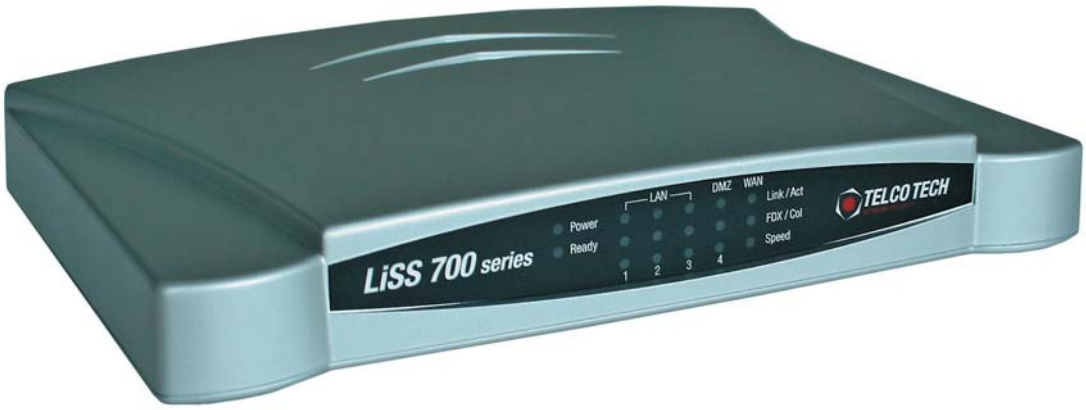
TELCO TECH GmbH
NETWORK SECURITY

Dokumentation



LiSS 700 series

Made In Germany

Telco Tech GmbH

Potsdamer Straße 18a
14513 Teltow

LiSS 700 series
Dokumentation

Firmwareversion 1.0.0

Autor(en):

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Zu dieser Dokumentation

In dieser Dokumentation wird die LiSS 700 series der Telco Tech GmbH vorgestellt und im einzelnen beschrieben. Es werden alle Funktionen beschrieben, die für LiSS 700 series verfügbar sind. Nicht alle dieser Funktionen sind auf allen LiSS 700 series Geräten verfügbar. Aus der Beschreibung aller Funktionen der LiSS 700 series Systeme in dieser Dokumentation entsteht kein Anspruch auf Nutzung für den Anwender. Der Anwender erwirbt mit seinem LiSS 700 series System eine bestimmte Zusammenstellung von Funktionalitäten, diese entspricht nicht in jedem Fall der maximal verfügbaren Anzahl.

Diese Dokumentation bietet keinen Anspruch auf Vollständigkeit. Änderungen sind vorbehalten. Diese Dokumentation wird sich, ebenso wie die hier beschriebenen LiSS 700 series Systeme, weiterentwickeln. Als Leser und Anwender sind Sie herzlich dazu aufgefordert Ihre Wünsche und Vorschläge zur Verbesserung der Dokumentation mit einzubringen.

Die Sprache der Oberfläche ist von der Standardsprache des Webbrowsers abhängig. Zur Zeit sind Deutsch und Englisch verfügbar.

Abbildung 1: LiSS 700 series

1 LiSS series 700 Systeme

1.1 Funktionen im Überblick

LiSS Series Systeme sind Unified Threat Management[1] Appliances. Sie vereinen verschiedene Sicherheitsaufgaben auf nur einem System, welches als komplette Hardwarelösung angeboten wird. Basis der LiSS Appliances ist ein eigens entwickeltes Betriebssystem auf Linuxbasis, welches hinsichtlich Performance, Platzbedarf und Sicherheit optimiert wurde. LiSS series Systeme stellen eine Vielzahl von Sicherheitsfunktionen bereit.

Internet-Gateway

Als Internet-Gateway realisieren LiSS Geräte die Anbindung von Unternehmensnetzen an die Infrastruktur des Internet. Die Internet-Anbindung kann direkt über einen Router, oder über *PPPoE* (DSL) erfolgen.

Firewall

Die Firewall besteht zum einen aus einem *Paket-Filter*, der das Arbeiten mit *IP-Gruppen* genau so unterstützt, wie die Verwendung der verschiedensten Formen von *NAT*. Berechtigungen werden anhand von Diensten vergeben, so das eine Trennung von technischer Administration und organisatorischer Administration erreicht wird. Mit dem Paket-Filter wird definiert, welche Systeme mit welchen Diensten kommunizieren dürfen.

[1] Unified Threat Management - kurz UTM

Des weiteren sorgt das *Intrusion Detection System*[2] dafür, das über die zugelassenen Kommunikationskanäle Angriffe auf vorhandene Ressourcen erkannt und verhindert werden.

Virtual Private Network (VPN)

Verteilte Standorte oder Außendienstmitarbeiter können über die einfache Konfiguration von IPsec-VPN problemlos an den zentralen Standort angebunden werden. Durch Verwendung des IPsec-VPN-Standards ist eine Verbindung mit extrem hoher Sicherheit und guter Interoperabilität mit Geräten andere Hersteller möglich.

Surf Protection

Die Nutzung des Web kann über IP-Adressen kontrolliert werden. Das Protokollieren der Internetzugriffe ermöglicht eine Langzeitarchivierung ebenso wie die statistische Auswertung.

Die dabei übertragenen Inhalte können über einen leistungsfähigen *Contentfilter* gefiltert werden.

1.2 Hardware

Die LiSS 700 series ist ein auf einem Xscale 266MHz Prozessor basierendes System. Das Gerät ist durch den integrierten 4-Portswitch ideal für kleine Umgebungen wie Homeoffice und geringe Nutzerzahlen. Ein separater WAN-Port kann zur Anbindung an ein DSL-Modem bzw. einen Router genutzt werden.

[2] Intrusion Detection System - kurz IDS

2 Produkt-Merkmale

Verschlüsselter Administrationszugang (HTTPS)

Die Administration erfolgt nur über eine HTTPS-Verbindung.

Überwachung wichtiger Prozesse

Ein Softwarewatchdog prüft wichtige Prozesse und startet diese bei Ausfall oder Nichtreagieren ggf. automatisch neu.

Bestätigen von Firewallkonfigurationen

Etablieren neuer Firewall-Regeln erst nach einer Bestätigung verhindert ein “Aussperren” vom LiSS System bei Konfiguration der Firewall. So wird sichergestellt, das die Administrationsverbindung auch bei Fehleingaben des Administrators bestehen bleibt.

Plausibilitätsüberprüfung

Bei der Konfiguration am System werden nur die für die Konfiguration relevanten Daten ausgewählt und zur Anzeige gebracht. Dies verhindert Fehleingaben und erhöht die Übersichtlichkeit.

Bedienphilosophie

Häufige Fehlerquelle sind Fehleingaben von Konfigurationsdaten. LiSS series Systeme minimieren diese Fehlerquelle, indem einmal eingegebene Konfigurationswerte für spätere Verwendung gespeichert werden. Dies ist besonders sinnvoll beim Arbeiten mit IP-Adressen, RSA-Schlüsseln und X.509 Zertifikaten.

Unterstützung von IPv6

Die LiSS series Systeme unterstützen bereits IPv6. Somit können auch Datenpakete nach dem neuen Internetprotokollstandard geroutet werden.

LED	Anzeige	Bedeutung
power	dauerhaft grün	Gerät erhält Betriebsspannung
Ready	grün blinkend	Systemüberwachung, Gerät betriebsbereit
Ready	dauerhaft grün	erfolgreiche PPP-Einwahl über WAN-Schnittstelle
Ready	dauerhaft aus	beim Firmwarereset, Firmware des Auslieferungszustandes wird geladen

Tabelle 1: LiSS 700 series LEDs

Signalisierung von Systemzuständen per LEDs

Auf der Vorderseite der LiSS series Geräte befinden sich die *Power* und die *Ready* LED. Liegt Betriebsspannung vom externen Netzteil an, so leuchtet die *Power LED* grün.

Ist das LiSS 700 series Gerät in einem betriebsbereitem Zustand, dann blinkt die grüne *Ready LED*. Hat das Gerät erfolgreich eine PPP-Einwahl absolviert, dann leuchtet die *Ready LED* dauerhaft grün.

3 Hinweise zur Bedienung

Passwortänderung nach Erstanmeldung

Um zu vermeiden, daß dauerhaft Passwörter der Werkseinstellungen auf LiSS Systemen verwendet werden, wird bei der ersten Verbindung zum LiSS Gerät die Änderung des Passwortes erzwungen.

Arbeit mit mehrseitigen Assistenten

Zur verbesserten Benutzerführung und Übersichtlichkeit werden viele Eingaben durch Assistenten abgefragt. Dies verhindert unter anderem fehlerhafte Eingaben.

Speichern nur bei Veränderungen der Konfiguration möglich

Bei Veränderung der Konfigurationsdaten wird der Administrator aufgefordert seine Eingabe durch Speichern zu bestätigen, oder durch Abbrechen zu verwerfen.

Einheitliches Bedienkonzept

Alle Dialoge sind nach dem gleichen Prinzip gestaltet. Es wird in vielen Dialogen ein Querverweis zu anderen Konfigurationsmasken angeboten.

Automatische Abmeldung nach 15 Min Inaktivität

Findet 15 Minuten kein Zugriff per *https* auf das LiSS Gerät statt, wird der gerade angemeldete Administrator automatisch abgemeldet. Alle bis dahin noch nicht gespeicherten Änderungen gehen verloren.

Meldungen in der Statuszeile

Wichtige Informationen bei der Administration des Gerätes werden dem Benutzer in der Statuszeile angezeigt.

4 Erstinbetriebnahme

4.1 Auspacken und Anschließen des Gerätes

Das Liss series Gerät sollte nach dem Auspacken mit dem mitgeliefertem Netzteil an das Stromnetz angeschlossen werden. Um Hardwaredefekte zu vermeiden, ist das Gerät erst einzuschalten, wenn die Gerätetemperatur sich der Raumtemperatur angepaßt hat.

4.2 Netzwerkverbindung

Zur Ersteinrichtung liegt der LiSS 700 series ein Faltblatt bei, auf dem alle nötigen Schritte einzeln erklärt sind. Die Ersteinrichtung erfolgt dabei analog den größeren LiSS series Systemen. Über eine https-Verbindung kann die LiSS 700 series administriert werden. Dazu ist eine Netzwerkverbindung des Administrationsrechners zum LiSS Gerät nötig. Im einfachsten Fall sind *LAN-Schnittstelle* des LiSS 700 series Gerätes und Administrationsrechner über ein direktes Kabel miteinander verbunden und der Administrationsrechner besitzt eine IP-Adresse aus dem Netz 192.168.1.0/24.

Es besteht ebenso die Möglichkeit, sich am Administrationsrechner über den in Werkseinstellung aktiven DHCP-Server des LiSS Gerätes eine IP-Adresse zuweisen zu lassen.

4.3 Webbrowser

Für die Administration des LiSS Gerätes wird ein Webbrowser mit XML/XSLT Unterstützung und eine Bildschirmauflösung von 1024x768 Punkten benötigt. Es wird die aktuelle Programmversion des *Mozilla Firefox* Webbrowsers empfohlen.

4.3.1 Erste Anmeldung

Über die URL *https://192.168.1.1* wird die Loginseite des LiSS Gerätes erreicht. Ist das SSL-Zertifikat der HTTPS-Verbindung vom Webserver der LiSS, dem verwendeten Webbrowser unbekannt, wird der Benutzer aufgefordert dies zu akzeptieren. Wird das Zertifikat nicht akzeptiert, kann keine HTTPS-Verbindung aufgebaut werden.
Nach erfolgreicher Erstanmeldung mit den Logindaten der Werkseinstellungen wird die Passwortänderung erzwungen. Werkseinstellungsdaten sind auf Seite II im Anhang aufgeführt.

4.3.2 Änderung des Werkseinstellungspasswortes

Nach erfolgreichem Login mit den Werkseinstellungsdaten wird die Maske zum Ändern des Passwortes angezeigt. Hier ist ein neues Passwort gemäß der geltenden Passwortrichtlinie einzugeben und zu bestätigen.

Laut Statuszeile ist nun eine Abmeldung erforderlich. Erst wenn der Administrator mit dem geänderten Passwort angemeldet ist, kann er das Gerät uneingeschränkt administrieren.

5 Netzwerk

Die LiSS 700 series verfügt über zwei separate Ethernet-Netzwerkinterfaces. Diese sind einmal LAN-seitig als 4-Portswitch und WAN-seitig als einzelnes Ethernetinterface ausgelegt. In der Bedienoberfläche wird der 4-Portswitch als *eth0* und die WAN-Schnittstelle als *eth1* bezeichnet.

5.1 Main

5.1.1 Schnittstellen

Hier erfolgt die Konfiguration der IP-Adressen der verschiedenen Schnittstellen des LiSS 700 series Gerätes. Auf LiSS 700 series Geräten sind zeitgleich verschiedene Arten von Schnittstellen konfigurierbar. So ist eine Kombination von Router und Bridge auf einem Gerät möglich.

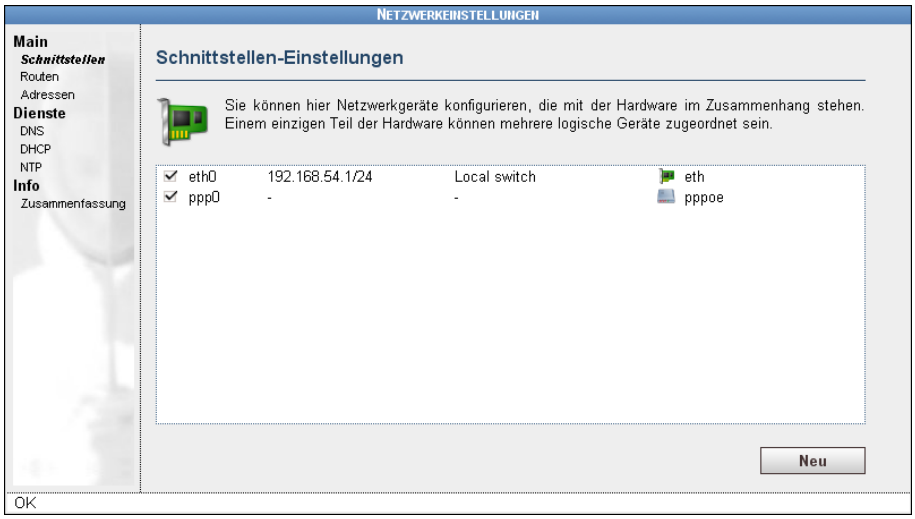


Abbildung 2: Netzwerk Main Schnittstellen

Über *Netzwerk - Main - Schnittstellen - Neu* kann eine neue Schnittstelle angelegt werden.

Ethernet-Schnittstelle

- eine IP-Adresse pro physikalischer Schnittstelle
- sind alle physikalischen Schnittstellen mit einer IP-Adresse belegt, führt die Einrichtung dieses Schnittstellentypes zu einer Einrichtung eines IP-Alias / virtuelle Schnittstelle
- *IP-Adresse*: - IP-Adresse ohne Netzmaske

- *Netzwerk-Präfix* entspricht Netzmaske in CIDR[3]-Schreibweise, Netzmaske in Kurzform
  - Beispiel: CIDR 24 entspricht 255.255.255.0
- *Kommentar (optional)* - zur besseren Dokumentation; empfehlenswert!
- *Redirects senden* - Erlaubt das Senden von ICMP-Redirect Nachrichten bei Verwendung von statischen Routen über das Liss series Gerät; der Client muß diese ICMP-Redirects annehmen, damit *redirect* funktioniert

DMZ-Port

Ein Port des 4-Portswitches ist als DMZ-Port ausgelegt. Der DMZ-Port ist kein separates Interface, dem eine IP-Adresse vergeben werden kann. Das Netzwerk, welches auf dem LAN-Port konfiguriert ist, liegt auch hier an. Ein direkter Zugriff von LAN / WAN in die DMZ wird dadurch verhindert, das die ARP-Request-Broadcasts aus den angeschlossenen Netzen im LiSS 700 series Gerät geblockt werden. Ein Zugriff auf die Endsysteme in der DMZ ist somit nur über das Routing der LiSS 700 series möglich.

Dadurch kann der Zugriff auf Systeme in der DMZ über die Firewall der LiSS 700 series kontrolliert werden. In der Firewall sind dann die IP-Adressen der Endsysteme in der DMZ als Filterkriterium anzugeben.

PPPoE-Schnittstelle

Eine PPP-Schnittstelle ist nur auf der WAN-Schnittstelle konfigurierbar.

- eine PPPoE-Schnittstelle pro Gerät möglich
- externes DSL-Modem erforderlich
- Bindung an eine physikalische Schnittstelle exklusiv
  - diese Schnittstelle kann nicht weiter für andere Schnittstellentypen verwendet werden
  - nur eine physikalische Schnittstelle pro PPPoE-Verbindung
- *Benutzername* - Nutzername beim DSL-Einwahl Provider

[3] Classless Inter-Domain Routing

  - Beispiel *t-online*: AnschlusskennungT-onlinenummer#Mitbenutzernummer@t-online.de
  - Beispiel *t-com Business*: t-online-com/Benutzername/@t-online-com.de

- *Passwort* - Passwort laut Angabe vom DSL-Einwahl Provider
- *Kommentar* - zur besseren Dokumentation; empfehlenswert!
- *Erweitert:*
  - *Reset PPP connection daily at (hour)* - Neueinwahl der DSL-Verbindung zur festen Zeit, verlagert eine eventuell störende Zwangstrennung in unkritischen Zeitbereich
    * 0..23 Uhr
    * Empfehlung: Trennung in die Nachtstunden verlegen
  - *MTU* - ermöglicht das manuelle verkleinern der MTU[4]
    * je nach Vorgabe des Providers vorzunehmen
  - *trennen nach* - nur nötig bei Verbindung bei Bedarf
    * Wartezeit
    * Zeit in der kein Datenpaket über die Leitung gehen darf, bis die Trennung erfolgt
  - *Wählen bei Bedarf* - verbinden bei Bedarf aktivieren
  - *eingehende Pakete ignorieren* - Pakete am Internetanschluß für das Rücksetzen der Wartezeit nicht berücksichtigen
    * wenn eine Verbindung bei Bedarf konfiguriert wird, ist diese Einstellung *unbedingt* zu aktivieren, damit die Wartezeit bis zur Trennung auch erreicht werden kann
  - *Fehlersuche* - aktiviert erhöhte Logausgabe

5.1.2 Routen

Routen zu nicht direkt an das LiSS series System angeschlossenen Netzen können hier konfiguriert werden. Mindestens eine solche Route existiert auf jedem Internetrouter, die *Defaultroute*.

