Root-) Server nicht erreichbar sein, dann ermöglicht die Eingabe von mehr als einem DNS- (Root-) Server dem Gerät das Ausweichen auf einen anderen DNS- (Root-) Server. Im Benutzer-Modus ignoriert das Gerät die von einen Internet-Service-Provider zugewiesenen DNS-Server.

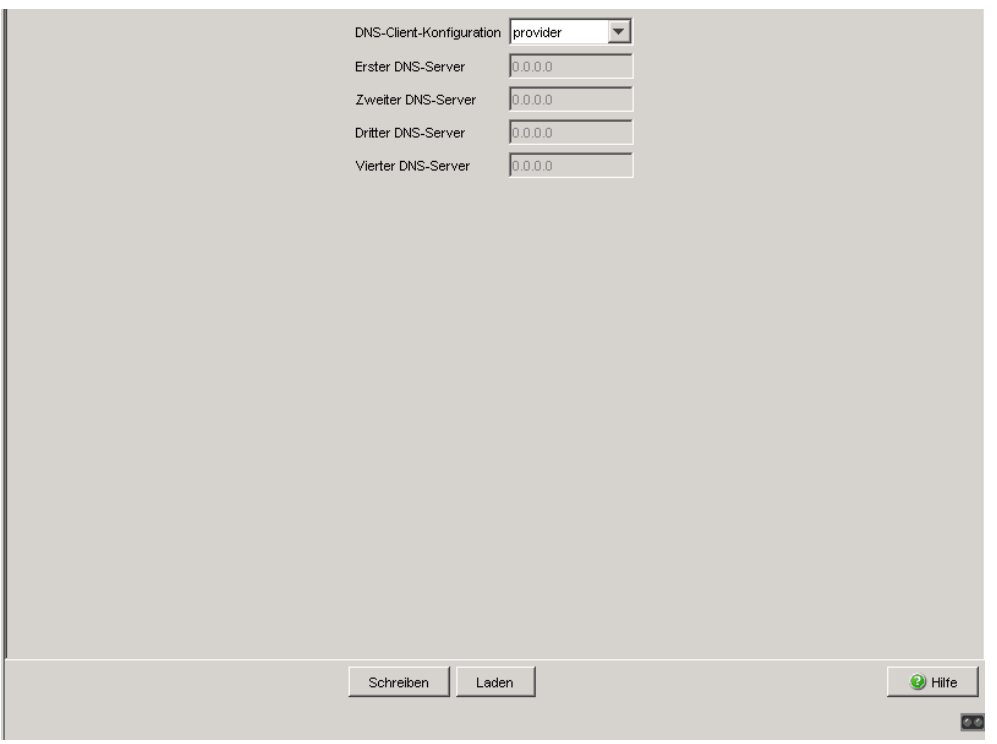


Abb. 40: DNS-Server

8.1.2 DynDNS

Melden Sie sich bei einem DynDNS-Dienst an, bevor Sie die DynDNS-Funktion nutzen. Das Gerät bietet Ihnen die Möglichkeit, diese Anmeldung auf der Web-Site „www.DynDNS.org” oder auf einer anderen von Ihnen wählbaren Website durchzuführen:

Dieser Dialog bietet Ihnen die Möglichkeit, die Registrierungsdaten aus Ihrer Anmeldung bei dem DynDNS-Dienst einzugeben. Über den registrierten Hostnamen kann das Gerät unter diesem Namen auch bei dynamisch zugewiesenen IP-Adressen (im PPPoE-Modus) über das Internet erreicht werden.

Parameter	Bedeutung
Provider	Auswahl der Web-Site des DynDNS-Anbieters: – dyndns-org: Web-Site www.DynDNS.org – other: von Ihnen wählbarer DynDNS-Anbieter Wenn Sie den Provider von „other" auf „dyndns-org" zurücksetzen, setzt das Gerät die Einstellungen für „Server" und „CheckIP Server" auf die von DynDNS.org vorgegebenen Einstellungen zurück.
Registrieren	Angekreuzt: Der DynDNS-Dienst ist eingeschaltet. Das Gerät prüft in den unter „Aktualisieren" angegebenen Zeitabständen seine IP-Adresse und übermittelt bei einer Änderung die neue Adresse zur Registrierung an den DynDNS-Dienst.. Nicht angekreuzt: Der DynDNS-Dienst ist ausgeschaltet.
Server	Eingeben des DNS-Servers. Verwenden Sie die vorgegebenen Einstellungen des von Ihnen unter „Provider" ausgewählten DynDNS-Anbieters. Voreinstellung: Von DynDNS.org vorgegebener DNS-Server „members.dyndns.org"
CheckIP Server	Eingeben des CheckIP-Servers zur Prüfung der IP-Adresse eines Gerätes. Verwenden Sie die vorgegebenen Einstellungen des von Ihnen unter „Provider" ausgewählten DynDNS-Anbieters. Voreinstellung: Von DynDNS.org vorgegebener CheckIP-Server „checkip.dyndns.org"
Login	Eingeben des Loginnamens aus der Registrierung bei dem von Ihnen gewählten DynDNS-Anbieter, z.B. bei DynDNS.org.
Passwort	Eingeben des Passworts aus der Registrierung bei dem von Ihnen gewählten DynDNS-Anbieter, z.B. bei DynDNS.org.
Hostname	Eingeben des Hostnamens aus der Registrierung bei dem von Ihnen gewählten DynDNS-Anbieter, z.B. bei DynDNS.org.
Aktualisieren	Aktualisierungsabstand in Minuten. Mögliche Werte: 1-6.000, Voreinstellung 10.
Status	Anzeige des Status des DynDNS-Client, (siehe auf Seite 210 „DynDNS - Status DynDNS-Client")

Tab. 85: DynDNS

Mögliche Werte	Bedeutung
Inactive	DynDNS ist nicht aktiv (z.B.“Registrieren“ist abgewählt, DNS-Server (siehe auf Seite 206 „DNS-Server“) ist nicht konfiguriert).
No change / in progress	DynDNS ist aktiv und prüft, ob sich die IP-Adresse geändert hat und damit, ob das Gerät die bei dem DynDNS-Dienst hinterlegte IP-Adresse aktualisieren muss.
Good / update done	Das Gerät hat die bei dem DynDNS-Dienst hinterlegte IP-Adresse erfolgreich aktualisert.
Bad user / bad password	Der DNS-Server des DynDNS-Dienstes hat den Login des Benutzers abgelehnt (Benutzer und/oder Passwort falsch).
No such host in system	Der DynDNS-Dienst kennt den angegebenen Hostnamen nicht.
Invalid hostname format	Der angegebene Hostname hat kein gültiges Format (FQDN = Fully Qualified Domain Name).
Host not in this account	Der angegebene Hostname ist für diesen DynDNS Account nicht bekannt (der Hostname gehört nicht diesem Benutzer).
No change	Der DynDNS-Dienst hat zweimal dasselbe Paar Hostname/IP-Adresse registriert.
Host has been blocked	Der DynDNS-Dienst hat mehrmals dasselbe Paar Hostname/IP-Adresse registriert (der Eintrag auf dem DynDNS-Server wurde dadurch blockiert).

