Administrationshandbuch Collax Security Gateway 7.0

Administrationshandbuch

Collax Security Gateway

Version 7.0

CSG COLLAX SECURITY GATEWAY

COLLAX Flexible IT

Administrationshandbuch Collax Security Gateway
Version 7.0

Stand: 1.12.2017

Collax GmbH
Gutenbergstr. 1 · D-85737 Ismaning
Tel. +49 (0) 89 / 99 01 57-0
Fax +49 (0) 89 / 99 01 57-11
<http://www.collax.com>

Inhaltsverzeichnis

Vorwort

Vielen Dank, dass Sie sich für den Collax Security Gateway entschieden haben, die Linux-basierte Serverlösung für kleine und mittelständische Unternehmen.

Der Collax Security Gateway integriert die Kontrolle über alle Ihre Serveranwendungen und -funktionen in eine grafische Benutzeroberfläche. So können Sie Kommunikation, Sicherheit und Netzwerkinfrastruktur leichter verwalten.

Sie benötigen lediglich Kenntnisse über vernetzte IT-Systeme, um Ihren Collax Security Gateway in Betrieb nehmen und konfigurieren zu können.

Dieses Handbuch zeigt Ihnen Schritt für Schritt, wie Sie Ihren Server so einrichten können, dass er am besten zu Ihren geschäftlichen Erfordernissen passt.

Bitte kontaktieren Sie das Collax-Support-Team über Telefon, E-Mail oder Fax, wenn Sie Fragen oder Probleme haben, die Sie selbst nicht beantworten oder lösen können.

Weitere aktuelle Informationen finden Sie im Web unter: <http://www.collax.com>

1 Übersicht

Mit dem Collax Security Gateway wurde ein leistungsfähiges System für Serveranwendungen geschaffen, welches gleichzeitig sehr einfach zu bedienen ist.

Der Anwender steuert das System mit einem nahezu beliebigen Browser über eine durchgängig einheitliche Weboberfläche. Unter dieser Oberfläche läuft eine speziell angepasste Linux-Variante. Bei dieser wurde gezielt die beste auf dem Markt verfügbare freie Software für eine jeweilige Aufgabenstellung ausgesucht. Dieser „Best of Breed"-Ansatz führt zu einem schlanken und übersichtlichen System, welches durch Konzentration auf das Wesentliche sehr sicher gehalten werden kann.

Mit den Wurzeln dieser Software, die weit in die Unix-Welt reichen, eignet sich der Collax Security Gateway zudem besonders gut für alle verknüpften Dienste wie Mail, Webserver und VPN. Auch hier liegt das Augenmerk auf einem möglichst sicheren Betrieb der jeweiligen Dienste.

Grundsätzlich sind alle Dienste zunächst deaktiviert. Der Anwender entscheidet, was er überhaupt einsetzen möchte. Assistenten helfen ihm, eine sinnvolle Konfiguration des Collax Security Gateways auf einfache Weise zu erstellen.

Das vorliegende Handbuch wird alle Aspekte der Konfiguration und des Betriebs des Collax Security Gateways behandeln. Bei einigen zentralen Themen werden zudem notwendige Hintergrundinformationen gegeben, um die Funktionsweise des Systems besser zu verstehen.

Mit beinahe jedem Softwareupdate werden weitere sinnvolle Funktionen zum Collax Security Gateway hinzugefügt. Dieses Handbuch

dient daher der Orientierung im System. Detaillierte Hinweise zu einzelnen seltenen oder zum Zeitpunkt der Drucklegung noch nicht vorhandenen Funktionen finden sich in der Onlinehilfe des Systems. Die Onlinehilfe wird regelmäßig automatisch aktualisiert.

2 Inbetriebnahme

Der Collax Security Gateway ist in zwei grundsätzlichen Ausführungen erhältlich, einmal als reine Softwareversion und einmal als vollständiges Hardware-Appliance-System. Für die Softwareversion wird ein Hardware-System mit x86_64-kompatibler CPU benötigt. Bei der Installation der Software wird die Festplatte vollständig gelöscht.

Zum Testen des Collax Security Gateways kann von der CD ein „Live-System“ gestartet werden. Dabei werden keinerlei automatische Änderungen an der Festplatte vorgenommen.

Die Hardware-Appliance ist in unterschiedlich leistungsfähigen Ausbaustufen erhältlich und reicht von kleinen kompakten Geräten bis zu ausgewachsenen Serversystemen in 19-Zoll-Technik.

2.1 Installation Softwareversion

Zur Installation der Software muss das System von der CD oder einem USB-Image gebootet werden.

Hinweis: Bei Installation der Collax Security Gateway-Software wird die gesamte Festplatte gelöscht. Es gibt keine Möglichkeit, bereits vorhandene Partitionen oder Daten zu erhalten.

Nach dem Start der Installation des Collax Security Gateways folgen Sie einfach den Anweisungen. Wenn die Installation abgeschlossen ist, kann das System neu gestartet werden.

2.2 Bedienung des LCD

Ältere Appliance-Systeme verfügen über ein LCD-Display. Darüber kann u. a. die voreingestellte IP-Adresse des Systems temporär geändert werden. Die weitere Konfiguration wird anschließend über die Web-Oberfläche vorgenommen.

Das LCD-Display besitzt zwei Modi:

Im Statusmodus werden verschiedene Informationen über CPU-Auslastung, Festplattenbelegung, Schnittstellenkonfiguration usw. angezeigt.

Im interaktiven Modus kann die IP-Adresse der Netzwerkkarte „eth0“ vorübergehend geändert und der Server heruntergefahren oder neu gestartet werden. Außerdem können die beiden Dienste *Firewall* und *Admin-Webserver* gestoppt und gestartet werden.

Im Statusmodus wechselt die Anzeige des Displays zwischen verschiedenen Informationen. Durch Drücken der Tasten << (links) und >> (rechts) kann durch die verschiedenen Informationen geblättert werden.

Um den interaktiven Modus zu aktivieren, muss die mit *Enter* bezeichnete Taste gedrückt werden. Zwischen den einzelnen Konfigurationsmöglichkeiten kann mit den Tasten << (links) und >> (rechts) gewechselt werden. Im interaktiven Modus ist ein Timeout wirksam; nach einer gewissen Zeitspanne wechselt die Anzeige wieder in den Statusmodus.

Zum Setzen der *IP-Adresse* muss diese mit *OK* ausgewählt werden. Daraufhin wird die aktuelle IP-Adresse angezeigt. Der Cursor steht auf der ersten Ziffer der IP-Adresse. Die Tastenbelegung hat sich geändert und wird jeweils in der unteren Displayzeile angezeigt. Mit + kann diese Stelle hochgezählt und mit − heruntergezählt werden. Mit >> und mit << wird der Cursor bewegt. Nach Eingabe der IP-Adresse wird das Feld nach rechts mit >> verlassen.

Nun wird die aktuelle Netzmaske angezeigt. Diese kann in sinnvollen Schritten vergrößert und verkleinert werden. Nach Eingabe der Netzmaske wird das Feld wieder mit >> verlassen. Nun kann die soeben eingestellte IP-Adresse entweder mittels *OK* aktiviert oder mit *No* verworfen werden. Bei Aktivierung wird zusätzlich die interne Firewall abgeschaltet. Damit ist der Collax Security Gateway nur noch über die Administrationsoberfläche und über SSH unter der eingestellten IP-Adresse erreichbar. Alle anderen Verbindungen (Internet, Ping usw.) werden geblockt. Diese Einstellungen sind bis zum Neustart oder bis zur Aktivierung einer Konfiguration über die Web-Oberfläche aktiv.

Hinweis: Über das Display kann kein Gateway angegeben werden. Die Grundkonfiguration kann daher nur von einem Client aus erfolgen, der sich in dem Netzwerksegment befindet, welches an der Schnittstelle „eth0“ angeschlossen ist.

2.3 Voreinstellungen

Werden bei der Installation der Software bzw. über das Display oder das Konsolen-Werkzeug setip am Server keine Änderungen vorgenommen, ist der Collax Security Gateway auf folgenden Voreinstellungen konfiguriert:

- Netzwerkschnittstelle eth0
- IP-Adresse 192.168.9.9
- Netzmaske 255.255.255.0
- Netzwerk 192.168.9.0
- Default-Gateway 192.168.9.1

3 Administration

3.1 Web-Oberfläche

Die Administration des Collax Security Gateways erfolgt vollständig über eine Web-Oberfläche. Der Zugriff erfolgt immer verschlüsselt über HTTPS. Für die Administration wird ein separater Webserver verwendet, der Anfragen auf Port 8001 entgegennimmt. Die URL zum Zugriff lautet daher: „https://192.168.9.9:8001“. Statt „192.168.9.9“ muss die bei der Installation eingestellte IP-Adresse eingesetzt werden.

Beim ersten Anmelden muss zunächst ein „EULA“ akzeptiert werden, danach werden die Passwörter für die beiden Systemkonten *admin* und *root* gesetzt. Auf der Weboberfläche meldet sich immer *admin* an, *root* wird nur auf der Kommandozeile verwendet. Das Root-Passwort ist dennoch das wichtigste Passwort auf dem System und sollte entsprechend sorgfältig aufbewahrt werden. Bei Verlust dieser beiden Passwörter ist das komplette Zurücksetzen des Collax Security Gateways in den Auslieferungszustand erforderlich.

Werden Passwörter gewählt, sollten diese ebenfalls ein gewisses Maß an Sicherheit bieten. Tabu sollten Passwörter wie „geheim“, „joshua“, der Firmenname oder der Name der Ehefrau sein. Ähnlich schlecht sind Passwörter aus normalen Wörtern, die mit einem Wörterbuchangriff geraten werden können. Ein Passwort sollte eine gute Mischung aus Groß- und Kleinbuchstaben sowie Ziffern aufweisen. Dabei sollte kein sinnvolles Wort in irgendeiner Sprache gebildet werden. Leerzeichen sollten vermieden werden.

Nach dem Anmelden präsentiert sich die Oberfläche mit einem Dashboard, mit welchem die wichtigen Informationen über den Zustand des Produkts eingesehen werden können.

3.1.1 Dashboard

Über das Dashboard wird der Gesamtstatus auf einen Blick dargestellt. In mindestens vier grafischen Gruppierungen zeigt der Collax Security Gateway Auswertungen über die folgenden Informationsbereiche. Klicken Sie auf eines der Felder, um direkt weitere Informationen oder Einstellungen vorzunehmen.

Der Bereich *Überwachung* gibt auf einen Blick Auskunft, ob die Bereiche Dienste und Hardware ordnungsgemäß funktionieren. Ein Ereignis-Log kann per Klick aufgerufen werden, um weitere Details zu erfahren.

Der Abschnitt *USV-Geräte* zeigt an, ob ein oder mehrere Unterbrechungsfreie Stromversorgungsgeräte an einem der Cluster Nodes per USB angeschlossen sind. Die Geräteliste und die Konfiguration mit einer Detailstatus-Seite wird per Mausklick geöffnet.

3.1.2 Stapelverwaltung der Dialoge

In der modern entworfenen Oberfläche werden bestimmte Dialoge innerhalb von Stapeln parallel verwaltet. Diese Stapel werden in der Kopfzeile der Oberfläche angezeigt. Zwischen diesen Stapeln kann mit der Fokussierung per Maus oder mit der Tastenkombination „Shift Tab“ gewechselt werden. Daraus resultiert der Vorteil, dass oft genutzte Dialoge geöffnet bleiben können und sofort in der Administration zur Verfügung stehen.

Die folgenden Dialoge können in separaten Stapeln adressiert werden. Unterdialoge werden innerhalb des einen geöffneten Stapel angezeigt.

- Dashboard, Einstellungen mit genereller Menüstruktur, Infrastruktur, Integriertes Administrationshandbuch, Suchergebnisse, Aktivierungsdialog, Statistiken.

Die Dialogreihe innerhalb eines Stapels wird direkt über einem Dialog angezeigt. Klicken Sie als Beispiel auf *Menü*, *Assistenten*, und dann auf *Benutzer* so wird diese Dialogreihe angezeigt: *Menü – System – Assistenten*
– *Assistent für Benutzer*

3.1.3 Nützliche Tastaturkürzel

- STRG + F1: Administrationshandbuch
- STRG + F9: Einstellungen sofort aktivieren
- STRG + UMSCHALT + F: Suche
- ESC: Dialog schließen

3.2 Erste Schritte

Um den Collax Security Gateway für Ihre Anforderungen einzurichten, empfiehlt es sich, zunächst eine Grundkonfiguration zur Anbindung an das lokale Netz und ans Internet vorzunehmen. Danach können Sie das System registrieren und ggf. auf den aktuellen Softwarestand updaten.

Bei der Konfiguration des Systems werden Sie auf Wunsch durch Assistenten unterstützt, die für bestimmte Konfigurationsaufgaben alle notwendigen Parameter abfragen und dann die entsprechenden Einstellungen vorbereiten. Diese von den Assistenten vorgenommenen Einstellungen können von Ihnen später manuell angepasst werden.

Im Anschluss sollten Sie sich mit dem im Collax Security Gateway genutzten Gruppenmodell zur Steuerung der Zugriffsberechtigungen

vertraut machen. Damit sind Sie in der Lage, jeden Dienst im Collax Security Gateway für einzelne Benutzer bzw. einzelne Computer freizugeben.

Die folgende Liste soll Ihnen helfen, die ersten Schritte vorzunehmen und die jeweils entsprechenden Stellen in der Dokumentation aufzufinden.

3.2.1 Schritt für Schritt: Einrichtung des System

- Benutzen Sie den Assistenten zum Setzen der Stammdaten (S. 27) oder nehmen Sie dies manuell unter *Benutzungsrichtlinien – Umgebung – Standort* vor.
- Unter *Benutzungsrichtlinien – Umgebung – Administrator* können Sie die E-Mail-Adresse eintragen, an die das System Statusinformationen senden kann. Zusätzlich müssen Sie noch den SMTP-Dienst starten.
- Nun müssen Sie den IP-Bereich des lokalen Netzes überprüfen und ggf. anpassen. Danach müssen Sie den Link ins lokale Netz anpassen. Folgen Sie dazu der Schritt-für-Schritt-Anleitung (S. 169). Wenn Sie zum Thema Netzwerk und Links Fragen haben, können Sie zunächst eine Einführung (S. 145) ins Thema lesen.
- Richten Sie nun die Internetverbindung ein. Dazu gibt es verschiedene Möglichkeiten (DSL, ISDN usw.), die alle in einer Anleitung (S. 236) aufgezeigt werden.
- Nun sollten Sie unter *Netzwerk – DNS – Allgemein* den FQDN Ihres Collax Security Gateways setzen. Weiterhin sollten Sie den Nameserver so einrichten, dass Sie Hostnamen im Internet auflösen können. Zu diesem Thema gibt es eine Schritt-für-Schritt-Anleitung (S. 350) und eine Einführung (S. 339).
- Nachdem Sie diese grundlegenden Einstellungen im System

vorgenommen haben, können Sie die Konfiguration „aktivieren“. Folgen Sie dazu den Anweisungen zur Aktivierung (S. 15).

- Wenn Sie die vorhergehenden Punkte bearbeitet haben, können Sie nun mit dem Collax Security Gateway ins Internet. Jetzt ist ein guter Zeitpunkt, um das System zu registrieren. Wechseln Sie dazu auf den seitlichen Reiter *System*, dort auf die Seite *Systembetrieb – Software – Registrierung* und folgen Sie den Anweisungen.

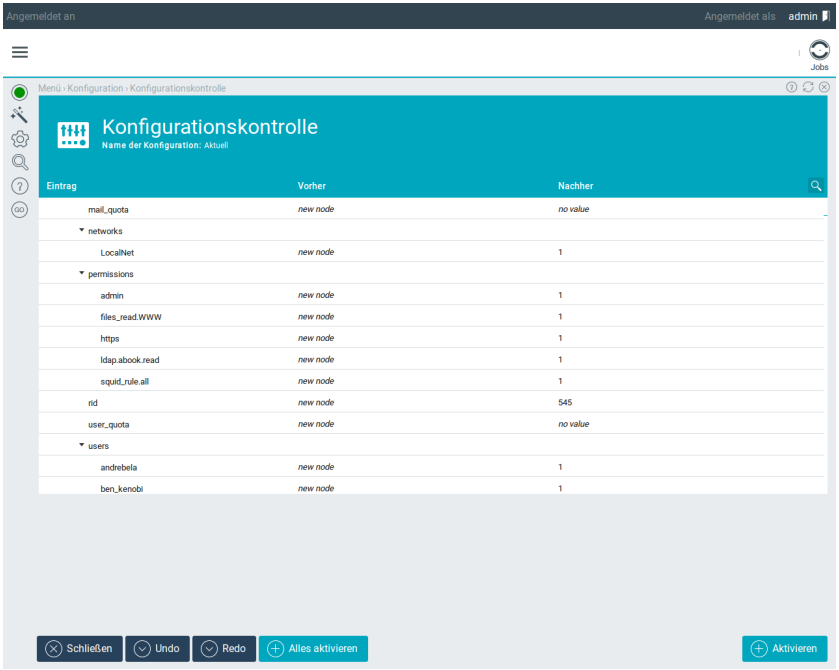
Damit ist die grundlegende Konfiguration des Systems abgeschlossen. Die weiteren Schritte sind nun davon abhängig, wie Sie Ihren Collax Security Gateway einsetzen möchten. Daher folgen hier nur einige Verweise auf häufig genutzte Dienste.

- In jedem Fall ist es sinnvoll, sich mit dem Konzept der Gruppen im Collax Security Gateway zu beschäftigen. Über diese Gruppen werden alle Zugriffe auf Dienste im Collax Security Gateway gesteuert. Zu diesem Thema gibt es eine Einführung (S. 43) und eine Schritt-für-Schritt-Anleitung (S. 48).
- Wenn Sie Dienste mit Verschlüsselung einsetzen möchten, benötigen Sie ein Zertifikat für Ihren Collax Security Gateway. Sinnvoll ist es, in diesem Zusammenhang gleich eine eigene CA anzulegen. Auch hierzu gibt es eine Einführung (S. 105) und eine schrittweise Anleitung (S. 118).

3.3 Konfiguration

Der Collax Security Gateway speichert intern verschiedene Konfigurationsstände. Dazu gehört die aktuell aktive Konfiguration des Systems, dann die aktuell im Webinterface sichtbare Konfiguration und zusätzlich der Konfigurationsstand der vorherigen Konfigurationsaktivierung.

Änderungen in der Weboberfläche werden nicht direkt im System umgesetzt. Vielmehr muss eine Konfiguration explizit „aktiviert“ werden. So ist es möglich, auch eine komplexe Konfiguration über die Weboberfläche zu erstellen und anschließend komplett zu aktivieren.



Im normalen Betrieb sollte die Konfiguration des Systems mit der in der Weboberfläche einsehbaren identisch sein. Sind beide jedoch durch Änderungen innerhalb der Weboberfläche verschieden, wird dies durch ein animiertes Symbol rechts oben in der Weboberfläche signalisiert. Das Anklicken dieses Symbols führt auf die Seite zur *Konfigurationskontrolle*. Hier werden die durchgeführten Änderungen aufgelistet und können aktiviert werden. Einzelne Änderungen können über *Undo* zurückgenommen bzw. durch *Redo* wiederhergestellt werden.

Die aktuell in der Weboberfläche genutzte Konfiguration kann jederzeit unter einem eigenen Namen innerhalb des Systems gespeichert werden.

Einzelne gespeicherte Konfigurationen können über einen Webdownload exportiert werden. Derart gespeicherte Konfigurationen können wiederum importiert werden. Dies stellt eine einfache Möglichkeit zum Sichern der Systemkonfiguration dar. Der Mechanismus kann aber auch genutzt werden, um eine Konfiguration auf einen zweiten Collax Security Gateway zu übertragen.

Diese Konfigurationsdateien beinhalten keinerlei Passwörter. Die Passwörter der beiden Systemkonten *admin* und *root* sind ebenfalls nicht enthalten. Die Benutzerkonten können separat exportiert werden. Eine vollständige Sicherung des Systems ist über die Datensicherung (S. 531) möglich.

3.3.1 Schritt für Schritt: Aktivieren der Konfiguration

- Um eine Konfiguration zu aktivieren, klicken Sie auf das animierte Symbol in der Weboberfläche.
- In den Details unter *Änderungen* sehen Sie, wie viele Änderungen durchgeführt wurden.

- Sie können nun entweder *Änderungen aktivieren* oder eine *Vollständige Konfiguration* ausführen. Normalerweise aktivieren Sie nur die Änderungen. Bei der vollständigen Konfiguration werden alle Konfigurationsdateien neu geschrieben. Dies empfiehlt sich beispielsweise, wenn eine importierte Konfiguration aktiviert werden soll.
- Der Konfigurationsdurchlauf wird durch eine Animation visualisiert. In der Zeile darunter wird angezeigt, welcher Dienst gerade bearbeitet wird. Warten Sie, bis mit *Done* das Ende angezeigt wird.
- Durch Anklicken der Animation wird ein Terminalfenster geöffnet, in dem detaillierte Ausgaben zu sehen sind. Beachten Sie, dass hier auch Meldungen auftauchen, die wie eine Fehlermeldung erscheinen, aber die korrekte Funktion des Systems nicht beeinflussen.
- Sollte die Konfiguration nicht bis *Done* durchlaufen, kann dies daran liegen, dass Sie die IP-Adresse des Systems geändert haben. Dann wird innerhalb des Konfigurationsdurchlaufs die neue IP-Adresse aktiviert. Geben Sie dann in der URL-Zeile Ihres Browsers die neue IP-Adresse ein und verbinden Sie sich erneut mit dem Collax Security Gateway.

3.3.2 Schritt für Schritt: Export und Import

- Wechseln Sie zur *Konfigurationskontrolle*.
- Unter *Speichern als ...* tragen Sie einen Namen für die aktuelle Konfiguration ein. Drücken Sie anschließend den Schalter *Speichern als*.
- Sie gelangen nun auf die Seite *Konfiguration – Konfigurationsdateien*.

- Unter *Eigene Konfigurationen* ist die gerade gespeicherte Konfiguration aufgelistet. Diese kann nun über das Kontextmenü mit *Exportieren* auf den eigenen Rechner gespeichert werden. Dazu öffnet sich der Download-Dialog Ihres Webbrowsers, sofern sie diesen nicht auf automatisches Speichern eingerichtet haben.
- Eine solche Konfigurationsdatei können Sie über den Schalter *Importieren* in die Liste der *Eigenen Konfigurationen* aufnehmen. Durch Anklicken des Schalters öffnet sich ein Dialog, der über *Durchsuchen* einen Dialog zur Dateiauswahl in Ihrem Browser startet. Wählen Sie die gewünschte Datei auf Ihrer Festplatte aus und klicken Sie anschließend *Importieren*.
- Die Konfiguration ist nun nur auf dem Collax Security Gateway gespeichert, aber weder in der Weboberfläche einsehbar noch aktiviert.
- Im Kontextmenü der Konfigurationsdatei können Sie diese durch *Bearbeiten* in die Weboberfläche „laden“.
- Nun können Sie die Konfiguration in der Weboberfläche bearbeiten oder über den gewohnten Mechanismus aktivieren.

3.3.3 GUI-Referenz: *Konfigurationskontrolle*

(Dieser Dialog befindet sich unter *Konfiguration – Konfigurationskontrolle*)

In diesem Dialog wird der Name der geladenen Konfiguration angezeigt. Die aktuell in der Weboberfläche sichtbare Konfiguration kann hier (innerhalb des Collax Security Gateways) gespeichert werden.

3.3.3.1 Abschnitt *In Bearbeitung*

Felder in diesem Abschnitt

- *Name der ursprünglich geladenen Konfiguration*: Hier wird der Name der ursprünglich zur Bearbeitung geladenen Konfiguration angezeigt.
- *Änderungen*: Hier wird die Anzahl der Änderungen in den jeweiligen Bereichen angezeigt. Mit Klicken auf *Details* werden genauere Informationen angezeigt.
- *Auch unveränderte Einstellungen erneut aktivieren*: Mit dieser Option werden alle Einstellungen des Systems, auch unveränderte, aktiviert. Dieser Vorgang kann einige Zeit in Anspruch nehmen.

  Hinweis: Ändert sich bei einer Konfiguration die IP-Adresse des Systems, ist die Konfigurationsoberfläche nicht mehr erreichbar. Es muss dann eine Verbindung zu der neuen IP-Nummer aufgebaut werden.

Aktionen für diesen Dialog

- *Undo*: Diese Aktion macht die Änderungen stufenweise rückgängig. Es werden pro Stufe immer alle Änderungen in einem Dialog zurückgenommen.
- *Redo*: Diese Aktion stellt zurückgenommene Änderungen wieder her.
- *Aktivieren*: Diese Aktion aktiviert die Änderungen, die gerade in der aktuellen Konfiguration vorgenommen wurden.

  Hinweis: Ändert sich bei einer Konfiguration die IP-Adresse des Systems, ist die Konfigurationsoberfläche nicht mehr erreichbar. Es muss dann eine Verbindung zu der neuen IP-Nummer aufgebaut werden.

3.3.3.2 Abschnitt *Speichern als ...*

Die aktuelle Konfiguration kann im System gespeichert werden.

Felder in diesem Abschnitt

- *Name*: Hier wird der Name angegeben, unter dem die Konfiguration gespeichert wird.

Aktionen für diesen Dialog

- *Speichern als ...*: Diese Aktion speichert die Konfiguration.

3.3.3.3 Abschnitt *Aktivierung ...*

Wird die Konfiguration aktiviert, ist in diesem Abschnitt der Fortschritt des Vorgangs sichtbar. Mit einem Klick auf den Fortschrittsbalken wird auf eine detaillierte Ausgabe umgeschaltet. Ein erneuter Klick führt zu dem einfachen Balken zurück.

3.3.3.4 Aktionen für diesen Dialog

- *Zurück*: Mit dieser Aktion gelangen Sie zurück zum Aktivierungsdialog.

3.3.4 GUI-Referenz: *Konfigurationsdateien*

(Dieser Dialog befindet sich unter *Konfiguration – Konfigurationsdateien*)

Dieser Dialog zeigt alle im Collax Security Gateway gesicherten Konfigurationen. Sie können hier exportiert, geladen und gelöscht werden. Zusätzlich ist der Import von Konfigurationen möglich.

3.3.4.1 Abschnitt *Konfigurationen*

Hier werden alle vom System automatisch gespeicherten Konfigurationen aufgelistet. Sie können hier in die Weboberfläche geladen werden.

Spalten in der Tabelle

- *Name*: Der Name der Konfiguration. Dies ist eine intern erzeugte Bezeichnung.
- *Kommentar*: Hier wird ein kurzer Kommentartext mit dem exakten Namen der Konfigurationsdatei angezeigt.
- *Datum*: Hier wird das Datum angezeigt, an dem die Konfiguration gespeichert wurde.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird die gespeicherte Konfiguration geladen. Dabei werden die Konfigurationseinstellungen in die Weboberfläche übernommen, jedoch nicht aktiviert.

3.3.4.2 Abschnitt *Eigene Konfigurationen*

Alle in der *Konfigurationskontrolle* gespeicherten Konfigurationen sind in diesem Dialog aufgelistet. Sie können hier geladen, exportiert oder gelöscht werden.

Spalten in der Tabelle

- *Name*: Der Name der Konfiguration. Dies ist der Name, der beim Speichern der Konfiguration vergeben wurde.
- *Datum*: Hier wird das Datum angezeigt, an dem die Konfiguration gespeichert wurde.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird die gespeicherte Konfiguration geladen. Dabei werden die Konfigurationseinstellungen in die Weboberfläche übernommen, jedoch nicht aktiviert.
- *Exportieren*: Mit dieser Aktion kann die ausgewählte Konfiguration über das Webinterface heruntergeladen und auf dem lokalen Rechner gespeichert werden. Die Konfiguration enthält keine Passwörter, Zertifikate oder Filterlisten.
- *Löschen*: Mit dieser Aktion wird die ausgewählte Konfiguration gelöscht.

3.3.4.3 Aktionen für diesen Dialog

- *Importieren*: Mit dieser Aktion kann eine Konfiguration über die Weboberfläche in das System importiert werden.

3.3.4.4 *Konfiguration importieren*

(Dieser Dialog befindet sich unter *Konfiguration – Konfigurationsdateien*)

Über diesen Dialog kann eine Konfigurationsdatei vom lokalen Rechner in das System importiert werden.

Felder in diesem Dialog

- *Datei*: Über dieses Feld wird auf dem lokalen System ein Dialog geöffnet, über den die Datei auf dem lokalen Rechner ausgewählt werden kann.
- *Ergebnis*: Bei gestartetem Import wird hier die Ausgabe des Vorgangs angezeigt.

Aktionen für diesen Dialog

- *Importieren*: Mit dieser Aktion wird der Import gestartet. Diese Konfiguration wird unter dem Namen *conf_upload* mit angehängtem Datum und Uhrzeit abgespeichert. Um die Konfiguration zu übernehmen, muss sie mit *Bearbeiten* in die Weboberfläche geladen und dann aktiviert werden.

3.3.5 Schritt für Schritt: Export von Benutzerdaten

- Unter *Überwachung/Auswertung – Auswertungen – Export von Benutzerdaten* können die aktuell angelegten Benutzer exportiert werden.
- Um die Liste weiter verarbeiten zu können, bietet sich das CSV-Format an. Dabei handelt es sich um eine Textdatei; jeder

Benutzer ist in einer Zeile erfasst, die Werte sind mit Komma getrennt.

- Wählen Sie als Format *CSV-Datei* und klicken Sie auf *Exportieren*. Der Download-Dialog Ihres Browsers öffnet sich, und Sie können die Datei auf Ihrem Rechner speichern.
- Sie können diese Datei mit einem Texteditor bearbeiten oder in eine Tabellenkalkulation oder Datenbank importieren.
- Sie können in diesem Format eine Benutzerliste vorbereiten und unter *Benutzungsrichtlinien – Benutzer – Benutzer importieren* importieren.

3.3.6 GUI-Referenz: Benutzerdaten exportieren

3.3.6.1 *Export von Benutzerdaten*

Über diesen Dialog kann eine PDF- oder CSV-Datei mit den Daten der Benutzer erstellt werden. In dem erstellten PDF-Dokument stehen der FQDN dieses Systems sowie Login und Passwort der ausgewählten Benutzer. Für jeden Benutzer wird dabei eine eigene Seite erstellt, die ihm ausgehändigt werden kann. Die CSV-Datei wird als reine Textdatei erstellt und enthält Login, Titel, Vorname, Nachname, Passwort und Telefonnummer. Sie dient hauptsächlich zum vereinfachten Import von Benutzerprofilen in andere Systeme.

3.3.6.2 Felder in diesem Dialog

- *Exportiere Benutzerdaten in eine*: Über dieses Feld wird ausgewählt, ob eine PDF- oder CSV-Datei mit den Daten der Benutzer erstellt wird.
- *Sprache des PDF*: Das PDF kann wahlweise in Deutsch oder Englisch erstellt werden.

- *Alle Benutzer oder einzelne auswählen?*: Hier wird festgelegt, ob die Daten aller lokal auf dem System angelegten Benutzer oder nur die Daten ausgewählter Benutzer exportiert werden.
- *Benutzer auswählen*: Hier muss mindestens ein Benutzer ausgewählt werden, dessen Daten in ein PDF exportiert werden.

3.3.6.3 Aktionen für diesen Dialog

- *Exportieren*: Mit dieser Aktion wird der Export der Benutzerdaten gestartet.

3.3.7 GUI-Referenz: Benutzer importieren

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Benutzer – Benutzer importieren*)

In diesem Dialog kann eine Datei im CSV-Format mit Benutzerdaten importiert werden. Über diese Funktion und den vorhergehenden Export von Benutzerdaten auf einem anderen System können Benutzer mit ihren Passwörtern auf ein zweites System übernommen werden (S. 68).

Die Datei muss pro Zeile einen Benutzer enthalten; die einzelnen Felder werden durch Komma getrennt. Es werden der Reihe nach folgende Werte erwartet: Login, Titel, Vorname, Nachname, Passwort und Telefonnummer. Weitere Einstellungen wie Mail-Aliase oder Fax-Nummer müssen über die Oberfläche des Collax Security Gateways vorgenommen werden.

3.4 Assistenten

Die grundlegende Konfiguration des Collax Security Gateways kann mit Hilfe von Assistenten durchgeführt werden. Die Assistenten sind in die Weboberfläche integrierte Dialoge, die für bestimmte Aufgaben die notwendigen Parameter erfragen, diese mit weiteren sinnvollen Annahmen bzw. Vorgabewerten kombinieren und Konfigurationseinstellungen vornehmen.

Alle von den Assistenten durchgeführten Konfigurationen sind in der normalen Administrationsoberfläche sichtbar und als solche erkennbar. Neu angelegte Objekte sind immer im Kommentarfeld als „Generated by Wizard“ bezeichnet. Die am System durchgeführten Einstellungen sind damit im Nachhinein nachvollziehbar und können durch den Administrator geändert werden.

In den folgenden Abschnitten werden die einzelnen Assistenten vorgestellt. Im Abschnitt „Ablauf“ ist jeweils skizziert, welche Fragen der Assistent stellt und welche Informationen er erwartet. Der Abschnitt „Konfiguration“ ist technisch anspruchsvoller und erläutert, welche Konfigurationsänderungen der Assistent im Einzelnen durchführt. Mit diesen Informationen ist es möglich, die Änderungen am Collax Security Gateway durch einen Assistenten nachzuvollziehen und anzupassen.

Da manche Assistenten teilweise Konfigurationen löschen bzw. bei mehrfachem Aufruf manuelle Anpassungen teilweise verwerfen, sollte nur die erste Installation des Systems über die Assistenten durchgeführt werden. Danach sollten die Assistenten mit einiger Vorsicht genutzt werden, insbesondere wenn parallel eine manuelle Konfiguration des Systems erfolgt.

3.4.1 *Bare Metal Restore*

(Dieser Dialog befindet sich unter *Assistenten – Bare Metal Restore*)

Benutzen Sie diesen Assistenten, um schnellstmöglich Ihren Server nach einem vollständigen Systemcrash wieder in Betrieb zu nehmen (Bare Metal Restore, Desaster-Recovery).

3.4.1.1 Ablauf und Konfiguration

Im ersten Schritt wird eine Recovery Token-Datei (recovery-token_host_datum.rto) gewählt, welche der Administrator per E-Mail erhielt.

Im nächsten Schritt werden folgende Aktionen automatisch ausgeführt:

- Überprüfung des Recovery Token
- Installation der Lizenz
- Installation der lizenzierten Zusatzmodule
- Einrichtung des Sicherungsziels und des Sicherungssystems
- Wiederherstellung des Inhaltsverzeichnisses (Katalog) aller Sicherungsdaten

Im letzten Schritte werden Informationen zur weiteren Vorgehensweise angezeigt. Es sind alle Einstellungen vorhanden, um auf alle gesicherten Daten zuzugreifen und diese wieder herzustellen.

Es ist zu beachten, dass während einer vollständigen Datenwiederherstellung in das laufende System keine manuellen Interaktionen mit dem System oder einzelnen Diensten getätigt werden sollen.

3.4.2 *Assistent für die Stammdaten*

(Dieser Dialog befindet sich unter *Assistenten – Stammdaten*)

Dieser Assistent fragt wichtige Daten über den Standort des Unternehmens ab. Diese Daten sind für die Registrierung und Aktivierung der Lizenz sowie später bei der Erstellung von Zertifikaten notwendig.

3.4.2.1 Ablauf

Dieser Assistent fragt die Adresse des Unternehmens ab. Bei mehreren Collax Security Gateway innerhalb eines Unternehmens sollte die Abteilung bzw. der Standort passend zu jedem System gesetzt werden.

Weiterhin erfragt der Assistent die Einstellungen für das Telefonsystem wie Landesvorwahl, Ortsnetz und Amtsholung.

3.4.2.2 Konfiguration

Die übergebenen Werte werden nach *Benutzungsrichtlinien – Umgebung – Standort* übernommen und können dort jederzeit angepasst werden.

3.4.3 *Registrierung des Servers*

(Dieser Dialog befindet sich unter *Assistenten – Registrierung*)

Mit Hilfe dieses Assistenten wird der Collax Security Gateway registriert. Dieser Assistent zeigt die beim Hersteller hinterlegten Daten des Kunden an. Falls Kundendaten nicht vorhanden sind, werden diese vom Assistenten abgefragt.

3.4.3.1 Ablauf

Im ersten Schritt wird die Erreichbarkeit des Collax Lizenzierungs-Servers getestet. Anschließend kann die erhaltene Lizenznummer eingegeben werden.

Falls Daten des Kunden vorhanden sind, werden diese nachfolgend zur Überprüfung angezeigt. Gegebenenfalls ist eine E-Mail-Adresse anzugeben. Wenn keine Daten vorhanden sind, kann die Registrierung mit einem Collax Web Account-Login oder mit der Eingabe von Kundendaten erfolgen. Im Anschluss werden die Daten zur Kontrolle angezeigt.

Über den Administrations-Newsletter können wichtige Informationen über Produkt-Updates, neue Funktionen oder Sicherheitsinformationen empfangen werden.

Der Server wird nach der Zusammenfassung registriert. Durch die Registrierung kann die Software-Update-Funktionen des Servers und der registrierten Software-Module für die Dauer der Laufzeit genutzt werden. Detailinformationen über die Lizenz können über das Collax Web Account unter http://www.collax.com abgerufen werden.

3.4.4 *Assistent für die Einrichtung des Intranets*

(Dieser Dialog befindet sich unter *Assistenten – Intranet*)

Mit Hilfe dieses Assistenten wird das lokale Netzwerk eingerichtet. Zudem wird die Konfiguration als DNS- oder DHCP-Server abgefragt. Für den Collax Security Gateway wird ein Serverzertifikat erzeugt, welches von einer eigenen CA signiert wird.

3.4.4.1 Ablauf

Dieser Assistent fragt den Hostnamen des Collax Security Gateways ab. Dabei soll der FQDN übergeben werden, also der vollständige Name inkl. der Domain.

Anschließend wird die IP-Adresse mit zugehöriger Netzmaske abgefragt, die der Collax Security Gateway auf der ersten Netzwerkschnittstelle (*eth0*) verwenden soll.

Der Assistent fragt ab, ob für diese Netzwerkkarte der DHCP-Dienst aktiviert werden soll. Falls ja, fragt er die erste und letzte IP-Adresse für den Pool ab. Aus diesem Adresspool werden die IP-Adressen für die Zuweisung per DHCP genommen. Diese IP-Adressen sollten nicht anderweitig genutzt werden.

Für die Erstellung einer Zertifikatshierarchie wird ein CA-Zertifikat erstellt. Dieses wird mit der hier abgefragten Passphrase geschützt.

3.4.4.2 Konfiguration

Zunächst wird überprüft, ob die angegebene IP-Adresse für die Schnittstelle *eth0* zu einem vorhandenen Netzwerk gehört. Falls nicht, wird ein neues Netz *LocalNet* angelegt. Existiert bereits ein Netzwerk dieses Namens, wird dem neu angelegten Netz eine fortlaufende Nummer angehängt.

Nun wird überprüft, ob es bereits einen Ethernet-Link gibt, der die angegebene IP-Adresse besitzt. Falls nicht, wird ein neuer Link angelegt. Dieser Link wird auf die höchste Priorität gesetzt, falls bereits Links mit dem gleichen erreichbaren Netz existieren.

Im Anschluss wird eine Gruppe *LocalNetworks* angelegt. Das angelegte lokale Netz wird als Mitglied aufgenommen, und die Berechtigungen für *DNS* (inkl. *rekursiver Anfragen*), *Webadmin* und *SSH-Connect* werden aktiviert.

Der Nameserver wird aktiviert, die (Sub-)Domain aus dem FQDN des Systems selbst wird in die Domainsuchliste aufgenommen. Das Weiterleiten von DNS-Anfragen wird deaktiviert, der Collax Security Gateway befragt die Root-Nameserver.

Für die (Sub-)Domain aus dem FQDN des Collax Security Gateways wird im DNS eine Vorwärtszone angelegt, zu der der Collax Security Gateway *Master* ist.

Für das angelegte lokale Netzwerk wird im DNS eine Rückwärtszone erzeugt. Auch hier ist der Collax Security Gateway *Master*.

Aus den Daten des *Standort* wird ein zehn Jahre gültiges CA-Zertifikat erzeugt. Das CA-Zertifikat wird mit der Passphrase gesichert.

Ein weiteres Zertifikat wird zur Verwendung durch die Serverdienste im Collax Security Gateway erstellt. Dieses ist von der CA signiert und ebenfalls zehn Jahre gültig.

Abschließend werden die Konfigurationsänderungen aktiviert. Wurde für das lokale Netz die IP-Adresse geändert, ist der Collax Security Gateway nicht mehr unter der alten IP-Adresse erreichbar.

3.4.5 *Assistent für den Internetzugang*

(Dieser Dialog befindet sich unter *Assistenten – Internetzugang*)

Dieser Assistent übernimmt die Einrichtung einer Internetverbindung. Er fragt ab, ob der Zugang über Router, DSL oder ISDN erfolgen soll, und nimmt eine Minimalkonfiguration der Firewall vor.

3.4.5.1 Ablauf

Zunächst wird ein Name für die Verbindung abgefragt. Der Vorschlag des Assistenten dafür lautet „InternetLink“.

Ist ein Link dieses Namens bereits vorhanden, fragt der Assistent, ob dieser Link überschrieben werden soll. Andernfalls muss ein anderer Name gewählt werden.

Danach wird die Verbindungsart abgefragt. Hier stehen die Möglichkeiten „Router“, „DSL“ und „ISDN“ zur Auswahl.

Abhängig von dieser Auswahl stellt der Assistent weitere Fragen. Bei der Auswahl „Router“ wird die IP-Adresse des Routers, die Netzwerkkarte zur Verbindung mit dem Router und die eigene IP-Adresse mit Netzmaske für den Collax Security Gateway auf dieser Schnittstelle abgefragt. Soll der Collax Security Gateway eine IP-Adresse per DHCP vom Router beziehen, muss das Feld für die eigene IP-Adresse leer bleiben.

In der Einstellung „DSL“ folgt die Abfrage, welches der beiden Protokolle „PPPoE“ oder „PPTP“ genutzt wird. Danach wird die Netzwerkkarte abgefragt, an der das DSL-Modem angeschlossen ist, bei PPTP erfolgt noch die Abfrage der IP-Adresse des Modems, und für beide Verfahren müssen Benutzername und Passwort angegeben werden.

Bei Auswahl von „ISDN“ werden das Protokoll, die Anschlussart und die eigene MSN (Rufnummer) des ISDN-Anschlusses abgefragt. Anschließend fragt der Assistent, ob Kanalbündelung oder Amtsholung aktiviert werden sollen. Nach Angabe der Rufnummer des Providers sowie der Benutzerkennung und des Passworts sind die Angaben zu ISDN vollständig.

Zur Konfiguration der Firewall können mehrere Dienstgruppen ausgewählt werden, die jeweils verschiedene Dienste zusammenfassen:

- „Terminalserver“ umfasst die Dienste RDP, VNC, PC-Anywhere, Citrix und X11.
- „Chat“ beinhaltet MSN, AIM, ICQ, IRC, Jabber-client und talk.
- HTTP, HTTPS und FTP gehören zu „Web-Dienste“.
- „Online-Banking“ ist mit HBCI möglich.
- „Mail“ beinhaltet SMTP, POP3, POP3S, IMAP sowie IMAPS.

- „VPN“ umfasst IPsec und PPTP.
- „Login-Dienste“ sind SSH und Telnet.

3.4.5.2 Konfiguration

Abhängig von der Einstellung der Verbindungsart werden die folgenden Konfigurationen vorgenommen:

Bei Verwendung eines Routers wird geprüft, ob die IP-Adresse des Routers zu einem vorhandenen Netzwerk gehört. Ist dies nicht der Fall, wird ein neues Netz *RouterNet* angelegt. Danach wird geprüft, ob es bereits einen Link gibt, auf dem dieses Netz erreichbar ist. Ist dies nicht der Fall, wird ein neuer *RouterNetLink* angelegt. Im Anschluss wird der Link für die Internetverbindung (dessen Name frei gewählt wurde) auf *Route* umgestellt und der Router als *Gateway* eingetragen.

Bei einer DSL-Konfiguration werden der Link für die Internetverbindung auf *DSL mit PPPoE* bzw. *DSL mit PPTP* eingestellt, die passende *Schnittstelle* und *MTU* gesetzt sowie die Zugangsdaten eingetragen.

Bei ISDN wird zunächst geprüft, ob eine Hardwarekonfiguration für ISDN vorliegt. Diese wird nicht modifiziert, ggf. nur neu angelegt. Danach wird überprüft, ob die angegebene MSN bereits angelegt ist. Gegebenenfalls wird diese neu angelegt und auf die ISDN-Karte gebunden. Nun wird der Link für die Internetverbindung mit den Zugangsdaten und der Rufnummer des Providers eingerichtet.

Zum Aufbau der Firewallregeln werden zunächst alle gesetzten Regeln für jedes Netzwerk (außer dem Internet) ins Internet gelöscht. Dann werden abhängig von den aktivierten Dienstegruppen die einzelnen Protokolle von allen angelegten Netzen (außer dem Internet) ins Internet und ins Netzwerk selbst erlaubt. Für jede gesetzte Regel wird die Protokollierung im Logfile aktiviert.

Abschließend werden die Änderungen der Konfiguration aktiviert.

3.4.6 *Assistent für Benutzer*

(Dieser Dialog befindet sich unter *Assistenten – Benutzer*)

Mit diesem Assistenten können einzelne Benutzer angelegt werden. Alternativ kann eine vorbereitete Datei im CSV-Format importiert werden, in der die Benutzer in Listenform hinterlegt sind.

3.4.6.1 Ablauf

Der Assistent fragt zunächst ab, ob ein einzelner Benutzer angelegt werden soll oder eine Liste im CSV-Format importiert werden soll.

Bei einem einzelnen Benutzer werden Vorname, Nachname und Login abgefragt. Der Assistent prüft, ob das Login bereits vergeben ist. In diesem Fall muss ein anderes Login gewählt werden. Danach wird das Kennwort für den Benutzer abgefragt, zu dem der Assistent einen Vorschlag liefert, der übernommen werden kann.

Beim Import der Liste muss eine Datei im CSV-Format ausgewählt und über einen Web-Upload auf den Collax Security Gateway transferiert werden.

3.4.6.2 Konfiguration

Der Benutzer wird neu angelegt und der Gruppe *Users* hinzugefügt.

Abschließend werden die Änderungen der Konfiguration aktiviert.

3.4.7 *Assistent für den Mailproxy*

(Dieser Dialog befindet sich unter *Assistenten – Mailproxy*)

Dieser Assistent übernimmt die Grundkonfiguration des Collax Security Gateways zum Einsatz als Mailproxy. Er konfiguriert und startet den Serverdienst für E-Mail (SMTP). Dabei wird alle E-Mail an einen weiteren Mailserver per SMTP weitergeleitet. Auf diesem Mailserver können die Postfächer selbst verwaltet werden.

3.4.7.1 Ablauf

Der Assistent fragt zunächst ab, wie E-Mail zu dem Collax Security Gateway gelangt. Entweder nimmt ein Provider die E-Mail an, und sie muss vom Collax Security Gateway von dort abgeholt werden, oder der Collax Security Gateway nimmt die E-Mail selbst per SMTP direkt aus dem Internet an. Dazu muss im DNS der Domain der Collax Security Gateway als MX (Mail-Exchanger) eingetragen sein.

Nun muss der Zielserver angegeben werden. Dabei stehen die Optionen *intern verwaltet* und *extern verwaltet* zur Auswahl. Dies bezieht sich nicht auf die IP-Adresse des Zielsystems, sondern auf den Urspung der E-Mail. Bei *intern verwaltet* werden für die Maildomain auch aus fremden Netzen E-Mails angenommen (Mail-Relay); bei *extern verwaltet* werden nur lokal erzeugte E-Mails bzw. E-Mails von Systemen angenommen, die über die *Berechtigungen* die Berechtigung *Mailrelay ohne Authentifizierung* besitzen.

Als nächstes fragt der Assistent die Maildomain ab.

Im nächsten Schritt können die Netze ausgewählt werden, die den SMTP-Dienst nutzen dürfen.

Ausgehende E-Mail kann entweder direkt ausgeliefert werden, oder sie wird gesammelt zu einem Relay-Server (meist beim Provider)

geschickt. Wird ein Relay-Server genutzt, fragt der Assistent dessen Namen bzw. IP-Adresse und optionale Zugangsdaten ab.

3.4.7.2 Konfiguration

Der Assistent aktiviert den SMTP-Dienst und setzt dort die Maildomain auf die eingegebene Domain. Die maximale Größe einer E-Mail wird auf 10 MB begrenzt. Je nach Einstellung wird der Versand über einen Relay-Host konfiguriert. Existiert ein geeignetes Zertifkat für den Collax Security Gateway, wird die Verschlüsselung über TLS aktiviert, wenn die jeweilige Gegenstelle dies unterstützt.

Zu der angegebenen Domain wird eine Maildomain vom eingestellten Typ der Weiterleitung (intern oder extern) angelegt.

Der Assistent legt eine entsprechende Gruppe für die angegebene Domain an. Es werden keine Quotas gesetzt. Die Gruppe erhält die Berechtigungen für den Dienst SMTP sowie *Mail-Relay ohne Authentifizierung* für die angegebene Maildomain. Als Mitglieder werden die ausgewählten Netzwerke aufgenommen.

Soll der Collax Security Gateway E-Mails direkt per SMTP aus dem Internet annehmen, wird geprüft, ob die Gruppe *Internet* vorhanden ist. Ist dies nicht der Fall, werden die Gruppe angelegt, das Netzwerk *Internet* als Mitglied aufgenommen und die Zugriffsberechtigung auf den SMTP-Dienst gewährt.

Abschließend werden die Änderungen der Konfiguration aktiviert.

3.4.8 *Assistent für den Webproxy*

(Dieser Dialog befindet sich unter *Assistenten – Webproxy*)

Mit einem Webproxy lässt sich neben dem ursprünglichen Zweck des schnelleren Surfens eine zusätzliche Sicherheitsbarriere installieren. Diese Barriere lässt nur HTTP-Traffic passieren und kann zudem die übertragenen Daten auf Viren filtern. Dieser Assistent übernimmt die Grundeinstellung des Proxyservers.

3.4.8.1 Ablauf

Der Assistent erfragt zunächst, aus welchen der bereits angelegten Netzwerke der Webproxy zugänglich sein soll.

Anschließend kann noch angegeben werden, ob eine Authentifizierung der Benutzer notwendig ist oder nicht.

3.4.8.2 Konfiguration

Wenn die Benutzerauthentifizierung gewählt wurde, wird geprüft, ob eine Gruppe „WebProxyUsers“ existiert. Diese wird ggf. neu angelegt. Die ausgewählten Netzwerke sowie alle aktuell existierenden Benutzer werden der Gruppe als Mitglied hinzugefügt. In den *Berechtigungen* wird *Regel ‚All‘ anwenden* aktiviert. Alle Proxy-Berechtigungen werden in der Gruppe „LocalNetworks“ entfernt.

Soll der Webproxy ohne Authentifizierung arbeiten, wird geprüft, ob die Gruppe „LocalNetworks“ existiert. Ist dies nicht der Fall, wird die Gruppe neu angelegt. In den *Berechtigungen* werden *Keine Authentifizierung erforderlich* und *Regel ‚All‘ anwenden* aktiviert. Zusätzlich werden die Rechte für *DNS-Connect* und *Webadmin* aktiviert.

Alle Proxy-Berechtigungen werden in der Gruppe „WebProxyUsers“ entfernt.

In der Firewallmatrix werden alle Regeln zum Dienst HTTP für das Zielnetz *Internet* entfernt. Bei aktivierter Authentifizierung wird die Regel „Drop/Verwerfen“ gesetzt. Ohne Authentifizierungszwang wird die Regel „Transparenter Proxy“ gesetzt.

Der Webproxy „Squid“ wird aktiviert, die Adresse „admin@localhost“ wird als Kontaktadresse für Proxy-Meldungen eingetragen, und die Proxy-Größe auf der Festplatte wird auf 1 GB begrenzt. Zur Handhabung von verschlüsselten SSL-Verbindungen wird Port 8001 zu den *SSL-Ports* hinzugefügt.

Abschließend werden die Änderungen der Konfiguration aktiviert.

3.4.9 *Assistent für VPN*

(Dieser Dialog befindet sich unter *Assistenten – VPN*)

Dieser Assistent hilft bei der Einrichtung von VPN-Verbindungen. Er legt dabei notwendige IP-Netze und Zertifikate an.

3.4.9.1 Ablauf

Der Assistent fragt zunächst ab, zu welcher Gegenstelle ein Tunnel aufgebaut werden soll. Je nach Wahl wird die entsprechende Konfiguration für die Gegenstellen am Ende des Assistenten erstellt und kann auf diesen importiert werden.

Im folgenden Dialog wird abgefragt, ob der Collax Security Gateway den Tunnel selbst aufbauen soll (*bei Bedarf* oder *immer*) oder ob er als Einwahlserver genutzt wird. Wurde zuerst ein VPN-Client als Gegenstelle ausgewählt, wird der Collax Security Gateway auto-

matisch als Einwahlserver konfiguriert. Dieser Verbindung wird im nächsten Schritt ein Name zugeordnet.

Nun muss der Name oder die IP-Adresse des Collax Security Gateways eingegeben werden, die für VPN genutzt wird. Über diese Zuordnung wird intern festgelegt, auf welcher Schnittstelle IPsec aktiviert wird.

Alle angelegten Netze werden angezeigt; aus ihnen müssen die lokalen Netze ausgewählt werden, also diejenigen, die auf der Tunnelseite des Collax Security Gateways für die Gegenstelle erreichbar sein sollen.

Im nächsten Schritt werden analog die gegenüberliegenden Netze ausgewählt. In dieser Maske gibt es noch die Möglichkeit, weitere Netze anzulegen.

Bei einem VPN-Client als Gegenstelle wird danach die virtuelle IP-Adresse gesetzt.

Zum Erstellen von Zertifikaten für VPN wird eine CA benötigt. Diese kann ausgewählt werden (falls vorhanden) oder komplett neu erzeugt werden.

Mit dieser CA wird ein Zertifikat für den Collax Security Gateway erstellt. Wurde bereits vorab ein Zerifikat angelegt, kann dieses aus der Liste ausgewählt werden.

Analog wird ein Zertifikat für die Gegenseite erstellt. Dieses kann am Ende des Assistenten zusammen mit der Konfiguration für die Gegenstelle heruntergeladen werden. Es ist auch möglich, die Zertifikate später unter *Benutzungsrichtlinien – X.509-Zertifikate* zu exportieren.

Zuletzt muss noch der Name oder die IP-Adresse der Gegenstelle angegeben werden, falls zu Beginn nicht die Konfiguration als Einwahlserver gewählt wurde.

3.4.10 *Datensicherung*

3.4.10.1 Felder in diesem Formular

- : Wählen Sie aus, ob Sicherungspläne für lokale Sicherungen erstellt werden sollen, oder ob Medien für eine Virtual Tape Library mit USB oder eSATA-Laufwerken eingerichtet werden soll.

3.4.11 *Assistent für Datensicherung*

(Dieser Dialog befindet sich unter *Assistenten – Datensicherung*)

Mit Hilfe dieses Assistenten richten Sie Sicherungspläne für Datensicherungen ein. Diese Sicherungspläne sind gleichermaßen für Sicherungen Ihres Collax Servers wie für Client-Rechner gültig und notwendig. Im Allgemeinen genügen diese generierten Sicherungspläne auch fortgeschrittenen Anwendungsfällen. Detaillierte, manuelle Modifikationen dieser Pläne sind möglich.

3.4.11.1 Ablauf

Im ersten Schritt wird die Periode für Vollsicherungen festgelegt. Es kann zwischen monatlicher, wöchentlicher oder täglicher Vollsicherung gewählt werden. Ergänzende Inkrementelle Sicherungen werden zu einem späteren Zeitpunkt konfiguriert.

Danach wählen Sie genauere Spezifikationen Ihrer Sicherungszeitpunkte.

Im dritten Schritt fragt der Assistent nach der Backup-Strategie.

Hierbei kann zwischen „Lineare Sicherung“, „Einfache Rotation“ und, abhängig von der Wahl der Periode, zwischen „Türme von Hanoi“ und „Großvater, Vater, Sohn“ gewählt werden.

Bei „Linearer Sicherung“ wird fortlaufend auf das jeweilige Ziel gesichert; neue Medien werden angelegt beziehungsweise angefordert, sobald das letzte Medium voll ist.

Bei „Einfacher Rotation“ werden Medien zyklisch für Sicherungen benutzt; die Zyklusdauer richtet sich nach der Periode für Vollsicherungen.

Ziel des Schemas „Türme von Hanoi“ ist es, so lange wie möglich auf alte Sicherungsdaten zurückgreifen zu können, ohne dabei zu viel Platz zu verbrauchen. Es ist aber zu beachten, dass der Platzbedarf dieses Schemas höher ist als der der anderen Schemata.

Das Schema „Großvater, Vater, Sohn“ hält drei Generationen von Sicherungen vor. Dabei wird monatlich eine Sicherung auf gesonderte Medien geschrieben, wöchentlich auf einen zweiten Satz, und täglich auf die Standardmedien. Viele Administratoren sichern die Vater- und Sohn-Generationen als differenzielle beziehungsweise inkrementelle Sicherungen. Diese Veränderung kann leicht im generierten Plan vorgenommen werden.

Bestimmen Sie im vierten Schritt, wie lange gesicherte Daten aufbewahrt werden sollen. Gemeinsam mit der Datenmenge ergibt sich daraus die benötigte Anzahl an Bändern bzw. der Gesamtplatzbedarf der Sicherung.

Im letzten Schritt wird eine Zusammenfassung der im Assistenten vorgenommenen Einstellungen angezeigt. Der Sicherungsplan wird mit einem Klick auf „Fertigstellen“ erstellt.

3.4.11.2 Konfiguration

Der Assistent erstellt einen Sicherungsplan, für den automatisch ein Name, der auf den konfigurierten Eigenschaften basiert, gewählt wird.

Weiterhin wird eine Zuordnung erstellt, die den neuen Plan mit dem lokalen Default-Ziel und dem lokalen System verbindet. Dies gescheit nur, wenn das Default-Ziel existiert und in der vorangegangenen Maske die Checkbox „Benutze diesen Sicherungsplan für eine lokale Sicherung“ aktiviert wurde.

Danach wird die Konfiguration aktiviert.

3.4.12 *Assistent für Virtual Tape Libraries mit Wechselmedien*

3.4.12.1 Felder in diesem Formular

- : Mit Hilfe dieses Assistenten richten Sie Virtuelle Bandwechsler auf Wechselmedien wie USB- oder eSATA-Platten ein.

4 Benutzungsrichtlinien

4.1 Einführung

Über die Benutzungsrichtlinien wird der Zugriff auf die einzelnen Dienste im Collax Security Gateway gesteuert. Dahinter verbirgt sich ein ausgefeiltes Konzept mit mehrstufiger Sicherheit. Die Benutzungsrichtlinien bilden somit ein zentrales Element in der Konfiguration des Systems.

Grundlage der Richtlinien sind „Gruppen“ und „Netzwerkgruppen“. Jede dieser Gruppenarten beinhaltet „Mitglieder“ und gewährt diesen „Berechtigungen“. Mitglieder einer Gruppe sind Benutzer, Mitglieder einer Netzwerkgruppe sind „Hosts“ oder auch ganze Netze. Die Berechtigungen sind in weiten Grenzen einstellbar.

Ein Benutzer identifiziert sich gegenüber dem Collax Security Gateway durch Angabe eines Logins mit zugehörigem Passwort. Ein Computersystem benutzt im Netzwerk eine IP-Adresse (mehr dazu im Abschnitt Netzwerke (S. 145)). Diese IP-Adresse sieht der Collax Security Gateway als Identifikation, wenn er Pakete von dem Computer empfängt. In einem lokalen Netz werden IP-Adressen aus einem zusammenhängenden Bereich vergeben, dieser Bereich wird als „Netz“ oder „Netzwerk“ bezeichnet.

Die Unterscheidung dieser Arten von Mitgliedern (Computersystemen, Netzwerke und menschlichen Benutzern) durch separate Gruppierung bietet eine transparente Darstellung, um den Zugriff auf Dienste zu konfigurieren.

Bei einfachen Diensten, wie beispielsweise dem Nameserver, wird die Zugriffskontrolle nur anhand der anfragenden IP-Adresse durchgeführt. Üblicherweise wird der Zugriff auf lokale Dienste nur für

interne Netze und aus Sicherheitsgründen nicht aus dem Internet gestattet. In diesem Fall muss die IP-Adresse eines Computers, dem der Zugriff auf den Nameserver gestattet werden soll, Mitglied der Netzwerkgruppe sein. Dazu kann entweder der Computer als einzelner Host oder das Netzwerk, zu dem seine IP-Adresse gehört, als Mitglied in die Gruppe aufgenommen werden.

Bei komplexeren Diensten, wie dem Abruf von E-Mail über POP3 oder IMAP, ist neben dem Netzwerkzugang zusätzlich eine Benutzerauthentifizierung erforderlich. Über dieses Login kann der Serverdienst das richtige Postfach öffnen. Über das Passwort kann er sicherstellen, dass nur berechtigte Benutzer Zugriff auf die E-Mail erhalten. Die Mitgliedschaft der IP-Adresse wird auch hier geprüft. Kommt der Zugriff aus einem unberechtigten Netzwerkbereich, wird der Zugriff in der Firewall geblockt und nicht zum E-Mail-Dienst durchgelassen.

Bei manchen Diensten ist die Authentifizierung optional möglich. Wenn beim Webproxy keine Benutzer angegeben werden, ist der Webproxy von allen Computern aus nutzbar, deren IP-Adresse bzw. deren Netzwerk Mitglied der entsprechenden Netzwerkgruppe ist.

Andere Dienste erfordern nur die Mitgliedschaft eines Benutzers, nicht jedoch eines Computers. Bei Zugriff auf ein Verzeichnis wird beispielsweise nur Login und Passwort abgefragt.

Durch die Einstellungen in den Netzwerkgruppen wird immer eine Firewall-Konfiguration vorgenommen, die bestimmte IP-Adressen zulässt und andere sperrt. Im Fall des E-Mail-Beispiels ist es daher nicht ausreichend, lediglich eine Benutzergruppe aufzunehmen. In diesem Fall würde die Firewall den Zugriff des Rechners abblocken, so dass keinerlei Kommunikation zwischen E-Mail-Client und Mail-Dienst im Collax Security Gateway zustande kommt.

Je nach Einstellung protokolliert die Firewall erfolgreiche und fehlgeschlagene Zugriffe in der Logdatei. Dies kann bei fehlschlagen-

den Zugriffen auf Dienste, die im Collax Security Gateway selbst laufen, dazu verleiten, in der Firewallmatrix (S. 305) Berechtigungen zu setzen. Dies wäre jedoch falsch. Für Zugriffe auf Dienste im Collax Security Gateway sind immer die Rechte in den *Benutzungsrichtlinien* ausschlaggebend.

Eine Mitgliedschaft von Benutzern in mehreren Gruppen ist möglich. Die Rechte sind additiv, d. h., es reicht die Berechtigung in einer einzigen Gruppe, um dieses Recht zu besitzen.

Netzwerke oder Hosts dürfen nur *einer* Netzwerkgruppe zugeteilt werden.

4.2 Netzwerkgruppen

Serienmäßig sind bereits mehrere Netzwerkgruppen angelegt. Die Gruppe *Internet* beinhaltet als Mitglied das Netz „Internet“ und damit alle IP-Adressen außerhalb der eigenen Netzwerkbereiche. Alle Berechtigungen, die über diese Gruppe erteilt werden, gelten damit für alle Computer, die sich mit diesem Server verbinden, aber nicht einer anderen Netzwerkgruppe angehören. Diese Gruppe sollte daher mit so wenig Rechten wie möglich ausgestattet werden.

Die Gruppe *LocalNetworks* hingegen beinhaltet als Mitglied das lokale Netz und gestattet diesem Zugriffe auf Dienste im Collax Security Gateway.

Im Feld *Erlaubte Dienste* sind alle Dienste im Collax Security Gateway aufgeführt, deren Berechtigung nur anhand einer IP-Adresse vergeben wird. Durch eine gesetzte Berechtigung wird der entsprechende Netzwerkport in der Firewall für die zugehörigen Netze oder Rechner geöffnet.

4.3 Benutzergruppen

Über die Gruppen *Users* und *Admins* können Berechtigungen für lokale Benutzer vergeben werden. *Admins* sollen dabei lokale Benutzer sein, denen administrative Zugriffe erlaubt werden, etwa auf den Überwachungs-Dienst oder auf das Viren-Quarantäneverzeichnis.

Der Einstellung der Benutzungsrichtlinien kann von zwei Seiten erfolgen, einerseits über die Konfigurationsdialoge zu den Benutzungsrichtlinien selbst und andererseits bei der Konfiguration der Dienste. Dazu sind in der Weboberfläche jeweils Reiter *Berechtigungen* vorhanden. Über diese erscheint ein Dialog, in dem einzelne Berechtigungen des Dienstes an eine oder mehrere Gruppen vergeben werden können.

4.4 Berechtigungen

In den Einstellungen lässt sich für jede Gruppe festlegen, ob sie in der Benutzerverwaltung sichtbar ist. Dies ist sinnvoll für Gruppen, die eine Benutzermitgliedschaft erfordern. So kann ein neuer Benutzer beim Anlegen direkt den entsprechenden Gruppen zugeordnet werden. Weiterhin lassen sich für jede Gruppe Quotas festlegen. Dies sind Begrenzungen des verfügbaren Speicherplatzes für Freigaben (Shares) und E-Mail.

Die übrigen Berechtigungen sind über eine Auswahlliste einstellbar. In der Liste sind die verschiedenen Dienste der einzelnen Berechtigungen in Klammern aufgeführt. Einige Berechtigungen sind auf einzelne Dienste beschränkt (*Fax*, *LDAP*, *Mail* usw.).

Für den Dienst *RAS* werden die Berechtigungen zur Einwahl auf

den Collax Security Gateway vergeben, u. a. ist hier mit *SSH* die verschlüsselte Konsolenverbindung auf den Collax Security Gateway selbst einstellbar.

Im Collax Security Gateway besteht die Möglichkeit, einzelnen Benutzern die gesamte oder Teile der Administration freizuschalten. Dazu können Berechtigungen für den Dienst *Role* aktiviert werden.

4.5 Gruppenplanung

Mit den vordefinierten Gruppen "Users" und "Administrators" Es gibt zwei vordefinierte Gruppen. Die Administrator Gruppe hat die Berechtigung für den Webaccess sowie den SSH-Zugang zum System.

Bei der Gruppenplanung sollte berücksichtigt werden, dass Benutzer nach Berechtigungen getrennt werden sollten. Am Beispiel einer Schule wären dies drei Gruppen: "Schüler", "Lehrer" und "Verwaltung".

Für den Zugriff auf die Anwenderseite, bzw den Webacess kann beispielsweise eine eigene Gruppe angelegt werden. Damit können lokale Benutzer angelegt werden, die die Berechtigung "Zugriff auf Anwenderseite" erhalten, weil sie Mitglied dieser Gruppe werden.

Zusätzlich muss für den dazugehörigen Netzwerkdienst der Port in der Firewall (HTTPS-Port) geöffnet werden. Dazu kann die Netzwerkgruppe ausgewählt werden, welche das entsprechende Netzwerk enthält, und dieser wird der Zugriff auf diesen Dienst erlaubt.

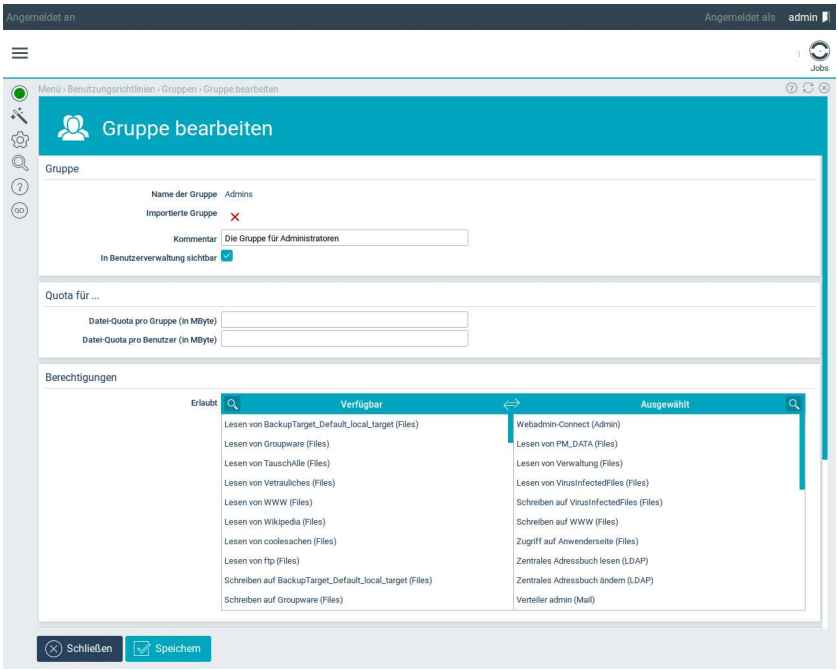
Werden neue Gruppen oder Netzwerkgruppen angelegt, ist es ratsam, für die Gruppennamen „sprechende“ Namen zu vergeben, die den Zweck und die dahinterliegenden Berechtigungen der Gruppe möglichst genau erklären. In diesem Beispiel ist es ersichtlich, dass alle Berechtigungen zum Webproxy, inkl. Eventuell später einzuführender Filterregeln, in der Gruppe ProxyUser abgewickelt werden

4.6 Schritt für Schritt: Anlegen einer Gruppe

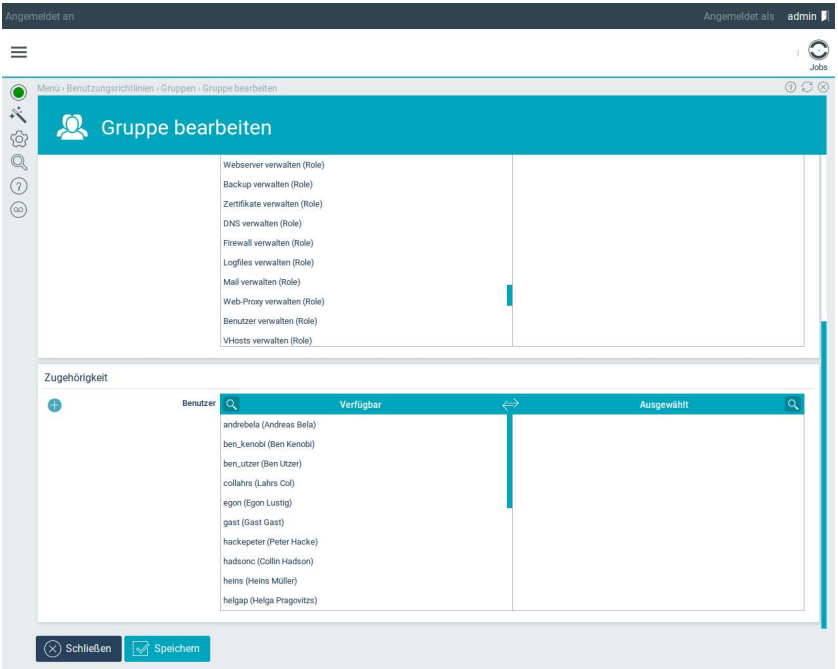
Im folgenden wird exemplarisch eine Gruppe eingerichtet, die die Fernwartung des Collax Security Gateways erlaubt. Obwohl dies eine konkrete Aufgabenstellung ist, ist das Vorgehen allgemeingültig und lässt sich analog für jede andere Gruppe nachvollziehen.

Beispielhaft soll der Web-Admin-Dienst für IP-Adressen aus dem lokalen Netz zugänglich sein. Dort soll sich neben dem *admin* auch ein neu angelegter Benutzer anmelden können, dem die Verwaltung von Zertifikaten, Benutzern und dem Backupsystem erlaubt wird.

Legen Sie zunächst unter *Benutzungsrichtlinien – Richtlinien – Gruppen* eine neue Gruppe an:

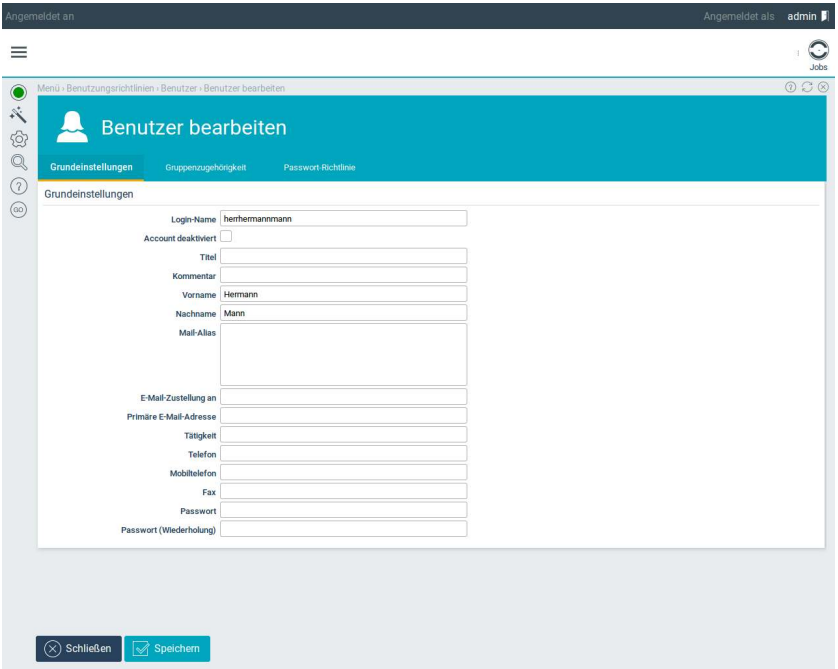


- Tragen Sie bei *Name* und *Kommentar* sinnvolle Texte ein. Der Name der Gruppe kann später nicht mehr geändert werden.
- Da diese Gruppe neu erstellt und nicht von einem Windows-Server o. ä. importiert wird, lassen Sie die Option *importierte Gruppe* deaktiviert. Andernfalls wird der Collax Security Gateway versuchen, eine Verbindung zum übergeordneten Server aufbauen und eine Gruppe dieses Namens abzurufen.
- Wenn Sie später Benutzer in die Gruppe aufnehmen möchten, aktivieren Sie die Option *In Benutzerverwaltung sichtbar*. Damit können Sie beim Anlegen eines Benutzers diesen direkt als Mitglied in die Gruppe aufnehmen.
- In den Feldern *Quota* können Sie Beschränkungen des Festplattenspeichers vornehmen. Da diese Gruppe nur dem Konfigurationszugriff auf den Collax Security Gateway dient und keine weitere Funktion bieten soll, nehmen Sie hier keine Einstellungen vor.
- Bei der Berechtigung suchen Sie nach Role. Die einzelnen Administrationsbereiche des Collax Security Gateways werden nun aufgelistet.

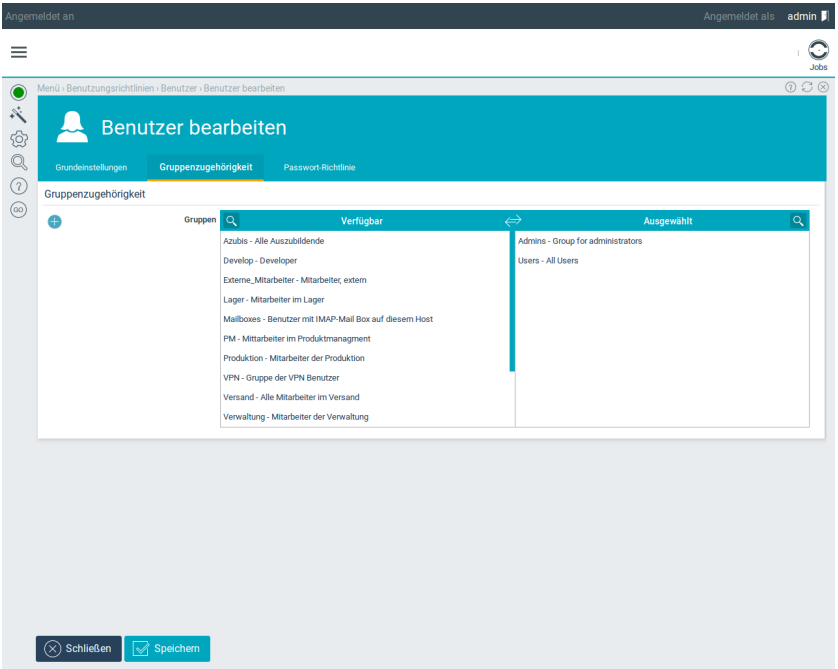


- Aktivieren Sie gemäß der Aufgabenstellung die Rechte zur Verwaltung von *Backup*, *Zertifikaten* und *Benutzern*.
- Geben Sie im Formular *Administrator* der gewünschten Netzwerkgruppe die Berechtigung zum "Web-Administrations-Port".

Ein neuer Benutzer kann durch klicken auf das Plus sowie unter *Benutzungsrichtlinien – Richtlinien – Benutzer – Benutzer anlegen* hinzugefügt werden.



- In diesem Dialog legen Sie zunächst das *Login* des Benutzers fest. Dieses Login muss innerhalb des Systems eindeutig sein. Es kann keiner der bereits angelegten Systembenutzer verwendet werden, auch wenn diese hier nicht sichtbar sind (z. B. „admin“).
- In den folgenden Feldern geben Sie den Namen des Benutzers, eventuelle Mail-Alias-Adressen und Telefonnummern an. Teilweise haben diese Einstellungen noch zusätzlich in weiteren Diensten des Collax Security Gateways eine Funktion. Beispielsweise wird über die Faxnummer die interne Zustellung eingehender Fax-Mitteilungen vorgenommen.
- Das *Passwort* müssen Sie zweimal eingeben, da es aus Sicherheitsgründen nicht sichtbar ist.



- Unter dem Reiter *Gruppenzugehörigkeit* können Sie die Gruppen aktivieren, zu denen der Benutzer gehören soll.
- Wählen Sie die neu angelegte *WartungsGruppe* aus.
- Nach dem Speichern der Einstellungen und Aktivieren der gesamten Konfiguration kann sich nun auch der neu angelegte Benutzer aus dem lokalen Netz auf der Administrationsoberfläche anmelden und hat Zugriff auf die dort für ihn freigeschalteten Bereiche.

4.7 GUI-Referenz: Richtlinien

4.7.1 *Gruppen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Gruppen*)

Über die Gruppen wird der Zugriff auf alle Dienste im Collax Security Gateway geregelt. In diesem Dialog werden Gruppen angelegt und deren Rechte verwaltet. Eine Gruppe besteht nur aus Benutzern.

Dieser Dialog besteht aus mehreren untergeordneten Dialogen.

4.7.1.1 *Gruppe wählen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Gruppen*)

In dieser Liste werden die bestehenden Gruppen angezeigt.

Felder in diesem Dialog

- *Name*: Der Name der Gruppe.
- *Kommentar*: Ein Kommentartext zur Gruppe.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird die Konfiguration der ausgewählten Gruppe bearbeitet.
- *Berechtigungen*: Mit dieser Aktion werden die Berechtigungen der Gruppe bearbeitet.
- *Benutzer*: Mit dieser Aktion werden alle Benutzer und ihre Mit-

gliedschaft in der Gruppe angezeigt. Der Mitgliedschaftsstatus kann geändert werden.

In eine importierte Benutzergruppe können keine Benutzer aufgenommen werden. Diese Aktion wird daher nur für lokal angelegte Gruppen angezeigt.

- *Rechner*: Mit dieser Aktion werden alle Rechner und ihr Mitgliedstatus in der Gruppe angezeigt. Der Mitgliedschaftsstatus kann geändert werden.
- *Netze*: Mit dieser Aktion werden alle Netzwerke und ihr Mitgliedstatus in der Gruppe angezeigt. Der Mitgliedschaftsstatus kann geändert werden.
- *Löschen*: Diese Aktion löscht die ausgewählte Gruppe.

Aktionen für diesen Dialog

- *Gruppe anlegen*: Mit dieser Aktion wird eine neue Gruppe angelegt.

4.7.1.2 *Gruppe bearbeiten*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Gruppen*)

In diesem Dialog wird eine zuvor ausgewählte Gruppe bearbeitet.

Abschnitt *Gruppe*
Felder in diesem Abschnitt

- *Name der Gruppe*: Der Name der Gruppe, er kann nicht nachträglich geändert werden.
- *Importierte Gruppe*: Mit dieser Option wird angegeben, dass die

Gruppe auf einem anderen System verwaltet wird. Dies kann beim Anlegen einer Gruppe festgelegt, jedoch später nicht mehr geändert werden.

- *Name der Gruppe*: Hier wird der Name der Gruppe angegeben. Der Name darf nicht mit einer Ziffer beginnen und darf auch keine Leerzeichen enthalten.
- *Importierte Gruppe*: Mit dieser Option wird angegeben, dass die Gruppe auf einem anderen System verwaltet wird, z. B. auf einem Windows-Server. Dies kann beim Anlegen einer Gruppe festgelegt, jedoch später nicht mehr geändert werden.
- *Kommentar*: In diesem Feld kann ein Kommentartext zu dieser Gruppe erstellt werden.
- *In Benutzerverwaltung sichtbar*: Wenn diese Option aktiviert ist, wird die Gruppe in der Benutzerverwaltung angezeigt. Dort kann ein neu angelegter Benutzer direkt in diese Gruppe aufgenommen werden.

Abschnitt *Windows-Gruppen Zuordnung*

Dieser Abschnitt wird eingeblendet, wenn der Collax Server mit dem Authentifizierungs-Modus PDC aktiviert ist.

Felder in diesem Abschnitt

- *Vordefinierte Windows-Gruppe*: Hier kann die Microsoft Windows-Gruppe angegeben werden, deren Rechte auf die Systemgruppe vererbt werden soll.

4.7.1.3 *Berechtigungen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Gruppen*)

Abschnitt *Gruppe*
Felder in diesem Abschnitt

- *Name der Gruppe*: Nach dem Anlegen einer Gruppe kann deren Name nicht mehr geändert werden.

Abschnitt *Berechtigungen*

Hier werden die Berechtigungen der Gruppenmitglieder für die verschiedenen Dienste konfiguriert.

Die Berechtigungen sind additiv, d. h., wenn ein Gruppenmitglied zu mehreren Gruppen gehört, in denen dieselbe Berechtigung in einigen aktiviert und in anderen deaktiviert ist, ist die Berechtigung für dieses Mitglied aktiviert. Es reicht aus, wenn eine Berechtigung für das Mitglied in einer einzigen Gruppe aktiviert ist.

Felder in diesem Abschnitt

- *Berechtigungen*: In dieser Liste werden alle Berechtigungen angezeigt.

4.7.1.4 *Benutzer*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Gruppen*)

In diesem Dialog sind alle angelegten Benutzer sichtbar. Benutzer, die zu der bearbeiteten Gruppe gehören, sind markiert.

In diesem Dialog werden die Mitglieder der Gruppe ausgewählt.

Felder in diesem Dialog

- *Name der Gruppe*: In diesem Feld wird der Name der Gruppe angezeigt.

4.7.1.5 *Rechner*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Gruppen*)

In diesem Dialog sind alle angelegten Rechner sichtbar. Rechner, die zu der bearbeiteten Gruppe gehören, sind markiert.

In diesem Dialog werden die Rechner ausgewählt, die zu der Gruppe gehören sollen.

Felder in diesem Dialog

- *Name der Gruppe*: Hier wird der Name der Gruppe angezeigt.

4.7.1.6 *Netzwerke*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Gruppen*)

In diesem Dialog sind alle angelegten Netzwerke sichtbar. Netze, die zu der bearbeiteten Gruppe gehören, sind markiert.

Felder in diesem Dialog

- *Name der Gruppe*: Hier wird der Name der Gruppe angezeigt.

4.7.2

4.7.2.1 Aktionen für dieses Formular

- :
- *Host-Analyse*: Funktionieren Berechtigungen von Netzwerken oder Hosts nicht korrekt, können mit dieser Analyse Details über Berechtigungen, Verwendung oder Firewallregeln bestimmter Netzwerkhosts abgerufen werden.

4.7.3 *Netzwerkgruppe*

4.7.3.1 XXX missing title found
Felder in diesem Abschnitt

- *Name*: Der Name darf maximal 28 Zeichen enthalten. Enthielt ein Netzwerkname mehr als 28 Zeichen wird bei der Umstellung eine eindeutige Zeichenkette angefügt, und der Name auf 28 Zeichen gekürzt.
- *Info*:
- *Gewichtung*: Jede Netzwerkgruppe erhält automatisch eine Ge-

wichtung. Mit Hilfe dieser Gewichtung werden Reihenfolgen für Firewall-Regeln bestimmt. Die Gewichtung bestimmt sich aus Position in der Hierchachie oder sie kann manuell gesetzt werden.
- *Übergeordnete Netzwerkgruppe*: Hier kann eine übergeordnete Netzwerkgruppe gewählt werden.

4.7.3.2 Felder in diesem Abschnitt

- *Verwendet von*: Zeigt an, ob in der Gruppierung Netzwerke, Hosts, oder Netzwerke und Hosts enthalten sind.
- *Erlaubte Dienste*: Für die Mitglieder dieser Netzwerkgruppe werden die gewählten Berechtigungen gewährt. Sind Hosts als Gruppenmitglieder zusätzlich in weiteren Netzwerkgruppen, richtet sich die Berechtigung zusätzlich nach der Gewichtung der jeweiligen Netzwerkgruppe.
- *Verbotene Dienste*: In diesem Feld können Dienste explizit für die Mitglieder der Netzwerkgruppen verboten werden, wenn aus übergeordneten Gruppen Rechte vererbt wurden.

4.7.4 *Importierbare Gruppen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Importierbare Gruppen*)

In diesem Dialog werden Gruppen angezeigt, die in der Benutzerverwaltung eines Active Directory benutzt werden. Damit Gruppen aus der Active Directory-Verwaltung angezeigt werden können, muss das System einem Active Directory als Mitglied beigetreten sein und

die Funktion *Active Directory-Proxy* auf dem System aktiviert sein. Die aufgelisteten Gruppen können dann in die lokalen Benutzungsrichtlinien eingebunden werden, sobald diese über die Aktion *Zu lokalen Gruppen hinzufügen* in die Verwaltung aufgenommen wurden. Die Benutzer der AD-Gruppen werden weiterhin über das Active Directory verwaltet und sind nicht Bestandteil des lokalen Systems.

4.7.4.1 *Liste der importierbaren Gruppen*

Die Liste zeigt Gruppen an, die Benutzer beinhalten. Der Benutzer Administrator wird nicht als Benutzer gelistet. Enthält eine Gruppe nur den Benutzer Administrator wird dieses Gruppe ebenfalls nicht gelistet.

Abschnitt *Hinweis*
Felder in diesem Abschnitt

- : Wenn der Active Directory-Proxy noch nicht aktiviert wurde, erscheint hier der entsprechende Hinweis.

Spalten in der Tabelle

- *Name*: Zeigt den Namen der Gruppe im Active Directory.
- *Kommentar*: Zeigt weitere Informationen über die Gruppe an.

Aktionen für jeden Tabelleneintrag

- *Benutzer dieser Gruppe*: Über diese Aktion können die Benutzer der AD-Gruppe aufgelistet werden.
- *Zu lokalen Gruppen hinzufügen*: Mit dieser Aktion können AD-

Gruppen der lokalen Richtlinienverwaltung zur Verfügung gestellt werden. Diese Gruppen tauchen nachfolgend im Menü *Gruppen* auf.

- *WARNUNG! Diese Gruppe existiert bereits ist aber nicht als Importierte Gruppe markiert. Aus lokalen Gruppen entfernen.*: Falls schon eine lokale Gruppe besteht, deren Name identisch zu einer Gruppe aus dem Active Directory ist, wird gewarnt. Um Konflikte zu vermeiden, empfiehlt es sich diese Gruppe nicht in die Richtlinienverwaltung zu übernehmen.
- *Aus lokalen Gruppen entfernen*: Wurde eine AD-Gruppe der lokalen Richtlinienverwaltung zur Verfügung gestellt und ab sofort nicht mehr benötigt, kann diese mit dieser Aktion entfernt werden.

4.7.4.2 *Mitglieder der entfernten Gruppe*

In diesem Dialog werden alle Benutzer einer entfernten Gruppe angezeigt.

Felder in diesem Formular

- *Name der Gruppe*: Zeigt den Namen der gewählten AD-Gruppe.

Aktionen für dieses Formular

- *Zurück*: Führt zurück in die Übersicht der importierbaren Gruppen.

4.7.5 *Berechtigungen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Berechtigungen*)

In diesem Dialog werden die Berechtigungen des Systems verwaltet.

4.7.5.1 *Berechtigungen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Berechtigungen*)

Hier werden alle im System definierten Berechtigungen aufgelistet. Statische und dynamische Berechtigungen können bearbeitet und den verschiedenen Gruppen zugewiesen werden. Prinzipiell werden statische oder dynamische Berechtigungen immer durch das System vordefiniert. Maßgeschneiderte Rollenberechtigungen können unter Administrative Rollen (S. 69) hinzugefügt oder verändert werden.

Felder in diesem Formular

- *Service*: Hier wird die Bezeichnung des Service angezeigt.
- *ID*: Hier wird die ID der Berechtigung angezeigt.
- *Kommentar*: Hier wird ein zusätzlicher Kommentar zur Berechtigung angezeigt.
- *Typ*: Hier wird der Typ der Berechtigung angezeigt. Statische und dynamische Berechtigungen werden vom System vorgegeben, der Typ „custom“ bezeichnet die individuell definierten Berechtigungen für administrative Rollen.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird die Konfiguration der ausgewählten Berechtigung bearbeitet.

4.7.5.2 *Berechtigung*

In diesem Formular werden Systemberechtigungen angezeigt. Nur die Gruppenzuweisung kann verändert werden, die Berechtigung selbst kann nicht geändert werden.

Abschnitt*Grundeinstellungen*
Felder in diesem Abschnitt

- *Service*: Hier wird der Service der Berechtigung angezeigt.
- *ID*: Hier wird die interne ID der Berechtigung angezeigt.
- *Beschreibung*: Hier ist eine kurze Beschreibung eingetragen.

Abschnitt *Gruppenzugehörigkeit*
Felder in diesem Abschnitt

- *Berechtigung für Gruppen*: Hier wird eingestellt, für welche Gruppe die Berechtigung gelten soll.

Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten der Berechtigung beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten der Berechtigung beenden. Die Änderungen werden übernommen.

4.7.6 *Benutzer*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Benutzer*)

In diesem Dialog werden die Benutzer des Systems verwaltet.

4.7.6.1 *Benutzer auswählen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Benutzer*)

Hier werden alle auf dem System angelegten Benutzer angezeigt. Neue Benutzer können hier angelegt, bestehende Benutzer können hier bearbeitet oder gelöscht werden.

Spalten in der Tabelle

- *Login*: Der Login-Name des Benutzers. Dieser wird zur Authentifizierung bei allen Diensten genutzt (beispielsweise am Mailserver). Für den Login-Namen sollten nur Kleinbuchstaben verwendet werden.
- *Vorname*: Der Vorname des Benutzers.
- *Nachname*: Der Nachname des Benutzers.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird das Benutzerkonto bearbeitet.
- *Löschen*: Mit dieser Aktion wird Benutzerkonto gelöscht.

Aktionen für diesen Dialog

- *Benutzer anlegen*: Mit dieser Aktion wird ein neues Benutzerkonto erstellt.
- *Benutzer importieren*: Mit dieser Aktion kann eine Liste von Benutzern aus einer Datei im CSV-Format importiert werden.
- *Benutzer exportieren*: Mit dieser Aktion werden alle im System angelegten Benutzerkonten exportiert. Die Datei ist im CSV-Format aufgebaut. Dabei wird pro Benutzerkonto eine Zeile erzeugt. Die einzelnen Werte sind durch Komma getrennt. Die erste Zeile des Exports ist eine Musterzeile mit einer genauen Aufschlüsselung der einzelnen Felder.

4.7.6.2 *Benutzer bearbeiten*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Benutzer*)

In diesem Dialog können die Einstellungen des Benutzerkontos bearbeitet werden.

Tab *Grundeinstellungen*, Abschnitt *Grundeinstellungen*
Felder in diesem Abschnitt

- *Login-Name*: Der Login-Name des Benutzers wird zur Authentifizierung bei den verschiedenen Diensten des Collax Security Gateways eingesetzt.

  Der Login-Name sollte in Kleinbuchstaben angegeben werden. Erlaubt sind nur die Buchstaben „a“ bis „z“ (keine Umlaute o. ä.), Ziffern, der Unterstrich „_“ sowie (nicht empfohlen) die Großbuchstaben „A“ bis „Z“. Der Login-Name darf nicht mit einer Ziffer beginnen.

Das Eingabefeld erscheint nur, wenn ein neues Benutzerkonto angelegt wird.

- *Login-Name*: Hier wird der Login-Name des Benutzerkontos angezeigt. Wenn ein Benutzerkonto bearbeitet wird, kann der Name nicht geändert werden.
- *Account deaktiviert*: Mit dieser Option kann ein Benutzerkonto zeitweilig deaktiviert werden. Dem Benutzer werden dann alle Berechtigungen entzogen. Soll ein Benutzerkonto wieder Berechtigungen erhalten und im System verfügbar sein, kann das Benutzerkonto einfach wieder aktiviert werden.
- *Titel*: In diesem Feld kann der persönliche Titel des Benutzers (Dr., Dipl.-Ing. usw.) eingetragen werden. Diese Angabe erscheint dann im LDAP-Verzeichnis.
- *Vorname*: Der Vorname des Benutzers.
- *Nachname*: Der Nachname des Benutzers.