- *Ziel* - Zielhost oder -netz, das über diese Route erreicht werden soll

[4] Maximum Transmission Unit

- *Gateway* - Routersystem, an welches die Daten zugestellt werden, um das *Ziel* zu erreichen
- *Gerät* - gibt die Schnittstelle an, über die die Daten das LiSS series Gerät in Richtung *Gateway* verlassen
- *Kommentar* - sollte für eine selbsterklärende Konfiguration genutzt werden

Defaultroute

Die Defaultroute gibt den Weg in Richtung Internet an. In Werkseinstellung existiert bereits eine Defaultroute, diese muß den Daten des Providers entsprechend angepaßt werden.

Als Ziel der *Defaultroute* wird die spezielle IP-Adresse 0.0.0.0/0 verwendet. Da 0.0.0.0/0 alle IP-Adressen von IPv4 einschließt, ist über diesen Routingeintrag jedes Paket zustellbar.

Soll ein System direkt mit dem Internet kommunizieren können, ist eine *Defaultroute* zwingend erforderlich. Ohne einen solchen Routingeintrag ist Internetzugriff lediglich über Proxies möglich.

Ist das nächste System in Richtung Internet ein Router mit fester IP-Adresse, wird als Gateway die IP-Adresse dieses Routers angegeben.

Bei Verwendung eines PPP-Anschlusses (DSL) ist kein *Gateway* bekannt. Hier wird nur die Schnittstelle mit ppp0 angegeben.

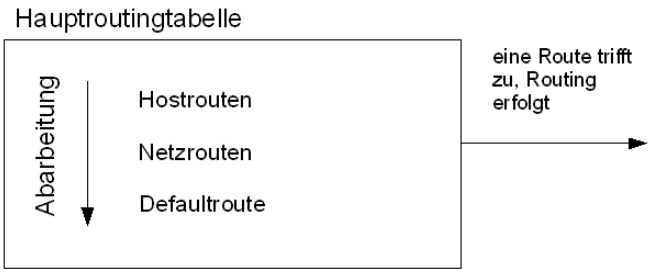


Abbildung 3: Netzwerk - Main - Routen

5.1.3 Adressen

Hier findet sich die zentrale IP-Adressverwaltung. Es können Adressen bearbeitet werden und ggf. Kommentare hinzugefügt werden. Über *Aufräumen* werden alle nicht in der Konfiguration des LiSS series Systems verwendeten Adressen gelöscht.

5.2 Dienste

5.2.1 DNS

Hier wird neben dem Hostnamen festgelegt, wie das LiSS 700 series System die Namensauflösung vornimmt.

LiSS 700 series Systeme können als Caching DNS-Proxy arbeiten. Dies ist sinnvoll, wenn im LAN kein DNS-Server verfügbar ist, der für die Clients die Namensauflösung durchführen kann.

- *Hostname* - DNS-Name des LiSS Gerätes
- *Hören an* - Schnittstelle, an der der Caching DNS-Proxy Anfragen entgegen nimmt
- *Forwarder* - erster und zweiter DNS-Server, an den die LiSS 700 series DNS-Anfragen stellt
- *Provider-DNS benutzen* - legt fest, ob und wenn ja von welcher PPP-Schnittstelle die übermittelten DNS-Server für die Namensauflösung benutzt werden
- *Zuerst die Forwarder anfragen* - hier kann die Reihenfolge der Abfrage definiert werden

- *Erweitert*:
  - *Anzahl der Cache-Einträge* - maximale Anzahl der Cache Einträge für den Caching DNS-Proxy
  - *Platzhalter zulassen* - Akzeptieren von Wildcardantworten zulassen, sonst sind nur konkrete Anfragen für Hosts bzw. MX-Record etc. möglich
  - *negative Antworten zwischenspeichern* - Aktivierung empfehlenswert, verringert Wartezeiten bei negativen Antworten
  - *SOA, SRV und Anfragen mit Unterstrichen sperren* - Anfragen an Active Directory typische Einträge nicht annehmen

5.2.2 DHCP

Die LiSS series Systeme bieten einen DHCP Server zur Nutzung an. Es können mehrere IP-Adresspools aus verschiedenen Netzen konfiguriert werden. Das LiSS series System ordnet die verschiedenen Bereiche automatisch den richtigen Netzwerkschnittstellen zu. Jeder DHCP-Bereich kann getrennt aktiviert werden. Das *Löschen* eines DHCP-Bereiches erfolgt innerhalb des *Bearbeiten* Dialoges.

5.2.3 NTP

Hier wird der NTP-Server auf dem LiSS series System konfiguriert, der Clients im LAN über NTP[5] die aktuelle Zeit zur Verfügung stellt. Die Administration beschränkt sich auf das Aktivieren des NTP-Servers und die Auswahl der Schnittstellen, an denen der Dienst zur Verfügung steht.

5.3 Info

5.3.1 Zusammenfassung

Hier werden alle aktuellen Schnittstellen-Konfigurationsparameter in einer Gesamtübersicht angezeigt.

[5] Net Time Protocol (UDP Port 123)

6 Firewall

Unter dem Punkt Firewall sind ein *Paket-Filter* und ein *Intrusion Detection System* angeordnet.

6.1 Paket-Filter

Mit Hilfe des Paket-Filters können Datenströme durch die LiSS series gezielt freigeschaltet werden. Weiterhin sind mit *Umleitung* und *Netmapping* Werkzeuge zur Paketmanipulation vorhanden. Um die Administration der Firewall zu vereinfachen werden die Kommunikationsparameter wie *Protokoll* und *Port* in *Diensten* zusammengefaßt. Der Paket-Filter bietet umfangreiche Loggingfunktionen, die bei der gezielten Freischaltung von Verbindungen hilfreich sind. Es wird vom Paket-Filter bereits IPv6 unterstützt.

6.1.1 Filterung

Der Paket-Filter enthält Regeln, die von oben nach unten abgearbeitet werden. Trifft eine Regel auf ein betrachtetes Datenpaket zu, wird die Aktion durchgeführt, die die Regel festlegt. Aktionen können dabei sein:

- *annehmen* - Erlauben der Verbindung
- *ablehnen* - Zurückweisen der Verbindung, Absender erhält eine ICMP-Nachricht “destination unreachable”
- *verwerfen*- Verbieten der Verbindung, Datenpaket wird einfach “weggeworfen”

Trifft keine der vorhandenen Regeln zu, entscheidet die *Standardrichtlinie*, wie letztendlich mit dem Paket zu verfahren ist. Es gibt zwei Möglichkeiten, den Paket-Filter zu konfigurieren:

- Standardrichtlinie: erlauben, Regelwerk besteht überwiegend aus Verbotsregeln
  - Problem: Was nicht verboten ist, ist erlaubt
- Standardrichtlinie: verbieten, Regelwerk besteht überwiegend aus Erlaubtregeln
  - Problem, was nicht erlaubt ist, kann nicht miteinander kommunizieren

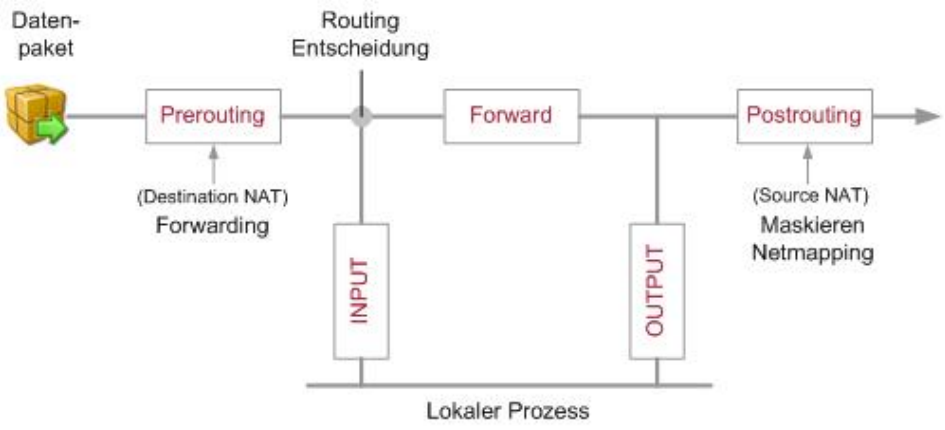


Abbildung 4: Firewall iptables Mechanismus

Die letztere Möglichkeit stellt dabei die sichere dar. Ist eine Verbindung (noch) nicht möglich, kann diese gezielt freigeschaltet werden. Siehe auch 6.1.6 auf Seite 30.

Die Regelliste des LiSS series Paket-Filters besteht aus *Systemregeln* und *nutzerdefinierten Regeln*.

Zuerst werden die Systemregeln und danach die nutzerdefinierten Regeln abgearbeitet. Systemregeln sind per Häkchen einfach ein- und ausschaltbar. Die Systemregeln des Paketfilters sind im Anhang in Tabelle 4 auf Seite VII aufgelistet.

Anlegen von Nutzerdefinierten Firewallregeln

Neue nutzerdefinierte Firewallregeln werden unter *Firewall - Paketfilter - Filterung - Neu* angelegt. Als erstes muß der Regeltyp angegeben werden. Hierzu ist es hilfreich den *iptables* Mechanismus in seiner Funktionsweise zu verstehen, siehe dazu auch Abb. 4. Es wird unterschieden, ob ein Ende der Kommunikation ein lokaler Prozeß auf dem LiSS System ist, oder ob beide Kommunikationspartner extern sind.

Mögliche Regeltypen sind:

- *extern - extern* - Kommunikationspartner außerhalb des LiSS Gerätes
- *LiSS - extern* - Kommunikation von LiSS Gerät nach extern
- *extern - LiSS* - Kommunikation von extern zum LiSS Gerät

Der Regeltyp kann später nicht geändert werden. Zum Ändern des Regeltyps muß eine neue Regel erstellt werden.

Weiterhin muß die IP-Version angegeben werden. Für die meisten Anwender wird IPv4 sicher ausreichen. Die LiSS series Systeme sind, soweit es die verwendeten Komponenten ermöglichen, IPv6 fähig. In der nächsten Seite des Assistenten werden weitere Konfigurationsdaten abgefragt. Zu bemerken ist, das es sich bei jeder Firewallregel um eine Definition einer Verbindung zwischen Quelle und Ziel handelt, dies also eine unidirektionale Kommunikation darstellt. Soll Datenverkehr zwischen zwei Standorten in beiden Richtungen freigegeben werden, müssen zwei separate Firewallregeln angelegt werden, zumindest solange es sich um Protokolle handelt, die richtungsabhängig sind, wie TCP.

- *Regelname* - Beschreibung der Firewallregel, empfehlenswert ist die Angabe der Standorte *ohne* Dienste. Diese werden bei *Diensten* angegeben und können sich im laufe der Zeit evtl. ändern
- *Plaziere Regel hinter/als* - Schnellpositionierung der Firewallregel in Regelliste
- *Aktion* - erlauben, verbieten, zurückweisen
- *Dienste* - Liste der anzuwendenden Dienste
- *Quelle (extern)* - IP-Adresse, IP-Netz bzw. MAC-Adresse oder IP-Gruppe und zugehörige eingehende Schnittstelle
- *Ziel (extern)* - IP-Adresse, IP-Netz oder IP-Gruppe und zugehörige ausgehende Schnittstelle
- *Weitere Einstellungen* - Maskierung / NAT, Logging und Limitierung

Für die Auswahl einer *IP-Gruppe* ist bei *Quelle* bzw. *Ziel* in der Zeile *IP-Gruppe verwenden* ein Häkchen zu setzen. Dann schaltet der Auswahldialog, erreichbar über das *gelbe Ordnersymbol*, in die Gruppenauswahl anstatt in die IP-Adressliste.

MAC-Adressen

MAC-Adressen aus lokal angeschlossenen Netzen können über die Quelle ausgewertet werden. Die Angabe der einzelnen hexadezimalen Werte der MAC-Adresse erfolgt durch Doppelpunkt ":" getrennt.

Schnittstellen

Bei der Auswahl der Schnittstellen gibt es auf einem Plus "+" endende Einträge. Die bedeutet, das das Plus als Platzhalter zu verstehen ist. *eth+* steht also für jede beliebige Ethernetschnittstelle.

NAT

Soll die LiSS series *NAT* durchführen, so ist dies in der Firewall zu definieren. *Source-* bzw. *Quell-NAT* läßt sich mit nutzerdefinierten Filterregeln bzw. über *Netz-Mapping* einrichten. *Destination-* bzw. *Ziel-NAT* läßt sich unter dem Punkt Umleitung definieren.

Die Einrichtung von *NAT* in nutzerdefinierten Firewallregeln erfolgt über *weitere Einstellungen*. Dort stehen verschiedene Einträge zur Auswahl:

- *nein* - die Absender-IP-Adresse wird nicht geändert
- *mask* - die Absender-IP-Adresse wird auf die IP-Adresse der Schnittstelle geändert, durch die das Datenpaket das LiSS Gerät verläßt; dazu ist eine Angabe der ausgehenden Schnittstelle unter *Ziel* nötig
- *überspringe* - es wird explizit *nicht* maskiert, ein Ausnahmeeintrag wird in der Postroutingchain eingetragen; evtl. nötig, wenn sich Regeln mit Maskierung und ohne Maskierung überlappen
- *statisch* - NAT mit einer ganz konkreten IP-Adresse, wenn ausgewählt, dann muß unter *Statische IP* die zu verwendende IP-Adresse eingetragen werden

NAT bzw. Maskierung ist dann zu wählen, wenn ein Übergang von einem Netz mit privatem IP-Adressraum in das Internet erfolgt, weil die privaten IP-Adressen im Internet nicht geroutet werden.

Protokollierung

Protokollierung kann bei Bedarf für jede Firewallregel separat angegeben werden. Somit ist es möglich nur ganz bestimmte Kommunikationen zu loggen. Zur Verringerung der Systemlast können verschiedene Loglevel ausgewählt werden. Um die jeweiligen Loggingeinträge besser im Logfile zu finden, kann ein *Log Präfix* angegeben werden. Dies ist ein Text, der zu Beginn des Logeintrags eingefügt wird. Wird kein Log Präfix angegeben, wird der Regelname als Log Präfix verwendet. Das Firewallog findet sich unter *Diagnose - Syslog - Firewall*.

Begrenzungen

Über *Begrenzungen* kann der Datenverkehr durch eine Firewallregel auf eine Anzahl an Clients oder Netze beschränkt werden. Somit läßt sich Last durch zahlreiche Zugriffe eingrenzen, die z.B. durch DoS-Attacken entstehen.

Verbotsregeln

Verbotsregeln sind Firewallregeln, denen als Aktion *ablehnen* oder *verwerfen* zugewiesen wurde. Durch das Einfügen von Verbotsregeln können Ausnahmen für einzelne Netze erstellt werden, für die Erlaubtregeln erstellt wurden. So kann z.B. einem Netz der Zugriff per HTTP erlaubt werden wobei der IP-Bereich der Hosts 13...27 davon ausgenommen bleiben sollen. Wichtig beim Arbeiten mit Verbotsregeln ist die Positionierung der Firewallregeln. Die Verbotsregeln müssen, bei Abarbeitung von oben nach unten, vor den Erlaubtregeln stehen!

Positionierung von Firewallregeln

Die Position einer Firewallregel im Gesamtregelwerk spielt zumindest beim Arbeiten mit Verbotsregeln eine Rolle. Es gibt zwei Möglichkeiten die Position einer Regel zu ändern:

- regelweises verschieben nach oben oder unten über die rechts in der Regelübersicht befindlichen Pfeile.
- durch editieren der Firewallregel und Angabe der Stelle, an der die Regel plaziert werden soll indem bei *Plaziere Regel hinter/als:* die vorangehende Firewallregel ausgewählt wird. (empfohlen bei größeren Sprüngen)

Regelübersicht

Unter *Firewall - Paket-Filter - Filterung* werden alle konfigurierten Firewallregeln in einer Übersicht dargestellt. Hier kann jede Regel per Häkchen aktiviert bzw. deaktiviert werden. Regelnamen und Dienstelisten können über Häkchen am unteren Bildrand aus- und eingeblendet werden. Somit sind mehr Firewallregeln darstellbar, ohne den vertikalen Scrollbar bemühen zu müssen. Über ein Suchfenster bei *Auswahl von Regeln* kann nach Bestandteilen der Regelkonfiguration gesucht werden. Soll in Regelnamen bzw. Diensten gesucht werden, ist die Anzeige dafür mit einzuschalten. Die Suche ist *caseinsensitiv*.

Anzeige erweiterter Einstellungen

Alle Firewallregeln, in denen *Maskiert* wird, werden durch ein “M” am rechten Rand gekennzeichnet.

Alle Firewallregeln, in denen statisches *NAT* verwendet wird, werden durch ein “S” am rechten Rand gekennzeichnet.

Alle Firewallregeln, die *Logging* aktiviert haben, werden durch ein “L” am rechten Rand gekennzeichnet.

Hinweise zum DMZ-Port

Da der DMZ-Port ein Port des Switches ist, ist dieser nicht als Interface bei der Firewallregelerstellung auswählbar. Um hier Sicherheit abzubilden, sollten die Endsysteme in der DMZ statische IP-Adressen haben, die dann als Ziel in der Firewallregel Verwendung finden.

6.1.2 Umleitung

Unter Umleitung wird *Destination-NAT* bzw. *Ziel-NAT* festgelegt. Es können Ziel-IP-Adresse bzw. Ziel-Port eines eingehenden Datenpaketes geändert werden. Dabei wird ebenfalls wieder mit Diensten gearbeitet. Welche Protokolle und Ports sich hinter einem Dienst verbergen, kann unter *Firewall - Paket-Filter - Dienste* eingesehen werden. Umleitungen sind dann sinnvoll, wenn eine Portumsetzung nötig ist, bzw. wenn in ein internes Netz mit privatem IP-Adressbereich von außen zugegriffen werden soll und das LiSS series Gerät das einzige System mit einer offiziellen IP-Adresse im Netz ist.

Einrichtung

Wird eine neue Umleitung eingerichtet, kann zwischen vier Typen gewählt werden. Siehe auch Tabelle 2 und Abb. 5.