Tab. 86: DynDNS - Status DynDNS-Client

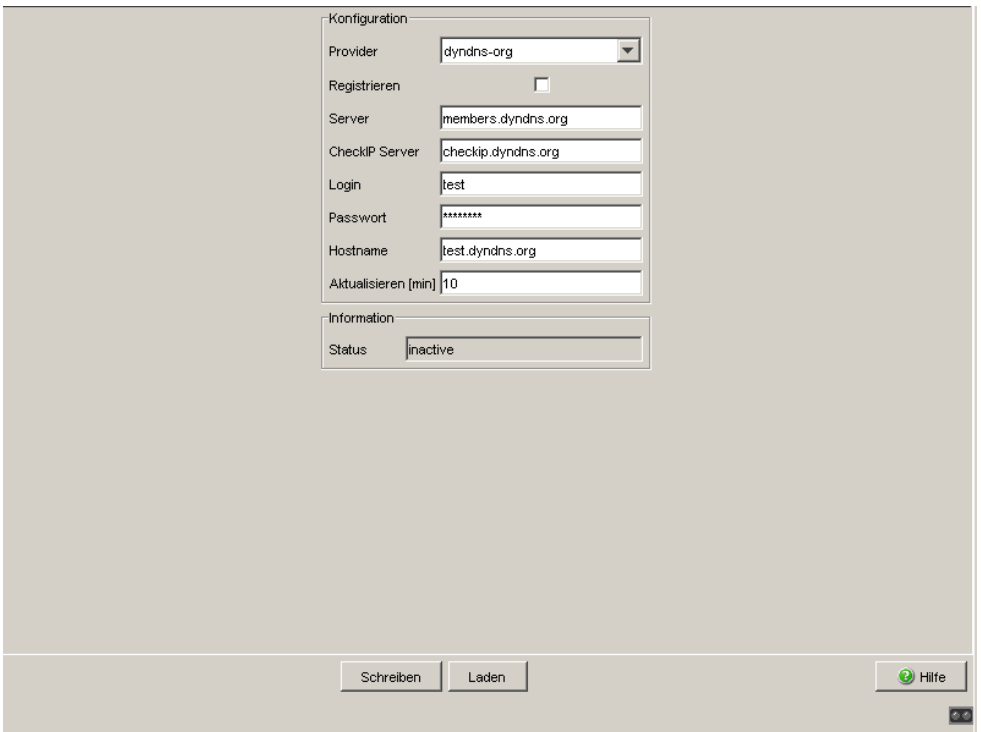


Abb. 41: DynDNS

8.2 Paketweiterleitung

Dieser Dialog bietet Ihnen die Möglichkeit, die Weiterleitung von RSTP-, GMRP- und DHCP-Datenpaketen im Transparent-Modus (siehe auf Seite 22 „Transparent-Modus“) ein- und auszuschalten.
Ist Paketweiterleitung eingeschaltet, dann ist das Gerät für diese Pakete transparent.
Im Router-Modus haben diese Einstellung keine Auswirkung, da das Gerät im Router-Modus keine Pakete auf Layer 2 weiterleitet.

Parameter	Bedeutung	Voreinstellung
RSTP	Weiterleitung von Rapid Spanning Tree Protokoll- (RSTP-) Datenpaketen ein-/ausschalten. RSTP ermöglicht bei mehrfache, redundante Verbindungen zwischen Teilnetzen Redundanz durch Unterbrechung von Schleifen.	`Ein`
GMRP	Weiterleitung von GMRP-Datenpaketen ein-/ausschalten. Das GMRP (GARP Multicast Registration Protocol) steuert die Weiterleitung von Multicasts. Indem das Gerät die Multicasts nur an die mit Hilfe von GMRP registrierten Geräte weiterleitet, reduziert es die Netzlast.	`Aus`
DHCP	Weiterleitung von DHCP-Datenpaketen ein-/ausschalten. Geräte mit DHCP als Konfigurationsmodus beziehen ihre Konfigurationsdaten von einem DHCP-Server. Dadurch können diese sehr einfach neu eingebunden oder ausgetauscht werden.	`Aus`

Tab. 87: Paketweiterleitung

Anmerkung: Die Weiterleitung von DHCP-Datenpaketen funktioniert nur im Transparent-Modus. Wenn Sie das Gerät im Router-Modus betreiben, bietet Ihnen das Gerät die Möglichkeit, den DHCP-Verkehr über das DHCP-Relay zulassen (siehe auf Seite 214 „DHCP-Relay-Agent“).

Abb. 42: Paketweiterleitung

8.3 DHCP-Relay-Agent

Dieser Dialog ermöglicht Ihnen, den DHCP-Relay-Agenten zu konfigurieren.

Anmerkung: Der DHCP-Relay-Agent funktioniert nur im Router-Modus. Wenn Sie das Gerät im Transparent-Modus betreiben, können Sie den DHCP-Verkehr über die Einstellung „Paketweiterleitung“ zulassen (siehe auf Seite 212 „Paketweiterleitung“).

Anmerkung: Der DHCP-Relay-Agent trägt beim Weiterleiten von DHCP-Paketen an den Server als Quelladresse die IP-Adresse des Interface ein, an dem das Paket empfangen wurde. Tragen Sie in der Konfiguration Ihres DHCP-Servers eine Route zu dieser Interface-Adresse ein. Das hilft Ihnen, die Kommunikation sicherzustellen.

☐ Geben Sie die DHCP-Server-IP-Adressen ein.
Sollte ein DHCP-Server nicht erreichbar sein, dann ermöglicht die Eingabe von bis zur drei weiteren DHCP-Server-IP-Adressen dem Gerät das Ausweichen auf einen anderen DHCP-Server.