  Abhängig von den SMTP-Einstellungen wird aus Vorname und Nachname des Benutzers die E-Mail-Adressierung erzeugt. Dabei werden nicht zulässige Zeichen automatisch konvertiert: Ein Leerzeichen wird zu einem Punkt, „ß“ wird zu „ss“. Umlaute werden in die Schreibweise mit folgenden „e“, z. B. „ä“ zu „ae“, und Zeichen mit Akzent werden zu Zeichen ohne Akzent umgewandelt.
- *Mail-Alias*: In diesem Eingabefeld können zusätzliche E-Mail-Adressen für den Benutzer angegeben werden, die als E-Mail-Alias angelegt werden. Wird dabei die Maildomain nicht angegeben, erhält der Benutzer den Alias in jeder der lokal verwalteten Maildomains, zu der er über die Gruppenberechtigung gehört. Wird die Adresse mit Maildomain angegeben, gilt der Alias nur in der angegebenen Domain.

  Pro Zeile wird eine Adresse eingegeben, ein Trennzeichen ist nicht erforderlich.

Hinweis: Wird eine Adresse in einer Domain angegeben, die nicht zu einer der lokal verwalteten Maildomains des Systems gehört, erscheint die Adresse zwar im LDAP-Verzeichnis, E-Mails an diese Adresse werden jedoch nicht zugestellt.

- *E-Mail-Zustellung an*: In diesem Feld kann die E-Mail-Adresse eines lokalen Benutzers, eines Verteilers, ein Alias eines Benutzers oder eine externe E-Mail-Adresse angegeben werden. An die eingetragene Adresse werden alle E-Mails dieses Benutzers umgeleitet. Die E-Mails werden nicht im lokalen Postfach des Benutzers gespeichert. Normalerweise kann dieses Feld leerbleiben.
- *Primäre E-Mail-Adresse*: Wenn E-Mail-Clients verwendet werden, die eine Einstellung der Absenderadresse des Benutzers nicht zulassen, ist es sinnvoll diese Option auf Server-Seite zu setzen. Betreffende E-Mail-Clients können Web-Mailer und Clients, die sich mit einem MAPI-Server verbinden, sein. In das Feld soll eine gültige lokale E-Mail-Adresse eingetragen werden. Diese Adresse wird als Absender in den versendeten E-Mails des Benutzers erscheinen.

  Diese Option überschreibt den eingestellten Adressaufbau der Primär-Adresse im Formular *SMTP-Empfang*.
- *Tätigkeit*: Hier kann eine Beschreibung der Tätigkeit des Benutzers für das LDAP-Verzeichnis angegeben werden.
- *Telefon*: Hier können eine oder mehrere Telefonnummern für das LDAP-Verzeichnis angegeben werden. Mehrere Nummern müssen durch Komma getrennt eingetragen werden.
- *Mobiltelefon*: Hier können eine oder mehrere Mobilfunknummern für das LDAP-Verzeichnis angegeben werden. Mehrere Nummern müssen durch Komma getrennt eingetragen werden.
- *Fax*: Hier können eine oder mehrere Nummern von Faxanschlüssen für das LDAP-Verzeichnis angegeben werden. Mehrere Nummern müssen durch Komma getrennt eingetragen werden.

Wird auf diesem System der Fax-Dienst genutzt und gehen Faxe auf einer der hier angegebenen Nummern ein, wird diesem Benutzer das Fax zugestellt.

- *Passwort*: Das Passwort des Benutzers.

  Hinweis: Bei einigen Sonderzeichen im Passwort kann es vorkommen, dass das Webmailinterface dieses nicht akzeptiert. Dann erhält der Benutzer beim Aufrufen des Webmailers eine Fehlermeldung, obwohl er sich zuvor an der Web-Access-Seite anmelden konnte.
- *Passwort (Wiederholung)*: Da das Passwort aus Sicherheitsgründen bei der Eingabe nicht angezeigt wird, muss es hier zur Kontrolle ein zweites Mal eingegeben werden.
- *Passwort-Richtlinie*: Dem Benutzer kann eine Passwort-Richtlinie zugewiesen werden, welcher er unterliegt. Wird das Feld leergelassen, oder auf Standard / Default gesetzt unterliegt der Benutzer der Standardrichtlinie.

Tab *Gruppenzugehörigkeit*, Abschnitt *Gruppenzugehörigkeit*
Felder in diesem Abschnitt

- *Gruppen*: Hier kann konfiguriert werden, zu welchen Gruppen der Benutzer gehört. Es sind nur die Gruppen aufgeführt, die „in der Benutzerverwaltung sichtbar“ sind.

4.7.6.3 *Benutzer importieren*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Benutzer*)

Felder in diesem Dialog

- *Benutzer importieren*: Mit diesem Dialog kann eine bestehende Liste von Benutzerkonten importiert werden. Diese müssen in einer Datei im CSV-Format gespeichert sein. Dabei wird pro Zeile ein Benutzerkonto angegeben, die einzelnen Werte sind in einer festgelegten Reihenfolge durch Kommas getrennt abgelegt.
- *CSV-Datei*: Hier wird die Datei mit den Benutzerkonten ausgewählt.
- *Ergebnis*: Nach dem Import wird hier das Ergebnis angezeigt.

Aktionen für diesen Dialog

- *Importieren*: Import der Benutzerliste starten.

4.7.7 *Administrative Rollen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Umgebung – Administrative Rollen*)

In diesem Dialog werden die administrativen Rollen von Benutzern verwaltet.

4.7.7.1 *Administrative Rollen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Umgebung – Administrative Rollen*)

In diesem Formular werden administrative Rollen für Benutzer angezeigt oder individuell definiert. Administrative Rollen sind Zugriffsberechtigungen von ausgewählten Benutzern auf entsprechende

Formulare der Collax-Administrationsoberfläche. Sie können flexibel definiert werden, Zugriff auf nur ein einzelnes oder auf mehrere Formulare zu gewähren ist möglich.

Felder in diesem Formular

- *Name*: Hier wird der Name der Admin-Rolle angezeigt. Dieser wird frei definiert und erscheint auch im Formular der Gruppenberechtigungen zur Auswahl.
- *Kommentar*: Hier wird ein zusätzlicher Kommentar zur administrativen Rolle angezeigt.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird die gewählte Rolle bearbeitet.
- *Löschen*: Mit dieser Aktion wird die gewählte Rolle gelöscht. Sie steht nachfolgend nicht mehr in den Gruppenberechtigungen zur Verfügung.

Aktionen für dieses Formular

- *Hinzufügen*: Mit dieser Aktion kann eine neue administrative Rolle für eine Benutzergruppe definiert werden.

4.7.7.2 *Berechtigung*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Umgebung – Administrative Rollen*)

Tab*Grundeinstellungen*, Abschnitt*Berechtigung*
Felder in diesem Abschnitt

- *Bezeichnung*: In dieses Feld wird die Namensbezeichnung der neuen Berechtigung eingegeben.
- *Beschreibung*: Hier wird eine spezifizierte Beschreibung der neuen Berechtigung eingegeben.

Tab*Formulare Zugewiesene Formulare*
Felder in diesem Abschnitt

- *Zugewiesene Formulare*: Hier werden die Formulare ausgewählt, die verwaltet werden dürfen.

Tab*Gruppen Zugewiesene Gruppen*
Felder in diesem Abschnitt

- *Zugewiesene Gruppen*: Hier werden die gewünschten Gruppen für die Berechtigung ausgewählt. Die Mitglieder der hier ausgewählten Gruppen dürfen die Funktionen der gewählten Formulare vollständig verwalten.

Aktionen für dieses Formular

- *Abbrechen*: Mit dieser Aktion wird die Bearbeitung beendet. Die Einstellungen werden nicht übernommen.
- *Speichern*: Mit dieser Aktion wird die Bearbeitung beendet. Die vorgenommenen Einstellungen werden übernommen.

4.7.8 *Zeiträume*

In diesem Dialog werden Zeiträume verwaltet. Auf diese Zeiträume wird in anderen Dialogen zurückgegriffen, etwa bei der Konfiguration von Filtern oder Mailabholaufträgen.

Vordefiniert ist der Zeitraum *always*, der rund um die Uhr gilt, also „24/7/365“. Weitere Zeiträume, etwa für die Arbeitszeiten, können angelegt werden.

4.7.8.1 *Zeitraum wählen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Zeiträume*)

In dieser Liste werden die definierten Zeiträume angezeigt.

Felder in diesem Dialog

- *Name*: Hier wird der Name des Zeitraumes angezeigt.
- *Kommentar*: Hier wird der Kommentartext zu dem Zeitraum angezeigt.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion kann der Zeitraum bearbeitet werden.
- *Löschen*: Diese Aktion löscht den gesamten Zeitraum.

Aktionen für diesen Dialog

- *Neuer Zeitraum*: Mit dieser Aktion wird ein neuer Zeitraum festgelegt.

4.7.8.2 *Zeitraum bearbeiten*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Zeiträume*)

In diesem Dialog wird der Zeitraum bearbeitet. Ein Zeitraum besteht aus einem oder mehreren Zeitabschnitten, die wiederum aus einer Angabe für den Beginn und das Ende sowie einer Liste von Wochentagen bestehen.

Abschnitt *Name*

Hier wird der Name des Zeitraums festgelegt.

Felder in diesem Abschnitt

- *Bezeichnung*: Hier kann der Name des Zeitraums geändert werden.
- *Kommentar*: Hier kann ein kurzer Kommentartext zum Zeitraum angegeben werden.

Abschnitt *Zeitabschnitt*

Jeder Zeitraum kann mehrere Zeitabschnitte umfassen. Für jeden dieser Zeitabschnitte wird dieser Teildialog angezeigt.

Aktionen für diesen Dialog

- *Zeitabschnitt hinzufügen*: Mit dieser Aktion wird ein weiterer Zeitabschnitt zum Zeitraum hinzugefügt.

Spalten in der Tabelle

- *von*: Hier wird der Beginn des Zeitabschnitts angegeben.
- *bis*: Hier wird das Ende des Zeitabschnitts angegeben. Falls das Ende zeitlich vor dem Beginn liegt, wird dies als „endet am nächsten Tag um diese Zeit“ angenommen.
- *Wochentage*: Hier werden alle Wochentage aktiviert, an denen der Zeitabschnitt gelten soll. Die Tage beziehen sich jeweils auf die Anfangszeit (die Endzeit kann auf den Folgetag fallen).

Aktionen für jeden Tabelleneintrag

- *Löschen*: Hiermit wird der markierte Zeitabschnitt gelöscht.

4.8 GUI-Referenz: Umgebung

In diesem Abschnitt werden globale Einstellungen für den Administrator und den Standort des Collax Security Gateways vorgenommen.

4.8.1 *Administrator*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Umgebung – Administrator*)

In diesem Dialog kann das Administrator-Passwort für die Oberfläche geändert und die E-Mail-Adresse für E-Mails des Systems selbst eingetragen werden.

4.8.1.1 Tab *Grundeinstellungen*, Abschnitt *Angaben*

Felder in diesem Abschnitt

- *Passwort*: Hier kann ein neues Passwort für den Administrator gesetzt werden. Das Passwort wird nur geändert, wenn in diesem Feld ein neues Passwort eingegeben wird, das dann mit der Eingabe im Kontrollfeld übereinstimmt.
- *Passwort (Wiederholung)*: Da aus Sicherheitsgründen das Passwort während der Eingabe nicht angezeigt wird, muss es hier zur Kontrolle noch einmal eingegeben werden.
- *E-Mail-Adresse*: Hier wird die E-Mail-Adresse des Systemverantwortlichen angegeben. An diese Adresse werden Fehlermeldungen des Systems und ähnliches geschickt.

  Die Adresse kann entweder eine externe E-Mail-Adresse, das Login eines lokalen Benutzers oder die Adresse eines lokalen Postfachs mit Angabe des kompletten Systemnamens als Domain (in der Form Login@FQDN) sein. Adressen aus einer der lokal verwalteten Maildomains und Adressen von Verteilern können hier nicht verwendet werden.

  Wird hier nichts eingetragen, werden Meldungen des Systems verworfen.

Aktionen für diesen Abschnitt

- *Test E-Mail*: Mit dieser Aktion wird eine Test E-Mail an die angegebene E-Mail Adresse gesendet.

4.8.1.2 Tab *Grundeinstellungen*, Abschnitt *SSH*

Felder in diesem Abschnitt

- *Secure Shell aktivieren*: Mit dieser Option wird der SSH-Dienst auf dem System aktiviert. Welche Rechner und Netze eine SSH-Verbindung aufbauen dürfen, kann innerhalb der Gruppen in den Benutzungsrichtlinien konfiguriert werden.

4.8.1.3 Tab *Grundeinstellungen*, Abschnitt *Administrations-Web-Server*

Felder in diesem Abschnitt

- *Serverzertifikat*: Für den verschlüsselten Zugriff auf die Web-Administration kann hier ein eigenes Zertifikat gewählt werden. Üblicherweise braucht kein Zertifikat gewählt werden, denn das System erzeugt dann ein auf den Server-Host-Namen abgestimmtes Zertifikat selbst. Das hat zur Folge, dass bei Änderung des Host-Namens ein neues Zertifikat mit geändertem Common Name erzeugt wird. Ist ein Zertifikat aus der Liste gewählt, wird dieses auch bei Änderung des FQDN weiter benutzt.
- *SSL/TLS Version*: Mit der Angabe der TLS-Version kann beeinflusst werden, welches Verschlüsselungsprotokoll der verbindende Client benutzen muss, um eine entsprechend sichere Verbindung mit dem Server herzustellen.

4.8.1.4 Tab *Grundeinstellungen*, Abschnitt *Sitzungsverwaltung* Felder in diesem Abschnitt

- *Automatische Abmeldung Admin-GUI*: Aus Sicherheitsgründen werden Administrationssitzungen nach einer bestimmten Leerlaufzeit unterbrochen. Mit diesem Feld wird eingestellt, wie lange diese Leerlaufzeit dauern darf.

4.8.1.5 Tab *Berechtigungen*, Abschnitt *Benutzerrechte* Felder in diesem Abschnitt

- *SSH-Zugang*: Hier werden die Benutzergruppen gewählt, die authorisierten Zugriff per SSH-konsole erhalten dürfen. Auch wenn keine Gruppen gewählt wurden, kann standardmäßig der Systembenutzer „admin“ per SSH zugreifen.

4.8.1.6 Tab *Berechtigungen*, Abschnitt *Netzwerkzugang* Felder in diesem Abschnitt

- *Web-Administrations-Port*: Erlaubt den Zugriff der gewählten Netzwerkgruppen auf den Port 8001 auf diesem Server.
- *SSH-Port*: Erlaubt den Zugriff der gewählten Netzwerkgruppen auf den Port 22 auf diesem Server.

4.8.2 *Standort*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Umgebung – Standort*)

In diesem Dialog werden verschiedene Angaben zum Standort des Systems und des Unternehmens eingegeben.

Die Angaben hier dienen als Vorgabewerte für andere Stellen im System.

4.8.2.1 Abschnitt *Firma/Organisation*

Die Felder in diesem Abschnitt werden im LDAP-Verzeichnis eingetragen. Außerdem werden sie als Vorgabe beim Erstellen von Zertifikaten verwendet. Die meisten Felder sind optional, jedoch sollten mindestens der Name der Organisation sowie das Land angegeben werden.

Felder in diesem Abschnitt

- *Firma/Organisation*: Hier wird der Name des Unternehmens oder der Einrichtung angegeben.
- *Abteilung/Sektion*: Hier kann eine Abteilung oder Sektion angegeben werden.
- *Straße*: Hier wird die Straße des Unternehmens angegeben.
- *Postleitzahl*: Hier wird die Postleitzahl des Unternehmens angegeben.
- *Ort*: Hier wird der Ort des Unternehmens angegeben.
- *Bundesland/Region*: Hier wird das Bundesland oder die Provinz des Unternehmens angegeben.
- *Land*: Hier wird das Land des Unternehmens ausgewählt.

4.8.2.2 Abschnitt *Telefonie*

Die Angaben in diesem Abschnitt dienen dazu, Telefonnummern in eine einheitliche Form umzusetzen und später aus dieser Form die zu wählende Rufnummer zu ermitteln.

Felder in diesem Abschnitt

- *Landesvorwahl*: Hier wird die Landesvorwahl der eigenen Telefonnummer angegeben. Führende Nullen entfallen dabei. Für Deutschland ist dies z. B. „49“, für die Schweiz „41“ und für Österreich „43“.
- *Ortsnetz*: Hier wird die Ortskennzahl der eigenen Telefonnummer angegeben, ebenfalls ohne vorangestellte Null.
- *Anlagenrufnummer*: Hier wird die Rufnummer der Telefonanlage angegeben. Wird keine Telefonanlage verwendet und ist das System direkt an das öffentliche Telefonnetz angeschlossen, bleibt dieses Feld leer.
- *Amtsholung*: Ist das System an einer Nebenstellenanlage angeschlossen und bekommt beim Abnehmen nicht automatisch eine Amtsleitung, muss hier die Kennzahl angegeben werden, mit der eine Amtleitung geschaltet wird. Dies ist meist eine Null.
- *Vorwahl für Fernverbindungen*: Hier wird die Vorwahl für nationale Verbindungen in andere Ortsnetze angegeben. Dies ist meist eine Null.
- *Vorwahl für internationale Verbindungen*: Hier wird die Vorwahl für internationale Fernverbindungen angegeben. Dies sind meist zwei Nullen.

4.8.3 GUI-Referenz: *Passwort-Richtlinien*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Authentifizierung – Passwort-Richtlinien*

Passwort-Richtlinien bestehen aus einer Liste von Regeln, die die Sicherheit auf dem Server und im Unternehmen erhöhen. Dies wird dadurch erreicht, dass Benutzer aufgefordert werden starke Passwörter im Unternehmen zu verwenden, oder dass Passwörter der Benutzer nur einen begrenzten Zeitraum gültig sind.

4.8.3.1 *Passwort-Richtlinie*

Felder in dieser Tabelle

- *Name*: Name der Passwortrichtlinie.
- *Kommentar*: Weitere Information über die Passwortrichtlinie.
- *Standard*: Zeigt an, ob die Richtlinie standardmäßig für die Benutzer gilt.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Diese Aktion öffnet den Dialog zum Bearbeiten einer Passwortrichtlinie. Die Richtlinie namens Default kann nicht bearbeitet werden, mit dieser Aktion können die Detaileinstellungen eingesehen werden.
- *Löschen*: Diese Aktion löscht die gewählte Richtlinie.
- *Als Standard setzen*: Mit dieser Aktion kann eine Richtlinie als Standardrichtlinie für die Benutzer gesetzt werden.

Aktionen für dieses Formular

- *Hinzufügen*: Diese Aktion öffnet den Dialog, um eine neue Richtlinie hinzuzufügen.

4.8.3.2 GUI-Referenz: *Passwort-Richtlinie editieren*

Tab *Allgemein*
Felder in diesem Abschnitt

- *Name*: Hier wird eine kurze Bezeichnung für die Richtlinie eingegeben oder angezeigt.
- *Kommentar*: Weitere Informationen können in diesem Feld eingegeben werden.
- *Passwort muss geändert werden nach (Tage)*: Die Zahl gibt an, nach wie viel Tagen der Benutzer sein Passwort ersetzen muss. Bei Angabe von 0 Tagen braucht das Passwort nie geändert werden.
- *Erlaubte Logins nach Ablauf*: Wenn das Passwort abgelaufen ist, darf der Benutzer diese bestimmte Anzahl von Logins noch vornehmen, bevor der Zugang gesperrt wird.
- *Benutzer vor Ablauf per E-Mail informieren*: Hier wird angegeben, ob eine E-Mail an den Benutzer versendet wird, bevor das Passwort geändert werden muss.
- *Tage vor Ablauf*: Dieser Wert gibt den Zeitpunkt an, zu dem der Benutzer vor dem Ablauf informiert werden soll.
- *Anzahl alter zu speichernder Passwörter*: Gibt an, wie viele verwendete Passwörter gemerkt werden sollen, um eine Wiederverwendung zu verhindern.

- *Minimale Passwort Länge*: Das Passwort muss mindestens die hier angegebene Anzahl von Zeichen aufweisen.
- *Passwort-Qualität prüfen*: Durch diese Option können weitere Kriterien angegeben werden, welche bei der Definition eines neuen Passworts überprüft werden.
- *Standard*: Gibt an, ob diese Richtlinie standardmäßig für Benutzer angewendet werden soll.

Tab *Qualitätskriterien*, Abschnitt *Minimale Anzahl von Zeichen* Felder in diesem Abschnitt

- *Zahlen*: Diese Anzahl von Zahlen muss mindestens im neuen Passwort vorkommen.
- *Großbuchstaben*: Diese Anzahl von Großbuchstaben muss mindestens im neuen Passwort vorkommen.
- *Kleinbuchstaben*: Diese Anzahl von Kleinbuchstaben muss mindestens im neuen Passwort vorkommen.
- *Sonderzeichen*: Diese Anzahl von Sonderzeichen muss mindestens im neuen Passwort vorkommen.

Tab *Benutzer* Felder in diesem Abschnitt

- *Benutzer*: Wenn die Passwort-Richtlinie nicht standardmäßig auf alle Benutzer angewendet wird, können hier die entsprechenden Benutzer gewählt werden. Diese Benutzer unterliegen noch keiner Passwort-Richtlinie.

Aktionen für dieses Formular

- *Als Standard setzen*: Diese Aktion setzt die gewählte Richtlinie als Standardrichtlinie, diese gilt dann für alle Benutzer, für die keine spezielle Richtlinie angegeben wurde.
- *Löschen*: Löscht die gewählte Richtlinie.
- *Abbrechen*: Beendet den Dialog, die Änderungen werden verworfen.
- *Speichern*: Beendet den Dialog, die Änderungen werden gespeichert.

5 Authentifizierung

5.1 LDAP

Das „Lightweight Directory Access Protocoll“ (kurz „LDAP“) ist ein Protokoll zum Zugriff auf Verzeichnisdienste. Solche Verzeichnisdienste enthalten Informationen über Benutzer, Rechner und weitere Resourcen in einem Netzwerk. Eine spezialisierte Form eines Verzeichnisdienstes ist „Active Directory“.

Im Collax Security Gateway wird „OpenLDAP“ eingesetzt, eine Implementierung von Version 3 des LDAP. Es wird genutzt, um Benutzer, deren Passwörter, Telefonnummer, Mailadressen usw. zu speichern. Dabei handelt es sich um Konfigurationseinstellungen, die von den verschiedenen beteiligten Diensten im Collax Security Gateway abgefragt werden. Das LDAP kann aber auch für die lokalen Anwender zugänglich gemacht und genutzt werden, um ein globales Adressbuch für den Mailclient aufzubauen.

Intern werden die Daten im LDAP in einer Baumstruktur abgelegt. Die Daten werden dabei als Objekte bezeichnet, die jeweils Attribute mit Einträgen haben. Durch die Baumstruktur ist etwa der Zugriff auf eine E-Mail-Adresse über folgenden Pfad möglich: Firma – Mitarbeiter – Abteilung – Person – E-Mail-Alias. Parallel zu Mitarbeiter könnte der Objektzweig „Server“ im LDAP-Baum existieren. Bei Abteilung wäre die Aufteilung in „Vertrieb“, „Entwicklung“ usw. denkbar.

Die Adressierung eines Objekts im LDAP erfolgt über den DN („Distinguished Name“). Jeder DN besteht seinerseits aus relativen Distinguished Names (RDN) (die den Ast im LDAP-Baum darstellen). Einzelne RDN-Attribute sind etwa:

- *uid:* Benutzername (User ID)
- *dc:* Domainnamen-Komponente

- *cn:* Name (Common Name)
- *l:* Ortangabe (Location)
- *st:* Bundesland (State)
- *o:* Organisation
- *ou:* Abteilung (Organisation Unit)

Wird bereits ein LDAP im Unternehmen eingesetzt, kann der Collax Security Gateway so konfiguriert werden, dass er auf dieses LDAP zugreift. Dann können vorhandene Benutzer und Gruppen verwendet werden. Voraussetzung dafür ist jedoch, dass die genutzten Objektklassendefinitionen kompatibel sind.

5.1.1 GUI-Referenz: *LDAP*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Authentifizierung – LDAP*)

In diesem Dialog werden die Einstellungen für das LDAP vorgenommen.

Hier kann angegeben werden, ob dieses System als Master arbeiten soll (also seinen eigenen LDAP-Datenbestand erzeugt), oder ob es nur Daten aus einem anderen LDAP-Verzeichnis importieren soll.

Damit dieses System der Master für ein LDAP-Verzeichnis auf einem anderen Rechner sein kann, müssen bestimmte Voraussetzungen an die Struktur des Verzeichnisses erfüllt sein.

5.1.1.1 Tab *Grundeinstellungen*

Felder in diesem Abschnitt

- *Arbeitsmodus*: Der Betrieb des LDAP-Servers kann in drei Modi erfolgen, wobei der Serverdienst in jedem Modus lokal gestartet

wird. Es ändert sich lediglich die Art der Datenhaltung und die Art des Datenaustauschs.

Im Modus „Lokaler Master“ werden die Daten lokal im LDAP-Verzeichnis verwaltet. Durch entsprechende Gruppenberechtigungen können diese von einer LDAP-Replik oder von einem LDAP-Proxy benutzt werden.

Im Modus „Replik“ werden Daten durch den angegebenen LDAP-Server (Master) repliziert. Dies geschieht innerhalb einer andauernden Netzwerkverbindung zwischen Master und Replik. Ändern sich die Daten des Masters, werden diese sofort über die bestehende Verbindung an die Replik übermittelt und somit abgeglichen. Man spricht von „push-based synchronization“. Bei Dialup-Verbindungen kann dies nach einem definierten Zeitintervall geschehen, so dass Kosten reduziert werden können.

Der Modus „Proxy“ leitet LDAP-Anfragen prinzipiell an den LDAP-Server (Master) weiter, ohne dass Daten zwischengespeichert werden. Der Proxy nimmt Anfragen also stellvertretend entgegen und reicht diese weiter.

- *LDAP-Server*: In diesem Eingabefeld wird der Hostname des LDAP-Servers angegeben. Dieses Feld wird nur sichtbar, wenn der lokale LDAP-Server deaktiviert ist.
- *Port*: Üblicherweise läuft ein LDAP-Server auf Port 389. Hier kann ein davon abweichender Port angegeben werden.
- *Optimierung für Dialup-Verbindungen*: Sollen Daten eines entfernten LDAP-Verzeichnisses auf diesen Server repliziert werden, so kann hier auf die Synchronisation per Abholung umgestellt werden. Die Replik gleicht nach einem zu bestimmenden Zeitintervall Daten aus dem entfernten LDAP-Verzeichnis ab. Dies ist vor allem für Dialup-Verbindungen, zum Beispiel ISDN, geeignet.
- *Synchronisationsintervall*: Hier kann das Intervall angegeben werden, nach dem die Daten des LDAP-Servers mit der lokalen Replik sychronisiert werden.

- *Wurzel der Hierarchie*: Hier muss die Wurzel des Namensraumes für das LDAP-Verzeichnis angegeben werden. Als Vorgabe erscheint die Umsetzung der DNS-Domain, die unter *Netzwerk – DNS* eingetragen ist. Die DNS-Domain muss jedoch nicht zwingend als Base-DN für das LDAP-Verzeichnis verwendet werden.

  Wenn dieses System der Master für das Verzeichnis ist, werden die meisten Daten aus der lokalen Konfiguration erzeugt. Bestimmte Angaben (wie etwa Benutzerpasswörter) werden aber nur im LDAP-Verzeichnis abgelegt. Daher kann die Wurzel der Hierarchie nicht mehr nachträglich geändert werden.
- *Wurzel der Hierarchie (Base-DN/Suffix)*: Hier wird die Wurzel des Namensraumes für das LDAP-Verzeichnis angezeigt.
- *Bind-DN*: Der Bind-DN wird zum Anmelden am LDAP-Server verwendet und entspricht einem Login-Namen bei anderen Protokollen.

  Wenn ein lokales LDAP-Verzeichnis erstellt wird, wird dieser DN als „Root-DN“ eingesetzt. Ein Benutzer, der sich mit dem Root-DN angemeldet hat, unterliegt keinen administrativen Einschränkungen.

  Wird ein anderes System als LDAP-Server benutzt, muss der Account ausreichende Rechte besitzen.

  Wird das Feld leer gelassen, wurde die Vorgabe „cn=Manager, <Base-DN>“ verwendet.
- *Bind-Passwort*: Hier wird das Passwort für die Verbindung zum LDAP-Server eingetragen.

  Wird der lokale LDAP-Server verwendet, bestimmt diese Angabe das Passwort für den Root-DN (mit dem der administrative Zugriff erfolgt), andernfalls wird das Passwort für die Verbindung zum anderen Server verwendet.
- *Bind-Passwort (Wiederholung)*: Da das Passwort aus Sicherheitsgründen während der Eingabe nicht angezeigt wird, muss es hier noch einmal wiederholt werden.

- *Serverzertifikat*: Hier kann für den LDAP-Server ein Zertifikat ausgewählt werden. In der Liste sind alle installierten Zertifikate enthalten, die für den Server geeignet sind. Wird das LDAP nur innerhalb dieses Systems verwendet, ist kein Zertifikat notwendig.
- *SSL/TLS Version*: Mit der Angabe der TLS-Version kann beeinflusst werden, welches Verschlüsselungsprotokoll der verbindende Client benutzen muss, um eine entsprechend sichere Verbindung mit dem Serverdienst herzustellen.

5.1.1.2 Tab *Berechtigungen*, Abschnitt *Benutzerrechte* Felder in diesem Abschnitt

- *Zugriff auf das globale Adressbuch*: Alle Benutzer, die zu einer der aktivierten Benutzergruppen gehören, bekommen Lesezugriff auf das im LDAP-Server gespeicherte globale Adressbuch. Rechner und Netze sind von dieser Einstellung nicht betroffen.
- *Schreibzugriff auf das globale Adressbuch*: Alle Benutzer, die zu einer der aktivierten Benutzergruppen gehören, dürfen Änderungen im globalen Adressbuch vornehmen. Rechner und Netze sind von dieser Einstellung nicht betroffen.

5.1.1.3 Tab *Berechtigungen*, Abschnitt *Netzwerkzugang* Felder in diesem Abschnitt

- *LDAP-Port*: Alle Rechner und Netze, die zu einer der aktivierten Netzwerkgruppen gehören, bekommen Zugriff auf den LDAP-Server. Benutzer sind von dieser Einstellung nicht betroffen.
- *LDAP-über-SSL-Port*: Alle Rechner und Netze, die zu einer der ak-

tivierten Netzwerkgruppen gehören, bekommen verschlüsselten Zugriff via SSL auf den LDAP-Server. Benutzer sind von dieser Einstellung nicht betroffen.

Hinweis: Um den Server mit SSL ansprechen zu können, muss in den Grundeinstellungen ein entsprechendes Zertifikat ausgewählt werden.

5.2 Unterstützung von Windows-Domänen

In einer Windows-Domäne ist immer ein zentraler Server vorhanden: der „primäre Domänencontroller“ oder kurz „PDC“. An diesem erfolgt die Anmeldung der Benutzer, und die Benutzer können hier Daten ablegen (Homeverzeichnisse, Desktop-Profile usw.). In manchen Netzen wird der PDC durch einen oder mehrere Server ergänzt, die für Redundanz sorgen. Sie verfügen aber auch nur über die Konfigurationsinformationen des PDC, sie sind „Backup Domain Controller“ oder kurz „BDC“.

Der Collax Security Gateway kann auf vielfältige Weise an Windows-Domänen teilnehmen. Ist bereits ein Windows-Server vorhanden, der eine Domäne bereitstellt, kann der Collax Security Gateway ein Mitglied in dieser Domäne werden. Bei einem NT4-Server ist weitreichender Zugriff auf die Domäne möglich. Bei Servern auf der Basis von *Active Directory* (ADS) geht die Integration noch nicht ganz so weit. Aber auch bei ADS-Domänen kann auf die Benutzer- und Gruppenkonfiguration der Domäne zurückgegriffen werden, um Dienste bereitzustellen.

5.2.1 GUI-Referenz: SMB-/CIFS-Server

Auf dem Collax Security Gateway wird für die Netzwerkfunktionalität in Windows-Netzen das Softwarepaket „Samba“ verwendet. Dies wird oft als „SMB“ abgekürzt, wobei SMB eigentlich nur das Protokoll bezeichnet („Server Message Block"“).

Das „CIFS“ („Common Internet File System“) stellt eine erweiterte Version von SMB dar und wird ebenfalls vom Collax Security Gateway unterstützt.

5.2.1.1 *Windows-Support – Allgemein*

In diesem Abschnitt wird die Unterstützung für Windows-Netzwerke konfiguriert. Wird diese eingeschaltet, erscheinen in anderen Dialogen zusätzliche Optionen.

In den Benutzungsrichtlinien kann im Dialog *PDC/ADS* die Authentifizierung an einer NT-Domäne aktiviert werden.

Tab *Grundeinstellungen*
Felder in diesem Abschnitt

- *Aktivieren*: Hiermit wird die Unterstützung für Windows-Netzwerke aktiviert.

  Wird diese Option aktiviert, erscheint das System in der Netzwerkumgebung der Windows-Rechner.
- *Arbeitsgruppe oder Domäne*: Hier muss der Name der Arbeitsgruppe oder der Windows-Domäne angegeben werden.

  Aus verschiedenen Gründen sollte der Name der Arbeitsgruppe normalerweise mit dem ersten Abschnitt der DNS-Domain in Großbuchstaben übereinstimmen (für eine Domain „intern.example.com“ also die Arbeitsgruppe „INTERN“).

Tab *Berechtigungen*, Abschnitt *Netzwerkzugang* Felder in diesem Abschnitt

- *Samba-Ports*: Rechner und Netze, die zu einer aktivierten Netzwerkgruppe gehören, erhalten Zugriff, damit sie sich an der Windows-Umgebung authentifizieren können.

Tab *Optionen* Felder in diesem Abschnitt

- *Serverinformation*: Hier kann ein Kommentartext für den Server gesetzt werden. Dieser wird auf Windows-Systemen in der Netzwerkumgebung angezeigt.
- *WINS*: Wenn die Unterstützung für Windows-Netzwerke aktiviert ist, kann in dieser Liste eingestellt werden, wie sich das System gegenüber dem WINS (Windows Name Service) verhalten soll.

  Wird im Netzwerk kein WINS-Server betrieben und soll das System auch nicht als WINS-Server arbeiten, wird *Nein* eingestellt.

  Wird ein WINS-Server im Netz betrieben, kann hier *Client* eingestellt und die IP-Adresse des WINS-Servers angegeben werden.

  Wenn der Collax Security Gateway selbst als WINS-Server arbeiten soll, sollte hier *Server* eingestellt werden.

  Mit der Einstellung *Proxy* ist es möglich, Anfragen von einem Subnetz an einen WINS-Server in einem anderen Netzwerksegment weiterzureichen. Die IP-Adresse des WINS-Servers muss dann im Folgenden Feld eingetragen werden.
- *WINS-Server*: Hier wird die IP-Adresse des WINS-Servers für die Arbeitsgruppe oder die Windows-Domäne angegeben.
- *Winbind-Cachezeit (in Sekunden)*: Winbind übernimmt die Namensauflösung im Windows-Netzwerk. Hier wird eingestellt, wie lange Namen im Cache behalten werden. Gültige Werte liegen

zwischen 0 und 3600 Sekunden. Bei Eingabe von ungültigen Werten werden 300 Sekunden eingetragen.

- *Domänenseparator*: Bei Namen von Gruppen und Benutzern, die aus einer Windows-Domäne importiert werden, wird immer der Domänenname vorangestellt. Das hier ausgewählte Zeichen wird als Trennzeichen zwischen dem Domänennamen und dem Benutzer- bzw. Gruppennamen eingefügt.
- *LDAP Verbindungen signieren*: Dadurch wird die LDAP Verbindung signiert.

5.2.1.2 *System für ADS-Domäne vorbereiten*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Windows-Support – Für ADS vorbereiten*)

Die *Vorbereitung für ADS-Domäne* soll helfen, die notwendigen Einstellungen vorzunehmen und zu prüfen, damit das System erfolgreich in eine ADS-Domäne aufgenommen werden kann.

Dazu müssen verschiedene Dienste, zum Beispiel der DNS-Dienst oder das Authentifizierungs-Subsystem, korrekt konfiguriert sein; die notwendigen Einstellungen hierfür sind jedoch auf verschiedene Dialoge verteilt.

Hinweis: Durch diese Angaben werden Einstellungen in anderen Dialogen ohne weitere Warnung überschrieben. Davon betroffen sind die Einstellungen für Kerberos, DNS, Authentifizierung und Windows-Unterstützung. Angaben zu Netzwerken, Netzwerklinks oder Gruppen werden nicht geändert.

Nachdem die Konfiguration angepasst wurde, muss die neue Konfiguration aktiviert werden, bevor das System über den Dialog *Domänenbeitritt* in die Domäne aufgenommen werden kann.

Abschnitt *ADS-Einstellungen*

In diesem Abschnitt können die Einstellungen für die ADS-Domäne angegeben werden. Wenn das System noch nicht für ADS konfiguriert ist, versucht das System, diese Einstellungen automatisch zu ermitteln.

Felder in diesem Abschnitt

- *Name des Systems*: Hier wird der Name des Systems angegeben. Dieser Name wird zusammen mit der ADS-Domäne verwendet, um den FQDN des Systems festzulegen.
- *Domäne*: Hier wird die Domäne eingetragen. Diese Einstellung beeinflusst den Namen der DNS-Domäne, den FQDN dieses Systems, die Kerberos-Realm und den abgekürzten Namen der ADS-Domäne.
- *IP-Adresse des Domänencontrollers*: Hier wird die IP-Adresse des zu verwendenden Domänencontrollers angegeben. Diese Einstellung konfiguriert den DNS-Dienst.
- *IP-Adresse eines Backup-Domänencontrollers*: Hier kann ein weiterer Domänencontroller angegeben werden, der benutzt wird, wenn der primäre Domänencontroller nicht erreichbar ist.
- *DC ist WINS-Server*: Wird ein größeres Windows-Netzwerk betrieben, ist meist ein WINS-Server zur Namensauflösung im Einsatz. Durch das Aktivieren dieser Option wird der Domänencontroller als WINS-Server verwendet.

Abschnitt *Report*

In diesem Abschnitt werden die Ergebnisse der Überprüfung aller zur Integration in eine ADS-Umgebung relevanten Einstellungen des Systems angezeigt.

Felder in diesem Abschnitt

- *DNS-Server*: Der DNS-Server sollte aktiviert sein. Diese Anzeige gibt Auskunft über den aktuellen Status.
- *DNS-Suchliste*: Die ADS-Domäne sollte in der DNS-Suchliste aufgeführt sein.
- *DNS-Zone*: In der Regel verwaltet der AD-Server die DNS-Zone, die zur ADS-Domäne gehört. Auf dem Collax Security Gateway sollte eine Weiterleitung dieser DNS-Zone zum ADS-Controller eingerichtet sein.

  Hinweis: Eine Weiterleitung aller DNS-Anfragen an den ADS-Controller ist in den meisten Fällen nicht sinnvoll.
- *Systemname*: Diese Anzeige gibt Auskunft, ob der Name des Systems in der ADS-Domäne enthalten ist.
- *Windows-Unterstützung*: Hier wird angezeigt, ob die Unterstützung für Windows-Netzwerke grundsätzlich aktiviert ist.
- *WINS*: Dieses Feld zeigt, ob die Verwendung eines WINS-Servers für die Namensauflösung im Windows-Netzwerk aktiviert ist.
- *Arbeitsgruppe/Domäne*: Hier wird geprüft, ob die eingestellte Domäne als Abkürzung für die ADS-Domäne passt. Die Abkürzung sollte dem ersten Teil der ADS-Domäne entsprechen.
- *Kerberos-Server*: Der lokale Kerberos-Server muss deaktiviert sein. Hier wird geprüft, ob dies der Fall ist.
- *Kerberos-Realm*: Die eingestellte Kerberos-Realm muss dem Namen der ADS-Domäne in Großbuchstaben entsprechen. Dieses Feld enthält das Ergebnis der entsprechenden Prüfung.
- *ADS-Authentifizierung*: Gibt an, ob die Authentifizierung gegen ADS eingeschaltet ist.

5.2.1.3 *Windows-Gruppen Zuordnung*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Windows-Support – Windows-Gruppen Zuordnung*

Um Mitgliedern von Systemgruppen, die sich am lokalen PDC-Server anmelden, Windows-Berechtigungen zu vererben, kann hier die entsprechende Zuordnung vorgenommen werden. Sollen angemeldete Benutzer aus der lokalen Administrator-Gruppe ebenso Administrator-Rechte auf dem Microsoft Windows-PC erhalten, ist die Zuordnung „Domain-Admins“ zu „Administrators“ einzustellen.

Zuordnungstabelle

Diese Tabelle dient als Übersicht der zugeordneten Windows-Gruppen. Jeder Eintrag kann hier ebenso bearbeitet werden, eine Vererbung der Rechte findet nur dann statt, wenn der Collax-Server als PDC aktiviert ist.

Spalten in der Tabelle

- *Vordefinierte Windows-Gruppe*: In dieser Spalte werden die von Microsoft Windows vordefinierten NT-Domänengruppen angezeigt.
- *Lokale Gruppe*: Wenn eine Zuordnung für die Vererbung von Windows-Berechtigungen gesetzt ist, wird in dieser Spalte die entsprechende Berechtigungsgruppe des Collax Servers angezeigt. Ist keine Zuordnung gesetzt, bleibt die entsprechende Zeile leer.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion über das Kontextmenü (rechter Mausklick oder Doppelklick) kann die ausgewählte Zuordnung bearbeitet werden.

Zuordnung bearbeiten

Felder in diesem Formular

- *Vordefinierte Windows-Gruppe*: Hier wird die Windows-Gruppe angezeigt, deren Berechtigungen auf eine lokale Gruppe vererbt werden soll.
- *Lokale Gruppe*: In dieser Auswahl stehen alle bestehenden lokalen Gruppen für die Zuordnung zur Auswahl. Es kann nur eine Gruppe ausgewählt werden. Das Auswahlfeld kann auch leergelassen werden.

Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten der Gruppenzuordnung beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten der Gruppenzuordnung beenden. Die Änderungen werden gespeichert.

5.2.1.4 *Der Windows-Domäne beitreten*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Windows-Support – Domänenbeitritt*)

Hier kann das System bei einem Windows-Domänencontroller angemeldet und in die Domäne aufgenommen werden.

Felder in diesem Dialog

- *Benutzerdatenbank*: Hier wird angezeigt, ob die Benutzerdatenbank lokal oder auf einem PDC abgelegt ist.
- *Hinweis:* In diesem Feld erscheint ein Hinweis, wenn ein Domänenbeitritt nicht möglich ist. Meistens wurden in diesem Fall noch nicht alle Einstellungen passend vorgenommen. Im angezeigten Text finden sich weitere Hinweise dazu.
- *Domäne*: Hier wird die auf dem System eingestellte Domäne angezeigt.
- *Administrator-Account*: Hier muss der Benutzername eines Administrator-Accounts auf dem Domänencontroller angegeben werden. Das Feld kann leer bleiben, wenn auf dem DC bereits ein Maschinenaccount angelegt wurde.
- *Passwort*: Hier muss das Passwort für den Administrator-Account angegeben werden. Auch dieses Feld kann leer bleiben, wenn der Maschinenaccount bereits angelegt wurde.

  Hinweis: Das Kennwort wird einzig für die Anmeldung des Systems beim Domänencontroller genutzt und nicht lokal gespeichert.
- *DC*: Hier ist der Hostname des Domänencontrollers anzugeben.

Aktionen für diesen Dialog

- *Anmelden*: Diese Aktion versucht, mit den eingestellten Werten eine Anmeldung am Domain-Controller durchzuführen.
- *Abmelden*: Diese Aktion meldet das System am Domänencontroller ab.

5.2.2 GUI-Referenz: *Kerberos*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Authentifizierung – Kerberos*)

Kerberos ist ein komplexes Verfahren zur Authentifizierung von Benutzern und Servern in einem ungesicherten TCP/IP-Netzwerk. Benutzer und Dienste werden mit Hilfe eines speziellen Netzwerkdienstes, des KDC (Key Distribution Center), authentifiziert. Der KDC stellt die vertrauenswürdige Instanz im Netz dar. Bei Kerberos werden keine Passwörter im Klartext über das Netzwerk übertragen.

Wenn eine *lokale* Benutzerdatenbank eingestellt wurde, kann zusätzlich der KDC auf dem System aktiviert werden. Die meisten Unix-Varianten (und auch Linux) können Kerberos zur Authentifizierung nutzen. Windows 2000 unterstützt ebenfalls Kerberos, benötigt jedoch eine manuelle Konfiguration.

Beim Aufbau einer Verbindung erfolgt eine Authentifizierung des Clients und des Servers gegen den KDC. Auch der KDC authentifiziert sich gegenüber Client und Server. Möchte der Client eine Verbindung zum Server aufbauen, identifiziert er sich am KDC und erhält im Gegenzug ein „Ticket“, eine Art elektronische Eintrittskarte. Mit diesem kann er die Verbindung zum Server aufbauen. Dadurch ist ein „Single-Sign-On“ möglich, bei dem sich der Benutzer nur einmal innerhalb der Sitzung authentifiziert und dennoch verschiedene Dienste (Server) nutzen kann.

5.2.2.1 Tab *Grundeinstellungen*

Felder in diesem Abschnitt

- *Lokalen Server aktivieren*: Diese Option aktiviert den Kerberos-Dienst auf diesem System.

- *UDP verwenden*: Wenn diese Option aktiviert ist, werden bei der Authentifizierung UDP-Datenpakete anstelle von TCP-Paketen verwendet.

  Ist diese Option nicht aktiviert, werden TCP-Pakete genutzt, um mögliche Probleme mit bestimmten KDCs zu vermeiden, die zu große Antwortpakete verschicken. Dies kann zum Beispiel geschehen, wenn ein Windows ADS-Server Tickets für Benutzer herausgibt, die in sehr vielen Gruppen Mitglied sind.

  Da UDP in der Regel schneller als TCP ist, sollte diese Option aktiviert werden, wenn ein KDC ohne ADS verwendet wird oder wenn sich der ADS-Controller an einem entfernten Standort befindet und das angesprochene Problem nicht auftritt.
- *KDCs*: Hier kann eine Liste von KDCs für die Kerberos-Realm angegeben werden. Die einzelnen Einträge werden durch ein Komma oder Leerzeichen voneinander getrennt.

  Dieses Feld kann leer bleiben, wenn der oder die KDCs im DNS aufgeführt sind.
- *Kerberos-Realm*: Die Kerberos-Realm ist der Bereich, in dem eine Authentifizierung gültig ist. Benutzer innerhalb eines Bereichs können sich gegenüber jedem Dienst auf einem Rechner in der Realm ausweisen.

  Aus verschiedenen Gründen sollte der Name der Realm normalerweise mit der DNS-Domain in Großbuchstaben übereinstimmen (für die Domain „intern.example.com“ also die Realm „INTERN.EXAMPLE.COM“).

5.2.2.2 Tab *Berechtigungen*

Felder in diesem Abschnitt

- *Authentifizierung über KDC*: Alle Rechner und Netze, die zu einer der aktivierten Gruppen gehören, dürfen auf den KDC zugreifen. Benutzer sind von dieser Einstellung nicht betroffen.

  Diese Berechtigung ist die Voraussetzung dafür, dass sich Benutzer und Server gegenseitig authentifizieren können.

  Das Feld wird nur angezeigt, wenn auf diesem System ein KDC betrieben wird.
- *Administration Kerberos-Dienst*: Alle Rechner und Netze, die zu einer der aktivierten Gruppen gehören, bekommen Zugriff auf den Kerberos-Administrations-Dienst. Benutzer sind von dieser Einstellung nicht betroffen.

  Diese Berechtigung ist nur für solche Rechner notwendig, die in die Kerberos-Realm aufgenommen werden sollen.

  Das Feld wird nur angezeigt, wenn auf diesem System ein KDC betrieben wird.

5.2.3 GUI-Referenz: *PDC/ADS*

In diesem Dialog wird festgelegt, wo die Prüfung von Benutzerpasswörtern erfolgen soll. Die Voreinstellung sieht die Verwendung einer lokalen Benutzerdatenbank vor.

Alternativ können die Benutzer und deren Passwörter auf einem anderen System verwaltet und die Daten über ein entsprechendes Protokoll importiert werden.

5.2.3.1 *PDC/ADS*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Windows-Support – PDC/ADS*)

Felder in diesem Dialog

- *Benutzerdatenbank*: Zur Authentifizierung von Benutzern können verschiedene Server befragt werden.

  Mit der Einstellung *Lokal* wird die Benutzerdatenbank auf diesem System verwendet. Alle Benutzerinformationen sind im LDAP-Verzeichnis gespeichert.

  Mit der *NT-Domäne* muss dieses System in eine bestehende NT-Domäne aufgenommen werden. Danach kann die Authentifizierung gegen den primären Domänencontroller („PDC“) durchgeführt werden.

  Moderne Windows-Domänen verwenden *Active Directory Service* („ADS“) als interne Datenbank. Mit der Einstellung *ADS-Mitglied* kann dieses System den ADS befragen. Es muss dazu in die ADS-Domäne aufgenommen werden.
- *NT-/ADS-Domäne*: Hier wird die Windows-NT- oder ADS-Domäne angezeigt, die in den Netzwerkeinstellungen konfiguriert wurde.
- *Benutzerabhängiges Anmeldeskript verwenden*: Diese Option darf nicht aktiviert werden, wenn bereits ein anderes System im Netzwerk als PDC betrieben wird. Andernfalls kann es dazu kommen, dass sich die Benutzer nicht mehr an der Domäne anmelden können.
- *Active Directory Server*: Wenn dieses System als Mitglied einer ADS-Domäne konfiguriert ist, wird die Authentifizierung ausschließlich am ADS-Server durchgeführt. In diesem Feld kann der Name des ADS-Servers eingegeben werden. Bleibt das Feld leer, wird der ADS-Server der Domäne automatisch gesucht.

- *PDC*: Hier wird der Name des PDC für die Domäne angegeben. Dieser wird für die Authentifizierung von Passwörtern kontaktiert. Bleibt das Feld leer, sucht das System automatisch nach einem PDC für die Domäne.

  Hinweis: In diesem Feld muss der *NetBIOS*-Name des PDC angegeben werden. Dieser ist nicht immer identisch mit dem DNS-Namen.
- *BDC*: Hier kann eine Liste von Backup-Domain-Controllern für die NT-Domäne angegeben werden. Die Angabe in diesem Feld kann IP-Adressen oder Namen der Server enthalten. Die Liste muss mit Komma und Leerzeichen getrennt werden: NT-BDC, NT-BDC1, NT-BDC2
- *Benutzer aus anderen Domänen zulassen*: Wird diese Option aktiviert, können sich Benutzer aus anderen Domänen am System anmelden. Voraussetzung ist, dass eine Vertrauensstellung zwischen den Domänen besteht.

  Durch das Aktivieren dieser Option wird der Domänencontroller der entfernten Domäne zur Authentifizierung kontaktiert. Dies kann bei großen Domänen und/oder langsamen Netzwerkverbindungen zu Problemen führen.

  Aus Sicherheitsgründen sollte eine Aktivierung dieser Option gründlich geprüft werden.
- *Active Directory-Proxy aktivieren*: Ist ein Collax Security Gateway Mitglied eines Active Directory kann mit dieser Option die Funktion gestartet werden, um benutzerbezogene Daten aus dem Active Directory ins lokale Benutzerverzeichnis zu kopieren. Diese Daten aus dem Active Directory werden regelmäßig überprüft, und, falls erforderlich, werden Änderungen aus dem Active Directory lokal übernommen.

  Diese Funktion kann benutzt werden, falls für lokale Dienste bestimmte Benutzerdaten aus dem Active Directory ausgelesen werden müssen.

Beim ersten Start des AD-Proxy kann, je nach Größe des AD-Verzeichnisses, das Synchronisieren der Benutzerdaten einige Minuten dauern.

- *Windows LDAP-Administrator*: Hier muss der Benutzer angegeben werden, der Leseberechtigung auf das Active Directory hat.
- *Passwort*: Hier wird das Passwort des Benutzers eingegeben.

6 Verschlüsselung

6.1 Einführung

Verschlüsselung dient der sicheren Übertragung von Information. Bereits im Altertum wurden erste Verschlüsselungsverfahren eingesetzt. Dabei wurden Ersetzungsvorschriften verwendet, die geheimgehalten werden mussten. Ende des 19. Jahrhunderts formulierte ein Wissenschaftler den Grundsatz, dass die Sicherheit eines kryptographischen Verfahrens allein auf dem Schlüssel basiert. Das Verfahren selbst kann offengelegt werden. In den letzten 60 Jahren machte die „Kryptographie“ durch zunehmend bessere technische Möglichkeiten rasante Fortschritte.

Heutzutage ist neben der Verschlüsselung zur Wahrung der „Vertraulichkeit“ auch die Sicherung der „Integrität“ wichtig. Beides schützt die Information vor unbefugtem Zugriff von außen, d. h. vor Einsichtnahme und vor Manipulation. Eine weitere wichtige Anforderung ist die „Authentizität“, d. h. die Gewissheit darüber, wirklich mit der richtigen Person Daten auszutauschen und nicht auf eine fingierte Information hereinzufallen.

Die ursprüngliche Information, die geschützt werden soll, wird als „Ursprungstext“ bezeichnet. Die verschlüsselte Information wird „Chiffriertext“ genannt. Die Transformation von Ursprungstext in Chiffriertext bezeichnet man als „Verschlüsselung“ oder „Chiffrierung“. Der Zurückwandlung vom Chiffriertext in den Ursprungstext ist die „Entschlüsselung“ oder „Dechiffrierung“. Dechiffrierung findet auch statt, wenn ein Angreifer mit eigenen Methoden eine Entschlüsselung vornehmen kann.

Zunächst wurden „symmetrische Verfahren“ entwickelt, bei denen

derselbe „Chiffrierschlüssel“ für die Verschlüsselung und später für die Entschlüsselung verwendet wird. Der offensichtliche Schwachpunkt dieses Verfahrens ist, dass der Austausch des Chiffrierschlüssels zum Kommunikationspartner gesichert erfolgen muss. Nachteilig ist zudem, dass mit jedem neuen Partner ein neuer Schlüssel ausgehandelt werden muss, was die Anzahl der Schlüssel schnell in die Höhe treibt. 1977 wurde mit „DES“ („Data Encryption Standard“) ein symmetrisches Verfahren als Standard für US-amerikanische Behörden eingeführt.

Diese Nachteile dieses Verfahrens werden durch „asymmetrische Verfahren“ umgangen; sie werden auch als „Public-Key-Kryptographie“ bezeichnet. Hierbei wird für jeden Teilnehmer ein „Schlüsselpaar“ erzeugt. Die eine Komponente ist der öffentliche Schlüssel („Public Key“), die andere der geheime, private Schlüssel („Private Key“). Entscheidend dabei ist, dass der zweite Schlüssel nicht einfach aus dem ersten Schlüssel errechnet werden kann. RSA ist ein verbreitetes asymmetrisches Verfahren.

Bei der Schlüsselerzeugung wird daher meist auf das Problem der Zerlegung einer natürlichen Zahl in ihre Primfaktoren zurückgegriffen: Die Zahl 2117 ist das Produkt der beiden Primzahlen 29 und 73. Die Zerlegung der Zahl 2117 in ihre Primfaktoren ist sehr aufwendig. Der umgekehrte Weg, zwei oder mehr Primzahlen auszuwählen und deren Produkt zu bilden, jedoch nicht. In der Praxis werden Primzahlen mit 300 und mehr Stellen verwendet, was auch für leistungsfähige Computersysteme eine deutliche Hürde darstellt (mit den heute bekannten Methoden wird die Dauer einer solchen Faktorisierung auf Millionen von Jahren geschätzt). Auf dieser Grundlage werden die beiden Schlüsselanteile aus einem gemeinsamen Satz an Primzahlen erzeugt. Dadurch, dass eine Zerlegung in die einzelnen Primbestandteile derzeit nicht möglich ist, kann der zugehörige zweite Schlüssel nicht berechnet werden.

Um zwischen zwei Teilnehmern eine Information verschlüsselt auszutauschen, benötigt der Absender den öffentlichen Schlüssel des Empfängers. Mit diesem verschlüsselt er den Ursprungstext und überträgt den Chiffretext an den Empfänger. Jeder, der diesen Chiffretext abfängt, sollte nur Zugriff auf den öffentlichen Schlüssel des Empfängers haben. Mit diesem ist eine Dechiffrierung jedoch nicht möglich. Nur der Empfänger verfügt über den passenden privaten Schlüssel, mit dem er die Information entschlüsseln kann.

Die Integrität der Information kann durch eine Prüfsumme garantiert werden. Dazu stehen verschiedene Algorithmen zur Verfügung, einer der bekanntesten ist MD5. Der Absender der Information berechnet dazu vor dem Versenden eine Prüfsumme über die Information. Diese Prüfsumme verschlüsselt er mit seinem privaten Schlüssel und fügt sie der Übertragung bei. Der Empfänger der Nachricht kann seinerseits eine Prüfsumme berechnen und mit Hilfe des öffentlichen Absenderschlüssels die Prüfsumme des Absenders entschlüsseln. Sind beide identisch, liegt die Originalinformation vor. Sind sie unterschiedlich, muss die Information auf dem Zwischenweg modifiziert worden sein.

Hier zeigt sich sehr deutlich das Zusammenspiel von Public und Private Key für Verschlüsselung und Integritätssicherung. Der Vorteil dieses Verfahrens ist der unkritische Schlüsselaustausch: Der Kommunikationspartner benötigt immer nur den eigenen öffentlichen Schlüssel. Dieser ist aber öffentlich, also nicht besonders schützenswert.

Nun muss als dritte Anforderung die Sicherung der Authentizität umgesetzt werden. Sind die beiden Kommunikationspartner miteinander bekannt, können sie die öffentlichen Schlüssel persönlich austauschen. So können sie sicher sein, wirklich mit der richtigen Gegenseite zu kommunizieren und nicht mit einem Angreifer, der seinen öffentlichen Schlüssel untergeschoben hat.

6.1.1 Zertifikate

Zertifikate sind in diesem Zusammenhang eine Art Transporthülle für asymmetrische Schlüssel und Informationen über den Besitzer des Schlüsselpaares. Beim Einlesen eines Zertifikats mit öffentlichem Schlüssel werden Name, Anschrift und weitere Informationen über den Inhaber des Zertifikats angezeigt. So kann sichergestellt werden, dass der Schlüssel des richtigen Kommunikationspartners verwendet wird.

Diese Informationen können jedoch auch gefälscht werden. Um diese Gefahr auszuschließen, kann jeder sein persönliches Zertifikat von einer Art elektronischem Notar „signieren“ lassen. Eine solche „Certificate Authority“ („CA“) prüft zunächst den Inhaber auf Echtheit (Lichtbildausweis, Handelsregisterauszug, usw.) und berechnet dann über den öffentlichen Schlüssel des Zertifikats eine Prüfsumme. Die Prüfsumme wird mit dem privaten Schlüssel der CA verschlüsselt und dem Zertifikat beigefügt.

Beim Verwenden eines auf diese Weise signierten Zertifikats muss wiederum die Prüfsumme ermittelt, die beigefügte Prüfsumme der CA mit dem öffentlichen Schlüssel der CA dechiffriert und beide miteinander verglichen werden. Sind sie identisch, ist garantiert, dass dieses Zertifikat tatsächlich dem angegebenen Inhaber zugeordnet ist.

Dieses Verfahren funktioniert nur, wenn die Signatur von einer vertrauenswürdigen CA ausgestellt wurde. Dies kann entweder eine eigene CA im Unternehmen oder eine externe sein, deren öffentlicher Schlüssel auf vertrauenswürdigem Wege besorgt werden kann. In modernen Webbrowsern beispielsweise sind die CA-Zertifikate der gängigen Anbieter solcher CA-Dienste hinterlegt. Damit ist der Anwender von der Beschäftigung mit Zertifikaten entbunden, üblicherweise schließt sich beim Aufbau einer verschlüsselten Verbindung

ein symbolisches Schloss. Achtung: In solchen Browsern können weitere CA-Zertifikate nachinstalliert werden. Der PC im Strandcafé von St. Tropez kann sich so schnell als falscher Freund erweisen.

Steht keine CA zur Verfügung, können auch „selbstsignierte“ Zertifikate erstellt werden. Auch solche Zertifikate können nicht automatisch auf ihre Vertrauenswürdigkeit hin überprüft werden.

Um den privaten Schlüssel eines Zertifikats zu schützen, kann dieser mit einer „Passphrase“ gesichert werden. Dieses Passwort muss dann jedes Mal, wenn mit dem privaten Schlüssel gearbeitet werden soll, eingegeben werden. Beim Einsatz eines Zertifikats für einen Server (Webserver o. ä.) darf keine Passphrase gesetzt sein. Ist dies doch der Fall, muss diese bei jedem Start des Servers eingegeben werden.

6.1.2 Aufbau eines X.509-Zertifikats

Ein häufig genutztes Format für Zertifikate ist der X.509-Standard.

```
Certificate:
    Data:
       Version: 3 (0x2)
       Serial Number: 1 (0x1)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: CN=ca@untrustworthy.example.com, C=DE,
          ST=Bayern, L=Muenchen, O=Untrustworthy Ltd.,
          OU=Certificate Authority/emailAddress=
          ca@untrustworthy.example.com
       Validity
          Not Before: Nov 11 10:14:58 2005 GMT
          Not After : Apr 10 10:14:58 2007 GMT
       Subject: C=DE, ST=NRW, O=Elektro Britzel,
          OU=Netzwerk, CN=www.elektro-britzel.de
       Subject Public Key Info:
```

```
          Public Key Algorithm: rsaEncryption
          RSA Public Key: (1024 bit)
            Modulus (1024 bit):
               00:c6:a5:4f:6b:cd:c3:b6:63:3f:6f:eb:a8:7c:13:
               3f:25:7e:ce:a1:45:09:cb:3c:23:33:c6:0f:3c:b1:
               7c:68:19:02:ab:80:7c:f9:e2:e4:fc:a1:1f:c5:ae:
               6f:76:fe:f8:e7:90:16:4b:3a:ab:d4:24:16:18:24:
               7a:bf:da:1f:45:d0:18:1a:1c:5e:b2:00:02:d2:e8:
               77:2e:99:c9:01:b8:a0:33:ed:77:ed:6b:47:ad:97:
               33:ae:97:18:f3:3e:cd:72:2b:bc:84:ad:cf:69:22:
               d1:f8:15:11:f0:29:bc:c2:6d:20:5c:6c:fa:d3:c0:
               79:7c:bd:4e:7c:df:d6:28:db
            Exponent: 65537 (0x10001)
       X509v3 extensions:
          Netscape Comment:
            Zertifikat fuer den Webserver der Firma Britzel
          X509v3 Basic Constraints:
            CA:FALSE
          X509v3 Key Usage:
            Digital Signature, Non Repudiation,
            Key Encipherment
          Netscape Cert Type:
            SSL Server
   Signature Algorithm: md5WithRSAEncryption
      3b:5d:ca:8a:01:14:e5:a4:7e:bb:12:e0:ff:7f:f6:7b:8f:5e:
      72:7d:eb:64:57:89:a1:97:2e:f8:58:ee:40:9e:7d:62:37:d5:
      1d:97:fb:43:70:37:26:24:09:15:59:50:2b:12:7b:ce:0f:e2:
      b5:d7:27:54:42:f0:c2:74:2e:14:5a:b2:5b:37:4c:cc:f7:4f:
      7e:95:b7:b1:04:20:f5:1b:d8:9e:f1:57:cd:b2:9c:ee:b4:5c:
      03:ff:36:0e:7c:60:ad:e2:a5:fa:96:c7:a1:f8:e0:61:5e:18:
      af:3f:ee:ee:0b:dd:2c:77:ce:40:15:34:b0:6c:a1:37:21:75:
      fc:8f
Certificate purposes:
SSL client : No
SSL client CA : No
SSL server : Yes
SSL server CA : No
Netscape SSL server : Yes
Netscape SSL server CA : No
```

```
S/MIME signing : No
S/MIME signing CA : No
S/MIME encryption : No
S/MIME encryption CA : No
CRL signing : No
CRL signing CA : No
Any Purpose : Yes
Any Purpose CA : Yes
OCSP helper : Yes
OCSP helper CA : No
```

Ein Zertifikat nach X.509 ist nach dem Schema Zertifikatsinhalt (Data), Signaturalgorithmus und Signatur aufgebaut.

- Version: Version des eingesetzten X.509-Standards. Üblicherweise heute Version 3.
- SerialNumber: Eine eindeutige Nummer des Zertifikats, die von der aussstellenden CA vergeben wird.
- Signature Algorithm: Algorithmus, mit dem der Signaturwert von der ausstellenden Instanz errechnet wurde. Dieser muss mit dem Signaturalgorithmus im Zertifikat übereinstimmen.
- Issuer: Die Zertifizierungsstelle, die die Authentizität der Person oder des Systems bestätigt.
- Validity: Gültigkeitszeitraum des Zertifikats.
- Subject: Informationen über die Person oder das System, für welche das Zertifikat erstellt wurde. Dabei enthält „C“ (Country) das Länderkürzel, „ST“ (State) das Bundesland, „O“ (Organisation) den Namen des Unternehmens oder der Einrichtung, „OU“ (Organisation Unit) die Abteilung und „CN“ (Common Name) den exakten Inhaber des Zertifikats. Für den Common Name wird üblicherweise bei einer Person die E-Mail-Adresse und bei einem Computersystem der FQDN eingesetzt. Nicht alle Felder müssen ausgefüllt sein, der CN sollte jedoch immer gesetzt sein.

- Subject Public Key Info: Der öffentliche Schlüssel. Der private Schlüssel ist in einem Serverzertifikat nicht enthalten.
- IssuerUniqueID: Ein optionaler, eindeutiger Identifikator des Zertifikatsausstellers, mit Version 2 eingeführt.
- SubjectUniqueID: Ein optionaler, eindeutiger Identifikator des Zertifikatsinhabers, mit Version 2 eingeführt.
- Extensions: Weitere Informationen, ab Version 3 nutzbar.

Im X.509-Standard ist ab Version 3 die Verwendung von Erweiterungen („Extensions“) definiert. Mit diesen lassen sich zusätzliche Informationen in einem Zertifikat abspeichern. Manche Erweiterungen sind im Standard festgelegt (etwa „KeyUsage“), es können aber auch private Erweiterungen definiert werden, die nur innerhalb einer bestimmten Nutzergruppe sinnvoll sind.

Folgende Erweiterungen gehören zum Standardumfang:

- AuthorityKeyIdentifier: Verfügt eine CA selbst über mehrere Zertifikate, gibt sie in diesem Feld an, mit welchem der Zertifikate das vorliegende signiert wurde. Dadurch kann zur Überprüfung der Prüfsumme der entsprechende Public Key der CA ausgewählt werden.
- SubjectKeyIdentifier: Falls der Inhaber des Zertifikats über mehrere Zertifikate verfügt, wird hier der genaue öffentliche Schlüssel angegeben. Handelt es sich beim Zertifikat um ein CA-Zertifikat, muss hier der Wert angegeben werden, den die CA beim Signieren ins Feld AuthorityKeyIdentifier schreibt. Bei Endbenutzerzertifikaten kann das Feld angegeben werden. Dies ist nützlich, falls das gleiche Ursprungszertifikat von mehreren CAs signiert wurde. Dann existieren mehrere Zertifikate mit gleichem Public Key, die über dieses Feld alle aufgefunden werden können.
- KeyUsage: Die Verwendung des Schlüssels kann hiermit beispielsweise nur auf die Überprüfung digitaler Signaturen oder zur verschlüsselten Datenübertragung eingeschränkt werden.

- ExtendedKeyUsage: Erweiterung zu „KeyUsage“, ist als Erweiterungsmöglichkeit für Einrichtungen gedacht, die weitere Einsatzzwecke zur Nutzung dieses öffentlichen Schlüssels angeben wollen.
- PrivateKeyUsagePeriod: Hiermit kann eine von der Gültigkeitsdauer des Zertifikats abweichende Gültigkeitsdauer für den privaten Schlüssel angegeben werden.
- CertificatePolicies: Gibt einen Indikator an, welcher auf die genauen Richtlinien verweist, unter deren Verwendung das Zertifikat erzeugt wurde. Die CA muss diese Richtlinien gesondert veröffentlichen. Es gibt auch die Möglichkeit, mit Verweis auf „any policy“ eine generische Richtlinie zu referenzieren. Dies wiederum kann über das Feld InhibitAnyPolicy auch gesperrt werden.
- PolicyMappings: Eine Auflistung von Zertifizierungsrichtlinien, die als gleichwertig zur verwendeten angesehen werden.
- SubjectAlternativeName: Hier können alternative Angaben über den Inhaber des Zertifikats gemacht werden. Bei einem Computersystem sind dies etwa weitere FQDNs oder die IP-Nummer.
- IssuerAlternativeName: Ein alternativer Name für die unterzeichnende CA. Hier wird oft eine Mailadresse angegeben.
- SubjectDirectoryAttributes: Weitere Angaben über den Zertifikatinhaber, etwa dessen Nationalität.
- BasicConstraints: Hier wird angegeben, ob das vorliegende Zertifikat selbst einen CA-Status hat, ob es also zum Signieren weiterer Zertifikate verwendet werden darf. Ist dies der Fall, kann zusätzlich der nachfolgende Zertifizierungspfad beschränkt werden.
- NameConstraints: Hiermit kann der Namespace, also etwa die im CN eingesetzten Domains, für nachfolgende Zertifikate beschränkt werden. Ein Unternehmen kann so etwa eine CA nur für die eigene Internetdomain betreiben.

- PolicyConstraints: Hier können Beschränkungen der Richtlinien für nachfolgende Zertifikate erwirkt werden.
- CrlDistributionPoints: Über dieses Feld wird angegeben, wo die Sperrlisten (CRLs) abgerufen werden können, die dieses Zertifikat für ungültig erklären können.
- FreshestCRL: Analog zu der Definition der Sperrlisten kann hier angegeben werden, wo die letzten Änderungen zu einer CRL abgerufen werden können.

6.1.3 Schlüssellänge

Die Sicherheit eines Schlüssels wird wesentlich durch die eingesetzte Schlüssellänge bestimmt. Bei einer Schlüssellänge von 2048 Bit werden Primzahlen von etwa 1024 Bit Länge benutzt. In diesem Bereich existieren etwa 10 hoch 305 verschiedene Primzahlen, mehr als es im gesamten Universum Atome gibt.

Man geht heute davon aus, dass Schlüssellängen von 2048 Bit bis etwa ins Jahre 2015 für Public-Key-Verfahren bei der Verwendung in Regierungseinrichtungen eine ausreichende Sicherheit gegen Angriffe bieten.

1024 Bit Schlüssellänge wurden im Jahre 2000 für Privatpersonen als ausreichend sicher angenommen. 1536 Bit gelten im Jahre 2006 als ausreichend für den Einsatz in Unternehmen.

Noch sicherer sind jeweils größere Schlüssellängen. Üblicherweise werden bis 4096 Bit unterstützt.

Bei symmetrischen Schlüsseln hingegen wird eine sichere Verschlüsselung ab ca. 100 Bit Schlüssellänge erreicht. Üblicherweise werden Schlüssellängen von 128 bis 256 Bit verwendet.

Der Faktor 10 in der Schlüssellänge gilt auch für den Aufwand zum (de-)chiffrieren. Auch mit immer leistungsfähigeren Computer-

systemen werden daher zum Austausch von Daten bevorzugt symmetrische Algorithmen wie AES eingesetzt. Asymmetrische Verfahren bieten hingegen eine höhere Sicherheit bezüglich des Schlüsselaustauschs. Sie werden daher eingesetzt, um beim Verbindungsbeginn eine gesicherte Übertragung aufzubauen. Dann wird ein zufällig generierter symmetrischer Schlüssel erzeugt und verschlüsselt zur Gegenseite übertragen. Dieser wird für die folgende Nutzdatenübertragung verwendet.

6.1.4 Laufzeit

Die Laufzeit jedes Zertifikats ist begrenzt. Üblicherweise werden Zertifikate mit einer Laufzeit von ein oder zwei Jahren erstellt. Diese Begrenzung sorgt im Fall des Verlusts eines Zertifikats für eine automatische Sperre nach Ablauf der Zeitspanne.

Bei einer CA sind alle abgeleiteten Zertifikate maximal so lange gültig wie die CA selbst. Hierbei sollte also eine längere Laufzeit (meist zehn Jahre) verwendet werden.

Zu beachten ist, dass Zertifikate nur für ein Zeitfenster gelten, also immer von einem Zeitpunkt bis zu einem anderen. Dies kann bei frisch erzeugten Zertifikaten auf zwei Systemen mit unterschiedlicher Uhrzeit zu Problemen führen.

6.1.5 Sperren eines Zertifikats

Es ist nie auszuschließen, dass ein vollständiger Schlüsselsatz aus Public und Private Key in falsche Hände gerät, etwa durch Diebstahl eines Notebooks. In diesem Fall muss der Inhaber des Schlüssels einen neuen Schlüsselsatz erstellen (lassen) und seinen

Public Key allen Kommunikationspartnern mitteilen. Der verlorene, kompromittierte Schlüssel existiert jedoch parallel weiter und scheint weiterhin gültig. Nach Ablauf der Laufzeit ist der kompromittierte Schlüssel irgendwann jedoch wertlos.

Bei der Nutzung einer CA bietet sich die Möglichkeit, einen kompromittierten Schlüssel noch vor Ablauf seiner eigentlichen Laufzeit zu sperren bzw. „zurückzuziehen". Dieser Vorgang kann ebenso wie die Signierung nur durch einen autorisierten Mitarbeiter der CA durchgeführt werden. Der zu sperrende Schlüssel wird widerrufen und in die sog. „Certificate Revocation List" CRL („Liste zurückgezogener Zertifikate") aufgenommen.

Problematisch dabei ist, dass jeder Teilnehmer unterhalb einer CA vor der Verwendung eines Schlüssels immer aktuell bei der CA anfragen muss, ob das zugehörige Zertifikat in der Sperrliste auftaucht. Auch wenn dies durch Software durchgeführt werden kann, geschieht es in der Praxis nur selten. Im Collax Security Gateway wird diese Überprüfung bei gleichzeitigem Einsatz als CA und als VPN-Einwahlpunkt immer durchgeführt.

6.1.6 Praktische Anwendung

Zertifikate können im Collax Security Gateway genutzt werden, um die Sicherheit von einigen Diensten im Internet zu verbessern. Das bekannteste Verfahren ist HTTPS zur verschlüsselten Übertragung von Webseiten. Damit dieses Verfahren angewendet werden kann, muss für den Webserver ein Zertifikat erstellt und eingebunden werden. Dies ist eine Voraussetzung zur Nutzung des User-Portal „Web-Access" im Collax Security Gateway.

Im E-Mail-Verkehr wird bei einigen Protokollen die Authentifizierung im Klartext übertragen (z. B. bei POP3). Mit Hilfe von

Verschlüsselung können diese Zugangsdaten sicher übermittelt werden. Auch hierfür muss für den Server ein Zertifikat erstellt und eingebunden werden. Solchen durch Verschlüsselung verbesserten Protokollen wird eine neue Bezeichnung zugewiesen (in diesem Beispiel POP3S). Achtung: Hier wird jeweils nur die Anmeldung am Server gesichert. Die E-Mail selbst wird weiter unverschlüsselt über das Internet übertragen.

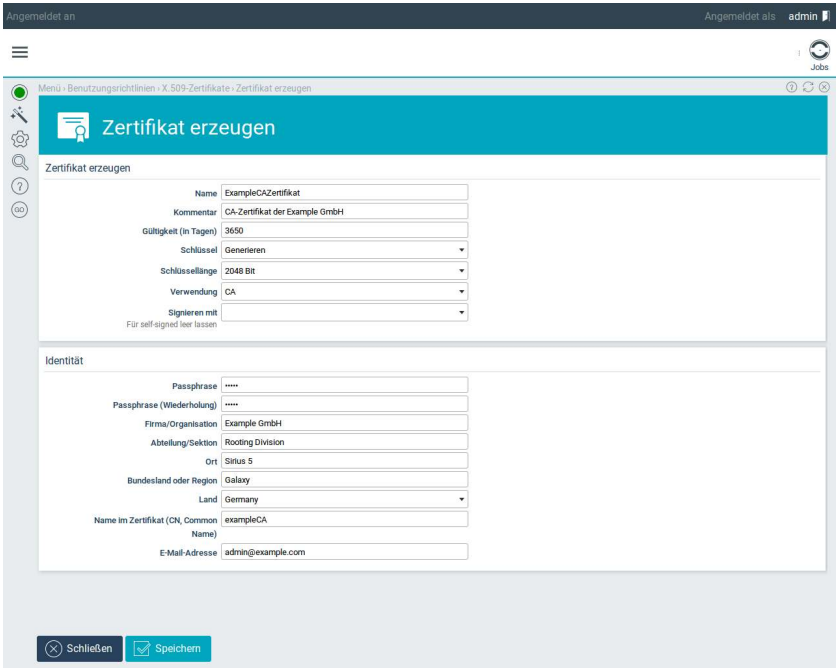
Natürlich lässt sich auch der Austausch von E-Mails zwischen zwei Personen durch Verschlüsselung schützen. Um den E-Mail-Verkehr zu verschlüsseln, müssen beide Beteiligte in ihrem Computer spezielle Software installieren (etwa PGP oder S/MIME), entsprechende Zertifikate für sich ausstellen lassen und die öffentlichen Schlüssel austauschen. Sie können dann Nachrichten verschicken. Hierbei wird der eigentliche Inhalt der E-Mail vor dem Versenden verschlüsselt und als „Buchstabensalat“ in einer normalen E-Mail übertragen. Die Mailserver, die die E-Mail übertragen, müssen also nicht speziell auf die Verschlüsselung abgestimmt werden. Virenscanner, die auf manchen Mailservern laufen, können jedoch den eigentlichen Inhalt der E-Mail ebenfalls nicht untersuchen. Der Inhalt kann erst auf dem Computer des Empfängers dechiffriert werden.

Für die sichere Datenübertragung zwischen zwei oder mehr Standorten über das Internet können VPN-Tunnel verwendet werden. In einem solchen Tunnel werden alle Daten durch Verschlüsselung gesichert. Über Zertifikate kann die Authentizität der Gegenstelle garantiert werden.

6.2 Schritt für Schritt: Erstellen eines Serverzertifikats

Um bestimmte Dienste durch Verschlüsselung abzusichern, muss für den Collax Security Gateway ein eigenes Zertifikat erzeugt werden. Dies geschieht in den *Benutzungsrichtlinien* unter *Zertifikate*. Hier können Zertifikate nach X.509-Standard und einfache RSA-Schlüssel verwaltet werden. Für die Serverdienste werden *X.509-Zertifikate* benötigt.

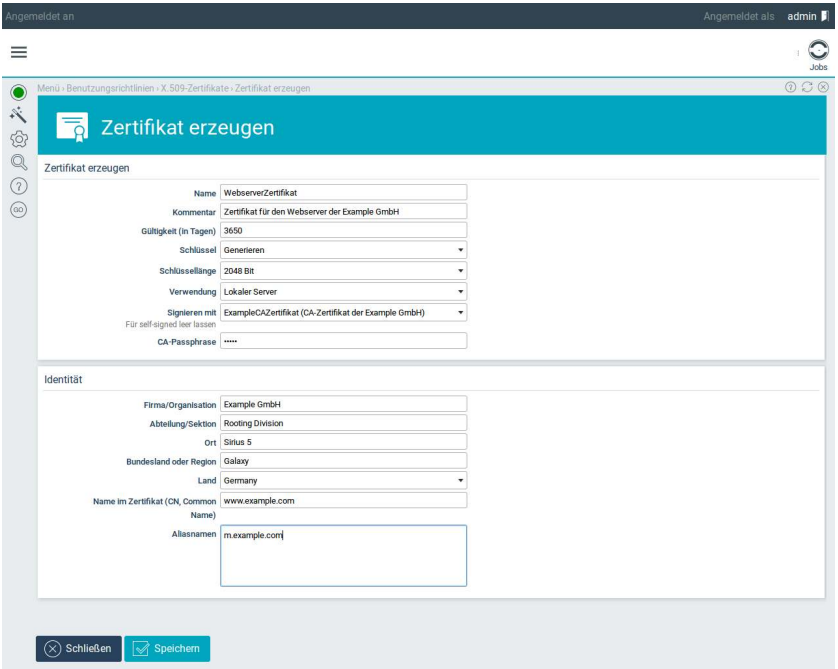
Zunächst wird eine eigene CA erstellt.



- Dazu wird mit *Zertifikat erstellen* ein Stammzertifikat erstellt. Mit diesem können dann weitere Zertifikate signiert werden.
- In den Feldern *Name* und *Kommentar* sollte ein möglichst sprechender Name eingegeben werden, da diese später nicht mehr geändert werden können.
- Unter *Gültigkeit* wird die Lebensdauer der CA festgelegt. Da alle mit dieser CA erzeugten Zertifikate maximal so lange wie die CA gültig sind, sollte hier eine ausreichene Zeitspanne gewählt werden.
- Wählen Sie unter *Verwendung* den Eintrag *CA* aus.
- Das CA-Zertifikat ist selbstsigniert (kein signierendes Zertifikat auswählen).
- Im Abschnitt *Identität* werden Informationen über den Inhaber des Zertifikats hinterlegt.
- Das unter *Passphrase* eingegebene Passwort sichert den privaten Schlüssel des Zertifikats. Es wird immer dann benötigt, wenn mit der CA signiert wird.

Nachdem das CA-Zertifikat erzeugt wurde, können mit diesem weitere Zertifikate signiert werden. Dazu wird jeweils ein neues Zertifikat angelegt.

- Wählen Sie unter *Verwendung* den Eintrag *lokaler Server* aus.
- Bei *Signieren mit* wird das erstellte CA-Zertifikat ausgewählt, dabei muss die hinterlegte *Passphrase* angegeben werden.
- Für den *Namen im Zertifikat* muss der FQDN eingetragen werden, sonst geben manche Clients später eine Fehlermeldung aus.



Ist das Zertifikat erzeugt, kann es in den Konfigurationsdialogen der jeweiligen Dienste zur Verschlüsselung ausgewählt werden, für den Webserver beispielsweise unter *Serverdienste – Webserver – Allgemein – Serverzertifikat*.

6.3 GUI-Referenz: *X.509-Zertifikate*

In diesen Dialogen werden im Collax Security Gateway Zertifikate nach dem X.509-Standard verwaltet. Es können neue Zertifikate erzeugt oder importiert werden. Ebenso ist der Aufbau und Betrieb einer Certificate Authority möglich.

6.3.1 *Vorhandene Zertifikate*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Zertifikate – X.509-Zertifikate*)

Hier sind alle Zertifikate aufgeführt, die auf diesem System erzeugt oder importiert wurden.

Unter *Zertifikate erstellen* können weitere Zertifikate hinzugefügt werden. Dabei können entweder neue Zertifikate generiert oder Zertifikate vom lokalen Rechner per Upload importiert werden.

Wenn ein eigenes CA-Zertifikat erzeugt wurde, werden alle von dieser CA signierten Zertifikate unterhalb des CA-Zertifikats angezeigt.

Bei einzelnen Zertifikaten aus der Liste besteht mit *Anzeigen* die Möglichkeit, das Zertifikat anzuzeigen, über einen Download zu exportieren und zu löschen.

Die aktive Überwachung führt regelmäßige Tests der Gültigkeit der Zertifikate durch. Ist ein Zertifikat noch nicht gültig wird eine Warnung ausgegeben. Steht ein Zertifikat kurz vor dem Ablauf (14 Tage oder weniger) wird eine Warnung ausgelöst.

Hinweis: Es ist nicht ausreichend, Zertifikate, die über eine CA erstellt wurden, zu löschen. Diese müssen vielmehr über *Anzeigen* zurückgezogen werden, damit sie ungültig werden. Werden CA-Zertifikate gelöscht, mit denen bereits Zertifikate signiert wurden, werden

gleichzeitig die noch vorhandenen signierten Zertifikate gelöscht. Bei einem CA-Zertifikat kann zudem die Certificate Revocation List (CRL) exportiert werden.

6.3.1.1 Spalten in der Tabelle

- *Typ*: In dieser Spalte werden die Typen der Zertifikate angezeigt.
- *Key*: In dieser Spalte wird angezeigt ob der private Key im Zertifikat enthalten ist.
- *Name*: In dieser Spalte werden die Namen der Zertifikate angezeigt.
- *Gültigkeit*: In dieser Spalte wird das Ablaufdatum eines Zertifikates angezeigt.
- *Kommentar*: In dieser Spalte werden die Kommentare der Zertifikate angezeigt.

6.3.1.2 Aktionen für jeden Tabelleneintrag

- *Anzeigen*: Diese Aktion zeigt das Zertifikat in Textdarstellung an.
- *Zertifikat exportieren*: Mit dieser Aktion kann das Zertifikat über einen Download auf ein Computersystem exportiert werden. Dort kann es entweder direkt verwendet, archiviert oder weiter transferiert werden.
- *Zurückziehen*: Mit dieser Aktion wird ein Zertifikat zurückgezogen. Das Zertifikat wird gelöscht und in die CRL (Certificate Revocation List) für die CA eingetragen. Ab diesem Zeitpunkt ist das Zertifikat auf dem Collax Security Gateway gesperrt.

  Es können nur solche Zertifikate zurückgezogen werden, die mit einer lokalen CA signiert wurden. Dies sind nur die Zertifikate, die auf diesem System erzeugt wurden.

- *CRL*: Bei einem CA-Zertifikat selbst kann mit dieser Aktion die Certificate Revocation List (CRL) über einen Download auf das zur Administration genutzte System exportiert werden. Zudem bietet diese Aktion die Möglichkeit, eine CRL zu erzeugen.
- *Löschen*: Mit dieser Aktion wird das Zertifikat gelöscht. Es können jedoch keine Zertifikate gelöscht werden, die von einer CA signiert wurden.

  Hinweis: Zum Sperren eines Zertifikats, das über eine CA erzeugt wurde, muss dieses Zertifikat *zurückgezogen* werden.

6.3.1.3 Aktionen für diesen Dialog

- *Zertifikat importieren*: Mit dieser Aktion kann ein Zertifikat auf das System importiert werden. Das Zertifikat kann dabei nur aus einem Public Key bestehen, aber auch ein vollständiges Zertifikat bilden.
- *Zertifikat erstellen*: Mit dieser Aktion wird ein neues Zertifikat angelegt. Dazu öffnet sich ein neuer Dialog, über den die Informationen über den Zertifikatsinhaber abgefragt werden.

6.3.2 *Zertifikat anzeigen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Zertifikate – X.509-Zertifikate*)

In diesem Dialog wird der Inhalt des Zertifikats angezeigt.

6.3.2.1 Tab *Zertifikat*
Felder in diesem Abschnitt

- *Name des Zertifikats*: Hier wird der Name angezeigt, unter dem das Zertifikat im Collax Security Gateway abgelegt ist. Dabei handelt es sich meist nicht um den Common Name, der im Zertifikat selbst gespeichert ist.
- *Inhalt*: Hier wird der Inhalt des Zertifikats angezeigt. Dabei wird die X.509-Textdarstellung verwendet.

6.3.2.2 RSA Public Key

- *RSA Public Key (HEX):* In diesem Textfeld wird der Public Key im RSA-Format in hexadezimaler Schreibweise angezeigt. Er kann hier markiert und über die Zwischenablage gespeichert werden.
- *RSA Public Key (Base64):* In diesem Textfeld wird der Public Key im RSA-Format in Base64-Kodierung angezeigt. Er kann hier markiert und über die Zwischenablage gespeichert werden.

6.3.3 *Zertifikat erzeugen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Zertifikate – X.509-Zertifikate*)

In diesem Dialog wird ein neues Zertifikat erstellt. Solch ein Zertifikat kann verwendet werden, um verschiedenen Diensten auf dem System die Möglichkeit zur Verschlüsselung zu geben.

Je nach der Art der Anwendung kann es sinnvoll sein, ein Zertifikat zu installieren, welches von einer offiziellen CA signiert wurde (etwa

beim Einsatz eines offiziellen Webservers mit Verschlüsselung). Außenstehende Personen werden selbst erzeugten Zertifikaten meist nicht vertrauen. Innerhalb der eigenen Organisation können selbst erstellte Zertifikate jedoch problemlos verwendet werden (etwa für eine sichere Anmeldung am eigenen Mailserver).

Wenn eigene Zertifikate erstellt werden, ist es meist sinnvoll, zunächst ein eigenes CA-Zertifikat anzulegen. Mit diesem werden dann die weiteren Zertifikate für die einzelnen Dienste oder Mitarbeiter signiert.

6.3.3.1 Abschnitt *Zertifikat erzeugen*
Felder in diesem Abschnitt

- *Name des Zertifikats*: Unter diesem Namen wird das Zertifikat im System abgelegt. Er dient dazu, das Zertifikat in der Administrationsoberfläche aufzufinden. Der Name wird nicht in die Inhaberinformation im Zertifikat aufgenommen. Es sollte ein möglichst aussagekräftiger Name für den späteren Einsatzzweck des Zertifikats gewählt werden.
- *Ausgabe*: In diesem Fenster werden während der späteren Erzeugung die Ausgaben der beteiligten Programme angezeigt. Ansonsten ist das Fenster nicht sichtbar.
- *Kommentar*: Mit diesem Kommentartext kann das Zertifikat genauer beschrieben werden. Der Inhalt dieses Feldes wird auch als Kommentar in das Zertifikat kopiert und ist für jeden sichtbar.
- *Gültigkeit (in Tagen)*: Jedes Zertifikat hat eine begrenzte Gültigkeitsdauer und kann danach nicht mehr benutzt werden. In diesem Feld wird diese Dauer in Tagen ab heute angegeben.

  Für ein CA-Zertifikat sollte ein langer Zeitraum gewählt werden (z. B. 5 Jahre), da nach Ablauf des CA-Zertifikats auch alle damit signierten Zertifikate ungültig werden.

- *Schlüssel*: Hier kann gewählt werden, ob ein neues Schlüsselpaar für das Zertifikat generiert oder ein vorhandener Schlüsselsatz in das Zertifikat importiert werden soll.
- *Schlüssellänge*: Die gewünschte Schlüssellänge wird hier vorgegeben. Die Sicherheit des Schlüssels ist von seiner Länge abhängig. Es ist ratsam, möglichst lange Schlüssel zu verwenden. Schlüssel mit weniger als 1024 Bit gelten als unsicher. 1024-Bit-Schlüssel sind möglicherweise ebenfalls nicht mehr sicher, allerdings können manche Clients nicht mit längeren Schlüsseln umgehen.

  Wird ein CA-Zertifikat erzeugt, sollte ein möglichst langer Schlüssel verwendet werden.
- *Datei*: Hier kann der zu importierende Schlüssel ausgewählt und hochgeladen werden. Momentan werden hier nur „ipsec.secrets"-Dateien von *FreeSWAN* aus Kompatibilitätsgründen akzeptiert.

  Im Normalfall wird ein neuer Schlüssel erzeugt. Diese Importfunktion wird nur in besonderen Fällen benötigt.
- *Verwendung*: Hier wird der Verwendungszweck für den Schlüssel gewählt. Wenn ein CA-Schlüssel erzeugt werden soll, muss hier *CA* gewählt werden. In den meisten anderen Fällen wird *lokaler Server* eingestellt. Das Feld kann auch leer bleiben, dann wird ein Schlüssel mit einem breiten Verwendungsspektrum erzeugt.
- *Signieren mit*: Hier muss das Zertifikat der CA ausgewählt werden, mit der das neue Zertifikat signiert werden soll. Wird ein neues CA-Zertifikat erzeugt, braucht kein weiteres Zertifikat ausgewählt werden. Das neue CA-Zertifikat signiert sich dann selbst. Dies ist grundsätzlich auch für einfache Zertifikate möglich.
- *CA-Passphrase*: Um zum Signieren den privaten Schlüssel des CA-Zertifikats nutzen zu können, muss hier die Passphrase der CA angegeben werden.

6.3.3.2 Abschnitt *Identität*

In diesem Abschnitt werden Angaben zur Identität des Inhabers für das Zertifikat gemacht.

Felder in diesem Abschnitt

- *Passphrase*: Hier kann eine Passphrase angegeben werden, mit der der private Schlüssel des Zertifikats gesichert wird. Dies ist nützlich, wenn ein Clientzertifikat erzeugt wird, bei dessen späterer Benutzung jedes Mal die Passphrase abgefragt werden soll.

  Für Serverzertifikate, die für Dienste auf diesem System verwendet werden sollen, darf keine Passphrase gesetzt werden. Die Passphrase würde beim Start der Netzwerkdienste auf der Systemkonsole abgefragt und der Startvorgang des Systems bis zur Eingabe unterbrochen werden. Bei der Erstellung eines Zertifikats für *lokale Server* ist das Feld daher auch nicht sichtbar.

  Die Passphrase wird nicht im System gespeichert. Sie wird immer wieder benötigt, wenn der private Schlüssel des Zertifikats benutzt werden soll. Bei einem CA-Zertifikat ist dies etwa beim Signieren oder Sperren weiterer Zertifikate der Fall.
- *Passphrase (Wiederholung)*: Um zu verhindern, dass eine dritte Person die Eingabe der Passphrase mitlesen kann, wird diese nicht im Klartext angezeigt. Um Fehleingaben zu vermeiden, muss sie daher ein zweites Mal eingegeben werden.
- *Firma/Organisation*: Hier wird der Name der Organisation oder der Firma angegeben, für die das Zertifikat ausgestellt werden soll.