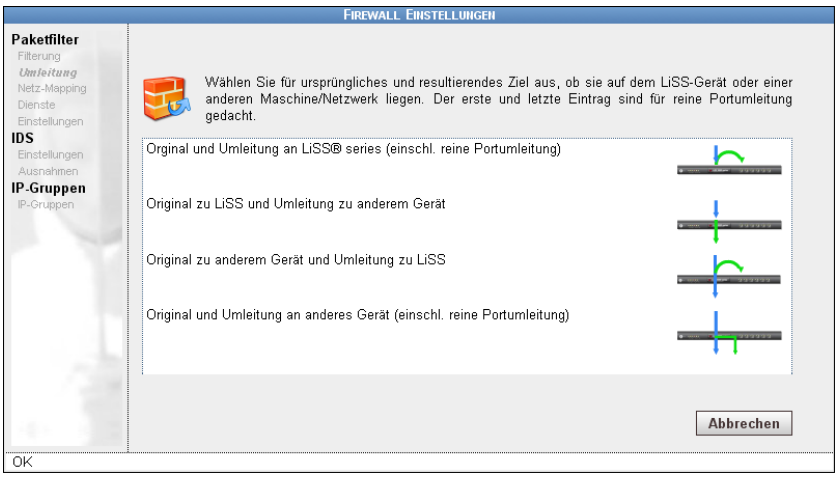


Abbildung 5: Firewall Umleitung Neu

Typ	Beispiel
Original und Umleitung an LiSS series (einschl. reine Portumleitung)	Einrichtung eines Hilfsadminports, wenn HTTPS für eine andere Umleitung benötigt wird
Original zu LiSS und Umleitung zu anderem Gerät	"klassische" Weiterleitung, z.B. HTTPS an Exchange-Server für Outlook Webaccess (OWA)
Original zu anderem Gerät und Umleitung zu LiSS	LiSS übernimmt Proxyanfragen der Clients, die an den alten Proxyserver gehen
Original und Umleitung an anderes Gerät (einschl. reine Portumleitung)	Server im LAN ändert seine IP-Adresse; Anfragen auf die alte Adresse werden auf neue IP-Adresse umgebogen

Tabelle 2: Firewall, Umleitungstypen

Der Typ einer Umleitung kann später nicht mehr geändert werden. Ist eine Änderung des Umleitungstypes nötig, so muß die Umleitungsregel neu erstellt werden.

Die Eingabemaske einer Umleitungsdefinition fragt folgendes ab:

- *Regelname:* - Beschreibung der Umleitungsregel, empfehlenswert ist die Angabe der Standorte *ohne* Dienste. Diese werden bei *Diensten* angegeben und können sich im laufe der Zeit evtl. ändern
- *Dienste:* - Liste der Dienste, für die die Umleitung gelten soll
- *Originales Ziel (LiSS):* - Ziel-IP-Adresse im eingehenden Datenpaket, Angabe der IP-Adresse, die für die Umleitung angesprochen wird
- *Neues Ziel (LiSS):* - neue Ziel-IP-Adresse, IP-Adresse des Systems, an das umgeleitet wird
- *Neue Zielports:* - Angabe der umzusetzenden Ports, wird Zielport bei der Umleitung nicht geändert, kann dieses Feld leer bleiben
- *Anhand Quelle erlauben:* - einschränken der Umleitung; Umleitung wird nur angewendet, wenn *Quelle* überein stimmt
- *Weitere Einstellungen:* - Maskierung, Logging, Begrenzung siehe auf Seite 23

Sind mehrere Umleitungsregeln definiert, können diese einzeln aktiviert und in der Reihenfolge verschoben werden.

6.1.3 Netz-Mapping

Mit Netz-Mapping kann *Source-NAT* bzw. *Quell-NAT* so definiert werden, das diese Umsetzung der Adressen für ganze IP-Netze gilt. Bedingung dafür ist, das altes Quell-Netz und neues Quell-Netz gleich groß sind, bzw. gleiche Netzmasken haben. Mapping für einzelne Systeme ist möglich, dann muß für jedes System eine Mappingregel erstellt werden.

Netz-Mapping wird benötigt, wenn an zwei verschiedenen Standorten die gleichen IP-Netze betrieben werden und eine Verbindung (VPN) zwischen den Standorten eingerichtet werden soll. So können mit Netz-Mapping beide Netze jeweils auf einen anderen Netzbereich umgesetzt werden, so das die Verbindung zwischen den Standorten dann zwischen unterschiedlichen Netzen erfolgt.

Auf den LiSS series Geräten gibt es verschiedene Netz-Mapping-Typen:

- Bidirektionales Mapping (alle Dienste)
- Quell-Mapping
- Ziel-Mapping

Bidirektionales Mapping gilt für alle Dienste. Das Mapping für die Rückrichtung wird automatisch eingerichtet. Soll das Netz-Mapping selektiv nur für einzelne Dienste eingerichtet werden, so ist dies separat für Hin- und Rückrichtung mit Quell- und Ziel-Mapping einzurichten. Die Einrichtung eines Bidirektionalen- bzw. Quell-Mappings erfordert folgende Eingaben:

- *Regelname:* - Beschreibung der Mappingregel
- *Originale Quelle:* - altes Quellnetz
- *Mappe Quelle auf:* - neues Quellnetz
- *Anhand Ziel erlauben:* - Einschränkung des Mappings; Mapping wird nur durchgeführt, wenn Bedingung *Ziel* erfüllt ist
- *Weitere Einstellungen:* - Logging, siehe auf Seite 23

Ziel-Mapping unterscheidet sich in der Angabe der Daten etwas vom Bidirektionalen- bzw. Quell-Mapping:

- *Originales Ziel:* - entspricht neuem Quellnetz

- *Mappe Ziel auf:* - entspricht altem Quellnetz

Für Quell- und Ziel-Mapping werden ebenfalls Dienste abgefragt

- *Dienste:* - Angabe der Dienste, für die das Mapping gültig ist

Sind mehrere Mappingregeln definiert, können diese einzeln aktiviert und in der Reihenfolge verschoben werden.

6.1.4 Dienste

Zur Vereinfachung der Konfiguration in Filterung, Umleitung und Netz-Mapping wird auf LiSS series Systemen mit Diensten gearbeitet. Dienste fassen dabei alle zu einer Kommunikation nötigen Daten zusammen. Gängige Dienste sind in der LiSS Firmware enthalten. Sind benötigte Dienste nicht vorhanden, können diese neu angelegt werden.

Ein Dienst beinhaltet neben Dienstname und Kommentar auch Angaben zu Protokollen und Ports. Diese können pro Dienst auch mehrfach angegeben werden. Weiterhin kann die Sichtbarkeit des Dienstes in der Diensteliste konfiguriert werden. Bei Angabe von Protokoll und Port können Hin- und Rückrichtung der Kommunikation auch getrennt konfiguriert werden. Angenehm ist jedoch das automatische Erstellenlassen der Rückdefinition.

Wird ein Dienst neu angelegt, muß zuerst die IP-Version angegeben werden, für die dieser erstellt wird. Neben Dienstname und Kommentar wird unter anderem unter *Erzeuge zustandsbehaftete Regeln* abgefragt, ob die Definition des Dienstes auch die Rückrichtung mit beinhaltet. Zustandsbehaftet heißt, der Dienst gibt nur die Hinrichtung vor, die Rückrichung wird über *stateful inspection* behandelt.

Bei Einrichtung eines Dienstes wird neben IP-Version und Protokoll folgendes abgefragt:

- Richtung:
  - Client - Server (Anfrage) - auszuwählen, wenn LiSS die Definition der Rückrichtung automatisch erstellen soll
  - Server Client (Antwort) - Antwort des Servers auf obige Anfrage, Ziel und Quellport sind vertauscht
  - Server Client (Anfrage) - Server fragt den Client an (Bsp. FTP Datenverbindung)
  - Client Server (Antwort) - Antwort des Clients auf obige Anfrage, Ziel und Quellport sind vertauscht

Die unteren drei Richtungsarten werden nur dann benötigt, wenn die Rückrichtung nicht automatisch erstellt wird.

- Service-Typ (ToS):
  - 0x00 - lösche ToS bits
  - 0x02 - min. Kosten
  - 0x04 - max. Zuverlässigkeit
  - 0x08 - max. Durchsatz
  - 0x10 - min. Verzögerung

Service-Typ meint hier die ToS[6]-Bits im IP-Header. Diese werden nur selten von einer Anwendung gesetzt. Für die meisten Dienste ist es deshalb ratsam hier nichts auszuwählen, d.h. *Service-Typ (ToS)* bleibt leer. Wird der Dienst mit einem speziellen ToS Wert definiert, trifft dieser Dienst auch nur zu, wenn im betrachteten Paket auch wirklich dieser ToS-Wert gesetzt ist! Die ToS-Bits sind nur dann bewußt zu ändern, wenn genaue Informationen über deren Wert vorliegen. Ist die Belegung der ToS-Bits unbekannt ist hier keine Einstellung vorzunehmen.

Ist das verwendete Protokoll TCP oder UDP, dann wird für die Absendeports der Bereich der nicht privilegierten oberen Ports (1024-65535) vorgeschlagen. Dies kann übernommen oder entsprechend angepaßt werden. Für *Zielports* ist der entsprechende Wert einzutragen. Dies kann ein einzelner Wert sein, ein Bereich (z.B. 1024-65535) oder eine Aufzählung von Ports (23, 1024-2048, 3333).

Ist *Automatische Antwort-Muster* aktiv, dann erstellt das LiSS Gerät die Definition für die Rückrichtung automatisch, was für die meisten Fälle zu empfehlen ist.

Das Anlegen eines Dienstes beschränkt sich also hauptsächlich auf Angabe von *Dienstname*, *Protokoll* und *Zielport*.

6.1.5 Einstellungen

Paketfilter aktivieren

Unter *Firewall - Paket-Filter - Einstellungen* wird der Firewalldienst ein- bzw. ausgeschaltet. Ist die Firewall ausgeschaltet, verhält sich das LiSS series Gerät wie ein normaler Router. Wenn das

[6] ToS = Type of Service, ein Feld im IPv4 Header

LiSS series Gerät das Grenzsystem zwischen Internet und LAN mit privatem IP-Adressbereich ist, dann kann das LAN nur mit dem Internet kommunizieren, wenn die Maskierfunktion der Firewall aktiv, d.h. die Firewall eingeschaltet ist. Die evtl. eingerichteten Fireallregeln mit NAT / Maskieren werden nicht angewendet, wenn der Paketfilterfilter deaktiviert ist.

Standard-Richtlinie

Zusätzlich zum Ein- und Ausschalten der Firewall findet sich hier die Konfiguration der Standardrichtlinie der Firewall. Empfehlungen zur Konfiguration siehe 6.1.6.

Conntrack leeren

Conntrack leeren bedeutet das komplette Löschen der Kernelhilfstabelle (*connection tracking table*) die für *stateful inspection* verwendet wird. Dies ist nötig, wenn Verbotsregeln eingerichtet wurden und es evtl. alte "Erlaubteinträge" in der *connection tracking table* gibt.

6.1.6 Einrichtungsempfehlung Firewall

Standard-Richtlinie

Die Konfiguration einer Firewall sollte so erfolgen, das nur der Datenverkehr zugelassen wird, der unbedingt nötig ist. Dazu ist das Standardverhalten einer Firewall auf "alles verwerfen" zu stellen und gezielt die Kommunikationen frei zu schalten, die benötigt werden.

Bei den LiSS series Systemen erfolgt dies folgendermaßen:

- *Firewall - Paket-Filter - Einstellungen*: Standard-Richtlinie für IPv4 und IPv6 auf "verwerfen" setzen
- *Firewall - Paket-Filter - Einstellungen*: Einschalten der Firewall durch Paket-Filter einschalten: *ja*

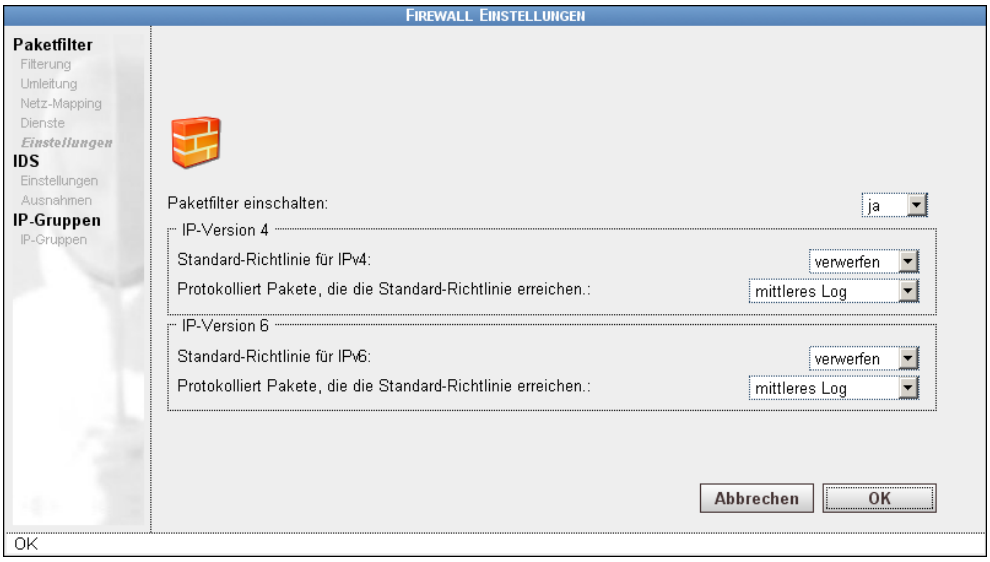


Abbildung 6: Firewall Einstellungen

Logging per Standard-Richtlinie

Um von der Firewall verworfene Pakete sichtbar zu machen, ist es ratsam das Logging für die *Standard-Richtlinie* zu aktivieren. Die geloggten Pakete erscheinen dann mit ihren Eckdaten im Firewallog unter *Diagnose - Syslog - Logs - Firewall.* Als Logprefix wird “Default” verwendet, wenn das Paket über die Standardrichtlinie geloggt wurde. Über die Suchfunktion kann somit gezielt nach Paketen gesucht werden, die über die Standard-Richtlinie geloggt wurden. Um die Systemlast nicht unnötig zu erhöhen, kann beim Logging mit Limitfunktionen gearbeitet werden. Diese sind von “*kein Log*” bis *“vollständiges Log”* wählbar. Eine empfehlenswerte Einstellung ist “mittleres Log”. Zu Analysezwecken kann die Limitfunktion ggf. auf “*vollständiges Log*” erweitert werden, sollte jedoch später wieder zurückgestellt werden.

Soll der Logprefix der *Standard-Richtlinie* geändert werden, so ist eine nutzerdefinierte Firewallregel zu erstellen, die alles verbietet, aber loggt. Bei Verwendung nutzerdefinierter Firewallregeln kann der Logprefix frei gewählt werden. Diese Firewallregel muß dann an letzter Stelle in das Regelwerk eingefügt werden.

Rechtevergabe über IP-Gruppen

Zur besseren Übersichtlichkeit der Firewallkonfiguration ist es ratsam mit IP-Gruppen zu arbeiten. IP-Gruppen können Rechner und Netze enthalten. Werden IP-Gruppen als Quell- oder Zielstandort verwendet, dann ergibt sich eine selbsterklärende Konfiguration, die dazu noch flexibel ist. Spätere Änderungen am Regelwerk der Firewall lassen sich so recht einfach durch Änderung der Gruppenmitglieder realisieren.

Quellen und Ziele

Der Paket-Filter der LiSS Systeme verwendet das Linux *iptables* Firewalling. Beim Anlegen einer Firewallregel erfragt der Assistent zwischen welcher Art von Standorten die Regel etabliert werden soll. Es wird zwischen *extern - extern*, *extern - LiSS* und *LiSS - extern* unterschieden. Diese Unterscheidung dient zur Festlegung in welcher *Chain* des *iptables* Mechanismus die Regel unterzubringen ist. In Abbildung 4 ist die Arbeitsweise von *iptables* schematisch dargestellt.

- Soll ein Dienst auf dem LiSS Gerät angesprochen werden, dann ist *extern - LiSS* auszuwählen
- Ist das Ziel der Verbindung nicht das LiSS Gerät, dann ist *extern - extern* zu wählen
- Bezeichnet die Kommunikation Datenverkehr vom LiSS Gerät weg, dann ist *LiSS - extern* zu wählen

6.2 IDS

Auf der LiSS 700 series wird ein Intrusion Detection System angeboten, welches sich auf die Erkennung und Sperrung von Portscans beschränkt.

Erkennungsempfindlichkeit gibt an, wie sensibel das Intrusion Detection System auf Anfragen reagieren soll. Derzeit gibt es drei Abstufungen:

- niedrig
- standard
- hoch

Wird die Empfindlichkeit des IDS auf *hoch* gestellt, dann sollte vorher unbedingt der Administrationsrechner in die Ausnahmeliste eingetragen werden. Ansonsten kann es durch andere vom Administrationsrechner ausgehende Kommunikationen dazu kommen, dass der Zugriff für den Administrationsrechner auf die LiSS 700 series gesperrt ist.

Wurde ein Portscan erkannt, kann der Angreifer sofort, beim zweiten oder erst beim dritten Versuch gesperrt werden. Die Aktivierung des IDS wird unter *Firewall - IDS - Einstellungen* vorgenommen. Hier kann die Sperrung der Angreifer getrennt für TCP und UDP vorgenommen werden.

Damit einige Systeme nicht fälschlich als Angreifer erkannt werden, können diese unter *Firewall - IDS - Ausnahmen* per Quell-IP-Adresse angegeben werden. Diese Systeme werden bei erkannten Portscans *nicht* gesperrt.

Systeme, die bereits vom IDS gesperrt wurden und sich in der Blockliste befinden, können nur aus dieser entfernt werden, indem ein Ausnahmeeintrag erstellt und die LiSS 700 series neu gestartet wird.

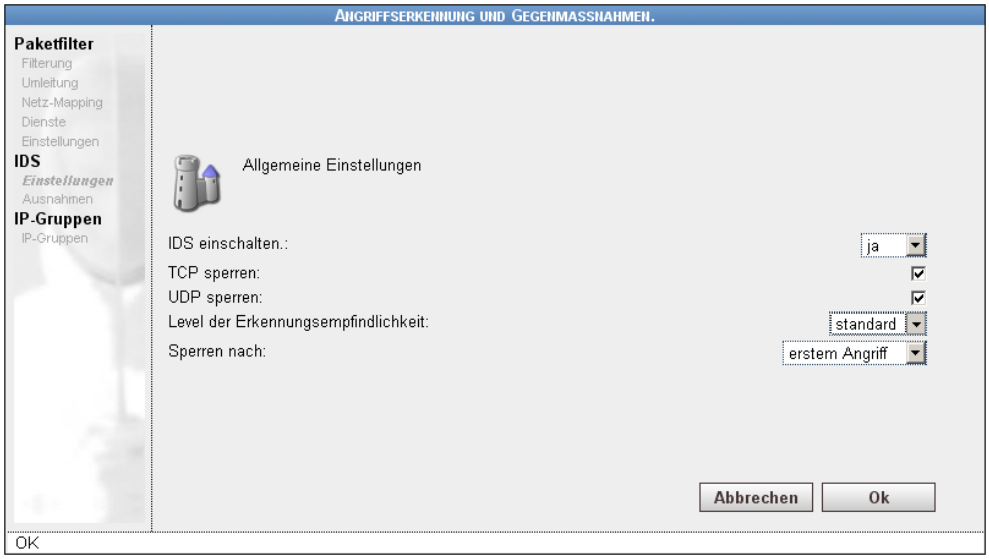


Abbildung 7: IDS Einstellungen

6.3 IP-Gruppen

Zur leichteren Handhabbarkeit können mehrere IP-Adressen, ob Einzelsysteme oder Netze, in Gruppen zusammen gefaßt werden.