Parameter	Bedeutung
Server-IP-Adresse	Eingeben der DHCP-Server-IP-Adresse. Sollte ein DHCP-Server nicht erreichbar sein, dann ermöglicht die Eingabe von bis zur drei weiteren DHCP-Server-IP-Adressen dem Gerät das Ausweichen auf einen anderen DHCP-Server.
DHCP-Relay-Status	Anzeige des DHCP-Relay-Status. Die DHCP-Relay-Funktion ist aktiv, wenn – in „Server-IP-Adresse“ mindestens eine IP-Adresse eingetragen ist und – der DHCP-Server (siehe auf Seite 218 „Pool“) auf keinem der beiden Interfaces aktiv ist.
Hirschmann-Gerät	Kreuzen Sie die Interfaces an, an denen ein Gerät von Hirschmann angeschlossen ist. Das hilft Ihnen sicherzustellen, dass der DHCP-Server an ein Hirschmann-Austauschgerät wieder die gleiche IP-Adresse vergibt. **Anmerkung:** Da die Firewall ein Sicherheitsgerät ist, unterstützt sie ausschließlich Standard-DHCP. Aus diesem Grund kreuzen Sie die Interfaces nicht an, an denen ein EAGLE One-Gerät angeschlossen ist.

Tab. 88: DHCP-Relay-Agent

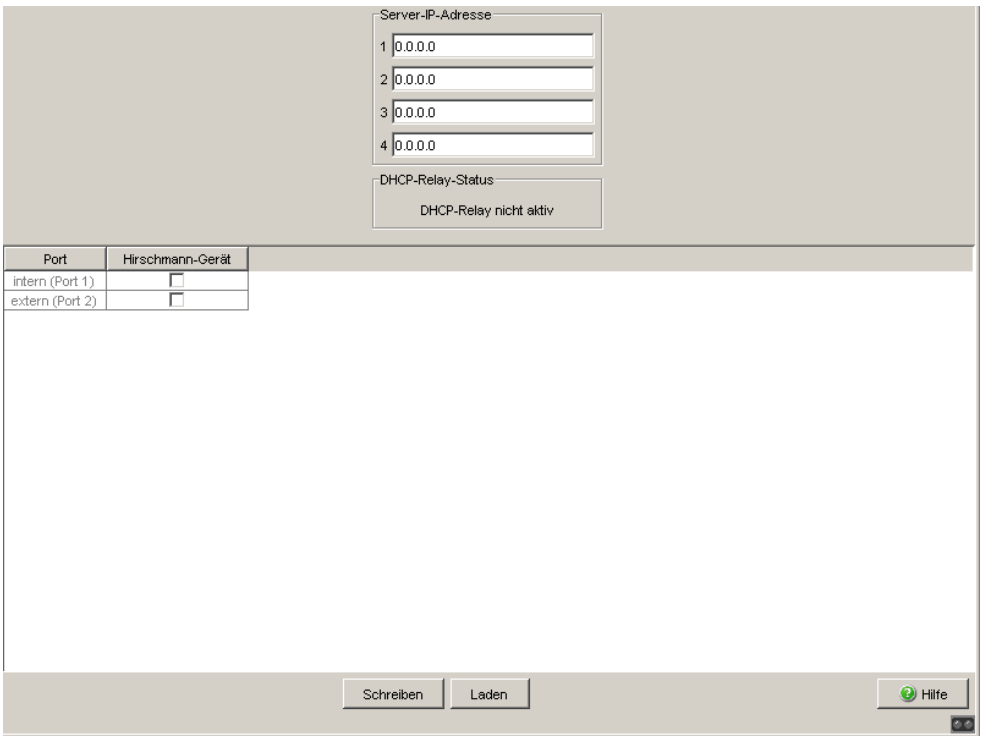


Abb. 43: Dialog DHCP-Relay-Agent

Anmerkung: Schalten Sie im Dialog `Erweitert:Paketweiterleitung` (siehe Seite 212) die Weiterleitung von DHCP-Paketen aus.

8.4 DHCP-Server

Die DHCP-Server-Dialoge bieten Ihnen die Möglichkeit, einfach Geräte (Clients) neu in Ihr Netz einzubinden oder in Ihrem Netz auszutauschen: Durch die Wahl von DHCP als Konfigurationsmodus beim Client holt sich dieser die Konfigurationsdaten von dem DHCP-Server.

Der DHCP-Server vergibt an den Client:

– eine fest eingestellte IP-Adresse (statisch) oder eine Adresse aus einem Adressbereich (dynamisch),
– die Netzmaske,
– die Gateway-Adresse,
– die DNS-Server-Adresse,
– die WINS-Server-Adresse und
– die Lease-Zeit.

Zusätzlich können Sie pro Port einen URL zur Übertragung von weiteren Konfigurationsparametern auf den Client angeben.

8.4.1 Pool

Dieser Dialog bietet Ihnen die Möglichkeit, die Vergabe von IP-Adressen detailliert zu steuern. Sie können den DHCP-Server pro Port oder pro VLAN ein- bzw. ausschalten. Der DHCP-Server bietet dazu einen sogenannten IP-Adress-Pool (kurz „Pool“), aus dem er IP-Adressen an Clients vergibt. Der Pool besteht aus einer Liste von Einträgen. Ein Eintrag kann eine bestimmte IP-Adresse oder einen zusammenhängenden IP-Adressbereich definieren. Sie haben die Wahl zwischen einer dynamischen und einer statischen Vergabe.

- Ein Eintrag für die dynamische Vergabe gilt für den Port des Geräts, für die Sie den DHCP-Server aktivieren. Meldet sich ein Client an diesem Port, dann weist der DHCP-Server eine noch freie IP-Adresse aus dem Pool-Eintrag für diesen Port zu.
  Für eine dynamische Zuteilung erstellen Sie einen Pool-Eintrag für einen Port und tragen die 1. und die letzte IP-Adresse des IP-Adressbereichs ein. Lassen Sie die Felder MAC-Adresse, Client-ID, Remote-ID und Circuit-ID frei.
  Sie haben die Möglichkeit, 1 Pool-Eintrag pro Port zu erzeugen.
- Bei einer statischen Vergabe weist der DHCP-Server stets die selbe IP-Adresse an einen Client zu. Der DHCP-Server identifiziert den Client über eine eindeutige Hardware-ID.
  Ein statischer Adress-Eintrag kann ausschließlich 1 IP-Adresse enthalten und gilt für den zugehörigen Port des Gerätes.
  Für eine statische Zuteilung erstellen Sie einen Pool-Eintrag für den Port, tragen die IP-Adresse ein und lassen das Feld „Letzte IP-Adresse“ frei. Geben Sie eine Hardware-ID an, mit der der DHCP-Server den Client eindeutig identifiziert. Diese ID kann eine MAC-Adresse, eine Client-ID, eine Remote-ID oder eine Circuit-ID sein. Meldet sich ein Client mit einer bekannten Hardware-ID, dann weist der DHCP-Server die statische IP-Adresse zu.