  Hinweis: Da Zertifikate international eingesetzt werden, sollten in den folgenden Textfeldern keine Umlaute und andere

Sonderzeichen aus speziellen Zeichensätzen verwendet werden.

- *Abteilung/Sektion*: Hier kann innerhalb der Einrichtung genauer spezifiziert werden, für welche Abteilung oder Sektion das Zertifikat erzeugt wird.
- *Ort*: Hier wird der Ort angegeben, an dem das Unternehmen bzw. die Organisation den Sitz hat.
- *Bundesland oder Region*: Hier wird das Bundesland oder die Provinz innerhalb des Landes angegeben.
- *Land*: Hier wird das Land ausgewählt.
- *Name im Zertifikat (CN, Common Name)*: Hier wird der Name der Person oder des Systems angegeben, für die das Zertifikat erzeugt werden soll. Diese Name muss eindeutig den Inhaber des Zertifikats beschreiben. Bei E-Mail-Zertifikaten sollte der Name oder die Mailadresse der Person, auf die das Zertifikat ausgestellt wird, benutzt werden. Bei Serverzertifikaten empfiehlt sich die Angabe des FQDNs des Rechners.

  Wird ein Zertifikat für einen Webserver erstellt, sollte hier der exakte FQDN verwendet werden, unter dem das System später von außen angesprochen wird. Manche Webbrowser nehmen eine Überprüfung vor, ob der Zertifikatsname mit dem Servernamen identisch ist.
- *Mail-Alias*: Wird ein Zertifikat für einen Benutzer angelegt, sollte hier die E-Mail-Adresse dieses Benutzers angeben werden.
- *DNS Aliasnamen*: Wird ein Serverzertifikat erzeugt, können hier zusätzliche Namen angegeben werden, unter denen der Server erreichbar ist.
- *E-Mail-Adresse*: Hier wird die E-Mail-Adresse angegeben, die zur CA gehört, z. B. die Adresse des Administrators.

6.3.3.3 Aktionen für diesen Dialog

- *Erzeugen*: Diese Aktion startet die Erzeugung des Zertifikats.

6.3.4 *Zertifikat exportieren*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Zertifikate – X.509-Zertifikate*)

Damit Zertifikate auch für Clients oder VPN-Verbindungen genutzt werden können, müssen sie vom Collax Security Gateway heruntergeladen werden. Dazu stehen verschiedene Exportformate zur Verfügung.

6.3.4.1 Felder in diesem Dialog

- *Zertifikat*: In diesem Feld wird der Name des Zertifikats angezeigt.
- *Format*: Hier wird das Format gewählt, in dem das Zertifikat gespeichert wird. Welches Format benötigt wird, richtet sich danach, welche Formate die Gegenseite bzw. der Client einlesen können. In den Formaten PEM, PKCS12 und DER wird der private Schlüssel des Zertifikats exportiert.

  PEM ist ein Base64-kodiertes Standardformat zum Zertifikatsaustausch mit anderen Linux-/Unix-Servern. Wird dieses Format gewählt, kann noch festgelegt werden, ob der private Schlüssel mit exportiert wird oder nicht. Der private Schlüssel der eigenen Zertifikate darf unter keinen Umständen an andere Personen weitergegeben werden.

  Das gepackte Zertifikat enthält auch den Public Key der CA, die das Zertifikat signiert hat. Nicht alle VPN-Produkte können

eine solche Kombination einlesen. In diesem Fall muss der CA-Schlüssel getrennt exportiert und auf der Gegenseite eingelesen werden.

PKCS12-Zertifikate werden von einigen Webbrowsern und Mailprogrammen verwendet (Netscape/Mozilla, Internet Explorer, Outlook). Dieses Format kann nur gewählt werden, wenn ein privater Schlüssel zum Zertifikat existiert. Der private Schlüssel wird in jedem Fall mit exportiert. Der private Schlüssel der eigenen Zertifikate darf unter keinen Umständen an andere Personen weitergegeben werden.

In diesem Format kann auf die Exportdatei eine Passphrase gelegt werden. Nur mit der Kenntnis dieser Passphrase kann das Zertifikat auf einem anderen System eingelesen bzw. verwendet werden.

DER-Zertifikate werden von einigen PDAs verwendet, um gesicherte Verbindungen aufzubauen. In einer DER-Datei können private Keys, Public Keys oder Zertifikate enthalten sein. DER-Zertifikate stellen das Standard-Format für die meisten Web-Browser dar.

- *Mit privatem Schlüssel*: Ist diese Option aktiviert, wird der private Schlüssel mit in den Export aufgenommen.

  Die Option steht zur Verfügung, wenn das Zertifikat im *PEM*- oder im *DER*-Format exportiert wird.

  Diese Option sollte nur dann aktiviert werden, wenn ein Clientzertifikat auf diesem System erzeugt wurde und dieses nun für den Client exportiert werden soll.
- *CA-Zertifikat*: Ist das Zertifikat von einer CA signiert worden, ist es sinnvoll, das CA-Zertifikat zusätzlich mit in die exportierte Datei aufzunehmen. Über dieses CA-Zertifikat wird das eigentliche Zertifikat gültig erklärt (vorausgesetzt, dem CA-Zertifikat wird vertraut).

- *Passphrase*: Ist der private Schlüssel des Zertifikats mit einer Passphrase gesichert, muss hier zum Exportieren diese Passphrase angeben werden.
- *Exportpasswort*: Wird ein Zertifikat im PKCS#12-Format exportiert, muss hier ein Passwort angegeben werden. Mit diesem wird die Exportdatei verschlüsselt. Das Passwort wird später beim Importieren des Zertifikats auf den Client wieder benötigt.
- *Exportpasswort (Wiederholung)*: Da das Exportpasswort bei der Eingabe aus Sicherheitsgründen nicht sichtbar ist, muss es hier zur Sicherheit nochmals eingegeben werden.

6.3.4.2 Aktionen für diesen Dialog

- *Download*: Mit dieser Aktion wird der Download des Zertifikats gestartet. Nach kurzer Zeit sollte im Browser ein *Speichern-unter*-Dialog geöffnet werden. Ist dies nicht der Fall, wurde im Browser eventuell eine automatische Speicherung in ein bestimmtes Verzeichnis aktiviert.

6.3.5 *Zertifikat importieren*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Zertifikate – X.509-Zertifikate*)

Über diesen Dialog kann ein Zertifikat auf das System importiert werden.

Ein Zertifikat besteht in der Regel aus drei Teilen: Dem von der CA signierten öffentlichen Schlüssel, dem privaten Schlüssel und dem Zertifikat der CA. Nicht alle drei Teile sind immer notwendig.

Manche Dateiformate für Zertifikate (PKCS#12 und PEM) können

alle drei Teile in einer Datei enthalten. Liegt das Zertifikat aber nur im DER-Format vor, müssen die einzelnen Teile separat angegeben werden.

Das Zertifikat einer CA muss nur einmal auf dem System installiert werden. Wurde bereits ein Zertifikat installiert, das von der gleichen CA unterschrieben wurde, muss das CA-Zertifikat nicht nochmals installiert werden.

Der private Schlüssel zum Zertifikat wird nur dann benötigt, wenn das Zertifikat für das System selbst verwendet werden soll, etwa für einen Serverdienst oder als VPN-Endpunkt. In allen anderen Fällen muss der private Schlüssel nicht auf dem System installiert werden.

6.3.5.1 Felder in diesem Dialog

- *Name für das Zertifikat*: Unter diesem Namen wird das Zertifikat im System abgelegt. Er dient dazu, das Zertifikat in der Administrationsoberfläche aufzufinden. Der Name muss nicht mit den Inhaberinformationen im Zertifikat identisch sein. Es sollte jedoch ein möglichst aussagekräftiger Name für den Einsatzzweck des Zertifikats gewählt werden.
- *Kommentar*: In diesem Kommentartext kann eine ausführlichere Information zum Zertifikat angegeben werden.
- *Ausgabe*: Während des Imports erscheint ein Fenster mit der Ausgabe des Installationsprozesses.
- *Passwort*: PKCS#12-Zertifikate und der private Schlüssel in PEM-Zertifikaten sind meist während des Transports mit einem Passwort geschützt. Dieses muss hier eingegeben werden, um auf das Zertifikat zugreifen zu können.
- *Zertifikat*: Mit diesem Dialog kann die Datei mit dem Zertifikat auf dem Computer ausgewählt werden, von dem aus gerade die Administration erfolgt.

- *Privater Schlüssel*: Wird das Zertifikat für einen Serverdienst oder für ein VPN verwendet, kann hier eine Datei ausgewählt werden, die den privaten Schlüssel für das Zertifikat enthält.

  Ist das Zertifikat im PKCS#12-Format oder als kombiniertes PEM-Zertifikat gespeichert, bleibt dieses Feld leer.
- *CA-Zertifikat*: Hier wird die Datei mit dem Zertifikat der CA ausgewählt, die das zu installierende Zertifikat unterschrieben hat.

  Dieses Feld bleibt leer, wenn das CA-Zertifikat bereits installiert wurde oder wenn das Zertifikat in einem Format vorliegt, das diese Information bereits enthält (PKCS12 oder kombiniertes PEM).

6.3.5.2 Aktionen für diesen Dialog

- *Upload*: Mit dieser Aktion wird der Import des Zertifikats gestartet. Nach erfolgreichem Import sollte das Zertifikat unter dem beim Import angegebenen Namen in der Zertifikatsübersicht aufgeführt sein.

6.3.6 *Zertifikat zurückziehen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Zertifikate – X.509-Zertifikate*)

In diesem Dialog kann ein Zertifikat zurückgezogen werden. Dieses Sperren ist nur für Zertifikate möglich, die von einer auf dem System betriebenen CA signiert wurden. Die Sperre kann nicht wieder aufgehoben werden. In diesem Fall muss ein neues Zertifikat erstellt werden.

Die Laufzeit eines Zertifikats wird normalerweise bei seiner Erzeu-

gung festgelegt. Wird ein CA-signiertes Zertifikat zur Authentifizierung (z. B. für VPN-Einwahl) benutzt, ist es nicht ausreichend, das Zertifikat zu löschen. Über die CA-Signatur und seine Restlaufzeit ist es weiterhin gültig.

Um Zertifikate vor Ablauf des Verfallsdatums für ungültig zu erklären, werden diese in eine Liste (die Certificate Revocation List CRL) eingetragen. Dienste, die mit Zertifikaten arbeiten, können in dieser Liste abfragen, ob ein Zertifikat für ungültig erklärt wurde.

6.3.6.1 Felder in diesem Dialog

- *Name für das Zertifikat*: Hier wird der Name des Zertifikats angezeigt, das gesperrt werden soll.
- *Kommentar*: Hier wird der Kommentartext angezeigt, der beim Erstellen oder Importieren des Zertifikats angegeben wurde.
- *CA-Passwort*: Um das Zertifikat zurückzuziehen, muss das Passwort der CA angegeben werden. Es muss die CA verwendet werden, mit der das Zertifikat bei der Erstellung signiert wurde.

  Das Feld wird nur dann angezeigt, wenn für die Verwendung des privaten Schlüssels der CA ein Passwort benötigt wird.
- *Log*: Während des Vorgangs erscheint ein Fenster mit der Ausgabe der aufgerufenen Programme.

6.3.6.2 Aktionen für diesen Dialog

- *Zurückziehen*: Hiermit wird der Sperrvorgang ausgelöst. Das Zertifikat wird widerrufen und danach gelöscht.

6.3.7 *CRL verwalten*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Zertifikate – X.509-Zertifikate*)

Eine CRL (Certificate Revocation List) ist eine Sperrliste von Zertifikaten, die von einer CA unterschrieben wurden, aber vor Ende der Laufzeit zurückgezogen wurden.

Für eine CA, die auf diesem System verwaltet wird, kann die CRL mit diesem Dialog erzeugt werden. Die CRL wird dann von allen lokalen Diensten automatisch verwendet. Diese CRL kann exportiert werden.

Wird auf einem anderen System eine CA betrieben, von der auf dem lokalen System Zertifikate eingesetzt werden, kann die CRL auf dem anderen System exportiert und ins lokale System importiert werden. Dieser Vorgang sollte spätestens nach jeder Sperrung eines Zertifikats durchgeführt werden.

6.3.7.1 Felder in diesem Dialog

- *Name der CA*: Hier wird der Name der CA angezeigt, für die die CRL verwaltet wird.
- *Kommentar*: Hier wird der Kommentartext angezeigt, der beim Erstellen oder Importieren der CA angegeben wurde.
- *CA-Passwort*: Um ein Zertifikat zurückzuziehen, muss das Passwort der CA angegeben werden. Dabei handelt es sich um die CA, die das Zertifikat ausgestellt hat.

  Dieses Feld wird nur dann angezeigt, wenn für die lokale CA ein Passwort benötigt wird.
- *Datei*: Wird eine CA auf einem anderen System verwaltet, kann die CRL der CA über dieses Feld in dieses System importiert

werden. Zertifikate können nur auf dem System mit der CA gesperrt werden. Um andere Systeme über diese Sperrungen zu informieren, muss die CRL exportiert und auf den beteiligten Systemen importiert werden.

- *Log*: Während des Vorgangs erscheint ein Fenster mit der Ausgabe der aufgerufenen Programme.

6.3.7.2 Aktionen für diesen Dialog

- *CRL erstellen*: Mit dieser Aktion wird die CRL erstellt.
- *Importieren*: Mit dieser Aktion wird der Upload der CRL gestartet.
- *Exportieren*: Mit dieser Aktion wird der Download der CRL gestartet. Nach kurzer Zeit sollte im Browser ein *Speichern-unter*-Dialog geöffnet werden. Ist dies nicht der Fall, wurde im Browser eventuell eine automatische Speicherung in ein bestimmtes Verzeichnis aktiviert.

6.4 GUI-Referenz: *Certificate Signing Requests (CSR)*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Zertifikate – Certificate Signing Requests*

6.4.1 *Certificate Signing Request wählen*

6.4.1.1 Spalten in der Tabelle

- *Name*: Hier wird der Name eines erstellten CSR angezeigt.
- *Distinguished Name (DN)*: Zeigt den DN des erstellten CSR an.

6.4.1.2 Aktionen für jeden Tabelleneintrag

- *Anzeigen*: Mit dieser Aktion werden Details des CSR angezeigt.
- *Löschen*: Mit dieser Aktion kann das gewählte CSR gelöscht werden.
- *Exportieren*: Durch diese Aktion öffnet sich ein Dialog, um das CSR zu exportieren.

6.4.1.3 Aktionen für dieses Formular

- *CSR erstellen*: Mit dieser Aktion kann ein neuer CSR erstellt werden.

6.4.2 GUI-Referenz: *CSR erzeugen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Zertifikate – Certificate Signing Requests*)

6.4.2.1 Abschnitt *CSR erzeugen*
Felder in diesem Abschnitt

- *Name des Zertifikats*: Unter diesem Namen wird das Zertifikat im System abgelegt. Er dient dazu, das Zertifikat in der Administrationsoberfläche aufzufinden. Der Name muss nicht mit den Inhaberinformationen im Zertifikat identisch sein. Es sollte jedoch ein möglichst aussagekräftiger Name für den Einsatzzweck des Zertifikats gewählt werden.
- *Kommentar*: In diesem Kommentartext kann eine ausführlichere Information zum Zertifikat angegeben werden.
- *Schlüssellänge*: Die gewünschte Schlüssellänge wird hier vorgegeben. Die Sicherheit des Schlüssels ist von seiner Länge abhängig. Es ist ratsam, möglichst lange Schlüssel zu verwenden. Schlüssel mit weniger als 1024 Bit gelten als unsicher. 1024-Bit-Schlüssel sind möglicherweise ebenfalls nicht mehr sicher, allerdings können manche Clients nicht mit längeren Schlüsseln umgehen.

  Wird ein CA-Zertifikat erzeugt, sollte ein möglichst langer Schlüssel verwendet werden.
- *Verwendung*: Hier wird der Verwendungszweck für den Schlüssel gewählt. Wenn ein CA-Schlüssel erzeugt werden soll, muss hier *CA* gewählt werden. In den meisten anderen Fällen wird *lokaler Server* eingestellt. Das Feld kann auch leer bleiben, dann wird ein Schlüssel mit einem breiten Verwendungsspektrum erzeugt.
- *Ausgabe*: Während des Imports erscheint ein Fenster mit der Ausgabe des Installationsprozesses.

6.4.2.2 Abschnitt *Identität*
Felder in diesem Abschnitt

- *Passphrase (privater Schlüssel)*: Hier kann eine Passphrase angegeben werden, mit der der private Schlüssel des Zertifikats gesichert wird. Dies ist nützlich, wenn ein Clientzertifikat erzeugt wird, bei dessen späterer Benutzung jedes Mal die Passphrase abgefragt werden soll.

  Für Serverzertifikate, die für Dienste auf diesem System verwendet werden sollen, darf keine Passphrase gesetzt werden. Die Passphrase würde beim Start der Netzwerkdienste auf der Systemkonsole abgefragt und der Startvorgang des Systems bis zur Eingabe unterbrochen werden. Bei der Erstellung eines Zertifikats für *lokale Server* ist das Feld daher auch nicht sichtbar.

  Die Passphrase wird nicht im System gespeichert. Sie wird immer wieder benötigt, wenn der private Schlüssel des Zertifikats benutzt werden soll. Bei einem CA-Zertifikat ist dies etwa beim Signieren oder Sperren weiterer Zertifikate der Fall.
- *Passphrase (Wiederholung)*: Um zu verhindern, dass eine dritte Person die Eingabe der Passphrase mitlesen kann, wird diese nicht im Klartext angezeigt. Um Fehleingaben zu vermeiden, muss sie daher ein zweites Mal eingegeben werden.
- *Firma/Organisation*: Hier wird der Name der Organisation oder der Firma angegeben, für die das Zertifikat ausgestellt werden soll.

  Hinweis: Da Zertifikate international eingesetzt werden, sollten in den folgenden Textfeldern keine Umlaute und andere Sonderzeichen aus speziellen Zeichensätzen verwendet werden.
- *Abteilung/Sektion*: Hier kann innerhalb der Einrichtung genauer spezifiziert werden, für welche Abteilung oder Sektion das Zertifikat erzeugt wird.

- *Ort*: Hier wird der Ort angegeben, an dem das Unternehmen bzw. die Organisation den Sitz hat.
- *Bundesland oder Region*: Hier wird das Bundesland oder die Provinz innerhalb des Landes angegeben.
- *Land*: Hier wird das Land ausgewählt.
- *Name im Zertifikat (CN, Common Name)*: Hier wird der Name der Person oder des Systems angegeben, für die das Zertifikat erzeugt werden soll. Diese Name muss eindeutig den Inhaber des Zertifikats beschreiben. Bei E-Mail-Zertifikaten sollte der Name oder die Mailadresse der Person, auf die das Zertifikat ausgestellt wird, benutzt werden. Bei Serverzertifikaten empfiehlt sich die Angabe des FQDNs des Rechners.

  Wird ein Zertifikat für einen Webserver erstellt, sollte hier der exakte FQDN verwendet werden, unter dem das System später von außen angesprochen wird. Manche Webbrowser nehmen eine Überprüfung vor, ob der Zertifikatsname mit dem Servernamen identisch ist.
- *Mail-Alias*: Wird ein Zertifikat für einen Benutzer angelegt, sollte hier die E-Mail-Adresse dieses Benutzers angeben werden.
- *Aliasnamen*: Wird ein Serverzertifikat erzeugt, können hier zusätzliche Namen angegeben werden, unter denen der Server erreichbar ist.
- *E-Mail-Adresse*: Hier wird die E-Mail-Adresse angegeben, die zur CA gehört, z. B. die Adresse des Administrators.

6.4.2.3 Abschnitt *Extra Attribute*

Felder in diesem Abschnitt

- *Optionaler Firmenname*: Hier kann ein optionaler Firmenname angegeben werden. Erkundigen Sie sich jedoch vorher bei Ihrer Zertifizierungsstelle, ob diese Angabe möglich ist.

- *Challenge Passwort (CSR)*: Hier kann ein optionales Challenge Passwort angegeben werden. Erkundigen Sie sich jedoch vorher bei Ihrer Zertifizierungsstelle, ob diese Angabe möglich ist.

6.4.2.4 Aktionen für dieses Formular

- *Zurück*: Diese Aktion führt zurück in die Zertifikatsübersicht.
- *Erzeugen*: Diese Aktion startet die Erzeugung des Zertifikats.

6.4.3 GUI-Referenz: *CSR anzeigen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Zertifikate – Certificate Signing Requests*)

6.4.3.1 Tab *CSR Information*
Felder in diesem Abschnitt

- *Name des CSR*: Hier wird der Name des CSR angezeigt.
- *Inhalt*: Hier wird der Inhalt des CSR angezeigt. Dabei wird die X.509-Textdarstellung verwendet.

6.4.3.2 Tab *CSR*
Felder in diesem Abschnitt

- *CSR-Quelltext*: Hier wird der Quelltext des CSR angezeigt.

6.4.3.3 Aktionen für dieses Formular

- *Zurück*: Diese Aktion führt zurück in die Zertifikatsübersicht.
- *Download*: Mit dieser Aktion können Sie den CSR herunterladen.

6.5 GUI-Referenz: *RSA-Schlüssel*

RSA-Schlüssel sind Schlüsselpaare aus Public und Private Key. Üblicherweise werden diese zusammen mit den Inhaberinformationen und einer CA-Signatur zu einem Zertifikat zusammengefasst. Dazu wird meist der Standard X.509 genutzt.

Gerade bei VPN-Verbindungen gibt es gelegentlich IPsec-Gegenstellen, die (noch) nicht mit X.509-Zertifikaten umgehen können. Stattdessen muss der reine RSA-Schlüssel verwendet werden. In diesem Dialog können öffentliche Schlüssel solcher Gegenstellen importiert werden.

Als Schlüsselpaar für den Collax Security Gateway wird immer ein X.509-Zertifikat verwendet. Der öffentliche RSA-Schlüssel dieses Zertifikats kann jedoch in der Zertifikatsansicht gespeichert und auf die Gegenstelle geladen werden.

6.5.1 *RSA-Schlüssel wählen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Zertifikate – RSA-Schlüssel*)

6.5.1.1 Felder in diesem Dialog

- *Name des RSA-Schlüssels*: Name, unter dem der Schlüssel abgelegt wird.
- *Kommentar*: Ein Kommentartext zu diesem Schlüssel.

6.5.1.2 Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion kann der öffentliche Schlüssel bearbeitet werden.
- *Löschen*: Diese Aktion löscht den Schlüssel.

6.5.1.3 Aktionen für diesen Dialog

- *Hinzufügen*: Mit dieser Aktion kann ein öffentlicher Schlüssel auf dem System abgelegt werden.

6.5.2 *RSA-Schlüssel installieren*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Zertifikate – RSA-Schlüssel*)

6.5.2.1 Felder in diesem Dialog

- *Name des RSA-Schlüssels*: Unter diesem Namen wird der Schlüssel abgelegt.
- *Name des RSA-Schlüssels*: Wurde der Schlüssel bereits früher

abgelegt, wird der Name des Schlüssels nur angezeigt und kann nicht geändert werden.

- *Kommentar*: Ein Kommentartext zu diesem Schlüssel.
- *Schlüssel*: In dieses Eingabefeld wird der öffentliche RSA-Schlüssel eingefügt. Der Schlüssel kann entweder als Hexadezimalzahl oder Base64-kodiert eingegeben werden.

7 Netzwerke

7.1 Einführung

Computer müssen ein gemeinsames Protokoll verwenden, um miteinander kommunizieren zu können. In der Vergangenheit kamen verschiedene, teils herstellerspezifische Protokolle zum Einsatz. Heutzutage setzt der Großteil der Systeme auf TCP/IP.

Grundlage ist das „Internet Protocol“ IP, auf dem weitere Protokolle basieren. Jedes dieser weiteren Protokolle ist für bestimmte Daten besonders geeignet. Eines dieser Protokolle ist das „Transmission Control Protocol“ TCP. Es ist so bedeutend, dass seine Abkürzung mit zur offiziellen Bezeichnung der Protokollfamilie TCP/IP beiträgt.

7.1.1 Adressierung von Computersystemen

Zur Kommunikation im Internet erhält jedes System eine 32 Bit breite „IP-Nummer“ als Adresse. Als übliche Schreibweise hat sich die Aufteilung in vier Oktette in dezimaler Darstellung durchgesetzt, z. B. 192.168.9.9. Diese Schreibweise wird auch als „Dotted Decimal Notation“ bezeichnet.

Diese IP-Adresse stammt aus dem Adressbereich von Version 4 des IP-Protokolls („IPv4“). Insgesamt lassen sich damit etwa 4 Milliarden unterschiedliche Adressen bilden. In diesem Handbuch ist immer IPv4 gemeint, wenn nicht ausdrücklich etwas anderes angegeben wird (wie im Folgenden Absatz).

Für die Zukunft ist IPv4 nicht ausreichend, da immer mehr Geräte eine IP-Adresse benötigen und die vorhandenen IP-Adressen etwas

ungleich verteilt sind (in Asien besteht großer Bedarf, aber die Mehrheit der IP-Adressen sind Europa und Nordamerika zugeordnet). Daher steht als Nachfolger bereits Version 6 („IPv6“) bereit, hier werden Adressen einer Größe von 128 Bit verwendet. Daraus ergeben sich Billiarden von IP-Nummern pro Quadratmillimeter Erdoberfläche, was nach heutigem Ermessen eine ganze Zeit ausreichen wird.

7.1.2 Adressierung von Computerdiensten

Auf einem Computersystem laufen unterschiedliche Programme, meist als eigenständige Prozesse, etwa Webserver, POP3-Server, IMAP-Server usw. Über die IP-Adresse wird das System selbst angesprochen. Die Zuordnung auf die einzelnen Dienste erfolgt über die Angabe einer Portadresse. Dabei handelt es sich um eine 16-Bit-Adresse, hinter der ein Dienst oder eine Applikation Verbindungen annimmt. Sie stellt bildlich betrachtet die Zimmernummer in dem großen Computerhaus dar. Dabei werden die Portnummern bis 1024 weitgehend für Systemdienste genutzt.

Die Portadresse muss entweder vor dem Verbindungsaufbau abgesprochen werden, oder es wird eine festgelegte Nummer verwendet, etwa Port 80 für HTTP/Webserver. Die Liste der offiziell zugewiesenen Portnummern wird von der „Internet Assigned Numbers Authority“ (IANA) verwaltet.

Die Portadresse des Absenders (in diesem Beispiel des Webbrowsers) wird vom Betriebssystem im Moment des Verbindungsaufbaus zufällig vergeben.

Gängige Portnummern

Dienst	Protokoll	Port
Webadmin	TCP	8001
DNS	UDP und TCP	53
HTTP-Webserver	TCP	80
HTTPS-Webserver	TCP	443
HylaFax-Dienst	TCP	4559
MySQL-Dienst	TCP	3306
Squid-Webproxy	TCP	3128
SMTP-Mailserver	TCP	25
POP3-Mailserver	TCP	110
POP3S-Mailserver	TCP	995
SSH	TCP	22

7.1.3 Protokolle

Für den Austausch von Daten über IP sind verschiedene Unterprotokolle definiert. ICMP („Internet Control Message Protocol“) ist ein Protokoll zum Betrieb des eigentlichen Netzwerkes. Computer tauschen darüber Informationen über Laufzeiten und Erreichbarkeitsprobleme im Netz aus.

Eines der einfachsten Protokolle zur Nutzdatenübertragung ist das „User Datagram Protocol“ UDP. Neben Absender- und Ziel-IP-Adresse werden die Nutzdaten, die Absender- und Zielportadresse sowie eine optionale Prüfsumme in einem Datenpaket übertragen. Es gibt keinerlei Rückmeldung, ob ein UDP-Paket beim Empfänger angekommen ist; es könnte also unterwegs verloren gehen. Ebenso ist es möglich, dass mehrere abgeschickte Pakete in unterschiedlicher Reihenfolge ankommen oder dass einzelne Pakete mehrfach ankommen. UDP ist durch den fehlenden Verbindungsaufbau sehr schnell und wird daher für DNS-Anfragen, NFS, Onlinespiele und VoIP-Verbindungen eingesetzt.

Das „Transmission Control Protocol“ TCP ist im Gegensatz zu UDP ein verbindungsorientiertes Protokoll. Zwischen den beiden beteiligten Systemen wird mittels eines Drei-Wege-Handshakes eine Verbindung aufgebaut. Gelingt dies, ist die Verbindung etabliert („established“). In diesem Zustand werden alle gesendeten Datenpakete durchnummeriert. Durch diese „Sequenznummer“ können verlorene Pakete erkannt und neu angefordert oder in unterschiedlicher Reihenfolge eingetroffene Pakete korrekt eingeordnet werden. Analog zum Aufbau muss die Verbindung wieder abgebaut werden.

Eine DNS-Anfrage über TCP würde drei Pakete für den Verbindungsaufbau, drei Pakete für die eigentliche Datenübertragung inkl. Bestätigungen sowie drei Pakete zum Abbau der Verbindung benötigen. Mittels UDP ist dasselbe mit insgesamt zwei Paketen erreichbar.

7.1.4 Paketzustellung

Das Versenden von Datenpaketen im lokalen Netzwerk – auch als „Local Area Network“ LAN bezeichnet – ist noch recht einfach. Ein Computersystem „fragt“ im LAN nach, welcher andere Computer die Ziel-IP-Adresse hat. Sobald dieser die Anfrage beantwortet, kann die Übertragung gestartet werden. Antwortet niemand, läuft die Anfrage in einen Timeout, und es gibt nach einiger Zeit eine entsprechende Fehlermeldung.

Liegt die Ziel-IP-Nummer dagegen außerhalb des lokalen Netzes in einem anderen Gebäude oder einer anderen Stadt, ist eine direkte Adressierung nicht möglich. Hier müssen „Router“ oder „Gateways“ verwendet werden. Üblicherweise ist ein Computer so eingestellt, dass er IP-Nummern aus dem eigenen lokalen Netzbereich direkt im lokalen Netz anfragt und alle Pakete zu fremden IP-Nummern zu einem „Default-Gateway“ im lokalen Netz sendet.

Dieses Gateway ist normalerweise das System mit der Internetverbindung und schickt die Datenpakete weiter zu seinem Default-Gateway beim Provider. Von dort aus läuft das Datenpaket über weitere Gateways und Router bis zum Zielsystem. Das Antwortpaket läuft den umgekehrten Weg zurück – es kann auch einen anderen Weg nehmen, da der genaue Weg im Internet nicht festgelegt ist und auch abhängig von Last und Ausfällen umgeschaltet wird. Dieser ganze Mechanismus der Paketzustellung wird als „Routing“ bezeichnet.

Um festzulegen, ob ein Paket für das lokale Netz bestimmt ist oder zum Default-Gateway gesendet werden muss, wird der „Adressbereich“ des lokalen Netzes benötigt. Dieser Adressbereich beinhaltet alle im lokalen Netz verwendeten IP-Nummern und besteht aus der „Netzwerkadresse“ und der „Netzmaske“.

Die Netzwerkadresse ist die erste IP-Adresse des Adressbereichs und wird nicht an Computer vergeben. Die Netzmaske legt die Größe des Adressbereichs fest und bestimmt damit die letzte IP-Adresse des Bereichs. Diese letzte Adresse ist die „Broadcastadresse“. Alle an diese Adresse geschickten Datenpakete werden von allen Computern im Adressbereich angenommen. Die Broadcastadresse sollte daher auch nicht für einen einzelnen Computer genutzt werden.

Der gesamte „IP-Adressraum“ von 0.0.0.0 bis 255.255.255.255 wurde anfangs in fünf Klassen unterteilt, um damit im Internet das Routing durchzuführen.

Für das Routing ist prinzipiell auf jedem zentralen Backbone-Router für jede IP-Nummer ein Eintrag notwendig, der klärt, wo diese IP-Nummer erreichbar ist. Um diese „Routingtabellen“ überschaubar zu halten, werden IP-Nummern zu IP-Netzen zusammengefasst. Damit sind in den Routingtabellen nur Einträge für Netze notwendig. Eine IP-Nummer kann in ihren Netzwerkanteil und den Hostanteil zerlegt werden. Dabei muss festgelegt werden, wie viele Bits (von links) innerhalb der IP-Adresse den Netzwerkanteil bilden.

Das Herausfiltern des Netzwerkanteils geschieht mit Hilfe der Netzmaske über eine logische UND-Verknüpfung. Dabei werden alle in der Netzmaske gesetzten Bits „stehen“ gelassen. Da der Netzanteil links und der Hostanteil rechts notiert ist, kann der Netzanteil (von links) 8 Bit, 9 Bit, 10 Bit, 11 Bit bis 32 Bit betragen. Daraus ergibt sich die heute verbreitete Schreibweise „/24“ für einen 24 Bit breiten Netzwerkanteil. Diese Schreibweise ist äquivalent zur Angabe der Netzmaske in der Form „255.255.255.0“.

Bei Class-A-Netzen ist der Netzwerkanteil 8 Bit groß. Die drei folgenden Oktette sind Hostnummern und können vom Inhaber des jeweiligen Class-A-Netzes beliebig in seinem Netzwerk verteilt werden. Weltweit gibt es 126 Class-A Netze mit jeweils über 16 Millionen Hosts.

Class-B-Netze haben einen 16 Bit großen Netzwerkanteil, 16 Bit bleiben für die (über 65000) Hosts übrig.

Bei Class-C-Netzen beträgt der Netzwerkanteil 24 Bit. Ihre Netzmaske ist die bekannte „255.255.255.0“. Weltweit gibt es knapp zwei Millionen Netze mit je 254 Hosts.

Ursprünglich konnte anhand der Netzklasse die Netzmaske für das Routing identifiziert werden. Heute wird dieses starre Schema nicht mehr angewandt, um mehr Flexibilität bei der Zuweisung von IP-Adressen zu erhalten. Der Adressraum ist damit „klassenlos“. Für die einzelnen Netze werden in den Internetroutern jeweils Einträge (mit den entsprechenden Netzmasken) vorgenommen. Diese gesamte Technik wird als „Classless Inter Domain Routing“ CIDR bezeichnet.

IP-Adressräume

Netzwerkadresse	Bit	Netzmaske	Verwendung
10.0.0.0	8	255.0.0.0	Für den privaten Gebrauch reservierter Block, darf im Internet nicht geroutet werden.
14.0.0.0	8	255.0.0.0	Für „Public Data Networks“ reservierter Block.
24.0.0.0	8	255.0.0.0	1996 für Kabelmodem-Anbieter reservierter Block, inzwischen freigegeben.
39.0.0.0	8	255.0.0.0	1995 für das „Klasse-A-Subnetz-Experiment“ reservierter Block, inzwischen freigegeben.
127.0.0.0	8	255.0.0.0	Als „Internet Host Loopback“ zur Kommunikation innerhalb eines Systems genutzter Block, darf nicht im Internet geroutet werden.
128.0.0.0	16	255.255.0.0	Ursprünglich von IANA reserviert, inzwischen freigegeben.
169.254.0.0	16	255.255.0.0	Systeme, die ihre IP-Adresse per DHCP beziehen, weisen sich aus diesem „Link Local“-Block eine Adresse zu, wenn kein DHCP-Server erreichbar ist.
172.16.0.0	12	255.240.0.0	Für den privaten Gebrauch reservierter Block, darf nicht im Internet geroutet werden.
192.255.0.0	16	255.255.0.0	Ursprünglich von IANA reserviert, inzwischen freigegeben.

192.0.0.0	24	255.255.255.0	Ursprünglich von IANA reserviert, inzwischen freigegeben.
192.0.2.0	24	255.255.255.0	„Test Netz“ zur Verwendung in Dokumentationen und Beispielen, darf im Internet nicht geroutet werden.
192.88.99.0	24	255.255.255.0	Reserviert für „6to4-Anycast-Adressen“ (siehe RFC3068).
192.168.0.0	24	255.255.255.0	Für den privaten Gebrauch reservierter Block, darf nicht im Internet geroutet werden.
192.18.0.0	15	255.254.0.0	Reserviert für Benchmark-Tests (siehe RFC2544).
223.255.255.0	24	255.255.255.0	Ursprünglich von IANA reserviert, inzwischen freigegeben.
224.0.0.0	4	240.0.0.0	Ehemaliger Klasse-D-Adressraum, reserviert für „IPv4-Multicast-Adresszuweisungen“.
240.0.0.0	4	240.0.0.0	Ehemaliger Klasse-E-Adressraum. Reserviert für zukünftige Freigabe, darf nicht geroutet werden.

Mit NAT („Network Address Translation“) wird der Vorgang bezeichnet, wenn in IP-Paketen die Quell- bzw. Ziel-Adresse ausgetauscht wird. Abhängig von der modifizierten Adresse werden SNAT („Source NAT“) und DNAT („Destination NAT“) unterschieden. Im Collax Security Gateway ist es auch möglich, NAT für ganze Netze durchzuführen („Netmap“). Dabei wird nur der Netzanteil ersetzt, der Hostanteil der IP-Adresse bleibt unverändert. Die Möglichkeiten der praktischen Anwendung sind in einfachen Netzwerkinstallationen begrenzt, da

bei NAT eine Eins-zu-Eins-Umsetzung von Adressen erfolgt. Beispielsweise muss der Provider vier öffentliche IP-Adressen bereitstellen, damit diese auf vier interne, private IP-Adressen umgesetzt werden können.

Da die Menge an IP-Nummern begrenzt ist und ein Administrator nicht immer genügend öffentliche IP-Nummern für alle Systeme in seinem Netz bekommen kann, wird das sogenannte „Masquerading" eingesetzt. Dabei ersetzt das Gateway in den IP-Paketen jeweils die Absender-IP-Adresse (aus dem lokalen Netz) durch seine eigene IP-Nummer im Internet. Zusätzlich wird der Absendeport durch eine neue Portnummer ersetzt. Das Paket gelangt zum Zielrechner, der ein Antwortpaket an die vermeintliche Absenderadresse zurückschickt. Dadurch gelangt das Paket zum Gateway, und dieses kann anhand der Portnummer die ursprüngliche Absender-IP-Adresse sowie die Portnummer als neue Ziel-Adresse eintragen. Durch diesen Mechanismus wird das gesamte lokale Netz versteckt bzw. maskiert.

Masquerading ist ein Sonderfall von DNAT, da hier neben den IP-Adressen auch die Portadressen modifiziert werden. Durch dieses Verfahren können viele Rechner aus dem LAN ins Internet zugreifen und sich eine IP-Adresse „teilen". Es ist jedoch kein Rechner aus dem LAN-Bereich im Internet sichtbar und von dort für den Aufbau einer neuen Verbindung erreichbar.

Für diesen Zweck ist die Verwendung von „privaten Netzen" im lokalen Netz wichtig. Dies sind spezielle IP-Bereiche, die nicht im Internet geroutet werden. Würden willkürlich IP-Nummern für das lokale Netz verwendet, die an anderer Stelle im Internet vergeben sind, können diese Systeme im Internet nicht erreicht werden, da der Zielhost im lokalen Netz gesucht und u. U. gefunden wird.

Folgende Netze sind für private Verwendung freigegeben:

- 10.0.0.0/8 (von 10.0.0.0 bis 10.255.255.255)
- 172.16.0.0/12 (von 172.16.0.0 bis 172.31.255.255)
- 192.168.0.0/16 (von 192.168.0.0 bis 192.168.255.255)

Um bei Verwendung privater Adressen von außen auf einzelne Systeme im lokalen Netz zugreifen zu können, kann „Portforwarding“ genutzt werden. Dabei wird auf dem Gateway eine Portadresse festgelegt, bei deren Adressierung die Datenpakete zu einem anderen System weitergeleitet werden. Die Portadresse auf dem Zielsystem kann dabei ebenfalls festgelegt werden. So ist es beispielsweise möglich, unter der Portnummer 2403 des Gateways auf einen internen HTTPS-Webserver (Port 443) zuzugreifen.

7.1.5 Links

Ein „Netzwerklink“ stellt im einfachsten Fall eine Verbindung zwischen zwei Computern dar. Im Collax Security Gateway ist das Konzept der Links auf grundsätzlich jede Netzwerkverbindung ausgeweitet. So kann ein Link auch zwei oder mehr Netze miteinander verbinden.

In jedem Fall stellt ein Link eine Netzwerkverbindung dar. Dabei kann es sich um die Konfiguration einer konkreten Netzwerkschnittstelle handeln, aber auch um mehr abstrakte Konfigurationen wie der einer Route oder eines Tunnels.

Bei allen Linktypen können die erreichbaren Netze angegeben werden. Damit wird eine Routing-Entscheidung vorgenommen, d. h., diese Netze werden auf den Link geroutet.

Im klassischen Modell kann ein Netz nur über einen Link erreichbar sein. Collax Security Gateway geht einen Schritt weiter. Hier kann ein und dasselbe Netz auf mehreren Links als erreichbar angegeben werden. Dies ist möglich, da intern „Policy-Routing“ verwendet wird. Die einzelnen Links zu einem Netz werden priorisiert, und der Link mit der höchsten Priorität wird verwendet. Mittels Link-Überwachung schaltet der Collax Security Gateway im Fehlerfall selbständig zwischen den einzelnen Links um.

Auf einem Link kann „Masquerading“ aktiviert werden. Dabei werden die zum Maskieren ausgewählten Netze aus der Quell-IP-Adresse der Pakete entfernt und durch die eigene IP-Adresse des Collax Security Gateways auf dem jeweiligen Link ersetzt. Die Konfiguration von SNAT oder DNAT hingegen erfolgt im Dialog DNAT/Portweiterleitung (S. 330) oder in Source NAT (S. 333).

Auf einem Link können ein oder mehrere Portweiterleitungen eingerichtet werden. Dabei wird als Port jeweils ein angelegter *Dienst* ausgewählt. Die Adresse, auf der dieser Port angenommen und umgeleitet wird, ist die Adresse auf dem Link selbst. Die Zieladresse (IP-Nummer und Port) für die Umleitung kann frei vergeben werden. Auf dem Zielsystem muss der Collax Security Gateway als Standard-Gateway eingetragen sein, damit Antwortpakete den Weg zurück finden.

7.1.5.1 Ethernet

TCP/IP spezifiziert Protokolle, Adressen und Ports, macht aber keinerlei Angaben über das eigentliche Übertragungsmedium. Der Transport der Daten ist Aufgabe eines untergeordneten Mediums. Dabei handelt es sich im LAN meist um „Ethernet“, dem wichtigsten Typ eines Links.

Ethernet ist eine Vernetzungstechnologie, bei der alle Teilnehmer analog zum Funkverkehr jederzeit zu senden anfangen können (daher auch der Name „Äthernetz“). Praktisch darf zu einem Zeitpunkt immer nur eine Station senden, sonst kommt es im Netz zu Kollisionen. Daher wartet jedes System zunächst, bis das Medium frei ist, und beginnt dann die Übertragung. Der Algorithmus „Carrier Sense Multiple Access with Collision Detection“ CSMA/CD sorgt dafür, dass Kollisionen durch mehrere gleichzeitig sendende Stationen erkannt

werden. Diese Stationen warten dann jeweils eine zufällige, sehr kurze Zeitspanne und senden erneut. Damit dieser Mechanismus sicher funktioniert, müssen die Datenpakete eine Mindestgröße haben (so dass die Übertragung eine minimale „Sendezeit“ nicht unterschreitet).

Diese Betriebsart wird Halbduplex genannt, d. h., bei der Übertragung zwischen zwei Stationen kann nur eine Station senden. Bei Vollduplex hingegen können beide beteiligten Stationen gleichzeitig senden und empfangen, was den Datendurchsatz erhöht.

Thin-Wire-Ethernet

Bei Thin-Wire-Ethernet (10Base2, Standard IEEE 802.3a) wird Koaxialkabel mit einem Wellenwiderstand von 50 Ohm (RG58-Kabel) in Kombination mit BNC-Steckverbindern eingesetzt. Alle angeschlossenen Systeme werden jeweils mit einem T-Stück wie auf einer Perlenkette zu einem Segment miteinander verbunden. Ein solches Segment darf insgesamt bis zu 185 m lang sein und wird an beiden Enden jeweils mit einem Abschlusswiderstand terminiert. Auf Thin-Wire-Ethernet sind Datenraten von 10 MBit/s möglich, die allerdings bei vielen Teilnehmern durch zunehmende Kollisionen nie erreicht werden. Zudem ist es sehr fehleranfällig, da eine einzelne Störung (defektes T-Stück o. ä.) bereits das gesamte Segment lahmlegen kann. Da es mit geringem Aufwand zu installieren ist und außer Netzwerkkarten keine weiteren Komponenten benötigt, war Thin-Wire-Ethernet bis vor wenigen Jahren sehr beliebt.

Twisted-Pair-Ethernet

Bei Twisted-Pair-Ethernet wird Kabel mit acht Adern eingesetzt, von denen je zwei zu einem Paar verdrillt sind. Als Steckverbinder

werden RJ45-Stecker genutzt. Im Gegensatz zu Thin-Wire-Ethernet ist bei TP eine Sternverkabelung notwendig, d. h., ein Hub oder Switch bildet das Zentrum des TP-Ethernets.

Die Kabel werden entsprechend ihrer Qualität und Abschirmung in verschiedene Kategorien unterteilt. Anfangs wurden von den vier Aderpaaren nur zwei zur Übertragung genutzt, zunächst wurden mit CAT-3-Kabeln Datenraten von 10 MBit/s erreicht (10Base-T), später auf CAT-5-Kabeln 100 MBit/s (100-Base-T) und heute ist 1 GBit/s möglich (dann werden allerdings vier Adernpaare genutzt). Varianten mit 10 GBit/s sind in Entwicklung und haben derzeit auf Kupferkabeln eine Reichweite von etwa 15 m.

Durch das zentrale Element ist TP-Ethernet wesentlich unanfälliger für Störungen, da durch Ausfall eines Kabels nur die Verbindung zu einem System unterbrochen ist.

Ein Hub dupliziert alle auf einer Schnittstelle ankommenden Datenpakete auf alle Schnittstellen, daher kann hier das Netzwerk nur im Halbduplex-Betrieb laufen. Jedes System sieht den gesamten Datenverkehr im Netzwerk. Dies ist gleichzeitig gut (für den Einsatz von IDS-Sensoren, die Angriffsmuster erkennen) und schlecht (Passwortsniffer).

Ein Switch ist ein intelligenter Ersatz für den Hub. Er erkennt anhand der MAC-Adresse, welches System an welchem Anschluss erreichbar ist. So schaltet er eingehende Pakete für ein System nur zu dessen Anschluss durch (es sind jedoch Angriffe möglich, um Pakete für andere Systeme auf den eigenen Anschluss geschaltet zu bekommen). Das Netzwerk kann auch im Vollduplex-Modus betrieben werden.

Größere Switches sind "managebar", d. h., sie können über eine Oberfläche verwaltet werden. So lassen sich einzelne Ports sperren, Datenvolumen können protokolliert werden, der gesamte Netzwerkverkehr kann auf einen Monitorport dupliziert werden (etwa für IDS-Sensoren) und vieles weitere mehr.

Glasfaser

Glasfaserkabel oder Lichtwellenleiter (LWL) sind flexible Kabel, deren Kern aus Glasfasern besteht. Diese sind jeweils mit einem Glas mit niedrigem Brechungsindex ummantelt. An der Grenzfläche zwischen Mantel und Faser kommt es zur Totalreflexion des Lichts. Eingespeistes Licht kann daher nahezu verlustfrei über große Entfernungen übertragen werden und ermöglicht gleichzeitig hohe Übertragungsraten bis in den Terabit-Bereich. Glasfaserverbindungen sind unempfindlich gegen elektromagnetische Störungen wie Übersprechen, technische Geräte und Gewitter.

Ethernet-Arten

Physical Layer	Kabelart	Geschwindigkeit	Reichweite	Topologie
10base-5	Koaxial (dick)	10 MBit/s halb-duplex	500 m	Ring
10base-T	Twisted Pair, CAT4, 2 Paare	10 MBit/s halb-duplex	100 m	Stern
100base-T	Twisted Pair, CAT5, 2 Paare	100 MBit/s halb-/vollduplex	100 m	Stern
100baseT4	Twisted Pair, CAT3, 4 Paare	100 MBit/s halb-/vollduplex	100 m	Stern
100baseFX	Glasfaser	100 MBit/s vollduplex	412 m	Point-to-Point, Stern
1000baseT	Twisted Pair, CAT5/6, 4 Paare	1000 Mit/s halb-/vollduplex	100 m	Point-to-Point, Stern
1000baseSX/LX	Glasfaser (short/long laser)	1000 MBit/s vollduplex	550 m/5000 m	Point-to-Point, Stern
10GBase-T	Twisted Pair, CAT 6a/7, 4 Paare	10000 MBit/s vollduplex	100 m	Point-to-Point, Stern

LAN-Adressierung

Neben den eingesetzten Kabeltypen definiert Ethernet auch Zugriffsprotokolle auf diese Medien. Zur Adressierung der einzelnen

Systeme werden „MAC-Adressen“ (Media Access Control) verwendet. Dabei handelt es sich um eine 48 Bit lange Hardwareadresse, die pro Netzwerkschnittstelle weltweit eindeutig sein sollte. Sie kann mit geringem Aufwand auf andere Werte gesetzt werden, ist also nicht fälschungssicher.

Meist wird die MAC-Adresse in der Form 00:D0:59:13:7C:e8 geschrieben. In Ethernet-Paketen taucht sie als Absender- wie auch als Empfängeradresse auf. MAC-Adressen sind nur innerhalb eines Netzwerksegments sichtbar.

Bevor die Kommunikation zwischen zwei Systemen beginnen kann, muss die Adresse des Partners ermittelt werden. Dazu wird das „Address Resolution Protocol“ (ARP) verwendet. Das sendende System fragt ins Netzwerk, welche MAC-Adresse einer bestimmte IP-Nummer entspricht:

```
arp who-has 192.0.2.9 tell 192.0.2.4
```

Das Zielsystem muss auf die IP-Nummer reagieren und seine MAC-Adresse mitteilen:

```
arp reply 192.0.2.9 is-at 00:50:c2:20:e0:8a
```

Hier findet das Zusammenspiel von TCP/IP und Ethernet statt. Aufgelöste MAC-Adressen werden von den Systemen eine Zeit lang im ARP-Cache zwischengespeichert, ein Switch kann anhand seiner ARP-Tabelle die Pakete an die entsprechenden Ports weitergeben.

Konfiguration

Im Collax Security Gateway bleiben all diese technischen Details verborgen, da sie von der Netzwerkkarte entsprechend umgesetzt werden. Sobald die Netzwerkkarte vom Collax Security Gateway mit einem Treiber unterstützt wird, steht die Schnittstelle in der Weboberfläche zur weiteren Konfiguration zur Verfügung.

Auf einem Ethernet-Link wird die IP-Adresse gesetzt, die der

Collax Security Gateway bekommen soll. Bleibt das Feld leer, wird er versuchen eine Adresse per DHCP zu beziehen. Dazu werden die erreichbaren Netze angegeben, meist die Bereiche, aus denen seine eigene IP-Adresse stammt.

7.1.5.2 Datenverkehr ins Internet

Die Verbindung zum Internet (manchmal auch als „Uplink“ bezeichnet) kann über verschiedene Medien und Protokolle hergestellt werden. Dabei hat sich der Begriff des „Wide Area Network“ WAN eingebürgert.

Modem

Ein analoges Modem ist die konsequente Weiterentwicklung des Akustikkopplers, einem Gerät, das digitale Signale in Töne und zurück umsetzt. Damit kann an jeden Telefonanschluss ein Computer zur Datenübertragung angeschlossen werden. Um den Einfluss von Störgeräuschen zu vermeiden, wird die Verbindung beim Modem (von MOdulator/DEModulator) elektrisch hergestellt. Mit vielen technischen Kniffen konnte die Datenrate von ursprünglich 300 Baud auf aktuell 57.600 Baud gesteigert werden.

Auch heute ist ein Modem noch eine weit verbreitete Möglichkeit zur Einwahl ins Internet, da ein normaler Telefonanschluss ausreicht, vorausgesetzt, ein entsprechenden Anschlussadapter ist vorhanden, in Deutschland ist dies meist ein TAE-Adapter.

Als Protokoll auf einer Modemverbindung wird „Point-to-Point Protocol“ PPP verwendet. Zur Authentifizierung kommen die Mechanismen „Paßword Authentication Protocol“ PAP oder „Challenge Handshake Authentication Protocol“ CHAP zum Einsatz. Bei diesen

Verfahren übermittelt der Provider die notwendige Netzwerkkonfiguration, also die eigene IP-Nummer, die IP-Nummer des Gateways auf der Gegenseite sowie die IP-Nummern von Nameservern.

Im Collax Security Gateway muss ein Modem zunächst in der Hardware-Konfiguration angelegt werden, bevor es bei der Konfiguration eines Links genutzt werden kann.

ISDN

ISDN ist im Gegensatz zur Modemverbindung eine rein digitale Verbindung und damit störungsunempfindlicher. ISDN steht für „Integrated Services Digital Network“, d. h., es können verschiedene Dienste über ISDN abgewickelt werden, etwa auch Sprachtelefonie. Ein einfacher ISDN-Anschluss wird mit einem „Netzwerk-Terminierung-Basis-Anschluss“ NTBA bereitgestellt. An diesem können eine ISDN-Karte oder eine TK-Anlage angeschlossen werden. Ein ISDN-Anschluss verfügt über zwei Kanäle mit je 64 kBit Bandbreite. Bei Datenübertragungen mit dem Computer können beide Kanäle mittels „Channel-Bundling“ zu 128 kBit zusammengeschaltet werden – dabei fallen natürlich auch doppelte Telefonkosten an.

Auf den ISDN-Anschluss können verschiedene Telefonnummern geschaltet werden. Im Gegensatz zum Modem, welches eingehende Anrufe einfach mit *RING* meldet, wird auf dem ISDN-Bus die angerufene Nummer signalisiert und das Endgerät muss reagieren.

Auch bei ISDN erfolgt die Interneteinwahl über PPP mit PAP oder CHAP.

Im Collax Security Gateway wird eine ISDN-Karte beim Starten des Systems automatisch erkannt und eingebunden. In der Hardware-Konfiguration muss zunächst eine Rufnummer (MSN) für die Karte eingestellt werden. Danach kann sie als Link konfiguriert werden. Dabei ist neben der Einwahl ins Internet auch der umgekehrte Weg

möglich, indem der Collax Security Gateway selbst die Einwahl annimmt.

DSL

„Digital Subscriber Line“ (DSL) ist eine Technik, die eine Internetanbindung mit hohen Datenraten ermöglicht. Das Problem des normalen Telefonnetzes ist, dass die Bandbreite nur auf Sprache ausgelegt ist und hohe sowie tiefe Frequenzen abgeschnitten werden. Damit ist das technisch Mögliche mit aktuellen 56k-Modems weitgehend ausgereizt.

Bei DSL wird die begrenzte Bandbreite ausgenutzt und ein hochfrequentes Signal zum normalen Sprach- oder ISDN-Signal gemischt. In diesem Signal werden Daten übertragen, damit sind durchaus Bandbreiten im MBit-Bereich möglich. Problematisch ist, dass die hochfrequenten DSL-Signale stark gedämpft werden und daher nur über kurze Strecken übertragen werden können. Für DSL wird in der nächsten Vermittlungsstelle ein „DSL-Multiplexer“ installiert, der das DSL-Signal herausfiltert, daraus die IP-Pakete extrahiert und diese auf den IP-Backbone des Providers weiterleitet. Es ist also nicht möglich, jemanden über DSL „anzurufen“.

Ist die Entfernung zwischen der Vermittlungsstelle und dem Telefonanschluss zu groß, ist die realisierbare Datenrate eventuell gering, oder es ist sogar (mit vertretbarem Aufwand) nicht möglich, eine DSL-Verbindung herzustellen. Zudem kann das DSL-Signal nur auf Kupferleitungen aufmoduliert werden, bei Telefonanschlüssen auf Glasfaserbasis ist es nicht möglich. Hier kann DSL nur am Übergabepunkt von der Glasfaser zum Hausnetz genutzt werden, allerdings müssen in diesem Fall jeweils sogenannte „Outdoor-DSLAMs“ pro Wohnblock oder Straßenzug installiert werden, was höhere Kosten verursacht als die Installation von Technik in der Vermittlungsstelle.

Typischerweise wird ein asymmetrischer Anschluss („ADSL“) gelegt, bei dem Up- und Downstream verschieden groß sind, etwa 192 kBit Upstream und 1 MBit Downstream. Damit ist schnelles Surfen möglich, da nur kleine Datenmengen ins Internet geschickt werden, aber große Datenmengen heruntergeladen werden. Für Firmen sind symmetrische DSL-Anschlüsse („SDSL“) sinnvoller, hier ist die Datenrate für Up- und Downstream gleich, etwa 512 kBit oder 2 MBit. Dies ist für den Betrieb eines Webservers oder für VPN-Verbindungen sinnvoller.

Bei DSL werden die IP-Pakete mit einem speziellen Protokoll transportiert, typischerweise kommen hier PPPoE („PPP over Ethernet“) und PPTP („Point-to-Point Tunneling Protocol“) zum Einsatz. Beide Varianten werden vom Collax Security Gateway unterstützt und können in der Konfiguration des Links ausgewählt werden.

7.1.5.3 Tunnel

Routing im Internet erfordert, dass alle Systeme auf dem Weg von einem Computer zu einem zweiten die Ziel-IP-Adresse kennen und die Pakete in die richtige Richtung weiterleiten. Wenn jedoch zwei Standorte mit privaten IP-Nummern im lokalen Netz über das Internet verbunden werden sollen, geht dies nicht mit den normalen Routingmechanismen.

Abhilfe schafft die Verwendung eines Tunnels. Dabei wird eine IP-Verbindung zwischen zwei Gateways, typischerweise jeweils das Internet-Gateway an beiden Standorten, hergestellt. Datenpakete aus dem lokalen Netz der einen Seite zur anderen werden am ersten Gateway als Nutzlast in ein neues Datenpaket verpackt. Dieses wird über das Internet zum Gateway der anderen Seite transportiert; dieser Vorgang heißt „tunneln“. Das Gateway auf der anderen Seite

entnimmt dem ankommenden Datenpaket das originale IP-Paket und kann es im lokalen Netz auf seiner Seite zustellen.

Im einfachsten Fall werden Daten unverschlüsselt durch den „IP-Tunnel“ übertragen. Soll die Verbindung sicherer sein, werden die eingepackten Datenpakete verschlüsselt übertragen. Ein solches Szenario wird als „Virtual Private Network“ VPN bezeichnet.

7.1.5.4 VPN

VPN steht für „Virtual Private Network“ und bezeichnet eine Technik, bei der Computernetze über ein Medium, meist das Internet, verbunden werden. Meist werden die Daten zwischen beiden Netzen verschlüsselt und mit Prüfsummen gesichert übertragen.

Es gibt verschiedene Protokolle, die ein VPN aufbauen können. Das bekannteste ist „IPsec“ („IP Security“), welches von vielen Systemen unterstützt wird. Leider sprechen verschiedene Systeme teilweise unterschiedliche Dialekte, so dass die Konfiguration eines IPsec-Tunnels mitunter schwieriger ist. Im Collax Security Gateway wird eine freie Softwarelösung eingesetzt, um eine möglichst hohe Kompatibilität zu erreichen.

Eine andere verbreitete VPN-Lösung ist „PPTP“ („Point-to-Point Tunneling Protocol“), welches in der Windows-Welt weit verbreitet ist. Der Collax Security Gateway kann als PPTP-Einwahlserver konfiguriert werden, so dass Windows-Clients eine VPN-Verbindung in ein Firmennetz aufbauen können. Experten haben Kritik an einigen Aspekten von PPTP geäußert, was die Sicherheit betrifft. Microsoft hat daraufhin einen verbesserten Verschlüsselungsalgorithmus MPPE („Microsoft Point-To-Point Encryption“) entwickelt.

IPsec selbst stellt zwei Verbindungen bereit. Zunächst die IKE-Verbindung („Internet Key Exchange“), bei der ausgehend von einer

Passphrase PSK („Pre-Shared Key“) oder einem Zertifikat eine gesicherte Verbindung zwischen beiden IPsec-Endpunkten aufgebaut wird. Auf dieser Verbindung wird dann von den Systemen ein Schlüssel für die weitere Verbindung erzeugt. Diese wird in der zweiten Verbindung genutzt, der ESP-Verbindung („Encrypted Secured Payload“). Über ESP werden dann die Nutzdaten übertragen. Als Schlüssel kommt bei ESP ein symmetrischer zum Einsatz, um den Overhead gering zu halten. Dieser Schlüssel wird in regelmäßigen Abständen neu generiert, um einen Angriff weiter zu erschweren.

In einem VPN-Tunnel kann bei Unterstützung durch die Gegenstelle Kompression aktiviert werden, so dass je nach übertragenen Daten ein höherer Datendurchsatz als bei der reinen Internetverbindung möglich ist.

Unter *Netzwerk – Links – Allgemein* finden Sie in der Oberfläche des Collax Security Gateways eine für VPN relevante Option. Durch Aktivieren von *NAT-Traversal* wird bei jedem Tunnelaufbau geprüft, ob die Gegenseite hinter einem maskierenden Router angeschlossen ist (NAT). Ist dies der Fall, werden die IPsec-Pakete in UDP-Pakete eingepackt und verschickt. Wird kein NAT erkannt, wird der Tunnel normal betrieben.

7.1.5.5 Link-Failover

Auf dem Collax Security Gateway findet eine permanente Link-Überwachung statt. Diese kontrolliert, ob auf den aktiven, konfigurierten Links Daten übertragen werden. Bei Ausfall eines Links wird der Link neu gestartet. Existieren zu einem Netz mehrere Links mit unterschiedlichen Prioritäten, schaltet eine aktivierte Link-Überwachung automatisch auf den Link mit der nächsten Priorität um, falls der Neustart nicht zum Erfolg geführt hat.

Beim Einsatz von VPN kann damit der Ausfall eines Tunnels schneller erkannt und der Neuaufbau des Tunnels schneller eingeleitet werden.

Hinweis: Die Umschaltung zurück auf einen höher priorisierten Link erfolgt selbständig, sobald dieser Link wieder funktionsfähig ist. Dadurch kann eine Verbindung erneut getrennt werden (etwa bei Rückschaltung von ISDN zu DSL).

7.1.5.6 Bandbreitenmanagement

„Quality of Service“ (QoS) bezeichnet Verfahren, bei denen einzelnen Diensten eine bestimmte Verbindungsqualität garantiert wird. Solche Verfahren sind mit zunehmender Nutzung von Echtzeit-Datenverbindungen immer wichtiger. Collax Security Gateway bietet mit seinem integrierten Bandbreitenmanagement die Möglichkeit, solches QoS umzusetzen. Die Implementierung arbeitet unidirektional, d. h., es ist keinerlei Unterstützung durch die Gegenstelle notwendig bzw. möglich. Dabei wird QoS nur auf ausgehende Daten angewandt, der Empfang von Daten ist nicht beeinflussbar.

Bei TCP-Verbindungen wird der Empfang jedes Pakets quittiert. Bleiben die Empfangsbestätigungen aus, wartet der Sender mit dem Versand weiterer Pakete. Kommen die Bestätigungen mit Verzögerung, stockt die Übertragung insgesamt. Gerade bei unsymmetrischen DSL-Anschlüssen kann es bei Verbindungen mit hohem Datenvolumen in beide Richtungen zu derartigen Situationen kommen. Dabei ist nicht immer die Bandbreite der Engpass. VoIP-Verbindungen benötigen beispielsweise wenig Bandbreite, stattdessen erfordern sie eine geringe Latenz (Laufzeitverzögerung).

Bei Nutzung des Bandbreitenmanagements wird jeder Netzwerkschnittstelle ein Pufferspeicher vorgeschaltet, die „Queueing Disci-

pline“, kurz QDisc genannt. Im Normalfall funktioniert eine QDisc nach dem FIFO-Prinzip („First In, First Out“), d. h., die Daten werden in der Reihenfolge versandt, in der sie bei der Netzwerkschnittstelle eintreffen. Es ist jedoch innerhalb einer QDisc auch möglich, bestimmte Verbindungen bevorzugt zu behandeln und so bestimmte Garantien oder Begrenzungen für Bandbreite und Latenz durchzusetzen.

Bandbreitenmanagement wird im Collax Security Gateway auf einem Link aktiviert. Dies ist nur auf Links möglich, die direkt auf einer Netzwerkschnittstelle aufsetzen. Bei einem Internetzugang über einen Router ist dies auf dem „RouterLink“ (Typ „Ethernet“) möglich, nicht hingegen auf dem „InternetLink“ (Typ „Route“). Auf dem Link wird auch die (ausgehende) Bandbreite der Schnittstelle festgelegt.

Bei den allgemeinen Einstellungen der Links kann der Queueing-Algorithmus festgelegt werden, der für alle QDiscs verwendet wird. Zur Auswahl stehen die Verfahren HTB („Hierarchical Token Bucket“) und H-FSC („Hierarchical Fair Service Curve“). HTB ist einfach zu konfigurieren und kann gewählt werden, wenn keine besondere Anforderung an die Latenz besteht. H-FSC unterscheidet die beiden Parameter Bandbreite und Verzögerungszeit und ist daher für QoS bei VoIP und Audio-/Video-Streaming die geeignete Wahl.

Ist das Bandbreitenmanagement auf einem Link aktiviert, lassen sich für den Link Traffic-Klassen anlegen, bei denen eine maximale Verzögerung, eine garantierte Rate und eine maximale Rate festgelegt werden kann. Bei HTB wird die Priorität der Klasse angegeben. Die Priorität ist für die Verteilung von ungenutzter Bandbreite entscheidend. Klassen mit höherer Priorität bekommen die überschüssige Bandbreite immer zuerst angeboten.

In der Firewallmatrix kann nun auf Diensteebene für Verbindungen, die Links mit aktiviertem Bandbreitenmanagement nutzen, die Traffic-Klasse festgelegt werden. So ist es möglich, für FTP ins

Internet beispielsweise maximal 20% der Bandbreite zu benutzen und gleichzeitig den SIP-Verbindungen eine kurze Latenz zu garantieren.

7.1.5.7 Policy-Based Routing

(Diese Option befindet sich im Zusatzmodul *Collax Advanced Networking*)

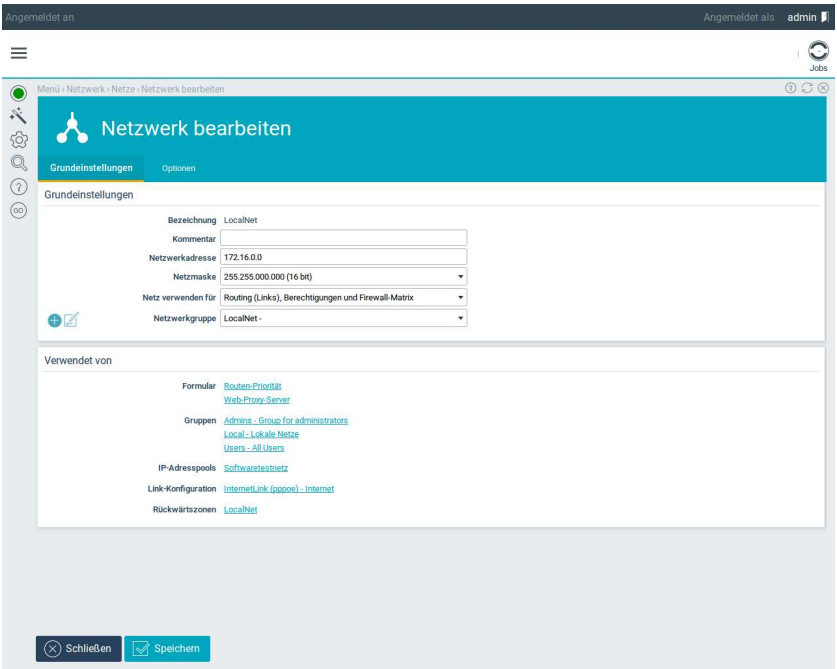
In modernen Netzwerken wird von Unternehmen immer mehr von der Möglichkeit Gebrauch gemacht, Netzwerkpakete nach individuellen Richtlinien weiterzuleiten. Diese Richtlinien gehen über die Methode des traditionellen Routing hinaus.

Normalerweise werden Pakete aufgrund von Informationen aus der Routing-Tabelle zu ihrem Ziel geleitet. Verwendet man Policy-Based Routing können Netzwerkpakete auch aufgrund ihrer Quell-Adresse und ihres Protokolltyps geroutet werden.

Das Policy-Routing betrachtet nicht nur Pakete, die durch die Firewall geleitet werden. In vielen Anwendungsbereichen ist es stattdessen erforderlich, Pakete von lokal gestarteten Diensten über bestimmte Netzwerk-Verbindungen zu leiten. So wird durch das Policy-Routing die Möglichkeit geschaffen System-Updates, Virenscanner-Updates, Web-Proxy-Verkehr oder E-Mail-Traffic über unterschiedliche Netzwerkverbindungen zu leiten.

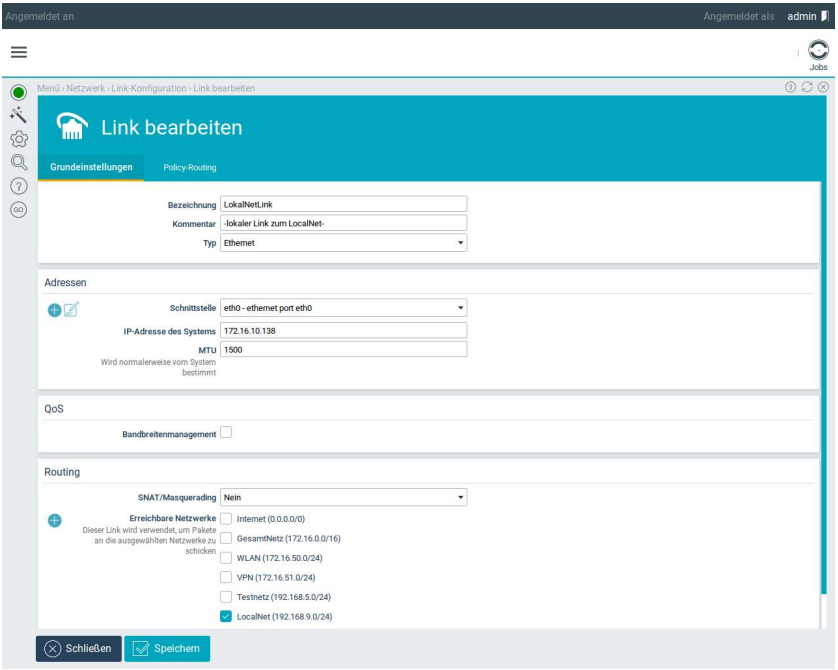
7.2 Schritt für Schritt: Einrichten des lokalen Netzes

Einer der ersten Schritte bei der Konfiguration des Collax Security Gateways ist das Einrichten des lokalen Netzwerks. Dazu gehören der IP-Bereich und die IP-Adresse des Collax Security Gateways in diesem Netz.



- Wechseln Sie zu *Netzwerk – Netze – Konfiguration*.
- Bearbeiten Sie das *LocalNet*, welches bereits in der Grundeinstellung vorhanden ist.
- Tragen Sie unter *Netzwerkadresse* die Basisadresse Ihres lokalen IP-Bereichs ein. Dies ist nicht die IP-Adresse, die der Collax Security Gateway später verwenden wird.

- Prüfen Sie die *Netzwerkmaske*.
- Speichern Sie das geänderte Netzwerk.



- Unter *Netzwerk – Links – Konfiguration* sind alle angelegten Links aufgelistet.
- Bearbeiten Sie den *LocalNetLink*, der ebenfalls in der Grundeinstellung vorhanden ist.
- Unter *Typ* legen Sie fest, welcher Art der Link ist. Mit dem lokalen Netz wird der Collax Security Gateway üblicherweise über ein Netzwerkkabel verbunden, die entsprechende Einstellung ist daher *Ethernet*.
- Die IP-Adresse des Collax Security Gateways tragen Sie unter *IP-Adresse des Systems* ein. Diese IP-Adresse muss unbedingt zu dem Netzwerkbereich des *LocalNets* gehören.

- Unter *Schnittstelle* legen Sie die Netzwerkkarte fest, an der das lokale Netz angeschlossen ist. Üblicherweise wird dazu die erste Netzwerkkarte im System verwendet, also *eth0*.
- Unter *Erreichbare Netzwerke* legen Sie fest, welche Netze (IP-Bereiche) auf diesen Link geroutet werden. Hier wird nur das *LocalNet* markiert, das *Internet* ist auf dem Netzwerkkabel an *eth0* nicht erreichbar.
- Speichern Sie Ihre Änderungen.

7.3 GUI-Referenz: *Netze*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Netze* sowie unter *Netzwerk – Netze – Konfiguration*)

In diesem Dialog werden alle angelegten Netzwerke angezeigt. Ein Netzwerk umfasst einen IP-Bereich, der in den Dialogen zu den *Links* auf Interfaces oder Routen geschaltet werden kann.

In diesem Dialog können weitere Netzwerke angelegt bzw. vorhandene Netze bearbeitet oder gelöscht werden.

Hinweis: Das vordefinierte Netzwerk *Internet* umfasst alle IP-Nummern dieser Welt außer denen, die in anderen hier angelegten Netzwerken spezifiziert sind. Dieses Netzwerk wird zum Routen ins Internet benötigt. Es kann daher nicht bearbeitet werden.

7.3.1 *Netzwerk wählen*

In diesem Dialog können ein Netzwerk zum Bearbeiten oder Löschen ausgewählt und weitere Netzwerke anlegt werden.

7.3.1.1 Felder in diesem Dialog

- *Bezeichnung*: Hier wird die Bezeichnung des Netzwerks angezeigt.
- *Netzwerkadresse*: In diesem Feld wird die zugehörige Netzwerkadresse angezeigt.
- *Netzmaske*: Über die hier angezeigte Netzmaske ergibt sich die Größe des Netzwerkbereichs.

7.3.1.2 Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion können die Einstellungen für ein Netzwerk geändert werden.
- *Löschen*: Mit dieser Aktion wird das angezeigte Netzwerk gelöscht.

7.3.1.3 Aktionen für diesen Dialog

- *Netzwerk anlegen*: Mit dieser Schaltfläche wird der Dialog zum Anlegen eines neuen Netzwerks geöffnet.

7.3.2 *Netzwerk bearbeiten*

In diesem Dialog werden für ein Netzwerk die Netzwerkadresse und die Netzmaske festgelegt und eine Bezeichnung vergeben.

Hinweis: Wird die Netzwerkadresse oder die Netzmaske eines Netzes geändert, kann es geschehen, dass eine IP-Adresse eines dem Netz zugeordneten Links außerhalb des Netzwerkes liegt. Solche Links werden nicht automatisch aus dem Netz entfernt oder einem anderen Netz zugeordnet. Als Folge ist das System eventuell nicht mehr erreichbar.

In solchen Fällen wird eine Warnung ausgegeben. Die Einstellungen werden dennoch gespeichert.

7.3.2.1 Tab *Grundeinstellungen*, Abschnitt *Grundeinstellungen*

Felder in diesem Abschnitt

- *Bezeichnung des Netzwerks*: Hier wird die Bezeichnung für das Netzwerk angegeben. Unter diesem Namen wird das Netzwerk in verschiedenen anderen Dialogen zur Auswahl angeboten.

  Diese Bezeichnung kann nachträglich nicht mehr geändert werden.
- *Bezeichnung*: Wird ein bereits angelegtes Netzwerk bearbeitet, wird das Feld *Bezeichnung* nur angezeigt, es kann nicht geändert werden.
- *Netzwerkadresse*: In diesem Feld wird die Adresse des Netzwerks festgelegt.
- *Netzmaske*: In diesem Feld wird die zugehörige Netzmaske für das Netzwerk eingestellt. Dabei können beide Schreibweisen (*255.255.255.0* und */24*) ausgewählt werden.
- *Netz verwenden für*: Ein Netzwerk kann für entweder für die

lokalen Benutzungsrichtlinien und in den Regeln der Firewall-Matrix, oder für lokales Routing, lokale Benutzungsrichtlinien und Regeln der Firewall-Matrix verwendet werden. Wird es für lokales Routing verwendet, kann das Netzwerk nicht nur als Element für Gruppenberechtigungen oder Firewall-Regeln verwendet werden, sondern es kann auch über die Link-Konfiguration als erreichbares Netzwerk geroutet werden.

- *Link*: Für neu angelegte Netzwerke kann bereits ein Link ausgewählt werden, auf dem das Netzwerk *erreichbar* ist. Es ist nur möglich, einen einzelnen Link auszuwählen. Weitere Einstellungen können in der „Link-Konfiguration“ vorgenommen werden.

7.3.2.2 Tab *Gruppenzugehörigkeit*, Abschnitt *Gruppenzugehörigkeit* Felder in diesem Abschnitt

- *Einstellungen*: Das bearbeitete Netz ist Mitglied in allen aktivierten Gruppen. Über die Gruppen werden in den *Benutzungsrichtlinien* Berechtigungen für Systeme aus den einzelnen Netzwerkbereichen vergeben.

7.3.2.3 Tab *Optionen*, Abschnitt *Optionen* Felder in diesem Abschnitt

- *Proxy-ARP aktivieren*: Normalerweise sind Systeme innerhalb eines Netzwerkbereichs in einem Netzwerksegment angeschlossen. Sie kommunizieren direkt über das ARP-Protokoll auf Ethernet-Ebene miteinander.

  In bestimmten Konfigurationen ist es sinnvoll, einzelne Rechner in anderen Segmenten anzuschließen, etwa ein Server in eine

DMZ. Wird seine IP-Adresse dabei nicht geändert, ist er für die anderen Systeme „unsichtbar“ (da Ethernet-Pakete nicht über Router weitergeleitet werden).

Durch das Aktivieren von Proxy-ARP erkennt der Collax Security Gateway ARP-Anfragen auf einem Segment für ein System, welches auf einem anderen Segment angeschlossen ist, und beantwortet diese. Dadurch erhält er selbst das Paket und kann es auf das richtige Netzwerksegment weiterleiten. Eine solche Konfiguration wird manchmal als „Pseudo Bridging“ bezeichnet.

Hinweis: Falsch eingesetzt kann ein aktiviertes Proxy-ARP zu erheblichen Störungen im Netzwerk führen.

- *Schnittstellen für Proxy-ARP*: Hier wird die Schnittstellen ausgewählt, auf denen ARP-Anfragen beantwortet werden sollen. Die Liste enthält nur die Ethernet-Schnittstellen, die durch einen Link vom Typ *Ethernet* in Verwendung sind.

7.4 GUI-Referenz: Links

Im Gegensatz zu den Netzen behandeln Links eine konkrete Schnittstellenkonfiguration und dienen der Einrichtung des Routings. Links können für verschiedenste Anwendungen eingerichtet werden. Der einfachste Fall ist die Einrichtung einer Netzwerkschnittstelle mit dem Setzen der IP-Adresse des Collax Security Gateways.

Genauso ist es über Links möglich, Routen zu setzen, eine Internet-Einwahl über DSL einzurichten oder Datentunnel aufzubauen.

7.4.1 *Links – Allgemein*

(Diese Option befindet sich im Zusatzmodul *Collax Gatekeeper*)
(Dieser Dialog befindet sich unter *Netzwerk – Links – Allgemein*)
In diesem Dialog werden allgemeine Einstellungen für die Links vorgenommen.

7.4.1.1 Abschnitt *VPN*

In diesem Abschnitt werden globale VPN-Optionen konfiguriert.

Felder in diesem Abschnitt

- *NAT-Traversal aktivieren*: NAT-Traversal ist eine Technik, mit der ein VPN-Client hinter einem maskierenden Router einen VPN-Tunnel aufbauen kann. Dazu werden die IPsec-Pakete in UDP-Pakete eingepackt, die gefahrlos maskiert werden können. Dies ist eine globale Option, die bei ihrer Aktivierung für jeden Verbindungsaufbau einzeln geprüft und ggf. verwendet wird.
- *Standard-Proposal*: Hier wird ein definiertes IPsec-Proposal als Standard definiert.

7.4.1.2 Abschnitt *Bandbreitenmanagement*

Über das Bandbreitenmanagement lassen sich für verschiedene Verbindungen Garantien oder Beschränkungen für Bandbreiten oder Latenzzeiten einrichten.

Felder in diesem Abschnitt

- *Queueing-Algorithmus*: Hier muss einer der beiden unterstützten Algorithmen ausgewählt werden:

  HTB erlaubt es, Klassen eine garantierte und eine maximale Bandbreite zuzuordnen. Jeder Klasse wird zudem eine Priorität zugeordnet, ungenutzte Bandbreite wird nach Priorität verteilt.

  HTB ist einfach zu konfigurieren und sollte ausgewählt werden, wenn keine besondere Anforderung an die Latenz („Verzögerungszeit“) besteht.

  H-FSC ist ein Algorithmus, der Klassen neben garantierter und maximaler Bandbreite unabhängig von der garantierten Bandbreite zusätzlich eine garantierte Latenz zuordnen kann.

  H-FSC sollte gewählt werden, wenn besondere Anforderungen an die Latenzzeiten bestehen, beispielsweise für VoIP oder Audio-/Video-Streaming.

  Hinweis: Die Konfigurationen von HTB und H-FSC sind nicht kompatibel. Es wird für beide Algorithmen eine eigene Konfiguration gespeichert, wobei immer nur eine aktiv ist und bearbeitet werden kann.
- *Detail-Level*: Hier kann der Detail-Level des verwendeten Algorithmus eingestellt werden. Der Level „Hoch“ ergänzt die Einstellungsmöglichkeiten der Traffic-Klassen eines Links mit Bandbreiten-Management.

7.4.2 *Link-Konfiguration*

In diesen Dialogen werden die Netzwerkverbindungen des Collax Security Gateways konfiguriert. Solche Verbindungen werden als *Links* bezeichnet.

7.4.2.1 *Link wählen*

(Dieser Dialog befindet sich unter *Netzwerk – Links – Link*)

In dieser Übersicht werden alle vorhandenen Links angezeigt. Hier können weitere Links angelegt oder vorhandene Links bearbeitet oder gelöscht werden.

Felder in diesem Dialog

- *Bezeichnung*: Hier wird die Bezeichnung des Links angezeigt. Unter diesem Namen wird der Link in weiteren Dialogen verwendet.
- *Typ*: Hier wird der Typ des Links angezeigt.
- *Kommentar*: Hier wird ein Kommentartext zum Link angezeigt.

Aktionen für jeden Tabelleneintrag

- *Link bearbeiten*: Mit dieser Aktion können die Einstellungen eines Links bearbeitet werden.
- *Traffic-Klassen*: Mit dieser Aktion können die auf dem Link verfügbaren Traffic-Klassen verwaltet werden. Diese Aktion ist nur verfügbar, wenn in der Konfiguration des Links *Bandbreitenmanagement* aktiviert und die maximale Bandbreite des Links gesetzt wurde.
- *Firewall*: Mit dieser Aktion können Portumleitungen und Dienstsperren in der Firewall des Systems eingerichtet werden.

- *Löschen*: Diese Aktion löscht den Link.

Aktionen für diesen Dialog

- *Link hinzufügen*: Mit dieser Aktion wird ein neuer Link hinzugefügt.

7.4.2.2 *Link bearbeiten*

(Dieser Dialog befindet sich unter *Netzwerk – Links – Link*)

In diesem Dialog werden die Einstellungen eines Links geändert.

In diesem Dialog werden die Konfigurationseinstellungen zu einem Link angegeben.

Abhängig von der unter *Typ* eingestellten Art des Links werden verschiedene Optionen ein- und ausgeblendet. Im folgenden werden die unterschiedlichen Linktypen mit ihren jeweiligen Optionen vorgestellt.

Felder in diesem Dialog für Typ *Ethernet*

- *Bezeichnung*: Hier muss eine eindeutige Bezeichnung für den Link angegeben werden. Unter diesem Namen steht der Link in verschiedenen anderen Dialogen zur Verfügung.
- *Kommentar*: Hier kann ein Kommentartext zu diesem Link angegeben werden.
- *Typ*: Hier wird der genaue Typ des Links angegeben. Abhängig davon werden weitere Felder in diesem Dialog sichtbar bzw. unsichtbar.
- *IP-Adresse des Systems*: Hier wird die lokale IP-Adresse für den Link angegeben. Bleibt das Feld leer, versucht das System, eine

dynamische IP-Adresse per PPP oder DHCP zu beziehen. Sollen mehrere IP-Adressen auf einen Netzwerkanschluss zugewiesen werden (IP-Alias), muss für jede IP-Adresse ein eigener Link angelegt werden. Dabei wird jedes Mal die gleiche Schnittstelle angegeben.

- *MTU*: Hier kann die maximale Paketgröße auf diesem Link eingestellt werden.

  Große Werte für die MTU verbessern den Durchsatz, da weniger Verwaltungsdaten übertragen werden. Kleine Werte für die MTU hingegen verbessern die Antwortzeiten für interaktive Anwendungen und Echtzeitdatenübertragung (etwa VoIP).

  Wird hier kein Wert eingetragen, wird abhängig von der Art des Links ein geeigneter Wert gewählt. Für Ethernet-Verbindungen wird typischerweise eine MTU von 1500 Byte verwendet.
- *Bandbreitenmanagement*: Mit dieser Option wird das Bandbreitenmanagement für den Link aktiviert. Für indirekte Links, die auf einen anderen Link aufsetzen (Typ Route, Tunnel, VPN usw.) muss auf dem untergeordneten Link bereits das Bandbreitenmanagement aktiviert sein.
- *Bandbreite*: Hier wird die Bandbreite des Links angegeben. Für die Bandbreite von indirekten Links (Typ Route, Tunnel, VPN usw.) ist die Bandbreite des benutzten Links entscheidend.

  Wenn sich mehrere Links eine Hardwareschnittstelle teilen (z. B. LocalNetLink1 und LocalNetLink2 jeweils über eth0), darf die Summe der Bandbreiten der Links die Bandbreite der Hardwareschnittstelle selbst nicht überschreiten.

  In diesem Feld wird als Eingabe eine Dezimalzahl, optional mit Dezimalpunkt, optional gefolgt von Leerzeichen und abschließend einer Einheit erwartet. Folgende Einheiten sind möglich: „k“ für Kilo, „M“ für Mega und „G“ für Giga. Abschließend wird die Einheit als „bps“ für 8 bit/s oder „bit“ für bit/s angegeben. Beispiele: „15.7 kbit“, „100 Mbit“ und „1 Gbit“.

- *Schnittstelle*: Wird für den Link eine Schnittstelle benötigt, kann diese hier eingestellt werden.
- *SNAT/Masquerading*: SNAT und Masquerading dienen dazu, ganze Netzwerke hinter einer einzelnen IP-Adresse zu „verstecken". Wird diese Option aktiviert, scheinen alle abgehenden Verbindungen von diesem System zu stammen und nicht vom wirklichen Absender.

  Diese Option muss aktiviert werden, wenn auf dem Internet-Link vom Provider nur eine einzelne IP-Adresse bereitgestellt wird und wenn Systeme aus dem lokalen Netz IP-Verbindungen aufbauen müssen.

  Die Unterscheidung zwischen SNAT und Masquerading erfolgt automatisch, abhängig davon, ob eine IP-Adresse für den Link angegeben wurde oder nicht.

  Hinweis: SNAT/Masquerading für Routen und VPN-Netze funktioniert nur, wenn auf dem unterliegenden Link kein Masquerading aktiviert ist.
- *Zu maskierende Netzwerke*: Wird Masquerading für *spezielle Netze* aktiviert, können in dieser Liste aus allen angelegten Netzwerken diejenigen ausgewählt werden, die maskiert werden müssen.

  Hinweis: Alle Subnetze eines ausgewählten Netzwerks werden ebenfalls maskiert.

  Wird ein Netzwerk aus der Liste ausgewählt, bedeutet das nicht automatisch, dass Daten aus diesem Netzwerk über diesen Link versendet werden können.
- *Erreichbare Netzwerke*: Hier können aus der Liste aller angelegten Netzwerken diejenigen ausgewählt werden, die über diesen Link erreichbar sind. Für jedes ausgewählte Netz wird ein Eintrag unter *Zuordnungen* angelegt.

  Bei VPN-Verbindungen muss das lokale Netz der Gegenstelle innerhalb einem der hier angegebenen Netze liegen.

- *Verifikation von MAC-Adressen*: Für Ethernet-Links kann der Zugriff auf das System auf bekannte und verifizierte Hosts beschränkt werden. Pakete von fremden Systemen werden dann verworfen. Zwei verschiedene Arten der Adressverifikation sind möglich:

  IP+MAC-Verifikation nimmt nur Pakete an, wenn die Absender-IP-Adresse von einem bestätigten, bekannten Host kommt und die MAC-Adresse mit der Adresse in der Hosts-Konfiguration übereinstimmt.

  Bei der *MAC*-Verifikation werden nur Pakete angenommen, deren Absender-MAC-Adresse einem bekannten und bestätigten Host gehört. Es wird nicht überprüft, ob die MAC-Adresse zu der entsprechenden IP-Adresse gehört. Diese Option wird genutzt, wenn DHCP verwendet wird.

  Hinweis: Vor dem Aktivieren dieser Option müssen die Systeme im lokalen Netz und allen anderen direkt angeschlossenen Ethernet-Segmenten im Collax Security Gateway angelegt und bestätigt werden. Zudem ist der Sicherheitsgewinn nicht sehr groß, da eine MAC-Adresse ohne großen Aufwand per Software geändert werden kann.

Tab Policy-Routing

- *Traffic-Policies*: Hier werden die Policies ausgewählt, die dafür sorgen, dass die entsprechenden Netzwerkpakete oder Dienste bevorzugt über diesen Link geleitet werden. Hier können Policies ausgewählt werden, die unternehmenskritischen Datenverkehr kennzeichnen. Werden hier Policies gewählt, die einen lokalen Service, wie Web-Proxy kennzeichnen, wird als Folge der Datenverkehr dieses Dienstes nur über diesen Link abgewickelt. Wenn ein zusätzlicher Link in das Zielnetzwerk als Fall-Back-Verbindung definiert ist, wird der Datenverkehr bei Link-Ausfall über diese Fall-Back-Verbindung geleitet.

- *Nur diese Traffic-Policies zulassen*: Mit dieser Option werden ausschließlich die Netzwerkpakete über den Link geroutet, die den Traffic-Policies entsprechen. Default-Routen, die unter dem Menüpunkt *Zuordnungen* gesetzt sind, werden nicht mehr berücksichtigt. Wenn nicht klar ist, was diese Option bedeutet, sollte sie leergelassen werden.

Felder in diesem Dialog für Typ *Route*

- *Bezeichnung*: Hier muss eine eindeutige Bezeichnung für den Link angegeben werden. Unter diesem Namen steht der Link in verschiedenen anderen Dialogen zur Verfügung.
- *Kommentar*: Hier kann ein Kommentartext zu diesem Link angegeben werden.
- *Typ*: Hier wird der genaue Typ des Links angegeben. Abhängig davon werden weitere Felder in diesem Dialog sichtbar bzw. unsichtbar.
- *IP-Adresse der Gegenstelle*: Hier wird die IP-Adresse der Gegenstelle angegeben. Bleibt das Feld leer, versucht das System, die Adresse der Gegenstelle automatisch zu bestimmen.
- *MTU*: Hier kann die maximale Paketgröße auf diesem Link eingestellt werden.

  Große Werte für die MTU verbessern den Durchsatz, da weniger Verwaltungsdaten übertragen werden. Kleine Werte für die MTU hingegen verbessern die Antwortzeiten für interaktive Anwendungen und Echtzeitdatenübertragung (etwa VoIP).

  Wird hier kein Wert eingetragen, wird abhängig von der Art des Links ein geeigneter Wert gewählt. Für Ethernet-Verbindungen wird typischerweise eine MTU von 1500 Byte verwendet.
- *Bandbreitenmanagement*: Mit dieser Option wird das Bandbreitenmanagement für den Link aktiviert. Für indirekte Links, die

auf einen anderen Link aufsetzen (Typ Route, Tunnel, VPN usw.) muss auf dem untergeordneten Link bereits das Bandbreitenmanagement aktiviert sein.

- *Bandbreite*: Hier wird die Bandbreite des Links angegeben. Für die Bandbreite von indirekten Links (Typ Route, Tunnel, VPN usw.) ist die Bandbreite des benutzten Links entscheidend.

  Wenn sich mehrere Links eine Hardwareschnittstelle teilen (z. B. LocalNetLink1 und LocalNetLink2 jeweils über eth0), darf die Summe der Bandbreiten der Links die Bandbreite der Hardwareschnittstelle selbst nicht überschreiten.

  In diesem Feld wird als Eingabe eine Dezimalzahl, optional mit Dezimalpunkt, optional gefolgt von Leerzeichen und abschließend einer Einheit erwartet. Folgende Einheiten sind möglich: „k“ für Kilo, „M“ für Mega und „G“ für Giga. Abschließend wird die Einheit als „bps“ für 8 bit/s oder „bit“ für bit/s angegeben. Beispiele: „15.7 kbit“, „100 Mbit“ und „1 Gbit“.
- *SNAT/Masquerading*: SNAT und Masquerading dienen dazu, ganze Netzwerke hinter einer einzelnen IP-Adresse zu „verstecken“. Wird diese Option aktiviert, scheinen alle abgehenden Verbindungen von diesem System zu stammen und nicht vom wirklichen Absender.

  Diese Option muss aktiviert werden, wenn auf dem Internet-Link vom Provider nur eine einzelne IP-Adresse bereitgestellt wird und wenn Systeme aus dem lokalen Netz IP-Verbindungen aufbauen müssen.

  Die Unterscheidung zwischen SNAT und Masquerading erfolgt automatisch, abhängig davon, ob eine IP-Adresse für den Link angegeben wurde oder nicht.

  Hinweis: SNAT/Masquerading für Routen und VPN-Netze funktioniert nur, wenn auf dem unterliegenden Link kein Masquerading aktiviert ist.