Alternativ zur Gruppierung von vorhandenen Adressen können auch IP-Bereiche angelegt werden. Somit lassen sich zum Beispiel alle IP-Adressen von 192.168.1.13...192.168.1.27 unter einem Bereichsnamen zusammenfassen.

Die Arbeit mit IP-Gruppen bzw. Bereichen ist sehr flexibel bzgl. der Änderung von Quell- bzw. Zieladressen in der Firewall. Durch einfaches Ändern einer IP-Gruppe, durch beispielsweise Hinzufügen eines Netzes, gelten sofort alle für diese Gruppe festgelegten Berechtigungen auch für das neu hinzugefügte Netz.

7 VPN

7.1 IPsec

Virtuelle Private Netzwerke (VPNs) dienen der gesicherten Datenübertragung über unsichere Datenverbindungen wie das Internet.

LiSS 700 series Geräte ermöglichen die Einrichtung von maximal 10 IPsec-Standard basierten VPNs. Gleichzeitig nutzen lassen sich 5 IPsec-Standard basierte VPNs. Die LiSS series Systeme arbeiten dabei mit dem IPsec-Tunnelmodus. So sind folgende VPN-Tunnel-Varianten realisierbar:

- Site-to-Site
- Site-to-Host
- Host-to-Host

Zur Authentifizierung werden folgende Verfahren angeboten:

- preshared secret (PSK) - Passwortauthentifizierung
- Authentifizierung mit RSA-Schlüsseln
- Authentifizierung mit X.509 Zertifikaten

Merkmale des IPsec-Standards

- Abhörsicherheit durch Verschlüsselung der Verbindung
- Authentifizierung der VPN-Gateways (Tunnelenden)
- Erkennung von Manipulationen der Daten durch Sicherung der Datenintegrität mittels Hash-Funktionen
- Erhöhung der Sicherheit durch Schlüsselwechsel (Rekeying)
- einfache Interoperabilität mit Geräten anderer Hersteller, solange deren VPN-Technologie dem IPsec Standard entspricht

VPN-Leistungsmerkmale der LiSS series Systeme

NAT-Traversal

NAT-Traversal bedeutet das Tunneln der IPsec-Daten in UDP-Paketen auf Zielport 4500. Dies ist nötig, wenn sich zwischen den VPN-Gateways Systeme befinden, die NAT durchführen, bzw. sich Firewalls befinden, die mit den IPsec-Protokollen ESP[7] und AH[8] nicht umgehen können. NAT-Traversal ist ein Zusatzmodul, das zwar aktiviert werden kann, aber erst dann benutzt wird, wenn dies wirklich nötig ist. Ob auf der Verbindung zwischen den VPN-Gateways NAT durchgeführt wird, ermitteln die Gatways beim Verbindungsaufbau und nutzen NAT-Traversal selbstänig, wenn dieses Feature auf beiden Seiten vorhanden und aktiviert ist.

Strict Mode

Der Strict Mode legt eine konkrete Kombination von Verschlüsselungsalgorithmus und Hashfunktion fest. Abweichungen sind nicht erlaubt. Der VPN-Tunnel ist nur dann aufbaubar, wenn beide Seiten gleiche Verschlüsselungsalgorithmus und Hashfunktion konfiguriert haben.

DPD

DPD steht für *Dead Peer Detection*. Diese dient zur Erkennung eines “toten Endes” um ggf. den VPN-Tunnel neu aufzubauen oder zu beenden. Zur Erkennung werden in einem Intervall Daten zur Gegenstelle geschickt, die diese beantwortet. Bleibt die Antwort aus, wird eine Aktion ausgeführt. Diese kann der Neuaufbau oder das Beenden des Tunnels sein. Ist die Gegenstelle durch eine statische IP-Adresse oder einen Hostnamen direkt erreichbar, wird der VPN-Tunnel neu aufgebaut. Ist die IP-Adresse der Gegenstelle unbekannt, wird der VPN-Tunnel beendet.

Main Mode

Die Authentifizierung in Phase 1 findet in über eine verschlüsselte Verbindung statt. Aus diesem Grund ist Main Mode dem Aggressive Mode vorzuziehen.

Aggressiv Mode

Die Authentifizierung in Phase 1 findet in über eine unverschlüsselte Verbindung statt. Verzicht der Verschlüsselung bedeutet schnellere Authentifizierung.

[7] ESP- Encapsulating Security Payload, IP-Protokoll Nummer 50
[8] Authentication Header, IP-Protokoll Nummer 51

Kompression

Ermöglicht Kompression der Daten im VPN-Tunnel. Dadurch ist ein effizientes Ausnutzen der Übertragungsrate möglich. Diese Funktion ist gerade bei textbasierten Daten sehr nutzbringend.

PFS

PFS - Perfect Forward Secrecy verhindert, daß die verwendeten Schlüssel beim Schlüsselwechsel voneinander abhängig sind.

Debugging

Detailierte Fehlersuche mittels erhöhtem Logging. Die Fehlersuche ist pro VPN-Tunnel aktivierbar.

Automatisches Erstellen von Firewallregeln

Erstellt für die Phase 2 Netze Firewallregeln automatisch, die zwischen diesen Netzen alles erlauben. Für die Ersteinrichtung eines Tunnels verringert dies die möglichen Fehlerquellen. Da damit aber lokale und entfernte Netze direkt ohne Filterung miteinander verbunden werden, sollten die Kommunikation im VPN-Tunnel im produktiven Einsatz später durch den Administrator auf das nötige eingeschränkt werden.

FW-Log im Tunnel

Zur Analyse kann der Datenverkehr im VPN-Tunnel im Firewallog mitgeschrieben werden. Dazu gibt es verschiedenen Limitfunktionen. Zur Konfiguration siehe 6.1.1.

Mehrere Phase 2 Netze in einem Tunnel

Um den Konfigurationsaufwand gering zu halten, ist es möglich mehrere Phase 2 Verbindungen in einem VPN-Tunnel anzugeben. Diese Kombinationen müssen auf beiden VPN-Gateways identisch sein.

Kombination verschiedener Authentifizierungstypen

LiSS series Systeme unterstützen das gleichzeitige Arbeiten mit verschiedenen Authentifizierungstypen. So können verschiedene VPN-Verbindungen mit Preshared Secret, RSA-Schlüsseln und X.509 Zertifikaten parallel eingerichtet werden.

Wichtig: Es kann nur *ein* VPN-Tunnel mit dynamischem Endpunkt und PSK-Authentifizierung eingerichtet werden.

Sollen beispielsweise mehrere mobile Clients angebunden werden, die stets eine dynamische IP-Adresse haben, dann ist mit RSA-Schlüsseln oder mit Zertifikaten zu arbeiten.

	Standort B		
Standort A	statische IP	dynamische IP	dynDNS-Hostname
statische IP-Adresse	Aufbau A ⟷B	Aufbau A ←B	Aufbau A ⟷B
dynamische IP-Adresse	Aufbau A→B		Aufbau A→B
dynDNS-Hostname	Aufbau A ⟷B	Aufbau A ←B	Aufbau A ⟷B

Tabelle 3: IPsec VPN - Authentifizierungstypen und Tunnelendpunkte

7.1.1 Überblick

Zur Vereinfachung der Administration werden VPN-Tunnel mit einem Assistenten eingerichtet. Verschiedene Zusatzdaten werden dabei in gesonderten Menüs vorher konfiguriert, die beim Durchlaufen des Assistenten zur Auswahl stehen. So sind Verschlüsselungsalgorithmen, Hashfunktion, Dead Peer Detection Parameter in Profilen abgelegt. Die Verwaltung der RSA-Schlüssel sowie der X.509 Zertifikate befindet sich ebenfalls außerhalb der eigentlichen Tunnelkonfiguration.

Im Überblick sind alle konfigurierten VPN-Tunnel dargestellt. Über ein Häkchen kann jeder Tunnel einzeln aktiviert bzw. deaktiviert werden. Deaktiviert bedeutet dabei, daß der Tunnel konfiguriert ist, diese Konfiguration jedoch nicht geladen wird. Ein deaktiver VPN-Tunnel wird *grau* dargestellt. Ein aktiver Tunnel kann je nach Konfiguration entweder vom LiSS series Gerät selbst aufgebaut werden, oder es wird auf einen eingehenden Verbindungsaufbau der Gegenseite gewartet. Konnte ein Tunnel erfolgreich aufgebaut werden, dann wird dieser in *grün* dargestellt. Wurde die Tunnelkonfiguration geladen, es kam aber noch nicht zu einem erfolgreichen Tunnelaufbau, dann wird der VPN-Tunnel *rot* dargestellt. Änderungen der Aktivierung müssen gespeichert werden, bevor diese übernommen werden.

Am unteren Rand der Tunnelübersicht werden alle aufgebauten Phase 2 Verbindungen gegenüber den insgesamt konfigurierten Phase 2 Verbindungen angezeigt.

Zur besseren Übersicht können über das Suchfeld nur bestimmte Tunnel angezeigt werden. Das Suchfeld sucht im Tunnelnamen. Die Suche unterscheidet nicht zwischen Groß- und Kleinbuchstaben.

Die Ansicht kann über *Auffrischen* aktualisiert werden. Durch Anklicken eines VPN-Tunnels sind mehr Details sichtbar. Es besteht nun die Möglichkeit den VPN-tunnel zu bearbeiten.

Neueinrichtung VPN-Tunnel

Die Einrichtung eines VPN-Tunnels ist komplexer als die Erstellung einer Firewallregel, denn die Einrichtung ist auf zwei Systemen vorzunehmen, die eventuell von verschiedenen Administratoren bedient werden und auch nicht immer vom gleichen Typ sein müssen. Aus diesem Grund sollte die Einrichtung Anfangs möglichst vereinfacht werden, um sich stückweise der endgültigen Konfiguration zu nähern. Siehe dazu auch Abschnitt 7.1.6.

Soll ein neuer VPN-Tunnel eingerichtet werden, ist der Assistent für die VPN-Einrichtung über *Neu* zu starten.

Allgemeine Einstellungen

- *Name:* - VPN-Tunnelname, keine Leerzeichen erlaubt
- *Authentifizierung:* - Auswahl zwischen
  - *Preshared Secret*
  - *RSA-Schlüssel*
  - *X.509 Cert*
- *Einstellungen:* - Aktivieren von Merkmalen
  - *Kompression*
  - *PFS*
  - *Erzwinge Nat-T* - Kapselung in UDP Pakete Zielport 4500 auch wenn kein NAT durchgeführt wird
- *Fehlersuche:* - Auswahl zwischen

  - *aus* - kein Debugging
  - *Standard* - alles unter *VPN - IPsec - Fehlersuche* - angegebene
  - *Alle* - komplettes Debugging

Phase 1

- *Tunnel Endpunkte:*
  - *Lokale IP* - Angabe der ausgehenden Schnittstelle in Richtung VPN-Gegenstelle, *Standard* bedeutet Schnittstelle die zum Standard Gateway zeigt
  - *Gegenstelle (Name/IP)* - statische IP-Adresse oder Hostname der VPN-Gegenstelle, sonst ohne Angabe
- *Nächster Hop (optional):* - Wenn die VPN-Gegenstelle nicht über das Standard Gateway erreicht wird, dann wird hier der nächste Router in Richtung VPN-Gegenstelle angegeben. *Die Nächster Hop Option* im Tunnel bedeutet, daß intern mit routing-policies gearbeitet wird. Dies führt zur Verlangsamung des Routings, deshalb gibt es eine Begrenzung auf 50 Tunnel mit *Nächster Hop Option*.
- *IKE Mode*
  - *Main Mode* - Authentifizierung mit Verschlüsselung (empfohlen)
  - *Aggressive Mode* - Authentifizierung ohne Verschlüsselung

Verbindungs Einstellungen

- *Profil:* - Auswahl des vorher festgelegten Profils, enthält Verschlüsselungsalgorithmus, Hashfunktion, DPD-Parameter
- *Bei Ausfall:* - Legt fest, was mit Paketen zu tun ist, wenn VPN-Aufbau fehlschlägt, mögliche Werte:
  - *tue nichts* - Paket wird nicht geroutet
  - *durchlassen* - Paket wird trotzdem zugestellt, Voraussetzung ist direkte Erreichbarkeit der VPN-Gegenseite, d.h. das Pakete zum Zielnetz auch ohne VPN geroutet werden
  - *verwerfen* - Paket wird nicht geroutet
  - *ablehnen* - Paket wird mit *Destination unreachable* beantwortet (empfohlen)

- *Erzeuge Firewallregel für Tunnel:*
  - *nein* - Firewallregeln für die Phase 2 Netze müssen manuell erstellt werden
  - *ja* - Firewall ist für alle Phase 2 Netze für alle Dienste geöffnet
  - *ja und hereinkommenden Verkehr maskieren* - Firewall ist für alle Phase 2 Netze für alle Dienste geöffnet, Pakete werden beim Austritt aus dem VPN-Tunnel maskiert, so das diese im LAN erscheinen, als kämen diese vom LiSS series Gerät
- *Loglevel:* - Logging im Tunnel siehe 6.1.1, Logausgabe im Firewallog
- *Verbindung:*
  - *aktiv verbinden* - LiSS series darf VPN-Tunnel aufbauen; nur möglich, wenn VPN-Gegenstelle direkt erreichbar
  - *kein eingehender Tunnel* - Eingehender Tunnel wird nicht akzeptiert

Phase 2

- mehrere Kombinationen möglich
- legt fest, welcher Datenverkehr durch den VPN-Tunnel geroutet wird
- *Lokales Netz* - Netze bzw. Hosts der lokalen Seite
- *Entferntes Netz* - Netze bzw. Hosts der entfernten Seite; Netze, welche durch den VPN-Tunnel erreicht werden sollen
- durch *Hinzufügen* erfolgt Übernahme in Liste

Authentifizierung

- Abhängig von der Auswahl auf der Seite *Allgemeine Einstellungen* des Assistenten
- Preshared Secret
  - *Preshared Key* - Passwort zur Authentifizierung; min 6 Zeichen
  - *Lokale Seite*
    - Bezeichner - ID der lokalen Seite, Angabe optional; entspricht IP-Adresse, wenn keine andere Angabe erfolgt

  - *Gegenstelle*
    - Bezeichner - ID der Gegenseite, Angabe optional; entspricht IP-Adresse, wenn keine andere Angabe erfolgt

- *RSA-Schlüssel*
  - *Lokale Seite*
    - Bezeichner - ID der lokalen Seite, Angabe optional; entspricht erster Phase 2 Angabe, wenn keine andere Angabe erfolgt
    - RSA-Schlüssel - RSA-Schlüssel über Ordnersymbol aus Liste auswählen, ggf. neuen Schlüssel anlegen; lokaler RSA-Schlüssel beinhaltet öffentlichen und privaten Schlüssel
  - *Gegenstelle*
    - Bezeichner - ID der Gegenseite, Angabe optional; entspricht erster Phase 2 Angabe, wenn keine andere Angabe erfolgt
    - RSA-Schlüssel - RSA-Schlüssel über Ordnersymbol aus Liste auswählen, ggf. neuen Schlüssel anlegen; RSA-Schlüssel der Gegenstelle beinhaltet nur öffentlichen RSA-Schlüssel

- X.509 Zertifikat
  - Lokales Zertifikat - lokales Zertifikat über Ordnersymbol aus Liste auswählen, es werden nur Server-Zertifikate angezeigt
  - Entferntes Zertifikat - Zertifikat der Gegenstelle über Ordnersymbol aus Liste auswählen, es werden nur Client-Zertifikate angezeigt
  - nach Auswahl der Zertifikate sind Angaben des *distinguished name* aus dem Zertifikat sichtbar

7.1.2 Profile

Hier sind alle VPN/IPsec - Profile aufgelistet, die definiert sind. Es können beliebig viele Profile angelegt werden. Ein Profil wird später einem VPN-Tunnel zugewiesen. Ein Profil kann mehreren VPN-Tunnel zugewiesen werden. Die Änderung eines Profils führt zum Neustart aller VPN-Tunnel.

- Allgemeine Parameter

  - *Profilname:* - Name des Profiles, Leerzeichen erlaubt
  - *DPD (Dead Peer Detection):* - Aktivierung von Dead Peer Detection (empfohlen)
  - *DPD Verzögerung (Voreinstellung 30sec):* - Sendeinterval der DPD Anfrage
  - *DPD Timeout (Voreinstellung 2min):* - Verzögerung bis DPD-Aktion ausgeführt wird
  - *Rekeying Phase 1 - IKE (Voreinstellung 8h):* - Zeit nach der ein neuer Schlüssel für Phase 1 erzeugt und verwendet wird
  - *Rekeying Phase 2 - ESP (Voreinstellung 1h):*- Zeit nach der ein neuer Schlüssel für Phase 2 erzeugt und verwendet wird
  - *Wiederholversuche (default 3):* - wie oft soll versucht werden den VPN-Tunnel aufzubauen

- IKE Vorschlag (Phase1)
  - *Verschlüsselungsalgorithmus:* - Art der Verschlüsselung
  - *Integritäts Funktion* - Art der Prüfsumme
  - *Diffie-Hellman Gruppe* - Diffie-Hellman-Gruppen werden zur Festlegung der Länge von Basisprimzahlen verwendet, die während des Schlüsselaustauschs verwendet werden
  - *Akzeptiere nur diese Werte für eingehende Verbindunsanfragen (strict mode):* - strict mode für Phase 1 aktivieren

- ESP Vorschlag (Phase2)
  - *Verschlüsselungsalgorithmus* - Art der Verschlüsselung
  - *Authentifizierungsalgorithmus* - Art der Prüfsumme
  - *Akzeptiere nur diese Werte für eingehende Verbindunsanfragen (strict mode):*- strict mode für Phase 2 aktivieren

7.1.3 RSA-Schlüssel

Für die Verwendung von RSA-Schlüsseln werden hier die nötigen Schlüssel hinterlegt. Dabei wird zwischen lokalem RSA-Schlüssel und RSA-Schlüssel einer Gegenstelle unterschieden. Lokale RSA-Schlüssel bestehen aus öffentlichem und privatem Schlüssel. RSA-Schlüssel einer Gegenstelle nur aus dem öffentlichen Schlüssel.

Lokalen RSA-Schlüssel anlegen

Unter *VPN - IPsec - RSA-Schlüssel - Neu* durch Auswahl zwischen 1024, 2048 und 4096 Bit Schlüssellänge wird ein neuer lokaler Schlüssel erzeugt. Es gibt keinen Zugriff auf den privaten RSA-Schlüssel über die Administrationsoberfläche, dieser ist jedoch im Konfigurationsbackup enthalten. Der RSA-Schlüssel sollte einen Kommentar als Namen erhalten.

RSA-Schlüssel einer Gegenstelle anlegen

Hat die Gegenstelle bereits einen RSA-Schlüssel, dann ist unter *VPN - IPsec - RSA-Schlüssel - Neu* bei *öffentlicher Schlüssel:* der öffentliche Schlüssel der Gegenstelle einzufügen mit einem Kommentar als Namen zu versehen und zu speichern.