Die Tabelle zeigt Ihnen die konfigurierten Einträge des DHCP-Server-Pools an. Sie haben die Möglichkeit, einen Eintrag neu zu erzeugen, einen bestehenden Eintrag zu editieren oder Einträge zu löschen.
Sie haben die Möglichkeit für jeden Port des Gerätes 1 Pool-Eintrag zu erzeugen. Die Pools können zusammen bis zu 64 Einträge enthalten.

Um einen neuen Eintrag zu erzeugen, klicken Sie auf „Eintrag erzeugen“. Das Gerät zeigt einen neuen Dialog an. Füllen Sie die Felder aus, die Sie benötigen und klicken Sie anschließend auf „Schreiben“. Klicken Sie auf „Zurück“, um zum Dialog „Pool“ zurückzugelangen.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Port	Port, für den dieser Eintrag gilt.	`intern (Port 1)`, extern (Port 2)	`intern (Port 1)`
Aktiv	Aktiviert oder deaktiviert den Pool-Eintrag.	`An`, `Aus`	`Aus`
IP-Adresse	▶ Für einen dynamischen Adress-Eintrag: Die 1. Adresse des IP-Adress-Pools, die der DHCP-Server an einen Client vergibt. ▶ Für einen statischen Adress-Eintrag: Die IP-Adresse, die der Server stets an den selben Client vergibt.	Gültige IPv4-Adresse	-
Letzte IP-Adresse	Für einen dynamischen Adress-Eintrag: Die letzte Adresse des IP-Adress-Pools, die der DHCP-Server an einen Client vergibt.	Gültige IPv4-Adresse	-

Tab. 89: DHCP-Server-Pool-Einstellungen, IP-Adress-Grundeinstellungen

Parameter	Bedeutung	Wertebereich	Voreinstellung
Lease-Time [s]	Zeit in s, für die der DHCP-Server die Adresse dem Client zuteilt. Innerhalb der Lease-Zeit kann der Client eine Verlängerung beantragen. Beantragt der Client keine Verlängerung, nimmt der DHCP-Server die IP-Adresse nach ihrem Ablaufen wieder in den Pool auf und teilt sie bei Bedarf einen beliebigen Client zu.	1 s - 4.294.967.295 s (2^{32}-1 s)	86.400 s (1 Tag)
MAC-Adresse	Für einen statischen Adress-Eintrag: MAC-Adresse, mit der sich der Client identifiziert.	MAC-Adresse des Clients, der die statische IP-Adresse erhält	-
Gateway	IP-Adresse des DHCP-Relays, über das der Client seine Anfrage stellt. Empfängt der DHCP-Server eine Anfrage über ein anderes DHCP-Relay, ignoriert er diese. Befindet sich zwischen dem Client und dem DHCP-Server kein DHCP-Relay, lassen Sie dieses Feld leer.	IPv4-Adresse des DHCP-Relays.	-
Client-ID	Für einen statischen Adress-Eintrag: Client-ID, mit der sich der Client identifiziert.	Client-ID des Clients, der die statische IP-Adresse erhält[a]	-
Remote-ID	Für einen statischen Adress-Eintrag: Remote-ID, mit der sich der Client identifiziert.	Remote-ID des Clients, der die statische IP-Adresse erhält[a]	-

Tab. 90: DHCP-Server-Pool-Einstellungen, Modus der Adressvergabe

Parameter	Bedeutung	Wertebereich	Voreinstellung
Circuit-ID	Für einen statischen Adress-Eintrag: Circuit-ID, mit der sich der Client identifiziert.	Circuit-ID des Clients, der die statische IP-Adresse erhält[a]	-
Hirschmann-Gerät	Kreuzen Sie die Zeilen an, in denen ein Gerät von Hirschmann als Client eingetragen ist. Das hilft Ihnen sicherzustellen, dass der DHCP-Server an ein Hirschmann-Austauschgerät wieder die gleiche IP-Adresse vergibt. **Anmerkung:** Da ein EAGLE One-Gerät ein Sicherheitsgerät ist, unterstützt es ausschließlich Standard-DHCP. Aus diesem Grund lassen Sie die Zeilen unmarkiert, in denen ein EAGLE One-Gerät eingetragen ist. **Anmerkung:** Ändern Sie beim Austausch eines Client-Gerätes die MAC-Adresse auf die des neuen Clients.	`An`, `Aus`	`Aus`

Tab. 90: DHCP-Server-Pool-Einstellungen, Modus der Adressvergabe

– [a] Eine Client-, Remote- oder Circuit-ID besteht aus 1 - 255 Bytes in Hexadezimalschreibweise (00 - ff), durch Leerzeichen getrennt.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Konfigurations-URL	TFTP-URL, von dem der Client weitere Konfigurationsinformationen beziehen soll. Geben Sie den URL an im Format tftp://servername-oder-ip-addresse/verzeichnis/datei.	Gültiger TFTP-URL	-
Default-Gateway	Default-Gateway-Eintrag für den Client.	Gültige IPv4-Adresse	-
Netzmaske	Netzmasken-Eintrag für den Client.	Gültige IPv4-Netzmaske	-
WINS-Server	WINS- (Windows Internet Name Service-) Eintrag für den Client.	Gültige IPv4-Adresse	-
DNS-Server	DNS-Server-Eintrag für den Client.	Gültige IPv4-Adresse	-
Hostname	Hostname für den Client. Ist dieser Name angegeben, überschreibt er den Systemnamen des Clients (siehe auf Seite 17 „Systemdaten“).	Max. 64 ASCII-Zeichen im Bereich 0x21 (!) - 0x7e (~).	- (Kein Hostname)