- *Zu maskierende Netzwerke*: Wird Masquerading für *spezielle Netze* aktiviert, können in dieser Liste aus allen angelegten Netzwerken diejenigen ausgewählt werden, die maskiert werden müssen.

  Hinweis: Alle Subnetze eines ausgewählten Netzwerks werden ebenfalls maskiert.

  Wird ein Netzwerk aus der Liste ausgewählt, bedeutet das nicht automatisch, dass Daten aus diesem Netzwerk über diesen Link versendet werden können.
- *Erreichbare Netzwerke*: Hier können aus der Liste aller angelegten Netzwerken diejenigen ausgewählt werden, die über diesen Link erreichbar sind. Für jedes ausgewählte Netz wird ein Eintrag unter *Zuordnungen* angelegt.

  Bei VPN-Verbindungen muss das lokale Netz der Gegenstelle innerhalb einem der hier angegebenen Netze liegen.

Tab Policy-Routing

- *Traffic-Policies*: Hier werden die Policies ausgewählt, die dafür sorgen, dass die entsprechenden Netzwerkpakete oder Dienste bevorzugt über diesen Link geleitet werden. Hier können Policies ausgewählt werden, die unternehmenskritischen Datenverkehr kennzeichnen. Werden hier Policies gewählt, die einen lokalen Service, wie Web-Proxy kennzeichnen, wird als Folge der Datenverkehr dieses Dienstes nur über diesen Link abgewickelt. Wenn ein zusätzlicher Link in das Zielnetzwerk als Fall-Back-Verbindung definiert ist, wird der Datenverkehr bei Link-Ausfall über diese Fall-Back-Verbindung geleitet.
- *Nur diese Traffic-Policies zulassen*: Mit dieser Option werden ausschließlich die Netzwerkpakete über den Link geroutet, die den Traffic-Policies entsprechen. Default-Routen, die unter dem Menüpunkt *Zuordnungen* gesetzt sind, werden nicht mehr be-

rücksichtigt. Wenn nicht klar ist, was diese Option bedeutet, sollte sie leergelassen werden.

Felder in diesem Dialog für Typ *Analoges Modem*

(Diese Option befindet sich im Zusatzmodul *Collax Gatekeeper*)

- *Bezeichnung*: Hier muss eine eindeutige Bezeichnung für den Link angegeben werden. Unter diesem Namen steht der Link in verschiedenen anderen Dialogen zur Verfügung.
- *Kommentar*: Hier kann ein Kommentartext zu diesem Link angegeben werden.
- *Typ*: Hier wird der genaue Typ des Links angegeben. Abhängig davon werden weitere Felder in diesem Dialog sichtbar bzw. unsichtbar.
- *Verbindungsaufbau*: Bei Verbindungen, für die eine Einwahl stattfindet oder die eine Einwahl annehmen können, wird in diesem Feld ausgewählt, wie genau die Einwahl erfolgen soll:

  Immer bedeutet, dass der Link beim Aktivieren der Konfiguration bzw. beim (Neu-)Start des Systems sofort versuchen wird, sich auf der Gegenstelle einzuwählen. Die Verbindung besteht also quasi permanent.

  Bei Bedarf wartet mit dem Einwahlvorgang, bis wirklich Pakete vom lokalen System oder aus dem lokalen Netz zur Gegenseite übertragen werden sollen.

  Auf Einwahl warten baut selbst keine Verbindung auf, sondern wartet darauf, dass eine Gegenstelle die Verbindung aufbaut. Dies kann beispielsweise die Einwahl eines Außendienstmitarbeiters über ISDN oder über VPN sein.
- *Neustart erzwingen*: Diese Option ermöglicht einen gezielten Neustart der Verbindung, um u. U. die Erreichbarkeit des Servers zu erhöhen.

- *Uhrzeit*: Der Zeitpunkt, zu dem die entsprechende Verbindung neu gestartet wird.
- *Inaktive Verbindung abbauen nach*: Werden Verbindungen *bei Bedarf* aufgebaut, sollen sie normalerweise möglichst schnell wieder abgebaut werden. Dazu wird geprüft, ob innerhalb einer einstellbaren Zeitspanne kein Datenverkehr mehr auf der Leitung erfolgt.

  In diesem Feld wird die Zeitspanne in Sekunden angegeben. Es können minimal 59 Sekunden eingestellt werden, in der Praxis werden meist Werte ab drei Minuten (180 Sekunden) verwendet.
- *Link-Aktivitätsfilter*: Bei der Erkennung auf Inaktivität einer Verbindung kann es vorkommen, dass von außen einkommende Daten für Verkehr auf der Leitung sorgen, obwohl diese Datenpakete in der Firewall geblockt werden. Dies ist sehr häufig bei Internetverbindungen der Fall, wenn der vorherige Nutzer der zugewiesenen IP-Nummer mit vielen Gegenstellen Datenverkehr hatte (meist Filesharing).

  Durch das Aktivieren dieser Option werden einkommende Pakete von der Gegenstelle nicht als Datenverkehr „gezählt“. Dies ist im Normalfall unkritisch, da bei Verbindungen Pakete in beide Richtungen ausgetauscht werden (mit Ausnahme einiger Medien-Streaming-Protokolle).
- *DNS-Server an Gegenstelle übermitteln*: Mit dem Aktivieren dieser Option wird der Gegenstelle beim Verbindungsaufbau ein DNS-Server zugewiesen.

  Diese Option wird nur sichtbar, wenn auf dem Link *Auf Einwahl warten* aktiviert wird.
- *1. DNS-Server: lokales DNS benutzen*: Durch das Aktivieren dieser Option wird der Collax Security Gateway der Gegenstelle als erster DNS-Server zugewiesen.
- *1. DNS-Server*: Alternativ kann hier die IP-Adresse eines anderen

Nameservers angegeben werden, der als erster DNS-Server zugewiesen wird.

- *2. DNS-Server*: Hier wird die IP-Adresse des zweiten DNS-Servers eingetragen.
- *ISP-Modus*: Durch Aktivieren dieser Option wird der Link im *ISP-Modus* betrieben. Dabei wird der Gegenstelle eine IP-Adresse zugewiesen, und es werden keine Netze zur Gegenseite geroutet. Dies ist der gebräuchlichste Modus.

  Wird der ISP-Modus deaktiviert, können aus den angelegten Netzwerken diejenigen ausgewählt werden, die über die Gegenseite erreichbar sind.
- *IP-Adresse des Systems*: Hier wird die lokale IP-Adresse für den Link angegeben. Bleibt das Feld leer, versucht das System, eine dynamische IP-Adresse per PPP oder DHCP zu beziehen. Sollen mehrere IP-Adressen auf einen Netzwerkanschluss zugewiesen werden (IP-Alias), muss für jede IP-Adresse ein eigener Link angelegt werden. Dabei wird jedes Mal die gleiche Schnittstelle angegeben.

  Ist der Link vom Typ *auf Einwahl warten* und bleibt das Feld leer, wird eine zufällig ausgewählte IP-Adresse als lokale IP-Adresse verwendet. Andernfalls wird die eingetragene IP-Adresse als lokale IP-Adresse genutzt.
- *IP-Adresse der Gegenstelle*: Hier wird die IP-Adresse der Gegenstelle angegeben. Bleibt das Feld leer, versucht das System, die Adresse der Gegenstelle automatisch zu bestimmen.
- *Benutzername*: Hier wird das Login angegeben, mit dem sich das System bei der Einwahl an der Gegenstelle authentifizieren soll.
- *Passwort*: Hier wird das zugehörige Passwort angegeben.
- *Zusätzliche Hayes-Befehle*: Bei einem Link vom Typ *Modem* können hier zusätzliche Hayes-Kommandos eingegeben werden, die bei der Initialisierung an das Modem geschickt werden. Oft

müssen spezielle Optionen gesetzt werden, um ein Modem an einer Telefonanlage zu betreiben.

- *Rufnummer der Gegenstelle*: Hier wird die Telefonnummer der Gegenstelle angegeben. Eine Rufnummer im Ortsnetz sollte ohne Vorwahl eingegeben werden. Die Vorwahl wird automatisch übernommen, wenn unter *Konfiguration – Hardware* die entsprechende Option aktiviert ist.
- *MTU*: Hier kann die maximale Paketgröße auf diesem Link eingestellt werden.

  Große Werte für die MTU verbessern den Durchsatz, da weniger Verwaltungsdaten übertragen werden. Kleine Werte für die MTU hingegen verbessern die Antwortzeiten für interaktive Anwendungen und Echtzeitdatenübertragung (etwa VoIP).

  Wird hier kein Wert eingetragen, wird abhängig von der Art des Links ein geeigneter Wert gewählt. Für Ethernet-Verbindungen wird typischerweise eine MTU von 1500 Byte verwendet.
- *Bandbreitenmanagement*: Mit dieser Option wird das Bandbreitenmanagement für den Link aktiviert. Für indirekte Links, die auf einen anderen Link aufsetzen (Typ Route, Tunnel, VPN usw.) muss auf dem untergeordneten Link bereits das Bandbreitenmanagement aktiviert sein.
- *Bandbreite*: Hier wird die Bandbreite des Links angegeben. Für die Bandbreite von indirekten Links (Typ Route, Tunnel, VPN usw.) ist die Bandbreite des benutzten Links entscheidend.

  Wenn sich mehrere Links eine Hardwareschnittstelle teilen (z. B. LocalNetLink1 und LocalNetLink2 jeweils über eth0), darf die Summe der Bandbreiten der Links die Bandbreite der Hardwareschnittstelle selbst nicht überschreiten.

  In diesem Feld wird als Eingabe eine Dezimalzahl, optional mit Dezimalpunkt, optional gefolgt von Leerzeichen und abschließend einer Einheit erwartet. Folgende Einheiten sind möglich:

„k“ für Kilo, „M“ für Mega und „G“ für Giga. Abschließend wird die Einheit als „bps“ für 8 bit/s oder „bit“ für bit/s angegeben. Beispiele: „15.7 kbit“, „100 Mbit“ und „1 Gbit“.

- *Schnittstelle*: Wird für den Link eine Schnittstelle benötigt, kann diese hier eingestellt werden.
- *SNAT/Masquerading*: SNAT und Masquerading dienen dazu, ganze Netzwerke hinter einer einzelnen IP-Adresse zu „verstecken“. Wird diese Option aktiviert, scheinen alle abgehenden Verbindungen von diesem System zu stammen und nicht vom wirklichen Absender.

  Diese Option muss aktiviert werden, wenn auf dem Internet-Link vom Provider nur eine einzelne IP-Adresse bereitgestellt wird und wenn Systeme aus dem lokalen Netz IP-Verbindungen aufbauen müssen.

  Die Unterscheidung zwischen SNAT und Masquerading erfolgt automatisch, abhängig davon, ob eine IP-Adresse für den Link angegeben wurde oder nicht.

  Hinweis: SNAT/Masquerading für Routen und VPN-Netze funktioniert nur, wenn auf dem unterliegenden Link kein Masquerading aktiviert ist.
- *Zu maskierende Netzwerke*: Wird Masquerading für *spezielle Netze* aktiviert, können in dieser Liste aus allen angelegten Netzwerken diejenigen ausgewählt werden, die maskiert werden müssen.

  Hinweis: Alle Subnetze eines ausgewählten Netzwerks werden ebenfalls maskiert.

  Wird ein Netzwerk aus der Liste ausgewählt, bedeutet das nicht automatisch, dass Daten aus diesem Netzwerk über diesen Link versendet werden können.
- *Erreichbare Netzwerke*: Hier können aus der Liste aller angelegten Netzwerken diejenigen ausgewählt werden, die über diesen Link erreichbar sind. Für jedes ausgewählte Netz wird ein Eintrag unter *Zuordnungen* angelegt.

Bei VPN-Verbindungen muss das lokale Netz der Gegenstelle innerhalb einem der hier angegebenen Netze liegen.

Tab Policy-Routing

- *Traffic-Policies*: Hier werden die Policies ausgewählt, die dafür sorgen, dass die entsprechenden Netzwerkpakete oder Dienste bevorzugt über diesen Link geleitet werden. Hier können Policies ausgewählt werden, die unternehmenskritischen Datenverkehr kennzeichnen. Werden hier Policies gewählt, die einen lokalen Service, wie Web-Proxy kennzeichnen, wird als Folge der Datenverkehr dieses Dienstes nur über diesen Link abgewickelt. Wenn ein zusätzlicher Link in das Zielnetzwerk als Fall-Back-Verbindung definiert ist, wird der Datenverkehr bei Link-Ausfall über diese Fall-Back-Verbindung geleitet.
- *Nur diese Traffic-Policies zulassen*: Mit dieser Option werden ausschließlich die Netzwerkpakete über den Link geroutet, die den Traffic-Policies entsprechen. Default-Routen, die unter dem Menüpunkt *Zuordnungen* gesetzt sind, werden nicht mehr berücksichtigt. Wenn nicht klar ist, was diese Option bedeutet, sollte sie leergelassen werden.

Felder in diesem Dialog für Typ *ISDN synchron*

(Diese Option befindet sich im Zusatzmodul *Collax Gatekeeper*)

- *Bezeichnung*: Hier muss eine eindeutige Bezeichnung für den Link angegeben werden. Unter diesem Namen steht der Link in verschiedenen anderen Dialogen zur Verfügung.
- *Kommentar*: Hier kann ein Kommentartext zu diesem Link angegeben werden.
- *Typ*: Hier wird der genaue Typ des Links angegeben. Abhängig

davon werden weitere Felder in diesem Dialog sichtbar bzw. unsichtbar.

- *Verbindungsaufbau*: Bei Verbindungen, für die eine Einwahl stattfindet oder die eine Einwahl annehmen können, wird in diesem Feld ausgewählt, wie genau die Einwahl erfolgen soll:

  Immer bedeutet, dass der Link beim Aktivieren der Konfiguration bzw. beim (Neu-)Start des Systems sofort versuchen wird, sich auf der Gegenstelle einzuwählen. Die Verbindung besteht also quasi permanent.

  Bei Bedarf wartet mit dem Einwahlvorgang, bis wirklich Pakete vom lokalen System oder aus dem lokalen Netz zur Gegenseite übertragen werden sollen.

  Auf Einwahl warten baut selbst keine Verbindung auf, sondern wartet darauf, dass eine Gegenstelle die Verbindung aufbaut. Dies kann beispielsweise die Einwahl eines Außendienstmitarbeiters über ISDN oder über VPN sein.
- *Neustart erzwingen*: Diese Option ermöglicht einen gezielten Neustart der Verbindung, um u. U. die Erreichbarkeit des Servers zu erhöhen.
- *Uhrzeit*: Der Zeitpunkt, zu dem die entsprechende Verbindung neu gestartet wird.
- *Inaktive Verbindung abbauen nach*: Werden Verbindungen *bei Bedarf* aufgebaut, sollen sie normalerweise möglichst schnell wieder abgebaut werden. Dazu wird geprüft, ob innerhalb einer einstellbaren Zeitspanne kein Datenverkehr mehr auf der Leitung erfolgt.

  In diesem Feld wird die Zeitspanne in Sekunden angegeben. Es können minimal 59 Sekunden eingestellt werden, in der Praxis werden meist Werte ab drei Minuten (180 Sekunden) verwendet.
- *Link-Aktivitätsfilter*: Bei der Erkennung auf Inaktivität einer Verbindung kann es vorkommen, dass von außen einkommende

Daten für Verkehr auf der Leitung sorgen, obwohl diese Datenpakete in der Firewall geblockt werden. Dies ist sehr häufig bei Internetverbindungen der Fall, wenn der vorherige Nutzer der zugewiesenen IP-Nummer mit vielen Gegenstellen Datenverkehr hatte (meist Filesharing).

Durch das Aktivieren dieser Option werden einkommende Pakete von der Gegenstelle nicht als Datenverkehr „gezählt". Dies ist im Normalfall unkritisch, da bei Verbindungen Pakete in beide Richtungen ausgetauscht werden (mit Ausnahme einiger Medien-Streaming-Protokolle).

- *DNS-Server an Gegenstelle übermitteln*: Mit dem Aktivieren dieser Option wird der Gegenstelle beim Verbindungsaufbau ein DNS-Server zugewiesen.

  Diese Option wird nur sichtbar, wenn auf dem Link *Auf Einwahl warten* aktiviert wird.
- *1. DNS-Server: lokales DNS benutzen*: Durch das Aktivieren dieser Option wird der Collax Security Gateway der Gegenstelle als erster DNS-Server zugewiesen.
- *1. DNS-Server*: Alternativ kann hier die IP-Adresse eines anderen Nameservers angegeben werden, der als erster DNS-Server zugewiesen wird.
- *2. DNS-Server*: Hier wird die IP-Adresse des zweiten DNS-Servers eingetragen.
- *ISP-Modus*: Durch Aktivieren dieser Option wird der Link im *ISP-Modus* betrieben. Dabei wird der Gegenstelle eine IP-Adresse zugewiesen, und es werden keine Netze zur Gegenseite geroutet. Dies ist der gebräuchlichste Modus.

  Wird der ISP-Modus deaktiviert, können aus den angelegten Netzwerken diejenigen ausgewählt werden, die über die Gegenseite erreichbar sind.
- *Kanäle*: Bei ISDN-Verbindungen kann hier die Anzahl der Kanäle

angegeben werden, die per Kanalbündelung für die Verbindung genutzt werden sollen.

Die Kanalbündelung muss von der Gegenstelle unterstützt werden. Bei manchen Providern (z. B. T-Online) können maximal zwei Kanäle zusammengefasst werden, andere Provider unterstützen mehrere Kanäle.

Die zusätzlichen Kanäle werden bei Bedarf hinzugenommen und wieder freigegeben, wenn die zusätzliche Bandbreite nicht mehr benötigt wird.

Die Kanalbündelung kann auch für Links verwendet werden, die eine Einwahl annehmen. In diesem Fall ist die Gegenstelle für den Auf- und Abbau der zusätzlichen Kanäle zuständig (und für die anfallenden Verbindungsgebühren).

- *IP-Adresse des Systems*: Hier wird die lokale IP-Adresse für den Link angegeben. Bleibt das Feld leer, versucht das System, eine dynamische IP-Adresse per PPP oder DHCP zu beziehen. Sollen mehrere IP-Adressen auf einen Netzwerkanschluss zugewiesen werden (IP-Alias), muss für jede IP-Adresse ein eigener Link angelegt werden. Dabei wird jedes Mal die gleiche Schnittstelle angegeben.

  Ist der Link vom Typ *auf Einwahl warten* und bleibt das Feld leer, wird eine zufällig ausgewählte IP-Adresse als lokale IP-Adresse verwendet. Andernfalls wird die eingetragene IP-Adresse als lokale IP-Adresse genutzt.
- *IP-Adresse der Gegenstelle*: Hier wird die IP-Adresse der Gegenstelle angegeben. Bleibt das Feld leer, versucht das System, die Adresse der Gegenstelle automatisch zu bestimmen.
- *IP-Adressen für Zuweisung an Gegenstelle*: In diesem Feld werden, durch Leerzeichen getrennt, die IP-Adressen angegeben, die bei einer Einwahl an die Gegenstelle zugewiesen werden. Dabei sollte pro unterstütztem Kanal eine IP-Adresse bereit gestellt werden.

Wird das Feld leer gelassen, wird der Gegenstelle eine zufällig ausgewählte IP-Adresse übermittelt. Dann kann sich jedoch zu einem Zeitpunkt immer nur ein System einwählen.

- *Benutzername*: Hier wird das Login angegeben, mit dem sich das System bei der Einwahl an der Gegenstelle authentifizieren soll.
- *Passwort*: Hier wird das zugehörige Passwort angegeben.
- *Rufnummer der Gegenstelle*: Hier wird die Telefonnummer der Gegenstelle angegeben. Eine Rufnummer im Ortsnetz sollte ohne Vorwahl eingegeben werden. Die Vorwahl wird automatisch übernommen, wenn unter *Konfiguration – Hardware* die entsprechende Option aktiviert ist.
- *MSN*: Wenn der Link ein ISDN-Interface benutzt, muss aus dieser Liste eine MSN ausgewählt werden. Die gewählte MSN wird als abgehende Rufnummer verwendet.
- *Secure MSN*: Wird auf dem Link eine Einwahl über ISDN angenommen, kann über Einträge in diesem Feld die Annahme von Verbindungen auf bestimmte Rufnummern beschränkt werden. In dem Feld können durch Leerzeichen getrennt auch mehrere MSNs eingegeben werden. Nur bei Anrufen von diesen MSNs aus wird eine Verbindung angenommen. Bleibt das Feld leer, werden alle Anrufe angenommen.

  Um diese Funktion nutzen zu können, muss das anrufende System seine Rufnummer übermitteln. Um die exakt übermittelte Rufnummer zu ermitteln, kann in den Logdateien nach Einträgen gemäß folgendem Muster gesucht werden:

  ```
  kernel: ipppX: call from 8793787 - > 12345 ignored
  ```

  IpppX ist dabei das Interface, auf dem der Anruf einging (mit X der entsprechenden Nummer der Schnittstelle). Die Rufnummer (MSN) des Anrufers ist in diesem Beispiel 8793787, die angerufene Nummer die 12345. In diesem Fall wurde der Anruf nicht angenommen (*ignored*), eine angenommene Verbindung wird als *accepted* angezeigt.

- *Callback aktivieren*: *Callback* ist ein spezielles Verfahren, welches bei Fernwartung bzw. Remotezugriff allgemein eine höhere Sicherheit bietet. Bei Callback signalisiert das anrufende System nur seine Rufnummer, eine Verbindung wird nicht aufgebaut. Stattdessen baut nun das angerufene System seinerseits eine Verbindung zum eigentlichen Anrufer auf.

  Bei abgehenden Verbindungen wird die Gegenstelle dazu aufgefordert, zurückzurufen. Bei ankommenden Verbindungen wird hingegen die Gegenstelle zurückgerufen.
- *Callbacknummer*: Hier muss die Rufnummer hinterlegt werden, die zurückgerufen werden soll.
- *MTU*: Hier kann die maximale Paketgröße auf diesem Link eingestellt werden.

  Große Werte für die MTU verbessern den Durchsatz, da weniger Verwaltungsdaten übertragen werden. Kleine Werte für die MTU hingegen verbessern die Antwortzeiten für interaktive Anwendungen und Echtzeitdatenübertragung (etwa VoIP).

  Wird hier kein Wert eingetragen, wird abhängig von der Art des Links ein geeigneter Wert gewählt. Für Ethernet-Verbindungen wird typischerweise eine MTU von 1500 Byte verwendet.
- *Bandbreitenmanagement*: Mit dieser Option wird das Bandbreitenmanagement für den Link aktiviert. Für indirekte Links, die auf einen anderen Link aufsetzen (Typ Route, Tunnel, VPN usw.) muss auf dem untergeordneten Link bereits das Bandbreitenmanagement aktiviert sein.
- *Bandbreite*: Hier wird die Bandbreite des Links angegeben. Für die Bandbreite von indirekten Links (Typ Route, Tunnel, VPN usw.) ist die Bandbreite des benutzten Links entscheidend.

  Wenn sich mehrere Links eine Hardwareschnittstelle teilen (z. B. LocalNetLink1 und LocalNetLink2 jeweils über eth0), darf die Summe der Bandbreiten der Links die Bandbreite der Hardwareschnittstelle selbst nicht überschreiten.

In diesem Feld wird als Eingabe eine Dezimalzahl, optional mit Dezimalpunkt, optional gefolgt von Leerzeichen und abschließend einer Einheit erwartet. Folgende Einheiten sind möglich: „k“ für Kilo, „M“ für Mega und „G“ für Giga. Abschließend wird die Einheit als „bps“ für 8 bit/s oder „bit“ für bit/s angegeben. Beispiele: „15.7 kbit“, „100 Mbit“ und „1 Gbit“.

- *SNAT/Masquerading*: SNAT und Masquerading dienen dazu, ganze Netzwerke hinter einer einzelnen IP-Adresse zu „verstecken“. Wird diese Option aktiviert, scheinen alle abgehenden Verbindungen von diesem System zu stammen und nicht vom wirklichen Absender.

  Diese Option muss aktiviert werden, wenn auf dem Internet-Link vom Provider nur eine einzelne IP-Adresse bereitgestellt wird und wenn Systeme aus dem lokalen Netz IP-Verbindungen aufbauen müssen.

  Die Unterscheidung zwischen SNAT und Masquerading erfolgt automatisch, abhängig davon, ob eine IP-Adresse für den Link angegeben wurde oder nicht.

  Hinweis: SNAT/Masquerading für Routen und VPN-Netze funktioniert nur, wenn auf dem unterliegenden Link kein Masquerading aktiviert ist.
- *Zu maskierende Netzwerke*: Wird Masquerading für *spezielle Netze* aktiviert, können in dieser Liste aus allen angelegten Netzwerken diejenigen ausgewählt werden, die maskiert werden müssen.

  Hinweis: Alle Subnetze eines ausgewählten Netzwerks werden ebenfalls maskiert.

  Wird ein Netzwerk aus der Liste ausgewählt, bedeutet das nicht automatisch, dass Daten aus diesem Netzwerk über diesen Link versendet werden können.
- *Erreichbare Netzwerke*: Hier können aus der Liste aller angelegten Netzwerken diejenigen ausgewählt werden, die über diesen Link

erreichbar sind. Für jedes ausgewählte Netz wird ein Eintrag unter *Zuordnungen* angelegt.

Bei VPN-Verbindungen muss das lokale Netz der Gegenstelle innerhalb einem der hier angegebenen Netze liegen.

Tab Policy-Routing

- *Traffic-Policies*: Hier werden die Policies ausgewählt, die dafür sorgen, dass die entsprechenden Netzwerkpakete oder Dienste bevorzugt über diesen Link geleitet werden. Hier können Policies ausgewählt werden, die unternehmenskritischen Datenverkehr kennzeichnen. Werden hier Policies gewählt, die einen lokalen Service, wie Web-Proxy kennzeichnen, wird als Folge der Datenverkehr dieses Dienstes nur über diesen Link abgewickelt. Wenn ein zusätzlicher Link in das Zielnetzwerk als Fall-Back-Verbindung definiert ist, wird der Datenverkehr bei Link-Ausfall über diese Fall-Back-Verbindung geleitet.
- *Nur diese Traffic-Policies zulassen*: Mit dieser Option werden ausschließlich die Netzwerkpakete über den Link geroutet, die den Traffic-Policies entsprechen. Default-Routen, die unter dem Menüpunkt *Zuordnungen* gesetzt sind, werden nicht mehr berücksichtigt. Wenn nicht klar ist, was diese Option bedeutet, sollte sie leergelassen werden.

Felder in diesem Dialog für Typ *DSL mit PPPoE*

(Diese Option befindet sich im Zusatzmodul *Collax Gatekeeper*)

- *Bezeichnung*: Hier muss eine eindeutige Bezeichnung für den Link angegeben werden. Unter diesem Namen steht der Link in verschiedenen anderen Dialogen zur Verfügung.
- *Kommentar*: Hier kann ein Kommentartext zu diesem Link angegeben werden.

- *Typ*: Hier wird der genaue Typ des Links angegeben. Abhängig davon werden weitere Felder in diesem Dialog sichtbar bzw. unsichtbar.
- *Verbindungsaufbau*: Bei Verbindungen, für die eine Einwahl stattfindet oder die eine Einwahl annehmen können, wird in diesem Feld ausgewählt, wie genau die Einwahl erfolgen soll:

  Immer bedeutet, dass der Link beim Aktivieren der Konfiguration bzw. beim (Neu-)Start des Systems sofort versuchen wird, sich auf der Gegenstelle einzuwählen. Die Verbindung besteht also quasi permanent.

  Bei Bedarf wartet mit dem Einwahlvorgang, bis wirklich Pakete vom lokalen System oder aus dem lokalen Netz zur Gegenseite übertragen werden sollen.
- *Neustart erzwingen*: Diese Option ermöglicht einen gezielten Neustart der Verbindung, um u. U. die Erreichbarkeit des Servers zu erhöhen. DSL-Verbindungen werden teilweise von Providerseite nach einem bestimmten Zeitintervall getrennt. Diese Option kann benutzt werden, um den Zeitpunkt der Trennung zu verschieben.
- *Uhrzeit*: Der Zeitpunkt, zu dem die entsprechende Verbindung neu gestartet wird.
- *Inaktive Verbindung abbauen nach*: Werden Verbindungen *bei Bedarf* aufgebaut, sollen sie normalerweise möglichst schnell wieder abgebaut werden. Dazu wird geprüft, ob innerhalb einer einstellbaren Zeitspanne kein Datenverkehr mehr auf der Leitung erfolgt.

  In diesem Feld wird die Zeitspanne in Sekunden angegeben. Es können minimal 59 Sekunden eingestellt werden, in der Praxis werden meist Werte ab drei Minuten (180 Sekunden) verwendet.
- *Link-Aktivitätsfilter*: Bei der Erkennung auf Inaktivität einer Verbindung kann es vorkommen, dass von außen einkommende Daten für Verkehr auf der Leitung sorgen, obwohl diese Daten-

pakete in der Firewall geblockt werden. Dies ist sehr häufig bei Internetverbindungen der Fall, wenn der vorherige Nutzer der zugewiesenen IP-Nummer mit vielen Gegenstellen Datenverkehr hatte (meist Filesharing).

Durch das Aktivieren dieser Option werden einkommende Pakete von der Gegenstelle nicht als Datenverkehr „gezählt". Dies ist im Normalfall unkritisch, da bei Verbindungen Pakete in beide Richtungen ausgetauscht werden (mit Ausnahme einiger Medien-Streaming-Protokolle).

- *IP-Adresse des Systems*: Hier wird die lokale IP-Adresse für den Link angegeben. Bleibt das Feld leer, versucht das System, eine dynamische IP-Adresse per PPP oder DHCP zu beziehen. Sollen mehrere IP-Adressen auf einen Netzwerkanschluss zugewiesen werden (IP-Alias), muss für jede IP-Adresse ein eigener Link angelegt werden. Dabei wird jedes Mal die gleiche Schnittstelle angegeben.

  Ist der Link vom Typ *auf Einwahl warten* und bleibt das Feld leer, wird eine zufällig ausgewählte IP-Adresse als lokale IP-Adresse verwendet. Andernfalls wird die eingetragene IP-Adresse als lokale IP-Adresse genutzt.
- *IP-Adresse der Gegenstelle*: Hier wird die IP-Adresse der Gegenstelle angegeben. Bleibt das Feld leer, versucht das System, die Adresse der Gegenstelle automatisch zu bestimmen.
- *Benutzername*: Hier wird das Login angegeben, mit dem sich das System bei der Einwahl an der Gegenstelle authentifizieren soll.
- *Passwort*: Hier wird das zugehörige Passwort angegeben.
- *MTU*: Hier kann die maximale Paketgröße auf diesem Link eingestellt werden.

  Große Werte für die MTU verbessern den Durchsatz, da weniger Verwaltungsdaten übertragen werden. Kleine Werte für die MTU hingegen verbessern die Antwortzeiten für interaktive Anwendungen und Echtzeitdatenübertragung (etwa VoIP).

Wird hier kein Wert eingetragen, wird abhängig von der Art des Links ein geeigneter Wert gewählt. Für Ethernet-Verbindungen wird typischerweise eine MTU von 1500 Byte verwendet.

- *Bandbreitenmanagement*: Mit dieser Option wird das Bandbreitenmanagement für den Link aktiviert. Für indirekte Links, die auf einen anderen Link aufsetzen (Typ Route, Tunnel, VPN usw.) muss auf dem untergeordneten Link bereits das Bandbreitenmanagement aktiviert sein.
- *Bandbreite*: Hier wird die Bandbreite des Links angegeben. Für die Bandbreite von indirekten Links (Typ Route, Tunnel, VPN usw.) ist die Bandbreite des benutzten Links entscheidend.

  Wenn sich mehrere Links eine Hardwareschnittstelle teilen (z. B. LocalNetLink1 und LocalNetLink2 jeweils über eth0), darf die Summe der Bandbreiten der Links die Bandbreite der Hardwareschnittstelle selbst nicht überschreiten.

  In diesem Feld wird als Eingabe eine Dezimalzahl, optional mit Dezimalpunkt, optional gefolgt von Leerzeichen und abschließend einer Einheit erwartet. Folgende Einheiten sind möglich: „k“ für Kilo, „M“ für Mega und „G“ für Giga. Abschließend wird die Einheit als „bps“ für 8 bit/s oder „bit“ für bit/s angegeben. Beispiele: „15.7 kbit“, „100 Mbit“ und „1 Gbit“.
- *Schnittstelle*: Wird für den Link eine Schnittstelle benötigt, kann diese hier eingestellt werden.
- *SNAT/Masquerading*: SNAT und Masquerading dienen dazu, ganze Netzwerke hinter einer einzelnen IP-Adresse zu „verstecken“. Wird diese Option aktiviert, scheinen alle abgehenden Verbindungen von diesem System zu stammen und nicht vom wirklichen Absender.

  Diese Option muss aktiviert werden, wenn auf dem Internet-Link vom Provider nur eine einzelne IP-Adresse bereitgestellt wird und wenn Systeme aus dem lokalen Netz IP-Verbindungen aufbauen müssen.

Die Unterscheidung zwischen SNAT und Masquerading erfolgt automatisch, abhängig davon, ob eine IP-Adresse für den Link angegeben wurde oder nicht.

Hinweis: SNAT/Masquerading für Routen und VPN-Netze funktioniert nur, wenn auf dem unterliegenden Link kein Masquerading aktiviert ist.

- *Zu maskierende Netzwerke*: Wird Masquerading für *spezielle Netze* aktiviert, können in dieser Liste aus allen angelegten Netzwerken diejenigen ausgewählt werden, die maskiert werden müssen.

  Hinweis: Alle Subnetze eines ausgewählten Netzwerks werden ebenfalls maskiert.

  Wird ein Netzwerk aus der Liste ausgewählt, bedeutet das nicht automatisch, dass Daten aus diesem Netzwerk über diesen Link versendet werden können.
- *Erreichbare Netzwerke*: Hier können aus der Liste aller angelegten Netzwerken diejenigen ausgewählt werden, die über diesen Link erreichbar sind. Für jedes ausgewählte Netz wird ein Eintrag unter *Zuordnungen* angelegt.

  Bei VPN-Verbindungen muss das lokale Netz der Gegenstelle innerhalb einem der hier angegebenen Netze liegen.

Tab Policy-Routing

- *Traffic-Policies*: Hier werden die Policies ausgewählt, die dafür sorgen, dass die entsprechenden Netzwerkpakete oder Dienste bevorzugt über diesen Link geleitet werden. Hier können Policies ausgewählt werden, die unternehmenskritischen Datenverkehr kennzeichnen. Werden hier Policies gewählt, die einen lokalen Service, wie Web-Proxy kennzeichnen, wird als Folge der Datenverkehr dieses Dienstes nur über diesen Link abgewickelt. Wenn ein zusätzlicher Link in das Zielnetzwerk als Fall-Back-Verbindung

definiert ist, wird der Datenverkehr bei Link-Ausfall über diese Fall-Back-Verbindung geleitet.

- *Nur diese Traffic-Policies zulassen*: Mit dieser Option werden ausschließlich die Netzwerkpakete über den Link geroutet, die den Traffic-Policies entsprechen. Default-Routen, die unter dem Menüpunkt *Zuordnungen* gesetzt sind, werden nicht mehr berücksichtigt. Wenn nicht klar ist, was diese Option bedeutet, sollte sie leergelassen werden.

Felder in diesem Dialog für Typ *DSL mit PPTP*

(Diese Option befindet sich im Zusatzmodul *Collax Gatekeeper*)

- *Bezeichnung*: Hier muss eine eindeutige Bezeichnung für den Link angegeben werden. Unter diesem Namen steht der Link in verschiedenen anderen Dialogen zur Verfügung.
- *Kommentar*: Hier kann ein Kommentartext zu diesem Link angegeben werden.
- *Typ*: Hier wird der genaue Typ des Links angegeben. Abhängig davon werden weitere Felder in diesem Dialog sichtbar bzw. unsichtbar.
- *Verbindungsaufbau*: Bei Verbindungen, für die eine Einwahl stattfindet oder die eine Einwahl annehmen können, wird in diesem Feld ausgewählt, wie genau die Einwahl erfolgen soll:

  Immer bedeutet, dass der Link beim Aktivieren der Konfiguration bzw. beim (Neu-)Start des Systems sofort versuchen wird, sich auf der Gegenstelle einzuwählen. Die Verbindung besteht also quasi permanent.

  Bei Bedarf wartet mit dem Einwahlvorgang, bis wirklich Pakete vom lokalen System oder aus dem lokalen Netz zur Gegenseite übertragen werden sollen.
- *Neustart erzwingen*: Diese Option ermöglicht einen gezielten Neu-

start der Verbindung, um u. U. die Erreichbarkeit des Servers zu erhöhen. DSL-Verbindungen werden teilweise von Providerseite nach einem bestimmten Zeitintervall getrennt. Diese Option kann benutzt werden, um den Zeitpunkt der Trennung zu verschieben.

- *Uhrzeit*: Der Zeitpunkt, zu dem die entsprechende Verbindung neu gestartet wird.
- *Inaktive Verbindung abbauen nach*: Werden Verbindungen *bei Bedarf* aufgebaut, sollen sie normalerweise möglichst schnell wieder abgebaut werden. Dazu wird geprüft, ob innerhalb einer einstellbaren Zeitspanne kein Datenverkehr mehr auf der Leitung erfolgt.

  In diesem Feld wird die Zeitspanne in Sekunden angegeben. Es können minimal 59 Sekunden eingestellt werden, in der Praxis werden meist Werte ab drei Minuten (180 Sekunden) verwendet.
- *Link-Aktivitätsfilter*: Bei der Erkennung auf Inaktivität einer Verbindung kann es vorkommen, dass von außen einkommende Daten für Verkehr auf der Leitung sorgen, obwohl diese Datenpakete in der Firewall geblockt werden. Dies ist sehr häufig bei Internetverbindungen der Fall, wenn der vorherige Nutzer der zugewiesenen IP-Nummer mit vielen Gegenstellen Datenverkehr hatte (meist Filesharing).

  Durch das Aktivieren dieser Option werden einkommende Pakete von der Gegenstelle nicht als Datenverkehr „gezählt“. Dies ist im Normalfall unkritisch, da bei Verbindungen Pakete in beide Richtungen ausgetauscht werden (mit Ausnahme einiger Medien-Streaming-Protokolle).
- *IP-Adresse des Systems*: Hier wird die lokale IP-Adresse für den Link angegeben. Bleibt das Feld leer, versucht das System, eine dynamische IP-Adresse per PPP oder DHCP zu beziehen. Sollen mehrere IP-Adressen auf einen Netzwerkanschluss zugewiesen werden (IP-Alias), muss für jede IP-Adresse ein eigener Link

angelegt werden. Dabei wird jedes Mal die gleiche Schnittstelle angegeben.

Ist der Link vom Typ *auf Einwahl warten* und bleibt das Feld leer, wird eine zufällig ausgewählte IP-Adresse als lokale IP-Adresse verwendet. Andernfalls wird die eingetragene IP-Adresse als lokale IP-Adresse genutzt.

- *IP-Adresse der Gegenstelle*: Hier wird die IP-Adresse der Gegenstelle angegeben. Bleibt das Feld leer, versucht das System, die Adresse der Gegenstelle automatisch zu bestimmen.
- *Benutzername*: Hier wird das Login angegeben, mit dem sich das System bei der Einwahl an der Gegenstelle authentifizieren soll.
- *Passwort*: Hier wird das zugehörige Passwort angegeben.
- *MTU*: Hier kann die maximale Paketgröße auf diesem Link eingestellt werden.

  Große Werte für die MTU verbessern den Durchsatz, da weniger Verwaltungsdaten übertragen werden. Kleine Werte für die MTU hingegen verbessern die Antwortzeiten für interaktive Anwendungen und Echtzeitdatenübertragung (etwa VoIP).

  Wird hier kein Wert eingetragen, wird abhängig von der Art des Links ein geeigneter Wert gewählt. Für Ethernet-Verbindungen wird typischerweise eine MTU von 1500 Byte verwendet.
- *Bandbreitenmanagement*: Mit dieser Option wird das Bandbreitenmanagement für den Link aktiviert. Für indirekte Links, die auf einen anderen Link aufsetzen (Typ Route, Tunnel, VPN usw.) muss auf dem untergeordneten Link bereits das Bandbreitenmanagement aktiviert sein.
- *Bandbreite*: Hier wird die Bandbreite des Links angegeben. Für die Bandbreite von indirekten Links (Typ Route, Tunnel, VPN usw.) ist die Bandbreite des benutzten Links entscheidend.

  Wenn sich mehrere Links eine Hardwareschnittstelle teilen (z. B. LocalNetLink1 und LocalNetLink2 jeweils über eth0), darf

die Summe der Bandbreiten der Links die Bandbreite der Hardwareschnittstelle selbst nicht überschreiten.

In diesem Feld wird als Eingabe eine Dezimalzahl, optional mit Dezimalpunkt, optional gefolgt von Leerzeichen und abschließend einer Einheit erwartet. Folgende Einheiten sind möglich: „k“ für Kilo, „M“ für Mega und „G“ für Giga. Abschließend wird die Einheit als „bps“ für 8 bit/s oder „bit“ für bit/s angegeben. Beispiele: „15.7 kbit“, „100 Mbit“ und „1 Gbit“.

- *Schnittstelle*: Wird für den Link eine Schnittstelle benötigt, kann diese hier eingestellt werden.
- *IP-Adresse des Modems*: Um mit einem DSL-Modem über das PPTP-Protokoll Daten austauschen zu können, wird ein IP-Transfernetz benötigt. In diesem Feld wird die IP-Adresse des Modems im Transfernetz angegeben. Bleibt das Feld leer, wird die Adresse „10.0.0.138“ benutzt. Dies ist die voreingestellte Adresse bei Alcatel-Modems.
- *IP-Adresse im Transfernetz*: Um mit einem DSL-Modem über das PPTP-Protokoll Daten austauschen zu können, wird ein IP-Transfernetz benötigt. In diesem Feld wird die IP-Adresse des Collax Security Gateways in diesem Netz angegeben. Bleibt das Feld leer, wird die Adresse „10.0.0.140“ benutzt.
- *SNAT/Masquerading*: SNAT und Masquerading dienen dazu, ganze Netzwerke hinter einer einzelnen IP-Adresse zu „verstecken“. Wird diese Option aktiviert, scheinen alle abgehenden Verbindungen von diesem System zu stammen und nicht vom wirklichen Absender.

  Diese Option muss aktiviert werden, wenn auf dem Internet-Link vom Provider nur eine einzelne IP-Adresse bereitgestellt wird und wenn Systeme aus dem lokalen Netz IP-Verbindungen aufbauen müssen.

  Die Unterscheidung zwischen SNAT und Masquerading erfolgt

automatisch, abhängig davon, ob eine IP-Adresse für den Link angegeben wurde oder nicht.

Hinweis: SNAT/Masquerading für Routen und VPN-Netze funktioniert nur, wenn auf dem unterliegenden Link kein Masquerading aktiviert ist.

- *Zu maskierende Netzwerke*: Wird Masquerading für *spezielle Netze* aktiviert, können in dieser Liste aus allen angelegten Netzwerken diejenigen ausgewählt werden, die maskiert werden müssen.

  Hinweis: Alle Subnetze eines ausgewählten Netzwerks werden ebenfalls maskiert.

  Wird ein Netzwerk aus der Liste ausgewählt, bedeutet das nicht automatisch, dass Daten aus diesem Netzwerk über diesen Link versendet werden können.
- *Erreichbare Netzwerke*: Hier können aus der Liste aller angelegten Netzwerken diejenigen ausgewählt werden, die über diesen Link erreichbar sind. Für jedes ausgewählte Netz wird ein Eintrag unter *Zuordnungen* angelegt.

  Bei VPN-Verbindungen muss das lokale Netz der Gegenstelle innerhalb einem der hier angegebenen Netze liegen.

Tab Policy-Routing

- *Traffic-Policies*: Hier werden die Policies ausgewählt, die dafür sorgen, dass die entsprechenden Netzwerkpakete oder Dienste bevorzugt über diesen Link geleitet werden. Hier können Policies ausgewählt werden, die unternehmenskritischen Datenverkehr kennzeichnen. Werden hier Policies gewählt, die einen lokalen Service, wie Web-Proxy kennzeichnen, wird als Folge der Datenverkehr dieses Dienstes nur über diesen Link abgewickelt. Wenn ein zusätzlicher Link in das Zielnetzwerk als Fall-Back-Verbindung definiert ist, wird der Datenverkehr bei Link-Ausfall über diese Fall-Back-Verbindung geleitet.

- *Nur diese Traffic-Policies zulassen*: Mit dieser Option werden ausschließlich die Netzwerkpakete über den Link geroutet, die den Traffic-Policies entsprechen. Default-Routen, die unter dem Menüpunkt *Zuordnungen* gesetzt sind, werden nicht mehr berücksichtigt. Wenn nicht klar ist, was diese Option bedeutet, sollte sie leergelassen werden.

Felder in diesem Dialog für Typ *VPN*

(Diese Option befindet sich im Zusatzmodul *Collax Gatekeeper*)

- *Bezeichnung*: Hier muss eine eindeutige Bezeichnung für den Link angegeben werden. Unter diesem Namen steht der Link in verschiedenen anderen Dialogen zur Verfügung.
- *Kommentar*: Hier kann ein Kommentartext zu diesem Link angegeben werden.
- *Typ*: Hier wird der genaue Typ des Links angegeben. Abhängig davon werden weitere Felder in diesem Dialog sichtbar bzw. unsichtbar.
- *Verbindungsaufbau*: Bei Verbindungen, für die eine Einwahl stattfindet oder die eine Einwahl annehmen können, wird in diesem Feld ausgewählt, wie genau die Einwahl erfolgen soll:

  Immer bedeutet, dass der Link beim Aktivieren der Konfiguration bzw. beim (Neu-)Start des Systems sofort versuchen wird, sich auf der Gegenstelle einzuwählen. Die Verbindung besteht also quasi permanent.

  Bei Bedarf wartet mit dem Einwahlvorgang, bis wirklich Pakete vom lokalen System oder aus dem lokalen Netz zur Gegenseite übertragen werden sollen.

  Auf Einwahl warten baut selbst keine Verbindung auf, sondern wartet darauf, dass eine Gegenstelle die Verbindung aufbaut. Dies kann beispielsweise die Einwahl eines Außendienstmitarbeiters über ISDN oder über VPN sein.

- *Neustart erzwingen*: Diese Option ermöglicht einen gezielten Neustart der Verbindung, um u. U. die Erreichbarkeit des Servers zu erhöhen.
- *Uhrzeit*: Der Zeitpunkt, zu dem die entsprechende Verbindung neu gestartet wird.
- *Host-zu-Netz-Verbindung*: Mit dieser Option verhält sich das System auf der Verbindung wie ein „Roadwarrior", es ist nur unter einer IP-Adresse sichtbar. Alle Netze auf anderen lokalen Links sind für die Gegenstelle auf diesem Link nicht sichtbar. Diese lokalen Netze können jedoch bei aktivierten Masquerading auf die Gegenseite zugreifen.

  Host-zu-Netz-Verbindungen sind sinnvoll, wenn das System außerhalb des lokalen Netzes steht (z. B. als Webserver bei einem Provider) und dennoch in das lokale Netz eingebunden werden soll. Die Einbindung eines solchen Systems birgt jedoch Sicherheitslücken und sollte vermieden werden.

  Da keine lokalen Netze ausgewählt werden, muss statt dessen eine IP-Adresse für das System gesetzt werden. Je nach Typ des Links kann diese leer bleiben, dann wird sie von der Gegenseite zugewiesen.
- *IP-Adresse des Systems*: Hier wird die lokale IP-Adresse für den Link angegeben. Bleibt das Feld leer, versucht das System, eine dynamische IP-Adresse per PPP oder DHCP zu beziehen. Sollen mehrere IP-Adressen auf einen Netzwerkanschluss zugewiesen werden (IP-Alias), muss für jede IP-Adresse ein eigener Link angelegt werden. Dabei wird jedes Mal die gleiche Schnittstelle angegeben.

  Ist der Link vom Typ *auf Einwahl warten* und bleibt das Feld leer, wird eine zufällig ausgewählte IP-Adresse als lokale IP-Adresse verwendet. Andernfalls wird die eingetragene IP-Adresse als lokale IP-Adresse genutzt.

- *Auf Link*: Werden VPN-Verbindungen eingerichtet, muss bei Links vom Typ *auf Einwahl warten* der Link ausgewählt werden, auf dem die IPsec-Verbindung angenommen wird. Technisch wird dabei ein IPsec-Device auf die Schnittstelle gebunden. Dabei handelt es sich meist um den Link ins Internet.
- *IPsec-Gateway*: Bei VPN-Verbindungen muss die Gegenstelle angegeben werden, zu der der VPN-Verbindungsaufbau erfolgt. Hier kann entweder eine IP-Adresse oder ein Hostname angegeben werden. Der Name wird erst beim Verbindungsaufbau aufgelöst, die Verwendung sogenannter DynDns-Namen ist daher möglich.

  Für die Annahme von Verbindungen kann das Feld leer bleiben, dann werden Verbindungen von einer beliebige IP-Adresse angenommen.
- *Eigener Schlüssel*: Aus dieser Liste kann bei VPN-Verbindungen der eigene Schlüssel ausgewählt werden. Hier sind X.509-Zertifikate und RSA-Schlüssel aufgeführt, zu denen ein privater Schlüssel auf dem System installiert ist. Wird ein Schlüssel ausgewählt, muss in einem Feld weiter unten der Schlüssel der Gegenseite ausgewählt werden. Dazu muss auf diesem System nur der Public Key installiert sein.

  Durch Auswahl der Option *PSK* („Pre Shared Key“) wird der VPN-Tunnel nur durch eine Passphrase aufgebaut. Es erscheint ein Eingabefeld für die Eingabe des Schlüssels.

  RSA-Schlüssel und X.509-Zertifikate werden unter *Benutzungsrichtlinien – Zertifikate* verwaltet.

  Hinweis: Wann immer möglich, sollten X.509-Zertifikate verwendet werden. Diese sind in der Handhabung erheblich einfacher als RSA-Schlüssel und sehr viel sicherer als die PSK-Authentifizierung.
- *Eigene ID*: Bei einer VPN-Verbindung wird jedem der beiden Endpunkte eine ID zugewiesen, eine Art Stationskennung. In

diesem Feld wird die eigene ID eingegeben. Das Feld kann leer bleiben, dann wird bei X.509-Verbindungen der DN des Zertifikats verwendet.

Bei Verbindungen mit RSA- oder PSK-Schlüsseln wird die eigene IP-Adresse verwendet. Wird eine Internetanbindung mit dynamischer Adresse verwendet, sollte hier ein anderer Wert angegeben werden.

Der angegebene Wert wird normalerweise als IP-Adresse oder Hostname betrachtet (und muss in diesem Fall über DNS auflösbar sein). Soll ein anderer Wert angegeben werden, muss als erstes Zeichen ein @-Zeichen eingegeben werden.

- *Passphrase für Verschlüsselung*: Hier muss die Passphrase für die PSK-Verbindung angegeben werden.
- *Schlüssel der Gegenstelle*: Für VPN-Verbindungen mit RSA- oder X.509-Schlüsseln kann hier der Schlüssel der Gegenstelle ausgewählt werden.

  In der Liste sind auch CA-Zertifikate aufgeführt. Wird ein solches Zertifikat ausgewählt, werden auf diesem Link alle Gegenstellen akzeptiert, die ein von dieser CA signiertes und gültiges Zertifikat benutzen. Dies ist für Konfigurationen mit mehreren „Roadwarriors“ nützlich.
- *ID der Gegenstelle*: Hier wird die ID für die Gegenstelle angegeben. Analog zur eigenen ID werden Eingaben als IP-Adresse oder Hostname betrachtet. Diese müssen über DNS auflösbar sein. Sollen andere Werte verwendet werden, muss ein @-Zeichen vorangestellt werden.

  Bleibt das Feld leer, wird die ID vom System selbständig ermittelt.

  Ist als Zertifikat der Gegenstelle ein normales X.509-Zertifikat ausgewählt, wird als ID der DN aus dem Zertifikat verwendet.

  Bei RSA- und PSK-Verbindungen werden als Voreinstellung für

die ID der Name oder die IP-Adresse verwendet, die als IPsec-Gateway angegeben sind.

- *Aggressive Mode*: Der Aggressive Mode kann bei IPsec-Verbindungen mit PSK verwendet werden. In diesem Modus wird die ID der Gegenstelle bereits beim Verbindungsaufbau übermittelt. Diese Option wird für Verbindungen zu bestimmten Gegenstellen benötigt (beispielsweise Cisco).
- *Komprimierung*: Über diese Option kann die Kompression der übertragenen Daten im Tunnel aktiviert werden.
- *Verschlüsselung für Schlüsselaustausch (IKE)*: In dieser Liste stehen verschiedene Algorithmen zur Auswahl, die für die Verschlüsselung beim Schlüsselaustausch verwendet werden können. Die Voreinstellung ist *3DES*, ein Verfahren, das von den meisten Gegenstellen unterstützt wird. Wenn möglich, sollte *AES* als Verfahren genutzt werden.
- *Hash-Algorithmus für Schlüsselaustausch (IKE)*: In dieser Liste stehen verschiedene Verfahren zur Prüfsummenbildung zur Auswahl. Mit dem gewählten Algorithmus wird die Echtheitsprüfung von Paketen während des Schlüsselaustausches durchgeführt. Voreingestellt ist das verbreitete Verfahren *MD5*. Wenn die Gegenstelle es unterstützt, kann *SHA-1* verwendet werden.
- *Verschlüsselung für Daten (ESP)*: Analog zur IKE-Verbindung wird hier der Verschlüsselungsalgorithmus für die eigentliche Datenübertragung eingestellt. Es gelten die gleichem Empfehlungen wie bei der IKE-Verbindung.
- *Hash-Algorithmus für Datenaustausch (ESP)*: Analog zur IKE-Verbindung wird hier der Prüfsummenalgorithmus für die eigentliche Datenübertragung eingestellt. Es gelten die gleichem Empfehlungen wie bei der IKE-Verbindung.
- *Keylife*: Nach Ablauf der eingestellten Zeit wird ein neuer Schlüssel für die reine Datenübertragung ausgehandelt.

- *Lifetime*: Nach Ablauf der eingestellten Zeit wird der Tunnel getrennt und die Verbindung mit der Gegenstelle neu ausgehandelt.
- *Perfect Forwarding Secrecy*: Wird diese Option aktiviert, wird bei jedem Verbindungsaufbau ein neuer Schlüsselsatz für die Übertragung ausgehandelt. Ein eventuell noch gültiger Schlüssel aus der vorhergehenden Verbindung wird verworfen.
- *MTU*: Hier kann die maximale Paketgröße auf diesem Link eingestellt werden.

  Große Werte für die MTU verbessern den Durchsatz, da weniger Verwaltungsdaten übertragen werden. Kleine Werte für die MTU hingegen verbessern die Antwortzeiten für interaktive Anwendungen und Echtzeitdatenübertragung (etwa VoIP).

  Wird hier kein Wert eingetragen, wird abhängig von der Art des Links ein geeigneter Wert gewählt. Für Ethernet-Verbindungen wird typischerweise eine MTU von 1500 Byte verwendet.
- *Bandbreitenmanagement*: Mit dieser Option wird das Bandbreitenmanagement für den Link aktiviert. Für indirekte Links, die auf einen anderen Link aufsetzen (Typ Route, Tunnel, VPN usw.) muss auf dem untergeordneten Link bereits das Bandbreitenmanagement aktiviert sein.
- *Bandbreite*: Hier wird die Bandbreite des Links angegeben. Für die Bandbreite von indirekten Links (Typ Route, Tunnel, VPN usw.) ist die Bandbreite des benutzten Links entscheidend.

  Wenn sich mehrere Links eine Hardwareschnittstelle teilen (z. B. LocalNetLink1 und LocalNetLink2 jeweils über eth0), darf die Summe der Bandbreiten der Links die Bandbreite der Hardwareschnittstelle selbst nicht überschreiten.

  In diesem Feld wird als Eingabe eine Dezimalzahl, optional mit Dezimalpunkt, optional gefolgt von Leerzeichen und abschließend einer Einheit erwartet. Folgende Einheiten sind möglich: „k“ für Kilo, „M“ für Mega und „G“ für Giga. Abschließend wird

die Einheit als „bps“ für 8 bit/s oder „bit“ für bit/s angegeben. Beispiele: „15.7 kbit“, „100 Mbit“ und „1 Gbit“.

- *SNAT/Masquerading*: SNAT und Masquerading dienen dazu, ganze Netzwerke hinter einer einzelnen IP-Adresse zu „verstecken“. Wird diese Option aktiviert, scheinen alle abgehenden Verbindungen von diesem System zu stammen und nicht vom wirklichen Absender.

  Diese Option muss aktiviert werden, wenn auf dem Internet-Link vom Provider nur eine einzelne IP-Adresse bereitgestellt wird und wenn Systeme aus dem lokalen Netz IP-Verbindungen aufbauen müssen.

  Die Unterscheidung zwischen SNAT und Masquerading erfolgt automatisch, abhängig davon, ob eine IP-Adresse für den Link angegeben wurde oder nicht.

  Hinweis: SNAT/Masquerading für Routen und VPN-Netze funktioniert nur, wenn auf dem unterliegenden Link kein Masquerading aktiviert ist.
- *Zu maskierende Netzwerke*: Wird Masquerading für *spezielle Netze* aktiviert, können in dieser Liste aus allen angelegten Netzwerken diejenigen ausgewählt werden, die maskiert werden müssen.

  Hinweis: Alle Subnetze eines ausgewählten Netzwerks werden ebenfalls maskiert.

  Wird ein Netzwerk aus der Liste ausgewählt, bedeutet das nicht automatisch, dass Daten aus diesem Netzwerk über diesen Link versendet werden können.
- *Erreichbare Netzwerke*: Hier können aus der Liste aller angelegten Netzwerken diejenigen ausgewählt werden, die über diesen Link erreichbar sind. Für jedes ausgewählte Netz wird ein Eintrag unter *Zuordnungen* angelegt.

  Bei VPN-Verbindungen muss das lokale Netz der Gegenstelle innerhalb einem der hier angegebenen Netze liegen.

- *Lokale Netzwerke*: Bei VPN-Verbindungen mit Netz-Netz-Kopplung müssen in dieser Liste die lokalen Netze angegeben werden, die für die Gegenstelle erreichbar sein sollen. Die Angabe für die lokalen Netze dient nur der Autorisierung der Verbindungen; es werden jedoch keine Firewall-Regeln angelegt.

  Die Netzwerke, die hier als *lokale Netze* ausgewählt werden, müssen bei der Gegenstelle als *erreichbare Netze* eintragen werden. Für jedes Paar aus lokalem und erreichbarem Netz wird ein eigener Tunnel eingerichtet. Dies wird im *IPsec-Status* sichtbar.
- *Absenderadresse*: Bei VPN-Verbindungen kann hier die IP-Adresse des Systems gewählt werden. Diese wird als Absenderadresse verwendet, wenn die Daten vom System selbst stammen. Bei anderer VPN-Software heißt dieses Feature manchmal „virtuelle IP-Adresse“.

  Wird hier nichts ausgewählt, wird die IP-Adresse des Links verwendet, über den die verschlüsselten Daten versendet werden. Bei einer Internetverbindung ist dies die öffentliche IP-Adresse. Dies führt dazu, dass Rechner aus den *erreichbaren Netzen* nicht erreichbar sind, wenn der Collax Security Gateway nicht gleichzeitig das Default-Gateway für diese Rechner ist.

  Normalerweise wird hier eine IP-Adresse aus einem der als „lokalen Netze“ ausgewählten Netze gewählt.

Tab Policy-Routing

- *Traffic-Policies*: Hier werden die Policies ausgewählt, die dafür sorgen, dass die entsprechenden Netzwerkpakete oder Dienste bevorzugt über diesen Link geleitet werden. Hier können Policies ausgewählt werden, die unternehmenskritischen Datenverkehr kennzeichnen. Werden hier Policies gewählt, die einen lokalen Service, wie Web-Proxy kennzeichnen, wird als Folge der Daten-

verkehr dieses Dienstes nur über diesen Link abgewickelt. Wenn ein zusätzlicher Link in das Zielnetzwerk als Fall-Back-Verbindung definiert ist, wird der Datenverkehr bei Link-Ausfall über diese Fall-Back-Verbindung geleitet.

- *Nur diese Traffic-Policies zulassen*: Mit dieser Option werden auschließlich die Netzwerkpakete über den Link geroutet, die den Traffic-Policies entsprechen. Default-Routen, die unter dem Menüpunkt *Zuordnungen* gesetzt sind, werden nicht mehr berücksichtigt. Wenn nicht klar ist, was diese Option bedeutet, sollte sie leergelassen werden.

Felder in diesem Dialog für Typ *IP-Tunnel*

(Diese Option befindet sich im Zusatzmodul *Collax Gatekeeper*)

- *Bezeichnung*: Hier muss eine eindeutige Bezeichnung für den Link angegeben werden. Unter diesem Namen steht der Link in verschiedenen anderen Dialogen zur Verfügung.
- *Kommentar*: Hier kann ein Kommentartext zu diesem Link angegeben werden.
- *Typ*: Hier wird der genaue Typ des Links angegeben. Abhängig davon werden weitere Felder in diesem Dialog sichtbar bzw. unsichtbar.
- *IP-Adresse des Systems*: Hier wird die lokale IP-Adresse für den Link angegeben. Bleibt das Feld leer, versucht das System, eine dynamische IP-Adresse per PPP oder DHCP zu beziehen. Sollen mehrere IP-Adressen auf einen Netzwerkanschluss zugewiesen werden (IP-Alias), muss für jede IP-Adresse ein eigener Link angelegt werden. Dabei wird jedes Mal die gleiche Schnittstelle angegeben.

  Ist der Link vom Typ *auf Einwahl warten* und bleibt das Feld leer, wird eine zufällig ausgewählte IP-Adresse als lokale IP-

Adresse verwendet. Andernfalls wird die eingetragene IP-Adresse als lokale IP-Adresse genutzt.

- *IP-Adresse der Gegenstelle*: Hier wird die IP-Adresse der Gegenstelle angegeben. Bleibt das Feld leer, versucht das System, die Adresse der Gegenstelle automatisch zu bestimmen.
- *MTU*: Hier kann die maximale Paketgröße auf diesem Link eingestellt werden.

  Große Werte für die MTU verbessern den Durchsatz, da weniger Verwaltungsdaten übertragen werden. Kleine Werte für die MTU hingegen verbessern die Antwortzeiten für interaktive Anwendungen und Echtzeitdatenübertragung (etwa VoIP).

  Wird hier kein Wert eingetragen, wird abhängig von der Art des Links ein geeigneter Wert gewählt. Für Ethernet-Verbindungen wird typischerweise eine MTU von 1500 Byte verwendet.
- *Bandbreitenmanagement*: Mit dieser Option wird das Bandbreitenmanagement für den Link aktiviert. Für indirekte Links, die auf einen anderen Link aufsetzen (Typ Route, Tunnel, VPN usw.) muss auf dem untergeordneten Link bereits das Bandbreitenmanagement aktiviert sein.
- *Bandbreite*: Hier wird die Bandbreite des Links angegeben. Für die Bandbreite von indirekten Links (Typ Route, Tunnel, VPN usw.) ist die Bandbreite des benutzten Links entscheidend.

  Wenn sich mehrere Links eine Hardwareschnittstelle teilen (z. B. LocalNetLink1 und LocalNetLink2 jeweils über eth0), darf die Summe der Bandbreiten der Links die Bandbreite der Hardwareschnittstelle selbst nicht überschreiten.

  In diesem Feld wird als Eingabe eine Dezimalzahl, optional mit Dezimalpunkt, optional gefolgt von Leerzeichen und abschließend einer Einheit erwartet. Folgende Einheiten sind möglich: „k“ für Kilo, „M“ für Mega und „G“ für Giga. Abschließend wird die Einheit als „bps“ für 8 bit/s oder „bit“ für bit/s angegeben. Beispiele: „15.7 kbit“, „100 Mbit“ und „1 Gbit“.

- *SNAT/Masquerading*: SNAT und Masquerading dienen dazu, ganze Netzwerke hinter einer einzelnen IP-Adresse zu „verstecken“. Wird diese Option aktiviert, scheinen alle abgehenden Verbindungen von diesem System zu stammen und nicht vom wirklichen Absender.

  Diese Option muss aktiviert werden, wenn auf dem Internet-Link vom Provider nur eine einzelne IP-Adresse bereitgestellt wird und wenn Systeme aus dem lokalen Netz IP-Verbindungen aufbauen müssen.

  Die Unterscheidung zwischen SNAT und Masquerading erfolgt automatisch, abhängig davon, ob eine IP-Adresse für den Link angegeben wurde oder nicht.

  Hinweis: SNAT/Masquerading für Routen und VPN-Netze funktioniert nur, wenn auf dem unterliegenden Link kein Masquerading aktiviert ist.
- *Zu maskierende Netzwerke*: Wird Masquerading für *spezielle Netze* aktiviert, können in dieser Liste aus allen angelegten Netzwerken diejenigen ausgewählt werden, die maskiert werden müssen.

  Hinweis: Alle Subnetze eines ausgewählten Netzwerks werden ebenfalls maskiert.

  Wird ein Netzwerk aus der Liste ausgewählt, bedeutet das nicht automatisch, dass Daten aus diesem Netzwerk über diesen Link versendet werden können.
- *Erreichbare Netzwerke*: Hier können aus der Liste aller angelegten Netzwerken diejenigen ausgewählt werden, die über diesen Link erreichbar sind. Für jedes ausgewählte Netz wird ein Eintrag unter *Zuordnungen* angelegt.

  Bei VPN-Verbindungen muss das lokale Netz der Gegenstelle innerhalb einem der hier angegebenen Netze liegen.
- *Absenderadresse*: Bei VPN-Verbindungen kann hier die IP-Adresse des Systems gewählt werden. Diese wird als Absenderadresse

verwendet, wenn die Daten vom System selbst stammen. Bei anderer VPN-Software heißt dieses Feature manchmal „virtuelle IP-Adresse“.

Wird hier nichts ausgewählt, wird die IP-Adresse des Links verwendet, über den die verschlüsselten Daten versendet werden. Bei einer Internetverbindung ist dies die öffentliche IP-Adresse. Dies führt dazu, dass Rechner aus den *erreichbaren Netzen* nicht erreichbar sind, wenn der Collax Security Gateway nicht gleichzeitig das Default-Gateway für diese Rechner ist.

Normalerweise wird hier eine IP-Adresse aus einem der als „lokalen Netze“ ausgewählten Netze gewählt.

Tab Policy-Routing

- *Traffic-Policies*: Hier werden die Policies ausgewählt, die dafür sorgen, dass die entsprechenden Netzwerkpakete oder Dienste bevorzugt über diesen Link geleitet werden. Hier können Policies ausgewählt werden, die unternehmenskritischen Datenverkehr kennzeichnen. Werden hier Policies gewählt, die einen lokalen Service, wie Web-Proxy kennzeichnen, wird als Folge der Datenverkehr dieses Dienstes nur über diesen Link abgewickelt. Wenn ein zusätzlicher Link in das Zielnetzwerk als Fall-Back-Verbindung definiert ist, wird der Datenverkehr bei Link-Ausfall über diese Fall-Back-Verbindung geleitet.
- *Nur diese Traffic-Policies zulassen*: Mit dieser Option werden ausschließlich die Netzwerkpakete über den Link geroutet, die den Traffic-Policies entsprechen. Default-Routen, die unter dem Menüpunkt *Zuordnungen* gesetzt sind, werden nicht mehr berücksichtigt. Wenn nicht klar ist, was diese Option bedeutet, sollte sie leergelassen werden.

Felder in diesem Dialog für Typ *PPTP-Server*

(Diese Option befindet sich im Zusatzmodul *Collax Gatekeeper*)

- *Bezeichnung*: Hier muss eine eindeutige Bezeichnung für den Link angegeben werden. Unter diesem Namen steht der Link in verschiedenen anderen Dialogen zur Verfügung.
- *Kommentar*: Hier kann ein Kommentartext zu diesem Link angegeben werden.
- *Typ*: Hier wird der genaue Typ des Links angegeben. Abhängig davon werden weitere Felder in diesem Dialog sichtbar bzw. unsichtbar.
- *DNS-Server an Gegenstelle übermitteln*: Mit dem Aktivieren dieser Option wird der Gegenstelle beim Verbindungsaufbau ein DNS-Server zugewiesen.

  Diese Option wird nur sichtbar, wenn auf dem Link *Auf Einwahl warten* aktiviert wird.
- *1. DNS-Server: lokales DNS benutzen*: Durch das Aktivieren dieser Option wird der Collax Security Gateway der Gegenstelle als erster DNS-Server zugewiesen.
- *1. DNS-Server*: Alternativ kann hier die IP-Adresse eines anderen Nameservers angegeben werden, der als erster DNS-Server zugewiesen wird.
- *2. DNS-Server*: Hier wird die IP-Adresse des zweiten DNS-Servers eingetragen.
- *ISP-Modus*: Durch Aktivieren dieser Option wird der Link im *ISP-Modus* betrieben. Dabei wird der Gegenstelle eine IP-Adresse zugewiesen, und es werden keine Netze zur Gegenseite geroutet. Dies ist der gebräuchlichste Modus.

  Wird der ISP-Modus deaktiviert, können aus den angelegten Netzwerken diejenigen ausgewählt werden, die über die Gegenseite erreichbar sind.

- *IP-Adresse des Systems*: Hier wird die lokale IP-Adresse für den Link angegeben. Bleibt das Feld leer, versucht das System, eine dynamische IP-Adresse per PPP oder DHCP zu beziehen. Sollen mehrere IP-Adressen auf einen Netzwerkanschluss zugewiesen werden (IP-Alias), muss für jede IP-Adresse ein eigener Link angelegt werden. Dabei wird jedes Mal die gleiche Schnittstelle angegeben.

  Ist der Link vom Typ *auf Einwahl warten* und bleibt das Feld leer, wird eine zufällig ausgewählte IP-Adresse als lokale IP-Adresse verwendet. Andernfalls wird die eingetragene IP-Adresse als lokale IP-Adresse genutzt.
- *IP-Adressen für Zuweisung an Gegenstelle*: In diesem Feld werden, durch Leerzeichen getrennt, die IP-Adressen angegeben, die bei einer Einwahl an die Gegenstelle zugewiesen werden. Dabei sollte pro unterstütztem Kanal eine IP-Adresse bereit gestellt werden.

  Wird das Feld leer gelassen, wird der Gegenstelle eine zufällig ausgewählte IP-Adresse übermittelt. Dann kann sich jedoch zu einem Zeitpunkt immer nur ein System einwählen.
- *Verschlüsselungsalgorithmus*: Hier werden die unterstützten Schlüssellängen für den Algorithmus der PPTP-Verbindung ausgewählt. Zur Auswahl stehen 40, 56 und 128 Bit. Grundsätzlich bietet eine größere Schlüssellänge eine höhere Sicherheit.

  Hinweis: Der Verschlüsselungsalgorithmus ist schwach und wurde bereits gebrochen.
- *Auf Verschlüsselung bestehen*: Das Aktivieren dieser Option verhindert unverschlüsselte Verbindungen.
- *MTU*: Hier kann die maximale Paketgröße auf diesem Link eingestellt werden.

  Große Werte für die MTU verbessern den Durchsatz, da weniger Verwaltungsdaten übertragen werden. Kleine Werte für die MTU hingegen verbessern die Antwortzeiten für interaktive Anwendungen und Echtzeitdatenübertragung (etwa VoIP).

Wird hier kein Wert eingetragen, wird abhängig von der Art des Links ein geeigneter Wert gewählt. Für Ethernet-Verbindungen wird typischerweise eine MTU von 1500 Byte verwendet.

- *Bandbreitenmanagement*: Mit dieser Option wird das Bandbreitenmanagement für den Link aktiviert. Für indirekte Links, die auf einen anderen Link aufsetzen (Typ Route, Tunnel, VPN usw.) muss auf dem untergeordneten Link bereits das Bandbreitenmanagement aktiviert sein.
- *Bandbreite*: Hier wird die Bandbreite des Links angegeben. Für die Bandbreite von indirekten Links (Typ Route, Tunnel, VPN usw.) ist die Bandbreite des benutzten Links entscheidend.

  Wenn sich mehrere Links eine Hardwareschnittstelle teilen (z. B. LocalNetLink1 und LocalNetLink2 jeweils über eth0), darf die Summe der Bandbreiten der Links die Bandbreite der Hardwareschnittstelle selbst nicht überschreiten.

  In diesem Feld wird als Eingabe eine Dezimalzahl, optional mit Dezimalpunkt, optional gefolgt von Leerzeichen und abschließend einer Einheit erwartet. Folgende Einheiten sind möglich: „k“ für Kilo, „M“ für Mega und „G“ für Giga. Abschließend wird die Einheit als „bps“ für 8 bit/s oder „bit“ für bit/s angegeben. Beispiele: „15.7 kbit“, „100 Mbit“ und „1 Gbit“.

Tab Policy-Routing

- *Traffic-Policies*: Hier werden die Policies ausgewählt, die dafür sorgen, dass die entsprechenden Netzwerkpakete oder Dienste bevorzugt über diesen Link geleitet werden. Hier können Policies ausgewählt werden, die unternehmenskritischen Datenverkehr kennzeichnen. Werden hier Policies gewählt, die einen lokalen Service, wie Web-Proxy kennzeichnen, wird als Folge der Datenverkehr dieses Dienstes nur über diesen Link abgewickelt. Wenn

ein zusätzlicher Link in das Zielnetzwerk als Fall-Back-Verbindung definiert ist, wird der Datenverkehr bei Link-Ausfall über diese Fall-Back-Verbindung geleitet.

- *Nur diese Traffic-Policies zulassen*: Mit dieser Option werden ausschließlich die Netzwerkpakete über den Link geroutet, die den Traffic-Policies entsprechen. Default-Routen, die unter dem Menüpunkt *Zuordnungen* gesetzt sind, werden nicht mehr berücksichtigt. Wenn nicht klar ist, was diese Option bedeutet, sollte sie leergelassen werden.

7.4.2.3 *Traffic-Klassen*

(Diese Option befindet sich im Zusatzmodul *Collax Net Security*)
(Dieser Dialog befindet sich unter *Netzwerk – Links – Konfiguration*)
Über die Traffic-Klassen können im Bandbreitenmanagement bestimmte Garantien bzw. Begrenzungen für einzelne Verbindungen gesetzt werden. In diesem Dialog werden die vorhandenen Traffic-Klassen angezeigt und bearbeitet.

Abschnitt *Angelegte Traffic-Klassen*, Spalten in der Tabelle

- *Name*: Hier wird der Name der Klasse angezeigt.
- *Kommentar*: Hier wird der Kommentartext angezeigt.
- *Garantierte Rate*: In dieser Spalte wird die garantierte Rate der Klasse angezeigt.
- *Maximale Rate*: In dieser Spalte wird die maximale Rate der Klasse angezeigt.
- *Priorität*: In dieser Spalte wird die Priorität der Klasse angezeigt.
- *Maximale Einheit*: In dieser Spalte wird die größte Einheit, für die eine Latenzgarantie besteht, angezeigt.

- *Maximale Latenz*: In dieser Spalte wird die garantierte maximale Latenz der Klasse angezeigt.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird eine Traffic-Klasse bearbeitet.
- *Löschen*: Diese Aktion löscht die Klasse.

Abschnitt *Traffic-Klasse bearbeiten* Felder in diesem Abschnitt

- *Name*: Hier wird der Name für die Klasse angegeben.
- *Kommentar*: Hier kann ein Kommentartext zu der Klasse angegeben werden.
- *Garantierte Rate (in Prozent oder absolut)*: Hier wird bei HTB die garantierte Bandbreite der Klasse angegeben. Falls die Klasse nicht die gesamte verfügbare Bandbreite benötigt, kann die restliche Bandbreite von Verbindungen aus anderen Traffic-Klassen genutzt werden.

  In diesem Feld wird als Eingabe eine Dezimalzahl, optional mit Dezimalpunkt, optional gefolgt von Leerzeichen und abschließend einer Einheit erwartet. Folgende Einheiten sind möglich: „k“ für Kilo, „M“ für Mega und „G“ für Giga. Abschließend wird die Einheit als „bps“ für 8 bit/s oder „bit“ für bit/s angegeben. Beispiele: „15.7 kbit“, „100 Mbit“ und „1 Gbit“.
- *Maximale Rate (in Prozent oder absolut)*: Hier wird bei HTB die maximale Bandbreite angegeben, die die Klasse benutzen darf. Eingaben werden in dem gleichen Format akzeptiert, das für die garantierte Rate verwendet wird.
- *Priorität*: Hier wird bei HTB die Priorität der Klasse angegeben. Die Priorität ist für die Verteilung von ungenutzter Bandbreite

entscheidend. Klassen mit höherer Priorität bekommen die überschüssige Bandbreite immer zuerst angeboten.

- *Maximale Einheit*: Hier wird bei H-FSC die größte Einheit angegeben, für die eine Latenzgarantie gewünscht wird. Im Falle des normalen Netzwerkverkehrs ist dies die MTU (inklusive der Größe des Ethernet-Headers bei Ethernet-Links). Für eine Audio- oder Video-Klasse sollte eine Frame-Größe benutzt werden. Falls kein Wert angegeben ist, wird die MTU zuzüglich der Größe des Headers benutzt.

  Diese Eingabe ist nicht notwendig, wenn keine speziellen Latenzgarantien benötigt werden.
- *Maximale Latenz (in Prozent oder absolut)*: Hier wird bei H-FSC die maximale Latenz angegeben. Im Normalfall bestimmt sich die maximale Latenz direkt aus der garantierten Bandbreite. Falls eine Klasse besondere Anforderungen hat (VoIP, Video, interaktiver Netzwerkverkehr) oder für Netzwerkverkehr, der nicht unter höherer Latenz leidet (FTP), kann die garantierte Latenz unabhängig von der garantierten Rate angegeben werden.

  In diesem Feld wird als Eingabe eine Dezimalzahl, optional mit Dezimalpunkt, optional gefolgt von Leerzeichen und abschließend einer Einheit akzeptiert. Folgende Einheiten sind möglich: „u“ für Micro und „m“ für Milli, abschließend die Einheit „s“. Beispiele: „250us“, „400ms“, „0.4s“.

  Diese Eingabe ist nicht notwendig, wenn keine speziellen Latenzgarantien benötigt werden.
- *Garantierte Rate (in Prozent oder absolut)*: Hier wird bei H-FSC die garantierte Bandbreite der Klasse angegeben. Falls die Klasse nicht die gesamte verfügbare Bandbreite benötigt, kann die restliche Bandbreite von Verbindungen aus anderen Traffic-Klassen genutzt werden.

  In diesem Feld wird als Eingabe eine Dezimalzahl, optional mit

Dezimalpunkt, optional gefolgt von Leerzeichen und abschließend einer Einheit erwartet. Folgende Einheiten sind möglich: „k“ für Kilo, „M“ für Mega und „G“ für Giga. Abschließend wird die Einheit als „bps“ für 8 bit/s oder „bit“ für bit/s erwartet. Beispiele: „15.7 kbit“, „100 Mbit“ und „1 Gbit“.

- *Maximale Rate (in Prozent oder absolut)*: Hier wird bei H-FSC die maximale Bandbreite angegeben, die die Klasse benutzen darf. Eingaben werden in dem gleichen Format akzeptiert, das für die garantierte Rate verwendet wird.
- *Innere Queueing-Disziplin*: Hier wird der Typ der inneren Queue gewählt. Zur Auswahl stehen FIFO (First-In-First-Out) und SFQ (Stochastic Fairness Queue).
- *Limit (Pakete)*: Hier kann bei der Verwendung einer FIFO-Queue die maximale Anzahl von Paketen, die gehalten werden, angegeben werden. Wird kein Wert angegeben, wird automatisch ein Wert verwendet, der sich an der garantierten Rate orientiert.
- *Verteilung*: Bei einer SF-Queue kann hier die Verteilung der Bandbreite gewählt werden: *Per-flow* verteilt die Bandbreite fair unter allen Verbindungen, *per-source* zwischen allen Absender-IP-Adressen und *per-destination* zwischen allen Ziel-IP-Adressen.
- *Limit (Pakete)*: Hier kann bei einer SF-Queue die maximale Anzahl von Paketen angegeben werden, die gehalten werden sollen. Wird kein Wert angegeben, wird automatisch ein Wert verwendet, der sich an der garantierten Rate orientiert.
- *Traffic-Markierung*: Mit dieser Auswahl wird festgelegt, dass Paketen mit den angegebenen Markierungen Bandbreite aus dieser Klasse zugeteilt werden soll. Traffic-Markierungen können pro Link nur einer der verschiedenen Klassen zugeordnet werden. Die Zuordnung der gewünschten Bandbreite zum Dienst wird über die Firewallmatrix definiert.
- *Traffic-Markierung (Antwort)*: Mit dieser Auswahl wird festge-

legt, dass Antwortpaketen mit den angegebenen Markierungen Bandbreite aus dieser Klasse zugeteilt werden soll. Traffic-Markierungen können pro Link nur einer der verschiedenen Klassen zugeordnet werden. Die Zuordnung der gewünschten Bandbreite zum Dienst wird über die Firewallmatrix definiert.

Abschnitt *Plot*
Felder in diesem Abschnitt

- *Plot*: In dieser Grafik werden alle angelegten Traffic-Klassen grafisch dargestellt.

Aktionen für diesen Dialog

- *Traffic-Klasse hinzufügen*: Mit dieser Aktion wird eine neue Klasse angelegt.
- *Traffic-Klassen speichern*: Bearbeiten der Traffic-Klassen beenden. Die Änderungen werden gespeichert.

7.4.3 *Zuordnung*

Unter *Zuordnung* wird die „Routingtabelle“ des Collax Security Gateways angezeigt. Da intern Policy-Routing genutzt wird, existiert keine starre Routingtabelle. Vielmehr können zu einem Zielnetz alternative Wege (Links) bestehen, die über Prioritäten gesteuert werden.

Hinweis: Bei der Zuordnung von Links zu den Netzwerken ist zu beachten, dass auch Konfigurationen möglich sind, die ohne spezielle Einstellungen an anderen Routern im Netzwerk nicht funktionieren.

7.4.3.1 *Prioritäten*

(Dieser Dialog befindet sich unter *Netzwerk – Links – Zuordnung*)

In diesem Dialog wird die Zuordnung von Links und den jeweils erreichbaren Netzen dargestellt. Über einstellbare Prioritäten kann das Routing gesteuert werden. In diesem Dialog können neue Zuordnungen angelegt und vorhandene gelöscht werden.

Felder in diesem Dialog

- *Priorität*: In diesem Feld wird die Priorität angezeigt. Existieren zu einem Zielnetz alternative Wege, unterscheiden sich diese durch die Priorität. Dabei wird zunächst der Weg mit der höchstmöglichen Priorität verwendet. Der Vorgabewert ist 1 (höchste Priorität).
- *Netz*: Hier wird der Name des Netzwerks angezeigt.
- *Link*: Hier wird der Link angezeigt, auf dem das Netz als *erreichbar* markiert ist.
- *Typ*: Hier wird der Typ des Links angezeigt.

Aktionen für jeden Tabelleneintrag

- *Höher*: Mit dieser Aktion wird die Priorität des Links erhöht.
- *Niedriger*: Mit dieser Aktion wird die Priorität des Links verringert.
- *Löschen*: Mit dieser Aktion wird die Zuordnung gelöscht. Das Netz wird auf dem zugehörigen Link aus der Liste der *erreichbaren Netze* entfernt.

Aktionen für diesen Dialog

- *Anlegen*: Mit dieser Aktion wird eine neue Zuordnung angelegt.

7.4.3.2 *Neue Zuordnung*

(Dieser Dialog befindet sich unter *Netzwerk – Links – Zuordnung*)

Felder in diesem Dialog

- *Netzwerk*: Hier wird das Netzwerk ausgewählt, für das ein neuer Eintrag angelegt werden soll.
- *Link*: Hier wird der zugehörige Link ausgewählt, über den das Netzwerk erreichbar sein soll.

7.4.4 *Traffic-Policies*

(Diese Option befindet sich im Zusatzmodul *Collax Net Security Advanced*)

Um die Funktionen Policy-Routing nutzen zu können, müssen Netzwerkpakete markiert werden. Für die Kennzeichnung werden hierzu die Traffic-Policies benutzt. Sie bilden die Schnittstelle zwischen dem eigentlichen Netzwerkverkehr, der in der Firewall-Matrix spezifiziert ist, den lokalen Diensten und dem Policy-Routing andererseits. Mit den Traffic-Policies kann bestimmter Netzwerkverkehr oder eine bestimmte Dienstegruppe (Subsystem) über bestimmte Verbindungen (Links) geleitet werden.

7.4.4.1 *Traffic-Policy wählen*

(Dieser Dialog befindet sich unter *Netzwerk – Links – Traffic-Policies*)

- *Name*: Hier wird der Name der Traffic-Policy angezeigt.
- *Kommentar*: Hier wird der Kommentar zur Traffic-Policy angezeigt.

Aktionen für diesen Dialog

- *Bearbeiten*: Hier kann die ausgewählte Traffic-Policy bearbeitet werden.
- *Löschen*: Hier wird die gewählte Traffic-Policy gelöscht.

Aktionen für diesen Dialog

- *Hinzufügen*: Hier kann eine Traffic-Policy hinzugefügt werden.

7.4.4.2 *Traffic-Policy bearbeiten*

(Dieser Dialog befindet sich unter *Netzwerk – Links – Traffic-Policy*)

- *Name*: Hier wird der Name der Traffic-Policy angezeigt oder eingegeben. Der Name sollte entsprechend der nachfolgenden Anwendung für das Policy-Routing gewählt werden.
- *Kommentar*: In diesem Feld kann ein Kommentartext zur angelegten Traffic-Policy eingegeben werden. Hier können Informationen hinterlegt werden, die die Anwendung kennzeichnen.

7.4.4.3 Tab *Lokale Dienste*, Abschnitt *Lokale Dienste*

Felder in diesem Abschnitt

- *Verwenden für*: Hier wird die Dienstegruppe (Subsystem) angegeben, die über einen bestimmte Verbindung (Link) geroutet werden soll.

7.4.4.4 Tab *Traffic zwischen Netzwerkgruppen*, Abschnitt *Netzwerkgruppe → Netzwerkgruppe*

Felder in diesem Abschnitt

- *Anwenden auf Regel*: Hier wird der erlaubte Verkehr von Netzwerkgruppe zu Netzwerkgruppe ausgewählt, der über eine bestimmte Verbindung (Link) geroutet werden soll. Entsprechende Erlaubnis-Regeln sind vorweg in der Firewall-Matrix zu konfigurieren.

7.4.4.5 Tab *Senden über Link*, Abschnitt *Netzwerk Links*

Felder in diesem Abschnitt

- *Bevorzugt versenden über*: Hier wird bestimmt, über welche Verbindung (Link) die zuvor gewählten lokalen Dienstegruppen, oder der gewählte Netzwerkverkehr geroutet werden soll. Wenn möglich, werden die entsprechenden Netzwerkpakete über den angegebenen Link geroutet. Ansonsten werden die Netzwerkpakete über die normale Route versendet.

7.4.5 *IPsec-Proposals*

(Diese Option befindet sich im Zusatzmodul *Collax Gatekeeper*)

In diesem Formular werden Verschlüsselungsmethoden und Hash-Algorithmen für die verschiedenen Stufen von VPN-Verbindungen vordefiniert. Diese vordefinierten IPsec-Proposals können anschließend den gewünschten VPN-Verbindungen zugewiesen werden.

7.4.5.1 *IPsec-Proposal wählen*

In der Tabelle werden alle vordefinierten Proposals gelistet. Informationen werden in der Tabelle angezeigt, Aktionen können über das Kontextmenü oder den Aktionsknopf im Formular vorgenommen werden.

(Dieser Dialog befindet sich unter *Netzwerk – Links – IPsec-Proposals*)

Felder in diesem Formular

- *Bezeichnung*: Hier wird der Name des definierten Proposals angezeigt.
- *Kommentar*: Ist eine zusätzliche Beschreibung hinterlegt, wird diese hier angezeigt.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion im Kontextmenü (rechter Mausklick oder Doppelklick) kann das ausgewählte IPsec-Proposal bearbeitet werden.
- *Löschen*: Mit dieser Aktion im Kontextmenü (rechter Mausklick) kann das gewählte Element gelöscht werden.

- *Anzeigen*: Mit dieser Aktion können die Werte des definierten IPsec-Proposals abgerufen werden.

Aktionen für dieses Formular

- *Hinzufügen*: Mit dieser Aktion wird ein neues IPsec-Proposal erzeugt.

7.4.5.2 *IPsec-Proposal bearbeiten*

Abschnitt *Grundeinstellungen*

Felder in diesem Abschnitt

- *Bezeichnung*: Hier wird die Bezeichnung des Proposals angezeigt oder eingegeben.
- *Kommentar*: Zusätzliche Informationen werden in diesem Feld eingegeben.

Abschnitt *Schlüsselaustausch (IKE)*

Felder in diesem Abschnitt

- *Aggressive Mode*: Der Aggressive Mode kann bei IPsec-Verbindungen mit PSK verwendet werden. In diesem Modus wird die ID der Gegenstelle bereits beim Verbindungsaufbau übermittelt. Diese Option wird für Verbindungen zu bestimmten Gegenstellen benötigt (beispielsweise Cisco).
- *Verschlüsselungsmethode*: In dieser Liste stehen verschiedene Algorithmen zur Auswahl, die für die Verschlüsselung beim Schlüsselaustausch verwendet werden können. Die Voreinstellung ist *3DES*, ein Verfahren, das von den meisten Gegenstellen unterstützt wird. Wenn möglich, sollte *AES* als Verfahren genutzt werden.

- *Hash-Algorithmus*: In dieser Liste stehen verschiedene Verfahren zur Prüfsummenbildung zur Auswahl. Mit dem gewählten Algorithmus wird die Echtheitsprüfung von Paketen während des Schlüsselaustausches durchgeführt. Voreingestellt ist das verbreitete Verfahren *MD5*. Wenn die Gegenstelle es unterstützt, kann *SHA-1* verwendet werden.
- *DH-Gruppen*: Für die Einigung auf einen gemeinsamen Schlüssel wird das Verfahren nach Diffie und Hellmann benutzt. Hier wird die Diffie-Hellmann-Gruppe, mit der entsprechenden Angabe der Primzahllänge in Bit, ausgewählt.
- *Lifetime*: Nach Ablauf der eingestellten Zeit wird der Tunnel getrennt und die Verbindung mit der Gegenstelle neu ausgehandelt.
- *Perfect Forwarding Secrecy*: Wird diese Option aktiviert, wird bei jedem Verbindungsaufbau ein neuer Schlüsselsatz für die Übertragung ausgehandelt. Ein eventuell noch gültiger Schlüssel aus der vorhergehenden Verbindung wird verworfen.

Abschnitt *Datenaustausch (ESP)*
Felder in diesem Abschnitt

- *Kompression*: Über diese Option kann die Kompression der übertragenen Daten im Tunnel aktiviert werden.
- *Verschlüsselungsmethode*: Analog zur IKE-Verbindung wird hier der Verschlüsselungsalgorithmus für die eigentliche Datenübertragung eingestellt. Es gelten die gleichem Empfehlungen wie bei der IKE-Verbindung.
- *Hash-Algorithmus*: Analog zur IKE-Verbindung wird hier der Prüfsummenalgorithmus für die eigentliche Datenübertragung eingestellt. Es gelten die gleichem Empfehlungen wie bei der IKE-Verbindung.
- *Keylife*: Nach Ablauf der eingestellten Zeit wird ein neuer Schlüssel für die reine Datenübertragung ausgehandelt.

Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten des IPsec-Proposals beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten des IPsec-Proposals beenden. Die Änderungen werden übernommen.

7.4.5.3 *IPsec-Proposal anzeigen*

Mit dieser Aktion können die Werte eines definiertes IPsec-Proposal angezeigt werden.

Felder in diesem Abschnitt

- *Bezeichnung*: Hier wird die Bezeichnung des IPsec-Proposals angezeigt.
- *Kommentar*: Ist ein Kommentar hinterlegt, wird dieser hier angezeigt.

Abschnitt *Schlüsselaustausch (IKE)*
Felder in diesem Abschnitt

- *Aggressive Mode*: Hier wird angezeigt, ob Aggressive Mode aktiviert ist.
- *Verschlüsselungsmethode*: Hier wird die gewählte Verschlüsselungsmethode angezeigt.
- *Hash-Algorithmus*: Hier wird der gewählte Hash-Algorithmus angezeigt.
- *DH-Gruppen*: Hier wird die gewählte DH-Gruppe angezeigt.
- *Lifetime*: Hier wird Lifetime in Minuten angezeigt.

- *Perfect Forwarding Secrecy*: Hier wird angezeigt, ob Perfect Forwarding Secrecy aktiviert ist.

Abschnitt *Datenaustausch (ESP)*
Felder in diesem Abschnitt

- *Kompression*: Hier wird angezeigt, ob Kompression aktiviert ist.
- *Verschlüsselungsmethode*: Hier werden die gewählte Verschlüsselungsmethode angezeigt.
- *Hash-Algorithmus*: Hier wird der gewählte Hash-Algorithmus angezeigt.
- *Keylife*: Hier wird Keylife in Minuten angezeigt.