7.1.4 Einstellungen

Hier finden sich globale VPN/IPsec-Einstellungen. Dazu gehören

- *Einschalten:* - Aktivieren des VPN-Dienstes, ohne aktivierten VPN-Dienst startet kein VPN-Tunnel
- *NAT Traversal:* - NAT Traversal Modul laden (empfohlen)
- *Eindeutige IDs:* - wird ein neues VPN mit einer gleichen ID aufgebaut, wird der alte Tunnel gelöscht

7.1.5 Fehlersuche

Das Logging kann sehr detailiert ausgewählt werden. Die Aktivierung einzelner Teillogs ist abhängig von der Situation.

7.1.6 Einrichtungsempfehlung IPsec VPN mit LiSS series Systemen

Als Beispiel soll hier die Einrichtung eines VPNs zwischen zwei LiSS series Geräten beschrieben werden. Beide LiSS Systeme sind im Beispiel über einen DSL-Anschluß mit dem Internet verbunden. Beide DSL-Anschlüsse haben eine dynamische IP-Adresse.

Voraussetzungen

- erfolgreiche Netzwerkkonfiguration:
  - Schnittstelle zum lokalen Netz
  - Internetverbindung
  - default Route
  - Konfiguration eines DynDNS Accounts bei einem DynDNS-Anbieter
  - Konfiguration der DynDNS-Hostname-Aktualisierung auf dem LiSS series System

Begonnen wird mit dem Assistenten zur Einrichtung einer neuen VPN-Verbindung unter *VPN - IPsec - Übersicht - Neu*. Unter *Allgemeine Einstellungen* wird ein Name für das VPN vergeben. Dieser darf keine Leerzeichen enthalten.

Allgemeine Einstellungen

Als *Authentifizierung* wird anfangs *Preshared Secret* gewählt. Die Authentifizierung kann später auf X.509 Zertifikate geändert werden. Alle weiteren Einstellungen dieser Seite bleiben auf Standardeinstellung. Über Weiter geht es zur Seite: *Phase 1*.

Phase 1

In *Phase 1* wird unter *Tunnel Endpunkte* für die *lokale Seite Standard* eingestellt, für die *Gegenstelle* wird hier der DynDNS-Hostname der Gegenstelle eingetragen. Alle weiteren Einstellungen werden nicht verändert. Über Weiter geht es zur Seite: *Verbindungs Einstellungen*.

Verbindungs Einstellungen

In *Verbindungs Einstellungen* bleiben alle Werte auf Standardeinstellung. Über Weiter geht es zur Seite: *Phase 2*.

Phase 2

In *Phase 2* wird in dem linken Auswahlfeld über das Ordnersymbol das lokale Netz ausgewählt. Im rechten Auswahlfeld wird das entfernte lokale Netzwerk, welches an der Gegenstelle als LAN existiert und zu dem der VPN-Tunnel führen soll, angegeben. Ist einer der Werte nicht

in der Auswahlliste, dann wird dieser unter *IP-Adresse* eingetragen. Dabei ist darauf zu achten, daß für eine Netzangabe eine Netzmaske nötig ist. Beispiel: 192.168.81.0/24. Sind beide Auswahlfelder mit Werten gefüllt, wird diese Netz-zu-Netz-Kombination über *Hinzufügen* in die Liste der Phase 2 Netze übernommen. Über Weiter geht es zur Seite: *Authentifizierung*.

Authentifizierung

Auf der Seite *Authentifizierung* wird das Passwort oder auch der *Preshared Key* eingetragen. Alle weiteren Angaben bleiben unverändert. Über *OK* wird der Einrichtungsassistent verlassen und mit *Speichern* wird die Konfiguration übernommen.

Damit der VPN-Tunnel vom LiSS series Gerät auch gestartet werden kann, muß der VPN-Dienst unter *VPN - IPsec - Einstellungen - Einschalten - ja* gestartet werden.

Übersicht

Konnte der VPN-Tunnel erfolgreich zur Gegenstelle aufgebaut werden, wird der VPN-Tunnel *grün* in der Übersicht dargestellt.

8 Application Level Gateway

Die LiSS 700 series bietet einen Webproxy zur Inhaltsfilterung an. Die Webnutzung kann anhand von IP-Adressen, IP-Netzen oder IP-Bereichen geregelt werden. Zur Filterung stehen ein externer URL-Filter, das *Orange Filter*, und eine URL-Filterung anhand regulärer Ausdrücke zur Verfügung.

8.1 URL-Filter

Ein sehr leistungsfähiger Contentfilter ist das *Orange Filter*, das in diesem Menüpunkt konfiguriert werden kann.

Die Verwendung des *Orange Filters* ermöglicht eine einfache Filterung von Webinhalten anhand von Kategorien. Eine Liste der verfügbaren Kategorien ist im Anhang auf Seite III zu finden.

Arbeitsweise des URL-Filters

Suchroboter durchsuchen das Internet nach Webseiten, die über spezielle Algorithmen vom Dienstanbieter kategorisiert werden. Das LiSS series System fragt zu einer angeforderten URL nur die zugewiesenen Kategorien ab, um dann nach der gegebenen Konfiguration den Webzugriff zu erlauben oder zu sperren. In Abbildung und ist die Arbeitsweise veranschaulicht.

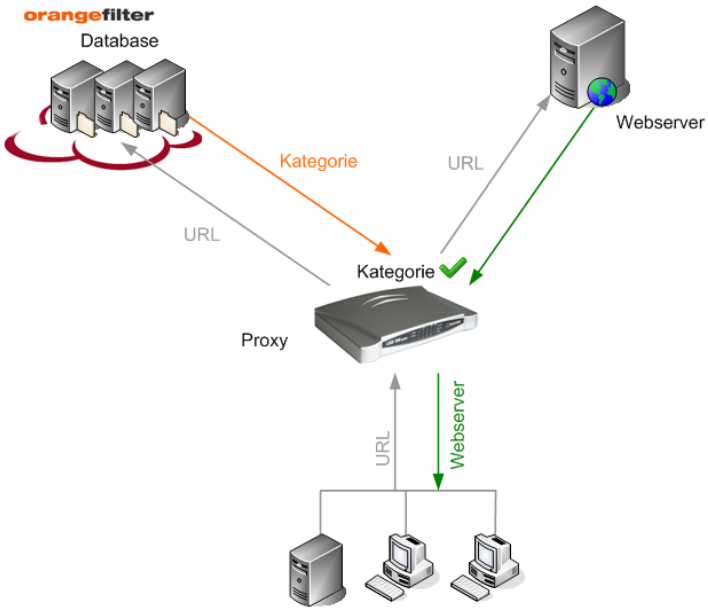


Abbildung 8: APLGW URL-Filter Arbeitsweise erlauben

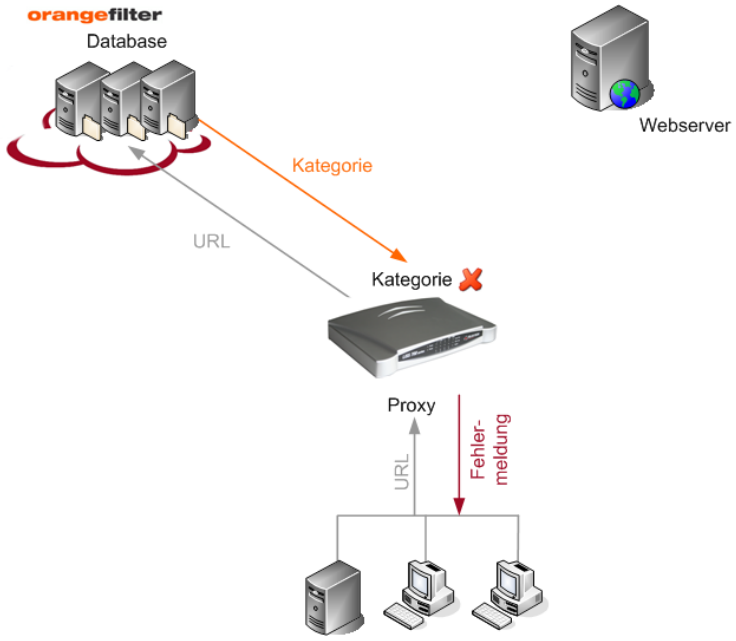


Abbildung 9: APLGW URL-Filter Arbeitsweise blocken

8.1.1 Einstellungen

Hier wird der Contentfilter ein- bzw. ausgeschaltet und konfiguriert. Vom angegebenen *zu verwendender Standardserver* wird beim Starten des Filters eine Serverliste bezogen. Der *zu verwendender Standardserver* muß in der Regel nicht geändert werden.

Fehlerhafte URLs ignorieren bedeutet, dass das Prüfen der URLs vor dem Senden an den Dienstanbieter nicht durchgeführt wird. Dies sollte nur aktiviert werden, wenn es mit bestimmten URLs und der Verwendung des Contentfilters Probleme gibt.

In Netzwerkumgebungen, in denen keine DNS-Anfragen nach außen möglich sind, können die mit Hostnamen angegebenen Server in der Serverliste nicht aufgelöst werden. In diesem Fall ist *DNS nicht verwenden* zu aktivieren.

8.1.2 Ticket

Zum Aktivieren des Orange Filters benötigt man ein gültiges Ticket, welches mit der Lizenz erworben wird. Es besteht die Möglichkeit für 30 Tage ein Demo-Ticket direkt vom Orange Filter Server zu beziehen. Nach Ablauf des Demo-Tickets kann kein erneutes Demo-Ticket bezogen werden. Zum aktivieren eines Tickets muß der Orange Filter Caching Daemon bereits eingeschaltet und der Startvorgang erfolgreich durchgeführt sein.

Startvorgang des Orange Filters

Wird der Orange Filter Caching Daemon (OFCD) gestartet, dann bezieht er vom konfigurierten *Standardserver* eine Serverliste. Ist diese erfolgreich übertragen worden, wird jeder Server in der Liste kontaktiert und die Erreichbarkeit mittels Antwortzeit bewertet. Letztendlich wird der am schnellsten antwortende Server zum neuen *Standardserver* gewählt. Alle Anfragen bzgl. Kategoriesierung von URLs gehen nun an diesen Server. Das ganze läßt sich im Log unter *Diagnostics - Logs - Daemon* beobachten.

8.2 Webfilter

Der Webfilter arbeitet als Webproxy. Das heißt, Nutzer und IP-Adresse des Anfragenden werden vor dem Webserver verborgen.

Funktionsweise

Der Client schickt die angefragte URL direkt zum Proxy. Dieser nimmt die URL an und prüft diese gegebenenfalls, bevor er die URL im Internet anfragt.

8.2.1 Einstellungen

In diesem Menü werden die globalen Einstellungen für den Webproxy vorgenommen. Diese gelten für alle Proxynutzer und Clients.

- *Einschalten - Ein- und Ausschalten des Webfilters*
- *Hören an* - legt fest, an welchen Schnittstellen der Webproxy läuft. Hier sollten nur die Interfaces ausgewählt werden, die bei den Clients als Proxy IP-Adresse angegeben werden. Dies sind gewöhnlich die Interfaces die in ein LAN zeigen, in dem sich Clients befinden, die den Proxy nutzen sollen. Die Standardeinstellung *"all devices"* funktioniert immer, kann aber zu Mißbrauch des Proxys durch Fremde an der WAN-Schnittstelle führen.
- *Hören an Port* - Der verwendete Standardport des Proxys ist 3128. Dieser hier festgelegte Port ist bei der Proxykonfiguration der Clients anzugeben. Ist auf den Clients bereits ein Proxy konfiguriert, kann dieser Port entsprechend übernommen werden.
- *Standardverhalten* - sollte ohne Verwendung von Berechtigungsprofilen auf *erlauben* gestellt werden, da sonst der Proxy alle Zugriffe auf Webinhalte blockt.

- *sperren* - der Proxy verbietet generell den Zugriff auf das Internet, Einzelne Zugriffe sind explizit in Profilen zu definieren und zuzuweisen
- *erlauben* - der Proxy erlaubt generell den Zugriff auf das Internet, Verbote von bestimmten Inhalten müssen über Profile definiert und zugewiesen werden

Regeltypen

Im Folgenden werden die verschiedenen Regeltypen erklärt und Beispiele genannt.

URL

Erlauben bzw. verbieten von einzelnen URLs. Die URL ist als regulärer Ausdruck[9] anzugeben. Mittels URL-Regeln können Whitelisteinträge (erlaubte Ausnahmen) für das Orange Filter definiert werden. So kann über das Orange Filter eine Kategorie gesperrt sein, einzelne Webseiten dieser Kategorie können jedoch mit einer URL-Erlaubtregel zugelassen werden.

Beispiel: Kein Zugriff auf www.waffen.de

- url : .*www\.waffen\.de.*
- Aktion : block

Orange Filter

Blockieren bestimmter Webseiten durch Angabe von Kategorien. Für die Anwendung ist eine Lizenz nötig, da die Kategorisierung von einem externen Dienstanbieter durchgeführt wird.

Um zu ermitteln welche Kategorie auszuwählen ist, um eine bestimmte Webseite zu sperren, können auf folgender Webseite die Kategorien der Webseite abgefragt werden:

http://filterdb.iss.net/urlcheck

Die Filterung mit dem *Orange Filter* ist immer ein verbieten. Kategorien die ausgewählt werden, sind dem Anwender nicht zugänglich. Steht die Standardaktion auf *sperren*, und es wird eine Orange Filter Regel angewendet, wird für diesen Client erst alles erlaubt und dann nur das gesperrt, was an Kategorien in der Orange Filter Regel definiert ist.

[9] siehe auch: http://www.weitz.de/regex-coach

Profilzuweisung an Clients

Die Verwendung von Clients ermöglicht es Profile an IP-Adressen zu binden. IP-Adressen können einzelne Host IP-Adressen sein, IP-Adressbereiche oder IP-Netze.

Die Zuweisung des Webfilterprofils erfolgt unter *Einstellungen - Nutzer - Clients* pro Client durch Auswahl von Profilen aus der Liste der aktiven Profile.

8.2.2 Protokoll

Die Protokollierung des Webfilters kann separat aktiviert werden. Im Log erscheint die IP-Adresse des Anfragenden gefolgt von der URL.

8.2.3 Zusammenfassung

Unter Zusammenfassung sind alle definierten Profile mit ihren Regeln aufgelistet. Welches Objekt, welches Profil zugewiesen hat, ist unter *Diagnose - Berichte - APLGW* einzusehen.

9 Einstellungen

9.1 System

9.1.1 Proxy

Wird das LiSS series Gerät hinter einem anderen HTTP / HTTPS-Proxy betrieben, kann dieser hier angegeben werden. Für jede HTTP / HTTPS Kommunikation des LiSS series Systems wird nun dieser Proxy verwendet. Dies betrifft:

Nötige Angaben sind:

- *Hostname / IP-Adresse*
- *Port*

Bei Verwendung von Nutzerauthentifizierung am entfernten Proxy

- *Nutzername*
- *Passwort*

9.1.2 DynDNS

Hier wird die Aktualisierung der dynamischen IP-Adresse bei einem DynDNS-Anbieter eingerichtet. Diese kann bei der Verwendung von PPP-Verbindungen erfolgen und für jede PPP-Schnittstelle getrennt konfiguriert und aktiviert werden.

Der DynDNS-Account ist dazu vorher bei einem entsprechenden Anbieter einzurichten. Derzeit werden von der LiSS series die auf Seite VI gelisteten DynDNS-Anbieter unterstützt.

Zur Konfiguration des DynDNS-Accounts sind folgende Angaben nötig:

- *Hostname* - Hostname, für den die IP-Adresse aktualisiert werden soll
- *Anbieter* - DynDNS-Anbieter aus der obigen Liste
- *Nutzer* - Nutzer zur Authentifizierung beim DynDNS-Anbieter
- *Passwort* - Passwort zur Authentifizierung beim DynDNS-Anbieter
- *Gerät* - Schnittstelle für die obige Daten gelten sollen

9.1.3 Zeit

Hier wird die Systemzeit des LiSS series Systems gesetzt und konfiguriert. Die Systemzeit kann eingesehen und eventuell manuell nachgestellt werden. Dazu übernimmt die Adminoberfläche bei aktiviertem Javascript die Systemzeit des Administrationsrechners in die entsprechenden Felder. Durch betätigen von *Uhrzeit* kann die Systemzeit des LiSS series Systems sofort gestellt werden.

Wurde die Systemzeit des Administrationsrechners nicht richtig übernommen, können die Felder auch manuell mit den richtigen Zeitwerten gefüllt werden, bevor diese mit *Uhrzeit* übernommen werden.

Für eine richtige Zeitangabe ist die korrekte Angabe der *Zeitzone* Voraussetzung. Diese kann aus einer Liste der verfügbaren Zeitzonen ausgewählt werden.

Um die Systemzeit der LiSS series dauerhaft genau zu halten, kann die genaue Zeit von einem NTP Zeitserver bezogen werden. Dieser Zeitserver kann als *Hostname* oder *IP-Adresse* unter *NTP*[10] *Server* angegeben werden.

NTP beschleunigt oder verringert die Geschwindigkeit der Systemuhr, um Zeitsprünge zu umgehen. Somit können nur geringe Zeitunterschiede korrigiert werden. Ist der Zeitunterschied größer als eine viertel Stunde[11] (15 min), dann verweigert der NTP-Dienst das Stellen der Systemzeit.

Eine genaue Systemzeit ist wichtig bei Verwendung von X.509 Zertifikaten beim VPN, da diese einen Gültigkeitszeitraum haben.

Die Systemzeit des LiSS series Gerätes kann über NTP an Systeme im LAN weiter gereicht werden. Dazu siehe LiSS als NTP-Server unter 5.2.3.

9.1.4 Zertifikate

Unter *Einstellungen - System - Zertifikate* werden alle X.509 Zertifikate zentral verwaltet. Es wird zwischen Server-, Client- und CA-Zertifikat unterschieden. CA-Zertifikate werden z.Z. vom LiSS series System nicht verwendet.

Nutzbare Zertifikatstypen:

Server-Zertifikat - wird für das LiSS series System verwendet, beinhaltet öffentlichen und privaten Schlüssel

[10] NTP - Network Time Protocol; TCP,UDP Port 123
[11] genauer 1000sec, was etwa 16,6 Minuten entspricht

Client-Zertifikat - wird für zu authentifizierende Gegenstellen verwendet, beinhaltet nur den öffentlichen Schlüssel

Ein X.509 Zertifikat enthält einen RSA[12]-Schlüssel und Zusatzinformationen. Wichtige Zusatzinformationen sind:

- *Antragsteller* - System, für dass das Zertifikat ausgestellt wurde
- *Aussteller* - Aussteller des Zertifikates
- *Gültigkeitszeitraum* - von wann bis wann ein Zertifikat gültig ist
- *RSA-Schlüssel* - je nach Dateiformat entweder nur öffentlicher RSA-Schlüssel oder öffentlicher und privater RSA-Schlüssel

Jedem System wird ein Zertifikat zugewiesen, welches als Serverzertifikat bezeichnet wird. Werden auf einem LiSS series System mehrere Verbindungen zum Internet konfiguriert, kann für jeden dieser Zugänge ein Server-Zertifikat verwendet werden.