Tab. 91: DHCP-Server-Pool-Einstellungen, Optionsvergabe an den Client

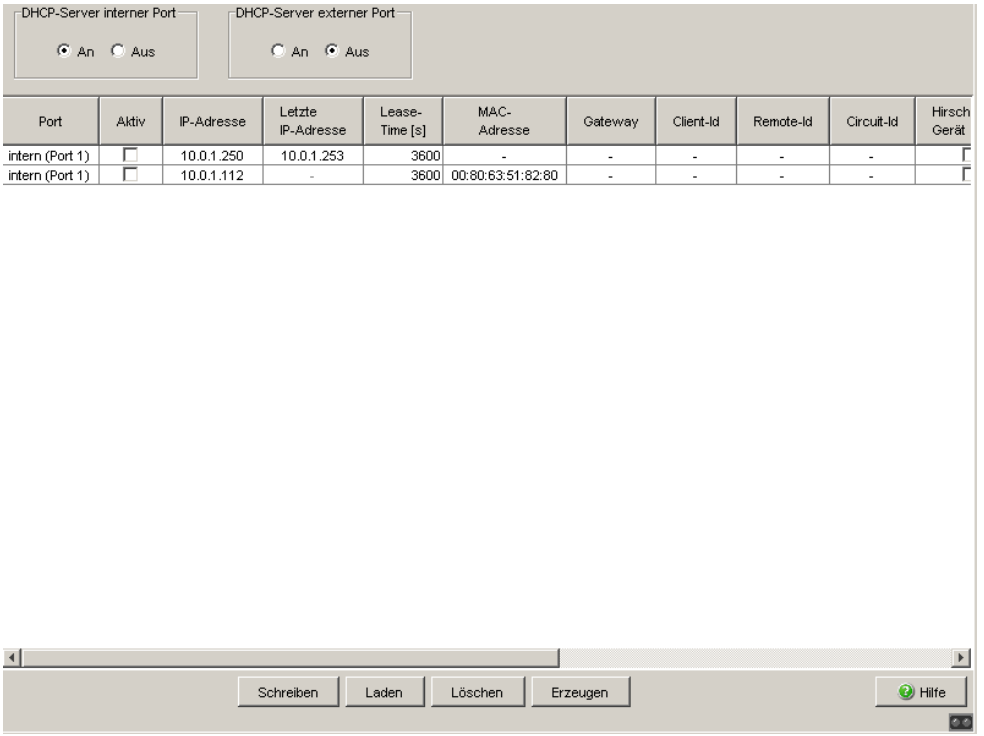


Abb. 44: Dialog DHCP-Server-Pool pro Port

8.4.2 Lease-Tabelle

Die Lease-Tabelle (engl. Lease: Vermietung) zeigt Ihnen die IP-Adressen an, die der DHCP-Server aktuell vergeben hat.
Zu jeder vergebenen IP-Adresse zeigt das Gerät die zugehörigen Details an.
Das Gerät bietet Ihnen die Möglichkeit, bis zu 1.024 Adressen zu vergeben.

Parameter	Bedeutung	Wertebereich
Port	Port, für die dieser Eintrag gilt.	`intern (Port 1)`, `extern (Port 2)`
IP-Adresse	IP-Adresse, die der DHCP-Server an das Gerät mit der angegebenen MAC-Adresse vergeben hat.	Eine IPv4-Adresse aus dem Pool.
Status	Zustand der DHCP-Adressvergabe gemäß dem Dynamic Host Configuration Protocol.	`bootp`, `offering`, `requesting`, `bound`, `renewing`, `rebinding`, `declined`, `released`
Verbleibende Lease-Zeit [s]	Verbleibende Zeit in Sekunden, bis die Gültigkeit der IP-Adresse abläuft, es sei denn der Client beantragt eine Verlängerung.	-
Vergeben an (MAC-Adresse)	MAC-Adresse des Clients, der die IP-Adresse aktuell geleast hat.	Format xx:xx:xx:xx:xx
Gateway	IP-Adresse des DHCP-Relay, über das der Client die Anfrage gestellt hat.	IPv4-Adresse oder leer
Lokale (Client-) ID	Die Client-ID, die der Client bei der DHCP-Anfrage angegeben hat.	[a]
Entfernte ID	Die Remote-ID, die der Client bei der DHCP-Anfrage angegeben hat.	[a]
Circuit-ID	Die Circuit-ID, die der Client bei der DHCP-Anfrage angegeben hat.	[a]

Tab. 92: DHCP-Lease-Tabelle

– [a] Eine Client-, Remote- oder Circuit-ID besteht aus 1 - 255 Bytes in Hexadezimalschreibweise (00 - ff), durch Leerzeichen getrennt.

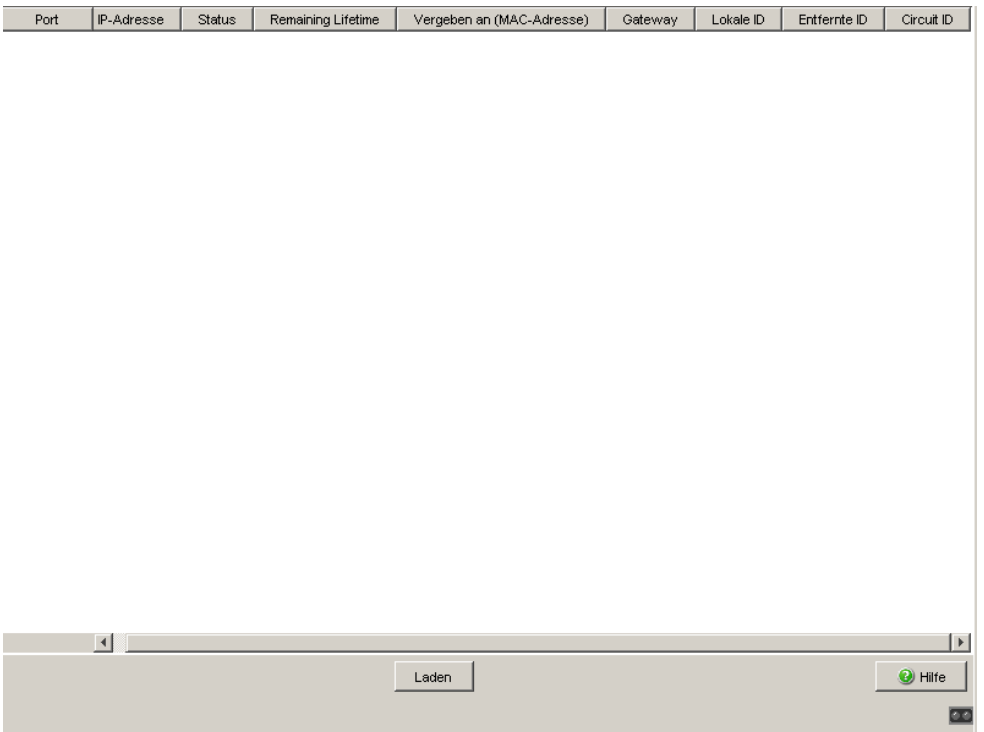


Abb. 45: Dialog DHCP-Server-Lease-Tabelle

9 Abmelden

Dieser Dialog bietet Ihnen die Möglichkeit, die automatische Abmeldung für die verschiedenen Benutzeroberflächen zu konfigurieren. Außerdem können Sie sich sofort von der grafischen Benutzeroberfläche abmelden.