Aktionen für dieses Formular

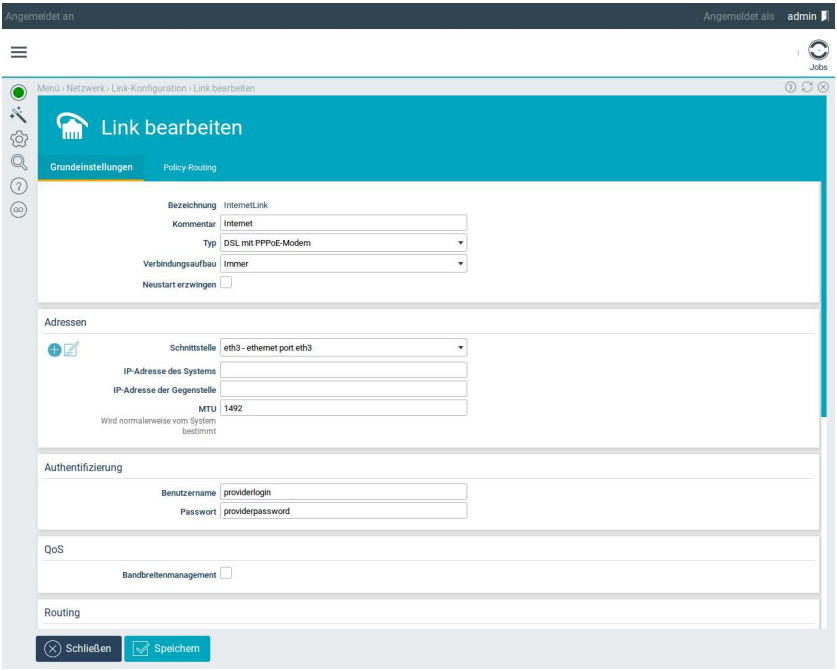
- *Zurück*: Diese Aktion beendet die Anzeige und führt zurück zum Hauptformular.

7.5 Schritt für Schritt: Internetzugang einrichten

Abhängig von der Leitungsart kann die Verbindung zum Internet auf verschiedenen Wegen erfolgen. In diesem Abschnitt werden die gängigsten Verbindungen vorgestellt.

7.5.1 Zugang über DSL

(Diese Option befindet sich im Zusatzmodul *Collax Gatekeeper*)

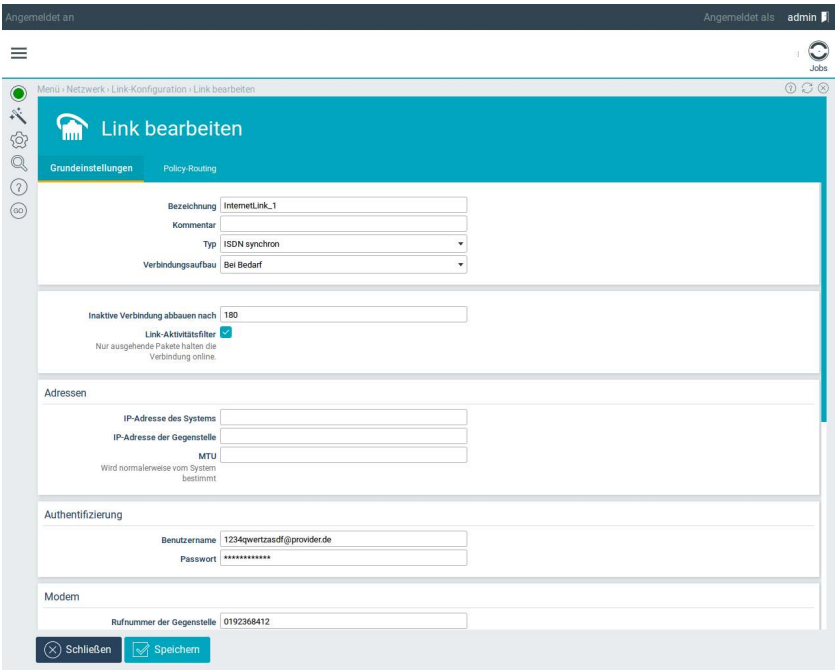


- Bearbeiten Sie unter *Netzwerk – Links – Konfiguration* den aus der Grundeinstellung vorhandenen *InternetLink*.
- Ändern Sie den *Typ* auf *DSL mit PPPoE* bzw. *DSL mit PPTP*. Diese Einstellung ist abhängig von Ihrem Provider. Sehr weit verbreitet ist *PPPoE*.
- Unter *Verbindungsaufbau* legen Sie fest, wann die Verbindung aufgebaut werden soll. *Immer* ist bei einer Flatrate eine sinnvolle Einstellung. Wird Ihnen die Zeit, in der Sie online sind, berechnet, ändern Sie den Wert auf *Bei Bedarf*. Lesen Sie hierfür die Erläuterungen zur Internetverbindung mit ISDN.

- Die *IP-Adressen* Ihres Systems und der Gegenstelle können leer bleiben. Bei dynamischen (wechselnden) IP-Adressen müssen sie sogar leer bleiben. Diese Werte werden dem Collax Security Gateway beim Login vom Providersystem mitgeteilt.
- Tragen Sie unter *Benutzername* und *Passwort* Ihre Zugangsdaten ein.
- Die *MTU* ist bei DSL-Verbindungen kleiner als 1500. Beim Speichern der Einstellungen nimmt der Collax Security Gateway eine Korrektur vor, Sie können also den Wert 1500 zunächst so belassen.
- Wählen Sie unter *Schnittstelle* aus, mit welchem Netzwerkanschluss des Collax Security Gateways Sie das DSL-Modem verbunden haben. Für ein DSL-Modem darf die Schnittstelle in keinem anderen Link verwendet werden.
- Ändern Sie die Einstellung von *SNAT/Masquerading* auf *Alle Netze*, wenn Sie im lokalen Netz private IP-Adressen verwenden und von dort aus auf das Internet zugreifen möchten.
- Unter *Erreichbare Netze* wählen Sie das *Internet* aus. Nur dieses Netz befindet sich „auf der anderen Seite“ der DSL-Verbindung.
- Speichern Sie den geänderten Link.

7.5.2 Zugang über ISDN

(Diese Option befindet sich im Zusatzmodul *Collax Gatekeeper*)



- Prüfen Sie, ob unter *Systembetrieb – Hardware – Konfiguration – ISDN* eine ISDN-Karte und eine passende MSN-Rufnummer vorhanden sind. Legen Sie andernfalls zunächst eine MSN an.
- Bearbeiten Sie unter *Netzwerk – Links – Konfiguration* den aus der Grundeinstellung vorhandenen *InternetLink*.
- Wählen Sie unter *Typ* die Einstellung *ISDN synchron* aus.
- Da bei einer ISDN-Verbindung meist die Onlinezeit abgerechnet wird, stellen Sie *Verbindungsaufbau* auf *Bei Bedarf*. Wenn Sie eine Flatrate nutzen, können Sie auch die Einstellung *Immer* wählen, um eine permanente Verbindung mit dem Internet herzustellen.
- Wird die Verbindung bei Bedarf aufgebaut, kann unter *Inaktive Verbindung abbauen nach* eine Zeitspanne eingegeben werden, nach deren Ablauf die Verbindung bei Inaktivität abgebrochen

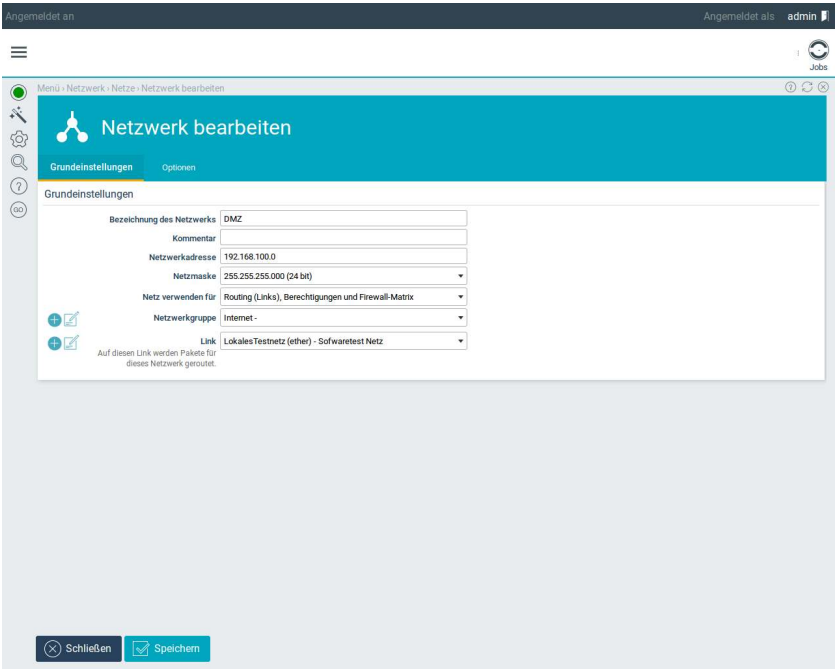
wird. In diesem Fall darf jedoch kein Netzwerkverkehr mehr stattfinden. Wenn Sie durch DNS-Anfragen oder VPN-Verbindungen Datenpakete austauschen, wird der Inaktivitätstimer wieder auf Null gesetzt.

- Durch das Aktivieren von *Link-Aktivitätsfilter* werden zur Analyse des Datenverkehrs nur ausgehende Pakete herangezogen. Pakete aus dem Internet, die womöglich noch von der Firewall blockiert werden, setzen dann den Inaktivitätstimer nicht zurück.
- Unter *Kanäle* kann die Anzahl der ISDN-Kanäle angegeben werden. Einige Provider unterstützen Kanalbündelung, womit dann mehrere ISDN-Kanäle zusammengeschaltet werden können.
- Die *IP-Adressen* von Ihrem System und der Gegenstelle können leer bleiben. Bei dynamischen (wechselnden) IP-Adressen müssen sie sogar leer bleiben. Diese Werte werden dem Collax Security Gateway beim Login vom Providersystem mitgeteilt.
- Tragen Sie unter *Benutzername* und *Passwort* Ihre Zugangsdaten ein.
- Unter *Rufnummer der Gegenstelle* geben Sie die Rufnummer des Providers ein.
- Unter *MSN* wählen Sie die Nummer, die Ihre ISDN-Karte als eigene Rufnummer signalisiert.
- *Secure MSN* und *Callback* sind sinnvolle Optionen, wenn Sie über ISDN Fernwartungsverbindungen zu anderen Systemen konfigurieren. Für eine Internetverbindung lassen Sie diese Felder leer.
- Die *MTU* für ISDN beträgt 1500.
- Ändern Sie die Einstellung von *SNAT/Masquerading* auf *Alle Netze*, wenn Sie im lokalen Netz private IP-Adressen verwenden und von dort auf das Internet zugreifen möchten.
- Unter *Erreichbare Netze* wählen Sie das *Internet* aus. Nur dieses Netz befindet sich „auf der anderen Seite“ der ISDN-Verbindung.
- Speichern Sie den geänderten Link.

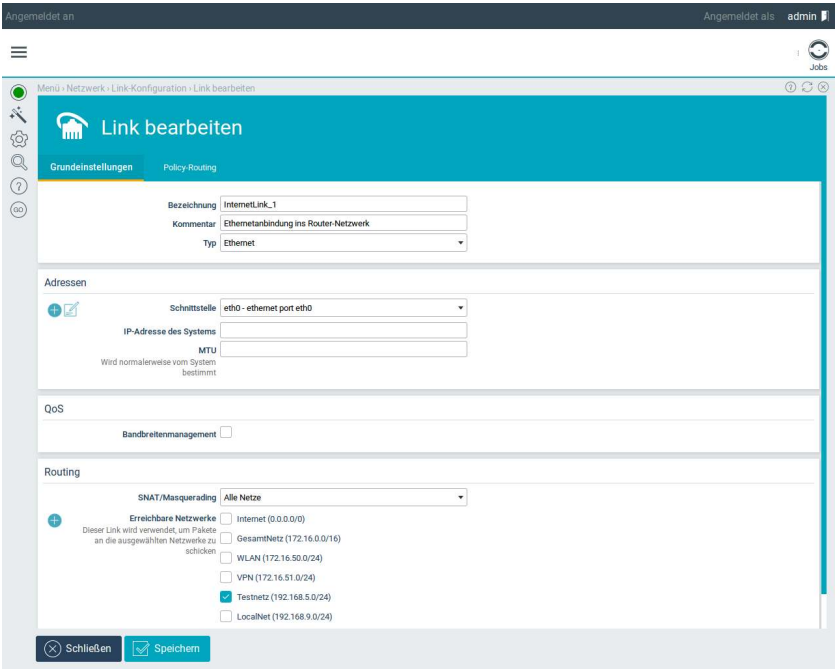
7.5.3 Zugang über einen Router

Wird vom Provider ein Router für die Internetverbindung bereitgestellt, ist die Einrichtung etwas aufwendiger. Damit der Collax Security Gateway als Trennstelle zwischen lokalem Netz und dem Internet fungieren kann, müssen beide Bereiche auf eigenen Netzwerkschnittstellen angeschlossen sein. Zunächst müssen Sie daher das Netzwerk und einen entsprechenden Link für die Verbindung zum Router anlegen. Darüber können Sie dann die Internetverbindung leiten.

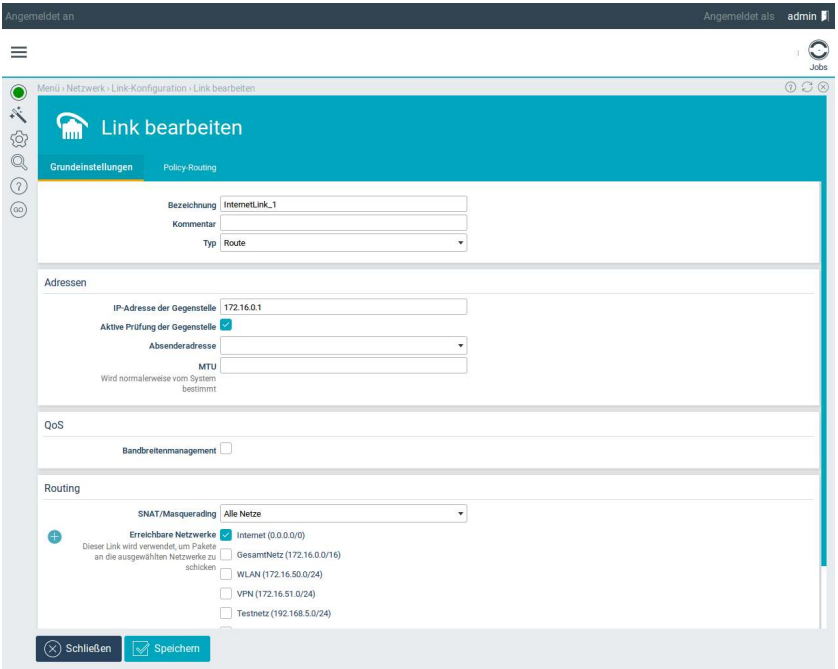
Existiert bereits eine Firewall im Netz und soll der Collax Security Gateway nur für spezielle Serverdienste (PDC, Fileserver usw.) verwendet werden, müssen Sie weder das Netz noch einen Link für einen Router anlegen. Diese Firewall stellt dann das Gateway zum Internet dar und hat eine IP-Adresse im *LocalNet*. Sie ist dadurch über den *LocalNetLink* für den Collax Security Gateway erreichbar. In diesem Fall müssen nur der *InternetLink* modifiziert und die IP-Adresse der Firewall als *Gegenstelle* eingetragen werden.



- Wechseln Sie zu *Netzwerk – Netze – Konfiguration* und legen Sie ein neues *RouterNetz* an.
- Verwenden Sie den IP-Bereich und die Netzmaske, die Ihr Provider Ihnen mitgeteilt hat.
- Speichern Sie das neu erstellte Netz.



- Wechseln Sie zu *Netzwerk – Links – Konfiguration* und legen Sie einen neuen *RouterLink* an.
- Setzen Sie den *Typ* auf Ethernet.
- Tragen Sie unter *IP-Adresse* die IP-Nummer für Ihren Collax Security Gateway ein. Diese muss zum IP-Bereich des Routernetzes gehören. Soll der Collax Security Gateway eine IP-Adresse per DHCP beziehen, lassen Sie das Feld leer.
- Wählen Sie unter *Schnittstelle* das Netzwerkinterface aus, an dem der Router angeschlossen ist.
- *SNAT/Masquerading* kann deaktiviert bleiben, da nur der Collax Security Gateway selbst Datenpakete zum Router schicken wird.
- Unter *Erreichbare Netze* wählen Sie das *RouterNetz* aus.
- Speichern Sie das neu erstellte Netz.



- Bearbeiten Sie unter *Netzwerk – Links – Konfiguration* den aus der Grundeinstellung vorhandenen *InternetLink*.
- Ändern Sie die Einstellung von *Typ* auf *Route*.
- Unter *IP-Adresse der Gegenstelle* geben Sie die IP-Adresse des Routers ein.
- Die *MTU* kann auf 1500 eingestellt bleiben.
- Ändern Sie die Einstellung von *SNAT/Masquerading* auf *Alle Netze*, wenn Sie im lokalen Netz private IP-Adressen verwenden und von dort auf das Internet zugreifen möchten.
- Unter *Erreichbare Netze* wählen Sie das *Internet* aus. Nur dieses Netz befindet sich hinter dem Router.
- Speichern Sie Ihre Änderungen.

7.6 Schritt für Schritt: Einwahllink für VPN

(Diese Option befindet sich im Zusatzmodul *Collax Gatekeeper*)

- Über ein VPN werden zwei Netze über Gateways gekoppelt. Werden zwei Collax Security Gateway gekoppelt, ist auf einem Server ein Einwahllink und auf dem anderen ein Auswahllink erforderlich. Wird ein Client angekoppelt, ist ein Einwahllink ausreichend. Definieren Sie zunächst unter *Netzwerk – Netze – Konfiguration* ein neues Netz mit dem IP-Bereich der anderen Seite.
- Nun legen Sie unter *Netzwerk – Links – Konfiguration* einen neuen Link für den VPN-Tunnel an.
- Stellen Sie den *Typ* auf „VPN“. Dies bezeichnet einen IPsec-Tunnel.
- Wählen Sie unter *Verbindungsaufbau* die Einstellung „auf Einwahl warten“, um Verbindungen anzunehmen.
- Wenn Sie das lokale Netz auf Seite des Collax Security Gateways zugänglich machen möchten, lassen Sie die Option *Host-zu-Netz-Verbindung* deaktiviert.
- Wenn Sie mit einem symmetrischen Schlüssel den Tunnelaufbau sichern wollen, wählen Sie unter *Eigener Schlüssel* „PSK“ aus und tragen Sie die Passphrase entsprechend unter *Passphrase für Verschlüsselung* ein. Wird die Gegenstelle den Tunnelaufbau im *Aggressive Mode* durchführen, aktivieren Sie bitte diese Einstellung.
- Wenn Sie mit Zertifikaten arbeiten möchten, müssen Sie zunächst geeignete Zertifikate erstellen bzw. importieren. Alle Zertifikate mit einem privaten Schlüsselteil sind unter *Eigener Schlüssel* aufgelistet. Wählen Sie das für Ihren Collax Security Gateway passende aus. Den *Schlüssel der Gegenstelle* wählen Sie

ebenfalls entsprechend aus. Die Verwendung von Zertifikaten ist einer PSK-Verbindung vorzuziehen.

- Wenn Sie mit einer CA arbeiten, können Sie für *Schlüssel der Gegenstelle* auch den CA-Schlüssel auswählen. Dann können sich auf diesem Link alle Gegenstellen einwählen, die ein gültiges Zertifikat haben, welches von der gewählten CA signiert wurde. Diese Einstellung eignet sich, wenn mehrere Roadwarrior mit dem Netzwerk verbunden werden sollen. Falls ausgeteilte Zertifikate für die VPN-Verbindung nicht mehr benutzt werden sollen, können diese über die CA-bezogene Certificate Revocation List (CRL) ungültig gemacht werden.
- Unter *eigene ID* und *ID der Gegenstelle* müssen jeweils die eindeutigen Stations-IDs der beiden VPN-Endpunkte angegeben werden. Sie können dazu beispielsweise die Hostnamen (FQDN) der Systeme oder Zeichenketten einsetzen. Werden Zeichenketten verwendet, sollte darauf geachtet werden, dass diese mit einem @-Zeichen beginnen. Bei Verwendung von Zertifikaten können die Felder leer bleiben, in diesem Fall wird der Name im Zertifikat als ID verwendet.
- Stellen Sie nun die Tunnelparameter wie *Kompression*, *Algorithmen* und *PFS* (Perfect Forwarding Secrecy) ein. Achten Sie darauf, dass Sie exakt die gleichen Einstellungen auf beiden Systemen vornehmen.
- Als Empfehlung für die Kopplung zweier Collax Security Gateway aktivieren Sie PFS. Benutzen Sie für IKE und ESP die Algorithmen „AES-256Bit“ und „SHA2-256Bit“.
- *Keylife* und *Lifetime* können Sie leer lassen. Hier werden die Defaultwerte verwendet.
- Normalerweise lassen Sie bei VPN das *Masquerading* deaktiviert. Wählen Sie unter *Erreichbare Netze* das vorhin angelegte Netz auf der anderen Seite des Tunnels aus. Unter *Lokale Netzwerke*

wählen Sie die lokalen Netze aus, die von der anderen Tunnelseite aus erreichbar sein sollen.
- Unter *Absenderadresse* wählen Sie die interne IP-Adresse des Collax Security Gateways aus, unter der er von der anderen Tunnelseite aus erreichbar sein wird.
- Vergessen Sie nicht, in den Benutzungsrichtlinien und in der Firewallmatrix für das neu angelegte Netz entsprechende Berechtigungen zu vergeben.
- Nach Aktivieren der Konfiguration können Sie unter *Überwachung/Auswertung – Status – IPsec* den gerade angelegten Tunnel sehen. Ist der Tunnel aufgebaut, wird dies als *Etabliert: Ja* angezeigt.

7.7 Schritt für Schritt: Aufbau eines VPN-Tunnels

- Das Einrichten eines Links zum Aufbau eines VPN-Tunnels zu einer Gegenstelle verläuft weitgehend analog zum Einrichten des Links für VPN-Einwahl.
- Legen Sie nun einen VPN-Link an, den Sie unter *Verbindungsaufbau* auf „Bei Bedarf“ oder „Immer“ einstellen, je nachdem, ob der Tunnel zeitweise oder permanent aufgebaut werden soll.
- Unter „IPsec-Gateway“ geben Sie die IP-Adresse oder den Hostnamen der Gegenstelle an. Sie können hier auch einen dynamischen Hostnamen verwenden.
- Die restlichen Werte stellen Sie analog wie im Abschnitt „Einwahllink für VPN“ ein.
- Nach Aktivieren der Konfiguration finden Sie diesen Link auch auf der IPsec-Statusseite. Wenn der Tunnel aufgebaut ist, wird der Link als *Etabliert: Ja* angezeigt.

7.8 Schritt für Schritt: Einwahllink für PPTP

- Über ein VPN werden zwei Netze gekoppelt. Daher müssen Sie zunächst unter *Netzwerk – Netze – Konfiguration* ein neues Netz mit dem IP-Bereich der anderen Seite anlegen.
- Nun legen Sie unter *Netzwerk – Links – Konfiguration* einen neuen Link für den PPTP-Tunnel an.
- Stellen Sie den *Typ* auf „PPTP-Server“.
- Möchten Sie zwei Netze verbinden, lassen Sie *ISP-Modus* deaktiviert. Dann können Sie unter *Erreichbare Netze* den IP-Bereich der Gegenseite auswählen.
- Wenn Sie nur einzelne Windows-Systeme einwählen lassen möchten, aktivieren Sie den *ISP-Modus*. Dann tragen Sie unter *IP-Adresse des Systems* eine IP-Adresse für den Collax Security Gateway ein. Unter *IP-Adressen für Zuweisung an Gegenstelle* können durch Leerzeichen getrennt ein oder mehrere IP-Adressen angegeben werden, die der Gegenseite zugewiesen werden. Eventuell ist es sinnvoll, in diesem Setup auch *DNS-Server an Gegenstelle übermitteln* zu aktivieren.
- Aktivieren Sie die *Komprimierung*, wenn die Gegenseite dies unterstützt.
- Wählen Sie eine möglichst hohe Anzahl von Bits für den *Verschlüsselungsalgorithmus*, etwa „MPPE 128Bit“.
- Um eine gewisse Sicherheit zu gewährleisten, aktivieren Sie *Auf Verschlüsselung bestehen*. So wird der Aufbau von unverschlüsselten Verbindungen abgelehnt.

7.9 Schritt für Schritt: L2TP über IPsec

L2TP ist ein weiteres Protokoll zum Aufbau von virtuellen privaten Netzen. Die Authentifizierung wird hier analog zu PPP mit den Verfahren PAP oder CHAP durchgeführt. L2TP selbst bietet jedoch keine Verschlüsselung. Um sie zu ermöglichen, kann es in Kombination mit IPsec eingesetzt werden.

In dieser Anleitung erfahren Sie, wie Sie den Collax Security Gateway als Einwahlserver für solche L2TP-über-IPsec-Verbindungen einrichten.

- Über ein VPN werden zwei Netze gekoppelt. Daher müssen Sie zunächst unter *Netzwerk – Netze – Konfiguration* ein neues Netz anlegen, aus dem die L2TP-Clients jeweils eine IP-Adresse zugewiesen bekommen.
- Möchten Sie über den *ISP-Modus* (Details weiter unten) einzelne Systeme einwählen lassen, müssen Sie nun einen Pool von IP-Adressen anlegen. Dies geschieht unter *Netzwerk – DHCP – IP-Adresspools*. Legen Sie dort einen neuen Pool an und stellen Sie den *Typ* auf *L2TP über IPsec*. Wählen Sie als *Netzwerk* das neu angelegte Netz und setzen Sie die erste und letzte IP-Adresse, die Sie vergeben möchten.
- Nun legen Sie unter *Netzwerk – Links – Konfiguration* einen neuen Link für den L2TP-Tunnel an.
- Stellen Sie den *Typ* auf „VPN“.
- Aktivieren Sie die Option *L2TP über IPsec verwenden*.
- Für die Einwahl mehrerer Clients aktivieren Sie den *ISP-Modus*. Unter *Folgenden Adresspool verwenden* wählen Sie den vorher angelegten IP-Adresspool aus. In diesem Setup ist es sinnvoll, auch *DNS-Server an Gegenstelle übermitteln* zu aktivieren.
- Die weitere Konfiguration der IPsec-Verbindung kann mit Zertifi-

katen oder Pre-Shared-Keys (PSK) erfolgen. Nehmen Sie dazu die Schritt-für-Schritt-Anleitung zur IPsec-Einwahl (S. 245) zu Hilfe.

- Für das korrekte Routing erzeugen Sie unter *Netzwerk – Links – Zuordnung* eine neue Zuordnung. Wählen Sie hierzu das L2TP-Netzwerk und die oben erzeugte L2TP-Verbindung aus.
- Die Einwahl über L2TP geschieht mit Login und Passwort. Wechseln Sie dazu nach *Benutzungsrichtlinien – Richtlinien – Gruppen*. Legen Sie hier eine neue Gruppe für die L2TP-Benutzer an (oder verwenden Sie alternativ eine geeignete vorhandene Gruppe).
- Aktivieren Sie für diese Gruppe unter dem Reiter *Berechtigungen* im Abschnitt *RAS* die Option *L2TP-Zugang über IPsec*.
- Selektieren Sie unter dem Reiter *Benutzer* diejenigen Benutzer, die sich über L2TP einwählen dürfen. Fügen Sie bei Bedarf weitere Benutzer hinzu.
- Über die *Benutzungsrichtlinien* und die *Firewallmatrix* können Sie einstellen, welche Berechtigungen das neu angelegte Netzwerk erhält.
- Nach Aktivieren der Konfiguration können sich Benutzer mit L2TP über IPsec auf den Collax Security Gateway einwählen.

8 SSL-VPN

(Diese Option befindet sich im Zusatzmodul *Collax SSL-VPN*)

8.1 Einführung

8.1.1 Allgemein

Die Bezeichnung SSL-VPN wird für die Beschreibung einer wachsenden Produkt-Kategorie verwendet, die viele verschiedene Technologien beinhaltet. Es gilt als Ziel des Einsatzes dieser Technologien, ein VPN zur Übertragung von privaten Daten durch ein öffentliches Netzwerk, das Internet als Beispiel, herzustellen. Aus dem zweiten Teil der Bezeichnung geht hervor, dass SSL als Transportmechanismus für die sichere Übertragung dieser Daten benutzt wird.

SSL-VPN kann als sinnvolle Ergänzung zu VPN mit IPsec angesehen werden. Dadurch, dass jeder gängige Browser bereits die Anforderungen erfüllt und keine weitere Software installiert werden muss, kann man praktisch von jedem Rechner und vielen mobilen Geräten auf bestimmte Anwendungen von jedem Ort der Welt zugreifen. Dabei legt der Administrator fest, welcher Benutzer einen Zugang für welche Anwendung bekommt.

8.1.2 Benutzung

Um diese Technologie anzuwenden, ist lediglich ein Standard-Web-Browser erforderlich. Es muss also keine zusätzliche Software installiert werden, da SSL zur Standardausstattung jedes Web-Browsers gehört. Im Unterschied zu VPNs mit dem IPsec-Standard, bei dem die Verbindung auf Netzwerk-Ebene hergestellt wird, verwendet eine Verbindung mittels SSL-VPN die Anwendungs-Schicht, den Application-Layer.

Durch die Gruppenverwaltung des Collax Server ist es sehr einfach möglich, den Zugang zu unterschiedlichen SSL-VPN-Ressourcen nur für ausgewählte Benutzergruppen zu gewähren. Benutzer loggen sich dafür auf der Collax Benutzerseite ein und starten eine definierte SSL-VPN-Ressource.

8.1.3 Sicherheit

Bei der Benutzung von SSL-VPN-Ressourcen müssen sicherheitsbezogene Gesichtspunkte unbedingt beachtet werden.

Die Ressourcen verbinden auf unkomplizierte Weise einen Datenstrom verschlüsselt in ein Netzwerk mit unternehmenskritischen Daten. Für den Zugang über die Collax Benutzerseite ist daher ein strenges Passwort zu definieren. Nachfolgend ist darauf zu achten, sobald die Ressourcen nicht mehr benutzt werden, dass der Benutzer sich ordnungsgemäß abmeldet.

8.2 GUI-Referenz: *SSL-VPN*

(Diese Option befindet sich im Zusatzmodul *Collax SSL-VPN*)

8.2.1 *SSL-Tunnel*

Mit der Definition eines SSL-Tunnel wird ein beliebiger Dienste-Port vom lokalen Rechner durch den Collax Server auf einen Zielrechner und Ziel-Port getunnelt. Wenn der SSL-Tunnel aufgebaut ist, kann die Zielanwendung von dem lokalen Rechner aus mit „localhost:Ziel-Port“ angesprochen werden.

8.2.1.1 *SSL-Tunnel auswählen*

(Dieser Dialog befindet sich unter *Netzwerk – SSL-VPN – SSL-Tunnel*)

Felder in diesem Formular

- *Name*: In dieser Tabellenspalte werden die Namen der definierten SSL-Tunnel angezeigt.
- *Kommentar*: In dieser Tabellenspalte eine weitere Information zum betreffenden SSL-Tunnel angezeigt.
- *Zielrechner*: Der eingetragene Zielrechner wird hier zur Kontrolle angezeigt.
- *Ziel-Port*: In dieser Spalte wird der eingegebene Port angezeigt.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion im Kontextmenü (rechter Mausklick oder Doppelklick) kann der ausgewählte SSL-Tunnel bearbeitet werden.
- *Löschen*: Mit dieser Aktion im Kontextmenü (rechter Mausklick) kann das gewählte Element gelöscht werden.

Aktionen für dieses Formular

- *Hinzufügen*: Mit dieser Aktion kann ein neuer SSL-Tunnel hinzugefügt werden.

8.2.1.2 *SSL-Tunnel bearbeiten*
Tab *Grundeinstellungen*
Felder in diesem Abschnitt

- *Name*: Hier wird der Name des SSL-Tunnels definiert, oder angezeigt.
- *Kommentar*: Für weitere Informationen zum SSL-Tunnel kann hier ein Kommentar angegeben werden.
- *Lokaler Port*: Hier wird der gewünschte lokale Netzwerk-Port angegeben. Er kann im Bereich von 1 bis 65535 definiert werden. Um eventuell auftretende Konflikte mit lokal gestarteten Diensten zu vermeiden, wird empfohlen, einen Port im Bereich zwischen 1024 und 65535 zu wählen.
- *Zielrechner*: Hier wird der gewünschte Zielrechner mit IP-Adresse oder Host-Namen angegeben.
- *Ziel-Port*: Hier wird der zu erreichende Dienste-Port des Zielrechners angegeben. Er kann im Bereich von 1 bis 65535 definiert

werden. Die Erreichbarkeit dieses Dienste-Ports und die Authentifizierung an diesem Dienst obliegt der Einstellungen auf dem Zielrechner.

Tab *Berechtigungen*
Felder in diesem Abschnitt

- *Zugriff für ...*: Die Benutzer und die Netzwerke der ausgewählten Gruppen haben authorisierten Zugriff auf den definierten SSL-Tunnel.

Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten des Formulars beenden, die Änderungen werden verworfen.
- *Speichern*: Bearbeiten des Formulars beenden, die Änderungen werden übernommen.

8.2.2 *Anwendungen*

Für einen Fernzugriff auf interne Rechner, können in diesem Formular die entsprechenden Anwendungen eingerichtet und den gewünschten Gruppen über die Benutzerseite zur Verfügung gestellt werden. Zu den unterstützten Protokollen zählt Remotedesktop, VNC und Citrix ICA.

8.2.2.1 *Anwendung auswählen*

(Dieser Dialog befindet sich unter *Netzwerk – SSL-VPN – Anwendungen*)

Felder in diesem Formular

- *Name*: In dieser Tabellenspalte werden die Namen der definierten Anwendung angezeigt.
- *Kommentar*: In dieser Tabellenspalte werden weitere Informationen der definierten Anwendung angezeigt.
- *Zielrechner*: Der eingetragene Zielrechner wird hier zur Kontrolle angezeigt.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion im Kontextmenü (rechter Mausklick oder Doppelklick) kann die ausgewählte Anwendung bearbeitet werden.
- *Löschen*: Mit dieser Aktion im Kontextmenü (rechter Mausklick) kann das gewählte Element gelöscht werden.

Aktionen für dieses Formular

- *Hinzufügen*: Mit dieser Aktion kann eine neue Anwendung hinzugefügt werden.

8.2.2.2 *Anwendung bearbeiten*

(Dieser Dialog befindet sich unter *Netzwerk – SSL-VPN – Anwendungen*)

Tab *Grundeinstellungen*
Felder in diesem Abschnitt

- *Name*: Hier wird der Name der Anwendung definiert, oder angezeigt.
- *Kommentar*: Für weitere Informationen zur Anwendung kann hier ein Kommentar angegeben werden.
- *Anwendung*: Aus dieser Liste kann hier die gewünschte Anwendung ausgewählt werden. Diese Anwendungen sind im System fest hinterlegt. Für eine optimale Fensterdarstellung werden für die gewählte Anwendung verschiedene Auflösungen zur Auswahl gestellt. Wird die Anwendung im Vollbild-Modus gestartet, kann dieser mit der Tastenkombination „Alt-Return“ wieder beendet werden.
- *Zielrechner*: Die gewählte Anwendung verbindet sich mit einem Zielrechner. Dieser wird hier mit IP-Adresse oder Host-Namen angegeben.
- *Ziel-Port*: Ist der Dienst des Zielrechners auf einem speziellen Port gebunden, muss hier dieser Ziel-Port angegeben werden. Läuft der Dienst des Zielrechners auf dem Standard-Port der Anwendung, kann dieses Feld leergelassen werden.

  Remote-Desktop-Verbindungen benutzen üblicherweise den Port 3389, VNC-Verbindungen werden über den Port 5900 hergestellt, bei Citrix ICA-Client-Verbindungen wird der Port 1494 benutzt.
- *SSO aktivieren*: Wenn diese Option aktiviert ist, werden die Login-

Daten des Webaccess-Benutzers automatisch an die Fernzugriffsanwendung übergeben. Der Benutzer muss sich daran nicht mehr authentifizieren. Diese Option kann für alle drei Protokolle benutzt werden.

- *Tastaturbelegung*: Je nach verwendeter Tastatur ist erforderlich, die Belegung anzupassen. Hier können die entsprechenden Ländereinstellungen der Tastaturbelegung für die Anwendung angepasst werden. Diese Option steht für RDP-Verbindungen zur Verfügung.
- *Passwort*: VNC-Verbindungen können mit einem Passwort geschützt sein. Hier kann dieses Passwort angegeben werden, um die VNC-Verbindung korrekt zu öffnen.

Tab *Grundeinstellungen*,Abschnitt *Auflösung*
Felder in diesem Abschnitt

- *Breite*: Statt Vollbild kann hier die Fensterbreite angegeben werden.
- *Höhe*: Statt Vollbild kann hier die Fensterhöhe angegeben werden.

Tab *Grundeinstellungen*, Abschnitt *Authentifizierung*

In diesem Abschnitt können Login-Informationen für RDP-Verbindungen hinterlegt werden, um ein automatisches Einloggen beim Start der SSL-VPN-Anwendung zu ermöglichen.

Felder in diesem Abschnitt

- *Benutzername*: Hier wird der Benutzername für die RPD-Verbindung angegeben. Die Voreinstellung übernimmt den Benutzer

des Web-Access. Die Einstellung kann auch leergelassen werden, dann erfolgt erfolgt die Authentifizierungsabfrage nach dem Aufbau der Verbindung.
- *Passwort*: Hier wird das Passwort für die RDP-Verbindung angegeben. Die Einstellung kann auch leergelassen werden, dann erfolgt erfolgt die Authentifizierungsabfrage nach dem Aufbau der Verbindung.
- *Domain*: Soll ein Domänen-Login (Active Directory oder NT-Domäne) erfolgen, kann hier die Domäne angegeben werden.

Tab *Grundeinstellungen*, Abschnitt Felder in diesem Abschnitt

- *Anwendung*: Name der Anwendung, die gestartet werden soll.
- *Breite*: Gibt die Fensterbreite für die Verbindung an.
- *Höhe*: Gibt die Fensterhöhe für die Verbindung an.

Tab *Native Optionen*, Abschnitt *Anzeige* Felder in diesem Abschnitt

- *Vollbild*: Hier wird angegeben, ob das RDP-Fenster als Vollbild geöffnet wird, oder in angegebenen Abmessungen.
- *Farben*: Hier wird die Farbtiefe für die Darstellung der RDP-Verbindung eingestellt. Weniger Farbtiefe verbessert die Übertragungsleistung.
- *Verbindungsleiste in Vollbildmodus anzeigen*: Hier kann eingestellt werden, ob der Benutzer die Möglichkeit haben soll, dass er das RDP-Fenster anhand der Verbindungsleiste am oberen Bildschirmrand verkleinern kann.
- *Konsolensitzung*: Stellt eine Verbindung mit der Sitzung zur Serververwaltung her.

Tab *Native Optionen*, Abschnitt *Lokale Ressourcen*
Felder in diesem Abschnitt

- *Remoteaudio*: Hier wird eingestellt, wo das Audio-Signal des Zielrechners ausgegeben werden soll.
- *Windows-Tastenkombinationen anwenden*: Gibt an, wo Windows-Tastenkombinationen ausgeführt werden sollen.
- *Lokalen Drucker verwenden*: Lokaler Drucker steht auf Zielrechner in der RDP-Verbindung zur Verfügung.
- *Lokale serielle Schnittstellen verwenden*: Lokale serielle Schnittstelle steht auf Zielrechner in der RDP-Verbindung zur Verfügung.
- *Lokale Smartcards verwenden*: Smart Cards stehen auf Zielrechner in der RDP-Verbindung zur Verfügung.
- *Lokale Laufwerke verwenden*: Lokal eingebundene Laufwerke stehen auf Zielrechner in der RDP-Verbindung zur Verfügung.
- *Lokale Zwischenablage verwenden*: Mit dieser Option können Inhalte von oder in die lokale Zwischenablage kopiert oder übertragen werden.
- *Credential Security Service Provider*: Hier kann CredSSP eingeschaltet werden.

Tab *Optionen*, Abschnitt *Leistung*

Diese Einstellungen dienen der Optimierung der Übertragungsrate.

Felder in diesem Abschnitt

- *Mauszeigereinstellung blockieren*: Mauszeigereinstellungen werden nicht übertragen.
- *Visuelle Stile blockieren*: Desktop-Design des Zielrechners wird nicht übertragen.

- *Hintergrundbild blockieren*: Hintergrundbild wird nicht übertragen.
- *Komprimierung anschalten*: Die Übertragung der Daten wird komprimiert.
- *Menü- und Fensteranimation blockieren*: Animationen werden nicht übertragen.
- *Dauerhafte Bitmapzwischenspeicherung*: Bitmaps werden dauerhaft zwischengespeichert.
- *Fensterinhalt beim Ziehen anzeigen*: Fensterinhalt wird bei Ziehen des Fensters übertragen und angezeigt.

Tab *Native Optionen*, Abschnitt *Programme*
Felder in diesem Abschnitt

- *Start-Programm*: Soll nur ein einzelnes Programm innerhalb einer Remote-Desktop-Verbindung benutzt werden dürfen, kann dieses hier angegeben werden. Dieses Programm wird direkt nach dem Aufbau der Verbindung gestartet. Bei Beenden dieses Start-Programmes wird auch die Remote-Desktop-Verbindung automatisch beendet.
- *In Ordner starten*: Hier kann ein Ordner mit Pfad angegeben werden, in dem das Startprogramm ausgeführt werden soll.
- *Fernanwendung*: Hier wird eine Fernanwendung (RemoteApp) angegeben, die durch den Terminalserverdienst definiert wurde.
- *Kommandozeile ausführen*: Hier wird angegeben, welche Kommandozeilenparameter der Fernanwendung übergeben werden sollen. Die Übergabe von Kommandozeilenparameter durch den RDP-Client muss auf dem Terminalserver erlaubt sein.
- *Ohne Benutzeroberfläche starten*: Mit dieser Option kann eingestellt werden, ob die Fernanwendung ohne Benutzeroberfläche des RDP-Client starten soll. Der RDP-Server oder Terminalserver muss diese Option unterstützen.

Tab *Berechtigungen*
Felder in diesem Abschnitt

- *Zugriff für ...*: Die Benutzer der ausgewählten Gruppen haben authorisierten Zugriff, um die definierte Anwendung zu benutzen. Hier sind auch Gruppen mit Netzwerken auszuwählen, aus denen die gewählten Benutzer Zugriff erhalten sollen.

Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten des Formulars beenden, die Änderungen werden verworfen.
- *Speichern*: Bearbeiten des Formulars beenden, die Änderungen werden übernommen.

8.2.3 *Web-Weiterleitungen*

Mit Hilfe von Web-Weiterleitungen können web-basierte Anwendungen im Intranet verschlüsselt angesteuert werden. In diesem Formular werden die entsprechenden Web-Weiterleitungen definiert und den gewünschten Gruppen über die Benutzerseite zur Verfügung gestellt.

8.2.3.1 *Web-Weiterleitung auswählen*

(Dieser Dialog befindet sich unter *Netzwerk – SSL-VPN – Web-Weiterleitungen*)

Bei *Getunnelte Web-Weiterleitung* wird die Weiterleitung durch einen SSL-Tunnel auf den angegebenen Server und auf das ange-

gebene Protokoll, http(80) oder https(443), erreicht. Hier ist es ausschließlich möglich, auf IP-Adresse / Namen und Port weiterzuleiten, nicht auf URLs.

Felder in diesem Formular

- *Name*: In dieser Tabellenspalte werden die Namen der definierten Web-Weiterleitung angezeigt.
- *Kommentar*: In dieser Tabellenspalte werden weitere Informationen der definierten Web-Weiterleitung angezeigt.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion im Kontextmenü (rechter Mausklick oder Doppelklick) kann die ausgewählte Web-Weiterleitung bearbeitet werden.
- *Löschen*: Mit dieser Aktion im Kontextmenü (rechter Mausklick) kann das gewählte Element gelöscht werden.

Aktionen für dieses Formular

- *Hinzufügen*: Mit dieser Aktion kann eine neue Web-Weiterleitung hinzugefügt werden.

8.2.3.2 *Web-Weiterleitung bearbeiten*

Tab *Grundeinstellungen*

Felder in diesem Abschnitt

- *Name*: Hier wird der Name der Web-Weiterleitung definiert, oder angezeigt.

- *Kommentar*: Für weitere Informationen zur Web-Weiterleitung kann hier ein Kommentar angegeben werden.
- *Ziel-URL*: Hier wird die Ziel-URL angegeben, deren Inhalt bei Aufruf der definierten Web-Weiterleitung wiedergegeben wird.

Tab *Berechtigungen*
Felder in diesem Abschnitt

- *Zugriff für ...*: Die Benutzer und Netzwerke der ausgewählten Gruppen haben authorisierten Zugriff, um die definierte Web-Weiterleitung zu benutzen.

Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten des Formulars beenden, die Änderungen werden verworfen.
- *Speichern*: Bearbeiten des Formulars beenden, die Änderungen werden übernommen.

8.2.4 *Reverse-Proxy*

(Dieser Dialog befindet sich unter *Netzwerk – SSL-VPN – Reverse-Proxy*)

Diese Web-Weiterleitungen werden per *Reverse-Proxy* auf die angegebene Ziel-URL umgeschrieben.

8.2.4.1 *Reverse-Proxy-Weiterleitung wählen*

Felder in diesem Formular

- *Name*: Kennzeichnung der Weiterleitung wird angezeigt.
- *Kommentar*: Enthält weitere Informationen.
- *Interne URL*: Zeigt die URL an, auf die weitergeleitet wird.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Öffnet den Dialog zum Bearbeiten der gewählten Reverse-Proxy-Weiterleitung.
- *Löschen*: Löscht den ausgewählten Eintrag.

Aktionen für dieses Formular

- *Weiterleitung hinzufügen*: Öffnet den Dialog um eine neue Weiterleitung hinzuzufügen.

8.2.4.2 *Reverse-Proxy-Weiterleitung bearbeiten*

Tab *Grundeinstellungen*

Felder in diesem Abschnitt

- *Name*: Hier wird der Name angezeigt oder angegeben.
- *Kommentar*: Weitere Informationen können hier hinterlegt werden.
- *Interne URL*: Die interne vollständige URL wird mit der Angabe des Protokolls http oder https angegeben.

Tab *Berechtigungen*, Abschnitt *Berechtigungen*
Felder in diesem Abschnitt

- *Zugriff für ...*: Benutzer und Netzwerke der gewählten Gruppen erhalten im Collax Webaccess Zugriff auf die Reverse-Proxy-Weiterleitung.

Aktionen für dieses Formular

- *Abbrechen*: Schließt den Dialog, die Änderungen werden verworfen.
- *Speichern*: Schließt den Dialog, die Änderungen werden gespeichert.

9 Hardwarekonfiguration

9.1 Grundlagen

In diesem Kapitel werden Schnittstellen des Collax Security Gateways behandelt, über die Verbindungen zur Außenwelt hergestellt werden können. Zu diesem Zweck können serielle Schnittstellen, ISDN-Karten und Netzwerkschnittstellen konfiguriert werden.

Das Linux-System zählt Schnittstellen beginnend mit Null. Daher wird bei seriellen Schnitstellen „COM 1“ als „ttyS0“, bei mehreren ISDN- oder Netzwerkkarten die jeweils erste Schnittstelle mit Null bezeichnet: „isdn0“ bzw. „eth0“.

9.1.1 Netzwerk-Bridges

Durch eine Bridge werden mehrere Ethernet-Ports zu einer Art Switch zusammengeschaltet. Dadurch erscheinen sie nach außen wie ein einziges Netzwerksegment (eine so genannte „Broadcast-Domain“). Dabei werden nur diejenigen Pakete auf einen Port der Bridge kopiert, deren Ziel-Adresse an diesem Port erreichbar ist.

Eine Bridge lernt die MAC-Adressen innerhalb eines jeden Teilnetzes, indem sie diese intern in einer Tabelle speichert. Anhand dieser Tabelle werden die Datenpakete in das entsprechende Ziel-Netzwerksegment weitergeleitet. Wird ein System auf ein anderes Netzwerksegment umgesteckt, dauert es eine gewisse Zeit, bis die Bridge den Umzug erkennt und die Adresse „neu lernt“.

Durch die Verwendung von Switches und Bridges kann nicht grundsätzlich ausgeschlossen werden, dass eine Verbindungsleitung

redundant geschaltet wird, so dass eine Schleife entsteht. Dies führt zu duplizierten Datenpaketen und damit zu Fehlfunktionen und Geschwindigkeitseinbußen im Netzwerk. Um dennoch solche Redundanz für eine höhere Funktionssicherheit nutzen zu können, wird das „Spanning Tree Protocol“ (STP) benötigt.

Bei aktiviertem STP ermitteln innerhalb einer Netzwerkumgebung alle Bridges abhängig von ihrer Priorität und der jeweiligen Mac-Adresse eine „Root-Bridge“. Diese Root-Bridge prüft nun, welche weiteren Bridges vorhanden sind und ob es redundante Pfade gibt. Letztere werden eliminiert, indem die entsprechenden Ports an den betroffenen Bridges deaktiviert werden. Auf diese Weise wird ist ein störungsfreier Betrieb des Netzwerks möglich.

Im laufenden Betrieb werden von der Root-Bridge aus Pakete zur Überwachung ins Netz geschickt, die von untergeordneten Bridges dupliziert werden. Dadurch können Störungen bzw. Änderungen im Netzwerk erkannt werden. In solchen Fällen findet eine Reorganisation des Netzes statt. In dieser Zeit sind im gesamten Netz nur noch STP-Pakete zulässig, jeder andere Netzwerkverkehr wird unterbunden.

Im Collax Security Gateway können mehrere Netzwerkschnittstellen zu einer Bridge zusammengefasst werden. Zwischen diesen Schnittstellen verhält sich der Collax Security Gateway transparant, d. h., es werden keine Firewallregeln angewendet.

9.1.2 VLAN-Routing

Mit VLANs (Virtual Local Area Networks) lässt sich ein lokales Netzwerk in mehrere virtuelle, voneinander getrennte Netze unterteilen. VLAN ist teilweise als IEEE 802.1q standardisiert.

Damit VLAN eingesetzt werden kann, muss ein Switch mit ent-

sprechender Unterstützung vorhanden sein. Jedem VLAN wird eine eigene Nummer zugewiesen, die den Headern der Datenpakete hinzugefügt wird. Derart markierte Datenpakete werden von einem entsprechenden Switch nur auf die Ports weitergeleitet, die dem VLAN zugeordnet sind. Ist am Zielport ein Endgerät angeschlossen, wird die VLAN-Markierung entfernt. Die Teilnehmer eines VLANs sind so an einem eigenen, virtuellen Switch angeschlossen. Broadcast-Pakete werden vom Switch nicht in andere VLANs weitergeleitet.

Um mehrere Switches miteinander zu verbinden, wird am Switch der Uplink-Port als „Trunked Port“ eingestellt. Auf solchen Ports werden ausgehenden Paketen entsprechende VLAN-Markierungen hinzugefügt. Werden derart markierte Pakete über einen Switch ohne VLAN-Unterstützung an ein Endgerät zugestellt, enthält der Paketheader noch die VLAN-Information. Ein Endgerät ohne VLAN-Unterstützung erkennt das Paket als ungültig und verwirft es.

Der Collax Security Gateway unterstützt VLAN-Technik. Mit einem entsprechenden Switch können mehrere virtuelle Netzwerksegmente angesteuert werden.

9.1.3 Schnittstellen-Bonding

Durch das Zusammenschalten von mehreren Ethernet-Verbindungen können Zuverlässigkeit und Durchsatz des Systems erhöht werden. Dazu ist jedoch die Unterstützung durch den eingesetzten Switch erforderlich. Der Switch muss „Bonding“, „EtherChannel“ bzw. „Trunking“ unterstützen.

Je nach Switch und Einstellung werden entweder mehrere Leitungen gebündelt verwendet („Load Balancing“), oder es wird nur eine genutzt, die dann im Fehlerfall umgeschaltet wird („Failover“).

Folgende Einstellungen werden vom Collax Security Gateway unterstützt:

- *Round Robin* – Es wird immer die nächste verfügbare physikalische Schnittstelle benutzt. Diese Arbeitsweise erreicht den höchsten Durchsatz, erfordert aber die Unterstützung des Switches.
- *XOR* – Jede Gegenstelle wird immer über dieselbe physikalische Schnittstelle angesprochen. Einige Switches verwenden dieses Verfahren, es wird aber nur ein geringer Durchsatz erreicht. Es ist nicht erforderlich, zur Kommunikation mit diesen Switches auch XOR zu benutzen, jedoch ist auch für diese Arbeitsweise die Unterstützung des Switches erforderlich.
- *Active Backup* – Diese Arbeitsweise erfordert keine Unterstützung durch die Gegenstelle. Es wird aber kein erhöhter Durchsatz, sondern nur erhöhte Zuverlässigkeit erreicht. Zu jedem Zeitpunkt ist nur ein Link aktiv. Zusätzlich zur MII-Link-Status-Überwachung kann in diesem Modus auch eine aktive Überprüfung des Links durch ARP-Anfragen erfolgen.
- *Broadcast* – In dieser Arbeitsweise werden alle Pakete auf allen Schnittstellen gesendet. Dieser Modus zielt auf Fehlertoleranz, kann aber auch z. B. für den Einsatz eines IDS nützlich sein.

9.2 GUI-Referenz: *Hardware*

(Dieser Dialog befindet sich unter *Hardware – Systemgeräte & Komponenten*)

In diesen Dialogen werden die Hardware-Ressourcen des Systems angezeigt. Einzelne Komponenten können bearbeitet werden.

Einige der angezeigten Ressourcen können nicht verändert werden, z. B. die vorhandenen Ethernet-Ports. Alle Hardwarekomponenten werden beim Starten des Systems erkannt und in die Oberfläche eingefügt. Dies gilt auch für „hotplug-fähige“ Komponenten wie USB-ISDN-Adapter.

Andere Ressourcen wie etwa VLANs oder MSNs müssen hingegen manuell eingerichtet werden. Hier ist keine automatische Erkennung möglich.

9.2.1 *Systemgeräte & Komponenten*

In diesem Dialog werden alle relevanten Komponenten des Systems angezeigt.

9.2.1.1 Tab *System*, Abschnitt *CPU*

In diesem Abschnitt werden Informationen über den Prozessor des Systems angezeigt.

Felder in diesem Abschnitt

- *Hersteller*: Hier wird der Code des CPU-Herstellers angezeigt.
- *Modell*: Hier wird die Modellbezeichnung der CPU angezeigt.
- *Geschwindigkeit*: Hier wird die ermittelte Taktrate der CPU angezeigt.
- *Cachegröße*: Hier wird Größe des Cachespeichers der CPU angezeigt.

9.2.1.2 Tab *RAM*, Abschnitt *RAM*

Felder in diesem Abschnitt

- *RAM gesamt*: Hier wird die Gesamtgröße des erkannten Hauptspeichers (RAM) angezeigt.
- *RAM frei*: Hier wird die Größe des aktuell verfügbaren freien Hauptspeichers angezeigt.
- *Swap gesamt*: Hier wird die Gesamtgröße des Auslagerungsspeichers angezeigt.
- *Swap frei*: Hier wird die Größe des aktuell verfügbaren freien Auslagerungsspeichers angezeigt.

9.2.1.3 Tab *Serielle Schnittstellen*

Spalten in der Tabelle

- *Art*: Die Art der Schnittstelle.
- *Name*: Der Name der Schnittstelle.
- *Kommentar*: Ein Kommentar zu dieser Schnittstelle.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird die Konfiguration der seriellen Schnittstelle bearbeitet.

9.2.1.4 Tab *ISDN*, Abschnitt *Karten*

Spalten in der Tabelle

- *Art*: Die Art der Schnittstelle.
- *Name*: Der Name der Schnittstelle.
- *Kommentar*: Ein Kommentar zu dieser Schnittstelle.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird die Konfiguration einer ISDN-Karte geändert. Dabei kann für jede ISDN-Karte die Betriebsart (Standleitung, EDSS1 (Euro-ISDN), 1TR6 oder US NI1) einzeln eingestellt werden.

9.2.1.5 Tab *ISDN*, Abschnitt *Rufnummern (MSN)*

Hier werden die Rufnummern (MSNs) verwaltet und einzelnen ISDN-Karten zugeordnet.

Spalten in der Tabelle

- *Art*: Die Art der Rufnummer.
- *Name*: Der Name der Rufnummer.
- *Kommentar*: Ein Kommentar zu dieser Rufnummer.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion kann eine Rufnummer geändert und ihre Zuordnung zu einer ISDN-Karte angepasst werden.
- *Löschen*: Mit dieser Aktion wird eine Rufnummer gelöscht. Dies ist nur möglich, wenn die Rufnummer im System nicht verwendet wird.

Aktionen für diesen Abschnitt

- *MSN anlegen*: Mit dieser Aktion wird eine neue MSN eingetragen.

9.2.1.6 Tab *IPMI*

IPMI ist eine integrierte Management-Technik, mit der die Stromversorgung und der Status eines Systems kontrolliert werden können. Damit IPMI auf einem Collax Security Gateway genutzt werden kann, muss entsprechende Hardware vorhanden sein.

Spalten in der Tabelle

- *Art*: Die Art der Schnittstelle.
- *Name*: Der Name der Schnittstelle.
- *Kommentar*: Ein Kommentar zu dieser Schnittstelle.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird die Funktion der Schnittstelle festgelegt.

9.2.2 *Serielle Schnittstelle bearbeiten*

(Dieser Dialog befindet sich unter *Hardware – Systemgeräte & Komponenten*)

In diesem Dialog werden die seriellen Schnittstellen konfiguriert.

Um die Änderungen vollständig zu aktivieren, muss ein Reboot des Systems durchgeführt werden.

9.2.2.1 Felder in diesem Dialog

- *Schnittstelle*: In diesem Feld wird der Name der Schnittstelle angezeigt. Die interne Nummerierung beginnt bei Null, d. h., die Schnittstelle *ttyS0* entspricht *COM 1*.
- *Verwendung*: Hier wird eingestellt, zu welchem Zweck die Schnittstelle verwendet werden soll.

  Bei der Auswahl von *serielle Konsole* wird auf der seriellen Schnittstelle eine Konsole bereitgestellt. Mit Hilfe eines Terminalprogramms kann dann auch ohne Netzwerk oder Bildschirm / Tastatur auf das System zugegriffen werden.

  Mit der Einstellung *Modem* müssen verschiedene Modem-Parameter gesetzt werden. Dann steht ein analoges Modem zur Einwahl bzw. zum Faxbetrieb zur Verfügung.

  Mit der Einstellung *Sonstiges* wird keine Konfiguration der Schnittstelle durchgeführt. Die Schnittstelle steht dann für andere Programme zur Verfügung, die die Konfiguration vornehmen (z. B. für den USV-Dienst oder einen Zeitsignalempfänger).

  Hinweis: Wird keine serielle Schnittstelle auf *Sonstiges* eingestellt, kann bei der USV-Konfiguration usw. keine Schnittstelle ausgewählt werden.
- *Übertragungsrate*: Hier wird die Übertragungsgeschwindigkeit für

die Schnittstelle eingestellt. Wird an diesem Port ein Modem angeschlossen, sollte hier ein Wert eingestellt werden, der mindestens so hoch wie die maximale Übertragungsrate des Modems ist. Normalerweise wird ein Wert eingestellt, der doppelt so groß ist, damit der Datenpuffer im Modem immer gefüllt ist.

- *Bits*: Hier wird die Anzahl der zur Datenübertragung genutzten Bits angegeben. Üblich ist der Wert 8, spezielle Gegenstellen könnten den Wert 7 benötigen.
- *Parität*: Hier wird angegeben, ob *Gerade* (even) oder *Ungerade Parität* (odd parity) genutzt wird. Dabei handelt es sich um einfache Verfahren zur Erkennung von Übertragungsfehlern. Abhängig von der Einstellung wird im Paritätsbit signalisiert, ob die Anzahl der auf logisch Eins gesetzten Datenbits gerade oder ungerade ist. Mit der Einstellung *Keine* wird auf das Paritätsbit verzichtet.
- *Analoge Rufnummer*: Hier wird die Rufnummer des Analogmodems angegeben. Diese Rufnummer wird beispielsweise vom Fax-Dienst übermittelt. Die Nummer sollte im Format *+49xxxxxxxxx* eingegeben werden.
- *Allgemeine Amtsholung benutzen*: Diese Option muss aktiviert werden, wenn die allgemeine Einstellung zur Amtsholung für dieses Modem verwendet werden soll.
- *Wahlverfahren*: Hier wird eingestellt, ob das Modem mit dem Mehrfrequenzverfahren oder mit Impulswahl arbeiten soll.

9.2.3 *ISDN-Karte*

(Dieser Dialog befindet sich unter *Hardware – Systemgeräte & Komponenten*)

In diesem Dialog werden die Funktionsart und die Parameter für die ISDN-Karte(n) festgelegt.

Hinweis: Beim Anschluss eines USB-ISDN-Adapters wird die Schnittstelle erst nach einem Neustart des Systems in der Konfiguration sichtbar.

9.2.3.1 Felder in diesem Dialog

- *Karte*: In diesem Feld wird der Name der Schnittstelle angezeigt.
- *ISDN-Anschluss-Modus*: Hier wird eingestellt, ob die ISDN-Karte an einem Mehrgeräteanschluss (Multi-Device) oder an einem Anlagenanschluss (Point-To-Point) betrieben wird.
- *D-Kanal-Protokoll*: Hier wird das D-Kanal-Protokoll eingestellt. Damit kann die Karte auf Standleitungsbetrieb (keine Verwendung des D-Kanals), EDSS1 (Euro-ISDN), 1TR6 oder US NI1 konfiguriert werden.
- *Amtsholung*: Hier wird die Kennziffer angegeben, die zur Amtsholung verwendet werden soll. Diese Ziffer wird jeder zu wählenden Rufnummer vorangestellt.
- *B-Kanal auf Standleitungsbetrieb setzen*: Durch das Aktivieren dieser Option wird die ISDN-Karte auf Standleitungsbetrieb eingestellt. Dabei findet keine Signalisierung auf dem D-Kanal mehr statt. Der D-Kanal muss entsprechend eingestellt werden.
- *Kanäle*: Hier kann die Anzahl der zu bündelnden Kanäle im Standleitungsbetrieb festgelegt werden.

9.2.4 *MSN*

(Dieser Dialog befindet sich unter *Hardware – Systemgeräte & Komponenten*)

In diesem Dialog werden die MSNs (ISDN-Rufnummern) verwaltet.

9.2.4.1 Felder in diesem Dialog

- *MSN*: Hier wird die Rufnummer angegeben, auf die die ISDN-Karte reagieren soll. Dabei muss die Nummer angegeben werden, die tatsächlich signalisiert wird. Hinter einer Nebenstellenanlage ist dies meist die interne Rufnummer (Durchwahl). Ohne Anlage sollte die Rufnummer ohne Vorwahl angegeben werden.
- *ISDN-Karte*: Hier wird die ISDN-Karte ausgewählt, mit der die Rufnummer verknüpft wird.

9.2.5 *IPMI-Einstellungen bearbeiten*

(Dieser Dialog befindet sich unter *Hardware – Systemgeräte & Komponenten*)

9.2.5.1 Felder in diesem Abschnitt

- *Medientyp*: Der Medientyp ist die Art des Kanals, sichtbar ist derzeit nur 802.3 LAN. Weitere mögliche Kanäle bei IPMI wären etwa „SMBus“ oder „Seriell“.
- *Protokoll*: Als IPMI-Protokoll wird „IPMB-1.0“ verwendet.
- *LAN-Zugriff erlauben*: Mit dieser Option wird der Zugriff auf den LAN-Kanal aktiviert.

- *Schnittstelle*: Ein LAN-Kanal benötigt eine definierte Schnittstelle für den IPMI-Zugriff. Diese wird hier ausgewählt.
- *IP-Adresse*: Hier wird die IP-Adresse konfiguriert, die für den LAN-Zugriff verwendet werden soll. Diese IP-Adresse darf nicht anderweitig verwendet werden.
- *Netzmaske*: Hier wird die zugehörige Netzmaske eingegeben.
- *MAC-Adresse des Gateways*: Soll aus entfernten Netzen der Zugriff über IPMI möglich sein, muss hier die MAC-Adresse des Gateways angegeben werden.
- *IP-Adresse des Gateways*: In diesem Feld wird entsprechend die IP-Adresse des Gateways eingegeben.
- *SNMP-Community*: In diesem Feld wird der „Community String“ für die Authentifizierung bei SNMP angegeben.
- *Berechtigte Gruppen*: Alle aktivierten Gruppen erhalten Zugriff auf IPMI.

9.2.6 *Ethernet-Protokolle*

In diesem Formular können verschiedene Einstellungen vorgenommen oder bestimmte Dienste zu Ethernet aktiviert werden. Die Einstellungen werden generell gesetzt und sind somit unabhängig von den verwendeten lokalen Schnittstellen.

9.2.6.1 Abschnitt *STP/RSTP*

Felder in diesem Abschnitt

- *Verwende RSTP anstelle von STP*: Diese Option aktiviert einen Dienst für das Rapid Spanning Tree Protocol. Als Weiterentwicklung von STP beschleunigt das RSTP einerseits die Umstellung

auf alternative Netzwerkpfade. Zudem bleiben zum Zeitpunkt der Umstellung alle noch funktionierenden Pfade aktiv.

9.2.6.2 Abschnitt *GVRP*

Felder in diesem Abschnitt

- *VLANs mit GVRP registrieren*: Mit dem Generic Attribute Registration Protocol für VLAN (GVRP) können VLAN-Ports vom Server direkt am angeschlossenen Switch generiert werden. Der Switch muss dieses Protokoll unterstützen.

9.2.6.3 Abschnitt *LLDP*

Felder in diesem Abschnitt

- *LLDP aktivieren*: Hier kann das Link Layer Discovery Protocol (LLDP) aktiviert werden. Dieses Protokoll sendet und empfängt Informationen über die direkte Netzwerknachbarschaft.

Abschnitt *Andere Protokolle* ...

Felder in diesem Abschnitt

- *Aktiviere CDP (Cisco)*: Aktiviert CDP (Cisco).
- *Aktiviere FDP (Foundry)*: Aktiviert FDP (Foundry).
- *Aktiviere SONMP (Bay/Nortel/SynOptics)*: Aktiviert SONMP (Bay/Nortel/SynOptics).
- *Aktiviere EDP (Extreme)*: Aktiviert EDP (Extreme).

9.2.6.4 Aktionen für dieses Formular

- *Abbrechen*: Diese Aktion beendet den Dialog. Die Änderungen werden verworfen.
- *Speichern*: Diese Aktion beendet den Dialog. Die Änderungen werden gespeichert.

9.2.7 *Netzwerkschnittstellen*

(Dieser Dialog befindet sich unter *Systembetrieb – Hardware – Netzwerkschnittstellen*)

9.2.7.1 GUI-Referenz: *Netzwerkschnittstellen*

Spalten in der Tabelle

- *Art*: Die Art der Schnittstelle.
- *Name*: Der Name der Schnittstelle.
- *Kommentar*: Ein Kommentar zu dieser Schnittstelle.
- *Verwendung*: Anzeige, wo das Ethernet-Device verwendet wird.
- *Vorhanden*: Zeigt an, ob das Gerät vorhanden ist.

Aktionen für jeden Tabelleneintrag

- *Bridge bearbeiten*: Mit dieser Aktion wird die Konfiguration der Bridge bearbeitet.
- *Bridge löschen*: Mit dieser Aktion wird eine angelegte Bridge-Konfiguration gelöscht.
- *MacVLAN bearbeiten*: Hier kann ein auf MAC-Adressen bezogenes VLAN bearbeitet werden.

- *MacVLAN löschen*: Hier kann ein auf MAC-Adressen bezogenes VLAN gelöscht werden.
- *VLAN bearbeiten*: Mit dieser Aktion wird das gewählte VLAN bearbeitet.
- *VLAN löschen*: Mit dieser Aktion wird die Konfiguration des VLAN-Ports gelöscht. Dies ist nur möglich, wenn der VLAN-Port in keinem Link und in keiner Bridge mehr verwendet wird.
- *Bonding bearbeiten*: Mit dieser Aktion können die Einstellungen einer Bonding-Konfiguration bearbeitet werden.
- *Bonding löschen*: Mit dieser Aktion wird eine angelegte Bonding-Konfiguration gelöscht.
- *Ethernet bearbeiten*: Mit dieser Aktion können Einstellungen für die Ethernet-Schnittstellen vorgenommen werden.
- *Bridge hinzufügen*: Mit dieser Aktion können mehrere Ethernet-Schnittstellen zu einer Bridge zusammengeschaltet werden.

  Auch VLAN-Ports können mit in die Bridge aufgenommen werden. Dies sollte jedoch nicht mit zwei VLAN-Ports geschehen, die auf demselben physikalischen Ethernet-Port liegen. Dadurch würde das VLAN unbrauchbar.
- *VLAN-Port hinzufügen*: Mit dieser Aktion wird eine Ethernet-Schnittstelle für ein virtuelles LAN (VLAN) eingerichtet. Diese Schnittstelle kann danach nicht mehr für andere Zwecke benutzt werden. Es können jedoch mehrere VLAN-Ports auf derselben Ethernet-Schnittstelle eingerichtet werden.

  Hinweis: Die übrige Netzwerkinfrastruktur muss ebenfalls VLAN-fähig sein. Der auf dem Switch genutzte Ethernet-Port muss entsprechend konfiguriert sein.

  VLANs haben nichts (oder fast nichts) mit virtuellen Interfaces zu tun. Soll eine weitere IP-Adresse für den Collax Security Gateway vergeben werden, muss dazu nur ein weiterer Link auf dem Ethernet-Port angelegt werden.
- *MacVLAN-Port hinzufügen*:

- *Port-Bonding hinzufügen*: Mit dieser Aktion können mehrere Ethernet-Schnittstellen gebündelt werden, um dadurch gesteigerten Durchsatz und höhere Zuverlässigkeit zu erreichen.

9.2.7.2 *Ethernet-Einstellungen*

(Dieser Dialog befindet sich unter *Hardware – Netzwerkschnittstellen*)

In diesem Dialog wird eine einzelner Ethernet-Port bearbeitet.

Felder in diesem Dialog

- *Name*: Hier wird der Name des Ethernet-Ports angezeigt.
- *Jumbo-Frames verwenden*: Um Protokoll-Overhead zu minimieren kann es sinnvoll sein, größere Paketlängen als 1518 Bytes im Netzwerkverkehr auf dieser Schnittstelle zu verwenden. Voraussetzung für die Verwendung von Jumbo Frames, ist die Fähigkeit beteiligter Netzwerkgeräte ebenso mit Jumbo Frames umgehen zu können.
- *Kein GVRP auf diesem Port*: Verhindert, dass GVRP auf dem Port benutzt wird.

9.2.7.3 *VLAN-Port bearbeiten*

(Dieser Dialog befindet sich unter *Hardware – Netzwerkschnittstellen*)

In diesem Dialog wird ein einzelner VLAN-Port bearbeitet.

Auf einem physikalischen Ethernet-Port können ein oder mehrere VLANs konfiguriert werden. Das VLAN erscheint dann als virtueller

Port in der Hardwarekonfiguration und an allen Stellen, an denen ein Ethernet-Port ausgewählt werden kann (zum Beispiel in der Link-Konfiguration).

Ein physikalischer Ethernet-Port, auf dem ein VLAN konfiguriert wurde, kann nicht mehr für andere Zwecke verwendet werden. Er kann beispielsweise nicht mehr in eine Bridge integriert werden.

Felder in diesem Dialog

- *Ethernet-Port*: Hier wird die Netzwerkschnittstelle ausgewählt.
- *Jumbo-Frames verwenden*: Um Protokoll-Overhead zu minimieren kann es sinnvoll sein, größere Paketlängen als 1518 Bytes im Netzwerkverkehr auf dieser Schnittstelle zu verwenden. Voraussetzung für die Verwendung von Jumbo Frames, ist die Fähigkeit beteiligter Netzwerkgeräte ebenso mit Jumbo Frames umgehen zu können.
- *VLAN-Tag*: In diesem Feld wird das VLAN-Tag angegeben.

9.2.7.4 *MacVLAN-Port hinzufügen*

(Dieser Dialog befindet sich unter *Hardware – Ethernet*)

In diesem Dialog wird ein einzelner VLAN-Port hinzugefügt, dem eine Mac-Adresse zugewiesen werden kann.

Ein physikalischer Ethernet-Port, auf dem ein VLAN konfiguriert wurde, kann nicht mehr für andere Zwecke verwendet werden. Er kann beispielsweise nicht mehr in eine Bridge integriert werden.

Felder in diesem Dialog

- *Ethernet-Port*: Hier wird die Netzwerkschnittstelle ausgewählt.
- *Jumbo-Frames verwenden*: Um Protokoll-Overhead im Gigabitnetzwerk zu minimieren kann es sinnvoll sein, größere Paketlängen als 1518 Bytes im Netzwerkverkehr auf dieser Schnittstelle zu verwenden. Voraussetzung für die Verwendung von Jumbo Frames, ist die Fähigkeit beteiligter Netzwerkgeräte ebenso mit Jumbo Frames umgehen zu können.
- *MAC-Adresse*: Hier wird eine MAC-Adresse eingetragen, die von keinem anderen Gerät verwendet wird.

Aktionen für dieses Formular

- *Zufällige MAC*: Mit dieser Aktion wird eine MAC-Adresse generiert und in das Feld *MAC-Adresse* eingetragen.

9.2.7.5 *MacVLAN-Port bearbeiten*

Felder in diesem Formular

- *Ethernet-Port*: Hier wird die Netzwerkschnittstelle angezeigt.
- *Jumbo-Frames verwenden*: Um Protokoll-Overhead im Gigabitnetzwerk zu minimieren kann es sinnvoll sein, größere Paketlängen als 1518 Bytes im Netzwerkverkehr auf dieser Schnittstelle zu verwenden. Voraussetzung für die Verwendung von Jumbo Frames, ist die Fähigkeit beteiligter Netzwerkgeräte ebenso mit Jumbo Frames umgehen zu können.
- *MAC-Adresse*: Hier wird eine MAC-Adresse eingetragen, die von keinem anderen Gerät verwendet wird.

Aktionen für dieses Formular

- *Zufällige MAC*: Mit dieser Aktion wird eine MAC-Adresse generiert und in das Feld *MAC-Adresse* eingetragen.

Aktionen für dieses Formular

- *Abbrechen*: Diese Aktion führt zurück zur Übersicht. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten der Mac-VLAN-Konfiguration beenden. Die Änderungen werden gespeichert.

9.2.7.6 *Bridge bearbeiten*

(Dieser Dialog befindet sich unter *Hardware – Netzwerkschnittstellen*)

In diesem Dialog wird die Konfiguration einer Ethernet-Bridge vorgenommen.

Felder in diesem Dialog

- *Name*: Hier wird der Name der Bridge angezeigt. Wird eine neue Bridge angelegt, ist das Feld leer. Der Name wird automatisch erzeugt.
- *Kommentar*: Hier wird eine erweiterte Information eingefügt.
- *STP-Protokoll aktivieren*: Das „Spanning Tree Protokoll“ STP dient dazu, bei Konfigurationen mit mehreren Bridges (oder Switches) immer nur einen Datenpfad zwischen zwei Geräten aufzubauen. Mittels STP werden daher Routingschleifen verhindert.

  Wenn zwischen einzelnen Geräten mehrere Datenpfade kon-

figuriert werden, kann STP die Ausfallsicherheit erhöhen. STP aktiviert im Fehlerfall einen redundanten Pfad.

STP kann deaktiviert werden, wenn es keine anderen Bridges im Netzwerk oder keine redundanten Pfade gibt.

- *Priorität*: Wird STP verwendet, kann hier die Priorität der Bridge festgelegt werden. Gibt es mehrere Bridges im Netzwerk, wird die Bridge mit dem niedrigsten Prioritätswert zur „root"-Bridge. Bei mehreren Bridges mit gleicher Priorität wird zusätzlich die MAC-Adresse mit herangezogen, um die Root-Bridge festzulegen.
- *Ageing-Zeit (s)*: Dieser Parameter gibt an, wie lange die MAC-Adressen gespeichert werden. Diese Zeit wird nach dem letzten empfangenen Paket eines Systems heruntergezählt.

  Wird ein System an einen anderen Port der Bridge angeschlossen, dauert es mindestens so lange wie angegeben, bis es im Netzwerk von anderen Systemen erreicht werden kann.
- *Ethernet-Ports*: In dieser Liste werden die Ethernet-Ports für die Bridge aktiviert. Es stehen nur solche Ports zur Auswahl, die entweder schon für die Bridge verwendet oder bisher nicht konfiguriert wurden.

9.2.7.7 *Gebündelte Ethernet-Schnittstellen bearbeiten*

(Dieser Dialog befindet sich unter *Hardware – Netzwerkschnittstellen*)

Durch das Zusammenschalten („Bundling") von Ethernet-Leitungen können Zuverlässigkeit und Durchsatz erhöht werden. Dazu ist Unterstützung durch den eingesetzten Switch erforderlich. Der Switch muss „EtherChannel" oder „Trunking" unterstützen.

Felder in diesem Dialog

- *Name*: Der Name der Schnittstelle.
- *Arbeitsweise*: Hier wird die Arbeitsweise der gebündelten Schnittstellen festgelegt. Sämtliche Konfigurationen benutzen die MII-Link-Status-Überwachung.

  Möglich sind:

  Active Backup – Diese Arbeitsweise erfordert keine Unterstützung der Gegenstelle, erreicht aber keinen erhöhten Durchsatz, sondern nur erhöhte Zuverlässigkeit. Zu jedem Zeitpunkt ist nur ein Link aktiv. Zusätzlich zur MII-Link-Status-Überwachung kann in diesem Modus auch eine aktive Überprüfung des Links durch ARP-Anfragen erfolgen.

  Broadcast – In dieser Arbeitsweise werden alle Pakete auf allen Schnittstellen gesendet. Dieser Modus zielt auf Fehlertoleranz, kann aber auch z. B. für den Einsatz eines IDS nützlich sein.

  Round Robin – Es wird immer die nächste verfügbare physikalische Schnittstelle benutzt, um Pakete zu versenden. Diese Arbeitsweise ermöglicht Load Balancing und Ausfallsicherheit, erfordert aber die Unterstützung des Switches.

  XOR – Jede Gegenstelle wird immer über dieselbe physikalische Schnittstelle angesprochen. Dies ist die Arbeitsweise einiger Switches, es wird aber nur geringerer Durchsatz erreicht. Es ist nicht erforderlich, zur Kommunikation mit diesen Switches auch XOR zu benutzen, jedoch ist auch für diese Arbeitsweise die Unterstützung des Switches erforderlich.

  LACP (802.3ad) – Innerhalb der IEEE-Spezifizierung stellt das Link Aggregation Control Protocol (LACP) eine Methode zur Verfügung, um die Bündelung von mehreren physischen Anschlüssen zusammen zu kontrollieren und einen einzelnen logischen Kanal zu bilden. LACP erlaubt einem Netzwerkgerät eine automatische

Aushandlung zur Bündelung von Anschlüssen indem es LACP Pakete an die Gegenstelle (direkt angeschlossenes Gerät, das auch LACP durchführt) sendet.

Adaptive Transmit Load Balancing – Ankommender Verkehr wird nur auf der aktiven Schnittstelle entgegengenommen, abgehender Netzwerkverkehr wird gemäß der gegenwärtigen Last auf jede Schnittstelle verteilt. Diese Option erfordert keine spezielle Switch-Unterstützung.

Adaptive Load Balancing – umfasst Adaptive Transmit Load Balancing inklusive Receive Load Balancing (RLB) für den IPV4-Verkehr. Diese Option erfordert keinen speziellen Switch-Unterstützung. Der Lastausgleich beim eingehenden Netzwerkverkehr wird durch die ARP-Verhandlung erreicht.

- *Verteilung nach*: Wählt die Sende-Richtlinie, um die korrekte Schnittstelle auszuwählen. Diese Option gilt für die XOR- und LACP-Arbeitsweise. Folgende Einstellungswerte sind möglich:

  Schicht 2 (MAC-Adressen) – Dieser Algorithmus lenkt den Netzwerkverkehr zu einer bestimmten Gegenstelle immer über dieselbe Schnittstelle.

  Schicht 2 und 3 (MAC- und IP-Adressen) – Arbeitet wie die Schicht 2-Verteilung, sorgt aber zusätzlich für ausgeglichenere Verteilung des Netzwerkverkehrs. Das trifft gerade in Umgebungen zu, in denen ein IP-Gateway eingesetzt wird.

  Schicht 3 und 4 (MAC-, IP-Adressen und UDP/TCP) – Diese Richtlinie betrachtet höhere Protokollschichten um die Sendeschnittstellen auszuwählen. Fragmentierte Pakete werden ignoriert.
- *ARP-Überprüfung*: Hier wird die aktive Überprüfung des Links durch ARP-Anfragen aktiviert.
- *Überprüfungsintervall (in ms)*: Hier wird das Intervall festgelegt, in dem eine Überprüfung stattfinden soll. Die Zeit wird in Millisekunden (ms) angegeben, der kleinste gültige Wert ist 100.

- *Up-Verzögerung (in ms)*: Hier wird die Verzögerung eingestellt, die eingehalten werden soll, bevor eine Schnittstelle wieder verfügbar gemacht wird. Die Zeit wird in Millisekunden (ms) angegeben.
- *Down-Verzögerung (in ms)*: Hier wird die Verzögerung eingestellt die eingehalten werden soll, bevor eine Schnittstelle heruntergefahren wird. Die Zeit wird in Millisekunden (ms) angegeben.
- *Carrier-Auswertung des Treibers benutzen*: Gibt an, ob miimon MII- oder ETHTOOL-ioctls statt netif_carrier_ok () verwenden werden soll, um den Status zu bestimmen.
- *IP*: Hier wird die IP-Adresse angegeben, die für die ARP-Anfragen benutzt wird. Werden für diese IP-Adresse keine ARP-Anfragen beantwortet, wird der Link als fehlerhaft eingestuft.
- *Ethernet-Ports*: In dieser Liste werden die Ethernet-Schnittstellen ausgewählt, die gebündelt werden. Es werden nur die Ports angezeigt, die unkonfiguriert sind.
- *Primärer Port*: Hier wird die primäre Schnittstelle angegeben. Diese wird bevorzugt verwendet. Erst wenn diese Schnittstelle gestört ist, wird auf eine der anderen umgeschaltet. Sobald die primäre Schnittstelle wieder verfügbar ist, wird auf diese zurückgeschaltet.

  Ein Anwendungsbeispiel ist die Failover-Bündelung einer 1000 MBit- und einer oder mehrerer 100 MBit-Schnittstellen, bei der bevorzugt die 1000 MBit-Schnittstelle benutzt werden soll.

9.2.7.8 *Gebündelte Ethernet-Schnittstellen bearbeiten*

(Dieser Dialog befindet sich unter *Hardware – Netzwerkschnittstellen*)

Hier werden die Einstellungen für gebündelte Ethernetports fest-

gelegt. Diese können verwendet werden, um Zuverlässigkeit und Durchsatz zu erhöhen. Unter Umständen ist die Unterstützung des Switches erforderlich (genannt EtherChannel oder Trunking). Weitere Informationen finden sich unter „Arbeitsweise“.

Eine (unvollständige) Liste von Switches mit der erforderlichen Unterstützung:

Felder in diesem Dialog

- *Name*: Der Name der Schnittstelle.
- *Arbeitsweise*: Hier wird die Arbeitsweise der gebündelten Schnittstellen festgelegt. Sämtliche Arten benutzen MII-Link-Status-Überwachung.

  Möglich sind:

  Active Backup – Diese Arbeitsweise erfordert keine Unterstützung der Gegenstelle, erreicht aber keinen erhöhten Durchsatz, sondern nur erhöhte Zuverlässigkeit. Zu jedem Zeitpunkt ist nur ein Link aktiv. Zusätzlich zur MII-Link-Status-Überwachung kann in diesem Modus auch eine aktive Überprüfung des Links durch ARP-Anfragen erfolgen.

  Broadcast – In dieser Arbeitsweise werden alle Pakete auf allen Schnittstellen gesendet. Dieser Modus zielt auf Fehlertoleranz, kann aber auch z. B. für den Einsatz eines IDS nützlich sein.

  Round Robin – Es wird immer die nächste verfügbare physikalische Schnittstelle benutzt, um Pakete zu versenden. Diese Arbeitsweise ermöglicht Load Balancing und Ausfallsicherheit, erfordert aber die Unterstützung des Switches.

  XOR – Jede Gegenstelle wird immer über dieselbe physikalische Schnittstelle angesprochen. Dies ist die Arbeitsweise einiger Switches, es wird aber nur geringerer Durchsatz erreicht. Es ist nicht erforderlich, zur Kommunikation mit diesen Switches auch

XOR zu benutzen, jedoch ist auch für diese Arbeitsweise die Unterstützung des Switches erforderlich.

LACP (802.3ad) – Innerhalb der IEEE Spezifizierung stellt das Link Aggregation Control Protocol (LACP) eine Methode zur Verfügung, die Bündelung von mehreren physischen Anschlüssen zusammen zu kontrollieren, um einen einzelnen logischen Kanal zu bilden. LACP erlaubt einem Netzwerkgerät eine automatische Aushandlung zur Bündelung von Anschlüssen indem es LACP Pakete an die Gegenstelle (direkt angeschlossenes Gerät, das auch LACP durchführt).

Adaptive Transmit Load Balancing – Ankommender Verkehr wird nur auf der aktiven Schnittstelle entgegengenommen, abgehender Netzwerkverkehr wird gemäß der gegenwärtigen Last auf jede Schnittstelle verteilt. jeder Sklave. Diese Option erfordert keine spezielle Switch-Unterstützung.

Adaptive Load Balancing – umfasst Adaptive Transmit Load Balancing inklusive Receive Load Balancing (RLB) für den IPV4-Verkehr. Diese Option erfordert keinen speziellen Switch-Unterstützung. Der Lastausgleich beim eingehenden Netzwerkverkehr wird durch die ARP-Verhandlung erreicht.

- *Verteilung nach*: Wählt die Sende-Richtlinie, um die korrekte Schnittstelle auszuwählen. Diese Option gilt für die XOR- und LACP-Arbeitsweise. Folgende Einstellungswerte sind möglich:

  Schicht 2 (MAC-Adressen) – Dieser Algorithmus lenkt den Netzwerkverkehr zu einer bestimmten Gegenstelle immer über dieselbe Schnittstelle.

  Schicht 2 und 3 (MAC- und IP-Adressen) – Arbeitet wie die Schicht 2-Verteilung, sorgt aber zusätzlich für ausgeglichenere Verteilung des Netzwerkverkehrs. Das trifft gerade in Umgebungen zu, in denen ein IP-Gateways eingesetzt werden.

  Schicht 3 und 4 (MAC-, IP-Adressen und UDP/TCP) – Diese

Richtlinie betrachtet höhere Protokollschichten um die Sendeschnittstellen auszuwählen. Fragmentierte Pakete werden ignoriert.

- *ARP-Überprüfung*: Hier wird die aktive Überprüfung des Links durch ARP-Anfragen aktiviert.
- *Überprüfungsintervall (in ms)*: Das Intervall, in dem die Überprüfung stattfinden soll (in ms). Der kleinste gültige Wert ist 100.
- *IP*: Die IP-Adresse, die für die ARP-Anfragen benutzt wird. Falls für diese IP-Adresse keine ARP-Anfragen beantwortet werden, wird der Link als unbenutzbar eingestuft.
- *Ethernet-Ports*: In dieser Liste wird ausgewählt, welche Ethernet-Ports gebündelt werden. Es werden nur diejenigen Ports angezeigt, die ansonsten unbenutzt sind.
- *Up-Verzögerung (in ms)*: Hier wird die Verzögerung eingestellt die eingehalten werden soll, bevor eine Schnittstelle wieder verfügbar gemacht wird. Die Zeit wird in Millisekunden (ms) angegeben.
- *Down-Verzögerung (in ms)*: Hier wird die Verzögerung eingestellt die eingehalten werden soll, bevor eine Schnittstelle heruntergefahren wird. Die Zeit wird in Millisekunden (ms) angegeben.
- *Carrier-Auswertung des Treibers benutzen*: Gibt an, ob miimon MII- oder ETHTOOL-ioctls statt netif_carrier_ok () verwenden werden soll, um den Status zu bestimmen.
- *Primärer Port*: Hier wird die primäre Schnittstelle angegeben. Wenn diese Schnittstelle gestört ist, werden alternative Schnittstellen benutzt, und dies auch nur solange, bis die primäre Schnittstelle wieder funktionsfähig ist. Ein Anwendungsbeispiel wäre die Failover-Bündelung einer 1000 MBit- und einer/mehrerer 100 MBit-Schnittstellen, bei der bevorzugt die 1000 MBit-Schnittstelle benutzt werden soll.

9.3 GUI-Referenz: *iSCSI Initiator*

(Dieser Dialog befindet sich unter *iSCSI – iSCSI Initiator*)

9.3.1 Abschnitt *Modus*

9.3.1.1 Felder in diesem Abschnitt

- *Aktiviert*: Mit dieser Option wird der iSCSI Initiator aktiviert. Die Aktivierung ist erforderlich, um iSCSI-Knoten ins System einzubinden.
- *Initiatorname*: Hier wird der eindeutig identifizierbare (IQN) Name des Initiator angegeben.

9.3.2 Abschnitt *iSCSI Discovery*

9.3.2.1 Felder in diesem Abschnitt

- *Authentifizierung*: Um iSCSI Targets zu ermitteln, kann es aus Sicherheitsgründen erforderlich sein, dass dafür Authentifizierungsdaten anzugeben sind. Die Option kann aktiviert werden, falls ein iSCSI discovery login erforderlich ist.
- *Benutzer*: Hier wird der Benutzer-Login für die Authentifizierung angegeben.
- *Passwort*: Hier wird das Passwort zum Benutzer-Login angegeben.

9.3.3 Aktionen für dieses Formular

- *Abbrechen*: Bearbeitung des Formulars beenden, die Einstellungen werden verworfen.
- *Speichern*: Bearbeitung des Formulars beenden, die Einstellungen werden gespeichert.

9.4 GUI-Referenz: *iSCSI-Knoten*

(Dieser Dialog befindet sich unter *iSCSI Initiator – iSCSI-Knoten*)

9.4.1 *iSCSI-Knoten wählen*

9.4.1.1 Spalten in der Tabelle

- *IP-Adresse*: Hier wird die IP-Adresse des definierten iSCSI-Knoten angezeigt.
- *Port*: Zeigt den TCP/IP-Port des iSCSI-Knoten.
- *iSCSI Target*: Hier wird der Name des iSCSI Target angezeigt. Üblicherweise ist dies ein iSCSI Qualified Name (IQN).
- *Info*: Zeigt Details des definierten iSCSI-Knoten.
- *Clustered*: Zeigt an, ob die iSCSI-Festplatte im Cluster-Verbund verwaltet wird.

9.4.1.2 Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion öffnet sich ein Dialog, um den iSCSI-Knoten zu bearbeiten.
- *Löschen*: Mit dieser Aktion wird der gewählte iSCSI-Knoten gelöscht.

9.4.1.3 Aktionen für dieses Formular

- *Target discovery*: Die Aktion ermittelt iSCSI Targets und weitere Informationen, um iSCSI-Knoten hinzuzufügen.
- *Hinzufügen*: Diese Aktion öffnet einen Dialog, um manuell iSCSI-Knoten hinzuzufügen.

9.4.2 *iSCSI-Knoten bearbeiten*

9.4.2.1 Tab *Grundeinstellungen*, Abschnitt *iSCSI-Knoten*
Felder in diesem Abschnitt

- *Name*: Hier wird der iSCSI Qualified Name angegeben oder angezeigt.
- *Info*: Hier können Details zum iSCSI-Knoten eingetragen werden.
- *IP-Adresse*: Hier wird die IP-Adresse eingegeben, unter der der iSCSI-Knoten angesteuert werden kann.
- *Port*: Hier wird der TCP/IP-Port angegeben, über den mit dem iSCSI-Knoten kommuniziert wird.

9.4.2.2 Tab *Grundeinstellungen*, Abschnitt *Authentifizierung*

Felder in diesem Abschnitt

- *iSCSI Initiator gegenüber iSCSI Target*: Diese Option muss aktiviert werden, wenn der iSCSI Initiator sich am iSCSI Target authentifizieren muss.
- *Benutzer*: Hier wird das CHAP-Login angegeben.
- *Passwort*: Hier wird das Passwort für die Authentifizierung angegeben.
- *iSCSI Target gegenüber iSCSI Initiator*: Diese Option muss aktiviert werden, wenn das iSCSI Target sich am iSCSI Initiator authentifizieren muss.
- *Benutzer*: Hier wird das CHAP-Login angegeben.
- *Passwort*: Hier wird das Passwort für die Authentifizierung angegeben.

9.4.2.3 Tab *Optionen*, Abschnitt *Name*

Felder in diesem Abschnitt

- *iSCSI Target verwendet ungültigen Namen*: Wird die Namens-Konvention auf Seite des iSCSI Target nicht eingehalten und kein iSCSI Qualified Name (IQN) verwendet, kann diese Option aktiviert werden, um dennoch eine korrekte Funktionsweise zu ermöglichen.

9.4.2.4 Aktionen für dieses Formular

- *Abbrechen*: Beenden der Bearbeitung, die Einstellungen werden verworfen.

- *Speichern*: Beenden der Bearbeitung, die Einstellungen werden gespeichert.

9.4.3 : *iSCSI Target Discovery*

9.4.3.1 Abschnitt *Einstellungen*
Felder in diesem Abschnitt

- *IP-Adresse*: Hier wird die IP-Adresse angegeben, auf der iSCSI Targets ermittelt werden sollen.
- *Port*: Hier wird der TCP/IP-Port angegeben, über den Informationen von iSCSI Targets zur Verfügung gestellt werden.