Zur Hinterlegung eines Zertifikates ist unter *Zertifikats-Typ* der richtige Typ auszuwählen.

- *Zertifikats-Datei* - Zertifikatsdatei mit öffentlicher Schlüssel im PEM-Format (z.B. hostcert.pem)
- *Privater Schlüssel (nur Server)* - nur bei Serverzertifikat nötig, Zertifikatsdatei mit privatem Schlüssel im PEM-Format (z.B. privkey.pem)
- *Kommentar* - optionaler Kommentar

Nachdem die Zertifikatsdateien zum LiSS series System übertragen wurden, wird jedes X.509 Zertifikat mit Angabe des Zertifikat-Types mit seinem *distinguished name* des Antragstellers gelistet.

Bei Anwahl eines Zertifikates werden Gültigkeitzeitraum, und der *distinguished name*[13] des Antragstellers gelistet.

[12] RSA - asymmetrisches Kryptosystem, RSA ist nach seinen Erfindern Ronald L. Rivest, Adi Shamir und Leonard Adleman benannt

[13] eindeutige Bezeichnung, hirarchisch geordnet

9.2 Verwaltung

9.2.1 Firmware

Hier kann die aktuell auf dem LiSS 700 series Gerät laufende Firmwareversion aktualisiert werden. Unter dem hier angegebenen Link ist die aktuelle Firmwareversion zu finden. Diese wird per Webbrowser herunter geladen, und dann über *Durchsuchen* und *Laden* auf das LiSS 700 series Gerät übertragen. Anschließend kann über *Installieren* in die neue Firmware gestartet werden. Das LiSS 700 series Gerät ist wieder betriebsbereit, wenn die Ready-LED blinkt.

Um eine ältere Firmwareversion als die gerade genutzte Version zu installieren, ist das Gerät auf Werkseinstellungen zu setzen und dann das Update auf eine ältere Firmwareversion durchzuführen.

Während des Firmwareupdates darf das Gerät auf keinen Fall neu gestartet werden. Sollte dennoch das Firmwareupdate nicht erfolgreich durchgelaufen sein, kann das Gerät zur Reparatur zum Hersteller eingeschickt werden.

Zurücksetzen auf Werkseinstellung

Um die LiSS 700 series auf Werkseinstellungen zu setzen, ist der mit “Reset” beschriftete versenkte Taster auf der Geräterückseite drei mal hintereinander zu betätigen, wobei die minimale Pause dazwischen etwa 800ms zu betragen hat. Dadurch wird die aktuelle Konfiguration mit den Werten der Werkseinstellung überschrieben und das Gerät startet neu.

Beim “Reset” wird gleichzeitig die Firmware auf die Version des Auslieferungszustandes zurückgesetzt. Während dem Wiederherstellen der Urfirmware erlischt die READY-LED. Die Firmware des LiSS 700 series Gerätes ist nach einem “Reset” auf die aktuelle Version zu bringen.

Eine Konfigurationssicherung kann nur dann eingespielt werden, wenn die Firmwareversion des LiSS 700 series Gerätes nicht älter als die vom Backup ist! Ein Firmwareupdate nach erfolgtem “Reset” kann also zwingend sein, um eine Konfiguration laden zu können.

9.2.2 Dienste

Sie können hier die derzeit laufenden Dienste neustarten. Um Dienste zu starten oder zu stoppen sind die entsprechenden Dienste-Dialoge zu verwenden. Ob ein Dienst bei einem Neustart des LiSS series Gerätes gestartet wird, legt die Dienstekonfiguration des entsprechenden Moduls fest.

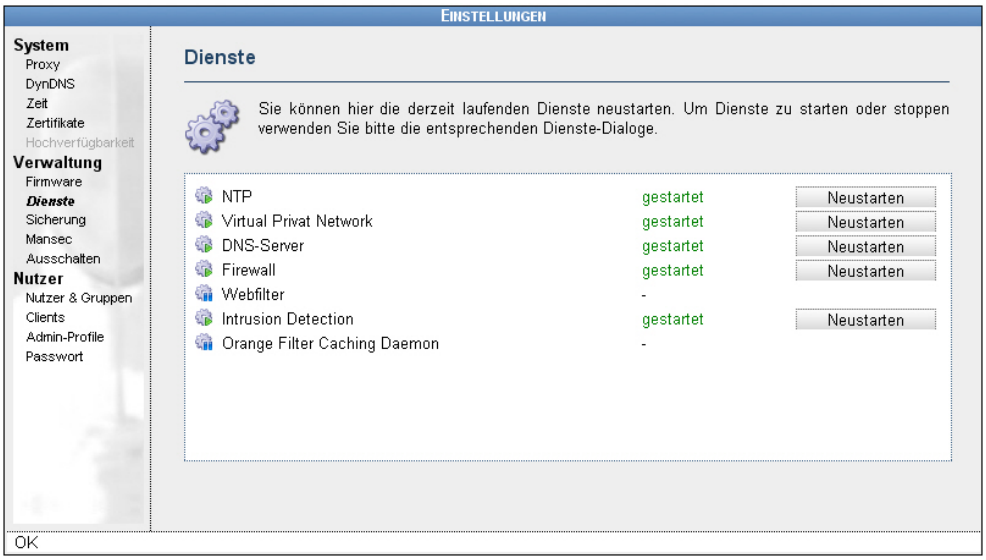


Abbildung 10: Einstellungen Verwaltung Dienste

9.2.3 Sicherung

Backup

Die gesamte Konfiguration des LiSS series Systems kann in einer Backupdatei gespeichert werden. Über *Einstellungen - Verwaltung - Sicherung - Neu* kann eine neue Sicherung angelegt werden, die vorerst nur auf dem LiSS series Gerät gespeichert ist. Nach Anwahl dieser Sicherung kann diese per *https-Verbindung* vom Gerät heruntergeladen und in der verfügbaren Netzwerkumgebung (lokal, Netzlaufwerke) des Administrationsrechners gespeichert werden.

Es wird empfohlen nach jeder Konfiguration eine Sicherung zu erstellen.

Wiederherstellung

Um eine Konfiguration aus einer Sicherung wieder herzustellen, ist unter *Einstellungen - Verwaltung - Sicherung - Durchsuchen* die Backupdatei auszuwählen und über *Laden* zum LiSS series System zu übertragen. Nach erfolgreicher Übertragung kann über *Wiederherstellen* die Konfiguration aus der Datei geladen werden. Um diese Konfiguration nun zu aktivieren ist ein Neustart des LiSS 700 series Systems notwendig.

Ein Backup eines Systems mit einer neueren Firmwareversion kann nicht zur Wiederherstellung benutzt werden, wenn das LiSS series System eine ältere Firmware hat. Hat ein LiSS series System eine ältere Firmware als in der Sicherung vermerkt, dann ist zuerst über ein Firmwareupdate die Firmwareversion auf dem LiSS series System auf die gleiche bzw. eine neuere Version zu aktualisieren.

Liegt eine Sicherung von einer älteren Firmwareversion vor, als die, die derzeit auf dem LiSS series System verwendet wird, dann wird beim Wiederhertsellen die Datenbankstruktur der Konfiguration konvertiert. Dies geschieht automatisch, es ist keinerlei Nutzereingriff nötig.

9.2.4 Mansec

Hier wird der Managementclient für die LiSS series Systeme konfiguriert. Dieser arbeitet mit dem Managementserver der Telco Tech GmbH zusammen. Dieser hält zu jedem gemanagten LiSS series Gerät ein aktuelles Backup vor. Desweiteren werden vom Managementserver Systemzustände der LiSS series Systeme abgefragt.

Bei Nutzung des Managementclients werden Konfigurationsänderungen vom System selbständig erkannt und es wird automatisch eine Konfigurationssicherung über eine verschlüsselte Mailverbindung zum Backupserver geschickt. Der Backupserver wird unter *Einstellungen - Verwaltung - Mansec - Automatische Sicherungen - Zertifikat d. Backupservers* über den Hostnamen aus dem X.509-Zertifikat des Backupservers ausgelesen. Das Zertifikat des Backupservers wird der LiSS series in der zentralen Zertifikatsverwaltung unter *Einstellungen - System - Zertifikate* bekannt gegeben.

Unter *Max. Sendehäufigkeit* ist das Überprüfungsintervall zu verstehen, in dem die Änderung der Konfiguration beobachtet wird. Liegt keine Konfigurationsänderung vor, wird keine Sicherung versendet.

Über *Backup senden* kann das Senden einer Sicherung manuell ausgelöst werden.

Unter *Einstellungen - Verwaltung - Mansec - Management-Einstellungen* wird der Managementserver der LiSS series ebenfalls über ein X.509-Zertifikat bekannt gegeben. Der Managementserver fragt über SNMP[14] bestimmte Statuswerte des LiSS series Systems ab, um so Veränderungen am System rechtzeitig zu erkennen. Der Managementserver ist ein eigenständiges Produkt der Telco Tech GmbH.

9.2.5 Ausschalten

Das *Ausschalten* des Gerätes erfolgt über das Trennen der Stromversorgung. Um das System herunterzufahren und anschließend neu zu starten wählen Sie *Neustart*.

[14] SNMP - Simple Network Management Protocol

9.3 Nutzer

Hier werden alle Nutzer des LiSS series Systems verwaltet. Somit lassen sich mehrere LiSS-Administratoren mit unterschiedlichen Administrationsrechten einrichten.

Lokalen Nutzer anlegen

Neben dem standard LiSS-Administrator, der immer existiert und ggf. umbenannt werden kann, können zusätzliche lokale Nutzer eingerichtet werden. Dazu ist unter *Einstellungen - Nutzer - Nutzer - Neu* ein lokaler Nutzer hinzuzufügen.

- *Anmeldename* - Name, mit dem sich der Nutzer am Gerät anmeldet
- *Datenquelle - Local users*; bei lokalem Repository fest vorgegeben
- *Anzeigenname* - vollständiger Name, der in der Nutzerliste angezeigt wird, Bsp.: *Max Mustermann*
- *E-Mail-Adresse* - wird eine E-Mail-Adresse angegeben, erhält der Nutzer auch Systemwarnungen des LiSS series Gerätes
- *Ablaufdatum (JJJJMMTT)* - bei zeitlich begrenzten Nutzerkonten kann hier das Ablaufdatum eingetragen werden. 20101231 bedeutet, das sich der Nutzer nach dem 31. Dezember 2010 nicht mehr am LiSS series System anmelden kann.
- *Passwort* - Passworteingabe in einem separaten Dialogfenster, Passwort Wiederholung um Tippfehler auszuschließen. Das Passwort wird anhand der eingestellten *Passwortrichtlinie* auf Komplexität hin überprüft.

Lokalen Nutzer Löschen

Das *Löschen* von lokalen Benutzern erfolgt direkt nach Betätigung der *Löschen* Schaltfläche in der Zeile, die den Nutzer auflistet. Es erfolgt keine Sicherheitsabfrage. Nur durch *Abbrechen* kann ein eventueller Bedienfehler wieder rückgängig gemacht werden.

Lokalen Nutzer bearbeiten

Die Konfiguration eines lokal gepflegten Nutzers kann über *Einstellungen - Nutzer - Nutzer - Anwahl des Nutzers* erfolgen.

Nutzer aus CSV-Datei importieren

Um eine größere Zahl neuer lokaler Nutzer zu erstellen, eignet sich der Import aus einer CSV-Datei. Die Datei muss eine reine Text-Datei sein, in der jede Zeile einen Nutzer enthält. Die verschiedenen Werte für jeden Nutzer werden durch Kommata voneinander getrennt (deshalb dürfen die Werte selbst keine Kommata enthalten). Die ersten drei Werte sind zwingend erforderlich.

- *Anzeigename* - ein beschreibender Name, der in der Nutzer-Übersicht angezeigt wird.
- *Anmeldename* - der Anmeldename des Nutzers, mit welchem er sich am Web-Interface der LiSS series oder dem Proxy anmeldet. Darf keine Leerzeichen oder Nicht-ASCII-Zeichen enthalten und akzeptiert derzeit keine Großbuchstaben
- *Passwort* - das unverschlüsselte Passwort. Darf keine Leerzeichen oder Nicht-ASCII-Zeichen enthalten. Braucht nicht der Passwort-Richtlinie zu entsprechen. Wenn es auf *start* gesetzt wird, muss der Nutzer das Passwort beim ersten Zugriff auf das LiSS series Web-Interface neu setzen.

Alle weiteren Werte sind optional. Ein fehlender Wert muss durch ein leeres Feld (...,,...) gekennzeichnet werden, wenn in der Zeile weitere Werte folgen.

- *E-Mail Adresse* - E-Mailadresse des Nutzers

Nutzer Ansicht

Die vorhandenen Nutzer werden tabellarisch dargestellt. Die erste Spalte enthält alle lokalen Nutzer.

Die zweite Spalte gibt die Datenquelle an. Die dritte Spalte enthält für lokale Nutzer die Aktion *Löschen*.

Um Nutzer besser zu finden, kann mit der *Suche* gearbeitet werden. Im Feld *Auswahl von Nutzern* kann der Nutzername als Text oder Textteil angeben werden. Über *Auffrischen* wird die Suchmaske auf die gesamte Nutzerliste angewandt. Die Suche ist *casesensitiv*, d.h. Groß- und Kleinschreibung wird unterschieden. Nach einer Änderung ist über *Auffrischen* die Darstellung zu aktualisieren.

Datenquelle Local users

Bei Auswahl der Datenquelle *Local users* können Name der Datenquelle und Passwortrichtlinie geändert werden.

- *Datenquelle* - hier kann der Name des lokalen Repositories angepasst werden
- *Passwortrichtlinie* - legt die Komplexität der Passwörter fest, mögliche Werte sind:
  - *Scherz* - Länge 4, score 3
  - *leicht* - Länge 5, score 5
  - *normal* - Länge 6, score 6
  - *schwer* - Länge 8, score 8
  - *schieriger* - Länge 10, score 8
- *Vergleiche letzte n Passwörter* - LiSS series merkt sich die letzten 1, 3, 5 bzw. 8 Passwörter, diese können dann nicht als neue Passwörter verwendet werden, wenn die Passwortänderung erfolgt
- *Passwortmanager des Browsers zulassen* - hier kann die Speicherung des Passwortes im Webbrowser zugelassen werden

9.3.1 Clients

Clients werden benötigt, um Webfilter-Profile an IP-Adressen, IP-Adressenbereiche oder IP-Netze zu binden. Die Arbeit mit Clients ist nur solange möglich, solange nicht die Nutzerauthentifizierung für den Webfilter eingeschaltet wird.

Bei der Einrichtung von Clients wird die Zeile für IP-Bereich mehrfach genutzt. Soll nur eine Host IP-Adresse oder ein Netzwerk eingegeben werden, dann werden diese Daten in das linke Feld der Zeile *Client IP-Bereich* eingetragen.

9.3.2 Admin-Profile

Admin-Profile dienen der Einschränkung von Berechtigungen für Administratoren und Nutzer des lokalen Repositories. Somit ist es z.B. möglich, ein Nutzerkonto einzurichten, welches auf alle Administrationsdialoge nur Leserechte hat. Dies kann unter Umständen sinnvoll sein, wenn das LiSS series System von extern nicht erreichbar ist.

Es gibt acht verschiedene Profile, von denen zwei eine besondere Bedeutung haben.

- *Administrators* - Administratorprofil des liss-Benutzers, hat alle Rechte
- *Profil 3..8* - anpassbare Profile, Profile können umbenannt werden und bzgl. der Dialoge und Zugriffsrechte eingeschränkt werden

Jeder neu eingerichtete lokale Nutzer erhält automatisch das Admin-Profil *Service Users.* Soll der neu eingerichtete Nutzer ein LiSS series Administrator werden, dann ist im Nachhinein das Admin-Profil zu ändern.

9.3.3 Passwort

Hier kann das Passwort des gerade angemeldeten Benutzers geändert werden. Das Passwort muß den Passwortrichtlinien des lokalen Repositories entsprechen.

10 Diagnose

LiSS series Systeme bieten eine Vielzahl von Diagnosemöglichkeiten. Dazu gehören neben den *Systemlogs* auch *Berichte*, die Konfigurationen zusammenfassend darstellen. Mit den LiSS series eigenen *Werkzeugen* können einfache Netzwerkanalysen betrieben werden.

10.1 Syslog

10.1.1 Logs

Das LiSS series System schreibt Ausgaben einzelner Komponenten ins Log. Dieses befindet sich unter *Diagnose - Syslog - Logs*. Das *ALL-Log* enthält alle Ausgaben in einer Ansicht. Um detailierte Loganalysen betreiben zu können, sind einzelne Logausgaben auf verschiedenen Teillogs aufgeteilt:

- *All* - alle Logausgaben in einer Ansicht
- *Auth* - Ausgaben vom VPN
- *Daemon* - Ausgaben der PPP-Einwahl, des NTP-Dienstes
- *Firewall* - Firewallog
- *Kern* - Kernellog, enthält Systemmeldungen des Systemstartes
- *Local* - Ausgaben der Webadministrationsoberfläche
- *APLGW* - Ausgabe der Virenscanner und Webfilter

10.1.2 Einstellungen

Der Speicherplatz auf dem LiSS series System für Systemlogs ist begrenzt. Ist dieser vollständig ausgenutzt, wird das entsprechende Log neu angelegt. Somit stehen die Logdaten des LiSS series Systems nur zeitlich begrenzt zur Verfügung. Um dies zu umgehen, bietet die LiSS series unter *Diagnose - Syslog - Einstellungen* die Möglichkeit extern zu loggen. Dabei werden die Ausgaben, die normalerweise im Log der LiSS series Systeme erscheinen, über das Netzwerk an einen Syslogserver gesendet. Dies erfolgt mittels Syslog-Protocol, welches per UDP Port 514 in Klartext die Logdaten zum Syslogserver überträgt.

Es können alle Logausgaben zu einem entfernten Syslogserver übertragen werden, indem unter *Diagnose - Syslog - Einstellungen - All* die IP-Adresse oder der Hostname des Syslogservers

eingetragen wird. Sollen nur Teillogs an einen Syslogserver übertragen werden, dann ist beim jeweiligen Teillog der entsprechende Syslogserver anzugeben. Somit besteht auch die Möglichkeit zwei Syslogserver anzusprechen.

Der bei *All* eingetragene Syslogserver sollte nicht auch noch bei den Teillogs angegeben werden, da sonst Logeinträge doppelt gesendet werden.

10.2 Berichte

10.2.1 Einstellungen

Berichte können per "Knopfdruck" auf *Report versenden* an eine konfigurierte E-Mailadresse geschickt werden. Die Konfiguration für den Versand erfolgt hier.