- Grafische Benutzeroberfläche: automatisches Abmelden aktivieren / deaktivieren und Zeitspanne für automatisches Abmelden einstellen. Außerdem sofortiges Abmelden von der grafischen Benutzeroberfläche.
- SSH-Verbindung: Zeitspanne für automatisches Abmelden einstellen.
- Command Line Interface (V.24): automatisches Abmelden aktivieren / deaktivieren und Zeitspanne für automatisches Abmelden einstellen.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Grafische Benutzer-oberfläche			
Jetzt abmelden	Sofortiges Abmelden durch einen Klick auf „Jetzt abmelden“.		
Automatisch	Ein-/Ausschalten der automatischen Abmeldefunktion.	An/Aus	An
Nach [min]	Eingabe der Zeit in Minuten, nach der das Gerät die Verbindung trennt, wenn Sie keine Eingaben vornehmen.	0-120 (0: Aus)	5 (An)
SSH-Verbindung			
Automatisch nach [min]	Eingabe der Zeit in Minuten, nach der das Gerät die Verbindung trennt, wenn Sie keine Eingaben vornehmen.	1-120	5
Command Line Inter-face			
Automatisch	Ein-/Ausschalten der automatischen Abmeldefunktion.	An/Aus	An
Nach [min]	Eingabe der Zeit in Minuten, nach der das Gerät die Verbindung trennt, wenn Sie keine Eingaben vornehmen.	0-120 (0: Aus)	5 (An)

Tab. 93: Abmelden

Anmerkung: Um nach einem Abmelden wieder Zugriff auf das Gerät über die grafische Benutzeroberfläche zu erhalten, starten Sie die grafische Benutzeroberfläche erneut und melden Sie sich an.

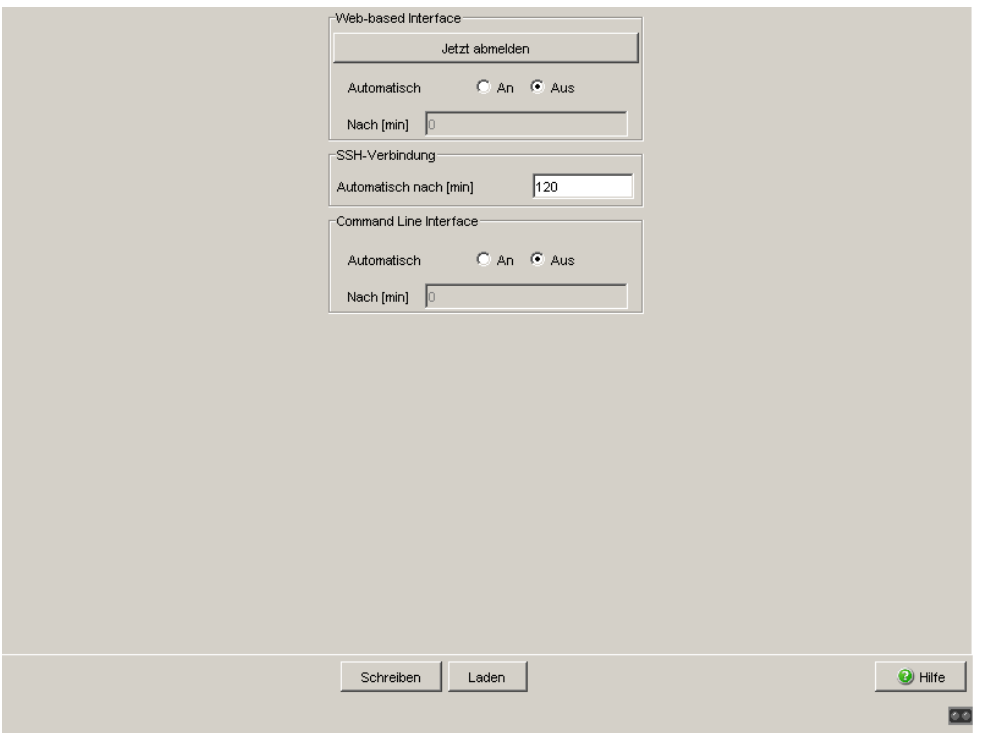


Abb. 46: Abmelden

A Allgemeine Informationen

A.1 Liste der RFCs

RFC 768	UDP
RFC 791	IP
RFC 792	ICMP
RFC 793	TCP
RFC 826	ARP
RFC 1157	SNMPv1
RFC 1155	SMIv1
RFC 1212	Concise MIB Definitions
RFC 1213	MIB2
RFC 1769	SNTP
RFC 1867	Form-Based File Upload in HTML
RFC 1901	Community based SNMP v2
RFC 1905	Protocol Operations for SNMP v2
RFC 1906	Transport Mappings for SNMP v2
RFC 1907	Management Information Base for SNMP v2
RFC 1908	Coexistence between SNMP v1 and SNMP v2
RFC 1918	Address Allocation for Private Internets
RFC 1945	HTTP/1.0
RFC 2068	HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03
RFC 2131	DHCP
RFC 2132	DHCP-Options
RFC 2233	The Interfaces Group MIB using SMI v2
RFC 2246	The TLS Protocol, Version 1.0
RFC 2271	SNMP Framework MIB
RFC 2346	AES Ciphersuites for Transport Layer Security
RFC 24xx	IPsec, IKEv1 - there are several RFCs that apply to IPsec, IKEv1
RFC 2570	Introduction to SNMP v3
RFC 2571	Architecture for Describing SNMP Management Frameworks
RFC 2572	Message Processing and Dispatching for SNMP
RFC 2573	SNMP v3 Applications
RFC 2574	User Based Security Model for SNMP v3
RFC 2575	View Based Access Control Model for SNMP
RFC 2576	Coexistence between SNMP v1, v2 & v3
RFC 2578	SMIv2
RFC 2579	Textual Conventions for SMI v2
RFC 2580	Conformance statements for SMI v2
RFC 2618	RADIUS Authentication Client MIB
RFC 2663	IP Network Address Translator (NAT) Terminology and Considerations
RFC 2818	HTTP over TLS