Aktionen für diesen Abschnitt

- *Prüfen*: Mit der Ausführung dieser Aktion wird versucht, iSCSI Targets über die angegebene IP-Adresse zu ermitteln.

9.4.3.2 Aktionen für dieses Formular

- *Importieren*: Die ermittelten Daten von iSCSI Targets können mit dieser Aktion für die weitere Bearbeitung übernommen werden.
- *Zurück*: Beenden der Bearbeitung.

9.5 GUI-Referenz: *iSCSI-Knoten Status*

(Dieser Dialog befindet sich unter *Überwachung/Auswertung – Status – iSCSI-Knoten*)

9.5.1 *iSCSI-Knoten - Status*

In diesem Dialog kann der Status von eingebundenen iSCSI-Knoten eingesehen werden.

9.5.1.1 Spalten in der Tabelle

- *IP-Adresse*: Hier wird die IP-Adresse des definierten iSCSI-Knoten angezeigt.
- *Port*: Zeigt den TCP/IP-Port des iSCSI-Knoten.
- *iSCSI Target*: Hier wird der Name des iSCSI Target angezeigt. Üblicherweise ist dies ein iSCSI Qualified Name (IQN).
- *Aktion*: Hier wird angezeigt, ob der iSCSI-Knoten im System eingebunden ist. Je nach Status, kann an dieser Stelle die entsprechende Aktion ausgeführt werden.

9.5.1.2 Aktionen für jeden Tabelleneintrag

- *Login*: Mit dieser Aktion kann der gewählte iSCSI-Knoten ins System eingebunden werden.
- *Logout*: Mit dieser Aktion kann der gewählte iSCSI-Knoten vom System gelöst werden.

- *Detail*: Mit dieser Aktion können Detailinformationen angezeigt werden.

9.5.2 *iSCSI-Knoten*

9.5.2.1 Tab *Info*
Felder in diesem Abschnitt

- *iSCSI Target*: Hier wird der vollständige Name des iSCSI-Targets angezeigt.
- *IP-Adresse*: Zeigt die IP-Adresse des Target-Hosts.
- *Port*: Zeigt den Port, über den der iSCSI-Knoten erreichbar ist.
- *Verbindung*: Zeigt an, ob der iSCSI-Knoten verbunden ist.

9.5.2.2 Tab *Info*, Abschnitt *Status*
Felder in diesem Abschnitt

- : In diesem Feld wird der detaillierte Status über den iSCSI-Knoten angezeigt.

9.5.2.3 Tab *Konfiguration*
Felder in diesem Abschnitt

- : Zeigt die detaillierte Konfiguration des iSCSI-Knoten an.

9.5.2.4 Aktionen für dieses Formular

- *Zurück*: Führt zurück zur Übersicht.

10 Firewall

10.1 Einführung

Eine Firewall sichert einzelne Netzwerksegmente gegeneinander ab. Die Firewall kontrolliert, welche Verbindungen zwischen den einzelnen Netzen zulässig sind, und lehnt verbotene Verbindungen ab.

Die einfachste Form einer Firewall ist der Paketfilter. Dieser entscheidet bei jedem IP-Paket anhand der Quell- und Zieladressen und der jeweiligen Ports, ob das Paket passieren darf oder nicht. Ein solcher Paketfilter muss in jedem der Netze, die er voneinander trennen soll, eine Netzwerkschnittstelle haben. Sind mehrere Netze auf einem Switch zusammengelegt, kann die Firewall leicht umgangen werden.

Im Collax Security Gateway ist eine leistungsfähige Firewall enthalten, die „Stateful Inspection“ (zustandsgesteuerte Filterung) unterstützt. Bei dieser Technik wird im Unterschied zu einem reinen Paketfilter für jede Verbindung im Speicher ein Eintrag erzeugt. So ist für jede aktive Verbindung der Status bekannt, und IP-Pakete können einer laufenden Verbindung zugeordnet bzw. fehlerhafte und gefälschte Pakete erkannt werden.

Ein weiterer Vorteil von Stateful Inspection ist die Unterstützung komplexer Protokolle, die mit getrennten Kontroll- und Datenverbindungen arbeiten, wie etwa FTP oder SIP. Die Firewall ist hier in der Lage, anhand des Kontrollkanals eine neu eröffnete Datenverbindung einer Verbindung zuzuordnen und passieren zu lassen.

In einer Firewall lassen sich Berechtigungen bis auf die Ebene eines einzelnen Hosts setzen. Meist werden jedoch zusammenhän-

gende IP-Bereiche zu Netzen zusammengefasst, etwa *LocalNet* oder *Internet*.

Pakete können auf zwei verschiedene Arten abgelehnt werden. Im einfachsten Fall verwirft die Firewall sie einfach. Alternativ kann zusätzlich eine Ablehnung in Form eines ICMP-Pakets mit dem Inhalt „Host unreachable – Zielhost nicht erreichbar“ verschickt werden. Im ersten Fall wird der IP-Stack des Absendersystems das Paket erneut versenden, bis sein Timeout abgelaufen ist. Im zweiten Fall erfolgt umgehend eine Rückmeldung, dass dieser Dienst nicht verfügbar ist.

Ein Paketfilter bzw. eine Stateful-Inspection-Firewall schaut nur in die IP-Header der Pakete und nimmt anhand der Quell- und Ziel-Portadressen eine Unterscheidung vor. Eine Ausnahme bildet die Behandlung spezieller Protokolle wie FTP oder SIP, bei denen das eigentliche Protokoll teilweise mitgelesen wird. Eine Analyse der Nutzdaten findet jedoch nicht statt. Ein „Application Layer Filter“ geht einen Schritt weiter: Hier wird der konkrete Inhalt des IP-Pakets untersucht. Bei einem HTTP-Proxy etwa wird der HTTP-Header gelesen und ausgewertet. Dann wird der Proxy seinerseits eine vollständig neue Anfrage generieren und an den ursprünglich adressierten Host senden. Dessen Antwort schickt der Proxy an den ursprünglichen Absender weiter, ebenfalls in einem neuen, wohlgeformten Paket. Durch diese Technik ist es unmöglich, den Zielport 80 für andere Dienste als HTTP zu missbrauchen, da der Proxy nur HTTP versteht und andere Pakete verwirft. Collax Security Gateway unterstützt solche Application Layer Filter für die oft genutzten Dienste HTTP und SMTP. Beim Application Layer Filter ist es zusätzlich möglich, konkrete Inhalte zu filtern, etwa zur Überprüfung auf Viren.

10.1.1 Firewall im Collax Security Gateway

Bei der im Collax Security Gateway eingesetzten Paketfilter-Firewall werden drei unterschiedliche Filter verwendet: Der INPUT-Filter bestimmt, welche Dienste auf dem Collax Security Gateway selbst erreichbar sind. Der FORWARD-Filter kontrolliert, welche Verbindungen von einem Netzwerk in ein anderes zulässig sind, und die OUTPUT-Regel gewährt dem Collax Security Gateway selbst Zugriff auf andere Systeme.

Diese Dreiteilung findet sich in der Konfiguration des Collax Security Gateways wieder. Zugriffe auf Dienste im Collax Security Gateway (INPUT-Regel) werden über die Netzwerkgruppen (S. 45) gewährt. Zugriffe von einem Netz bzw. einer Netzwerkgruppe in eine andere (FORWARD-Regel) werden in der *Firewallmatrix* eingestellt. Ausgehender Datenverkehr von Diensten innerhalb des Collax Security Gateways (OUTPUT-Regel) ist grundsätzlich immer erlaubt und kann nicht eingeschränkt werden.

In der *Firewallmatrix* werden pro Dienst die Regeln für den Datenverkehr zwischen Netzwerkgruppen konfiguriert. Über die Bildung von Untergruppen lässt sich der Verkehr bis hinunter zu einzelnen Systemen kontrollieren. Statt einzelner Netze für jeden Host können auch mehrere Hosts in den *Netzwerkgruppen* zu einer Netzwerkgruppe zusammengefasst werden. Die Matrix selbst ist dabei eine visuelle Darstellung der Firewall. Jede angelegte Netzwerkgruppe taucht einmal pro Spalte und einmal pro Zeile auf. Die jeweilige Regel findet sich im Kreuzungspunkt von der Zeile mit dem Quellnetz und der Spalte des Zielnetzes. Die Matrix ist also in der Form „von Zeile nach Spalte“ aufgebaut. Um festzulegen welche Regel gültig ist, kann am Kreuzungspunkt festgelegt werden, welcher *Dienst*, beispielsweise HTTP oder HBCI, erlaubt oder verboten wird.

Die einzelnen Regeln werden in der Firewallmatrix durch bestimm-

te Zeichen symbolisiert: „Verwerfen“ durch ein schwarzes Loch bzw. einen schwarzen Klecks, „Ablehnen“ durch ein Durchfahrt-Verboten-Symbol, „Erlauben“ entsprechend durch ein Vorfahrtssymbol. Ist für einen bestimmten Dienst, wie HTTP oder DNS, eine Regel manuell gesetzt, wird das entsprechende Symbol durch zwei farbige Klammern ergänzt.

In der Matrix wird ein wirkungsvoller Vererbungsmechanismus eingesetzt. Existiert für eine Verbindung keine explizit gesetzte Regel, wird implizit die Regel des übergeordneten Dienstes bzw. der übergeordneten Netze angewendet. So lassen sich einfach Vorgaberegeln für größere Netzbereiche festlegen („Default-Policies“).

Implizit gesetzte Regeln werden in der Matrix durch graue Symbole dargestellt, während explizit von Hand gesetzte Regeln farbig dargestellt sind. Durch Rechtsklick mit der Maus wird zu jedem Punkt in der Matrix ein Fenster mit einem Hilfetext geöffnet. In diesem wird auch erläutert, wie die Vererbung für diese Regel zustande kommt. Die Vererbungstiefe von Regeln wird durch Färbung jeglicher betroffener Schnittpunkte dargestellt, wenn Schnittpunkte mit dem Mauszeiger überfahren werden. Die maximale Vererbung wird durch die Netzwerkgruppe Internet verursacht.

Durch die Vererbung kann es in seltenen Fällen vorkommen, dass für einen Punkt in der Matrix mehrere widersprüchliche Regeln vererbt werden könnten. An solchen Punkten wird dann ein Warndreieick angezeigt und die Policy „Verwerfen“ angewendet. Durch Setzen einer expliziten Regel an dieser Stelle wird der Konflikt aufgelöst.

In der Voreinstellung wird die Policy „Verwerfen“ auf alle Verbindungen angewendet. Damit Datenverkehr möglich wird, müssen in der Matrix die gewünschten Verbindungen erlaubt werden.

Für jede explizit gesetzte Regel kann die Protokollierung aktiviert werden. Dabei wird dann für jeden (versuchten) Verbindungsaufbau

ein Eintrag im Log erzeugt. Dies kann große Datenmengen erzeugen, so dass diese Option mit Bedacht genutzt werden sollte. In den meisten Fällen ist es nicht notwendig, erlaubte Verbindungen zu protokollieren. Vielmehr macht es Sinn, die durch die Default-Policy vom lokalen Netz kommenden abgelehnten Pakete zu protokollieren, um schnell zu sehen, ob eine Verbindung an der Firewall scheitert.

10.1.2 DMZ

Als DMZ („Demilitarisierte Zone“) wird ein Konzept bezeichnet, welches die Sicherheit beim Betrieb von Systemen erhöht, die aus dem Internet erreichbar sind. Würde man ein solches System, beispielsweise den Webserver mit dem Onlineshop, im lokalen Netz platzieren, könnte ein Angreifer bei erfolgreichem Einbruch umgehend auf die benachbarten Systeme im lokalen Netz zugreifen. Eine Firewall kann in diesem Fall nicht schützen, da der interne Netzwerkverkehr direkt über den Switch abgewickelt wird.

Beim Aufbau einer DMZ wird ein separater Netzwerkstrang eingerichtet, der an einer Netzwerkschnittstelle der Firewall angeschlossen wird und keinerlei direkte Verbindung mit dem lokalen Netz hat. Jeglicher Datenverkehr zwischen lokalem Netz und Server in der DMZ muss durch die Firewall laufen. Hier können entsprechende Regeln gesetzt werden, die die möglichen Zugriffe einschränken.

Üblicherweise wird jeder Verbindungsaufbau aus der DMZ ins lokale Netzwerk geblockt. Ein Angreifer, der über den Webshop in den Server einbricht, kann dann nicht direkt auf Systeme im lokalen Netz zugreifen. Werden in der DMZ mehrere Server betrieben, ist hier natürlich ein Zugriff ohne Firewallschutz möglich. Das Konzept der DMZ kann allerdings auf jeden Server angewendet werden, eine entsprechende Anzahl von Netzwerkschnittstellen in der Firewall

vorausgesetzt. Über die Verwendung von VLAN (S. 268) können die notwendigen Schnittstellen virtualisiert werden.

Das Konzept der DMZ kann natürlich auch genutzt werden, um einzelne Netzwerkbereiche in einem Unternehmen voneinander abzugrenzen, z. B. Entwicklung und Produktion. Auch der Betrieb eines Wireless-LAN-Access-Points ist auf einem eigenen Netzwerksegment anzuraten.

10.2 Schritt für Schritt: Firewallregeln setzen

In der Firewallmatrix regeln Sie den Datenverkehr zwischen einzelnen Netzwerken. Wichtig ist, dass die einzelnen Netze auf verschiedenen Netzwerkschnittstellen erreichbar sind, so dass die IP-Pakete den Collax Security Gateway durchlaufen müssen.

In den folgenden Schritten wird zunächst die Default-Policy für abgehende Verbindungen aus dem lokalen Netz angepasst.

- Wechseln Sie in die Firewallmatrix unter *Netzwerk – Firewall – Firewallmatrix*.
- Prüfen Sie, dass unter *Dienst* die Einstellung *Alle* ausgewählt ist. Dies ist die Default-Policy für alle Dienste.
- In der Vorgabeeinstellung sind alle Felder der Matrix mit grauen Symbolen „Verwerfen“ belegt. Das Symbol zeigt ein „Schwarzes Loch“.
- Gehen Sie in die Zeile „LocalNet“ und klicken Sie auf das Symbol im Kreuzungspunkt mit der Spalte „Internet“.
- Eine neue Seite öffnet sich, dort sollte „Dienst any von LocalNet nach Internet“ angezeigt werden.
- Unter *Regel* wählen Sie nun *Ablehnen* aus. Dadurch werden die Pakete verworfen, und es wird eine ICMP-Warnung generiert.

Aus dem lokalen Netz heraus erfolgt so eine umgehende Rückmeldung, dass der betreffende Dienst gesperrt ist.

- Aktivieren Sie *Protokollieren*, um alle gesperrten Verbindungsversuche in der Logdatei aufzuzeichnen. Darüber ist es später möglich, einzelne Verbindungsversuche im Logfile nachzuvollziehen und ggf. zu erlauben.
- Speichern Sie die Seite. Sie gelangen zurück zur Firewallmatrix.
- In der Matrix ist im Kreuzungspunkt nun ein farbiges Symbol „Durchfahrt verboten“ sichtbar. Dies ist eine explizite Regel. Rechts davon ist das gleiche Symbol in grauer Darstellung zu sehen. Hierbei handelt es sich um implizite Regeln durch Vererbung, da die Netze in den rechten Spalten alle Teilnetze des Internets sind. Fahren Sie mit der Maus auf die Kreuzungspunkte, ohne zu klicken. Nach kurzer Zeit klappen Fenster auf, die genaue Informationen zu den jeweiligen Verbindungen enthalten.

Nun soll beispielhaft der Dienst HTTP aus dem lokalen Netz erlaubt werden. Diese Schritte müssen für jeden gewünschten Dienst durchgeführt werden.

Es empfiehlt sich nicht, die Default-Policy auf „Erlauben“ zu setzen, da dadurch auch unerwünschte Dienste aus dem lokalen Netz ins Internet gelangen können, etwa Filesharing oder sog. Würmer.

- Um für das Protokoll HTTP eine Berechtigung zu setzen, wählen Sie unter *Dienst* die Einstellung *HTTP* aus.
- Sie sehen nun eine untergeordnete Ansicht der Matrix, für die Verbindungen aus dem lokalen Netz ist die vorhin eingestellte Policy „Ablehnen“ sichtbar. Sie ist in grau dargestellt, weil sie nicht explizit für HTTP gesetzt wurde, sondern von der Regel für alle Dienste auf diese Schicht der Matrix vererbt wurde. Kontrollieren Sie dies durch Überfahren des Kreuzungspunkts mit dem Mauszeiger.
- Klicken Sie auf den Kreuzungspunkt der Zeile *LocalNet* und der Spalte *Internet*.

- Eine neue Seite öffnet sich, dort sollte „Dienst http von LocalNet nach Internet“ angezeigt werden.
- Wählen Sie hier als *Regel* die Einstellung *Erlauben* aus. Sie können über *Protokollieren* die HTTP-Zugriffe aus dem lokalen Netz in der Logdatei aufzeichnen, dies kann jedoch eine große Anzahl Einträge erzeugen und ist normalerweise nicht erforderlich.
- Speichern Sie die Seite.
- Sie gelangen wieder zurück zur Matrix. Dort ist für die Verbindung ein farbiges Vorfahrt-Symbol für Ihre Einstellung sichtbar. Rechts davon sind wieder graue Symbole für die vererbten Regeln zu sehen.
- Sie haben damit den Aufbau von Verbindungen aus dem lokalen Netz ins Internet und untergeordnete Netze zum Zielport 80 (HTTP) erlaubt. Durch die Stateful-Inspection-Firewall im Collax Security Gateway sind die Antwort- und Folgepakete dieser Verbindung automatisch erlaubt. Es ist nicht notwendig, den umgekehrten Weg „vom Internet ins LocalNet“ für HTTP zu öffnen.

10.3 Schritt für Schritt: Einrichten einer DMZ

Die Einrichtung einer DMZ ist nicht nur zum Betrieb eines aus dem Internet zugänglichen Servers sinnvoll. Es empfiehlt sich auch, einen Access Point für Wireless LAN an einer eigenen Netzwerkschnittstelle des Collax Security Gateways anzuschließen und so das Funknetz vom lokalen Netz zu trennen.

- Legen Sie zunächst unter *Netzwerk – Netze – Konfiguration* ein neues Netz für die DMZ an. Sie benötigen auf dem neuen Netzwerkstrang einen anderen IP-Adressbereich als im lokalen

Netz. Dies ist notwendig, damit die Systeme im lokalen Netz die Datenpakete zum Collax Security Gateway schicken. Dieser muss als Standard-Gateway eingetragen sein.

- Fügen Sie nun unter *Netzwerk – Links – Konfiguration* einen neuen Link für die DMZ hinzu.
- Dieser Link ist vom *Typ* „Ethernet".
- Vergeben Sie unter *IP-Adresse des Systems* eine Adresse für den Collax Security Gateway aus dem neu angelegten Netzwerkbereich. Diese Adresse muss das Standard-Gateway für die in der DMZ betriebenen Systeme werden.
- Wählen Sie unter *Schnittstelle* das Netzwerkinterface aus, an dem Sie die DMZ anschließen.
- *SNAT/Masquerading* kann im Normalfall deaktiviert bleiben. Die beiden Netzbereiche verwenden den Collax Security Gateway als Standard-Gateway und werden auf dem *InternetLink* maskiert. Prüfen Sie letzteres, insbesondere, wenn auf dem *InternetLink* nicht *Alle maskieren* eingestellt ist.
- Unter *erreichbare Netze* wählen Sie das für die DMZ neu angelegte Netz aus.
- Wechseln Sie nun zu *Netzwerk – Firewall – Firewallmatrix* . Sie sehen hier das für die DMZ angelegte Netz. Setzen Sie alle erforderlichen Berechtigungen. Wenn Sie in der DMZ einen Webserver betreiben möchten, müssen Sie HTTP und/oder HTTPS aus dem Internet in die DMZ erlauben.
- Wenn Sie ein Wireless-LAN betreiben wollen, möchten Sie vielleicht stattdessen den Zugriff aus der DMZ ins lokale Netz für *Windows Networking* erlauben.
- In den Benutzungsrichtlinien unter *Benutzungsrichtlinien – Richtlinien – Gruppen* werden die Zugriffe auf Dienste im Collax Security Gateway gesteuert. Fügen Sie hier das Netz der DMZ entsprechend den Gruppen als Mitglied hinzu.
- Sie können die Konfiguration nun aktivieren.

10.4 GUI-Referenz: Firewall

10.4.1 *Firewall – Allgemein*

(Dieser Dialog befindet sich unter *Netzwerk – Firewall – Allgemein*)

In den folgenden Abschnitten werden allgemeine Einstellungen für die Firewall vorgenommen. Dabei lässt sich u. a. der Umfang der Protokollierung in Logdateien sowie die Auswertung dieser Logdateien anpassen.

10.4.1.1 Tab *Grundeinstellungen*, Abschnitt *Grundeinstellungen*

In diesem Abschnitt werden einige Optionen für das Verhalten und die Protokollierung der Firewall eingestellt. Die Protokollierungsoptionen betreffen dabei nur Verbindungen, die direkt an den Collax Security Gateway gerichtet sind. Die Protokollierung durchlaufender Verbindungen wird in der Firewallmatrix konfiguriert. In Windows-Netzwerken verursachen Broadcast-Pakete oft eine Flut von Logmeldungen. Mit der Einstellung *Alles außer Broadcasts* werden solche Pakete ignoriert.

Felder in diesem Abschnitt

- *Verhalten bei ICMP-Echo-Request (Ping)*: ICMP-Echo-Request-Pakete (*pings*) dienen dazu, festzustellen, ob ein bestimmter Rechner erreichbar ist und wie lange die Laufzeit der Datenpakete dorthin ist. Hier wird eingestellt, wie der Collax Security Gateway auf ICMP-Echo-Requests reagiert.

  Normalerweise wird *ratenlimitiert* auf ICMP-Echo-Requests

geantwortet. Dann werden ca. 10 Ping-Pakete pro Sekunde beantwortet, alle anderen werden verworfen. Falls viele Systeme gleichzeitig versuchen, den Collax Security Gateway anzupingen, kann es auch erforderlich sein, *unlimitiert* zu antworten (dann wird jedes Ping beantwortet).

10.4.1.2 Tab *Grundeinstellungen*, Abschnitt *Layer-7-Protokollunterstützung*

Funktionsweise

Einige IP-Protokolle verwenden mehr als eine Verbindung. Bei aktivem FTP wird beispielsweise zunächst vom Client zum Server eine Kontrollverbindung geöffnet, über die die Anmeldung am Server und die Kommandos des Clients geschickt werden. Für eine Datenübertragung (Verzeichnisanzeige, Download usw.) wird vom Server eine Datenverbindung zum Client aufgebaut. Gerade bei der Verwendung von „Masquerading“ führt dies zu Problemen, da die Firewall diese neue Verbindung einem internen, maskierten System zuordnen muss.

Mit Hilfe dieser Unterstützungsmodule werden für einzelne Protokolle die Datenpakete analysiert und es kann entsprechend auf die Besonderheiten des jeweiligen Protokolls reagiert werden. Bei einer FTP-Verbindung wird beispielsweise der neu geöffnete Datenkanal dem richtigen Client zugeordnet.

Dieses Problem lässt sich auch durch den Einsatz von passivem FTP lösen. Dabei baut der Client die Datenverbindung zum Server auf. Allerdings unterstützen nicht alle FTP-Client-Programme dieses Verfahren (in der Voreinstellung).

Felder in diesem Abschnitt

- *FTP-Unterstützung*: Mit dieser Option wird die Unterstützung von FTP aktiviert.
- *IRC-Unterstützung*: Mit dieser Option wird die Unterstützung von IRC aktiviert.
- *PPTP-Unterstützung*: Mit dieser Option wird die Unterstützung von PPTP aktiviert.
- *SIP-Unterstützung*: Mit dieser Option wird die Unterstützung von SIP aktiviert.
- *SIP Media nur zwischen Signalisierungs-Endpunkten*: Diese Einstellung erlaubt es, die Remote-Adressen für den Audio- und Video-Datenstrom einzuschränken. Ist diese Option aktiviert, muss die Übertragung der RTP-Daten von dem selben System erfolgen wie der Rufaufbau. (Media-Proxy = SIP-Proxy).
- *SIP Signalisierung nur vom Registrar.*: Diese Einstellung erlaubt es, die Remote-Adressen für den Rufauf- und abbau einzuschränken. Ist diese Option aktiviert, muss der Registrar und der SIP-Proxy ein und das selbe System sein. (Registrar = Sip-Proxy)
- *TFTP-Unterstützung*: Mit dieser Option wird die Unterstützung von TFTP aktiviert.

10.4.1.3 Tab *Optionen*, Abschnitt *Logging für lokale Dienste*

Felder in diesem Abschnitt

- *Erlaubte Verbindungen*: Durch das Aktivieren dieser Option wird der Aufbau erlaubter Verbindungen auf den Collax Security Gateway protokolliert.
- *Verbotene Verbindungen*: Durch das Aktivieren dieser Option werden nichtautorisierte Verbindungsversuche protokolliert.

- *Verbindungen von gefälschten Absenderadressen*: Mit dieser Option werden Verbindungsversuche von gefälschten Absenderadressen protokolliert.
- *Verbindungen zu nicht vorhandenen Diensten*: Durch das Aktivieren dieser Option werden Verbindungsversuche auf Ports protokolliert, die keinen Diensten zugeordnet sind.

10.4.1.4 Tab *Optionen*, Abschnitt *Logging für Firewallmatrix*

Felder in diesem Abschnitt

- *Erlaubte Verbindungen*: Durch das Aktivieren dieser Option werden alle Verbindungen protokolliert, die in der Firewallmatrix als erlaubt eingestellt sind.
- *Verbotene Verbindungen*: Durch das Aktivieren dieser Option werden alle Verbindungsversuche zwischen Netzwerken protokolliert, deren Regel in der Firewallmatrix auf ablehnen oder wegwerfen gesetzt ist.

10.4.1.5 Tab *Optionen*, Abschnitt *Report*

Felder in diesem Abschnitt

- *Firewall-Report aktivieren*: Mit dieser Option wird die automatische Erstellung von Firewall-Reports aktiviert. Ein solcher Report enthält eine statistische Auswertung der Einträge in der Firewall-Logdatei.
- *Täglicher Report*: Mit dieser Option wird täglich ein Firewall-Report erstellt.
- *Wöchentlicher Report*: Mit dieser Option wird wöchentlich ein Firewall-Report erstellt.

- *E-Mail-Adresse des Empfängers*: In diesem Feld wird die E-Mail-Adresse angegeben, an die der Report gesendet wird.
- *Format*: Der Report kann wahlweise als einfacher Text oder HTML-formatiert werden.
- *Schwellenwert für Protokollierung*: Mit diesem Schwellenwert wird festgelegt, wie oft ein Ereignis auftreten muss, damit es in den Report aufgenommen wird.
- *Angezeigte Ereignisse pro Logreport beschränken*: Dieser Wert beschränkt die Anzahl der im Report aufgeführten Ereignisse.
- *IP-Adressen auflösen*: Durch das Aktivieren dieser Option werden IP-Adressen im Report über den Nameserver in Hostnamen aufgelöst. Dies kann erheblichen Netzwerkverkehr erzeugen und die Erstellung des Reports verlangsamen.
- *Nach Absenderadressen unterscheiden*: Verschiedene Logeinträge können als einzelne oder als getrennte Ereignisse aufgefasst werden. Durch das Deaktivieren dieser Option können mehrere Meldungen mit unterschiedlichen Absenderadressen zu einem Ereignis zusammengefasst werden.
- *Nach Zieladressen unterscheiden*: Durch das Deaktivieren dieser Option können mehrere Meldungen mit unterschiedlichen Zieladressen zu einem Ereignis zusammengefasst werden.
- *Nach Protokollen unterscheiden*: Durch das Deaktivieren dieser Option können mehrere Meldungen mit unterschiedlichen Protokollen (TCP, UDP usw.) zusammengefasst werden.
- *Nach Quellports unterscheiden*: Durch das Deaktivieren dieser Option können mehrere Meldungen mit unterschiedlichen Quellports zusammengefasst werden.
- *Nach Zielports unterscheiden*: Durch das Deaktivieren dieser Option können mehrere Meldungen mit unterschiedlichen Zielports zusammengefasst werden.

10.4.2 *Netzwerkdienste*

(Dieser Dialog befindet sich unter *Netzwerk – Firewall – Dienste*)

In dieser Liste werden alle bekannten Dienste angezeigt. Dabei handelt es sich jeweils um die Zuordnung von einem IP-Protokoll und zugehörigen Quell- und Zielports, die unter dem Namen des Dienstes im System an anderer Stelle ausgewählt werden können. Es sind serienmäßig Dienste für die gängigen Protokolle vordefiniert. Weitere Dienste können hinzugefügt werden.

10.4.2.1 *Dienst wählen*

(Dieser Dialog befindet sich unter *Netzwerk – Firewall – Dienste*)

In der Tabelle werden alle vorhandenen Dienste angezeigt. Es können weitere Dienste hinzugefügt werden. Selbst definierte Dienste können bearbeitet oder gelöscht werden.

Felder in diesem Dialog

- *Name*: Hier wird der Name des Dienstes angezeigt.
- *Kommentar*: Hier wird der zugehörige Kommentartext angezeigt.
- *Berechtigung*: Hier wird angezeigt ob es sich bei der Berechtigung um einen benutzerbezogenen Dienst (Berechtigung) oder um einen Dienst, welcher über die Firewall geregelt wird handelt.

Aktionen für jeden Tabelleneintrag

- *Dienst bearbeiten*: Mit dieser Aktion wird die Konfiguration des Dienstes bearbeitet. Diese Aktion ist nur für selbstdefinierte Dienste verfügbar.

- *Löschen*: Mit dieser Aktion wird der Dienst gelöscht. Diese Aktion ist nur für selbstdefinierte Dienste verfügbar.
- *Dienst anzeigen*: Mit dieser Aktion wird die Konfiguration des Dienstes angezeigt.

Aktionen für diesen Dialog

- *Dienst hinzufügen*: Mit dieser Aktion kann ein weiterer Dienst hinzugefügt werden.

10.4.2.2 *Dienst bearbeiten*

(Dieser Dialog befindet sich unter *Netzwerk – Firewall – Dienste*)

In diesem Dialog können die Einstellungen eines selbstdefinierten Dienstes geändert werden.

In diesem Dialog werden die notwendigen Daten zu einem Dienst angegeben.

Felder in diesem Dialog

- *Name*: Hier wird der Name für den Dienst angegeben.
- *Name*: Wird ein vorhandener Dienst bearbeitet, kann der Name nicht mehr geändert werden.
- *Kommentar*: Hier sollte ein Kommentartext zu dem Dienst angegeben werden. Der Dienst ist unter diesem Kommentartext in verschiedenen anderen Dialogen sichtbar.
- *Protokoll*: Hier muss das von dem Dienst genutzte Protokoll ausgewählt werden.
- *Quellport (Bereichsanfang)*: Hier wird der Anfang des Quellportbereiches angegeben.

Normalerweise wird der Quellport vom System, welches die Verbindung aufbaut, willkürlich vergeben. Meist liegt der Quellport im Bereich 1024 bis 65535. In bestimmten Fällen, etwa bei manchen UDP-Verbindungen, kommen Anfragen immer vom gleichen Absenderport. Dann kann hier eine sinnvolle Einschränkung gemacht werden.

Hinweis: Einige seltene Ausnahmen (zum Beispiel Windows-Netzwerkdienste) bauen Verbindungen von einem festen Quellport zu beliebigen Zielports auf (in diesem Beispiel von Quellport 137). Die Gefahr bei diesen Diensten besteht darin, dass ein Angreifer seinen Quellport auf 137 setzen kann und damit Zugriff auf alle Ports ab 1024 erhält. Dienste dieser Art sollten unter keinen Umständen von nicht vertrauenswürdigen Netzen angenommen oder besser komplett vermieden werden.

- *Quellport (Bereichsende)*: Hier wird das Ende des Quellportbereiches angegeben. Bleibt das Feld leer, wird nur der Anfangsport als einziger Quellport verwendet.
- *Zielport (Bereichsanfang)*: Hier wird der Anfang des Zielportbereiches angegeben.
- *Zielport (Bereichsende)*: Hier kann das Ende des Zielport-Bereiches angegeben werden. Bleibt das Feld leer, wird nur der Anfangsport als einziger Zielport verwendet.
- *ICMP-Typ*: Ist als Protokoll ICMP ausgewählt, kann hier der genaue ICMP-Typ ausgewählt werden. Zur Auswahl stehen nur ICMP-Anfragen, alle ICMP-Antworten werden automatisch intern über das „Connection-Tracking“ behandelt.

10.4.2.3 *Dienst anzeigen*

(Dieser Dialog befindet sich unter *Netzwerk – Firewall – Dienste*)
In diesem Dialog werden die genauen Einstellungen eines Dienstes angezeigt.

Felder in diesem Dialog

- *Name*: Hier wird der Name des Dienstes angezeigt.
- *Kommentar*: Hier wird der Kommentartext angezeigt.

10.4.3 *Portumleitung*

(Dieser Dialog befindet sich unter *Netzwerk – Firewall – Portumleitung*)

10.4.3.1 *Portumleitung*

(Dieser Dialog befindet sich unter *Netzwerk – Firewall – Portumleitung*)

Felder in diesem Dialog

- *Bezeichnung*: Hier wird die eindeutige Bezeichnung für die Portumleitung angezeigt.
- *Kommentar*: In diesem Feld wird der Kommentar angezeigt.
- *Dienst*: Hier wird der Dienst angezeigt, der umgeleitet wird.
- *Ziel*: In diesem Feld wird der Zielrechner der Portumleitung angezeigt.

- *Zielport*: Auf diesen Zielport werden ankommende Pakete umgeleitet.
- *Aktiv*: Diese Spalte zeigt an, ob die Funktion aktiv oder inaktiv ist.

10.4.3.2 *Portumleitung*

(Dieser Dialog befindet sich unter *Netzwerk – Firewall – Portumleitung*)

Felder in diesem Dialog

- *Bezeichnung der Portumleitung*: In diesem Feld muss eine eindeutige Bezeichnung für die Portumleitung eingegeben werden. Die Bezeichnung kann nach dem Speichern nicht mehr geändert werden.
- *Kommentar*: Um die Portumleitung weiter zu beschreiben, kann in diesem Feld ein Kommentar eingegeben werden.
- *Dienst*: Aus dieser Liste kann der Dienst ausgewählt werden, der weitergeleitet werden soll. Hier werden vordefinierte und auch selbst hinzugefügte Dienste zur Auswahl bereitgestellt.
- *Umleitung auf folgende Links beschränken*: Die Auswahl bestimmt, auf welchen Links die Portumleitung angewendet werden soll. Wird kein Link gewählt, wird die Umleitung auf alle IP-Pakete angewendet, die an einem beliebigen lokalen Link ankommen. Wird ein Link gewählt, so wird die Portumleitung auf den entsprechenden Link beschränkt.
- *Zugriff von Netzen und Hosts in folgenden Gruppen beschränken*: Soll die Umleitung nur von bestimmten Netzwerken oder Hosts in Anspruch genommen werden können, ist hier die entsprechende Gruppe auszuwählen. Befinden sich die IP-Adresse des Ziels

und die Source-IP-Adresse im selben Netzwerk, muss auf dem entsprechenden Link dieses Netzwerk maskiert werden. Sobald in einer Gruppe das Netz Internet enthalten ist, kann keine weitere Unterscheidung nach Netzwerken vorgenommen werden. Hier ist zu empfehlen, dass dann eine separate Portumleitung nur mit Zugriff aus dem Internet, und auf einen Internet-Link beschränkt, vorgenommen wird.

- *IP-Adresse des Ziels*: Der Rechner, auf den die Portanfragen umgeleitet werden sollen. Befinden sich die IP-Adresse des Ziels und die Source-IP-Adresse im selben Netzwerk, muss auf dem entsprechenden Netzwerk-Link dieses Netzwerk maskiert werden.
- *Zielport*: Der Zielport, auf den die Netzwerkpakete umgeschrieben werden sollen.
- *Protokollieren*: Für eine weitere Überwachung der Funktion und ihrer Nutzung kann hier die Protokollierung der Netzwerkpakete aktiviert werden. Protokollierte Pakete können durch den Firewall-Report erfasst werden.
- *Deaktivieren*: Eine Umleitung kann hier deaktiviert bzw. wieder reaktiviert werden. Dadurch kann wiederholtes Löschen und Neuanlegen vermieden werden, wenn eine Umleitung nur gelegentlich benötigt wird.

10.4.4 *Dienste abweisen*

(Dieser Dialog befindet sich unter *Netzwerk – Firewall – Dienste abweisen*)

10.4.4.1 *Dienste abweisen*

(Dieser Dialog befindet sich unter *Netzwerk – Firewall – Dienste abweisen*)

Felder in diesem Dialog

- *Bezeichnung*: Hier wird die eindeutige Bezeichnung für die Dienstabweisung angezeigt.
- *Kommentar*: In diesem Feld wird der Kommentar angezeigt.
- *Dienst*: Hier wird der Dienst angezeigt, der abgewiesen wird.

Aktionen für diesen Dialog

- *Neuen Dienst abweisen*: Diese Aktion legt einen neuen Eintrag für einen abzuweisenden Dienst an.

10.4.4.2 *Dienste abweisen*

(Dieser Dialog befindet sich unter *Netzwerk – Firewall – Dienste abweisen*)

Felder in diesem Dialog

- *Bezeichnung des abzuweisenden Dienstes*: In diesem Feld muss eine eindeutige Bezeichnung für den abzuweisenden Dienst eingegeben werden. Die Bezeichnung kann nach dem Speichern nicht mehr geändert werden.
- *Kommentar*: Um die Dienstabweisung weiter zu beschreiben, kann in diesem Feld ein Kommentar eingegeben werden.

- *Deaktivieren*: Durch Aktivieren dieser Option wird die Abweisung deaktiviert, bleibt aber in der Konfiguration erhalten.
- *Dienst*: Aus der Liste der angelegten Dienste kann derjenige ausgewählt werden, der abgewiesen werden soll.
- *Auf Netzwerklinks*: Hier können die Netzwerklinks ausgewählt werden, auf denen der Dienst abgewiesen wird. So ist es möglich, einen Dienst nur bei Zugriffen aus dem Internet abzulehnen, Zugriffe aus dem lokalen Netz jedoch zuzulassen.
- *Protokollieren*: Durch das Aktivieren dieser Option werden abgewiesene Verbindungen protokolliert.

10.4.5 *Firewallmatrix*

10.4.5.1 *Firewallmatrix*

(Dieser Dialog befindet sich unter *Netzwerk – Firewall – Firewallmatrix*)

Die Firewallmatrix ist eine visuelle Darstellung der integrierten Firewall. Hier wird festgelegt, welche Netzwerkverbindungen erlaubt bzw. geblockt sind. Zusätzlich können bei aktiviertem Bandbreitenmanagement jeweils für einzelne Verbindungen bestimmte Bandbreiten garantiert bzw. begrenzt werden.

Hinweis: Die Firewallmatrix ist nur für durchlaufende Datenpakete relevant. Zugriffe auf Dienste im Collax Security Gateway selbst werden in den *Netzwerkgruppen* (Link) (S. 45) gesteuert.

Die Firewallmatrix ist das zentrale Schaltelement zwischen den *Netzwerkgruppen*. Hier kann für jedes Protokoll eingestellt werden, ob ein Verbindungsaufbau erlaubt oder verboten wird. Die Matrix wird immer „von Zeile nach Spalte“ gelesen. Am Schnittpunkt wird eingestellt, wie der ausgewählte Dienst behandelt wird. Dabei werden leicht verständliche Symbole eingesetzt. Die Matrix wird daher auch als „Graphical Ruleset Generator“ bezeichnet.

Werden neue Netzwerkgruppen definiert, ist als Ziel in der Matrix die Standardregel „Wegwerfen“ zwischen diesen Netzwerken eingestellt.

Ein „schwarzes Loch“ bedeutet, dass Pakete verworfen werden, ohne dass für den Absender eine ICMP-Meldung erzeugt wird („Drop“).

Das „Durchfahrt-verboten-Schild“ zeigt an, dass Verbindungen aktiv abgewiesen werden. Der Absender erhält eine entsprechende ICMP-Nachricht („Reject“).

Ein „Vorfahrtsstraßen-Schild“ zeigt an, dass der Verbindungsaufbau erlaubt ist („Accept“).

Ein „Achtung-Schild“ zeigt an, dass an dieser Stelle ein Konflikt besteht. Weitere Informationen dazu finden sich weiter unten bei den „Aktionen“.

Manuell gesetzte Regeln werden immer durch farbige Symbole dargestellt. Durch „Vererbung“, etwa aus übergeordneten Netzwerkgruppen oder über die Default-Regel, entstehen implizite Regeln. Diese werden in grau dargestellt und können jederzeit durch explizite Regeln „überschrieben“ werden.

Hinweis: In der Matrix muss immer nur eine Regel für das erste Paket der Verbindung, also den Verbindungsaufbau, gesetzt werden. Die Folgepakete sind durch das im Collax Security Gateway integrierte „Connection Tracking“ automatisch enthalten.

Neben einer „Default-Regel“ können einzelne Dienste aus der Liste ausgewählt werden, für die jeweils die Firewall-Regeln eingestellt werden.

Ist für einen bestimmten Dienst, wie HTTP oder DNS, eine Regel manuell gesetzt, wird dies in der Ansicht *Dienst: Alle* angezeigt. Das entsprechende Symbol wird dann durch zwei farbige Klammern ergänzt. Zusätzlich können im Popup-Fenster weitere Informationen zu den definierten Regeln und Diensten eingesehen werden.

10.4.5.2 *Regelsatz bearbeiten*

(Dieser Dialog befindet sich unter *Netzwerk – Firewall – Firewallmatrix*)

- *Von Netzwerkgruppe*: Der Verbindungsaufbau erfolgt immer von einem Netz in ein weiteres Netz. Hier wird die ausgewählte Quellnetzwerkgruppe angezeigt.
- *Nach Netzwerkgruppe*: Hier wird die Zielnetzwerkgruppe der Regel angezeigt.
- *Dienst*: Für jeden Dienst kann es in der Matrix eine eigene Regel geben. Als Standard existiert der Dienst Default, der im Prinzip den Dienst „any", also alle Dienste, für die nicht explizit etwas eingestellt wurde, widerspiegelt. Für jeden Firewall-Dienst kann eine weitere spezielle Regel hinzugefügt werden. Einzelne Dienste-Regeln können gelöscht werden. Die Default-Regel kann zurückgesetzt werden, indem der Regelsatz gelöscht wird.
- *Regel*: Über das Feld Regel wird festgelegt, wie mit den Verbindungen verfahren werden soll:

  Die Regel *Übernehmen* bedeutet, dass die Regel von übergeordneten Netzwerkgruppen übernommen wird.

  Die Regel *Wegwerfen* blockiert den Verbindungsaufbau. Die Pakete werden gelöscht, und es wird keinerlei Rückmeldung per ICMP erzeugt.

  Die Regel *Ablehnen* blockiert ebenfalls den Verbindungsaufbau. Allerdings wird eine ICMP-Nachricht an den Absender erzeugt, die darüber informiert, dass die Verbindung nicht erlaubt ist.

  Mit der Regel *Erlauben* wird der Verbindungsaufbau gestattet. Ist das Bandbreitenmanagement aktiviert, kann hier zusätzlich die Traffic-Policy angegeben werden.
- *Protokollieren*: Mit dem Aktivieren dieser Option werden die Verbindungen für diesen Dienst in der Logdatei protokolliert.

- *Traffic-Policy*: Hier kann die zuvor definierte Traffic-Policy eingesetzt werden.

10.4.6 *Firewall-Viewer*

Über den Firewall-Viewer werden die in der Matrix eingestellten Firewallregeln in einer Listendarstellung angezeigt. Über die Suche können einzelne Quell- und Zielnetze sowie die Dienste gesucht werden. Wird keine Netzwerkgruppe oder Dienst mit der Suche in der Anzeige gefiltert, werden alle explizit hinzugefügten Regeln gelistet.

Ein Regelsatz in der Liste besteht immer aus einer Zeile, in der die Default-Regel für Quell- und Zielnetzwerkgruppe und die angewendete Regeln gezeigt wird. Danach folgen die Zeilen, in denen die einzelnen Dienste-Regeln angezeigt werden. Diese enthalten nur den Dienst und die angewendete Regel.

10.4.6.1 *Regeln auswählen*

(Dieser Dialog befindet sich unter *Netzwerk – Firewall – Viewer*)

Felder in der Tabelle

- *Von (Netzwerkgruppe) Nach (Netzwerkgruppe)*: Hier wird die Absender-Netzwerkgruppe und die Ziel-Netzwerkgruppe angezeigt. Die Regel gilt für diese angezeigten Netzwerkgruppen.
- *Aktion (Regel)*: Die Aktion (Regel) zeigt an, ob Netzwerkpakete weggeworfen, abgelehnt oder erlaubt werden. Standardmäßig werden Regelaktionen von übergordneten Regeln übernommen.
- *Info*: In diesem Feld stehen zusätzliche Informationen.

- *Gewichtung*: Der höchste Wert bezeichnet die höchste Gewichtung innerhalb des angezeigten Regelsatzes. Die Regel mit dem höchsten Gewicht wird als erstes beachtet. Üblicherweise wird die Gewichtung mit Hilfe der Netzwerkgruppen automatisch berechnet. Um die Gewichtung zu verändern, gibt es zwei Möglichkeiten:

  Die betreffende Netzwerkgruppe kann unterhalb einer weitere Netzwerkgruppe eingegliedert werden. Damit steigt die Priorität der damit verknüpften Regeln. Wird die Netzwerkgruppe weiter oberhalb eingegliedert sinkt die Priorität.

  Alternativ kann der betreffenden Netzwerkgruppe direkt ein beliebig hoher Wert im Feld Gewichtung vergeben werden.

  Bestehen mehrere Regeln mit derselben Gewichtung und sich überschneidenden Quellnetzen oder -hosts und Zieldiensten, dann werden Verbotsregeln vor Erlaubnisregeln angewendet.

Aktionen für diesen Dialog

- *Regeln anzeigen*: Mit dieser Aktion wird die Erstellung der Liste gestartet.

10.4.6.2 *Regeln anzeigen*

(Dieser Dialog befindet sich unter *Netzwerk – Firewall – Viewer*)

Spalten in der Tabelle

- *Von*: Hier wird der Name des Quellnetzes angezeigt.
- *Nach*: Hier wird der Name des Zielnetzes angezeigt.
- *Dienst*: Hier wird der jeweilige Dienst angezeigt. *Alle* steht dabei

für den Vorgabewert, der verwendet wird, wenn keine Regel für einen bestimmten Dienst gesetzt wird (entsprechend die „Default Policy“).
- *Aktion*: Hier wird angezeigt, welche Regel (Erlauben, Ablehnen usw.) für die Verbindung eingestellt ist.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird die Regel bearbeitet. Dabei wird derselbe Dialog verwendet, der in der Matrix beim Bearbeiten der entsprechenden Verbindung erscheint.

10.4.7 *Host Analyse*

Funktionieren Berechtigungen von Netzwerken oder Hosts nicht korrekt, können mit dieser Analyse Details über Berechtigungen, Verwendung oder Firewallregeln bestimmter Netzwerkhosts abgerufen werden.

Geben Sie dazu die IP-Adresse oder den kompletten Hostnamen (FQDN) für den zu prüfenden Host an.

10.4.8 *DNAT/Portweiterleitung*

10.4.8.1 *DNAT*

Felder in diesem Formular

- *Bezeichnung*: Hier wird die eindeutige Bezeichnung für die Portumleitung angezeigt.
- *Kommentar*: In diesem Feld wird der Kommentar angezeigt.
- *Typ*: In diesem Feld wird der Typ angezeigt.
- *Originales Ziel*: In diesem Feld wird der Zielrechner der Portumleitung angezeigt.
- *Neues Ziel*: Auf diesen Zielport werden ankommende Pakete umgeleitet.
- *Dienst*: Hier wird der Dienst angezeigt, der umgeleitet wird.
- *Log*: Diese Spalte zeigt an, ob das Log aktiv oder inaktiv ist.
- *Aktiv*: Diese Spalte zeigt an, ob die Funktion aktiv oder inaktiv ist.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird die Konfiguration der Weiterleitung bearbeitet.
- *Löschen*: Mit dieser Aktion wird die Weiterleitung gelöscht.

Aktionen für dieses Formular

- *Hinzufügen*: Mit dieser Aktion kann eine Portumleitung neu definiert werden.

10.4.8.2 *Destination NAT*

Abschnitt*Grundeinstellungen*

Felder in diesem Abschnitt

- *Bezeichnung*: In diesem Feld muss eine eindeutige Bezeichnung für die Portumleitung eingegeben werden. Die Bezeichnung kann nach dem Speichern nicht mehr geändert werden.
- *Bezeichnung*: Die Bezeichnung der Portumleitung.
- *Kommentar*: Um die Portumleitung weiter zu beschreiben, kann in diesem Feld ein Kommentar eingegeben werden.
- *Typ*: Aus dieser Liste kann der Typ ausgewählt werden, der weitergeleitet werden soll.
- *Ursprüngliches Ziel*: Mit diesem Feld bestimmt man die Quelle, von der aus Netzwerkpakete ausgesendet wurden.
- *Ankommend auf Link*: Hier wird die Netzwerkverbindung (Link) gefiltert, auf dem die umzuschreibenden Netzwerkpakete auftreffen.
- *Neues Ziel (Destination Netmap)*: Auf dieses Netzwerk werden die Netzwerkpakete dann als neues Ziel umgeschrieben.
- *Dienst*: Aus dieser Liste kann der Dienst ausgewählt werden, der weitergeleitet werden soll. Hier werden vordefinierte und auch selbst hinzugefügte Dienste zur Auswahl bereitgestellt.
- *Neues Ziel (Portweiterleitung)*: Der Rechner, auf den die Portanfragen umgeleitet werden sollen. Befinden sich die IP-Adresse des Ziels und die Source-IP-Adresse im selben Netzwerk, muss auf dem entsprechenden Netzwerk-Link dieses Netzwerk maskiert werden.
- *Neuer Zielport*: Der Zielport, auf den die Netzwerkpakete umgeschrieben werden sollen.

Abschnitt*Filter*
Felder in diesem Abschnitt

- *Dienst*: *** MISSING ***
- *Anfragen nur von bestimmten Netzwerkgruppen akzeptieren*: *** MISSING ***
- *Protokollieren*: Für eine weitere Überwachung der Funktion und ihrer Nutzung kann hier die Protokollierung der Netzwerkpakete aktiviert werden. Protokollierte Pakete können durch den Firewall-Report erfasst werden.
- *Deaktivieren*: Eine Umleitung kann hier deaktiviert bzw. wieder reaktiviert werden. Dadurch kann wiederholtes Löschen und Neuanlegen vermieden werden, wenn eine Umleitung nur gelegentlich benötigt wird.

Aktionen für dieses Formular

- *Schließen*: Bearbeiten der Portumleitung beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten der Portumleitung beenden. Die Änderungen werden gespeichert und können anschließend aktiviert werden.

10.4.9 *Source NAT*

10.4.9.1 Felder

- *Tabelle*: In der Tabelle werden alle SNAT Regeln angezeigt, die vom Administrator angelegt wurden. Dabei ist die originale Quelle das Netz aus dem das Paket kam und die neue Quelle das Netz, welches danach in der Absendeadresse steht. Des Weiteren kann man sehen ob das Log für die einzelnen Regeln aktiv ist und ob sie angewendet wird.

10.4.9.2 *Source NAT*

Abschnitt*Grundeinstellungen*

Funktion

- *Neue Regel erstellen*: Hier werden die Grundeinstellungen für die SNAT Regel ausgewählt. Beim Typ ist zu beachten, dass bei Netmap die Netzmaske gleich bleibt. Deshalb muss die Netzmaske der ursprünglichen Quelle mit der Netzmaske der neuen Quelle übereinstimmen.

Abschnitt*Filter*

Felder

- *Dienst*: Hier kann aus einer Liste von Diensten der passende Dienst ausgewählt werden. Wenn kein Dienst ausgewählt wird, trifft die SNAT regel auf alle zu.
- *Ziel befindet sich in bestimmter Netzwerkgruppe*: Hier wird ausgewählt in welcher Netzwerkgruppe sich das Ziel befindet. Wenn keine Netzwerkgruppe ausgewählt wurde, spielt es keine Rolle wo sich das Ziel befindet. Ist mindestens eine Netzwerkgruppe

gewählt, werden Pakete, die nicht an die gewählten Netzwerkgruppen gerichtet sind, nicht umgeschrieben.

- *Protokollieren*: Für eine weitere Überwachung der Funktion und ihrer Nutzung kann hier die Protokollierung der Netzwerkpakete aktiviert werden. Protokollierte Pakete können durch den Firewall-Report erfasst werden.
- *Deaktivieren*: Eine Umleitung kann hier deaktiviert bzw. wieder reaktiviert werden. Dadurch kann wiederholtes Löschen und Neuanlegen vermieden werden, wenn eine Umleitung nur gelegentlich benötigt wird.

Aktionen für dieses Formular

- *Schließen*: Bearbeiten beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten beenden. Die Änderungen werden gespeichert und können anschließend aktiviert werden.

10.5 *Schutz vor Brute-Force-Attacken*

10.5.1 Abschnitt

10.5.1.1 Felder in diesem Abschnitt

- *Aktivieren*: Der Dienst zum Schutz vor Brute-Force-Attacken wird hier eingeschaltet.
- *Anzahl erlaubter Loginversuche*: Wenn ein Angreifer mehr als die angegebene Anzahl versucht hat, sich unerlaubt einzuloggen, wird die IP-Adresse des Angreifers gesperrt. Achtung: Eine Unterscheidung zwischen Angreifer und Benutzer kann nicht getroffen werden.
- *Dauer der Sperrung (Sek.)*: Die IP-Adresse kann für die hier angegebene Dauer in Sekunden nicht mehr auf den Server zugreifen. Die Sperrung wird nach Ablauf der Dauer automatisch aufgehoben. Alternativ kann die Sperrung im Status-Dialog manuell aufgehoben werden.

  Die IP-Adressen werden auch entsperrt, sobald der Server oder der Dienst neu gestartet wird.
- *Nicht sperren*: Selektierte Netzwerke werden nicht gesperrt. Diese Einstellung ist nützlich, um interne Netzwerke vor eventuellen Sperrungen zu bewahren. Möglicherweise ist es auch beabsichtigt gerade interne Netzwerke zu prüfen und IP-Adresse gegebenenfalls zu sperren. Dann sollten die internen Netzwerke hier nicht selektiert werden.

10.5.2 Aktionen für dieses Formular

- *Speichern*: Die Einstellungen werden gespeichert.

10.5.3 *Brute-Force-Schutz - Status*

10.5.3.1

In dieser Tabelle werden die gesperrten IP-Adressen gelistet.

XXX missing title found
Spalten in der Tabelle

- *Gesperrte IP-Adressen*: IP-Adressen können öffentlich oder im privaten Adressbereich liegen.

Aktionen für jeden Tabelleneintrag

- *Sperre aufheben*: Mit dieser Aktion wird die Sperre für die IP-Adresse aufgehoben. Ein Fenster mit entsprechendem Hinweis erscheint.

Aktionen für dieses Formular

- *Manuell sperren*: Mit dieser Aktion wird ein Dialog geöffnet, in dem weitere IP-Adressen manuell gesperrt werden können.
- *Aktualisieren*: Die Anzeige wird aktualisiert.

10.5.3.2 *IP-Adressen manuell sperren*

Abschnitt
Felder in diesem Abschnitt

- *IP-Adressen angeben*: In das Feld können mehrere IP-Adressen mit Leerzeichen getrennt eingegeben werden, die nachfolgend vom Serverzugriff gesperrt werden. IP-Adressen innerhalb der Netzwerke der Option *Nicht sperren* werden dennoch gesperrt.

Aktionen für dieses Formular

- *Jetzt sperren*: Die angebenen IP-Adressen werden für den Zugriff auf den Server sofort gesperrt. Die Sperre dauert so lange, wie in den Einstellungen angegeben.

11 DNS und DHCP

11.1 Einführung

11.1.1 Host- und Domainnamen

Die Adressierung von Computersystemen erfolgt im Internet durch die Angabe der IP-Nummer bzw. im Ethernet durch die Verwendung der MAC-Adresse. Im Normalfall erfolgt die Umsetzung der IP-Adresse auf eine MAC-Adresse durch das Betriebssystem selbst.

Die IP-Nummer besteht aus einer 32 Bit breiten Adresse, die gewöhnlich in vier durch Punkte getrennten Oktette dargestellt wird, etwa 192.168.9.9.

Um das Handling für Benutzer einfacher zu gestalten, werden den Systemen Namen zugewiesen, die damit auch IP-Adressen entsprechen. Diese werden meist als „Hostname“ bezeichnet. Im einfachsten Fall wird dazu eine Zuordnung vom Namen auf die IP-Nummer in der *hosts*-Datei vorgenommen. Diese befindet sich bei Windows-Systemen im Verzeichnis *\WINNT* und bei Unix/Linux-Systemen im Verzeichnis */etc*. Diese Datei muss auf jedem Computersystem separat gepflegt werden. Die Wartung ist daher recht aufwendig, da bei Neueinträgen und Änderungen jede Instanz dieser *hosts*-Dateien modifiziert werden muss.

11.1.2 Domain

Ein Hostname muss zu einem Zeitpunkt eindeutig auf eine IP-Nummer aufgelöst werden. Da aber in vielen Fällen an unterschiedlichen Standorten dieselben Namen für Computersysteme verwendet werden (oftmals auch symbolische Namen wie *mail* oder *www*), muss dem Namen eine weitere Bezeichnung hinzugefügt werden, die für Eindeutigkeit sorgt. Mitunter löst ein Hostname auf mehrere IP-Adressen auf, um damit über DNS eine Lastverteilung auf mehrere Server zu erreichen. Da diese Server allerdings alle gleiche Inhalte bereitstellen, ist dies ein Sonderfall von „einer IP-Nummer".

Dazu wird die „Domain" verwendet, die quasi den Namen des Unternehmens oder des Standorts darstellt.

Im Internet werden ebenfalls Domains genutzt. Im Unterschied zur Windows-Domäne können diese nicht beliebig gewählt werden. Stattdessen werden sie über zentrale Einrichtungen verwaltet. Ein Anwender muss prüfen, ob der von ihm gewünschte Domainname noch frei ist und kann diesen dann über einen Provider „registrieren". Ist die Domain bereits anderweitig vergeben, muss eine andere ausgesucht werden.

Im folgenden handelt es sich bei der Verwendung des Begriffs „Domain" immer um Internet-Domains. Bei Windows-Domänen wird dies explizit erwähnt.

Eine Domain gehört immer zu einer „Top-Level-Domain" TLD. Diese TLDs sind bis auf wenige Ausnahmen Landeskennungen mit einem Kürzel aus zwei Buchstaben, etwa „de" für Deutschland oder „at" für Österreich. Diese werden auch als „ccTLD" (= „Country-Code TLD") bezeichnet.

Daneben gibt es noch allgemeine TLDs, die in den USA beim Aufbau des Internet zunächst festgelegt wurden („gTLD" = „generic TLD"). Dazu gehören etwa „com" für kommerzielle Unternehmen,

„edu“ für Hochschulen (Education), „org“ für nicht-kommerzielle Organisationen oder „gov“ für US-amerikanische Regierungsorgane.

In letzter Zeit sind einige weitere TLDs hinzugekommen, von denen manche „gesponsert“ („sTLD“) sind und manche nicht („uTLD“ = „unsponsored TLD“). Ein Sponsor ist in diesem Fall eine Organisation, die eine bestimmte Klientel vertritt und die Vergaberichtlinien für Domains innerhalb der TLD festlegt. Zudem muss der Sponsor einen Registrar zur Abwicklung der Registrierungen beauftragen. Eine ungesponserte TLD unterliegt den normalen Richtlinien der *ICANN.*

Tabelle einiger ausgesuchter TLDs

Name	Erläuterung	Zuständiger Registrar	Typ	Seit
.at	Österreich	www.nic.at	ccTLD	1988
.ch	Schweiz	www.switch.ch	ccTLD	1987
.de	Deutschland	www.denic.de	ccTLD	1986
.com	Kommerzielle Organisationen	www.verisign-grs.com	g/uTLD	1985
.edu	Bildungseinrichtungen		g/uTLD	1985
.gov	Regierungsorgane der USA	www.dotgov.gov	g/uTLD	1985
.int	Internationale Regierungsorganisationen	http://www.iana.org/int-dom/int.htm	g/uTLD	1985
.mil	Miltärische Einrichtungen der USA	www.nic.mil/dodnic/	g/uTLD	1985
.net	Netzwerk-Organisationen	www.verisign-grs.com	g/uTLD	1985
.org	Nichtkommerzielle, Nicht-Regierungs-Organisationen	www.pir.org	g/uTLD	1985
.aero	Luftfahrtindustrie	www.information.aero	g/sTLD	2001

.biz	Handelsfirmen („Business“)	www.neulevel.biz	g / uTLD	2001
.coop	Kooperationen / Genossenschaften	www.nic.coop	g / sTLD	2001
.info	Informationsanbieter	www.afilias.info	g / uTLD	2001
.museum	Museen, Ausstellungen	musedoma.museum	g / sTLD	2001
.name	Für natürliche Personen oder Familien	www.gnr.com	g / uTLD	2001
.pro	best. Berufsgruppen	www.registrypro.pro	g / uTLD	2002
.eu	Europäische Personen und Einrichtungen	www.eurid.org	g / sTLD	2003
.travel	Reiseindustrie	http://www.tralliance.travel	g / sTLD	2005

Daneben existiert noch die weitere, zunächst provisorisch eingerichtete TLD „arpa“, die für Rückwärtsauflösung (siehe weiter unten) verwendet wird. Inzwischen wird sie als „Address and Routing Parameter Area“ übersetzt.

Unterhalb einer TLD kann eine Domain immer nur ein einziges Mal existieren. Allerdings darf eine Domain in mehreren TLDs genutzt werden. Beispiele wären etwa „google.com“ und „google.de“.

Vor allem große Unternehmen oder Einrichtungen müssen ihre Domain auf verschiedene Standorte oder Gebäude verteilen. Dies geschieht durch „Subdomains“, die unterhalb der Domain quasi abgeteilte eigene Domains bilden. Manchmal werden dazu die Namen der Standorte verwendet, etwa „muenchen.collax.com“ und „boston.collax.com“. Formal korrekt ist „muenchen.csg.com“ eine Domain und gleichzeitig eine Subdomain von „csg.com“. Diese wiederum ist eine Domain und gleichzeitig eine Subdomain von „.com“.

11.1.3 FQDN

Das Gebilde aus Hostname und Domain wird als „Fully Qualified Domain Name“ (FQDN) bezeichnet. Damit ist ein Computersystem mit einem weltweit einmalig vergebenen Namen versehen, der auf eine IP-Nummer verweist.

Der FQDN wird von links nach rechts aus mehreren Komponenten gebildet, die alle durch Punkte voneinander getrennt sind. Dies sind der Reihe nach der Hostname, Subdomain(s), Domain und Top-Level-Domain. Als Subdomain können keine, eine oder auch mehrere Komponenten verwendet werden.

Beispiele für gültige FQDNs sind etwa „www.heise.de“, „mail.muenchen.csg.com“ oder auch „mail.intern.hamburg.de.unser-weltkonzern.com“.

11.1.4 Domain Name Service

Der „Domain Name Service“ (DNS) ist eine weltweit verteilte Datenbank, in der die IP-Adressen und ihre korrespondierenden Hostnamen gespeichert werden. Dabei muss nicht zwingend zu jeder IP-Nummer ein Hostname vorhanden sein. Bis auf Ausnahmen löst jeder Hostname auf eine IP-Nummer oder einen weiteren Hostnamen auf.

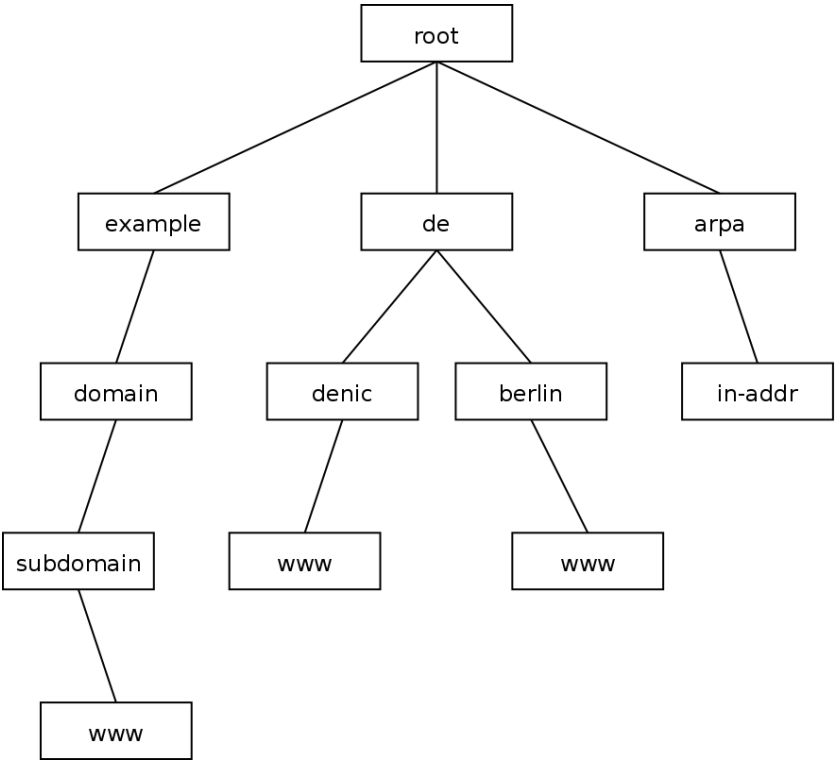
Die DNS-Datenbank wird in einer hierarchischen Baumstruktur verwaltet. Dabei ist die oberste Ebene die „Root-Zone“ (die „Wurzel“). Innerhalb dieser Root-Zone werden Verweise auf die untergeordnete Ebene gespeichert, in der die TLDs gespeichert sind. Weltweit existieren 13 Root-Nameserver, die in den meisten Systemen fest eingegeben sind und nicht manuell eingetragen werden müssen.

In der zweiten Ebene sind die einzelnen TLD-Zonen abgelegt, hier

werden Verweise auf die jeweiligen Domains (bei „com“ etwa 40 Millionen) gespeichert. Diese Nameserver werden von den zuständigen Registraren betrieben, in Deutschland von der DeNIC eG („Deutsches Network Information Center“).

In der nächsten Ebene liegen einzelne Host-Einträge oder Subdomains. Diese Informationen werden meist auf den Nameservern der zuständigen Provider gespeichert. In seltenen Fällen betreibt der Inhaber der Domain seine eigenen Nameserver.

Durch Subdomains können weitere Ebenen gebildet werden. Dabei können die ganzen Einträge unterhalb einer Domain auf einem einzigen Nameserver verwaltet werden. Es können jedoch auch für jede Subdomain eigenständige Nameserver betrieben werden.



Administrativ umfasst eine Domain immer auch alle Subdomains, d. h., für alle Geschehnisse inner- und unterhalb einer Domain ist der Domaininhaber verantwortlich.

Werden technisch für die Subdomains jeweils einzelne Nameserver betrieben, werden diese Subdomains als „Zonen“ im DNS bezeichnet. Jede Subdomain mit eigenständigem Nameserver ist eine solche Zone. Wenn alle Subdomains innerhalb der Domain selbst verwaltet werden, werden in diesem Fall die Begriffe „Domain“ und „Zone“ synonym verwendet.

In der weltweiten Datenbank ist jeder Nameserver nur für einen

kleinen Teil des gesamten Datenbestands verantwortlich. Er ist „autoritativ“ für seine Zonen. Sicherheitshalber gibt es zu jeder Zone mindestens zwei autoritative Nameserver, sonst wäre durch einen Ausfall des Servers die gesamte Domain „weg“.

Um die Datenhaltung zu vereinfachen, wird die Zone nur auf einem Masterserver, dem „Primary DNS“ gepflegt. Die weiteren autoritativen Server für diese Zone kopieren als *Slaves* nur die gesamten Zoneninformationen, sie sind „Secondary DNS“. Der Primary kennt die Secondaries und informiert diese bei Änderungen, so dass sie die Zone neu „transferieren“ können.

Um Anfragen an das gesamte Netzwerk von Nameservern möglichst rasch zu beantworten, dürfen die Zonen-Daten in einem Cache zwischengespeichert werden. Dazu gibt jede Zone jeweils eine Gültigkeitsdauer vor. Bei Änderungen im DNS kann es daher vorkommen, dass Teile des Internets noch eine gewisse Zeit mit veralteten Daten arbeiten.

11.1.5 Ablauf einer DNS-Anfrage

Um eine DNS-Anfrage zu stellen, schickt ein Clientrechner alle Anfragen gewöhnlich an einen DNS-Server im lokalen Netz. Dieser prüft, ob er für die Zone autoritativ ist und die Anfrage selbst beantworten kann.

Ist dies nicht der Fall, prüft der Nameserver, ob sich die Information in seinem Cache befindet und gültig ist und er damit die Anfrage direkt beantworten kann. Er arbeitet dann als „Resolver“.

Ist die Zone nicht im Cache vorhanden, muss der Nameserver selbst eine Anfrage stellen. Dazu kann er entweder alle Anfragen an einen bestimmten Nameserver weiterleiten (= „forwarden“). Dazu wird meist der DNS des Internet-Providers genutzt.

Ist im Nameserver kein Forwarder eingestellt, befragt dieser die Root-Nameserver nach den zuständigen Nameservern für die angefragte TLD. Dort fragt er nach den zuständigen Nameservern für die Domain und kontaktiert diese daraufhin, um die Anfrage aufzulösen oder weitere Verweise auf Nameserver für Subdomains zu erhalten. Der Nameserver hangelt sich durch den gesamten DNS-Baum bis hin zu dem Blatt, welches den angefragten Eintrag enthält.

Dieser aufgelöste Eintrag wird an den Client geschickt und für einen Zeitraum von wenigstens zehn Minuten im Cache zwischengespeichert. Erfolgt innerhalb des Zeitraums eine erneute Anfrage, wird diese direkt mit den Daten aus dem Cache beantwortet.

11.1.6 Rückwärtsauflösung

Die gesamten Mechanismen zu Auflösung von Hostnamen in IP-Adressen stehen auch für den rückwärtigen Weg zur Verfügung: Mit einem „Reverse-Lookup“ können IP-Adressen in Namen aufgelöst werden.

Technisch wird die Rückwärtsauflösung mit Hilfe der Domain *in-addr.arpa* realisiert. Um beispielsweise die IP-Adresse 192.0.2.129 aufzulösen, wird eine DNS-Anfrage nach „129.2.0.192.in-addr.arpa“ gestellt.

Unterhalb in-addr.arpa sind drei Ebenen von Subdomains realisiert, die jeweils für eins der Oktette der IP-Nummer zuständig sind. Dazu sind die Oktette in umgekehrter Reihenfolge in die Abfrage eingesetzt.

Über die Root-Nameserver erfolgt der Verweis auf die zuständigen Nameserver von in-addr.arpa und von dort ein weiterer Verweis abhängig von der ersten Subdomain (also dem ersten Oktett der IP-Nummer). Dort kann ein weiterer Verweis abhängig vom zweiten

Oktett erfolgen und dort wiederum einer abhängig vom dritten Oktett.

Auch für Reverse-DNS gibt es die Mechanismen von autoritativen Servern, Primaries und Secondaries sowie Zonentransfers.

Dadurch, dass für Domains und für IP-Netze jeweils separate DNS-Datenbanken bestehen, ist es nicht ungewöhnlich, dass Vorwärts- und Rückwärtsauflösung nicht synchron sind. Gerade bei Internetanbindung mit einfachen DSL-Leitungen lösen die IP-Adressen oft auf den Hostnamen des Leitungsproviders auf. Dies kann mitunter Schwierigkeiten verursachen, wenn hinter einer solchen Leitung Serverdienste betrieben werden.

11.1.7 Lokale Domain

Gerade diese Rückwärtsauflösung ist innerhalb eines Unternehmens sehr interessant, um einer IP-Nummer einen Namen zuordnen zu können. Meist werden im Unternehmen IP-Nummern aus den privaten Netzen verwendet. Zudem erfolgen sehr oft Änderungen durch Rechnerwechsel usw.

Hat das Unternehmen eine oder mehrere Domains bei einem Provider registriert, ist es aufwendig, all diese Einträge und Änderungen in der offiziellen Domain durchzuführen. Gelegentlich wird intern im Unternehmen unter der Adresse „www“ ein anderer Webserver genutzt als aus dem Internet.

Eine Möglichkeit ist, die offizielle Domain auf einem Nameserver im lokalen Netz des Unternehmens parallel zum Internet zu betreiben. Dieses Vorgehen kann allerdings gelegentlich zu Problemen führen, wenn Einträge aus dem offiziellen Nameserver beim Provider in den internen Nameserver kopiert wurden und der Provider Änderungen durchführt (Umstellung von IP-Adressen usw.).

Sinnvoller ist die Verwendung einer Subdomain *intern* oder *lan*, die dann als eigenständige Zone im lokalen Netz genutzt wird und so nicht mit der offiziellen Zone kollidiert.

Mitunter werden auch eigene TLDs im lokalen Netz verwendet, die auf die private, interne Nutzung hinweisen. Gängig sind *prv*, *priv* (jeweils für „privat“), *lan*, *local* oder *intern* (nicht *int*). Keine dieser TLDs ist allerdings für eine solche Verwendung offiziell freigegeben – die Nutzung erfolgt auf „eigene Gefahr“. *Apple Computer* benutzt inzwischen die TLD *local* für das „Bonjour-Protokoll“. Dies muss dann bei Macintosh-Geräten umgestellt werden.

11.1.8 Dynamische Adressvergabe

Die Konfiguration einer IP-Adresse für einen Computer kann meist manuell über das Betriebssystem vorgenommen werden. Eine einfachere und flexiblere Möglichkeit ist die Verwendung von DHCP („Dynamic Host Configuration Protocol“). Dabei fragt das Betriebssystem im Netzwerk nach einem DHCP-Server und lässt sich von diesem eine IP-Adresse zuteilen.

In der einfachsten Form wird dem DHCP-Server ein Bereich von IP-Nummern genannt, aus dem er nach Belieben IP-Adressen verwenden kann. Ein solcher Bereich wird auch als „Pool“ bezeichnet. Der Server identifiziert die Computer anhand ihrer Hardware-MAC-Adresse und verfolgt intern, welche IP-Adressen er an welches System zugewiesen hat (sog. „Leases“).

Eine DHCP-Lease hat eine bestimmte Laufzeit, nach deren Ablauf das System erneut beim DHCP-Server nach einer IP-Adresse fragen muss. Meist erhält es (auch nach Tagen) vom Server die gleiche IP-Adresse erneut, aber sie kann sich auch ändern.

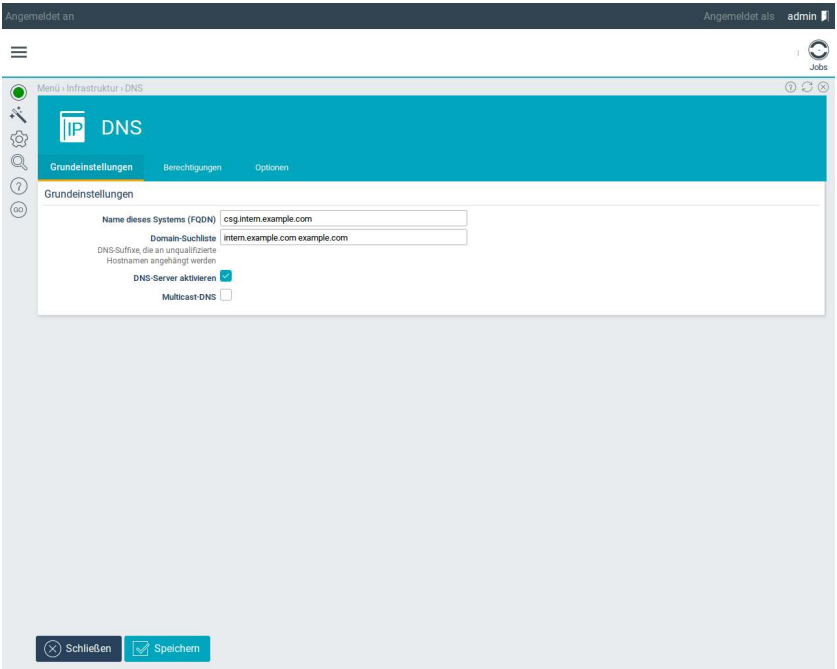
Um eine feste Zuweisung einer IP-Adresse an ein System zu erreichen, muss dieses anhand seiner MAC-Adresse bekannt sein. So ist eine dauerhafte statische Zuordnung der Adresse durch den DHCP-Server möglich.

Im Collax Security Gateway werden beide Varianten angeboten. Es kann ein Pool für unbekannte Rechner angelegt werden. Damit sind Systeme gemeint, die nicht als Hosts im Collax Security Gateway eingetragen sind. Sobald ein System in den *Benutzungsrichtlinien* bzw. unter *Netzwerk – DNS* als *Host* angelegt wird, können die MAC-Adresse und die IP-Adresse eingestellt werden. Ist der DHCP-Server aktiviert und stellt das System eine DHCP-Anfrage, wird die gesetzte IP-Adresse zugewiesen.

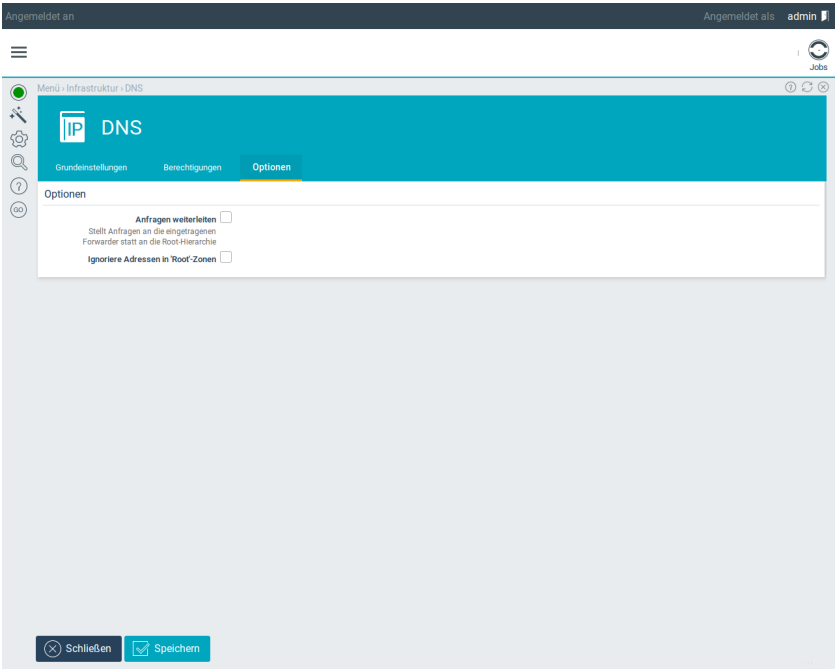
11.2 Schritt für Schritt: DNS für lokale Domain einrichten

Der Collax Security Gateway benötigt den Zugriff auf einen funktionsfähigen Nameserver, um die Registrierung durchzuführen und Updates herunterzuladen. Hierfür kann ein beispielsweise beim Provider ein anderer Server als Nameserver verwendet werden.

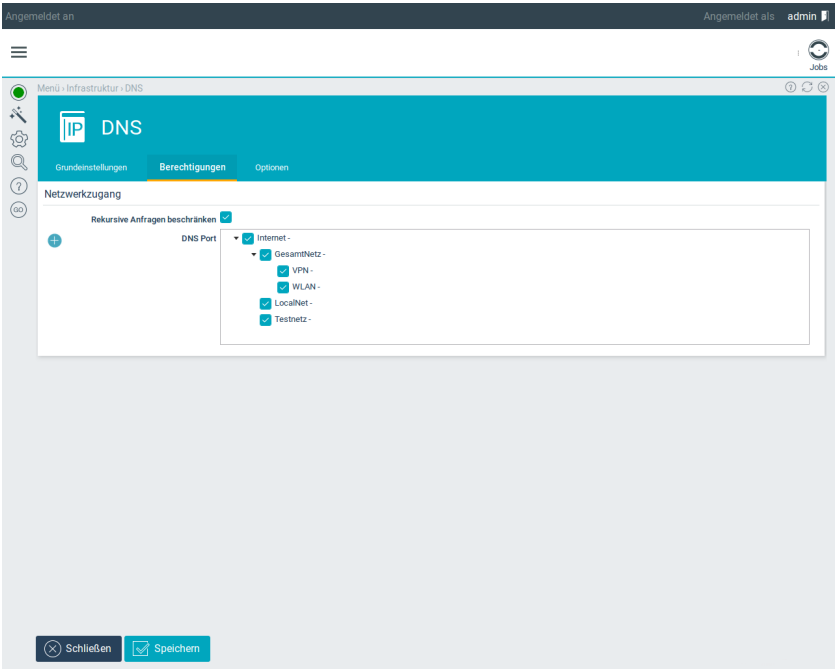
Wesentlich mehr Möglichkeiten bietet der Betrieb eines Nameservers auf dem Collax Security Gateway selbst. Hier können eigene Zonen verwaltet und so ein privates IP-Netz in Namen übersetzt werden.



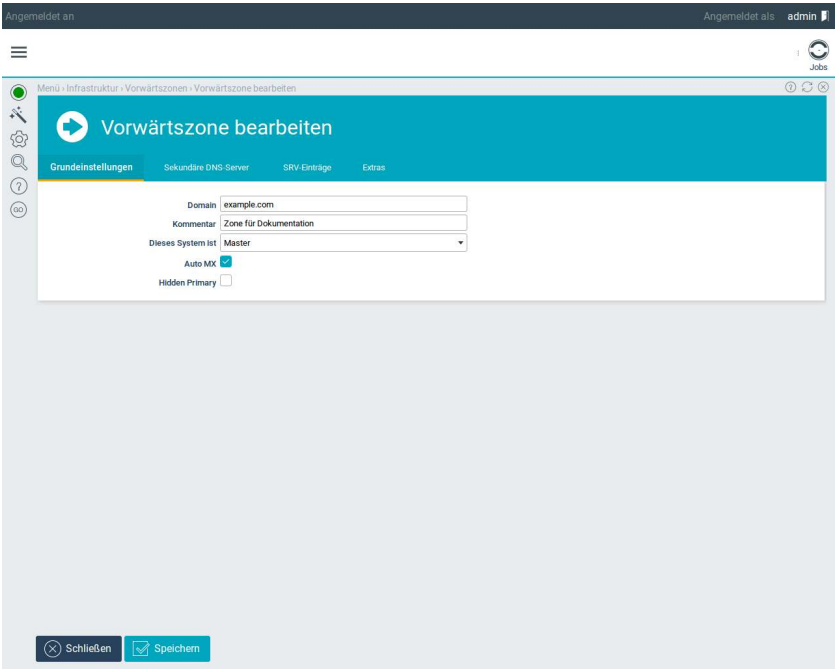
- Sie finden die Grundeinstellungen des Nameservers unter *Netzwerk – DNS – Allgemein*.
- Unter *Name dieses Systems* tragen Sie den FQDN des Collax Security Gateways ein. Dieser Name wird u. a. vom Mail-Dienst verwendet.
- Mit *DNS-Server aktivieren* schalten Sie den Nameserver im Collax Security Gateway ein.



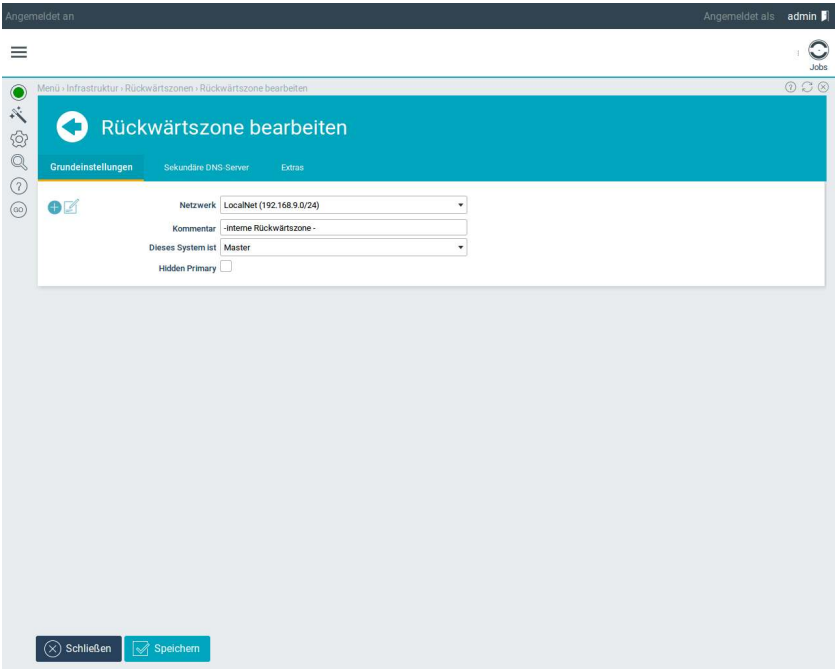
- Wechseln Sie auf den Reiter *Optionen*.
- Abhängig von der Einstellung *Anfragen weiterleiten* erfolgt die Auflösung von fremden Adressen. Lassen Sie die Option deaktiviert, befragt der Collax Security Gateway die Root-Nameserver eigenständig.
- Wenn Sie die Option hingegen aktivieren, können Sie bis zu zwei *Forwarder* angeben, an die alle DNS-Anfragen weitergereicht werden. Dabei sollten Sie die Nameserver Ihres Providers verwenden.



- Wechseln Sie auf den Reiter *Berechtigungen*.
- Hier können Sie auswählen, welche Gruppen Zugriff auf den Nameserver erhalten dürfen. Die Option *Rekursive Anfragen* erlaubt Anfragen nach jeglichen Namen.
- *Zugriff auf DNS-Port erlauben* hingegen gestattet nur Anfragen auf Systeme, deren DNS-Einträge auf dem Collax Security Gateway selbst verwaltet werden.
- Üblicherweise wird dem lokalen Netz der vollständige Zugriff auf den Nameserver gewährt. Das lokale Netz ist Mitglied der Gruppe *Users*, geben Sie daher der Gruppe Users beide Rechte.

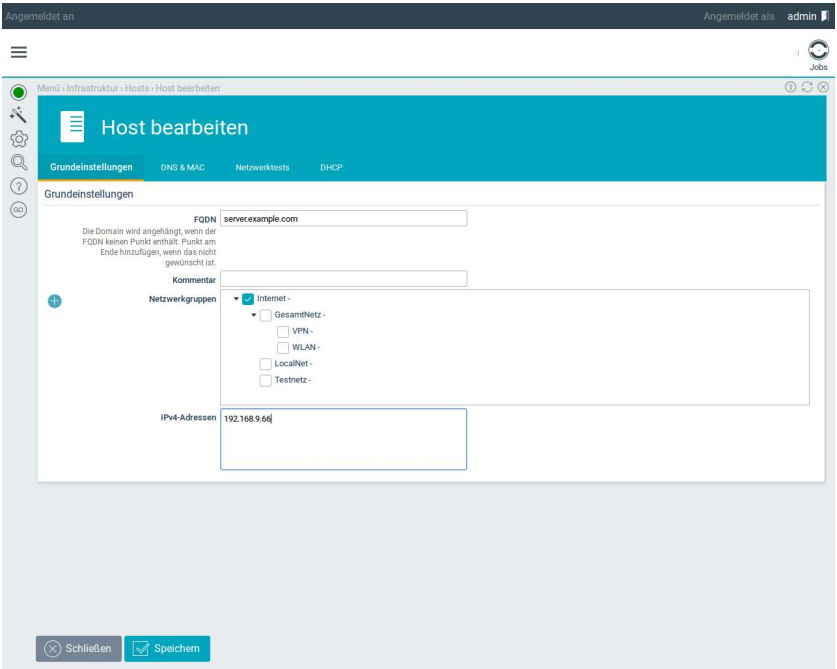


- Im nächsten Schritt legen Sie die lokale Domain an. Dabei kann es sich um Ihre offizielle Internet-Domain handeln. Meist ist es – auch im Hinblick auf die Verwendung privater IP-Adressen im lokalen Netz – jedoch besser, eine nicht existente Domain zu verwenden.
- Wechseln Sie hierfür zu *Netzwerk – DNS – Vorwärtszonen*.
- Legen Sie eine neue Zone an.
- Unter *Domain* tragen Sie den Namen der Zone ein.
- Belassen Sie die Einstellung *Dieses System ist* auf *Master*. Dadurch können Sie Einträge innerhalb der Domain auf dem Collax Security Gateway anlegen.

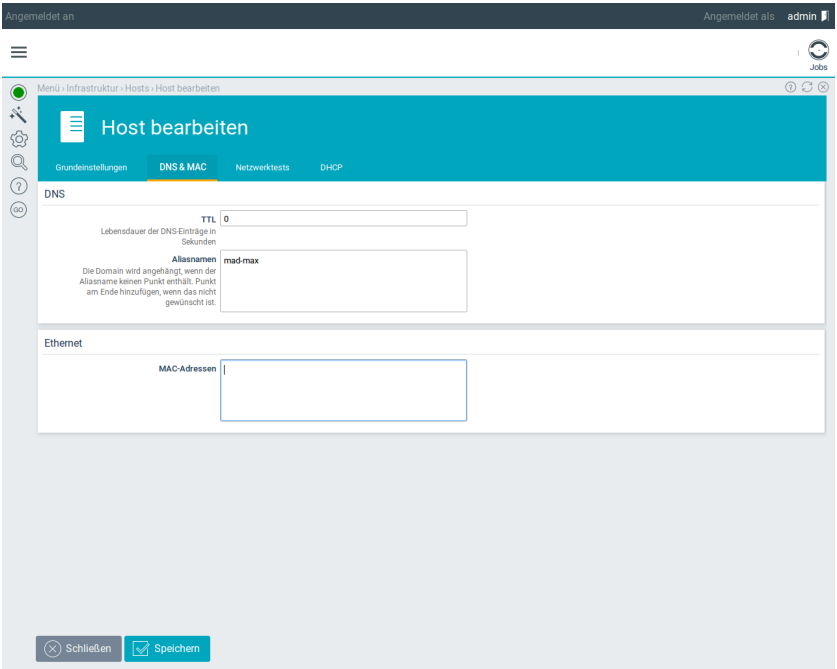


- Wechseln Sie zu den *Rückwärts-Zonen*.
- Legen Sie eine neue Rückwärts-Zone an.
- Wählen Sie als *Netzwerk* das *LocalNet* aus. Für diesen IP-Bereich sollen die Nameservereinträge verwaltet werden.
- Auch für diese Zone ist der Collax Security Gateway *Master*.

Nun ist der Nameserver grundlegend konfiguriert. Einzelne Einträge im Nameserver werden im Folgenden als *Hosts* angelegt.



- Wechseln Sie dazu nach *Netzwerk – DNS – Hosts*.
- Legen Sie einen neuen Host an.
- Setzen Sie den *Hostnamen*. Dieser kann später noch geändert werden.
- Prüfen Sie, ob *Bestätigt* aktivert ist. Andernfalls wird kein DNS-Eintrag erzeugt.
- Geben Sie unter *IP-Adresse* die IP-Nummer des Hosts an. Dabei muss die IP-Nummer nicht zwingend aus dem lokalen Netzwerk stammen.



- Wechseln Sie auf den Reiter *DNS*.
- Wählen Sie bei *Zone* die von Ihnen angelegte Domain aus.
- Unter *Aliasnamen* können Sie weitere Namen des Systems angeben.
- Speichern Sie den angelegten Host.

11.3 GUI-Referenz: DNS

11.3.1 *DNS*

(Dieser Dialog befindet sich unter *Netzwerk – DNS – Allgemein*)

In diesen Dialogen können die Einstellungen für den DNS-Dienst bearbeitet werden. Über diesen Dienst ist es möglich, Hostnamen in IP-Adressen aufzulösen und umgekehrt. Außerdem wird hier der Hostname des Systems gesetzt. Dieser wird u. a. vom Mailsystem verwendet.

11.3.1.1 Tab *Grundeinstellungen*, Abschnitt *Grundeinstellungen*

In diesem Dialog wird festgelegt, ob auf dem System der DNS-Dienst aktiviert werden soll. Andernfalls muss ein externer DNS eingestellt werden.

Hinweis: Ohne DNS-Dienst kann der Collax Security Gateway keine Registrierung durchführen, keine Updates herunterladen und keine E-Mails versenden.

Felder in diesem Abschnitt

- *Name dieses Systems (FQDN)*: Hier wird der vollständige DNS-Name (FQDN) dieses Systems angegeben, z. B. „csg.example.com“.
- *Domain-Suchliste*: In diesem Feld kann eine Liste von Domains angegeben werden, die der Reihe nach an einfache Hostnamen angefügt werden, um einen vollständigen Hostnamen zu erhalten.

  Wird hier „intern.example.com example.com“ angegeben und

innerhalb dieses Systems nach dem Namen „abox“ gesucht, wird der DNS-Server der Reihe nach „abox.intern.example.com“, „abox.example.com“ und schließlich „abox“ abfragen, bis er eine Antwort enthält. Mehrere Einträge werden durch Leerzeichen getrennt. Es werden maximal sechs Domains und 256 Zeichen unterstützt.

- *DNS-Server aktivieren*: Mit dieser Option wird der DNS-Server aktiviert.