- *E-Mail-Adresse des Empfängers* - legt fest, an wen die ausgewählten Berichte per E-Mail geschickt werden
- *E-Mail-Adresse des Absenders* - hier kann die Absenderadresse festgelegt werden, von welcher die Berichte geschickt werden sollen
- *SMTP-Server (FQDN oder IP-Adresse)* - SMTP-Server, der für den E-Mailversand benutzt wird
- *es folgt die Auswahl der Berichte aus:*
  - *Netzwerk*
  - *VPN*
  - *Firewall*
  - *IDS*
  - *APLGW*
  - *Firmware*
  - System

10.2.2 Netzwerk

Der Netzwerkbericht enthält eine *Liste aller Schnittstellen* mit

- IP-Adresse

- Mac-Adressen
- Die Ausgabe entspricht *ip addr show*

Weiter werden die Hauptroutingtabelle, die Routing Richtlinien und die Schnittstellenstatistik mit Paket- und Bytezählern für eingehenden und ausgehenden Datenverkehr gelistet.

Die DNS/DHCP-Konfiguration, die NTP-Dienst Konfiguration und eine Statistik der Priorisierung ist im unteren Teil des Berichtes zu finden.

10.2.3 VPN

Der VPN-Bericht listet die gerade auf dem LiSS Gerät vorhandene Entropie. Die RSA-Schlüsselerstellung langer Schlüssel wird durch eine hohe Entropie beschleunigt.

Der VPN Status listet alle geladenen Verschlüsselungsalgorithmen und alle konfigurierten VPN-Tunnel mit den IPsec Parametern der VPN-Tunnel.

10.2.4 Firewall

Hier ist das komplette *iptables* Regelwerk einsehbar. Gelistet werden die Inhalte folgender Tabellen mit allen Chains:

- filter IPv4
- mangle IPv4
- nat IPv4
- raw IPv4
- tproxy IPv4
- filter IPv6
- mangle IPv6

In der zweiten und dritten Spalte sind die *Paket-* und *Bytezähler* ersichtlich. Hiermit kann nachgewiesen werden, ob Daten durch eine entsprechende Firewallregel gehen. Über *Rücksetzen* werden alle Zähler auf Null gesetzt und über *Auffrischen* wird der Bericht neu geladen und die Zähler aktualisiert.

10.2.5 IDS

Hier werden alle durch das IDS geblockten Systeme gelistet. Um alle Systeme aus der Liste zu entfernen, ist die LiSS 700 series neu zu starten.

10.2.6 APLGW

Hier werden alle definierten Clients und Profile gelistet.

10.2.7 Firmware

Im Firmwarebericht sind Informationen über den am LiSS series System angemeldeten Benutzer und die IP-Adresse des Administrationsrechners ersichtlich.

Neben Seriennummer werden Datenbankversion und Firmwareversion einschließlich LiSS series Repository Revisionsnummer und Firmwareerstellungsdatum gelistet.

10.2.8 System

Der Systembericht gibt Auskunft über die aktuelle Systemlast (*Load*) und Laufzeit (*Uptime*) des LiSS series Systems.

Die Systemlast wird in drei Spalten angezeigt:

- erste Spalte - Mittelwert der letzten Minute
- zweite Spalte - Mittelwert der letzten 5 Minuten
- dritte Spalte - Mittelwert der letzten 15 Minuten

Unter *Process list* werden alle zur Zeit auf dem LiSS series System laufenden Prozesse gelistet. Wobei pro Prozess Speicher- und CPU-Auslastung angezeigt wird.

Im unteren Teil des Berichtes ist die Auslastung des Dateisystems unter *Disc usage* zu finden.

10.3 Werkzeuge

10.3.1 Ping

Dieses Werkzeug dient dem einfachen Test einer Verbindung mittels *ICMP echo request*. Unter *Ping nach* kann eine IP-Adresse oder ein Hostname angegeben werden. Wenn nötig, dann kann der Ping auch an IPv6 Adressen geschickt werden.

10.3.2 Traceroute

Traceroute schickt Datenpakete in Richtung Zielsystem, bei denen der TTL-Zähler schrittweise von 1 an erhöht wird. Der TTL-Zähler wird auf jedem Router um den Wert 1 verringert. Ist der Zähler gleich Null, meldet der Router dem Absender, das der TTL-Wert des Paketes den Wert Null erreicht hat. Somit erhält der Absender eine Information vom routenden System und der Weg der Pakete vom Absender zum Ziel kann somit aufgezeichnet werden.

- Ziel - IP-Adresse oder Hostname des Zielsystems
- Max. Anzahl Hops (6-255) - Begrenzung des TTL-Zählers auf einen Maximalwert
- IPv6 - traceroute mit Verwendung des IPv6 Protokolls
- Protokoll/Port - Auswahl zwischen:
  - UDP
  - TCP
  - ICMP

Durch Angabe des Ports kann traceroute somit benutzt werden, um andere Kommunikationen nachzubilden und um zu analysieren, ob diese auf dem Weg zum Ziel durch andere Firewalls geblockt wird. So simuliert ein traceroute mit TCP-Port 80 eine Webserveranfrage zu einem Webserver.

Im Ausgabefenster erscheint nach Beendigung des traceroute-Befehls dessen Ausgabe.

10.3.3 DNS

Um die korrekte Namensauflösung des LiSS series Systems oder eines DNS-Servers zu prüfen, können mit diesem Werkzeug verschiedene DNS-Anfragen vom LiSS series System aus gestartet werden

- *Hostname* - Abfragetext, Hostname oder Domainname
- *Alternativen DNS-Server verwenden* - um Antworten verschiedener DNS-Server zu vergleichen, kann hier ein alternativer DNS-Server per IP-Adresse angegeben werden
- *Abfrage-Typ:*
  - *A* - für die Forward-Auflösung von DNS-Namen in IPv4-Adressen

- *AAAA* - für die Forward-Auflösung von DNS-Namen in IPv6-Adressen
- *ANY* - Abfrage jeden Types
- *CNAME* - Alias eines Namens
- *MX* - mail exchanger; E-Mailserver der Domain
- *NS* - Nameserver der Domain
- *PTR* - pointer record; dient der Auflösung von IP-Adresse in Hostnamen
- *SOA* - start of authority; kennzeichnet das für eine Zone authorisierte System, an dem Änderungen der Zonendaten vorgenommen werden dürfen
- *TXT* - Texteintrag; wird für verschiedene Einträge genutzt, z.B. opportunistic encryption oder Sender Policy Framework

Über *Start* wird die DNS-Anfrage zum DNS-Server abgeschickt. Ist kein alternativer DNS-Server angegeben, dann wird die DNS-Konfiguration des LiSS series Systems angewendet.

11 Konfigurationsbeispiele

11.1 Erstkonfiguration für Eilige

Zur Ersteinrichtung liegt der LiSS 700 series ein Faltblatt bei, auf dem alle nötigen Schritte einzeln erklärt sind. Die Ersteinrichtung erfolgt dabei analog den größeren LiSS series Systemen. Der LAN Port hat die Werkseinstellungs IP-Adresse 192.168.1.1 . Über eine https-Verbindung kann die LiSS 700 series administriert werden. Werkseinstellungsdaten sind im Anhang auf Seite II aufgeführt.

11.1.1 Internetzugang einrichten

Externes Interface konfigurieren

PPPoE

Wird ein DSL Anschluß verwendet, dann ist hierfür die WAN-Schnittstelle als PPPoE-Interface einzurichten. Die nötigen Angaben beschränken sich oftmals auf Nutzername und Passwort.

Ethernet Interface

Wird kein PPPoE-Interface benötigt, weil z.B. ein Abschlussrouter vorhanden ist, dann wird die WAN-Schnittstelle entsprechend der Vorgabe des Providers als Ethernetschnittstelle mit IP-Adresse und Netzmaske konfiguriert. Meistens gibt es ein Verbindungsnetz in dem sich Router und LiSS Gerät befinden.

Default route

Um Pakete in unbekannte, entfernte Netze zustellen zu können ist die Einrichtung einer *default-route* nötig. Dies bedeutet, daß alle Datenpakete, die vom LiSS Gerät nicht in lokal angeschlossene Netze zugestellt werden können, an einen anderen Router weitergereicht werden, damit dieser sich um die Zustellung der Datenpakete kümmert.

Die *defaultroute* wird bei Einrichtung eines PPP-Zugangs nicht automatisch gesetzt. Dies erklärt sich daraus, das es möglich ist, mehrere Internetzugänge einzurichten und gleichzeitig zu nutzen.

Anlegen einer default route

- *Netzwerk - Main - Routen - Neu*
- Ziel: 0.0.0.0/0 [15]
- Gateway: IP-Adresse des nächsten Routers in Richtung Internet
  - bei PPPoE bleibt das Gateway leer, es ist nur das PPP-Interface anzugeben: ppp0

11.2 Konfiguration der Systeme im LAN

Standardgateway

Die Systeme im Netzwerk sollten als *Standardgateway* die IP-Adresse des LiSS Gerätes verwenden, die im selben Netzwerk wie die IP-Adresse des Systems liegt.

DNS

Gewöhnlicherweise wird bei der Internetnutzung mit Hostnamen gearbeitet. Zu jedem Hostnamen gehört mindestens eine IP-Adresse. Das *Domain Name System (DNS)* liefert eine Zuordnung von Hostname zu IP-Adressen. Um in Anwendungsprogrammen mit Hostnamen arbeiten zu können wird ein *DNS-Server* benötigt, der die IP-Adresse zu einem Hostnamen liefert.

Sollte sich im LAN kein DNS Server befinden, kann das LiSS Gerät als DNS-Server benutzt werden. Dazu sollte bei den Systemen im LAN die IP-Adresse des LiSS Gerätes als DNS-Server angegeben werden, die im selben Netzwerk wie die IP-Adresse des Systems liegt. Für die Nutzung der LiSS als DNS Server ist die Konfiguration in Abschnitt 5.2.1 zu beachten.

Der DNS Server auf dem LiSS Gerät ist standardmäßig eingeschaltet.

Maskierung

Werden im LAN private IP-Adressen[16] benutzt, die im Internet nicht geroutet werden, dann ist eine IP-Adressumsetzung nötig, damit die IP-Pakete ihr Ziel erreichen können. Diese Umsetzung wird *NAT (Network Address Translation)* genannt. Ein Spezialfall ist das Maskieren von Adressen.

Die Maskierfunktion wird über die Firewall bereitgestellt. Eine Firewallregel mit Maskierung für das LAN mit häufig genutzten Diensten wird folgendermaßen angelegt:

[15] 0.0.0.0/0 steht dabei für den gesamten IP-Adressraum von IPv4
[16] vgl. Anhang D

- *Firewall - Paketfilter - Filterung - Neu*
- *Erstelle Regel zwischen: extern - extern*
- *Regelname* - “LAN ins Internet”
- *Plaziere Regel hinter/als* - als erste
- *Aktion* - annehmen
- *Dienste* - gängige Internetdienste wie HTTP, HTTPS, FTP etc..
- *Quelle* - LAN, Netzwerkadresse/Netzmaske
- *Ziel* - 0.0.0.0/0 [17]
- *Weitere Einstellungen*
  - *Maskieren* - ja
- OK - Speichern
- unter *Firewall - Paketfilter - Einstellungen* die Firewall über
  - *Paketfilter einschalten* - ja starten
- weitere Empfehlungen zur Einrichtung der Firewall unter Abschnitt 6.1.6

Setzen der Systemzeit

Nach der Erstinbetriebnahme ist die Systemzeit noch nicht aktuell. Diese muß einmalig manuell korrigiert werden. Anschließend kann die Systemzeit per NTP aktuell gehalten werden.

11.3 VPN

11.3.1 VPN zwischen Standorten mit statischen IP-Adressen

Die Einrichtung eines VPN-Tunnels zwischen zwei Standorten mit festen IP-Adressen ist einfach und erhöht die Sicherheit, weil nur zu ganz konkreten IP-Adressen die IPSec-Dienste geöffnet werden müssen. Ein weiterer Vorteil besteht in der direkten Erreichbarkeit beider Seiten.

[17] 0.0.0.0/0 steht dabei für den gesamten IP-Adressraum von IPv4 und bezeichnet somit das gesamte Internet

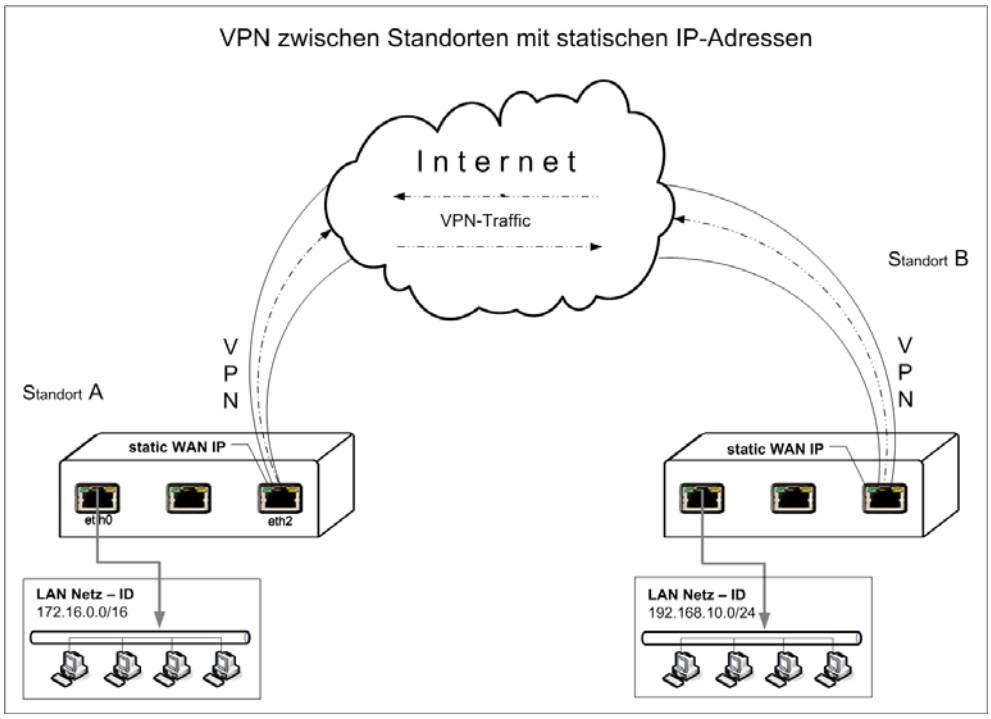


Abbildung 11: VPN mit statischen IP-Adressen

Der VPN-Tunnel kann von jeder Seite aus aufgebaut werden, da jede Seite die Andere eindeutig über Ihre statische IP-Adresse adressieren kann. Es sind keinerlei Hilfsmittel wie DynDNS-Dienste nötig, die eine zusätzliche Fehlerquelle darstellen könnten. In Abbildung 11 ist die Beschaltung schematisch dargestellt.

Besonderheiten zur Einrichtung eines VPN-Tunnels mit statischen IP-Adressen

Wichtig ist die Angabe der statischen offiziellen IP-Adresse der Gegenstelle bei den Phase 1 Einstellungen. Steht lokale IP auf Standard, dann verlassen die VPN-Pakete das LiSS series System über das default Gateway. Wenn beide Standorte eine Statische IP-Adresse haben, sollte unter *Verbindungs Einstellungen - Verbindung*: aktiv Verbinden aktiviert werden. Somit baut das LiSS series System nach einem Neustart denVPN-Tunnel selbständig wieder auf. Die Phase 2 Angaben entsprechen den zu verbindenden Netzen bzw. Hosts.

11.3.2 VPN zwischen zwei Standorten mit gleichen IP-Netzen, Anwendung von Netz-Mapping

Bei der Nutzung von VPNs kann es dann problematisch werden, wenn es an beiden Standorten die gleichen IP-Netze gibt. Dann wird das Datenpaket, welches zur anderen Seite durch den