RFC 2851	Internet Addresses MIB
RFC 2865	RADIUS Client
RFC 2868	RADIUS Attributes for Tunnel Protocol Support
RFC 2869	RADIUS Extensions
RFC 3022	Traditional IP Network Address Translator
RFC 3164	The BSD syslog Protocol
RFC 3947	Negotiation of NAT-Traversal in the IKE
RFC 3948	UDP Encapsulation of IPsec ESP Packets
RFC 43xx	IPsec, IKEv2 - there are several RFCs that apply to IPsec, IKEv2
RFC 5905	NTPv4

A.2 Zugrundeliegende IEEE-Normen

IEEE 802.1AB	Link aggregation
IEEE 802.1D	Switching, GARP, GMRP, Spanning Tree (the device supports packet forwarding only)
IEEE 802.1D-1998, IEEE 802.1D-2004	Media access control (MAC) bridges (includes IEEE 802.1p Priority and Dynamic Multicast Filtering, GARP, GMRP)
IEEE 802.3-2002	Ethernet
IEEE 802.3ac	VLAN Tagging

A.3 Technische Daten

VLAN	
VLAN ID	1 bis 4.094

Routing/Switching	
Anzahl zusätzlicher IP-Adressen	32
Maximale Anzahl statischer Routing-Einträge	64

Firewall	
Maximale Anzahl IP-Regeln (zusammen)	1024
Maximale Anzahl MAC-Regeln (zusammen)	256
Maximale Anzahl SPI-Einträge (Stateful Packet Inspection)	4.096

NAT	
Maximale Anzahl NAT-Regeln	bis zu 512, je nach NAT-Typ
Maximale Anzahl 1:1-NAT-Adressen-übersetzungs-Einträge (Mapping Table)	4.096 (einstellbar), Voreinstellung: 1.024

VPN	
Maximale Anzahl konfigurierbarer Verbindungen	256
Maximale Anzahl aktiver Verbindungen	64

DHCP-Server	
Maximale Anzahl konfigurierbarer IP-Adressen, die vergeben werden können	1.024
Lease-Zeit	Pro Pool-Eintrag konfigurierbar, Voreinstellung 86.400 s (1 Tag)

A.4 Wartung

Hirschmann arbeitet ständig an der Verbesserung und Weiterentwicklung der Software. Prüfen Sie regelmäßig, ob ein neuerer Stand der Software Ihnen weitere Vorteile bietet. Informationen und Downloads von Software finden Sie auf den Produktseiten der Hirschmann-Website.

A.4.1 Service-Shell

Die Service-Shell-Funktion dient der Wartung Ihres funktionsfähigen Gerätes durch einen Servicetechniker. Falls Sie Serviceunterstützung benötigen, bietet diese Funktion dem Servicetechniker die Möglichkeit, von außerhalb auf interne Funktionen Ihres Geräts zuzugreifen.

Anmerkung: Die Service-Shell-Funktion dient ausschließlich Servicezwecken. Sie ermöglicht den Zugriff auf interne Funktionen des Geräts. Führen Sie keinesfalls interne Funktionen ohne die Anweisung eines Servicetechnikers aus. Das Ausführen interner Funktionen wie beispielsweise das Löschen des NVM-Inhalts (permanenter Speicher) führt unter Umständen dazu, dass Ihr Gerät funktionsunfähig wird.

Anmerkung: Das Deaktivieren der Service-Shell-Funktion hat permanente Wirkung.
Um die Service-Shell-Funktion reaktivieren zu lassen, senden Sie das Gerät zurück an den Hersteller.

A.5 Copyright integrierter Software

A.5.1 Bouncy Castle Crypto APIs (Java)

The Legion Of The Bouncy Castle
Copyright (c) 2000 - 2004 The Legion Of The Bouncy Castle
(http://www.bouncycastle.org)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

A.5.2 Network Time Protocol Version 4 Distribution

Copyright © David L. Mills 1992-2007

Permission to use, copy, modify, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name University of Delaware not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability this software for any purpose. It is provided "as is" without express or implied warranty

The following individuals contributed in part to the Network Time Protocol Distribution Version 4 and are acknowledged as authors of this work.

- Mark Andrews <mark_andrews@isc.org> Leitch atomic clock controller
- Bernd Altmeier <altmeier@atlsoft.de> hopf Elektronik serial line and PCI-bus devices
- Viraj Bais <vbais@mailman1.intel.com> and Clayton Kirkwood <kirkwood@striderfm.intel.com> port to Windows NT 3.5
- Michael Barone <michael,barone@lmco.com> GPSVME fixes
- Jean-Francois Boudreault <Jean-Francois.Boudreault@viagenie.qc.ca>, IPv6 support
- Karl Berry <karl@owl.HQ.ileaf.com> syslog to file option
- Greg Brackley <greg.brackley@bigfoot.com> Major rework of WINNT port. Clean up recvbuf and iosignal code into separate modules.
- Marc Brett <Marc.Brett@westgeo.com> Magnavox GPS clock driver
- Piete Brooks <Piete.Brooks@cl.cam.ac.uk> MSF clock driver, Trimble PARSE support
- Reg Clemens <reg@dwf.com> Oncore driver (Current maintainer)
- Steve Clift <clift@ml.csiro.au> OMEGA clock driver
- Casey Crellin <casey@csc.co.za> vxWorks (Tornado) port and help with target configuration
- Sven Dietrich <sven_dietrich@trimble.com> Palisade reference clock driver, NT adj. residuals, integrated Greg's Winnt port.
- John A. Dundas III <dundas@salt.jpl.nasa.gov> Apple A/UX port
- Torsten Duwe <duwe@immd4.informatik.uni-erlangen.de> Linux port
- Dennis Ferguson <dennis@mrbill.canet.ca> foundation code for NTP Version 2 as specified in RFC-1119
- John Hay <jhay@@icomtek.csir.co.za> IPv6 support and testing
- Glenn Hollinger <glenn@herald.usask.ca> GOES clock driver