  Selbst wenn im lokalen Netz bereits ein DNS betrieben wird, kann es sinnvoll sein, auf diesem System einen DNS-Server als Gateway zu betreiben. Dadurch wird das interne System vom Internet abgeschottet.
- *Erster Nameserver*: Wird kein eigenes DNS betrieben, muss das System mindestens einen Nameserver kennen, um die Namensauflösung von Hosts durchzuführen. Dieser DNS-Server wird hier eingetragen.
- *Alternativer Nameserver*: Zusätzlich kann ein zweiter DNS-Server als Alternative eingetragen werden. Meist werden hier die Nameserver des Providers verwendet.
- *Multicast-DNS*: „Zeroconf“ ist ein noch unvollständiger Standard, der es erlauben wird, Rechnersysteme ohne Konfiguration durch den Administrator auf Dienste im Netzwerk zugreifen zu lassen. *Multicast-DNS* ist ein Teil dieses Systems und wird verwendet, um einen DNS-Server im LAN auffindbar zu machen.

  Bisher unterstützen nur Apple Macintosh („Rendezvous“) und Linux-Systeme dieses Verfahren, es kann daher in den meisten Fällen deaktiviert bleiben.

11.3.1.2 Tab *Berechtigungen*, Abschnitt *Netzwerkzugang*

Über die *Benutzungsrichtlinien* wird festgelegt, welche Netzwerkgruppen Zugriff auf den internen Nameserver haben und ob sie beliebige Domains oder nur interne Domains abfragen dürfen.

Felder in diesem Abschnitt

- *Rekursive Anfragen beschränken*: Rechner und Netzwerke in den aktivierten Netzwerkgruppen dürfen rekursive DNS-Anfragen stellen.

  Bei einer rekursiven Anfrage verwaltet der angefragte DNS-Server die Zone nicht selbst, sondern muss seinerseits einen weiteren DNS-Server befragen (eine Rekursion).

  Darf ein System keine rekursiven Anfragen stellen, kann es nur Hostnamen und IP-Adressen im lokalen Netz auflösen. Damit ist der Zugriff auf das Internet nicht bzw. nur sehr erschwert möglich.
- *DNS Port*: Rechner und Netzwerke in den aktivierten Netzwerkgruppen dürfen DNS-Anfragen stellen.

  Im Unterschied zu den *rekursiven Anfragen* ist über diese Berechtigung nur der Zugriff auf lokal verwaltete Zonen möglich.

11.3.1.3 Tab *Optionen*, Abschnitt *Optionen*

Felder in diesem Abschnitt

- *Anfragen weiterleiten*: Ein Nameserver kann zur Auflösung fremder Zonen entweder alle Anfragen an einen übergeordneten Nameserver („Forwarder“) schicken oder die Auflösung selbst in die Hand nehmen. Dazu muss ausgehend von den Root-

Nameservern der zuständige Nameserver für die Zone ermittelt werden, der den gefragten Hostnamen oder die IP-Adresse auflösen kann.

Durch das Aktivieren dieser Option werden keine Root-Nameserver befragt. Stattdessen werden alle Anfragen an einen oder zwei feste Nameserver weitergeleitet.

- *Vom Provider übermittelten DNS-Server benutzen*: Für Wählverbindungen ins Internet besteht die Möglichkeit, den vom Provider übermittelten DNS-Server für die Namensauflösung zu benutzen. Hier wird die Option aktiviert, wenn der übermittelte Provider-DNS-Server als Forwarder benutzt werden soll.
- *Link*: Hier ist die Verbindung auszuwählen, über die der DNS-Server des Providers übermittelt wird.
- *Forwarder*: Hier wird die IP-Adresse des Nameservers eingetragen, an den die Anfragen weitergeleitet werden.
- *Alternativer Forwarder*: Hier kann ein zweiter, alternativer Nameserver eingetragen werden. Dieser wird befragt, wenn der erste Forwarder nicht antwortet.
- *Ignoriere Adressen in 'Root'-Zonen*: Manche Betreiber von „Root-Nameservern" antworten auf Anfragen nach unbekannten Domains mit einer IP-Adresse und leiten so die Verbindungen auf diesen Server um. Oft handelt es sich dabei um eine Werbeseite für DNS-Dienstleistungen.

  Meist ist die Ursache für das Abfragen einer falschen Domain jedoch, dass sich ein Benutzer bei der Eingabe einer E-Mail-Adresse oder einer URL vertippt hat. Durch diese Umleitung auf eine andere Seite können vertrauliche Daten wie Passwörter oder E-Mails in falsche Hände geraten. Zudem führt es zu Verwirrung, wenn statt der angeforderten Seite plötzlich eine ganz andere erscheint.

  Durch das Aktivieren dieser Option werden solche Umleitun-

gen ignoriert. Ein Root-Nameserver kann dann nur noch auf einen anderen Nameserver verweisen.

11.3.2 *Vorwärtszonen*

Eine Zone umfasst in etwa alle DNS-Einträge einer einzelnen Domain. Im Gegensatz dazu sorgt eine „Rückwärtszone“ für die Auflösung von IP-Adressen in Hostnamen.

Es können auch Zonen angelegt werden, die nicht auf diesem System selbst, sondern auf einem anderen System verwaltet werden. Dies wird oft zur Einbindung einer ADS-Domäne genutzt.

11.3.2.1 *Zone auswählen*

(Dieser Dialog befindet sich unter *Netzwerk – DNS – Vorwärtszonen*)

In dieser Übersicht werden die angelegten Vorwärtszonen angezeigt. Hier können neue Zonen angelegt und vorhandene bearbeitet oder gelöscht werden.

Felder in diesem Dialog

- *Typ*: Hier wird die Art der Zone angezeigt.
- *Domain*: Hier steht der Name der Zone.
- *Kommentar*: Hier steht der Kommentartext zu der Zone.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird die Zone bearbeitet.
- *Löschen*: Mit dieser Aktion wird die Zone gelöscht.

Aktionen für diesen Dialog

- *Hinzufügen*: Mit dieser Aktion wird eine neue DNS-Zone angelegt.

11.3.2.2 *Vorwärtszone bearbeiten*

(Dieser Dialog befindet sich unter *Netzwerk – DNS – Vorwärtszonen*)
In diesem Dialog wird die Konfiguration einer Zone bearbeitet.

Tab *Grundeinstellungen*
Felder in diesem Abschnitt

- *Domain*: Beim Anlegen einer neuen Zone wird hier die Domain angegeben, für die eine Zonenkonfiguration erstellt werden soll.
- *Domain*: Wird eine Zone bearbeitet, wird hier die Domain nur angezeigt. Sie kann nicht geändert werden.
- *Kommentar*: Hier kann ein Kommentartext eingegeben werden.
- *Dieses System ist*: Hier wird eingestellt, wie die Zone auf diesem System verwaltet wird.

  Wird dieses System zum *Master* der Zone, werden alle Einträge innerhalb der Zone auf diesem System verwaltet. Zusätzlich eingetragene sekundäre Slave-Server werden automatisch bei Änderungen der Daten informiert.

  Ist das System ein *Slave*, werden die Einträge in der Zone von einem *Master* geholt. Dieses System arbeitet nur als „Backup-System“ für die Zone. Dabei versucht es, einen „Zonentransfer“ durchzuführen, der von dem Master erlaubt werden muss.

  Wird hier *Forwarder* eingestellt, werden alle Anfragen zur Domain an diesen Forwarder geschickt. Im Unterschied zum Slave wird hier kein Transfer der ganzen Zone durchgeführt, sondern es werden nur die angefragten Einträge weitergeleitet.

Die Einstellung *Parent* ist notwendig, wenn die Zone selbst auf einem anderen DNS-Server verwaltet wird und dieses System gleichzeitig für die übergeordnete Zone zuständig ist. Dann muss auf dem System ein Verweis auf den oder die Nameserver dieser „Subdomain" vorhanden sein.

- *IP-Adresse des primären DNS-Servers*: Hier wird die IP-Adresse des zuständigen Nameservers für die Zone angegeben.
- *IP-Adresse des sekundären DNS-Servers*: Hier kann ein zusätzlicher Nameserver angegeben werden, der bei einem Ausfall des ersten DNS-Servers die Namensauflösung übernimmt.
- *Auto MX*: Wenn diese Option aktiviert ist und eine lokale Maildomain existiert, deren Name mit dem Namen dieser Zone übereinstimmt, wird der angegebene Mailserver und/oder dieses System als MX („Mail-Exchanger") eingetragen.

  Bleibt diese Option deaktiviert, können die MX-Einträge manuell vorgenommen werden.
- *Hidden Primary*: Normalerweise trägt sich der Master einer Zone selbst in die Zone als zuständiger DNS-Server ein. Wenn als verantwortliche Nameserver allerdings zwei andere Systeme genutzt werden (etwa zwei Server bei einem Provider), sollten diese in den Zonendaten aufgeführt werden und dieses System selbst entfallen.

  Durch das Aktivieren dieser Option wird genau dies erreicht. Das lokale System verwaltet als primärer Server die Zonendaten, trägt aber zwei andere Systeme in die Zonendaten ein.

Tab *Sekundäre DNS-Server*, Abschnitt *Sekundäre DNS-Server* Spalten in der Tabelle

- *IP-Adresse*: Hier wird die IP-Adresse des sekundären DNS-Servers angegeben. Diese Angabe sorgt dafür, dass der sekundäre Server

über Änderungen an den Zonendaten informiert wird und erlaubt ihm, eine Kopie der kompletten Zonendatei anzufordern.

- *FQDN*: Hier wird der vollständige Name (inklusive Domain-Suffix) des sekundären DNS-Servers angegeben.

  Hinweis: Wird der Name des Servers nicht angegeben, wird er auch nicht als Nameserver in die Zone eingetragen, er erhält jedoch weiterhin Informationen über Änderungen und kann Zonentransfers durchführen. Dies kann für spezielle Konfigurationen sinnvoll sein, im Allgemeinen sollte der Name jedoch angegeben werden.

Aktionen für jeden Tabelleneintrag

- *Löschen*: Mit dieser Aktion wird der zusätzliche sekundäre DNS-Server gelöscht.

Arbeitet das System als primärer DNS-Server für die Zone, können sekundäre Nameserver angelegt werden. Diese werden in die Zonendaten als zuständige Nameserver aufgenommen und erhalten die Berechtigung, einen „Zonentransfer“ durchzuführen. Bei Änderungen der Zoneneinträge werden sie von diesem System informiert.

Aktionen für diesen Dialog

- *Sekundären DNS-Server hinzufügen*: Mit dieser Aktion wird ein zusätzlicher sekundärer DNS-Server angelegt.

Tab *MX-Einträge*, Abschnitt *MX-Einträge (Mailrouting)* Spalten in der Tabelle

- *Host*: Hier wird der Name des Mailservers angegeben, der für diese Zone zuständig ist.

- *Wildcard*: Wird diese Option aktiviert, gilt dieser Eintrag auch für alle Subzonen.
- *Priorität*: Hier wird die Priorität angegeben, mit der der Nameserver verwendet werden soll. Niedrigere Zahlenwerte bedeuten eine höhere Priorität.

Aktionen für jeden Tabelleneintrag

- *Löschen*: Löscht den jeweiligen MX-Eintrag.

MX-Einträge in der Zone geben an, welcher Mailserver für E-Mails an Empfänger in dieser Domain zuständig ist. Dabei können auch mehrere Mailserver mit unterschiedlichen Prioritäten angegeben werden. Im Collax Security Gateway existiert mit der Option *Auto MX* ein Mechanismus, der MX-Einträge für auf dem System verwaltete Maildomains automatisch anlegt. Wird diese Option deaktiviert, können hier eigene MX-Einträge angelegt werden.

Aktionen für diesen Dialog

- *MX-Eintrag hinzufügen*: Diese Aktion legt einen neuen MX-Eintrag für diese Zone an.

Tab *SRV-Einträge*, Abschnitt *SRV-Einträge*
Spalten in der Tabelle

- *Dienst*: Hier wird der Dienst ausgewählt, für den ein SRV-Eintrag erstellt werden soll.
- *Host*: Hier wird der Name des Rechners angegeben, auf dem der Dienst läuft.
- *Priorität*: Hier wird die Priorität angegeben, mit der der Eintrag verwendet werden soll. Niedrigere Zahlenwerte bedeuten eine höhere Priorität.

- *Gewichtung*: Hier wird die Gewichtung angegeben, mit der dieser Eintrag verwendet werden soll. Wenn mehrere Einträge für einen Dienst mit gleicher Priorität vorhanden sind, erhält ein Server mit der höheren Gewichtung mehr Anfragen.

Aktionen für jeden Tabelleneintrag

- *Löschen*: Löscht den jeweiligen SRV-Eintrag.

SRV-Einträge sind ein weiterer Bestandteil des „zeroconf"-Systems. Über SRV-Einträge in der Zone können Authentifizierungsserver im Netz gefunden werden.

Hinweis: Werden mehrere Einträge für denselben Dienst in der Zone angegeben, müssen die entsprechenden Server auch den gleichen Datenstand haben. SRV-Einträge für die gesamte Zone sind nicht identisch mit den Einträgen, die für DNS-SD („DNS Service Discovery") benötigt werden.

Aktionen für diesen Dialog

- *SRV-Eintrag hinzufügen*: Mit dieser Aktion wird ein neuer SRV-Eintrag angelegt.

Tab *Extras*, Abschnitt *Zusätzliche Angaben*
Felder in diesem Abschnitt

- *Zusätzliche Angaben*: In diesem Eingabefeld können zusätzliche Einträge für die Zonendatei vorgenommen werden. Die Eingaben in diesem Feld werden hinter den SOA-Eintrag der Zonendatei kopiert.

  Hinweis: Fehlerhafte Einträge in diesem Feld können den Start des Nameservers verhindern.

- *Datei*: Alternativ zum Eingabefeld kann für den eigenen Konfigurationsabschnitt auch eine Datei importiert werden.

Aktionen für diesen Dialog

- *Importieren*: Mit dieser Funktion wird der Import der Konfiguration gestartet.

11.3.3 *Rückwärtszonen*

(Dieser Dialog befindet sich unter *Netzwerk – DNS – Rückwärtszonen*)

Eine „Rückwärtszone“ dient dazu, IP-Adressen in Hostnamen aufzulösen. Dazu wird die Domain „in-addr.arpa“ verwendet. Die Konfiguration einer „Reverse-Zone“ ist daher in vielen Belangen identisch mit einer normalen Zone.

Hinweis: Eine funktionierende Rückwärtsauflösung von IP-Adressen in Hostnamen sind im Internet für manche Dienste essenziell wichtig.

11.3.3.1 *Zone auswählen*

(Dieser Dialog befindet sich unter *Netzwerk – DNS – Rückwärtszonen*)

In diesem Dialog werden die angelegten Rückwärtszonen angezeigt und können bearbeitet werden. Weitere Zonen können angelegt werden.

In dieser Tabelle werden die angelegten Rückwärtszonen angezeigt.

Felder in diesem Dialog

- *Typ*: Hier wird die Art der Zone angezeigt.
- *Netzwerk*: Hier wird der Name des Netzwerks angezeigt, das zur Rückwärtszone gehört.
- *Kommentar*: Hier wird ein Kommentartext zu der Zone ausgegeben.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird die Zone bearbeitet.
- *Löschen*: Mit dieser Aktion wird die Zone gelöscht.

Aktionen für diesen Dialog

- *Hinzufügen*: Mit dieser Aktion wird eine neue Rückwärtszone angelegt.

11.3.3.2 *Rückwärtszone bearbeiten*

(Dieser Dialog befindet sich unter *Netzwerk – DNS – Rückwärtszonen*)

In diesen Dialogen werden die Einstellungen für die Rückwärtszonen vorgenommen.

Tab *Grundeinstellungen*
Felder in diesem Abschnitt

- *Netzwerk*: Hier wird das Netzwerk ausgewählt. Dabei stehen nur Netze zur Verfügung, die als Netzwerk auf dem System angelegt sind.

- *Netzwerk*: Wird eine Zone bearbeitet, wird das Netzwerk nur angezeigt. Es kann nicht mehr geändert werden.
- *Kommentar*: Hier kann ein Kommentartext zu der Zone angegeben werden.
- *Dieses System ist*: Hier wird eingestellt, wie die Zone auf diesem System verwaltet wird:

  Wird dieses System zum *Master* der Zone, werden alle Einträge innerhalb der Zone auf diesem System verwaltet. Zusätzlich eingetragene sekundäre Slave-Server werden automatisch bei Änderungen der Daten informiert.

  Ist das System ein *Slave*, werden die Einträge in der Zone von einem *Master* geholt. Dieses System arbeitet nur als „Backup-System“ für die Zone. Dabei versucht es, einen „Zonentransfer“ durchzuführen, der von dem Master erlaubt werden muss.

  Wird hier *Forwarder* eingestellt, werden alle Anfragen zur Domain an diesen Forwarder geschickt. Im Unterschied zum Slave wird hier kein Transfer der ganzen Zone durchgeführt, sondern es werden nur die angefragten Einträge weitergeleitet.

  Die Einstellung *Parent* ist notwendig, wenn die Zone selbst auf einem anderen DNS verwaltet wird und gleichzeitig dieses System für die übergeordnete Zone zuständig ist. Dann muss auf dem System ein Verweis auf den oder die Nameserver dieser „Subdomain“ vorhanden sein.
- *Primärer DNS-Server*: Hier wird die IP-Adresse des zuständigen Nameservers für die Zone angegeben.
- *Sekundärer DNS-Server*: Hier kann ein zusätzlicher Nameserver angegeben werden, der bei einem Ausfall des ersten DNS die Namensauflösung übernimmt.
- *Hidden Primary*: Normalerweise trägt sich der Master einer Zone selbst in die Zone als zuständiger DNS-Server ein. Wenn als verantwortliche Nameserver allerdings zwei andere Systeme

genutzt werden (etwa zwei Server bei einem Provider), sollten diese in den Zonendaten aufgeführt werden und dieses System selbst entfallen.

Durch das Aktivieren dieser Option wird genau dies erreicht: Das lokale System verwaltet als primärer Server die Zonendaten, trägt aber zwei andere Systeme in die Zonendaten ein.

Tab *Sekundäre DNS-Server*, Abschnitt *Sekundäre DNS-Server*

Spalten in der Tabelle

- *IP-Adresse*: Hier wird die IP-Adresse des sekundären DNS-Servers angegeben. Der sekundäre Server wird über Änderungen an den Zonendaten informiert und darf eine Kopie der kompletten Zonendatei anfordern.
- *FQDN*: Hier wird der vollständige Name (inklusive Domain-Suffix) des sekundären DNS-Servers angegeben.

  Hinweis: Wird der Name des Servers nicht angegeben, wird er nicht als Nameserver in die Zone eingetragen. Er erhält jedoch weiterhin Informationen über Änderungen und kann Zonentransfers durchführen. Dies kann für spezielle Konfigurationen sinnvoll sein, im Allgemeinen sollte der Namen jedoch angegeben werden.

Aktionen für jeden Tabelleneintrag

- *Löschen*: Mit dieser Aktion wird der zusätzliche sekundäre DNS-Server gelöscht.

Aktionen für diesen Dialog

- *Sekundären DNS hinzufügen*: Mit dieser Aktion wird ein zusätzlicher sekundärer DNS-Server angelegt.

Tab *Extras*, Abschnitt *Zusätzliche Angaben*
Felder in diesem Abschnitt

- *Zusätzliche Angaben*: In diesem Eingabefeld können zusätzliche Einträge für die Zonendatei vorgenommen werden. Die Eingaben in diesem Feld werden hinter den SOA-Eintrag der Zonendatei kopiert.

  Hinweis: Fehlerhafte Einträge in diesem Feld können den Start des Nameservers verhindern.
- *Datei*: Alternativ zum Eingabefeld kann für den eigenen Konfigurationsabschnitt auch eine Datei importiert werden.

Aktionen für diesen Dialog

- *Importieren*: Mit dieser Funktion wird der Import der Konfiguration gestartet.

11.3.4 *Hosts*

Als „Host“ werden einzelne Rechner bezeichnet, die dem Collax Security Gateway bekannt sind. Im einfachsten Fall muss nur die IP-Adresse eingetragen werden. Damit kann ein Host in den DNS eingetragen, überwacht oder in den *Benutzungsrichtlinien* einer Gruppe zugeordnet werden. Wird zusätzlich die MAC-Adresse angegeben, kann der Host mit DHCP seine IP-Adresse beziehen.

Wenn unter *Systembetrieb* die *passive Netzwerküberwachung* aktiviert wurde, kann in diesem Dialog über *Hosts importieren* eine Liste aller aktiven Systeme im Netz erstellt werden. Diese Systeme müssen zwar einzeln *bestätigt* werden, die aktuelle IP-Adresse sowie die MAC-Adresse sind allerdings bereits eingetragen.

11.3.4.1 *Übersicht*

In dieser Liste werden alle dem System bekannten Hosts im lokalen Netz angezeigt.

Felder in diesem Formular

- *FQDN*: Hier wird der vollständige Domainname angezeigt.
- *Kommentar*: Hier wird der Kommentartext angezeigt.
- *IPv4-Adresse*: Die IPv4-Adresse des Hosts.
- *MAC-Adresse*: Hier wird die Netzwerk-MAC-Adresse angezeigt.
- *Netzwerkgruppe*: Hier wird die ausgewählte Netzwerkgruppe angezeigt.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion können die Einstellungen zu einem Host bearbeitet werden.
- *Löschen*: Mit dieser Aktion wird ein Host gelöscht.

Aktionen für dieses Formular

- *Hosts importieren*: Mit dieser Aktion werden alle derzeit aktiven Systeme im Netz, die von der passiven Netzwerküberwachung

gefunden werden, in die angezeigte Liste importiert. Sie sind zunächst nicht *bestätigt* und müssen manuell übernommen werden.
- *Hinzufügen*: Mit dieser Aktion wird ein neuer Eintrag für einen Host erzeugt.

11.3.4.2 *Host bearbeiten*

In diesem Dialog werden die Einstellungen zu einem einzelnen System bearbeitet.

Tab *Grundeinstellungen*, Abschnitt *Grundeinstellungen*
Felder in diesem Abschnitt

- *FQDN*: Hier wird der vollständige Name der Domain angegeben. Wenn nur ein Hostname gewünscht ist muss ein Punkt am Ende angehängt werden, sonst wird die Domain automatisch angehängt.
- *Netzwerkgruppe*: Hier wird der Host einer Netzwerkgruppe zugeordnet.
- *IPv4-Adressen*: Wenn dem Host eine bestimmte IPv4-Adresse zugewiesen werden soll, muss diese hier eingetragen werden. Bleibt das Feld leer und fragt der Host mit der passenden MAC-Adresse per DHCP an, bekommt er als Antwort eine IP-Adresse aus einem DHCP-Pool.

Tab*DNS & MAC*,Abschnitt*DNS*
Felder in diesem Abschnitt

- *TTL*: Zeitspanne in Sekunden, für die die Angaben gültig sein sollen. Clients dürfen Anfragen für diese Zeit zwischenspeichern, ohne beim Server nochmals anzufragen. Wird hier nichts oder 0 (Null) angegeben, wird als Voreinstellung der Wert 86400 s (ein Tag) eingesetzt.
- *Aliasnamen*: Wenn der Rechner unter weiteren Namen bekannt sein soll, können diese, durch Leerzeichen getrennt, hier eingegeben werden. Endet der Name mit einem Punkt „.“, wird er als FQDN aufgefasst und in der entsprechenden Zone eingetragen, andernfalls wird der Name um die Zone erweitert.

  Wenn beispielsweise der Rechner „web01“ in der Zone „example.com“ angelegt wurde und der Alias „www“ gesetzt wurde, wird der Name zu „www.example.com“ erweitert.

  Aliase werden nur in den Zonen eingetragen, die als *Master* konfiguriert sind. Mehrere Namen werden durch Leerzeichen getrennt.

Tab*DNS & MAC*, Abschnitt*Ethernet*
Felder in diesem Abschnitt

- *MAC-Adressen*: In diesem Feld wird die MAC-Adresse der Netzwerkschnittstelle angegeben.

Tab*Netzwerktests*, Abschnitt*Netzwerktests*
Felder in diesem Abschnitt

- *Alarmierungszeitraum*: In dieser Liste kann der Zeitraum ausgewählt werden, in dem die unten angegebenen Tests durchgeführt

werden und einen Alarm auslösen. Dies ist nützlich, wenn das System nur zu bestimmten Zeiten eingeschaltet ist, etwa während der Bürozeiten.

Bleibt das Feld leer, wird die Einstellung der zu alarmierenden Gruppe benutzt.

- *Erreichbar über*: Ist das System über ein anderes System, etwa einen Router, erreichbar, kann hier dieser andere Host ausgewählt werden. Bei einem Ausfall des anderen Hosts wird für dieses System keine Überprüfung mehr durchgeführt und kein Alarm ausgelöst. Es wechselt in den Zustand „unbekannt“. Bei Rückkehr des anderen Hosts werden die Tests für dieses System wieder aufgenommen. *Nagios* nutzt diese Information außerdem zur Darstellung der Netzwerkkarte.

  Bleibt das Feld leer, wird versucht, anhand der Routinginformationen den richtigen Router für den Rechner zu finden. Dies funktioniert allerdings nur, wenn der Host lediglich über einen einzigen anderen Router erreicht werden kann.

  Wenn jedoch mehrere Router zwischen diesem System und dem Host liegen, sollte hier der letzte bekannte „Hop“ zum gewünschten Host angegeben werden. Wenn der Host „X“ über die Strecke „A“ – „B“ – „C“ erreichbar ist, muss hier „C“ angegeben werden. Für „C“ kann ebenfalls eine Überwachung angelegt werden, „C“ ist dann über „B“ erreichbar.

Tab *Netzwerktests*, Abschnitt *Test*
Felder in diesem Abschnitt

- *Dienst*: Hier wird der jeweilige Dienst angezeigt, der überwacht werden kann.
- *Port*: Hier kann die Portnummer angegeben werden, auf der der Dienst geprüft werden soll. Dies ist wichtig, wenn ein Dienst nicht auf dem gewöhnlichen Port läuft.

- *Host*: Hier kann eine gesonderte IP-Adresse angegeben werden, auf der der Dienst geprüft werden soll.
- *URL*: Hier kann eine URL angegeben werden, die bei der Überprüfung abgefragt werden soll.
- *Benutzer*: Bei Diensten, die eine Authentifizierung erfordern, kann hier das Login angegeben werden.
- *Passwort*: Hier wird das zugehörige Passwort für die Authentifizierung an einem Dienst angegeben.
- *Parameter*: Für Tests für die Fernüberwachung über NRPE kann hier der entsprechende Testparameter angegeben werden. Mit dem Parameter „-c Mailqueue“ kann als Beispiel die Anzahl der E-Mails in der E-Mail-Warteschlange eines entfernten Collax-Servers überprüft werden.
- *Prozess*: Sollen Prozesse eines Microsoft Windows-Betriebssystems geprüft werden, ist hier der entsprechende ausführbare Prozess anzugeben.

Für jeden Rechner können die Dienste angegeben werden, die auf ihre Funktionsfähigkeit hin überwacht werden sollen. Diese Dienste werden dann regelmäßig kontaktiert. Wird ein Dienst als nicht mehr funktionsfähig erkannt, wird ein Alarm ausgelöst.

Die Überwachung funktioniert nur für Rechner, die eine feste IP-Adresse haben.

Die einzelnen Tests können nicht alle Aspekte eines bestimmten Dienstes überprüfen. Wenn beispielsweise der Test für den Dienst SMTP aktiviert ist, wird geprüft, ob eine Verbindung zum Mailserver hergestellt werden kann und ob der Server eine sinnvolle Antwort liefert, es wird jedoch nicht versucht, tatsächlich eine E-Mail zu versenden. Es kann also grundsätzlich vorkommen, dass der Dienst nicht funktioniert, obwohl der Test erfolgreich war.

Tab*DHCP*, Abschnitt*DHCP*
Felder in diesem Abschnitt

- *DHCP-Pool*: Soll dem System eine IP-Adresse automatisch zugewiesen werden, muss hier der Pool ausgewählt werden, aus dem eine IP-Adresse verwendet werden soll.

  Hinweis: Bleibt dieses Feld leer, kann die IP-Adresse nicht automatisch zugewiesen werden.
- *DHCP-Optionsgruppe*: Spezielle Optionen für DHCP können angegeben werden, indem Optionen für eine Gerätegruppe definiert werden und diese Gruppe hier ausgewählt wird.

Aktionen für dieses Formular

- *Schließen*: Dieser Aktion führt zurück zur Übersicht. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten der Hostkonfiguration beenden. Die Änderungen werden gespeichert.

11.3.5 *Dynamische DNS-Namenszuweisung*

Normalerweise wird einer IP-Adresse ein Hostname fest zugeordnet und in der DNS-Datenbank eingetragen. Über diesen Hostnamen ist das System zukünftig erreichbar. Dieser Weg ist jedoch nicht möglich, wenn die Anbindung ans Internet über eine Leitung erfolgt, auf der bei jeder Einwahl eine neue, andere IP-Adresse zugewiesen wird („dynamische IP-Adresse“). Da die jeweils aktuelle IP-Adresse für Außenstehende unbekannt ist, kann sie weder dauerhaft im DNS eingetragen werden, noch kann von außen auf das System zugegriffen werden.

Eine einfache Möglichkeit zur Lösung dieses Problems ist die Verwendung eines dynamischen DNS-Providers. Dabei werden Nameserver genutzt, die eine sehr kurze Cache-Zeit in ihren Zonen verwenden. Abgerufene Daten von einem solchen Nameserver sind nur sehr kurze Zeit gültig. Wählt sich ein System ins Internet ein, baut es zunächst eine Verbindung zu einem solchen Provider auf. Der Provider „sieht“ die aktuelle IP-Nummer des Systems und trägt diese IP-Nummer in seinen DNS zu einem festgelegten Hostnamen ein. Wird von außen dieser Hostname abgefragt, liefert der Nameserver die aktuelle IP-Nummer zurück, und von extern kann eine Verbindung zu dem System aufgebaut werden.

11.3.6 GUI-Referenz: *Dynamisches DNS*

(Dieser Dialog befindet sich unter *Netzwerk – DNS – Dynamisches DNS*)

In diesem Dialog können mehrere dynamische DNS-Namen verwaltet werden. Dadurch ist es möglich, dynamische DNS-Namen über bestimmte Ethernet-Verbindungen oder bestimmte Einwahlverbindungen vom Typ DSL oder ISDN, beim gewählten DynDNS-Anbieter aktualisieren zu lassen.

Soll im einfachsten Fall ein DynDNS-Name über DSL-Einwahl aktualisiert werden, kann dies mit der Definition eines einzigen DynDNS-Eintrags erreicht werden.

Das Anlegen von mehreren DynDNS-Einträgen kann sinnvoll sein, wenn man weitere Verbindungen ins Internet als Alternativ-Routen bei Ausfall der Hauptverbindung benutzt. In diesem Fall kann ein und derselbe DynDNS-Name auf verschiedenen Verbindungen, angelegt werden. Die Option *Auf Link* wird jeweils unterschiedlich gesetzt. Dieser DynDNS-Name wird erst dann aktualisiert, sobald der angegebene Link aufgebaut wurde.

Können mehrere Internet-Verbindungen gleichzeitig benutzt werden, kann es sinnvoll sein, für die verschiedenen Verbindungen auch unterschiedliche DynDNS-Namen zu definieren und aktualisieren zu lassen.

11.3.6.1 Spalten in der Tabelle

- *Name*: Zeigt die interne Bezeichnung des dynamischen DNS-Kontos.
- *Anbieter (Protokoll)*: Zeigt den DynDNS-Anbieter bzw. das Protokoll, mit dem der DNS-Name mit der dynamischen IP-Adresse aktualisiert wird.
- *DynDNS-Name*: Zeigt den DNS-Namen, der über dieses Konto beim Anbieter aktualisiert wird.
- *Auf Link*: Hier wird angezeigt, über welche Netzwerkverbindung und mit welcher damit verbundenen IP-Adresse, der angegebene DynDNS-Name aktualisiert wird.
- *Aktiviert*: Zeigt an, ob die angegebenen Werte bei Bedarf aktualisiert werden.

11.3.6.2 Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird der gewählte Eintrag bearbeitet.
- *Deaktivieren*: Mit dieser Aktion im Kontextmenü kann die Aktualisierung des DynDNS-Namen im gewählten Konto deaktiviert werden.
- *Aktivieren*: Mit dieser Aktion im Kontextmenü kann die Aktualisierung des DynDNS-Namen im gewählten Konto aktiviert werden.

- *Löschen*: Mit dieser Aktion kann der gewählte Eintrag gelöscht werden.

11.3.6.3 Aktionen für dieses Formular

- *Hinzufügen*: Mit dieser Aktion kann ein weiteres DynDNS-Konto hinzugefügt werden.

11.3.7 *Dynamisches DNS bearbeiten*

11.3.7.1 Tab *Grundeinstellungen*

Felder in diesem Abschnitt

- *Name*: Hier wird ein interner Name des dynamischen DNS-Konto angezeigt oder eingegeben. Dieses Feld dient der Verwaltung.
- *Aktiviert*: Mit dieser Option kann die Aktualisierung des DynDNS-Namen aktiviert oder deaktiviert werden.
- *DynDNS-Name*: Hier wird der DNS-Name eingetragen, der auch beim Anbieter für dynamische Adressaktualisierung definiert wurde.
- *Anbieter (Protokoll)*: Aus dieser Liste wird der Anbieter bzw. das Protokoll ausgewählt, mit dem der DNS-Name mit der dynamischen IP-Adresse aktualisiert wird. Wird im Feld „Alternativ-Anbieter“ ein abweichender Anbieter eingetragen, wird dasselbe Protokoll wie beim ausgewählten verwendet. Viele Anbieter setzen dasselbe Protokoll wie DynDNS.org ein.
- *Registrierung bei*: Zu jedem Anbieter wird die URL der Webseite angezeigt, über die die Anmeldung erfolgen kann. Manche Angebote sind nur für private Zwecke kostenfrei, die Nutzungsbedingungen auf der Webseite des Anbieters klären darüber auf.

- *Alternativ-Anbieter*: Basierend auf ausgewähltem Anbieter kann in diesem Feld ein separater Anbieter-Server eingetragen werden, bei dem der Dyndns-Name mit der IP-Adresse aktualisiert wird. Die Angabe eines Ports ist optional. Bleibt dieses Feld leer, wird der ausgewählte Anbieter direkt verwendet. Wird ein Alternativ-Anbieter eingetragen, dient das Feld „Anbieter“ zur Auswahl des verwendeten DynDNS-Protokols. Viele Anbieter setzen dasselbe Protokoll wie DynDNS.org ein
- *Benutzername*: Hier wird der Benutzername eingegeben, mit dem die Anmeldung beim Anbieter erfolgt.
- *Passwort*: Hier wird das zugehörige Passwort angegeben.

11.3.7.2 Tab *Optionen*, Abschnitt *DynDNS-Optionen*

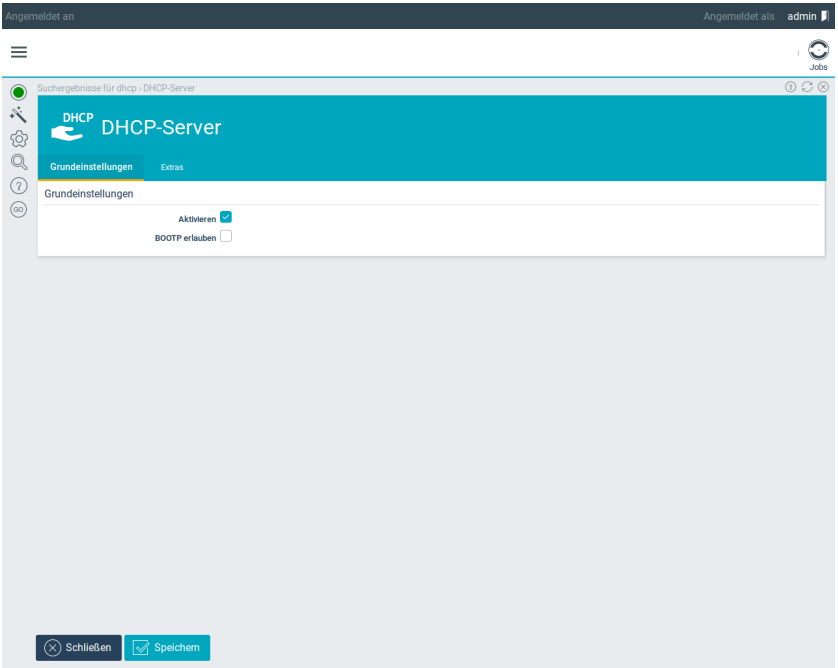
Felder in diesem Abschnitt

- *Auf Link*: Hier wird die Netzwerkverbindung ausgewählt, über den die Aktualisierung vorgenommen werden soll. Die IP-Adresse dieser Verbindung wird für die Auflösung des angegebenen DynDNS-Namen bei Anbieter hinterlegt.
- *Wildcard*: Durch das Aktivieren dieser Option wird ein Wildcard-Alias angelegt. Damit wird der ausgewählte DynDNS-Name als Subdomain betrachtet, und alle vorangestellten Hostnamen lösen auf die gleiche IP-Adresse auf. Wenn beispielsweise die Domain „lion.dns.example.com“ registriert wurde, wären bei aktiviertem Wildcard-Alias ebenfalls die Hostnamen „www.lion.dns.example.com“ und „wild.lion.dns.example.com“ existent und würden auf dieselbe IP-Adresse auflösen.
- *MX-Eintrag*: Hier kann der Mail-Exchanger (MX) hinterlegt werden, der die E-Mails für diese Domain annimmt. Soll der dynamische DNS-Dienst nur genutzt werden, um ein System zur Fernwartung

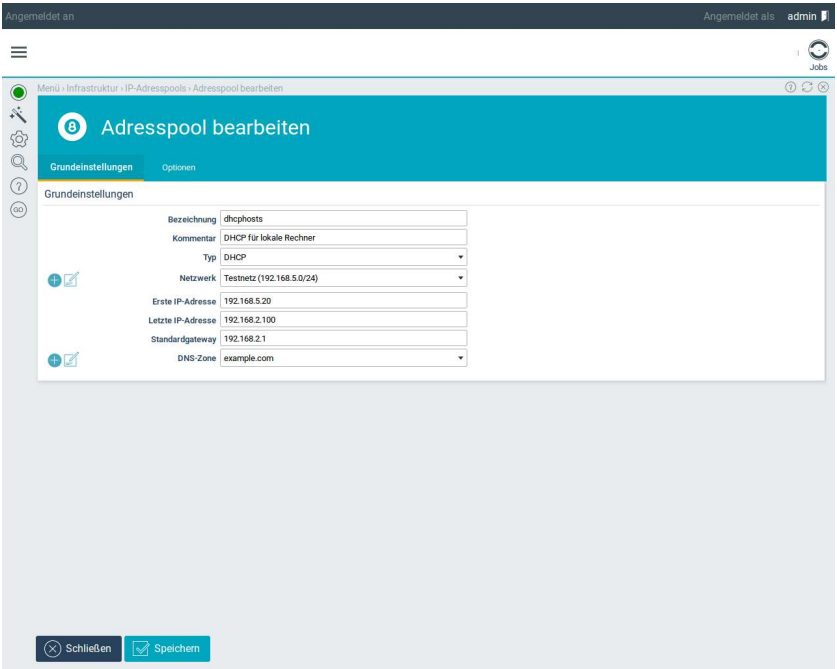
oder als VPN-Gateway anzusprechen, muss kein Mailsystem konfiguriert werden.

- *Url*: Hier wird eine Zeichenkette eingetragen, die als URL-Parameter gesendet wird. Diese Zeichenkette wird durch die Spezifikationen des Anbieterservers definiert. Im Normalfall kann das Feld leergelassen werden.

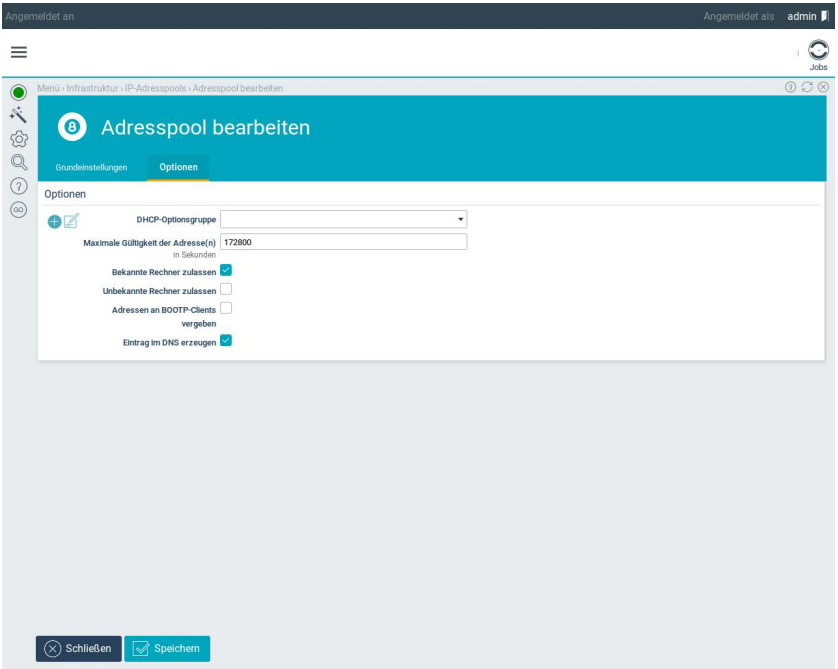
11.4 Schritt für Schritt: DHCP aktivieren



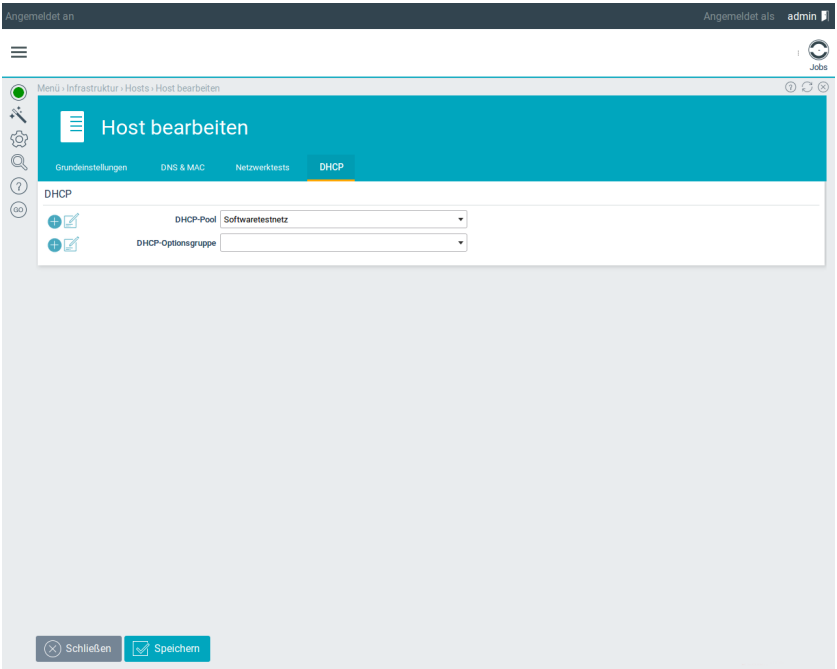
- Sie können den DHCP-Server unter *Netzwerk – DHCP – Allgemein* aktivieren.
- Die Option *BOOTP* wird nur benötigt, wenn Sie Systeme betreiben, die Ihr Betriebssystem über das Netzwerk booten. Lassen Sie sie daher zunächst deaktiviert.



- Wechseln Sie zu *Netzwerk – DHCP – IP-Adresspools*.
- Legen Sie einen neuen Pool an. Dabei handelt es sich um einen Adressbereich, aus dem der DHCP-Server IP-Adressen verteilen darf. Vergeben Sie keine IP-Adressen aus diesem Bereich manuell ohne Kenntnis des DHCP-Servers.
- Wählen Sie unter *Netzwerk* das *LocalNet* aus. Nur auf den Netzwerkschnittstellen, auf denen dieses Netz erreichbar ist, wird der Collax Security Gateway später DHCP-Anfragen beantworten.
- Mit der Angabe von *Erster* und *Letzter IP-Adresse* legen Sie den Bereich für den DHCP-Server fest.
- Unter *Standard-Gateway* geben Sie die IP-Adresse an, die per DHCP als Gateway an die Clients übermittelt wird.
- Unter *DNS-Zone* wählen Sie Ihre interne DNS-Zone aus.



- Wechseln Sie auf den Reiter *Optionen*.
- Aktivieren Sie die Option *Bekannte Rechner zulassen*, um später einzelnen Hosts immer die gleiche IP-Adresse zuweisen zu können.
- Haben Sie die Hosts im lokalen Netz noch nicht alle erfasst, aktivieren Sie den Eintrag *Unbekannte Rechner zulassen*. Aktivieren Sie dann auch *Eintrag im DNS erzeugen*.



- Um einzelne Systeme immer mit der gleichen IP-Adresse zu versorgen, muss die MAC-Adresse im Collax Security Gateway hinterlegt werden. Wechseln Sie dazu nach *Netzwerk – DNS – Hosts*.
- Wählen Sie ein System zur Bearbeitung aus oder legen Sie ein neues an.
- Wechseln Sie auf den Reiter *DHCP*.
- Wählen Sie hier den passenden *DHCP-Pool*.
- Geben Sie die *MAC-Adresse* des Systems ein.

Wenn Sie eine Anzahl von vorhandenen PCs erfassen möchten, können Sie unter *Überwachung – Passiv* die *Passive Netzwerküberwachung* aktivieren und nach einer gewissen Zeitspanne die Funktion *Hosts importieren* auslösen. Dadurch werden alle Systeme, die der

Collax Security Gateway auf seinen Netzwerkschnittstellen erkannt hat, als Vorschläge importiert. Sie müssen nur noch einzeln *bestätigt* werden, IP- und MAC-Adressen sind jedoch bereits ausgefüllt.

11.5 GUI-Referenz: DHCP

11.5.1 *DHCP-Server*

(Dieser Dialog befindet sich unter *Netzwerk – DHCP – Allgemein*)

Der DHCP-Server dient dazu, den Systemen im lokalen Netz beim Starten eine IP-Adresse zuzuteilen und die Netzwerkkonfiguration zu übermitteln.

11.5.1.1 Tab *Grundeinstellungen*, Abschnitt *Grundeinstellungen*

Felder in diesem Abschnitt

- *Aktivieren*: Durch das Aktivieren dieser Option wird der DHCP-Dienst auf diesem System gestartet.
- *BOOTP erlauben*: BOOTP ist der Vorläufer von DHCP, es gibt aber immer noch Clients, die dieses Protokoll benötigen. Mit dieser Option wird die Unterstützung für das BOOTP-Protokoll aktiviert.

11.5.1.2 Tab *Extras*, Abschnitt *Zusätzliche Angaben*

Felder in diesem Abschnitt

- *Zusätzliche Angaben*: In diesem Eingabefeld können zusätzliche Einträge vorgenommen werden, die an den Anfang der Konfigurationsdatei des DHCP-Dienstes eingefügt werden.

So können spezielle Optionen gesetzt werden, die über die Oberfläche nicht einstellbar sind.

Hinweis: Fehlerhafte Einträge in diesem Feld können den Start des DHCP-Dienstes verhindern.

- *Datei*: Alternativ zum Eingabefeld kann für den Konfigurationsabschnitt auch eine Datei importiert werden.

Aktionen für diesen Dialog

- *Importieren*: Mit dieser Funktion wird der Import der Konfiguration gestartet.

11.5.2 *IP-Adresspools*

(Dieser Dialog befindet sich unter *Netzwerk – DHCP – IP-Adresspools*)

Der DHCP-Dienst vergibt IP-Adressen nur aus festgelegten Bereichen, den sogenannten „IP-Adresspools“. Für jedes angelegte Netzwerk können Pools angelegt werden.

DHCP-Anfragen werden nur innerhalb eines Netzwerksegments verschickt. Aus anderen Netzwerken sind DHCP-Anfragen nur mit Zusatzmodulen auf dem jeweiligen Router möglich.

11.5.2.1 *Adresspool wählen*

(Dieser Dialog befindet sich unter *Netzwerk – DHCP – IP-Adresspools*)

In diesem Dialog werden die angelegten Pools angezeigt. Hier können neue Pools angelegt sowie bestehende bearbeitet oder gelöscht werden.

Felder in diesem Dialog

- *Bezeichnung*: Hier wird die Bezeichnung des Adresspools angezeigt.
- *Typ*: In diesem Feld wird die Art des Pools angezeigt. Der Typ *DHCP* gibt an, dass Adressen aus diesem Pool über DHCP vergeben werden. Der Typ „l2tp“ zeigt an, dass Adressen aus diesem Pool für L2TP-über-VPN-Verbindungen verwendet werden.
- *Kommentar*: Hier wird der Kommentartext zum Pool angezeigt.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird der Dialog zum Bearbeiten eines Pools geöffnet.
- *Löschen*: Diese Aktion löscht den ausgewählten Pool.
  Hinweis: Ein Pool kann nicht gelöscht werden, solange Clients noch IP-Adressen aus diesem Pool verwenden.

Aktionen für diesen Dialog

- *Adresspool anlegen*: Mit dieser Aktion wird ein neuer Pool von IP-Adressen angelegt.

11.5.2.2 *Adresspool bearbeiten*

(Dieser Dialog befindet sich unter *Netzwerk – DHCP – IP-Adresspools*)

In diesem Dialog werden die Einstellungen für einen Adresspool bearbeitet.

Tab *Grundeinstellungen*, Abschnitt *Grundeinstellungen* Felder in diesem Abschnitt

- *Bezeichnung*: Hier wird der Name des Pools eingegeben.
- *Bezeichnung*: Wird ein bereits vorhandener Pool bearbeitet, kann die Bezeichnung des Pools nicht mehr geändert werden. Hier wird die Bezeichnung nur angezeigt.
- *Kommentar*: In diesem Feld kann ein Kommentartext zu diesem Pool eingegeben werden.
- *Typ*: Hier wird festgelegt, welcher Dienst den Pool nutzen kann. Als Typen sind *DHCP* oder *L2TP/PPTP* möglich.
- *Netzwerk*: Hier muss das Netzwerk ausgewählt werden. Abhängig von den angelegten Links wird damit das Interface ausgewählt, auf dem auch die DHCP-Anfragen beantwortet werden.
- *Erste IP-Adresse*: Hier wird die erste IP-Adresse für diesen Adresspool angegeben.

  Wird hier keine Adresse angegeben, wird die kleinste mögliche Adresse verwendet.
- *Letzte IP-Adresse*: Hier wird die letzte IP-Adresse für diesen Adresspool angegeben.

  Wird hier keine Adresse angegeben, wird die größte mögliche Adresse verwendet.
- *Standardgateway*: Hier wird die Adresse des „Default-Gateways“ angegeben. Dieses wird per DHCP an die Clients übermittelt.

  Hinweis: Diese IP-Adresse muss im gleichen Subnetz liegen, aus dem die Adressen verteilt werden. Andernfalls können die Clients dieses Gateway nicht erreichen.
- *DNS-Zone*: Hier kann eine der DNS-Zonen ausgewählt werden, die in der Zonenkonfiguration angelegt sind.

  Diese Zone wird benötigt, um Rechnern mit dynamisch zugewiesenen Namen auch eine Domain zuordnen zu können. Auch

die zugewiesenen Nameserver werden aus der Zonendefinition übernommen.

Tab *Optionen*, Abschnitt *Optionen*
Felder in diesem Abschnitt

- *DHCP-Optionsgruppe*: Hier kann eine Optionsgruppe ausgewählt werden, die für diesen Pool verwendet wird. Über eine solche Optionsgruppe kann ein System über das Netzwerk einen *Kernel* mit Betriebssystem booten, etwa für plattenlose Clients.
- *Maximale Gültigkeit der Adresse(n)*: Mit diesem Parameter wird festgelegt, wie lange eine IP-Adresse aus diesem Pool höchstens gültig bleibt.
- *Bekannte Rechner zulassen*: Wird diese Option aktiviert, werden bekannten Rechnern (die als „Hosts“ angelegt sind) IP-Adressen aus diesem Pool zugewiesen.
- *Unbekannte Rechner zulassen*: Wird diese Option aktiviert, werden unbekannten Rechnern IP-Adressen aus diesem Pool zugewiesen.
- *Adressen an BOOTP-Clients vergeben*: Mit dieser Option werden IP-Adressen aus dem Pool an BOOTP-Clients vergeben.

  Hinweis: Adressen, die an BOOTP-Clients vergeben wurden, können nach Ablauf der maximalen Gültigkeitsdauer nicht zurückgezogen werden, da dies das BOOTP-Protokoll nicht vorsieht.
- *Eintrag im DNS erzeugen*: Wird diese Option aktiviert, wird für jede vergebene IP-Adresse ein Eintrag im Nameserver erzeugt.

11.5.3 *DHCP-Optionsgruppen*

(Dieser Dialog befindet sich unter *Netzwerk – DHCP – Optionsgruppen*)

In diesem Dialog können für Gruppen von Systemen oder für ganze Pools spezielle DHCP-Optionen angegeben werden.

11.5.3.1 *Optionsgruppe auswählen*

(Dieser Dialog befindet sich unter *Netzwerk – DHCP – Optionsgruppen*)

Felder in diesem Dialog

- *Bezeichnung*: Hier wird die Bezeichnung für die Optionsgruppe angezeigt.
- *Kommentar*: Hier wird der Kommentartext zu der Gruppe angezeigt.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird eine Optionsgruppe bearbeitet.
- *Löschen*: Diese Aktion löscht die Optionsgruppe.

Aktionen für diesen Dialog

- *Hinzufügen*: Mit dieser Aktion wird eine neue DHCP-Optionsgruppe hinzugefügt.

11.5.3.2 *DHCP-Optionsgruppe bearbeiten*

(Dieser Dialog befindet sich unter *Netzwerk – DHCP – Optionsgruppen*)

Tab *Grundeinstellungen*, Abschnitt *Grundeinstellungen* Felder in diesem Abschnitt

- *Bezeichnung*: Hier wird die Bezeichnung für die Gruppe angegeben.
- *Kommentar*: Hier kann ein Kommentartext zu dieser Gruppe angegeben werden.
- *TFTP-Server*: Hier wird die IP-Adresse des TFTP-Servers angegeben, von dem die Boot-Image-Datei geladen werden soll.
- *Boot-Image*: Hier muss der genaue Dateiname mit vollständigem Pfad zu der Boot-Image-Datei angegeben werden.
- *NFS-Root*: Als Boot-Image-Datei wird üblicherweise nur ein Betriebssystem-Kernel geladen. Um damit ein funktionsfähiges System zu erhalten, muss ein Dateisystem mit weiterer Software vorhanden sein. Bei Unix-/Linux-Systemen kann dieses Dateisystem über das Protokoll NFS über das Netzwerk eingebunden werden.

  In diesem Feld wird dazu der komplette NFS-Pfad angegeben. Wird kein Server vorangesetzt, wird das Verzeichnis auf diesem System gesucht. Um es von einem anderen Server zu verbinden, muss mit Doppelpunkt getrennt die IP-Nummer des NFS-Servers vorangestellt werden.

Tab *Extras*, Abschnitt *Zusätzliche Angaben*
Felder in diesem Abschnitt

- *Zusätzliche Angaben*: In diesem Eingabefeld können zusätzliche Einträge für diese Gerätegruppe vorgenommen werden. Die Eingaben in diesem Feld werden in die DHCP-Konfigurationsdatei eingefügt.

  Hinweis: Fehlerhafte Eingaben in diesem Feld können dazu führen, dass der DHCP-Server nicht mehr startet.

12 Webproxy

12.1 Einführung

Ein Webproxy-Server dient in erster Linie dazu, das Surfen im Internet zu beschleunigen. Er speichert jede übertragene Datei (Webseite, Schmuckbilder usw.) auf seiner Festplatte und kann bei erneutem Aufrufen einer Seite feststellen, welche Elemente sich auf dem Server geändert haben und welche Elemente er aus seinem Cache wiederverwenden kann. Dadurch entfällt der Download dieser Elemente über die Internetverbindung.

Um dies zu erreichen, muss der Webproxy in die Datenpakete hineinschauen, die HTTP-Steuerinformationen lesen und diese auswerten. Durch diesen Vorgang wird „nebenbei“ eine deutliche Sicherheitsverbesserung erreicht: Bei der Verwendung eines Webproxys ist es nur möglich, HTTP-Verbindungen aufzubauen. Versucht ein Client mit einem anderen Protokoll – beispielsweise SMTP für E-Mail – eine Verbindung zu einem vorgetäuschten Mailserver auf Zielport 80 (normal verwendet für HTTP) aufzubauen, kann eine einfache Firewall dies nicht verhindern. Ein Webproxy jedoch versteht kein SMTP und verwirft das ungültige Paket.

Einen weiteren Beitrag zur Sicherheit bietet der Webproxy, indem er die Anfrage eines Clients annimmt und bearbeitet. Sind die gewünschten Daten nicht in seinem Cache gespeichert, formuliert er eine neue HTTP-Anfrage an den Server. Auf diese Weise wird gewährleistet, dass immer regelkonforme HTTP-Pakete ins Internet geschickt werden.

In einem Setup mit dem Webproxy als Sicherheitsschleuse müssen

in der Firewall ausgehende Verbindungen vom lokalen Netz ins Internet für Zielport 80 (HTTP) geblockt werden. Deaktiviert ein User in seinem Browser den Webproxy, werden ihm keine Webseiten angezeigt.

12.1.1 Zugriff auf den Webproxy

Der Port, auf dem der Proxy angesprochen wird, ist seitens des Collax Security Gateways fest auf 3128 eingestellt. Dies muss zusammen mit der IP-Adresse des Webproxy im Browser konfiguriert werden.

Diese Einstellung kann automatisiert werden, indem im Browser bei der Proxy-Konfiguration ein automatisches Konfigurationsskript eingetragen wird. Dies ist nur vorhanden, wenn auf dem Collax Security Gateway neben dem Webproxy auch der Webserver aktiviert ist. Das Skript ist dann unter „http://Collax Security Gateway-Adresse/proxy.pac“ abrufbar. Statt „Collax Security Gateway-Adresse“ muss entsprechend der Hostname oder die IP-Adresse des Collax Security Gateways verwendet werden.

Bei Verwendung eines transparenten Proxys ist im Browser keine spezielle Konfiguration erforderlich. Der transparente Proxy kann in der *Firewallmatrix* für den *Dienst* HTTP aktiviert werden. Datenpakete zum Zielport 80 werden dann von der Firewall „abgefangen“ und an den Webproxy umgeleitet.

Auf Wunsch ist auch eine Authentifizierung möglich. Damit müssen die Benutzer bei jedem Neustart ihres Browsers die Frage des Webproxys nach Login und Passwort beantworten. Es ist möglich, hierfür lokale Benutzerkonten auf dem Collax Security Gateway oder Benutzerkonten eines Windows-Servers zu verwenden. Authentifizierung kann aus technischen Gründen nicht gemeinsam mit dem transpa-

rentem Proxy genutzt werden (der Webproxy erkennt die Firewall als Absender der Pakete).

12.1.2 Filtermöglichkeiten

Der Webproxy bietet sich als zentrale Stelle zum Filtern des HTTP-Datenverkehrs an. Eine einfache Möglichkeit ist das „Anonymisieren“ von HTTP-Paketen. Dadurch werden je nach Einstellung verschiedene Einträge im HTTP-Header entfernt, beispielsweise die Kennung des genutzten Browsers.

Durch aktivierte Anonymisierung kann es bei der Darstellung oder Verwendung von Webseiten zu Problemen kommen. Shopsysteme erkennen oftmals den Benutzer anhand eines hinterlegten „Cookies“ wieder und können seinen Warenkorb zuordnen. Andere Webseiten prüfen den Absender der Anfrage auf bestimmte installierte Browserversionen oder Plugins und zeigen ggf. eine Seite mit einem Hinweis, dass die eigentlich angeforderte Seite nicht dargestellt werden kann, weil zunächst eine bestimmte Software installiert werden müsse (die eigentlich vorhanden ist, deren Kennung jedoch gefiltert wird).

Eine andere Filtermöglichkeit ist der Schutz vor Viren. Da jede Datei durch den Webproxy heruntergeladen und danach an den Client geschickt wird, kann ein Virenfilter eingeschleift werden. Nur Dateien, bei denen kein Virus vorgefunden wurde, werden an den Client weitergegeben. Wird ein Virus erkannt, zeigt der Proxy stattdessen eine entsprechende Fehlermeldung.

Ein weiterer Filtermechanismus ist das Sperren bzw. Freigeben von bestimmten Webseiten. Diese als „Content-Filter“ bezeichnete Technik arbeitet mit umfangreichen Filterlisten, die in bestimmte Klassen zusammengefasst werden. So ist es etwa möglich, (weitgehend) alle Seiten der Kategorien „Pornographie“, „Raubkopien“ usw. zu sperren.

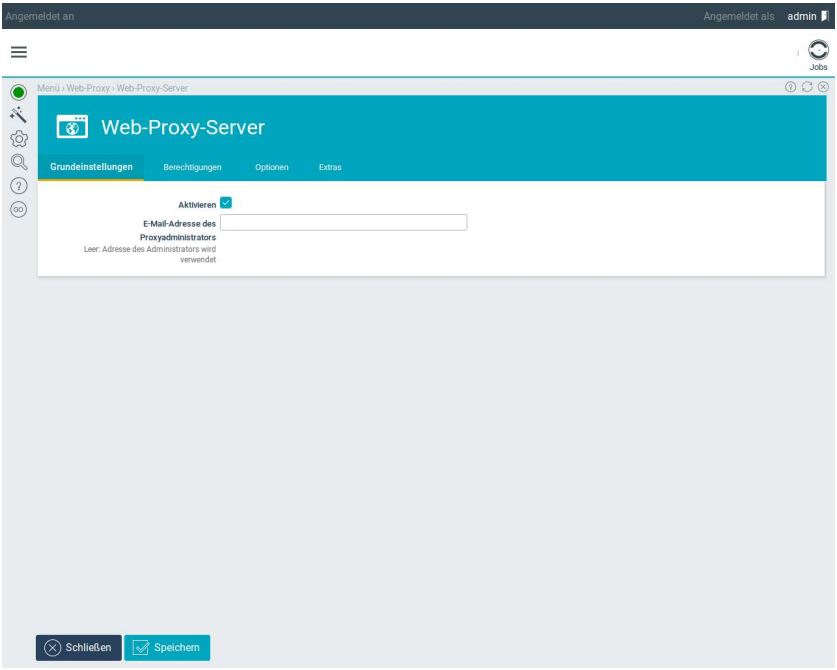
12.1.3 Verschlüsselte Inhalte

Wird die SSL-Verschlüsselung für den Zugriff auf Webseiten eingestellt, ist der Webproxy „ausgehebelt“. Er kann die Inhalte nicht in seinem Cache speichern, da sie speziell für einen Client verschlüsselt wurden – der Proxy kann die Inhalte also nicht lesen.

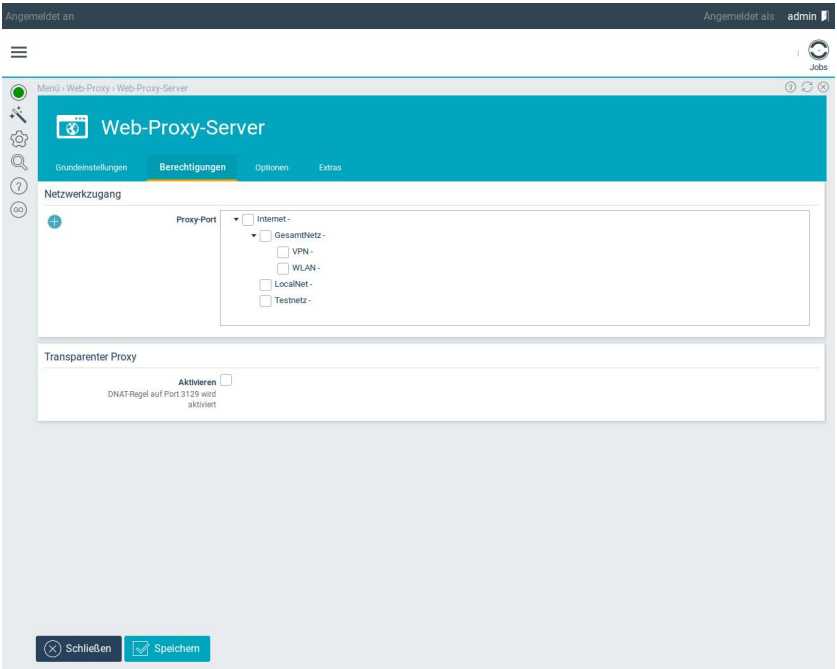
Werden Seiten mit HTTPS durch den Proxy abgerufen, kann er diese Anfragen und Antworten nur weiterreichen. Er muss dazu wissen, auf welchen Ports HTTPS-Übertragungen stattfinden. Das sind üblicherweise die Ports 443, 563 und 8443. Werden auf anderen Ports HTTPS-Pakete ausgetauscht, müssen diese Ports dem Collax Security Gateway bekannt gemacht werden. Dazu zählt z. B. die Administrationsoberfläche auf Port 8001.

Der Einsatz von Anonymisierung und Virenfilter ist bei HTTPS-Verbindungen nicht möglich. Es gibt zunehmend Seiten mit gefährlichen Inhalten, die verschlüsselt bereit gestellt werden. Dagegen hilft nur die Verwendung von Content-Filtern zum Sperren bestimmter Adressen.

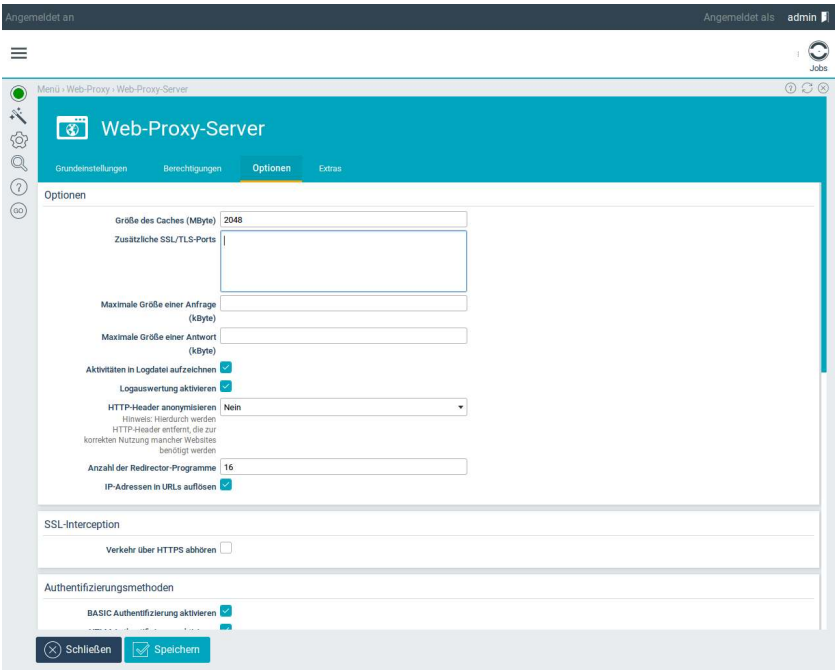
12.2 Schritt für Schritt: Webproxy einrichten



- Rufen Sie die Webproxy-Konfiguration unter *Netzwerk – Webproxy – Allgemein* auf.
- *Aktivieren* Sie den Webproxy.
- Im Feld *E-Mail-Adresse* können Sie eine Adresse eingeben, die den Benutzern in einer Fehlermeldung des Proxy-Servers angezeigt wird.



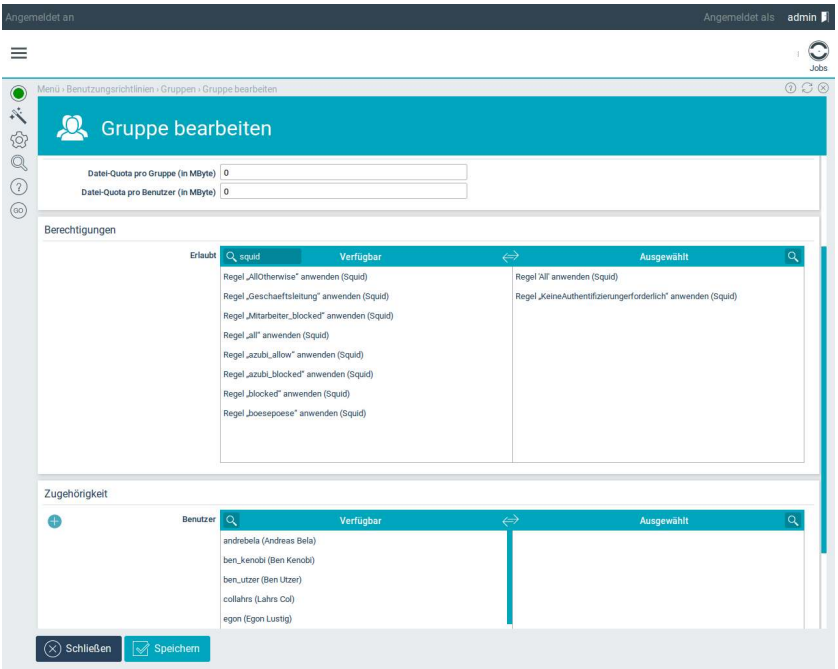
- Wechseln Sie auf den Reiter *Berechtigungen*.
- Nun können Sie die Gruppen auswählen, die ohne Authentifizierung Zugriff auf den Webproxy erhalten sollen.
- Sie können für den Zugriff auf den Webproxy eine eigene Gruppe anlegen. Wenn Sie das nicht möchten, aktivieren Sie hier die Gruppe *Users*.



- Wechseln Sie auf den Reiter *Optionen*. Es sind bereits sinnvolle Voreinstellungen vorgenommen worden.
- Unter *Größe des Caches* können Sie die Größe des auf der Platte maximal belegten Bereichs durch den Webproxy festlegen. Die Einstellung *1024* (1GB) ist für die meisten Anwendungen sinnvoll. Bedenken Sie, dass ein Cache ab einer gewissen Größe durch aufwendigere Zugriffe wieder langsamer wird.
- Unter *Zusätzliche SSL-Ports* können Sie weitere Ports angeben, auf denen Sie verschlüsselte HTTPS-Verbindungen betreiben. Tragen Sie hier *8001* ein, wenn Sie durch den Proxy einen Collax Security Gateway administrieren möchten.
- Aktivieren Sie *Aktivitäten in Logdatei aufzeichnen,* damit alle Zugriffe durch den Proxy protokolliert werden. Klären Sie ggf. im

Vorfeld, ob dies mit den gültigen Datenschutzrichtlinien für den Betrieb übereinstimmt.

- Falls Sie die Protokollierung einschalten, können Sie durch *Logauswertung aktivieren* eine statistische Auswertung der Logdaten erstellen lassen. Sie finden diese über den seitlichen Reiter *System* unter *Überwachung/Auswertung – Auswertungen – Webproxy*.



- Abschließend müssen Sie in den Benutzungsrichtlinien noch festlegen, welche Seiten durch die Benutzer besucht werden dürfen. Wechseln Sie hierfür zu *Benutzungsrichtlinien – Richtlinien – Gruppen*.
- Bearbeiten Sie die *Berechtigungen* Ihrer für den Webproxy genutzten Gruppe, hier die Gruppe *Users*.

- Öffen Sie die Kategorie *Squid*.
- Hier ist die vorhin in der Proxy-Konfiguration vorgenommene Einstellung zur Authentifizierung und eine Filterregel zu sehen.
- Aktivieren Sie die Filterregel *Regel All*. Sie erlaubt den Zugriff auf alle Webseiten. Wird sie nicht aktiviert, sind keinerlei Seiten erlaubt, d. h., alle Seiten sind gesperrt.

12.3 GUI-Referenz: *Web-Proxy-Server*

(Diese Option befindet sich im Zusatzmodul *Collax Web Security*)
(Dieser Dialog befindet sich unter *Netzwerk – Webproxy – Allgemein*)
In diesen Dialogen wird der Webproxyserver konfiguriert.

12.3.1 Tab *Grundeinstellungen*

12.3.1.1 Felder in diesem Abschnitt

- *Aktivieren*: Mit dieser Option wird der HTTP-Proxy aktiviert.
- *E-Mail-Adresse des Proxyadministrators*: Tritt ein Fehler auf, zeigt der Proxyserver eine Webseite mit einer Fehlermeldung an. Auf dieser Webseite wird die E-Mail-Adresse des lokalen Administrators angezeigt. Die Adresse wird in diesem Feld hinterlegt.

12.3.2 Tab *Grundeinstellungen*, Abschnitt *HTTPS-Anfragen*

Der Inhalt von verschlüsseltem HTTP-Traffic (HTTPS) kann üblicherweise nicht bewertet oder gefiltert werden, da eine Verschlüsselung zwischen Web-Server und Browser stattfindet. In diesem Abschnitt können Einstellungen vorgenommen werden, die es dem Web-Proxy ermöglichen sich in diesen verschlüsselten Traffic einzuklinken, um den Inhalt auf z.B. auf schadhafte Software oder ungewollten Inhalt zu untersuchen.

12.3.2.1 Felder in diesem Abschnitt

- *Abhören und entschlüsseln*: Um HTTPS-Traffic auf Inhalt oder auf schadhafte Software prüfen zu können, kann hier die Abhörfunktion eingeschaltet werden.

  Diese Option gilt auch für Seiten, die mit großer Wahrscheinlichkeit vertrauenswürdig sind, aber über die sicherheitsrelevante Informationen des Unternehmens übertragen werden, z.B. Online-Banking-Seiten oder ähnliches. Für solche HTTPS-Seiten ist es zu empfehlen, den HTTPS-Verkehr nicht abzuhören. Eine entsprechende Ausnahme kann mit der Option *Nur URLs/Domains filtern* einer speziellen Web-Proxy-Regel im Dialog *Web-Proxy – Regeln* gesetzt werden.
- *CA-Zertifikat ohne Passwort*: Damit der Web-Proxy den verschlüsselten Verkehr untersuchen kann, ist ein CA-Zertifikat erforderlich, welches vom Web-Proxy an den Browser geliefert wird. Dieses Zertifikat wird bei jeder HTTPS-Verbindung an den Browser weitergegeben. Das gewählte Zertifikat kann für die Benutzer zum Download im Benutzer-Webaccess des Collax Security Gateway zur Verfügung gestellt werden, und

anschließend auf den Client-PCs importiert werden, damit der Browser diesem Zertifikat automatisch vertraut. Eine Beispielanleitung für den Import unter Windows ist hier zu finden: http://www.augusta.de/Services/CA/cawin/ .

Die Verteilung dieses CA auf die Browser ist für die Netzwerke zwingend erforderlich, deren HTTPS-Verkehr gescannt werden soll, und deren Benutzer sich authentifizieren müssen.

Das CA-Zertifikat darf nicht mit einem Passwort gesichert sein.

- *SSL-Fehler ignorieren*: Hier können Domains von Webseiten angegeben werden, die ein ungültiges Zertifikat anbieten. Der Web-Proxy ignoriert diese Zertifikatsfehler.

12.3.3 Tab *Berechtigungen*, Abschnitt *Netzwerkzugang*

12.3.3.1 Felder in diesem Abschnitt

- *Proxy-Port*: Hier wird der Port für die Netzwerkgruppen freigeschaltet.

12.3.4 Tab *Berechtigungen*, Abschnitt *Transparenter Proxy*

12.3.4.1 Felder in diesem Abschnitt

- *Aktivieren*: Hier wird der Web-Proxy-Server als Transparenter Proxy aktiviert. Damit die Netzwerkgruppen auf den Transparenten Proxy zugreifen dürfen, muss der Proxy-Port für die jeweiligen Netzwerkgruppen freigegeben sein.
- *Anfragen nur von bestimmten Netzwerkgruppen akzeptieren*: Hier werden die Netzwerkgruppen ausgewählt für die der Proxy transparent gemacht werden soll.

12.3.5 Tab *Berechtigungen*,Abschnitt *Transparenter HTTPS Proxy*

Die Funktion des tranparenten HTTPS-Proxies ermöglicht es, Anfragen an HTTPS-Seiten zu filtern, ohne dass Internet-Anwender Umstellungen auf Clientseite vornehmen brauchen.

12.3.5.1 Felder in diesem Abschnitt

- *Aktivieren*: Hier wird der Web-Proxy-Server als Transparenter Proxy für SSL Verbindungen aktiviert. Damit die Netzwerkgruppen auf den Transparenten Proxy zugreifen dürfen, muss der Proxy-Port für die jeweiligen Netzwerkgruppen freigegeben sein.
- *Anfragen nur von bestimmten Netzwerkgruppen akzeptieren*: Hier werden die Netzwerkgruppen ausgewählt für die der Proxy transparent gemacht werden soll.

12.3.6 Tab *Optionen*, Abschnitt *Optionen*

12.3.6.1 Felder in diesem Abschnitt

- *Größe des Caches (MByte)*: Mit diesem Parameter wird die maximale Größe des Caches auf der Festplatte eingestellt. Dieser Wert sollte größer als 128 MByte sein. Der Maximalwert beträgt 10240 MB (10 GB). Je nach Geschwindigkeit des Plattensystems gibt es eine Grenze, bei deren Überschreitung der Cache langsamer wird. Übliche Werte liegen zwischen 512 MB und 2 GB.

  Hinweis: Hier wird nur der reine Zahlenwert in Megabyte (ohne Einheit) angegeben.
- *Zusätzliche SSL/TLS-Ports*: Der HTTP-Proxy kann prinzipbedingt

keine HTTPS-Anfragen cachen, da er die verschlüsselten Daten nicht lesen kann. Um dennoch HTTPS-Daten über den Proxy weiterleiten zu können, gibt es die Connect-Methode, mit der ein Client eine indirekte Verbindung zu einem HTTPS-Server aufnehmen kann.

Der HTTP-Proxy kann jedoch nicht prüfen, ob die Verbindung tatsächlich eine HTTPS-Verbindung ist. Darum sind für die Connect-Methode nur bestimmte Ports zugelassen, nämlich 443, 563 und 8443.

Hier können zusätzliche Ports angegeben werden, die für die Connect-Methode erlaubt sind. Zum Zugriff auf andere Collax-Server durch den Proxy muss hier etwa „8001“ zusätzlich eingetragen werden.

- *Maximale Größe einer Anfrage (kByte)*: Diese Einstellung gibt an, wie groß eine einzelne Anfrage an einen Webserver sein darf. Dies limitiert insbesondere die Größe von Dateien, die an einen Webserver geschickt werden können.

  In der Voreinstellung ist dieses Feld leer, wodurch die Größe von Anfragen nicht beschränkt ist.
- *Maximale Größe einer Antwort (kByte)*: Diese Einstellung begrenzt die maximale Größe einer Datei, die über den Proxy heruntergeladen werden kann.

  In der Voreinstellung ist dieses Feld leer, wodurch keine Größenbeschränkung existiert.

  Hinweis: Ein zu kleiner Wert kann verhindern, dass der Proxy antworten kann. Wenn eine Fehlermeldung des Proxys größer ist als die maximale Größe einer Antwort, erscheint keine Meldung bei einem Fehler. Aus diesem Grund werden Einträge, die kleiner als 10 kByte sind, auf 10 kByte gesetzt.
- *Aktivitäten in Logdatei aufzeichnen*: Wird diese Option aktiviert, werden alle Zugriffe in einer Logdatei protokolliert. In diesen

Logdateien werden Datum, Uhrzeit, IP-Nummer des Clients und die aufgerufene URL gespeichert. Ist die Benutzerauthentifizierung eingeschaltet, steht auch der Benutzername in der Logdatei.

Hinweis: Dabei handelt es sich um nutzerbezogene Daten, die gesetzlichen Bestimmungen und dem Datenschutz unterliegen können. Es ist möglich, dass geltende Gesetze die Protokollierung untersagen, so dass sie deaktiviert bleiben muss.

- *Logauswertung aktivieren*: Wird diese Option aktiviert, wird aus den Logdateien eine statistische Auswertung aufbereitet. Diese ist anonymisiert, d. h., es ist keine konkrete Zuordnung von URLs auf Nutzer möglich. Sehr wohl gibt es eine Aufschlüsselung des gesamten Traffics eines Nutzers oder eines Systems.
- *HTTP-Header anonymisieren*: Durch das Aktivieren dieser Option entfernt der Proxy bestimmte HTTP-Header aus den Anfragen, die er nach außen weiterreicht.

  Wird hier die Einstellung *ja* gewählt, werden die Header entfernt, die direkt Aufschluss über den Benutzer geben könnten. Dies sind:

  - From
  - Referer
  - Server
  - WWW-Authenticate
  - Link

  Die Auswahl *paranoid* entfernt auch Header, die nur dann Auskunft über den Benutzer geben können, wenn ein Webserver mehrere Anfragen vom gleichen Benutzer erhält. Dies sind:

  - Allow
  - Authorization
  - Cache-Control
  - Content-Encoding
  - Content-Length
  - Content-Type

- Date
- Expires
- Host
- If-Modified-Since
- Last-Modified
- Location
- Pragma
- Accept
- Accept-Charset
- Accept-Encoding
- Accept-Language
- Content-Language
- Mime-Version
- Retry-After
- Title
- Connection
- Proxy-Connection

Hinweis: Manche Webseiten sind nicht mehr oder nur eingeschränkt nutzbar, wenn diese Optionen aktiviert werden. Insbesondere die Einstellung *paranoid* kann zu Problemen führen, da dadurch auch die Kennung des verwendeten Browsers entfernt wird.

- *Anzahl der Redirector-Programme*: Hier wird die Anzahl der Prozesse angegeben, die der Webproxy zur Verarbeitung von URL-Anfragen startet. Das Redirect-Programm wird mehrfach gestartet, damit die eingehenden URLs zeitgleich abgearbeitet werden können. Die Anzahl kann erhöht werden, falls Anfragen verzögert abgearbeitet werden.

  Entsprechende Logmeldungen können mit der Angabe Programm „squid“ unter *System – Überwachung/Auswertung – Logdateien – System-Logdateien* eingesehen werden. Beispiel:

```
    Consider increasing the number of redirector processes
to at least ## in your config file.
```

- *IP-Adressen in URLs auflösen*: Die IP-Adressen werden dadurch in eine URL aufgelöst.

12.3.7 Tab *Optionen*, Abschnitt *Authentifizierungsmethoden*

12.3.7.1 Felder in diesem Abschnitt

- *BASIC Authentifizierung aktivieren*: Die einfachste Methode zur Authentifizierung von Benutzern ist die BASIC-Methode. Hiermit werden über ein Pop-Up des Web-Browsers die Benutzerinformationen abgefragt, wenn ein Benutzer über den Web-Proxy Internetseiten aufrufen will. An der Arbeitsstation sind keine weiteren Einstellungen erforderlich.
- *NTLM Authentifizierung aktivieren*: Diese Methode funktioniert nur, wenn der SMB/CIFS-Dienst aktiviert ist und kann verwendet werden, um Single-Sign-On mit älteren Betriebssystemen und Web-Browser zu bewerkstelligen. Entsprechende Arbeitsstationen müssen einer NT-Domäne oder AD beigetreten sein (gilt nicht für Windows Server 2008).
- *Kerberos Authentifizierung aktivieren (SPNEGO)*: Diese Methode ermöglicht es Windows-, Linux-, und Mac OS-Benutzern per Single-Sign-on in einem Kerberos-Realm am Web-Proxy anzumelden. Windows-Arbeitsstationen innnerhalb eines Active-Directory werden mit dieser Methode automatisch per Single-Sign-On authentifiziert.

12.3.8 Tab *Optionen*, Abschnitt *Parent-Proxy*

12.3.8.1 Felder in diesem Abschnitt

- *Parent-Proxy aktivieren*: Mit dieser Option wird die Nutzung eines Parent-Proxy eingeschaltet. Proxyserver können „in Reihe“ geschaltet werden. Der Client schickt die Anfrage an seinem Proxy im lokalen Netz und dieser Proxy fragt wiederum einen weiteren Proxyserver, etwa beim Provider. Der Parent-Proxy ist solch ein übergeordnetes System.
- *Parent-Proxy*: Hier wird die IP-Adresse des Parent-Proxy angegeben.
- *Port des Parent-Proxys*: Hier muss die Portnummer des Parent-Proxyservers angegeben werden. Der Squid-Webproxy verwendet meist Port 3128. Andere Proxys benutzen manchmal 8000 oder 8080.
- *Parent-Proxy als Fallback verwenden*: Die Aktivierung dieser Option sorgt dafür, dass der oben eingetragene Parent-Proxy als Fallback genutzt wird, wenn keine direkte Internetverbindung möglich ist. Dies ist natürlich nur sinnvoll, wenn sich der Parent-Proxy nicht im Internet befindet, sondern beispielsweise über das interne Interface erreichbar ist.

  Hinweis: Um diese Option nutzen zu können, ist es aus technischen Gründen notwendig, alle weiteren auf dem Collax Security Gateway selbst laufenden Parent-Proxys (insbesondere die Virenfilter) zu deaktivieren.
- *Authentifizierung für Parent-Proxy aktivieren*: Wenn der Parent-Proxy eine Authentifizierung verlangt, muss diese Option aktiviert werden.
- *Benutzername für Parent-Proxy*: Hier wird der Benutzername für die Authentifizierung am Parent-Proxy angegeben.
- *Passwort für Parent-Proxy*: Hier wird das Passwort für die Authentifizierung am Parent-Proxy angegeben.

12.3.9 Tab *Optionen*, Abschnitt *Proxy-Ausnahmen*

In diesem Abschnitt werden Netzwerke und Domains angegeben, für die der Proxy nicht verwendet werden soll.

Browser mit JavaScript-Unterstützung können automatisch für die Verwendung eines Proxys konfiguriert werden. Dazu muss in der Konfiguration des Browsers die URL einer JavaScript-Datei angegeben werden. Mit den Einstellungen in diesem Abschnitt wird die Konfigurationsdatei „proxy.pac“ erstellt und im Verzeichnis des Webservers abgelegt.

12.3.9.1 Felder in diesem Abschnitt

- *Keinen Proxy für Namen ohne Domain*: Wird diese Option aktiviert, wird kein Proxy verwendet, wenn keine Domain im Hostnamen enthalten ist, wenn also ein Server in der lokalen Domain angesprochen wird.
- *Keinen Proxy für folgende Domains*: Hier kann eine Liste von Domains angegeben werden, für die kein Proxy verwendet werden soll. Die Liste der Domains wird mit Leerzeichen getrennt.
- *Keinen Proxy für diese Netzwerke*: Hier können die Netzwerke ausgewählt werden, für die kein Proxy verwendet werden soll.
- *Keinen Proxy für diese Hosts*: Hier können die Hosts ausgewählt werden, für die kein Proxy verwendet werden soll.

12.3.10 Tab *Extras*, Abschnitt *NTLM*

12.3.10.1 Felder in diesem Abschnitt

- *NTLM-Authentifizierung ohne Domänenbeitritt*: NTLM (NT Lan Manager) kann zur Authentifizierung der Proxybenutzer gegenüber einem PDC genutzt werden. Der PDC kann entweder ein anderes System sein oder der Collax Security Gateway selbst. Bei dieser Variante wird der Collax Security Gateway nicht in die Domäne integriert; sie ist somit weit einfacher einzurichten als die Variante mit Domänenintegrierung. Die PDCs/BDCs, die weiter unten im Dialog eingetragen werden können, müssen per DNS auflösbar sein.
- *NTLM-Realm*: Der sogenannte *Realm* wird in dem Anmeldefenster des Clients angezeigt, damit der Benutzer weiß, wo er sich anmeldet. Wird dieses Feld leer gelassen, wird automatisch der FQDN eingetragen.
- *PDC, BDC, Domäne für NTLM*: In diesem Textfeld werden PDC (Primary Domain Controller), BDC (Backup Domain Controller) und die Domäne eingetragen. Ein einzelner Eintrag besteht immer aus diesen drei Werten, die mit einem Leerzeichen voneinander getrennt werden. Pro Zeile ist nur ein solcher Eintrag zulässig.

  Beispiel: „PDC1 BDC1 DOMAIN1“

  Sollte kein BDC existieren, muss hier der PDC zweimal angegeben werden. Zudem sollte der Netbios-Name des PDC/BDC angegeben und im DNS geprüft werden. Während der Aktivierung der Konfiguration ist zu sehen, welche Einträge korrekt aufgelöst werden und in die Systemkonfiguration übernommen werden.

12.3.11 Tab *Extras*, Abschnitt *Transfer-Encoding deaktivieren*

12.3.11.1 Felder in diesem Abschnitt

- *Transfer-Encoding deaktivieren*: Für bestimmte Web-Seiten ist es erforderlich Header-Zeilen zu entfernen, damit diese bei Benutzung des Web-Proxy korrekt angezeigt werden können. Statt dem Inhalt der Seite würde ansonsten ein weißes Browser-Fenster angezeigt. Hier werden die Domains der Web-Seiten eingetragen.

12.3.12 Tab *Extras*, Abschnitt *Zusätzliche Optionen*

12.3.12.1 Felder in diesem Abschnitt

- *Zusätzliche Optionen*: Hier können individuelle Einstellungen für den Webproxy hinterlegt werden. Es ist zu beachten, dass fehlerhafte Einstellungen zu Fehlfunktionen des Webproxy führen können.

12.4 Schritt für Schritt: Webfilter einrichten

- Zum Filtern von bestimmten Kategorien können Sie die „Dansguardian-Listen“ nutzen. Dabei handelt es sich um Zusatzsoftware, die gesondert auf den Collax Security Gateway installiert werden muss. Wechseln Sie dazu auf den seitlichen Reiter *System* und dort nach *Systembetrieb – Software – Lizenzen und Module*.
- Hier können Sie über den Schalter *Installieren* die Dansguardian-Listen auf den Collax Security Gateway installieren. Dies ist nur möglich, wenn Ihr Collax Security Gateway auf einem aktuellen Softwarestand ist. Sie erhalten andernfalls eine entsprechende Fehlermeldung.

- Wechseln Sie nun über den seitlichen Reiter *Einstellungen* zurück zum *Systembetrieb*.
- Öffnen Sie *Filter – Web-Content-Filter – Vordefinierte Listen*. Hier sehen Sie zwölf verschiedene Kategorien von URLs. Die Listen selbst sind nicht einsehbar und werden wöchentlich über den Collax-Updateserver aktualisiert. Dazu müssen Sie unter *Filter – Web-Content-Filter – Vordefinierte Listen* das *Automatische Update* aktivieren.
- Sie können hier bei Bedarf weitere eigene Listen hinzufügen.
- Diese Listen selbst haben noch keine Filterfunktion. Wechseln Sie zu *Filter – Web-Content-Filter – Regeln*. Hier sehen Sie die vordefinierte Regel „All“.
- Klicken Sie auf *Regel hinzufügen*. Geben Sie unter *Bezeichnung* und *Kommentar* sinnvolle Bezeichnungen ein. Sie möchten hier beispielhaft Werbeseiten blocken und nennen die Regel daher „WerbeBlocker“.
- Unter *Zeitraum* können Sie den Gültigkeitszeitraum einer Regel einschränken, etwa nur auf die Arbeitszeit. Weitere Zeiträume können Sie unter *Benutzungsrichtlinien* anlegen.
- *Typ der Regel* setzen Sie auf *Verbot*, da Sie URLs sperren möchten.
- *Regel gilt für alle URLs* deaktivieren Sie. Dadurch werden darunter alle vorhandenen *URL-Listen* sichtbar.
- In den *URL-Listen* aktivieren Sie nun die Liste *Ads* (Advertisements, Werbung).
- Durch *Speichern* der Regel gelangen Sie zurück zur Regelübersicht. Ihre neue Regel ist mit Priorität 2 unterhalb der Regel „All“ einsortiert.
- Ändern Sie die Priorität, so dass Ihre Regel vor der Regel „All“ aufgelistet wird. Die Regel „All“ erlaubt den Zugriff auf jede Seite und sollte in einem umfangreicheren Regelwerk stets die letzte Regel sein.

- Nun müssen Sie noch in den *Benutzungsrichtlinien* die neu angelegte Regel der Gruppe zuweisen, in der Sie die Proxy-Nutzung kontrollieren.
- Öffnen Sie den Abschnitt *Squid*, dort sind alle angelegten Filterregeln aufgelistet. Aktivieren Sie die Regeln, die für die Gruppe gelten sollen.
- Nun können Sie die Konfiguration aktivieren.

12.5 GUI-Referenz: Web Security

(Diese Option befindet sich im Zusatzmodul *Collax Web Security*)

Mit dem Web Security können bestimmte URLs anhand eines Web-Content-Filter gesperrt werden und der Inhalt auf Viren gefiltert werden. Der Benutzer erhält beim Aufruf einer gesperrten Seite eine Meldung des Filters mit dem Hinweis, dass die URL gesperrt ist.

Es stehen mit „Dansguardian“ und „Cobion“ zwei Pakete mit fertigen Listen zur Verfügung, die vom jeweiligen Hersteller verwaltet werden. Der Administrator kann nur einstellen, welche Kategorien er sperren will.

Um einzelne URLs zu sperren, können eigene Listen angelegt und verwaltet werden.

12.5.1 *URL-Listen allgemein*

(Dieser Dialog befindet sich unter *Netzwerk – Web Security – URL-Listen allgemein*)

12.5.1.1 Felder in diesem Formular

- *Rückwärtsauflösung aktivieren*: Hier wird die Rückwärtsauflösung für URLs aktiviert, die IP-Adressen enthalten.

  Gibt ein Benutzer einen URL mit einer IP-Adresse nach dem „http://“ ein, versucht der Web-Content-Filter bei aktivierter Option, den zu dem URL gehörigen Hostnamen zu ermitteln. Ist dies erfolgreich, wird für die weitere Verarbeitung in den entsprechenden Filterregeln die IP-Adresse im URL durch diesen Hostnamen ersetzt.