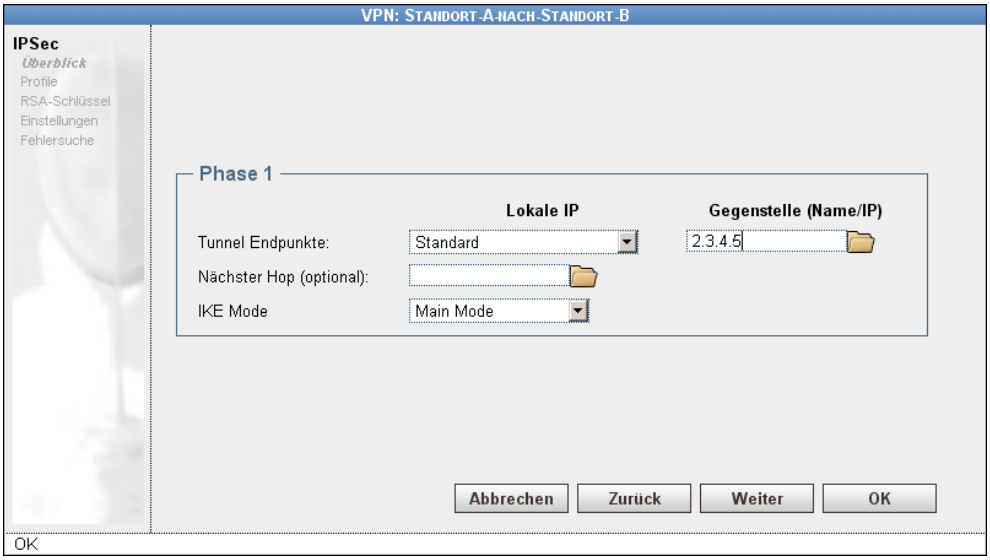


Abbildung 12: VPN statisch zu statisch Phase 1

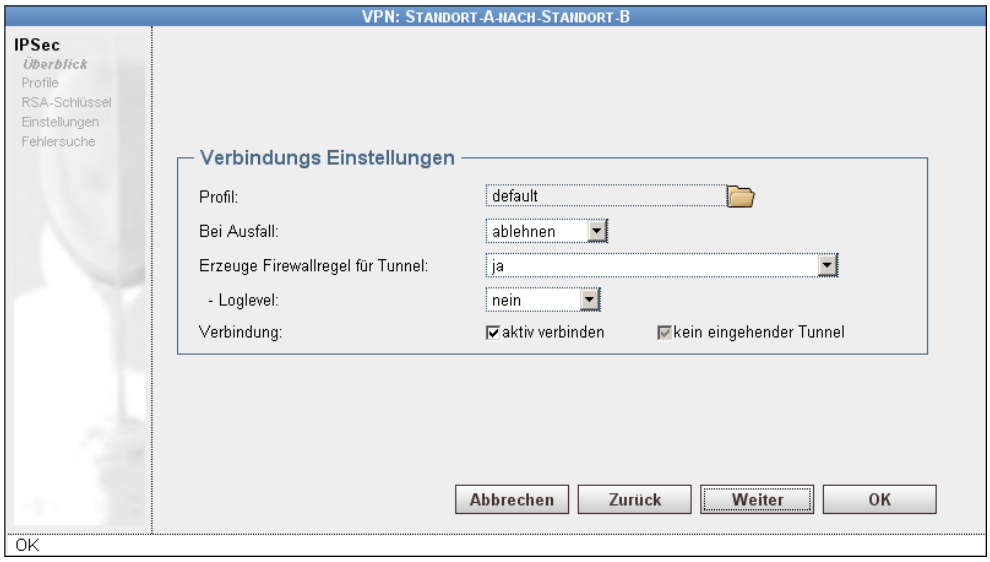


Abbildung 13: VPN statisch zu statisch - aktiv Verbinden

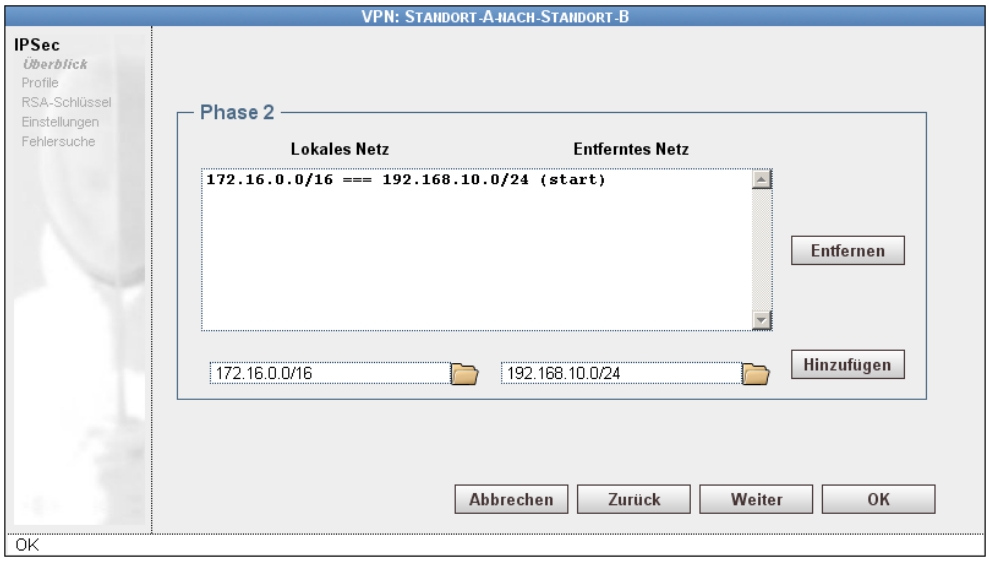


Abbildung 14: VPN statisch zu statisch Phase 2

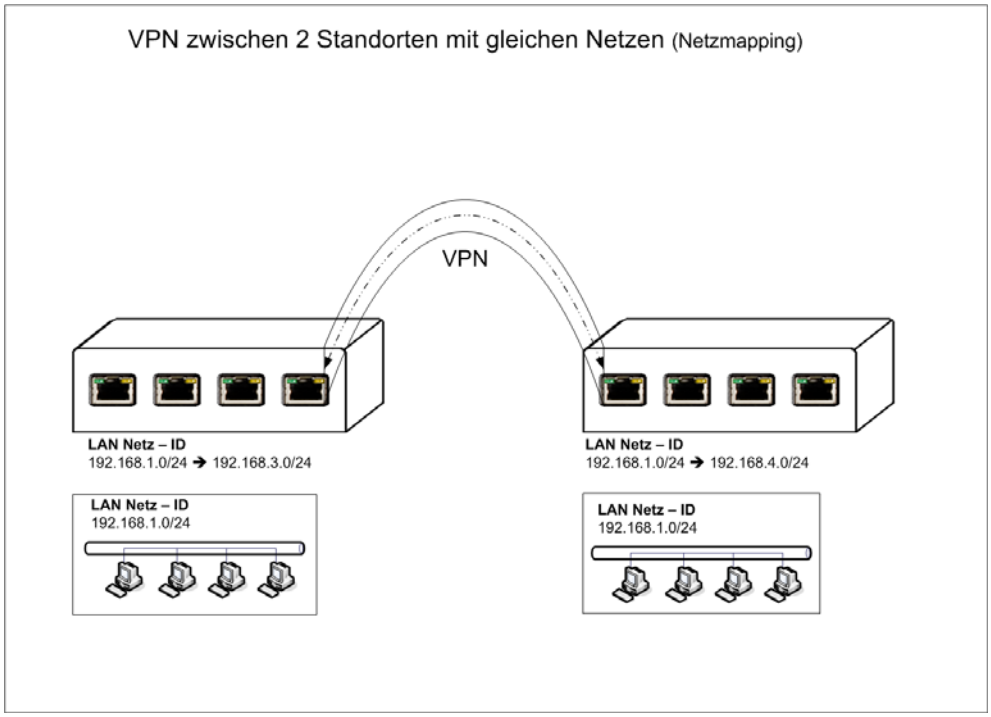


Abbildung 15: VPN mit gleichen Netzen, Netz-Mapping hilft

VPN-Tunnel geroutet werden soll, im lokalen Netzwerk zugestellt. Sein eigentliches Ziel erreicht es nicht. LiSS series Systeme bieten hierfür mit dem *Netz-Mapping* eine Möglichkeit auch diese Schwierigkeiten bei der Einrichtung von VPN-Tunneln zu meistern. Beim Netz-Mapping, welches sich unter dem Menupunkt *Firewall* befindet, wird die originale Absendeadresse für ein ganzes Netzwerk in eine andere Absendeadresse umgesetzt. Bedingung beim Netz-Mapping ist, das Original-Quellnetzwerk und umzusetzendes Netzwerk die gleiche Netzmaske haben, bzw. der Adressraum gleich groß ist. Die Umsetzung der Netzwerkadressen hat so zu erfolgen, dass jedes Netz an einem Standort so umgesetzt wird, das die umgestetzten Netze nacher nicht mehr gleich sind. Zwischen diesen umgesetzten Netzen wird dann der VPN Tunnel aufgebaut. Bedingung für eine erfolgreiche Kommunikation zur Gegenstellen ist, das die Systeme am Standort der Gegenstelle mit der umgesetzten IP-Adresse angesprochen werden, damit das Datenpaket dann durch den VPN-Tunnel läuft und die Gegenseite erreicht.

Bei der Auswahl von Netz-Mapping stehen 3 verschiedene Varianten zur Verfügung:

- *Bidirektionales Mapping* - Hin- und Rückumsetzung wird in *einer* Maske festgelegt, diese Umsetzung gilt für alle Dienste, sehr einfache Einrichtung
- *Quell-Mapping* - soll die Umsetzung nur für einzelne Dienste erfolgen, dann ist separat Quell- und Zielmapping einzurichten, etwas aufwendiger, jedoch genauer
- *Ziel-Mapping* - soll die Umsetzung nur für einzelne Dienste erfolgen, dann ist separat Quell- und Zielmapping einzurichten, etwas aufwendiger, jedoch genauer

Im obigen Beispiel in Abbildung 15 ist die Umsetzung für den hier beschriebenen Fall skizziert. Abbildung 16 zeigt die Einrichtung des Netz-Mappings für den linken Standort und Abbildung 17 die Einrichtung der Phase 2 im VPN Tunnel.

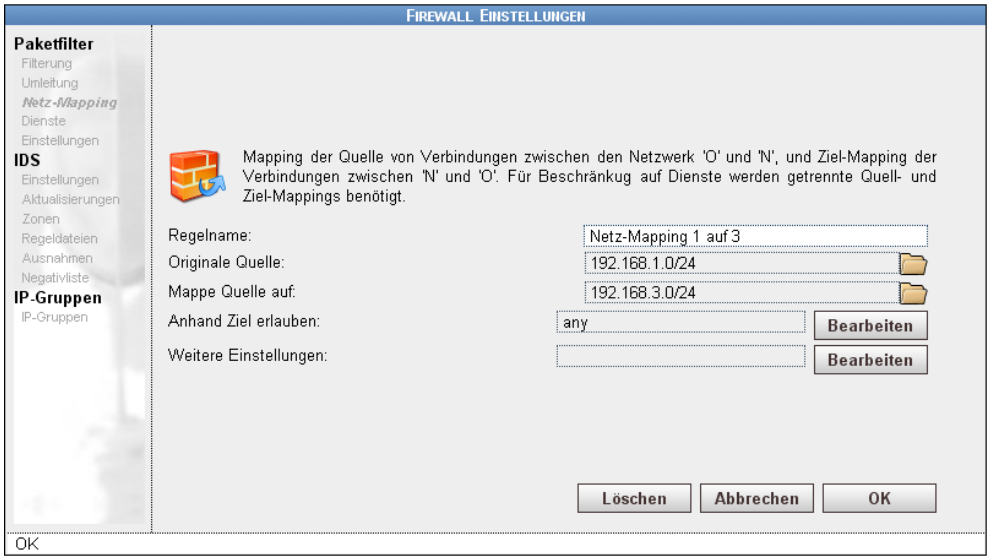


Abbildung 16: Bidirektionale Netz-Mapping

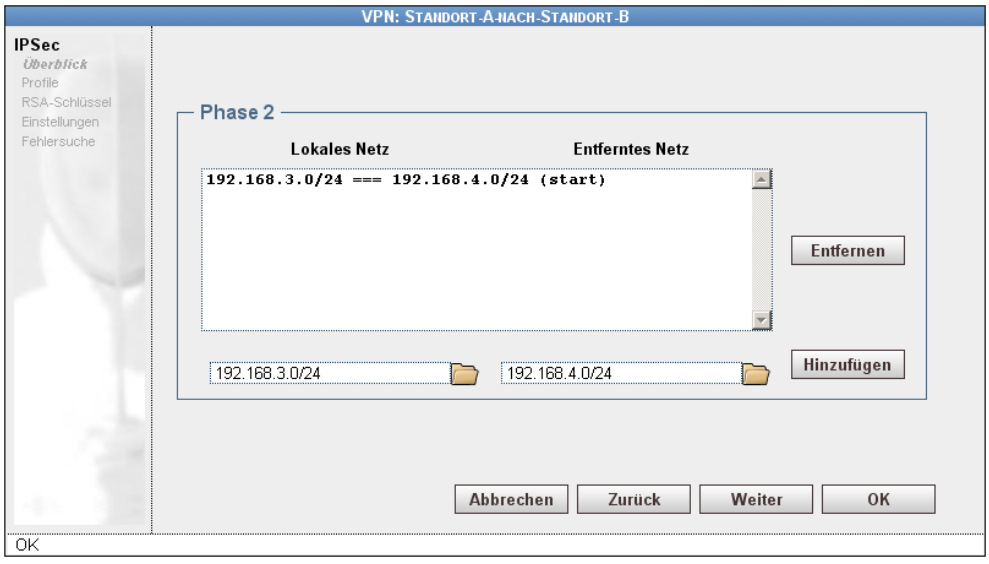


Abbildung 17: VPN Phase 2 mit Netz-Mapping

Anhang

- Werkseinstellungen
- Orange Filter Kategorien
- DynDNS Anbieter-Liste der LiSS series
- Systemregeln des Paketfilters
- Warenzeichen
- Hinweise für Ihre Sicherheit und zum Gerätebetrieb
- Firmendaten
- GNU GENERAL PUBLIC LICENSE Version 2, June 1991

Werkseinstellungen

Bei Auslieferung befindet sich das Gerät in Werkseinstellung.

- IP-Adresse des LAN-Ports 192.168.1.1/24
- Nutzername: *liss*
- Passwort: *start*

Orange Filter Kategorien

- Abtreibung
- Alkohol
- Allgemeine Neuigkeiten / Zeitschriften / MagazineAbtreibung
- Alkohol
- Allgemeine Neuigkeiten / Zeitschriften / Magazine
- Anonyme Proxies
- Auktionen / Branchenwerbung
- Bademode / Unterwäsche
- Banken / Home Banking
- Bauen / Wohnen / Architektur / Möbel
- Chat
- Computer
- Kriminalität
- Computer Spiele
- Digitale Postkarten
- Erotik / Sex
- Erziehung
- Extreme
- Fahrzeuge / Beförderung
- Finanz Makler / Aktien
- Finanzservices / Investitionen
- Freizeitbeschäftigung / Vergnügungen / Themen Parks
- Glücksspiele

- Haß / Diskriminierung
- Humor / Comic
- illegale Betätigung
- illegale Drogen
- Instant Messaging
- IT Security
- Jobsuche
- Jugendschutz (Deutsch)
- Kino / Fernsehen
- Kunst / Museen
- Literatur / Bücher
- Malware
- Mode / Kosmetik / Schmuck
- Musik
- Natur / Umgebung
- Newsgroups / Bekanntmachungen / Allgemeine Diskussionen
- Nichtstaatliche Organisationen
- Online Shopping
- Pishing URLs
- Politische Parteien
- Pornographie
- Private Homepages
- Reise
- Religion

- Restaurants / Bars
- Sekten
- Selbst-Hilfe / Sucht
- SMS / Mobilfunkzubehör
- Software und Hardware Anbieter / Distributoren
- Spam URLs
- Spielzeug
- Sport
- Staatliche Organisationen
- Städte / Länder / Staaten
- Suchmaschinen / Web Kataloge / Portale
- Tabak
- Übersetzungen
- Verabredungen / Beziehungen
- Waffen
- Warez / Hacking / illegale Software
- Webhosting / Breitband
- Web Mail

DynDNS Anbieter-Liste der LiSS series

- *dhs*
- *dnsexit*
- *dyndns*
- *dyndns-custom*
- *dyndns-static*
- *dyns*
- *easydns*
- *everydns*
- *ezip*
- *heipv6tp*
- *hn*
- *justlinux*
- *managed-security*
- *noip*
- *ods*
- *pgpow*
- *tzo*
- *zoneedit*

Systemregeln des Paketfilters

Systemregel	Beschreibung
IDS: IDS block rules	Prüfung auf durch das IDS geblockte Systeme
PPP: PPP traffic	Zulassen von PPP Datenverkehr
STATEFUL: Use connection tracking	Nutzen der connectiontracking Hilfstabelle des Kernels, dient zur Beschleunigung der Abarbeitung des Regelwerkes
ROUTER: Accept default router traffic and ICMP messages	Zulassen von benötigten ICMP-Typen zur Verständigung der Router untereinander bzw. Benachrichtigungen an Clients bzgl. Datenverbindung
KEYLOCK: Accept web connections if key is unlocked	Erlauben von HTTPS-Verbindungen zum LiSS series System zur Administration, wenn Schlüsselschalter auf unlock
LISS: Accept outgoing traffic from LiSS	Ausgehenden Datenverkehr vom LiSS series System erlauben; TCP alle Ports, Syslog
DNS: ACCEPT outgoing DNS traffic	vom LiSS series Gerät ausgehender DNS Datenverkehr
DHCP: Accept dhcp traffic	Datenverkehr zum DHCP der LiSS series
TIME: Accept traffic to external time server	Zeitsynchronisation des LiSS Systems
APLGW: Web/Mail proxy related traffic	Datenverkehr zum Webproxy je nach festgelegtem Proxyport, Datenverkehr zum SMTP-Proxy TCP Port 25
DIAGNOSTICS: Diagnostic utilities and Syslog	traceroute, ping, syslog vom LiSS System weg
NAT: Perform portforwarding and net mapping	Portweiterleitung und Netmapping
IPSEC: Accept traffic for vpn connections	IPsec Datenverkehr zwischen den VPN-Gateways, siehe IPsec Dienst
IPSEC_TUNNEL: Accept all traffic in vpn tunnels	Datenverkehr zwischen den Phase2 Netzen der VPNs, alles erlaubt!

Tabelle 4: Firewall, Paketfilter Systemregeln

Warenzeichen

Die aufgeführten und nicht aufgeführten Produkt- und Firmenbezeichnungen sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Firmen und Organisationen:

- LINUX ist eingetragenes Warenzeichen von Linus Torvalds
- Microsoft, Microsoft Office, Active Directory, Exchange Server, Windows, Windows NT und XP, Windows 2000 und 2003, Internet Explorer und Outlook sind eingetragene Warenzeichen der Microsoft Corporation
- NetWare und Novell sind eingetragene Warenzeichen der Novell Incorporation in den USA und anderen Ländern
- INTEL ist ein eingetragenes Warenzeichen der INTEL Corporation
- Antivir ist ein eingetragenes Warenzeichen der Avira GmbH

Hinweise für Ihre Sicherheit und zum Gerätebetrieb

Bitte beachten Sie unbedingt die folgenden Hinweise

- Lesen Sie vor der Inbetriebnahme das Handbuch gründlich
- Verwenden Sie nur das original Netzteil und die original Anschlusskabel
- Gerät und Netzteil niemals selbst öffnen
- Bei beschädigtem Netzteil ist das Gerät sofort vom Stromnetz zu trennen. Es besteht die Gefahr eines elektrischen Schlages.
- Kontakte nicht mit metallischen Gegenständen berühren.
- Anschlussleitungen und Kabel sind so zu verlegen, dass niemand darauf treten oder darüber stolpern kann
- Gerät nur entfernt von Wärmequellen betreiben und direkte Sonneneinstrahlung vermeiden
- Gerät vor Nässe, Staub aggressiven Flüssigkeiten und Dämpfen schützen
- Nur Originalzubehör verwenden
- Kabel nur an die dafür vorgesehenen Buchsen anschließen
- Lüftungsschlitze des Gerätes nicht verdecken
- Keine Gegenstände auf dem Gerät ablegen
- Für ausreichende Luftzirkulation sorgen
- Informieren Sie sich regelmäßig über aktuelle Hinweise und Updates zu Ihrem Gerät auf unserer Internet-Seite: http://www.liss.de
- Zur Installation folgen Sie den Installationsanweisungen. Bei technischen Funktionsstörungen wenden Sie sich bitte an den Technischen Kundendienst. Mailadressen und Rufnummern finden Sie auf der Internet-Seite http://www.liss.de

Firmendaten

TELCO TECH GmbH
Potsdamer Str. 18a
D-14513 Teltow
Deutschland

Geschäftsführer: Gerd Lochter
Tel: 03328 430810
Fax: 03328 430815
E-Mail: info@telco-tech.de
Web: www.telco-tech.de

Gerichtsstand: Amtsgericht Potsdam
HRB: 55 79
StNr: 046/121/05532
USt-IdNr: DE155862066
WEEE-Reg.-Nr. DE87860538
D-U-N-S® 33-170-9071

GNU GENERAL PUBLIC LICENSE Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software–to make sure the software is free for all its users. ThisGeneral Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights.These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "‘Program"’, below, refers to any such program or work, and a "‘work based on the Program"’ means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "‘modification"’.) Each licensee is addressed as "‘you"’.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program).Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program’s source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty

(or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed

need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify ordistribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannotimpose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "‘any later version"’, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTYFOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "‘AS IS"’ WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE

IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Index