– Mike Iglesias <iglesias@uci.edu> DEC Alpha port
– Jim Jagielski <jim@jagubox.gsfc.nasa.gov> A/UX port
– Jeff Johnson <jbj@chatham.usdesign.com> massive prototyping overhaul
– Hans Lambermont <Hans.Lambermont@nl.origin-it.com> or <H.Lambermont@chello.nl> ntpsweep
– Poul-Henning Kamp <phk@FreeBSD.ORG> Oncore driver (Original author)
– Frank Kardel <kardel (at) ntp (dot) org> PARSE <GENERIC> driver (>14 reference clocks), STREAMS modules for PARSE, support scripts, syslog cleanup, dynamic interface handling
– William L. Jones <jones@hermes.chpc.utexas.edu> RS/6000 AIX modifications, HPUX modifications
– Dave Katz <dkatz@cisco.com> RS/6000 AIX port
– Craig Leres <leres@ee.lbl.gov> 4.4BSD port, ppsclock, Magnavox GPS clock driver
– George Lindholm <lindholm@ucs.ubc.ca> SunOS 5.1 port
– Louis A. Mamakos <louie@ni.umd.edu> MD5-based authentication
– Lars H. Mathiesen <thorinn@diku.dk> adaptation of foundation code for Version 3 as specified in RFC-1305
– Danny Mayer <mayer@ntp.org>Network I/O, Windows Port, Code Maintenance
– David L. Mills <mills@udel.edu> Version 4 foundation: clock discipline, authentication, precision kernel; clock drivers: Spectracom, Austron, Arbiter, Heath, ATOM, ACTS, KSI/Odetics; audio clock drivers: CHU, WWV/H, IRIG
– Wolfgang Moeller <moeller@gwdgv1.dnet.gwdg.de> VMS port
– Jeffrey Mogul <mogul@pa.dec.com> ntptrace utility
– Tom Moore <tmoore@fievel.daytonoh.ncr.com> i386 svr4 port
– Kamal A Mostafa <kamal@whence.com> SCO OpenServer port
– Derek Mulcahy <derek@toybox.demon.co.uk> and Damon Hart-Davis <d@hd.org> ARCRON MSF clock driver
– Rainer Pruy <Rainer.Pruy@informatik.uni-erlangen.de> monitoring/trap scripts, statistics file handling
– Dirce Richards <dirce@zk3.dec.com> Digital UNIX V4.0 port
– Wilfredo Sánchez <wsanchez@apple.com> added support for NetInfo
– Nick Sayer <mrapple@quack.kfu.com> SunOS streams modules
– Jack Sasportas <jack@innovativeinternet.com> Saved a Lot of space on the stuff in the html/pic/ subdirectory
– Ray Schnitzler <schnitz@unipress.com> Unixware1 port
– Michael Shields <shields@tembel.org> USNO clock driver
– Jeff Steinman <jss@pebbles.jpl.nasa.gov> Datum PTS clock driver

– Harlan Stenn <harlan@pfcs.com> GNU automake/autoconfigure makeover, various other bits (see the ChangeLog)
– Kenneth Stone <ken@sdd.hp.com> HP-UX port
– Ajit Thyagarajan <ajit@ee.udel.edu>IP multicast/anycast support
– Tomoaki TSURUOKA <tsuruoka@nc.fukuoka-u.ac.jp>TRAK clock driver
– Paul A Vixie <vixie@vix.com> TrueTime GPS driver, generic TrueTime clock driver
– Ulrich Windl <Ulrich.Windl@rz.uni-regensburg.de> corrected and validated HTML documents according to the HTML DTD

B Leserkritik

Wie denken Sie über dieses Handbuch? Wir sind stets bemüht, in unseren Handbüchern das betreffende Produkt vollständig zu beschreiben und wichtiges Hintergrundwissen zu vermitteln, um Sie beim Einsatz dieses Produkts zu unterstützen. Ihre Kommentare und Anregungen helfen uns dabei, die Qualität und den Informationsgrad dieser Dokumentation weiter zu steigern.

Ihre Beurteilung für dieses Handbuch:

	sehr gut	**gut**	**befriedigend**	**mäßig**	**schlecht**
Exakte Beschreibung	O	O	O	O	O
Lesbarkeit	O	O	O	O	O
Verständlichkeit	O	O	O	O	O
Beispiele	O	O	O	O	O
Aufbau	O	O	O	O	O
Vollständigkeit	O	O	O	O	O
Grafiken	O	O	O	O	O
Zeichnungen	O	O	O	O	O
Tabellen	O	O	O	O	O

Haben Sie in diesem Handbuch Fehler entdeckt?
Wenn ja, welche auf welcher Seite?

Leserkritik

Anregungen, Verbesserungsvorschläge, Ergänzungsvorschläge:

Allgemeine Kommentare:

Absender:

Firma / Abteilung:

Name / Telefonnummer:

Straße:

PLZ / Ort:

E-Mail:

Datum / Unterschrift:

Sehr geehrter Anwender,

Bitte schicken Sie dieses Blatt ausgefüllt zurück

- als Fax an die Nummer +49 (0)7127 14-1600 oder
- per Post an

Hirschmann Automation and Control GmbH
Abteilung 01RD-NT
Stuttgarter Str. 45-51
72654 Neckartenzlingen

C Stichwortverzeichnis

D Weitere Unterstützung

Technische Fragen

Bei technischen Fragen wenden Sie sich bitte an den Hirschmann-Vertragspartner in Ihrer Nähe oder direkt an Hirschmann.

Die Adressen unserer Vertragspartner finden Sie im Internet unter http://www.hirschmann.com

Unser Support steht Ihnen zur Verfügung unter https://hirschmann-support.belden.eu.com

Sie erreichen uns

in der Region EMEA unter
- Tel.: +49 (0)1805 14-1538
- E-Mail: hac.support@belden.com

in der Region Amerika unter
- Tel.: +1 (717) 217-2270
- E-Mail: inet-support.us@belden.com

in der Region Asien-Pazifik unter
- Tel.: +65 6854 9860
- E-Mail: inet-ap@belden.com

Hirschmann Competence Center

Das Hirschmann Competence Center mit dem kompletten Spektrum innovativer Dienstleistungen hat vor den Wettbewerbern gleich dreifach die Nase vorn:

- Das Consulting umfasst die gesamte technische Beratung von der Systembewertung über die Netzplanung bis hin zur Projektierung.
- Das Training bietet Grundlagenvermittlung, Produkteinweisung und Anwenderschulung mit Zertifizierung.
  Das aktuelle Schulungsangebot zu Technologie und Produkten finden Sie unter http://www.hicomcenter.com
- Der Support reicht von der Inbetriebnahme über den Bereitschafts-service bis zu Wartungskonzepten.

Mit dem Hirschmann Competence Center entscheiden Sie sich in jedem Fall gegen jeglichen Kompromiss. Das kundenindividuelle Angebot lässt Ihnen die Wahl, welche Komponenten Sie in Anspruch nehmen.
Internet:
http://www.hicomcenter.com

HIRSCHMANN

A BELDEN BRAND