  Also wird beispielsweise der URL <http://192.0.34.166> so behandelt wie <http://www.example.com>. Es genügt also in diesem Fall, wenn in einer Regel „www.example.com“ gesperrt wird. Ein Zugriff über die zugehörige IP-Adresse ist dann ebenso ausgeschlossen.

12.5.1.2 Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten der allgemeinen Filtereinstellungen beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten der allgemeinen Filtereinstellungen beenden. Die Änderungen werden gespeichert.

12.5.2 *Eigene URL-Listen*

(Dieser Dialog befindet sich unter *Netzwerk – Web Security – Eigene URL-Listen*)

Eigene Listen bieten die Möglichkeit, eine oder mehrere Listen mit URLs zu verwalten. Diese Listen können dann in den *Regeln* genutzt werden.

12.5.2.1 *URL-Listen*

(Dieser Dialog befindet sich unter *Netzwerk – Web Security – Eigene URL-Listen*)

In diesem Dialog können URL-Listen angelegt und bearbeitet werden.

Felder in diesem Dialog

- *Name*: Hier wird der Name der Liste angezeigt.
- *Kommentar*: Hier wird der Kommentartext angezeigt.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird die ausgewählte Liste bearbeitet.
- *Löschen*: Mit dieser Aktion wird eine Liste gelöscht. Die Datei mit den URLs ist noch bis zur nächsten Aktivierung der Konfiguration vorhanden und wird erst dann entfernt.

Aktionen für diesen Dialog

- *Neue Liste*: Mit dieser Aktion kann eine neue Liste angelegt werden.

12.5.2.2 *URL-Liste bearbeiten*

(Dieser Dialog befindet sich unter *Netzwerk – Web Security – Eigene URL-Listen*)

In diesem Dialog wird eine URL-Liste bearbeitet.

Felder in diesem Dialog

- *Name*: Hier wird der Name der Liste angegeben.
- *Bezeichnung*: Hier wird der Name der Liste angezeigt. Wenn eine bestehende Liste bearbeitet wird, kann der Name nicht mehr geändert werden.
- *Kommentar*: Hier kann ein Kommentartext zur Liste eingegeben werden.
- *URLs und Domains*: In diesem Eingabefeld werden die URLs eingegeben. Wird eine Datei mit einer Liste hochgeladen, wird der Inhalt hier eingefügt.

  Jede URL muss in einer eigenen Zeile angegeben werden. Die Angaben für das Protokoll (z. B. „http:“) werden beim Speichern entfernt.

  Neben einzelnen URLs können hier auch ganze Domains eingegeben werden. Die Angabe einer Domain (z. B. „example.com“) schließt auch alle Subdomains ein („www.example.com,“ „www.intern.example.com,“ usw.). Bei einer URL sind Subdomains nicht eingeschlossen.

  Ein Eintrag, der nach dem Entfernen des Protokolls keine Schrägstriche mehr enthält, wird als Domainangabe interpretiert, z. B. „www.example.com“. Einträge mit Schrägstrich werden als URL betrachtet, etwa „www.example.com/“.
- *Ungültige Zeilen*: Werden bei einem Upload ungültige Zeilen gefunden, werden diese hier angezeigt.
- *Ausdrücke*: In diesem Eingabefeld können „reguläre Ausdrücke“ eingegeben werden. Damit lassen sich auch bestimmte Pfade oder Dateinamen sperren. Pro Zeile kann ein Ausdruck eingegeben werden.

  In solchen Ausdrücken haben einige Zeichen besondere Funktionen, beispielsweise markiert ein Punkt („.“) ein beliebiges

Zeichen. Soll nichts anderes als ein Punkt gefunden werden, muss dieser mit einem Backslash („\“) „maskiert“ werden.

Um beispielsweise Dateien mit der Endung „exe“ zu filtern, muss folgender Eintrag aufgenommen werden: „\.exe($|\?)“.

Mit „\.“ wird die besondere Funktion des Punktes aufgehoben und statt dessen auf einen Punkt in der URL gefiltert. Dahinter folgt der String „exe“. Das „($|\?)“ ist eine Oder-Verknüpfung aus den beiden Teilausdrücken „$“ und „\?“. Mit dem Dollarzeichen wird ein Zeilenende beschrieben, der Ausdruck endet also mit dem „.exe“. Das Fragezeichen hat selbst eine besondere Funktion und muss daher maskiert werden. In einer URL dient das Fragezeichen dem Anfügen von Parametern, etwa „http://www.example.com/download/fun.exe?action=download“. So zusammengesetzt wird die Filterregel also nicht auf „www.exeter.gov.uk“ passen.

Durch Klammern lassen sich folglich Klassen bilden, bei denen das Pipe-Symbol („|“) den Oder-Operator bildet. Folgender Ausdruck filtert beispielsweise eine ganze Reihe an bekannten Multimedia-Formaten mit nur einem Eintrag: „\.(ra?m|mpe?g?|mov|movie|qt|avi|mp3)($|\?)“. Das Fragezeichen hat die Funktion, dass das vorhergehende Zeichen einmal vorkommen kann, aber nicht vorkommen muss. Dieser Filter passt daher auf „.rm“ und „.ram“ .

Eine genaue Erläuterung der Möglichkeiten regulärer Ausdrücke ist im Internet unter <http://www.squidguard.org/Doc/expressionlist.html> abrufbar.

- *URL-Datei hochladen*: Hier kann eine Datei hochgeladen werden, die eine URL-Liste enthält. Der Inhalt dieser Datei wird zum derzeitigen Inhalt der URL-Liste hinzugefügt. Doppelte Einträge werden automatisch gelöscht. Das Format entspricht den im Eingabefeld eingegebenen URLs.

Aktionen für diesen Dialog

- *Importieren*: Mit dieser Aktion wird der Import der Datei mit der URL-Liste gestartet.

12.5.3 *Vordefinierte Listen*

(Dieser Dialog befindet sich unter *Netzwerk – Web Security – Vordefinierte URL-Listen*)

Über diesen Dialog kann die Aktualisierung der *Dansguardian*-Listen konfiguriert werden.

12.5.3.1 Tab*Listen*

Hier werden die aktuell installierten DansGuardian-Listen dargestellt.

Spalten in der Tabelle

- *Name*: In dieser Spalte wird der Name der voreingestellen Liste angezeigt. Dieser entspricht dem Namen, wie er vom Filter-System verarbeitet wird.
- *Kommentar*: Hier wird ein Kommentartext angezeigt.

12.5.3.2 Tab *Optionen*, Abschnitt *Automatisches Update*

Felder in diesem Abschnitt

- *Automatisches Update der Dansguardian-Listen aktivieren*: Hier kann die automatische Aktualisierung der Dansguardian-Blacklisten aktiviert werden. Diese werden zu einem zufälligen Zeitpunkt am Samstag oder Sonntag zwischen 0 und 2 Uhr geladen. Der zufällige Zeitpunkt kann sich durch Neukonfiguration erneut ändern.

12.5.3.3 Abschnitt *Hinweis*

Felder in diesem Abschnitt

- *Dansguardian-Listen sind noch nicht installiert*: Dieses Feld erscheint, wenn die Dansguardian-Listen noch nicht installiert sind. Die Dansguardian-Listen können unter *Lizenzen und Module* installiert werden.

12.5.4 *Regeln*

(Dieser Dialog befindet sich unter *Netzwerk – Web Security – Regeln*)

In diesem Dialog werden die Filterregeln für den Webproxyserver festgelegt. Eine solche Regel legt fest, welche URL-Listen zu welchen Zeiten gültig sind und ob die enthaltenen URLs gesperrt oder erlaubt werden.

In den Benutzungsrichtlinien kann festgelegt werden, für welche Gruppen die Regeln gültig sind. Dabei können für eine Gruppe auch mehrere Regeln gelten.

Die Reihenfolge der Regeln ergibt sich aus unterschiedlichen

Prioritäten. Treffen mehrere Regeln auf eine URL zu, wird die mit der höchsten Priorität verwendet. Grundsätzlich sollte festgelegt werden, ob alles erlaubt wird und nur bestimmte URLs gesperrt werden oder ob alles gesperrt ist und nur bestimmte URLs erlaubt werden. Diese „Policy“ sollte in der vorhandenen „All-Regel“ eingestellt werden und die „All-Regel“ sollte ganz unten mit niedrigster Priorität angeordnet werden.

12.5.4.1 *Regeln*

(Dieser Dialog befindet sich unter *Netzwerk – Web Security – Regeln*)

In diesem Dialog können neue Regeln hinzugefügt und vorhandene bearbeitet oder gelöscht werden. Zusätzlich können die Prioritäten geändert und die Regeln damit sortiert werden.

Felder in diesem Dialog

- *Priorität*: Hier wird die Priorität der Regel angezeigt.
- *Zweck*: Hier wird angezeigt, ob die Regel den Zugriff auf die URL erlaubt oder verbietet.
- *Bezeichnung*: Hier steht der Name der Regel.
- *Kommentar*: Hier wird ein Kommentartext angezeigt.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird die Regel bearbeitet.
- *Höher*: Mit dieser Aktion wird die Priorität der Regel erhöht.
- *Niedriger*: Mit dieser Aktion wird die Priorität der Regel verringert.
- *Löschen*: Diese Aktion löscht die Regel.

Aktionen für diesen Dialog

- *Regel hinzufügen*: Mit dieser Aktion wird eine neue Regel hinzugefügt.

12.5.4.2 *Regel bearbeiten*

(Dieser Dialog befindet sich unter *Netzwerk – Web Security – Regeln*)
In diesem Dialog wird eine Regel bearbeitet.

Tab *Grundeinstellungen*
Felder in diesem Abschnitt

- *Bezeichnung*: Hier wird der Name der Regel angegeben.
- *Priorität*: Die Priorität der Regel. Eine kleinere Zahl steht für eine höhere Priorität, die Regel wird dann weiter oben einsortiert.
- *Bezeichnung*: Wird eine bestehende Regel bearbeitet, wird in diesem Feld die Bezeichnung der Regel angezeigt.
- *Kommentar*: Hier kann ein Kommentartext zur Regel angegeben werden.
- *Zeitraum*: Hier muss der Zeitraum ausgewählt werden, zu dem die Regel gültig ist. Wird das Feld leergelassen, gilt die Regel zu jeder Zeit.
- *Typ der Regel*: Hier wird festgelegt, ob die Regel eine *Erlaubnis,* oder eine *Verbot*-Regel ist.
- *Regel gilt für alle URLs*: Wird diese Option aktiviert, bezieht sich die Regel auf alle URLs. Ist sie deaktiviert, können aus den vorhandenen URL-Listen diejenigen ausgewählt werden, die in der Regel enthalten sein sollen.
- *HTTPS: Nur URLs und Domains filtern*: Ist diese Option gesetzt,

wird für die angegebenen Seiten in dieser Regel der HTTPS-Verkehr nicht abgehört bzw. nicht entschlüsselt. Entscheidungen zur Durchsetzung der Regel werden dann, wenn möglich, anhand von SNI getroffen. Bei erlaubten Verbindungen wird die URL gefiltert werden, und das original Zertifikat der angefragten Seite an den Browser weitergegeben. Bei Aufruf verbotener URLs wird die Verbindung zu Client schlichtweg unterbrochen, ohne verschlüsselte Verbindung aufzubrechen. Soll der Web-Proxy-Server transparent arbeiten, ist diese Option in allen Regeln zu setzen. Ansonsten ist es erforderlich, das Web-Proxy CA-Zertifikat in allen Browsern zu importieren.

- *URL-Listen*: Hier sollten die Listen aktiviert werden, auf die sich die Regel bezieht. Diese Liste ist nur sichtbar, wenn die Option *Alle URLs* nicht aktiviert ist.
- *Cobion-Listen*: In dieser Übersicht sind die Listen aus dem Cobion-Filter sichtbar und können ausgewählt werden.

Tab *Berechtigungen*
Felder in diesem Abschnitt

- *Regel gilt für Benutzer*: Die Regel gilt für alle Benutzer in den jeweiligen Gruppen. Wenn diese Funktion aktiviert ist erscheint eine Auswahl der Benutzergruppen. Dadurch muss der Benutzer sich am Web-Proxy authentifizieren.
- *Gruppen*: Hier werden die Benutzergruppen ausgewählt.
- *Client in*: Hier kann angegeben werden aus welcher Netzwerkgruppe ein Client zugreifen darf. Wenn keine Benutzerauthentifizierung ausgewählt ist, wird lediglich die IP des Clienten geprüft.

12.5.5 *Cobion*

(Diese Option befindet sich im Zusatzmodul *Collax Surf Protection*)

(Dieser Dialog befindet sich unter *Netzwerk – Web Security – Cobion*)

In diesem Dialog kann der Cobion-Filter konfiguriert werden.

12.5.5.1 Felder in diesem Dialog

- *Cobion-Dienst aktivieren*: Mit dieser Option wird der Cobion-Dienst aktiviert. Wird der Cobion-Dienst nicht aktiviert und dennoch benutzt, werden alle Anfragen so beantwortet, als sei die entsprechende URL bei Cobion nicht gelistet.
- *Lizenz-Ticket*: Hier muss das Lizenz-Ticket eingegeben werden. Dieses gehört zum Lieferumfang. Ohne dieses Ticket kann der Cobion-Dienst nicht verwendet werden. Für Tests kann die Zeichenkette „wfcx“ als Lizenz-Ticket verwendet werden. Die Laufzeit dieses Tickets ist beschränkt auf 30 Tage ab Aktivierung.
- *Ticket gültig bis*: Hier wird angezeigt, wie lange das übermittelte Ticket gültig ist.
- *Anfragen bei Fehlern durchlassen*: Wird diese Option aktiviert, werden Anfragen bei Nichterreichbarkeit der Cobion-Server oder bei einem ungültigen oder abgelaufenen Lizenz-Ticket so beantwortet, als ob die URLs nicht von Cobion gelistet wären. Andernfalls werden die Anfragen mit einem Fehlercode abgewiesen. Normalerweise ist es ratsam, dieses Feld nicht zu aktivieren; ansonsten ist es Benutzern prinzipiell möglich, Verbindungsprobleme für das Umgehen der Filterrichtlinien auszunutzen.

12.5.6 *Cobion-Listen*

(Diese Option befindet sich im Zusatzmodul *Collax Surf Protection*)
(Dieser Dialog befindet sich unter *Netzwerk – Web Security – Cobion-Listen*)

12.5.6.1 *URL-Listen*

(Dieser Dialog befindet sich unter *Netzwerk – Web Security – Cobion-Listen*)

Felder in diesem Dialog

- *Bezeichnung*: Hier wird die Bezeichnung der angelegten Liste angezeigt.
- *Kommentar*: Hier wird ein Kommentartext zu der Liste angezeigt.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion können die Einstellungen einer Liste bearbeitet werden.
- *Löschen*: Mit dieser Aktion wird eine Liste gelöscht.

Aktionen für diesen Dialog

- *Hinzufügen*: Mit dieser Aktion wird eine neue Liste angelegt.

12.5.6.2 *Cobion-Liste bearbeiten*

(Dieser Dialog befindet sich unter *Netzwerk – Web Security – Cobion-Listen*)

Felder in diesem Dialog

- *Bezeichnung*: In diesem Feld wird ein Name für die Liste angegeben.
- *Kommentar*: Hier kann ein Kommentartext zu der Liste eingegeben werden.
- *Kategorien*: Alle in dieser Liste aktivierten Kategorien werden der Liste zugeordnet. Eine genaue Erläuterung der Inhalte der einzelnen Kategorien kann im Internet unter <http://www.cobion.de/support/techsupport/dbcategories/> abgerufen werden.

12.5.7 *Antivirus Web-Filterung*

(Dieser Dialog befindet sich unter *Netzwerk – Web Security – Antivirus Web-Filterung*)

12.5.7.1 Felder in diesem Formular

- *Aktivieren*: Diese Option schaltet die Filterung auf Viren für den Web-Traffic ein. Voraussetzung für die korrekte Filterung ist die Aktivierung des Web Proxy sowie die Aktivierung mindestens eines Virenscanners.
- *Benutze*: Hier werden Scanner ausgewählt, die für Webfilterung eingesetzt werden sollen.

12.5.7.2 Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten des Dialogs beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten des Dialogs beenden. Die Änderungen werden gespeichert.

13 E-Mail

13.1 Einführung

E-Mail ist einer der ältesten im Internet genutzten Dienste. Während viele andere Dienste durch das „World Wide Web“ verdrängt wurden, hat E-Mail seine wichtige Stellung bis heute behaupten können.

Aufgrund des Alters fehlen den für E-Mail genutzten Protokollen allerdings Schutzmechanismen, die vor gefälschten oder unerwünschten E-Mails schützen. Weder der vermeintliche Absender noch der Inhalt der E-Mail müssen zwingend echt sein. Mit Zertifikaten zur Verschlüsselung und Filtern gegen Spam und Viren lassen sich diese Probleme jedoch in den Griff bekommen.

13.1.1 Aufbau einer E-Mail

Eine E-Mail besteht aus einem als „Header“ bezeichneten Vorspann und dem „Body“ genannten eigentlichen Text. Im Header sind vielfältige Informationen über die E-Mail in der Form „Feldname: Feldinhalt“ gespeichert. Die Reihenfolge der Headerfelder ist willkürlich, dennoch sollten sie nicht während des Transports über das Internet umsortiert werden. Die einzigen Pflichtfelder sind Absendedatum und Absender. Die weiteren Felder für Message-ID, Empfänger, Betreff, Kopien, Transportinformation usw. sind optional. Im Header dürfen nur Zeichen des US-ASCII-Zeichensatzes verwendet werden. Andere Zeichen müssen kodiert werden.

Der Body der E-Mail ist durch eine einfache leere Zeile vom Header

getrennt. Auch im Body dürfen nur druckbare Zeichen des ASCII-Zeichensatzes enthalten sein. Andere Zeichen müssen umkodiert werden.

Binärdaten wie z. B. Bilder müssen in einen transportfähigen ASCII-Text konvertiert werden. Dies geschieht entweder durch UU-Kodierung oder durch das heutzutage sehr verbreitete MIME-Format („Multipurpose Internet Mail Extensions“). Mit der MIME-Codierung können in einer E-Mail mehrere Dateien übertragen werden. Vor jedem Block wird der „Medientyp“ des Blocks und weitere Parameter wie das Kodierungsverfahren und der Dateiname angegeben. Derzeit sind folgende Medientypen definiert:

- *application* für Binärdaten, die von bestimmter Software verarbeitet werden.
- *audio* für Audiodateien
- *image* für Bilddateien
- *message* für Nachrichten
- *model* für Dateien, die mehrdimensionale Strukturen repräsentieren, z. B. CAD-Daten
- *multipart* für Anhänge
- *text* für Textdateien
- *video* für Videodaten

Hinter dem Mediatyp wird jeweils ein Subtyp angegeben, der das Format genauer spezifiziert. Beispiele sind etwa „text/html“, „image/jpeg“ oder „application/msword“.

Zusammengesetzt sieht eine einfache E-Mail dann wie folgt aus:

```
Return-Path: <schulz@company.example.com>
X-Original-To: mustermann@mail.example.com
Delivered-To: mustermann@somehost.example.com
Received: by somehost.example.com (Postfix)
    id B16C07B4E2; Mon, 29 Jan 2007 17:29:06 +0100 (CET)
From: Hans Schulz <schulz@company.example.com>
```

```
Reply-To: Info <info@company.example.com>
To: mustermann@mail.example.com
Subject: Neue Artikel im System
Content-Type: text/plain; charset=iso-8859-1
Content-Transfer-Encoding: 8bit
MIME-Version: 1.0
Message-Id: <E1EuuMk-000370-00@pc17.company.example.com>
Date: Mon, 29 Jan 2007 17:22:58 +0100

Sehr geehrter Herr Mustermann,

wir haben einige neue Artikel in unserem Shopsystem
bereitgestellt:

http://www.company.example.com/shop/index.html

Mit freundlichem Gruss
Hans Schulz


--
http://www.company.example.com - Get everything online
```

13.1.2 SMTP

Das Versenden von E-Mails geschieht mit Hilfe des „Simple Mail Transfer Protocol“ (SMTP). Der Aufbau des Protokolls ist tatsächlich sehr simpel, so findet die gesamte Kommunikation zwischen den beteiligten Systemen in lesbarem Klartext statt, nicht in einem binären Format.

SMTP ist ein Client-Server-Protokoll. Es gibt einen Server, der eine permanente Verbindung an das Netzwerk benötigt. Zu diesem baut der Client zu einem beliebigen Zeitpunkt eine Verbindung zu Port 25 auf. Ist diese etabliert, muss sich der Client zunächst identifizieren

und sendet dazu seinen eigenen Namen mittels des Kommandos „HELO“. Der Server antwortet darauf mit einem Zahlenkode und seinem Namen. Dieser Zahlenkode ist dreistellig und wird bei jeder Antwort des Servers als erstes gesendet.

Danach werden mit „MAIL FROM“ (Absender) und „RCPT TO“ (Empfänger) die Adressen der beiden beteiligten Benutzer angegeben und vom Server jeweils quittiert. Mit „DATA“ wird die Übertragung der eigentlichen E-Mail gestartet, und der Client kann nun Zeile für Zeile die E-Mail einliefern. Mit einer Zeile, die nur aus einem Punkt besteht, wird der Datenmodus beendet, und mit „QUIT“ kann der Client die ganze Verbindung abbauen.

```
<- 220 gateway.example.com ESMTP (Postfix)
-> HELO  mail.company.example.com
<- 250 gateway.example.com
-> MAIL FROM: <schulz@company.example.com>
<- 250 Ok
-> RCPT TO: <mustermann@mail.example.com>
<- 250 Ok
-> DATA
<- 354 End data with <CR><LF>.<CR><LF<
-> Date: Mon, 29 Jan 2007 17:22:58 +0100
-> Subject: Neue Artikel im System
-> Content-Type: text/plain; charset=iso-8859-1
-> To: mustermann@mail.example.com
-> From: Hans Schulz <schulz@company.example.com>
-> Content-Transfer-Encoding: 8bit
->
-> Sehr geehrter Herr Mustermann,
->
-> wir haben einige neue Artikel in unserem Shopsystem
-> bereitgestellt:
->
-> http://www.company.example.com/shop/index.html
->
-> Mit freundlichem Gruss
```

```
-> Hans Schulz
->
->
-> --
-> http://www.company.example.com - Get everything online
-> .
<- 250 Ok: queued as CFC313AF38
-> QUIT
<- 221 Bye
```

Die Erläuterung aller Rückmeldekodes des Servers geht über den Umfang dieses Handbuches hinaus. Wichtig ist nur, dass die einzelnen Stellen bestimmte Bedeutungen haben.

So bedeuten in der ersten, linken Stelle die Ziffer „2“ eine positive Bestätigung des Servers, eine „4“ einen vorübergehenden Fehler und eine „5“ einen permanenten Fehler. Neben dem Zahlenkode wird vom Server immer eine Klartextmeldung mitgeliefert, so dass die Kodes selbst nicht aufgeschlüsselt werden müssen. Bei Zustellungsproblemen werden diese Fehlermeldungen im Kommentarfeld der Mailqueue des Collax Security Gateways angezeigt.

Im Laufe der Jahre wurde SMTP überarbeitet, aber nie grundlegend geändert. Es sind neue Funktionalitäten hinzugekommen, die als „Enhanced SMTP“ (ESMTP) nutzbar sind. Der Client muss bei der Kontaktaufnahme mit dem Server signalisieren, dass er ESMTP unterstützt, und sendet dazu eine „EHLO“-Zeile. Der Server wird im Gegenzug eine Liste mit den erweiterten Funktionen schicken, die er unterstützt.

13.1.3 Maildomain

Eine E-Mail-Adresse besteht aus zwei Komponenten, die über das Symbol „@“ verbunden sind. Das „@“ bedeutet dabei „at“ (englisch ausgesprochen). Insgesamt wird „Localpart@Domain“ unterschieden.

Der Abschnitt *Localpart* muss eine für die Domain eindeutige Adresse sein. Er bezeichnet meist den Namen eines Benutzers. Es werden mehrere Localpart-Adressen für verschiedene Zwecke empfohlen, etwa „info“, „support“ usw. Eingerichtet werden sollten in jedem Fall die beiden Adressen „abuse“ als Anlaufstelle für Beschwerden und „postmaster“ für die Behandlung von Zustellungsproblemen. Wird eine Webseite unter der Domain betrieben, empfiehlt sich zusätzlich die Einrichtung der Adresse „webmaster“.

Die Domain selbst besteht aus mehreren durch Punkte getrennten Komponenten. Von rechts nach links sind dies die Top-Level-Domain (etwa „com“), die Domain selbst („csg“) und optional ein oder mehrere Subdomains. Eine genauere Beschreibung der Internet-Domain findet sich im Kapitel über DNS.

Im Collax Security Gateway werden Maildomains getrennt von den Internet-Domains im DNS verwaltet. Für jede angelegte Maildomain kann festgelegt werden, ob die Zustellung lokal erfolgen soll oder ob die E-Mails per SMTP an ein anderes System weitergereicht werden sollen.

Beim Versenden einer E-Mail wird vom Mailclient gewöhnlich eine SMTP-Verbindung zum „Smarthost“ oder „SMTP-Relay“ aufgebaut. Dabei handelt es sich um den SMTP-Mailserver im lokalen Netzwerk oder beim eigenen Provider. Der Client baut eine SMTP-Verbindung zum Mailserver auf und liefert die E-Mail dort ab. Im Mailserver wird E-Mail nun in die „Mailqueue“ aufgenommen, eine Warteschlange, in der alle noch nicht zugestellten E-Mails aufbewahrt werden.

Bei allen E-Mails in der Mailqueue wird geprüft, ob die Empfän-

geradresse zu einer der angelegten Maildomains gehört. Ist dies der Fall, wird anhand der Konfiguration der Maildomain die weitere Zustellung vorgenommen. Ist die Domain lokal verwaltet, wird geprüft, ob es zum Localpart der Adresse einen Empfänger gibt, und die E-Mail in dessen Postfach gespeichert. Andernfalls wird eine Fehler-E-Mail erzeugt, die darüber informiert, dass der Empfänger unbekannt ist. Ist die Domain als SMTP-Weiterleitung konfiguriert, wird eine SMTP-Verbindung zum angegebenen System aufgebaut und ein Zustellversuch gestartet.

Stellt der Mailserver beim Annehmen einer eingelieferten E-Mail fest, dass die Zieldomain nicht zu einer der angelegten Maildomains gehört, muss er diese E-Mail per SMTP weiterreichen. Dieser Vorgang, also das Annehmen und Weiterreichen einer E-Mail per SMTP durch einen Mailserver, wird „Relayen“ genannt. Der Mailserver selbst ist ein „Relay“ (vergleichbar mit einer Relaisstation zum Pferdewechsel aus der Zeit der Postkutschen).

13.1.4 Mailrouting

Um eine E-Mail als Relayserver zu einem weiteren Mailserver übertragen zu können, muss der Zielserver bekannt sein. Zu den Zonendaten einer Domain im Nameserver gehört daher auch die Angabe eines oder mehrerer Mailserver, die für die Domain zuständig sind. Diese werden im Nameserver als „Mail-Exchanger“ MX eingetragen.

Normalerweise werden zu einer Domain mehrere Nameserver an unabhängigen Standorten betrieben. Fallen diese alle gleichzeitig aus, existiert für die Domain kein Nameservice mehr, der MX-Eintrag existiert nicht mehr, und die E-Mail wird mit einer Fehlermeldung umgehend an den Absender zurückgeschickt.

Dieser MX-Eintrag löst auf einen Hostnamen auf, zu dem dann in einer zweiten Abfrage die IP-Nummer aufgelöst wird. Zu dieser IP-Nummer wird nun die SMTP-Verbindung aufgebaut. Schlägt der Verbindungsaufbau fehl – etwa weil die Internetverbindung des Ziel-MTAs gestört ist – bleibt die E-Mail weiter in der Mailqueue. Dort wird sie üblicherweise bis zu fünf Tage lang aufbewahrt, bevor sie mit einer Fehler-E-Mail an den Absender zurückgeschickt wird. Vier Stunden nach dem ersten Versuch schicken viele Mailserver eine E-Mail an den Absender mit dem Hinweis, dass sich die Zustellung verzögert.

Soll oder kann der eigene Mailserver nicht direkt E-Mails in alle Welt ausliefern, kann ihm, ähnlich wie dem Client (MUA), ein Smarthost angegeben werden. Er liefert dann alle E-Mails, die nicht für seine lokalen Domains bestimmt sind, per SMTP an diesen Mailserver. Meist handelt es sich dabei um den MTA des eigenen Providers. Dieser MTA kann eine Authentifizierung verlangen („SMTP-AUTH“), damit ihn nur berechtigte Systeme als Relayserver nutzen.

Im Collax Security Gateway kann bei der Konfiguration einer Domain im DNS die Option *Auto-MX* aktiviert werden. Ist diese aktiv, wird geprüft, ob eine Maildomain gleichen Namens existiert, und in dem Fall der Collax Security Gateway selbst als MX für die Domain eingetragen.

13.1.5 Mailzustellung ohne SMTP

Zur Annahme von SMTP-Verbindungen muss eine permanente Verbindung mit dem Internet unter einer festen IP-Nummer bestehen. Ist dies nicht gegeben, müssen alternative Wege genutzt werden, um E-Mails zu erhalten.

Eine oft genutzte Möglichkeit ist die Nutzung der Protokolle POP3

oder IMAP. Hier nimmt der Provider die E-Mails an und stellt sie einem Postfach zu. Der eigentliche Ziel-Mailserver verbindet sich dann regelmäßig mit dem Server des Providers und prüft, ob neue E-Mails in den Postfächern angekommen sind, lädt diese ggf. herunter und speichert sie in den „richtigen" Postfächern der Benutzer.

Der Provider kann dabei für jeden Benutzer ein eigenes Postfach einrichten, welches mit je einem eigenen „Abholjob" abgefragt und einem bestimmten Benutzer zugestellt wird. Dies ist technisch die geeignetste Lösung. Allerdings ist sie bei vielen und oft wechselnden Nutzern aufwendig in der Verwaltung (pro Benutzer je ein Postfach auf dem eigentlichen Mailserver, ein Postfach beim Provider und ein Abholjob).

Eine Alternative ist die Nutzung eines „Multidrop"-Postfachs beim Provider. Dabei werden alle eingehenden E-Mails für eine bestimmte Domain einem Postfach zugestellt, unabhängig vom Localpart der E-Mail-Adresse des Ziels. Mit einem einzigen Abholjob wird dieses Postfach abgefragt, und die E-Mails werden auf die einzelnen Postfächer verteilt. Dieses Verfahren birgt ein großes Problem: Bei der einkommenden SMTP-Verbindung wird die E-Mail-Adresse des Empfängers genau angegeben („RCPT TO"). Bei Zustellung in ein Postfach geht jedoch die SMTP-Information verloren, und es bleibt eine normale E-Mail mit Header und Body. Aus dem Body ist es unmöglich, den Empfänger zu ermitteln (ging die E-Mail an die Person(en) im To-Feld, an die im CC-Feld oder an die im nicht sichtbaren BCC-Feld?). Viele Provider lösen dieses Problem, indem sie eine zusätzliche Zeile in den Mailheader einfügen, in der die Adresse hinterlegt wird, für die die SMTP-Verbindung angenommen wurde.

Eine weitere Möglichkeit bietet die Verwendung von *ESMTP*. Wenn beide Seiten das Kommando „Extended Turn" (ETRN) verstehen, kann der Client die Verbindung „umdrehen" (engl. to turn). Er sendet dazu seinen Hostnamen bzw. die Domain, für die er E-Mails abrufen

möchte, und wird dadurch zu einem Pseudo-Server. Der Mailserver selbst wird zum Pseudo-Client. Er überträgt alle E-Mails aus seiner Mailqueue, deren Zieldomain abgerufen wurde, mit einer neuen SMTP-Verbindung zum Pseudo-Server.

13.1.6 Berechtigungen

In den *Benutzungsrichtlinien* lässt sich unter *Firewall* die Berechtigung für SMTP setzen. Rechner, die Mitglied einer Gruppe mit dieser Berechtigung sind, dürfen eine Verbindung zum SMTP-Dienst aufbauen. Ohne weitere Berechtigungen nimmt der Collax Security Gateway hier nur E-Mails für angelegte Maildomains an. E-Mails an fremde Domains wird er mit „Relaying Denied“ ablehnen.

Weitere Berechtigungen lassen sich in den *Benutzungsrichtlinien* im Abschnitt *Mail* setzen.

Die Berechtigungen zum *IMAP Connect* bzw. *POP3 Connect* gestatten Computersystemen in der jeweiligen Gruppe den Zugriff auf die beiden Dienste. Eine sicherere Variante ist jeweils die Nutzung von *mit SSL*. Dazu ist es allerdings notwendig, zunächst ein geeignetes Serverzertifikat zu erzeugen.

Benutzer, die Mitglied einer Gruppe mit der Berechtigung *Zugriff auf administrativen Ordner ...* sind, können über IMAP auf die jeweiligen Ordner zugreifen. Bei diesen Ordnern handelt es sich um Quarantäneverzeichnisse, in denen von den Filtern im Collax Security Gateway abgefangene E-Mail zwischengespeichert wird. Da es jeweils nur ein Verzeichnis im System gibt, kann hier E-Mail mit persönlichen Inhalten anderer Nutzer enthalten sein. Diese Berechtigung sollte daher nur an Benutzer gegeben werden, die mit der Administration des Mailsystems betraut sind.

Mit der Berechtigung *Zugriff auf gemeinsamen Spam/Ham-Ordner*

können Benutzer über IMAP E-Mail getrennt nach den Kategorien „Spam“ und „Ham“ ablegen. Mit diesem Bestand an unerwünschten und erwünschten E-Mail trainiert der Spamfilter des Collax Security Gateways seine Erkennungsrate.

Die Berechtigung *nur lokale Mailzustellung* lässt nur E-Mails an interne Maildomains zu. E-Mails zu fremden Domains werden nicht angenommen.

Damit ein Benutzer überhaupt ein E-Mail-Postfach erhält, muss er einer Gruppe angehören, die die Berechtigung *Lokale Mailbox einrichten* hat. Damit werden noch keinerlei E-Mail-Adressen angelegt, lediglich das Postfach, welches über IMAP bereits zur Ablage von E-Mail genutzt werden könnte.

Durch die Berechtigung *Mail-Relay ohne Authentifizierung* können Systeme E-Mails von fremden an fremde Domains beim Collax Security Gateway einliefern. Dieser nimmt die E-Mails an und wird versuchen, sie zuzustellen. Diese Berechtigung sollte daher nie für eine Gruppe gesetzt werden, in der das Internet Mitglied ist. Andernfalls kann der Collax Security Gateway als „Spamquelle“ missbraucht werden.

Die Berechtigung *Postfach anlegen in ...* sorgt dafür, dass ein Benutzer eine E-Mail-Adresse in der ausgewählten Domain erhält. Dabei werden auch die in seiner Benutzerkonfiguration angelegten Alias-Adressen berücksichtigt. Zusätzlich muss der Benutzer aber noch die Berechtigung *Lokale Mailbox einrichten* besitzen, damit überhaupt ein Postfach angelegt wird.

Es empfiehlt sich, all diese Berechtigungen in einer eigenen Gruppe, etwa „Mailuser“, zusammenzufassen. Dadurch wird die Konfiguration übersichtlicher und kann später einfacher geändert werden.

13.1.7 Erweiterung der Sicherheit

Da das gesamte E-Mail-System bereits recht alt ist, hat es einige Schwachstellen, die von Personen mit unlauteren Absichten ausgenutzt werden.

Zum einen ist die gesamte E-Mail während der SMTP-Übertragung reines Transportgut. Das bedeutet, dass kein Mailserver prüft, ob die Angaben im Header der E-Mail stimmen. So ist es ohne weiteres möglich, den Absender einer E-Mail zu fälschen, gefälschte Received-Zeilen einzubauen, um die Herkunft der E-Mail zu verschleiern, usw. Der Inhalt einer E-Mail bzw. der Name des Absenders kann durch den Einsatz von digitalen Signaturen gegen Modifikationen gesichert werden. Dabei führen Änderungen im Text sofort zu einer ungültigen Prüfsumme. Die Nutzung solcher Möglichkeiten ist allerdings nicht weit verbreitet.

Der gesamte Relay-Mechanismus war ursprünglich dazu gedacht, ein in sich stabiles Netz aufzubauen. Bei großen Entfernungen und schlechten Verbindungen wurden die E-Mails über mehrere Mailserver übertragen, so dass die einzelnen Wege weniger kritisch waren. Dazu wurden die Mailserver als „offene Relays“ betrieben, d. h., sie nahmen E-Mails von fremden Servern für fremde Empfänger an und transportierten diese weiter. Inzwischen werden offene Relays zum Einschleusen von gefälschten E-Mails missbraucht, so dass niemand mehr seinen Mailserver in diesem Modus betreibt.

Es ist daher mit einfachen Mitteln möglich, E-Mails in Umlauf zu bringen, deren Absender nicht zu ermitteln ist. Typischerweise werden in diesen E-Mails Medikamente, billige Software oder sonstiger Ramsch angepriesen. Solche E-Mail wird umgangssprachlich als „Spam“ bezeichnet. Der Name stammt von einer Sorte Dosenfleisch und geht im Zusammenhang mit E-Mail auf eine Monty-Python-Episode zurück, in dem ein Chor mit penetranten „wonderful, lovely

Spam“-Gesängen nervt. Spam ist inzwischen zu einem kritischen Problem für Unternehmen geworden, da beachtliche Ressourcen durch das Lesen und Löschen solcher E-Mails verschwendet werden.

Die Übertragung von Authentifizierungsdaten (Login und Passwort) erfolgt im Klartext. Angreifer können diese Daten abfangen und E-Mails mitlesen. Dies lässt sich durch TLS-Verschlüsselung oder den Einsatz von VPN-Technologie verhindern. Beide Möglichkeiten werden vom Collax Security Gateway unterstützt.

Die E-Mail selbst ist nicht verschlüsselt. Kritische Daten, etwa die Kalkulationen für einen Auftrag, die zwischen zwei Standorten eines Unternehmens verschickt werden, könnten mitgelesen werden. Hier schafft Kryptographie im Mailclient oder der Einsatz von VPN-Technologie (bei unternehmensinterner Komunikation) Abhilfe.

Es gibt keinerlei Kontrolle, ob eine E-Mail beim Empfänger angekommen ist. Manche Mailclients implementieren eine „Lesebestätigung“, die jedoch nichts darüber aussagt, ob der Empfänger die E-Mail tatsächlich verstanden hat – er könnte z. B. der verwendeten Sprache nicht mächtig sein. Desweiteren gibt es viele Mailclients, bei denen solche Bestätigungsanforderungen nicht unterstützt werden oder deaktiviert sind. Eine E-Mail kann bis zu fünf Tage lang irgendwo im Internet „festhängen“, bevor sie mit einer Fehlermeldung zurückgesendet wird. Ein Mailserver kann eine E-Mail mit SMTP annehmen und quittieren, unmittelbar danach aber einen irreparablen Festplattenschaden erleiden. In den letzten Jahren hat sich gezeigt, dass E-Mail trotz all dieser Punkte ein stabiles und zuverlässiges Medium ist. In wirklich wichtigen Fällen sollte der Sender den Empfänger dennoch bitten, persönlich eine E-Mail zur Bestätigung des Empfangs zu senden.

Gegen E-Mails mit unerwünschten Inhalten (Spam, Viren usw.) können im Collax Security Gateway verschiedene Filter als Schutzmechanismen eingesetzt werden. Diese filtern nach bestimmten

Kriterien und nehmen bedenkliche E-Mails in Quarantäne, löschen sie oder schicken sie mit einer Fehlermeldung zum Absender zurück.

13.1.8 E-Mail-Archivierung

Damit Firmen der Verpflichtung nachkommen können, geschäftsrelevante E-Mails für 10 Jahre zu archivieren, wurde das Mailarchiv entwickelt. Ein Betriebsprüfer in der Rolle eines Auditors hat über den Webaccess die Möglichkeit das gesamte Mailarchiv nach allen darin enthaltenen E-Mails zu durchsuchen. Zusätzlich kann jeder Benutzer das Mailarchiv nach seinen eigenen E-Mails durchsuchen, d.h. E-Mails, die entweder von ihm versendet oder empfangen wurden. Dies beinhaltet auch die Mitgliedschaft in einem E-Mail-Verteiler.

Es ist möglich, E-Mails in Abhängigkeit von Absender- oder Empfänger-Domains zu archivieren. Um Datenintegrität zu gewährleisten, wird für jede archivierte E-Mail eine Signatur angelegt. Diese wird zusammen mit der archivierten E-Mail auf dem Datenträger gespeichert. Eine nachträgliche Veränderung kann so zuverlässig erkannt werden.

Das Archiv lässt sich in mehrere Segmente unterteilen, deren Größe frei bestimmt werden kann. Aus den einzelnen Segmenten lassen sich ISO-Dateien generieren, die anschließend auf einen Datenträger, wie z.B. CD, DVD oder Blue-Ray, gebrannt werden können.

13.2 Filtermechanismen

Zum Filtern von E-Mail gibt es verschiedene Ansatzpunkte und Verfahren. Die erste Möglichkeit besteht, sobald eine E-Mail per SMTP am eigenen Mailserver abgegeben wird. Zunächst erfolgt der SMTP-Dialog, bei dem der Name und die IP-Adresse des einliefernden Systems sowie der Absender und der Empfänger der E-Mail ausgetauscht werden. Mit diesen Informationen kann bereits eine unerwünschte E-Mail abgelehnt werden. In diesem Fall wird die E-Mail selbst nicht übertragen, sondern verbleibt beim einliefernden Mailserver. Dieser ist dann für die weitere Behandlung zuständig, etwa dem Zurücksenden mit einer Fehlermeldung an den Absender.

Nach dem SMTP-Dialog wird die eigentliche E-Mail übertragen. Diese wird vom Mailserver nach der Annahme in die Mailqueue aufgenommen. Von dort erfolgt die weitere Zustellung. Vor der Aufnahme in die Mailqueue kann die zweite Stufe von Filtern eingesetzt werden. Zu diesem Zeitpunkt liegt die E-Mail komplett vor, so dass die Filter auch den Inhalt analysieren können.

13.2.1 HELO-Identifikation

Eine einfache Überprüfung der HELO-Meldung des einliefernden Mailservers beim Aufbau der SMTP-Verbindung kann bereits einigen Spam ausschließen. Dabei prüft der Collax Security Gateway, ob der beim HELO übertragene Hostname ein gültiger FQDN ist. Bei einer verschärften Prüfung wird über DNS abgefragt, ob dieser Hostname überhaupt eingetragen ist. Normale Mailserver sollten diese Kriterien erfüllen, viele Spamsoftware sendet jedoch ungültige HELO-Daten. Leider gibt es auch einige wenige fehlerhaft konfigurierte Mailserver,

die keinen gültigen Hostnamen bei der HELO-Meldung ausgeben. Solche Systeme können dann auch keine E-Mail einliefern.

13.2.2 Blacklists

Ein anderer Filtermechanismus nutzt „Blacklists“ („Schwarze Listen“), um E-Mails von möglichen Spammer-Systemen abzulehnen. Im Internet werden dazu einige Blacklist-Server betrieben, die die IP-Adressen von unsicheren oder fehlerhaft konfigurierten Systemen bereitstellen, über die Spam versendet wird (oder wurde). Inzwischen sind auch die Einwahl-IP-Bereiche von großen Providern dauerhaft erfasst, da hier oft unsichere Systeme für den Versand von Spam missbraucht werden.

Bei einer einkommenden SMTP-Verbindung wird der Status der IP-Adresse des Mailservers bei allen konfigurierten Blacklist-Servern abgefragt. Dies geschieht in Echtzeit über das DNS-Protokoll. Ist die IP-Nummer auf mindestens einer Liste erfasst, wird die Annahme der E-Mail mit einer Fehlermeldung abgelehnt. In dieser Fehlermeldung steht ein qualifizierter Hinweis über den Eintrag in der Blacklist. In der Praxis kann die Verwendung von Blacklists gelegentlich zu Problemen führen, wenn auf der Gegenseite ein versehentlich geblockter Mailserver E-Mail einliefern möchte. In diesem Fall wird die Annahme von erwünschter E-Mail verweigert.

13.2.3 Greylisting

Eine weitere Möglichkeit zur Filterung bei der SMTP-Annahme ist der Einsatz von „Greylisting“. Dabei handelt es sich um keinen Filter im klassischen Sinne, sondern lediglich um eine Verzögerung der Mailannahme. Jede neu ankommende E-Mail wird mit einer temporären Fehlermeldung abgewiesen. Dadurch ist der einliefernde Mailserver gezwungen, die E-Mail in seiner Mailqueue aufzubewahren und später einen erneuten Zustellversuch zu unternehmen. Intern speichert der Collax Security Gateway die drei Daten „IP-Adresse des Mailservers“, „E-Mail-Adresse des Empfängers“ und „E-Mail-Adresse des Absenders“ (auch als „Tupel“ bezeichnet).

Dieses Tupel wird nach Ablauf einer Sperrzeit von üblicherweise 15 Minuten freigeschaltet. Wenn der einliefernde Mailserver ein weiteres Mal die SMTP-Verbindung aufbaut, findet der Collax Security Gateway das zugehörige Tupel in seiner Datenbank und kann prüfen, ob die Sperrfrist abgelaufen ist. Ist dies der Fall, wird die E-Mail angenommen. Die meisten Programme, die Spam versenden, implementieren keine Mailqueue, d. h., sie unternehmen nur einen einzigen Zustellversuch, der mittels aktiviertem Greylisting abgewehrt wird. Es gibt jedoch auch einige wenige Mailserverprogramme, die mit Greylisting Schwierigkeiten haben.

Anders als bei der Verwendung von Blacklists wird beim Greylisting die Annahme von E-Mails nicht permanent verweigert.

13.2.4 Header- und Attachmentfilter

Headerfilter können nach bestimmten Mustern in einzelnen Headerzeilen filtern. Damit ist es beispielsweise möglich, E-Mails mit einem bestimmten Betreff abzufangen oder auch Headerzeilen zu entfernen.

Mit Attachmentfiltern können Dateianhänge entweder anhand von Endungen im Dateinamen oder von MIME-Typen erkannt werden. Über solche Filter ist es möglich, E-Mails mit Anhängen abzulehnen, die unter *Microsoft Outlook* automatisch ausgeführt würden und somit eine potenzielle Gefährdung darstellen.

Header- und Attachmentfilter sind in einzelnen Fällen sehr hilfreich, bieten jedoch kaum Möglichkeiten, um die Verbreitung von Spam-E-Mails einzudämmen. Beispielsweise existiert inzwischen eine solche Vielzahl verschiedener (fehlerhafter) Schreibweisen für die berühmte blaue Potenzpille, dass es kaum möglich ist, dieses Wort in einer Betreffzeile sicher zu erkennen. Und dann besteht immer noch die Möglichkeit, dass damit eine E-Mail gefiltert wird, die sich kritisch mit dem Produkt auseinandersetzt und die somit vielleicht erwünscht gewesen wäre.

13.2.5 SpamAssassin

„SpamAssassin“ („Spam-Meuchelmörder“) ist ein Filterprogramm, welches auf eine vollständig vorliegende E-Mail angewandt werden kann. Dabei wird die E-Mail nach verschiedenen Kriterien untersucht, und pro erfülltem Kriterium werden Punkte vergeben. Je mehr Punkte eine E-Mail am Ende erhalten hat, desto größer ist die Wahrscheinlichkeit, dass es sich um Spam handelt. Innerhalb des Collax Security Gateways können zwei Punktegrenzen festgelegt werden, die die weitere Behandlung solcher E-Mail bestimmen.

Bei Überschreiten der ersten Punktegrenze wird die E-Mail als Spam markiert. Dazu wird der Betreff am Anfang um „***** SPAM *****“ erweitert. Damit kann beispielsweise ein Filter in Mail-Client-Software gesteuert werden, der Spam in einem separaten Ordner ablegt. Bei Überschreiten der zweiten Punktegrenze kann die E-Mail verworfen, in der Mailqueue angehalten oder in einem Quarantäne-Ordner abgelegt werden. Der Quarantäne-Ordner wird per IMAP exportiert und sollte nur für Administratoren zugänglich sein, da hier alle Spam-verdächtige E-Mail abgelegt wird.

Der bei SpamAssassin genutzte Regelsatz untersucht E-Mails auf bestimmte Phrasen und Muster, wird aber nur gelegentlich aktualisiert. Von engagierten Spammern wird er daher leicht unterlaufen. Bessere Filterergebnisse lassen sich durch das Trainieren des Filters erreichen. Dabei müssen zwei IMAP-Ordner mit erwünschten („Ham“) und unerwünschten (Spam) E-Mails gefüllt werden. Anhand dieser Daten wird ein im SpamAssassin integrierter Bayes-Filter trainiert, der bei intensivem Training ausgezeichnete Erkennungsergebnisse liefert.

13.2.6 Razor

Ein zusätzlicher Filter, der den Inhalt einer E-Mail analysiert, ist „Razor“. Vom Inhalt jeder E-Mail wird eine Prüfsumme erstellt, die an die Razor-Server übermittelt wird. Als Antwort liefert Razor die Wahrscheinlichkeit zurück, mit der diese E-Mail als Spam einzustufen ist. Bei einer ausreichenden Wahrscheinlichkeit bekommt die E-Mail innerhalb der SpamAssassin-Überprüfung weitere Spampunkte hinzuaddiert.

Bei Razor werden Signaturmuster von bekanntem Spam erfasst. Diese Signaturen werden von einem gemeinschaftlich betriebenen

weltweiten Netzwerk bereitgestellt. Sobald eine neue Spam-E-Mail irgendwo auftaucht, können registrierte Benutzer diese an das Razor-Netzwerk melden. Dabei erarbeitet sich jeder Benutzer im Laufe der Zeit eine Reputation, die direkt Einfluss auf die Bewertung seiner Meldungen hat. So wird vermieden, dass Unruhestifter die Signaturen erwünschter E-Mails in das Razor-Netzwerk einschleusen.

Im Gegensatz zu dem eher statischen Regelwerk von SpamAssassin bzw. dem aufwendig zu trainierenden Bayes-Filter kann das Razor-Netz kurzfristig auf neue bzw. modifizierte Spamwellen reagieren.

13.2.7 Filterkaskaden

Werden alle verfügbaren Filter im Collax Security Gateway aktiviert, durchläuft jede E-Mail sie in einer festgelegten Reihenfolge:

- Wird eine E-Mail per SMTP direkt eingeliefert, kann die HELO-Überprüfung durchgeführt werden, können E-Mails für unbekannte Empfänger je nach Einstellung sofort abgelehnt werden und können Blacklist-Anfragen zu der IP-Adresse des einliefernden Mailservers gestellt werden.

  Wird eine E-Mail in diesem Stadium abgelehnt, findet keine Übertragung der eigentlichen E-Mail statt, d. h., sie verbleibt bei dem einliefernden Mailserver.

  Wird die E-Mail jedoch angenommen, wird sie vom Mailsystem des Collax Security Gateways unter Anwendung der folgenden Filterstufen weiter verarbeitet.
- Im ersten Schritt werden eventuell definierte Header- und Attachmentfilter angewandt. Diese Reihenfolge bietet eine hohe Performanz, da das Filtern beispielsweise auf das Vorhandensein von „.exe“Attachments sehr schnell abläuft. Werden solche Anhänge abgelehnt, müssen diese Dateien später nicht mehr aufwendig vom Virenscanner geprüft werden.

- Im nächsten Schritt untersucht SpamAssassin die E-Mail nach seinen festgelegten Kriterien bzw. unter Zuhilfename von trainierten Filterdaten. Von SpamAssassin werden auch die Black- und Whitelist-Einträge für einzelne Absender ausgewertet und mit entsprechenden Punktegutschriften umgesetzt.
- Ist ein Collax Virus Protection dem System lizenziert und für E-Mail aktiviert, wird im nächsten Schritt die E-Mail bzw. deren Attachments mit diesem Produkt auf Viren überprüft.
- Ist auf dem System der ClamAV-Filter für E-Mail aktiviert, wird im letzten Schritt die E-Mail bzw. deren Attachments mit diesem freien Produkt auf Viren überprüft.

Ist die E-Mail ohne Auffälligkeiten bis zum Ende durch das Mailsystem gelaufen, wird sie nun abhängig von der genauen Konfiguration in das Postfach eines Benutzers zugestellt oder per SMTP bei einem weiteren Mailserver abgeliefert.

13.3 GUI-Referenz: *SMTP-Versand*

(Dieser Dialog befindet sich unter *Mail und Messaging – Mail – SMTP-Versand*

Dieser Dialog enthält die Basiseinstellungen für den allgemeinen Versand von E-Mails. Ist der Dienst nicht korrekt konfiguriert, kann das System keine eigenen Mails (etwa an den Administrator) versenden.

Soll dieser Dienst verschlüsselte Verbindungen über TLS verwenden, müssen zunächst eines oder mehrere Serverzertifikate erstellt oder installiert werden.

13.3.1 Felder in diesem Formular

- *Zertifikat*: Um TLS zu verwenden, kann für den SMTP-Dienst schon vorher ein Zertifikat erstellt oder importiert worden sein. In dieser Liste werden alle geeigneten Zertifikate auf dem System angezeigt. Hier wird das für den Mailserver entsprechende Zertifikat ausgewählt.

  Für abgehende und einkommende Verbindungen kann das gleiche Zertifikat verwendet werden, da es sich auch um den gleichen Mailserver handelt.

  Auch wenn kein Zertifikat ausgewählt wird, kann TLS für abgehende E-Mails verwendet werden.
- *TLS verwenden*: Hier wird eingestellt, ob und wann TLS für abgehende E-Mails verwendet werden soll. TLS dient zur Verschlüsselung der SMTP-Sitzung und damit auch der Verschlüsselung der Authentifizierungsinformationen.

  Niemals: Hier werden die Sitzungsinformationen im Klartext übertragen. Dies stellt kein Sicherheitsniveau dar, SMTP-Sitzungen funktionieren jedoch in den meisten aller Fälle.

  Die Option *Wenn möglich* führt dazu, dass der Server TLS-Verschlüsselung verwendet, falls der Remoteserver dies ebenso unterstützt. Dies gilt als optimale Einstellung, da das Sicherheitsniveau bei Bedarf erhöht wird und gleichzeitig gewährleistet ist, dass E-Mails ins Internet ausgeliefert werden können.

  Mit *Immer* und *Strikt* wird die TLS-Verschlüsselung der SMTP-Sitzung erzwungen, wobei *Strikt* zusätzlich den Namen des Remoteservers anhand der Zertifikatsinformationen prüft. Das Sicherheitsniveau ist damit hoch, allerdings sind diese Einstellungen für die Auslieferung von E-Mails ins Internet nicht geeignet.
- *Relay verwenden*: Diese Option muss aktiviert werden, wenn alle abgehenden E-Mails über einen bestimmten Relay-Server verschickt werden sollen.

Dies ist meist dann der Fall, wenn die eigene Internetanbindung mit wechselnden IP-Nummern versehen ist. Dann kommt es meist zu Schwierigkeiten, E-Mails direkt selbst auszuliefern, da die aktuelle, eigene IP-Nummer bei manchen Mailservern geblockt sein kann. In diesem Fall wird alle ausgehende E-Mail immer an den Mailserver des Providers geschickt, der die E-Mail dann wiederum weiterleitet und zustellt („Relay-Server“).

Ist diese Option nicht aktiviert, fragt der lokale SMTP-Server für jede Empfängerdomain im DNS den zuständigen Mailserver ab und baut eine SMTP-Verbindung zu ihm auf.

- *Relay-Host*: Soll ein Relay-Server verwendet werden, wird hier der Hostname (FQDN) oder die IP-Adresse dieses Servers eingetragen.
- *Port*: Soll ein Relay-Server verwendet werden, kann hier zusätzlich der Port des Relay-Hosts eingegeben werden, falls dieser vom Standard abweicht. Bleibt das Feld leer, wird der Standard-Port 25 für SMTP verwendet.
- *Benutzerkennung*: Verlangt der Relay-Server eine Authentifizierung, wird hier die Benutzerkennung zur Anmeldung hinterlegt.
- *Passwort*: Verlangt der Relay-Server eine Authentifizierung, wird hier das Passwort zur Anmeldung hinterlegt.
- *Maildomain*: Diese Domain wird bei abgehenden E-Mails angehängt, wenn der Absender keine Domain gesetzt hat. Dies ist insbesondere bei E-Mails der Fall, die vom System selbst generiert werden.

  Wird hier kein Eintrag ausgewählt, wird der Name dieses Systems (FQDN) verwendet. Dies kann jedoch zu Problemen führen, wenn Administrator-E-Mails an externe Empfänger weitergeleitet werden.
- *Zeit bis zur Warnung über verspätete Nachrichten*: Wenn eine E-Mail nicht sofort zugestellt werden kann, versendet das System regelmäßig eine Information an den Absender. Hier wird das

Zeitintervall eingestellt, in welchem die Warnungen versendet werden. Sinnvolle Intervalle liegen zwischen 1 bis 4 Stunden.

- *Sende Entwarnung*: Wenn eine E-Mail nach einer Verzögerung letztendlich versendet werden konnte, kann dies dem Absender mit dieser Option mitgeteilt werden.
- *Maximale Zeit einer Nachricht in der Warteschlange*: Dieser Wert gibt an, wie lange das System maximal versucht, eine verzögerte E-Mail zuzustellen. Nach dieser Zeit wird dem Absender mitgeteilt, dass die Zustellung nicht erfolgen konnte. Praktikable Werte liegen zwischen 1 und 3 Tagen.
- *Wartezeit beim Versand*: Wenn hier eine Wartezeit eingetragen ist, wird der Versand von E-Mails entsprechend lange verzögert. Nach Ablauf der von der ersten E-Mail ausgelösten Zeitspanne werden alle E-Mails in der Mailqueue versendet. Dadurch kann bei Wählverbindungen die Anzahl der Verbindungen ins Internet reduziert werden.
- *Absenderdomain auf Maildomain umschreiben*: Durch das Aktivieren dieser Option wird in den E-Mails von Benutzern, die den Mailbox-Namen als Absenderadresse verwenden, die Absenderadresse so umgeschrieben, dass sie einer der „offiziellen“ E-Mail-Adressen entspricht.

  Wenn der Benutzer mehr als eine Aliasadresse hat (z. B. weil mehr als eine Maildomain verwendet wird), wird die erste im LDAP gefundene Adresse verwendet. Welche das ist, ist mehr oder weniger zufällig.
- *Alternativer SMTP-Servername*: Für die Kommunikation über SMTP ist ein SMTP-Servername erforderlich. Soll der SMTP-Servername sich vom internen Hostnamen unterscheiden, ist hier der über externe DNS-Server auflösbarer Servername für den MX-Record einzutragen. Wird dieses Feld leergelassen, wird als SMTP-Servername der eingetragene FQDN dieses Servers verwendet.

- *Sprache für DSN Nachrichten*: Der Collax E-Mail Server unterstützt *Delivery Status Notifications (DSN)*. Über DSN werden dem Absender Informationen mitgeteilt, ob sich eine E-Mail-Zustellung verzögert oder diese sogar fehlgeschlagen ist. Mit dieser Option kann gewählt werden, ob die DSN in Englischer oder wahlweise in Deutsch und Englisch zugestellt wird.

13.3.2 Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten von SMTP-Versand beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten von SMTP-Versand beenden. Die Änderungen werden gespeichert.

13.4 GUI-Referenz: *SMTP-Empfang*

(Dieser Dialog befindet sich im Zusatzmodul *Collax Communication Server* und *Collax Mail Security* unter *Mail und Messaging – Mail – SMTP-Empfang*)

In diesem Dialog werden die verschiedenen Einstellungen vorgenommen, die den SMTP-Empfang betreffen.

Über die Berechtigungen kann eingestellt werden, aus welchen Netzen der SMTP-Dienst erreichbar sein soll. Ist das System mit einer wechselnden IP-Nummer mit dem Internet verbunden, können keine E-Mails aus dem Internet direkt per SMTP zugestellt werden. In diesem Fall müssen Postfächer bei einem Provider verwendet werden, und der Zugriff auf den SMTP-Server aus dem Internet kann deaktiviert bleiben.

Soll dieser Dienst verschlüsselte Verbindungen über TLS verwenden, müssen zunächst eines oder mehrere Serverzertifikate erstellt oder installiert werden.

TLS gewährleistet nur eine sichere Übertragung von E-Mails zwischen zwei benachbarten Systemen. Dies kann etwa zwischen einer Zweigstelle und der Zentrale eines Unternehmens oder einem Außendienstmitarbeiter und der Firma erfolgen. Sobald die E-Mail weiter durch das Internet versandt wird, wird sie unverschlüsselt übertragen. Um eine E-Mail verschlüsselt durch das gesamte Internet zu übertragen, muss auf den PCs beider Kommunikationspartner im Mailclient eine zusätzliche Software (PGP, S/MIME o. ä.) installiert werden.

13.4.1 Tab *Grundeinstellungen*, Abschnitt *Eingehende Verbindungen ...*

Eingehende Verbindungen sind alle SMTP-Verbindungen, die zum System aufgebaut werden und am System E-Mail einliefern. Das können Verbindungen aus dem Internet sein, mit einem meist größeren Anteil können dies aber auch Verbindungen aus dem lokalen Netz sein.

13.4.1.1 Felder in diesem Abschnitt

- *Postmaster*: Der „Postmaster“ ist die Person, die kontaktiert wird, wenn Probleme mit dem Mailsystem auftreten. Sehr häufig handelt es sich bei diesen Problemen um unzustellbare E-Mails. E-Mails für den Postmaster werden in bestimmten Situationen vom System selbst generiert, sie können aber auch von Personen versendet worden sein.

Wird hier kein Benutzer ausgewählt, ist „admin“ der Postmaster.

- *Zertifikat*: Um TLS zu verwenden, muss für den SMTP-Dienst im Vorfeld ein Zertifikat erstellt oder importiert worden sein. In dieser Liste werden alle geeigneten Zertifikate auf dem System angezeigt. Hier muss das für den Mailserver entsprechende Zertifikat ausgewählt werden.

  Wird kein Zertifikat ausgewählt, kann TLS nicht verwendet werden.

13.4.2 Tab *Grundeinstellungen*,Abschnitt *SMTP-Port (25)*

13.4.2.1 Felder in diesem Abschnitt

- *SMTP-AUTH aktivieren*: Normalerweise nimmt der SMTP-Dienst nur E-Mails an, die entweder für eine interne Maildomain bestimmt sind oder die von einem System eingeliefert werden, welches die Berechtigung zum „Weiterleiten“ („Relayen“) hat. Letzteres wird üblicherweise nur für IP-Adressen im lokalen Netz erlaubt.

  Wird diese Option aktiviert, kann der SMTP-Dienst auch von Systemen bzw. Benutzern in „fremden“ Netzen zum Relayen von E-Mail verwendet werden. Dazu müssen sich diese Benutzer am System authentifizieren.
- *Benutzeradresse prüfen*: Ist diese Option aktiviert, wird für authentifizierte Benutzer der Absender überprüft. Nur wenn der Login-Name und die Absenderadresse zusammengehören, wird die E-Mail angenommen.

  Wenn dieses System E-Mails von anderen Mailservern annehmen und weiterleiten soll und diese Systeme dazu eine Authentifizierung durchführen müssen, darf diese Option nicht

aktiviert sein. Da in diesem Fall die Absenderadressen nicht zu dem Login des anderen Mailservers gehören, wird die Annahme der E-Mails verweigert.

- *Authentifizierung nur mit TLS*: Grundsätzlich wird bei einer SMTP-Authentifizierung das Passwort im Klartext übermittelt und könnte abgehört werden. Eine sichere, verschlüsselte Übertragung des Passworts ist nur bei der Aktivierung von TLS (Transport Layer Security) gegeben. Mit dieser Option kann sichergestellt werden, dass der SMTP-Dienst eine Authentifizierung nur bei aktiviertem TLS durchführt. Ist TLS mit dem Client nicht möglich, ist auch die Verbindung nicht möglich.
- *Client-Zertifikat erzwingen*: Eine sichere Anmeldung an einem Mailserver ist nur bei verschlüsseltem Austausch der Zugangsdaten möglich. Dazu muss in jeder SMTP-Verbindung TLS (Transport Layer Security) aktiviert werden. Für eine TLS-Verbindung benötigt jedes der beiden Systeme ein Zertifikat.

  Ist diese Option aktiviert, wird bei eingehenden Verbindungen von der Gegenseite immer ein Zertifikat verlangt.

13.4.3 Tab *Grundeinstellungen*,Abschnitt *Submission-Port (587)*

Der Submission Port (587) wird verwendet, um ausschließlich von authentifizierten Benutzern E-Mails entgegenzunehmen. Die Trennung von Submission und SMTP Port 25 garantiert somit, dass Verbindungen zu externen SMTP-Servern durch internen E-Mail Verkehr nicht beeinflußt werden.

13.4.3.1 Felder in diesem Abschnitt

- *Benutzeradresse prüfen*: Ist diese Option aktiviert, wird für authentifizierte Benutzer der Absender überprüft. Nur wenn der Login-Name und die Absenderadresse zusammengehören, wird die E-Mail angenommen.

  Diese Option ist sinnvoll, wenn E-Mails nur von Mail-Clients angenommen werden.
- *Zugang nur mit TLS*: Eine sichere, verschlüsselte Übertragung des Passworts ist nur bei der Aktivierung von TLS (Transport Layer Security) gegeben. Mit dieser Option kann sichergestellt werden, dass der SMTP-Dienst eine Authentifizierung nur bei aktiviertem TLS durchführt. Ist TLS mit dem Client nicht möglich, ist auch die Verbindung nicht möglich.

13.4.4 Tab *Berechtigungen*, Abschnitt *Zugriff erlauben für ...*

13.4.4.1 Felder in diesem Abschnitt

- *SMTP-Dienst*: In dieser Liste wird ausgewählt, welche Gruppen eine Verbindung zum SMTP-Server herstellen dürfen. Die Berechtigung bezieht sich nur auf Rechner und Netze, nicht auf Benutzer.

  Zusätzlich zu den hier angegebenen Gruppen erhalten auch alle Gruppen, die dieses System als Mail-Relay verwenden dürfen, die Berechtigung, den SMTP-Server zu kontaktieren.
- *Mail-Relay ohne Authentifizierung*: In dieser Liste wird ausgewählt, welche Gruppen E-Mails an externe Maildomains ohne Authentifizierung versenden dürfen. Die Berechtigung bezieht sich nur auf Rechner und Netze, nicht auf Benutzer.

  Authentifizierte Benutzer bzw. Systeme dürfen immer E-Mails

an externe Maildomains versenden. Wenn nur authentifizierten Benutzern der Versand von E-Mails ermöglicht werden soll, muss hier keine Gruppe ausgewählt werden.

13.4.5 Tab *Optionen*

13.4.5.1 Felder in diesem Abschnitt

- *Logauswertung aktivieren*: Ist diese Option aktiv, wird die Logauswertung für den SMTP-Server aktiviert. Dann sind in der *Systemüberwachung* Statistiken über die Nutzung des Mailservers verfügbar.
- *Mailfilter für alle E-Mails*: Ist diese Option aktiviert, werden alle E-Mails durch die Spam- und Virenfilter geleitet. Die Kopfzeilen- und MIME-Filter sind davon nicht betroffen.

  Sollen E-Mails nur für Empfänger in bestimmten Maildomains gefiltert werden, muss diese Option deaktiviert und im Dialog *Domains* die Filteroption für die jeweilige Domain gesetzt werden.

13.4.6 Tab *Optionen*, Abschnitt *Eingehende Verbindungen …*

13.4.6.1 Felder in diesem Abschnitt

- *Client muss sich beim HELO identifizieren*: Abhängig von diesem Parameter wird die HELO-Meldung bei einkommenden SMTP-Verbindungen untersucht.

  Die Einstellung *nein* erlaubt dem Client, beliebige Angaben mit dem HELO zu senden.

  Wird die Einstellung *ja* aktiviert, muss der Client einen syntaktisch korrekten Hostnamen schicken. Es wird jedoch nicht anhand der DNS-Datenbank geprüft, ob der Name auch gültig ist.

Mit der Einstellung *strikt* muss der angegebene Name zusätzlich ein FQDN und per DNS auflösbar sein.

Die Einstellungen *ja* und *strikt* können die Kommunikation mit manchen fehlerhaft konfigurierten Gegenstellen unterbinden. Von diesen Systemen werden keine E-Mails angenommen. Dies ist in erster Linie eine wirkungsvolle Maßnahme gegen Spam, kann aber in Einzelfällen zu Problemen führen.

- *Maximale Größe einer E-Mail*: Dieser Parameter legt die maximale Größe einer einzelnen E-Mail in Megabyte fest. Folgendes ist bei der Angabe zu berücksichtigen: Da ein- oder ausgehende E-Mails mit Anhängen vom E-Mail-Client kodiert werden, ist die Größe beim Versand oder Empfang um ungefähr ein Drittel größer, als ursprünglich beim Verfassen der E-Mail-Daten auf dem Client.
- *Absenderadresse prüfen*: Bei der Aktivierung dieser Option wird geprüft, ob die Maildomain des Absenders in der DNS-Datenbank existiert (A- oder MX-Record). Ist dies nicht der Fall, wird die E-Mail zurückgewiesen.

  Für lokale Absender wird zusätzlich geprüft, ob die Absenderadresse auf dem Collax Security Gateway existiert. Ist dies nicht der Fall, wird die E-Mail zurückgewiesen.

13.5 GUI-Referenz: *Domains*

(Diese Option befindet sich im Zusatzmodul *Collax Communication Server* und *Collax Mail Security*)

(Dieser Dialog befindet sich unter *Mail und Messaging – Mail – Domains*)

In diesem Dialog werden die Maildomains angegeben, für die dieses System E-Mails annimmt und weiter zustellt.

13.5.1 *Maildomain wählen*

(Dieser Dialog befindet sich unter *Mail und Messaging – Mail – Domains*)

13.5.1.1 Felder in diesem Dialog

- *Gewichtung*: Zeigt den Wert der Gewichtung der angelegten Maildomain.
- *Domain*: Der Name der Maildomain darf Zeichen nach dem Standard für Internationalisierung von Domain-Namen in Anwendungen (IDNA) beinhalten.

  Es obliegt der E-Mail-Client-Anwendung den Domain-Namen korrekt in Punycode umzuwandeln, damit der Versand von E-Mails mit Umlauten funktioniert.
- *Kommentar*: Ein Kommentartext zu dieser Maildomain.

13.5.1.2 Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion können die Einstellungen einer Maildomain bearbeitet werden.
- *Löschen*: Mit dieser Aktion wird die ausgewählte Maildomain gelöscht.

13.5.1.3 Aktionen für diesen Dialog

- *Hinzufügen*: Mit dieser Aktion wird der Dialog zum Anlegen einer neuen Maildomain gestartet.

13.5.2 *Maildomain bearbeiten*

(Dieser Dialog befindet sich unter *Mail und Messaging – Mail – Domains*)

13.5.2.1 Tab *Grundeinstellungen*, Abschnitt *Grundeinstellungen*
Felder in diesem Abschnitt

- *Domain*: Der Name der Maildomain.
- *Gewichtung*: Hier wird der Wert der Gewichtung der Maildomain festgelegt. Die Gewichtung wird verwendet, um die primäre E-Mail-Adresse zu generieren. Wenn Benutzer Postfächer in mehreren Maildomains besitzen, wird durch den Gewichtungswert gesteuert, welche Domain für die primäre E-Mailadresse dieser Benutzer benutzt wird. Die Maildomain mit dem höchsten Gewichtungswert wird für die primäre E-Mail-Adresse eingesetzt.
- *Kommentar*: Ein Kommentartext zur Maildomain.

- *Art*: E-Mails können per SMTP an einen anderen Mailserver weitergeleitet werden. Dabei stehen die Optionen *interne Weiterleitung* und *externe Weiterleitung* zur Auswahl. Dies bezieht sich nicht auf die IP-Adresse des Zielsystems, sondern auf den Urspung der E-Mail.

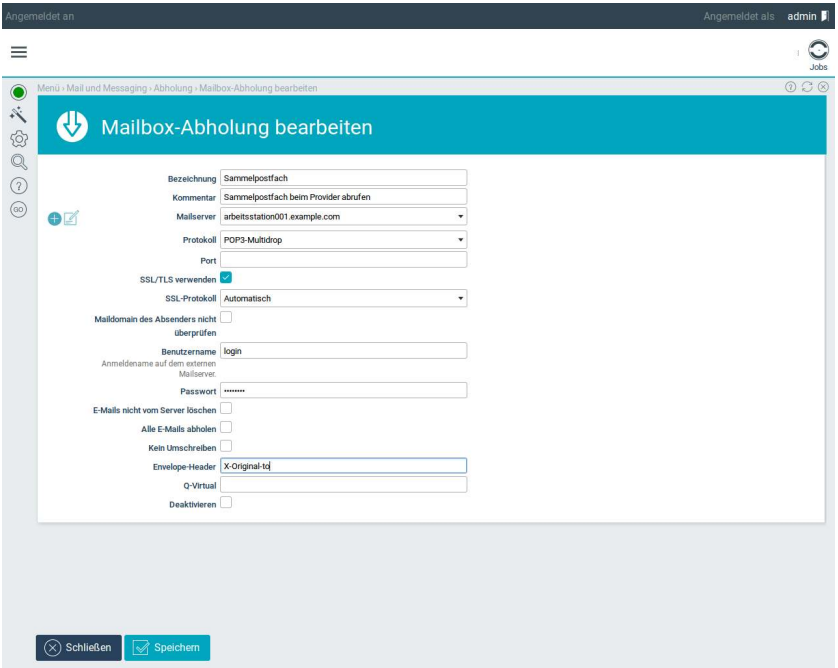
  Bei *interner Weiterleitung* wird für die Maildomain aus allen Netzen E-Mail angenommen, auch aus dem Internet. Der Collax Security Gateway arbeitet als Mail-Relay.

  Bei *externer Weiterleitung* werden nur lokal erzeugte E-Mails bzw. E-Mails von Systemen angenommen, die über die *Benutzungsrichtlinien* die *Relay-Berechtigung* besitzen. Der Collax Security Gateway arbeitet nur für bekannte Systeme als Relay.
- *E-Mails filtern*: Ist diese Option aktiviert, werden alle E-Mails an Empfänger in dieser Domain durch die E-Mail-Filter für Spam und Viren geleitet. Die Kopfzeilen- und MIME-Filter sind davon nicht betroffen.

  Die Einstellung hat keine weitere Wirkung, wenn die E-Mail-Filter in den Einstellungen zum SMTP-Dienst aktiviert sind.
- *Weiterleiten an Server*: Hier wird die IP-Adresse oder der Hostname des Mailservers angegeben, an den die E-Mails für diese Domain per SMTP weitergeleitet werden sollen.
- *SMTP-Port*: Soll ein Relay-Host verwendet werden, kann hier zusätzlich der Port des Relay-Hosts eingegeben werden, falls dieser vom Standard abweicht. Bleibt das Feld leer, wird der Standard-Port 25 für SMTP verwendet.
- *SSL/TLS verwenden*: Hier kann angegeben werden, ob mit diesem Mailserver eine Verschlüsselung mit SSL/TLS verwendet werden soll. Weitere Hinweise dazu bzw. zu möglichen Problemen werden in den allgemeinen SMTP-Einstellungen gegeben (S. 454).
- *Benutzername*: Wenn der oben angegebene Mailserver eine Authentifizierung verlangt, muss hier der Anmeldename angegeben werden.

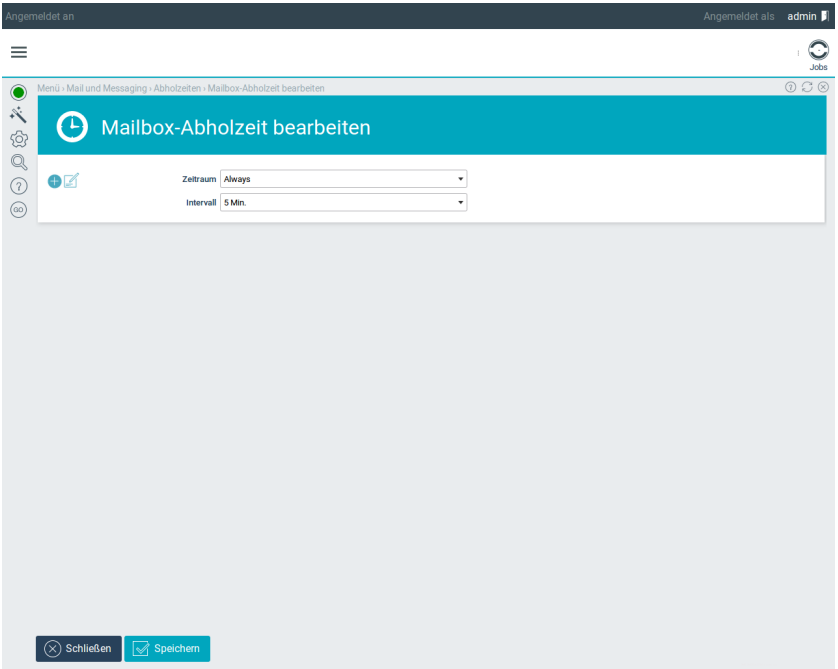
- *Passwort*: Wenn der oben angegebene Mailserver eine Authentifizierung verlangt, muss hier das Passwort angegeben werden.
- *Auch alle Subdomains weiterleiten*: Wird diese Option aktiviert, werden alle Subdomains der Maildomain weitergeleitet.

13.6 Schritt für Schritt: Postfach abrufen



- Wechseln Sie zu *Mail und Messaging – Mail – Abholung*.
- Öffnen Sie mit *Mailbox-Abholung einrichten* den Dialog zum Anlegen eines Abholjobs.
- Vergeben Sie einen *Namen* und einen *Kommentar* für das Postfach.
- Unter *Mail-Server* geben Sie den Mail-Server an, auf dem das zu leerende Postfach liegt.
- Unter *Protokoll* stellen Sie ein, mit welchem Verfahren die E-Mails heruntergeladen werden sollen. Meist wird *POP3-Multidrop* verwendet. Bei diesem Verfahren sind alle E-Mails in einem einzigen Postfach abgelegt.

- Wenn Sie kein Multidrop verwenden, sondern für jede Mail-Adresse ein eigenes Postfach beim Provider eingerichtet haben, dann müssen Sie für jedes Postfach einen eigenen Abholjob einrichten. Wählen Sie dann als *Protokoll POP3* bzw. *IMAP* aus. Dann können Sie im unteren Teil des Dialogs auswählen, an welchen *Benutzer* das jeweilige Postfach zugestellt werden soll.
- Normalerweise prüft der Collax Security Gateway, ob die Absenderdomain existiert. Ist diese nicht der Fall, werden die E-Mails verworfen. Wenn Sie alle E-Mails bekommen möchten, aktivieren Sie *Maildomain des Absenders nicht überprüfen*.
- Unter *Benutzername* und *Passwort* geben Sie die Zugangsdaten zum Mailserver an.
- Bei einem Sammelpostfach benötigt der Mailserver im Collax Security Gateway zusätzliche Informationen, an wen den die E-Mail ursprünglich verschickt wurde. Der Mailserver des Providers muss dies in einer gesonderten Zeile im Header der E-Mail speichern. Untersuchen Sie den Header einer E-Mail, um den Feldbezeichner herauszufinden. Diesen tragen Sie unter *Envelope-Header* ein. Benutzt Ihr Provider etwa den Mailserver *Postfix*, lautet der Bezeichner *X-Original-To*.



- Wechseln Sie zu *Abholzeiten*.
- Fügen Sie einen *Zeitraum* hinzu.
- Setzen Sie für den *Zeitraum Always* etwa ein *Intervall* von *5 Minuten*. Wenn Sie keine permanente Internetverbindung haben, wählen Sie das *Intervall* entsprechend größer.

13.7 GUI-Referenz: *Abholung*

(Diese Option befindet sich im Zusatzmodul *Collax Communication Server* und *Collax Mail Security*)

(Dieser Dialog befindet sich unter *Mail und Messaging – Mail – Abholung*)

In diesem Dialog können Abholaufträge verwaltet werden, die E-Mails aus externen Postfächern abholen und ins lokale Mailsystem einspeisen. Dies wird häufig für ein Sammelpostfach benötigt, in dem vom Provider die gesamte E-Mail für ein Unternehmen gespeichert wird.

13.7.1 *Mailboxen*

(Dieser Dialog befindet sich unter *Mail und Messaging – Mail – Abholung*)

13.7.1.1 Felder in diesem Dialog

- *Bezeichnung*: Hier wird der Name des konfigurierten Abholauftrags angezeigt.
- *Typ*: Diese Spalte gibt den genauen Typ des externen Postfachs an.
- *Kommentar*: Hier wird der Kommentartext zu diesem Abholauftrag angezeigt.
- *Aktiv*: Hier wird die Einstellung angezeigt, ob das externe E-Mailpostfach abgeholt werden soll (aktiv), oder ob dies deaktiviert wurde.

13.7.1.2 Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird die Konfiguration des ausgewählten Abholauftrags bearbeitet.
- *Löschen*: Mit dieser Aktion wird der Abholauftrag für das Postfach gelöscht.

13.7.1.3 Aktionen für diesen Dialog

- *Mailbox-Abholung anlegen*: Mit dieser Aktion wird ein neuer Abholauftrag für ein externes Postfach angelegt.

13.7.2 *Mailbox-Abholung bearbeiten*

(Dieser Dialog befindet sich unter *Mail und Messaging – Mail – Abholung*)

13.7.2.1 Felder in diesem Dialog

- *Bezeichnung*: Eine Bezeichnung für den Abholauftrag.
- *Deaktivieren*: Mit dieser Einstellung kann ein Abholauftrag vorübergehend deaktiviert werden. Die Daten des Auftrags bleiben erhalten, er wird jedoch nicht mehr durchgeführt.
- *Kommentar*: Ein Kommentartext zu dem Abholauftrag. Dieser wird in der Übersicht mit angezeigt.
- *Mailserver*: Hier wird die IP-Adresse oder der Hostname des Mailservers angegeben, bei dem das abzufragende Postfach liegt.
- *Protokoll*: Je nachdem, wie das Postfach auf dem Mailserver

eingerichtet ist, muss hier das entsprechende Protokoll zur Abfrage ausgewählt werden.

POP3 und IMAP sind Standardprotokolle für das Abfragen eines Postfachs. Wird ein solches abgefragt, kann die E-Mail pro Abholauftrag nur einem konkreten Benutzer zugestellt werden. Bei „Multidrop"-Postfächern werden alle E-Mails in ein einziges Postfach abgelegt und der Collax Security Gateway muss den Inhalt des Postfachs wieder auf unterschiedliche Benutzer verteilen.

ESMTP ist ein Sonderfall des SMTP-Protokolls, bei dem kein eigentliches Postfach auf dem Mailserver existiert. Vielmehr wird die E-Mail für dieses System in der Mailqueue aufbewahrt, und der Abholauftrag löst auf dem Mailserver eine Zustellung per SMTP auf das lokale System aus. Dazu muss in den Benutzungsrichtlinien für den Mailserver der SMTP-Zugriff freigeschaltet werden.

Im Zweifelsfall sollte der Provider über das eingestellte Verfahren Auskunft erteilen können.

- *Port*: Hier wird der Port auf dem Server angegeben, der für die Kommunikation benutzt werden soll. Bleibt dieses Feld leer, wird der Standardport für das eingestellte Protokoll verwendet.
- *SSL/TLS verwenden*: Wenn das eingestellte Protokoll verschlüsselte Verbindungen erlaubt, kann hier angegeben werden, ob SSL/TLS für das Postfach verwendet werden soll.

  Ob SSL/TLS tatsächlich genutzt werden kann, ist davon abhängig, ob der Mailserver entsprechende Unterstützung für SSL/TLS bietet.
- *SSL-Protokoll*: Mit diesem Parameter kann bei der Verwendung von Verschlüsselung ein bestimmtes SSL-Protokoll erzwungen werden. Dies ist notwendig, wenn die automatische Aushandlung des Protokolls nicht funktioniert (beispielsweise beim Abholen von bestimmten Versionen des *Microsoft Exchange-Servers*).

In den meisten Fällen kann diese Einstellung auf *automatisch* gesetzt werden.

- *Maildomain des Absenders nicht überprüfen*: Üblicherweise werden die E-Mails überprüft, ob die Maildomain des Absenders in der DNS-Datenbank existiert. E-Mails von nicht existenten Absendern werden verworfen. Durch das Aktivieren dieser Option wird die Überprüfung ausgeschaltet.
- *Benutzername*: Hier wird der Benutzername zur Anmeldung am Mailserver eingegeben.
- *Passwort*: Hier wird das Passwort zur Anmeldung eingegeben.
- *Benutzername*: Hier wird der Benutzername für die ESMTP-Authentifizierung angegeben.

  Dieses Feld kann leer bleiben, wenn der Provider keine ESMTP-Authentifizierung verlangt.
- *Passwort*: Das Passwort für die ESMTP-Authentifizierung wird hier eingegeben.
- *Maildomain*: Hier muss aus den auf dem lokalen System vorhandenen Domains diejenige ausgewählt werden, für die die ESMTP-Versendung gestartet werden soll.
- *Weiterleiten an*: Wenn das Postfach nicht vom Typ *Multidrop* ist, muss hier angegeben werden, wohin die E-Mails nach dem Herunterladen weitergeleitet werden sollen.

  Die E-Mails können an eine externe E-Mail-Adresse weitergeleitet werden.
- *Verteiler*: Hier kann aus der Liste der im System vorhandenen Verteilerlisten diejenige ausgewählt werden, an die die E-Mails zugestellt werden sollen.
- *Weiterleiten an diese E-Mail-Adresse*: Sollen die E-Mails an eine externe E-Mail-Adresse weitergeleitet werden, muss diese hier angegeben werden.
- *E-Mails nicht vom Server löschen*: Wird diese Option aktiviert,

löscht der Abholauftrag heruntergeladene E-Mails nicht auf dem Server. Dies ist bei der Einrichtung zum Testen oder bei Zugriff von verschiedenen Systemen auf das gleiche Postfach nützlich. Allerdings sollte das Postfach auf anderem Wege regelmäßig geleert werden.

Hinweis: In seltenen Fällen kann es zu mehrfacher Zustellung von E-Mails kommen, wenn diese Option aktiviert ist.

- *Alle E-Mails abholen*: Mit dieser Option wird festgelegt, dass bei jedem Abholvorgang alle auf dem E-Mail-Server vorhandenen Nachrichten abgeholt werden, auch wenn das Seen-Flag für Nachrichten schon gesetzt wurde. Diese Option ist nicht kombinierbar mit der Option *E-Mails nicht vom Server löschen*.
- *Kein Umschreiben*: Üblicherweise werden beim Abholprozess mit POP3 oder IMAP die Adressierungs-Kopfzeilen einer E-Mail umgeschrieben. Dies betrifft Adressen, die im To-, From-, CC-, BCC- und Reply-To-Feld stehen.

  Mit dieser Option kann unterbunden werden, dass das Mailsystem die Kopfzeilen editiert. Die Aktivierung dieser Option kann abhängig von Provider oder Postfach-Protokoll notwendig sein, falls ansonsten die weitere Filterung der E-Mails durch Spam- oder Kopfzeilenfilter nicht mehr funktioniert. Bei der Abholung aus einem POP3-Multidrop-Postfach kann es sein, dass die From-Adresse immer „root@domain.de“ beinhaltet. Die Zustellung der E-Mails funktioniert, aber die Spam- oder Kopfzeilen-Filterung kann fehlschlagen. In diesem Fall sorgt die Aktivierung dieser Option dafür, dass die Filtermechanismen wieder wirksam sind.
- *Envelope-Header*: Bei *Multidrop*-Mailboxen geht der ursprüngliche Empfänger der E-Mail „verloren“, da diese Information nicht unter allen Bedingungen in der E-Mail selbst enthalten ist (Problematik mit CC- und BCC-Feldern oder mehrfachen Empfängern). Die meisten Provider fügen daher beim Ablegen der E-

Mail in das Postfach eine zusätzliche Kopfzeile ein, in der der eigentliche Empfänger der E-Mail angegeben ist. Dies ist je nach Provider unterschiedlich, viele verwenden ein Feld „X-original-To“ für diese Information.

In diesem Feld muss der Name desjenigen Feldes im Header der E-Mail angegeben werden, das den tatsächlichen Empfänger einer E-Mail enthält. Nur mit dieser Hilfe kann der Inhalt eines Multidrop-Postfachs zuverlässig an die richtigen Benutzer zugeordnet werden. Fehlt eine solche Angabe, kann es zu Problemen kommen.

- *Q-Virtual*: Dieses Feld funktioniert analog zu *Envelope-Header*, eignet sich allerdings für den speziellen Fall, dass der Provider die Software „Qmail“ verwendet. Dann wird eine zusätzliche Headerzeile „Q-Virtual“ eingefügt. In dieser Zeile wird jedoch noch eine zusätzliche Information zum Postfach mitgespeichert. Diese muss entfernt werden, damit der richtige Empfänger ermittelt werden kann. In diesem Feld muss diese (immer gleiche) Zeichenkette angegeben werden, die dann aus dem Feld „Q-Virtual“ entfernt wird.

13.8 GUI-Referenz: *Abholzeiten*

(Diese Option befindet sich im Zusatzmodul *Collax Communication Server*und *Collax Mail Security*)

(Dieser Dialog befindet sich unter *Mail und Messaging – Mail – Abholzeiten*)

In diesem Dialog wird eingestellt, in welchen Zeiträumen und Intervallen die definierten Abholaufträge zum Leeren externer Postfächer ausgeführt werden sollen.

13.8.1 *Abholzeiten*

(Dieser Dialog befindet sich unter *Mail und Messaging – Mail – Abholzeiten*)

In dieser Tabelle wird festgelegt, in welchen Zeiträumen und Intervallen die definierten Abholaufträge zum Leeren externer Postfächer ausgeführt werden sollen.

13.8.1.1 Felder in diesem Dialog

- *Zeitraum*: Hier wird der im System angelegte Zeitraum angezeigt.
- *Intervall*: Hier wird das zugehörige Intervall angezeigt.

13.8.1.2 Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion können die Abholzeiten geändert werden.

- *Löschen*: Mit dieser Aktion wird der gewählte Abholzeitraum gelöscht.

13.8.1.3 Aktionen für diesen Dialog

- *Zeitraum hinzufügen*: Mit dieser Aktion kann ein weiterer Zeitraum hinzugefügt werden.

13.8.2 *Mailbox-Abholzeit bearbeiten*

(Dieser Dialog befindet sich unter *Mail und Messaging – Mail – Abholzeiten*)

13.8.2.1 Felder in diesem Dialog

- *Zeitraum*: Hier kann einer der im System angelegten Zeiträume ausgewählt werden. Darüber lässt sich beispielsweise beschränken, dass E-Mails nur tagsüber während der Arbeitszeit abgeholt werden. Jeder Zeitraum kann nur einmal für Abholaufträge konfiguriert werden.
- *Zeitraum*: Wird eine bereits bestehende Abholzeit bearbeitet, kann der Zeitraum selbst nicht geändert werden. Eine Änderung ist weiterhin in den *Benutzungsrichtlinien* möglich.
- *Intervall*: Hier wird das Intervall ausgewählt, in dem der Abholauftrag innerhalb des Zeitraums wiederholt ausgeführt wird. Das kleinste Intervall beträgt fünf Minuten.

13.8.3 GUI-Referenz: *E-Mail-Archivierung*

(Diese Option befindet sich im Zusatzmodul *Collax E-Mail Archive*)
(Dieser Dialog befindet sich unter *Mail und Messaging – Mail – E-Mail-Archivierung*)

13.8.3.1 Abschnitt *Hinweis*
Felder in diesem Abschnitt

- *Der SMTP-Dienst ist nicht aktiviert*: Um die E-Mail-Archivierung benutzen zu können, ist der SMTP-Dienst zu aktivieren. Falls dies nicht der Fall ist, kann über den angegebenen Link der SMTP-Dienst aktiviert werden.

13.8.3.2 Tab *Grundeinstellungen*, Abschnitt *Modus*
Felder in diesem Abschnitt

- *Aktivieren*: Mit dieser Option wird die Archivierung aktiviert.

13.8.3.3 Tab *Grundeinstellungen*, Abschnitt *Datenträger*
Felder in diesem Abschnitt

- *Größe*: Mit dieser Option lässt sich die Größe eines Volumes festlegen. Es kann entweder aus der Liste eine vorgegebene Größe für die gängigsten Medien ausgewählt werden, oder eine manuelle Eingabe erfolgen.
- *Größe in MB*: Bei manueller Größenangabe kann hier ein Wert eingetragen werden. Dieser Wert darf eine minimale Größe von 600 nicht unterschreiten.

- *Verzeichnis für ISO-Dateien*: In diesem Feld kann der Name des Verzeichnisses angegeben werden, in das die erzeugten ISO-Dateien abgelegt werden.

13.8.3.4 Tab *Berechtigungen*, Abschnitt *Zugriff auf ...*
Felder in diesem Abschnitt

- *Persönliche Archivsuche*: Benutzer der markierten Gruppen dürfen das E-Mail-Archiv durchsuchen. Die Suchfunktion kann über den Benutzer-Web-Access aufgerufen werden und beschränkt sich ausschliesslich auf die persönlich versendeten oder empfangenen E-Mails des eingeloggten Benutzers.

13.8.3.5 Tab *Berechtigungen*, Abschnitt *Zugriff auf Verzeichnis für ISO-Dateien*
Felder in diesem Abschnitt

- *Leseberechtigung*: Hier können die Gruppen ausgewählt werden, deren Mitglieder lesenden Zugriff auf das Share erhalten.
- *Schreibberechtigung*: Hier können die Gruppen ausgewählt werden, deren Mitglieder schreibenden Zugriff auf das Share erhalten.

13.8.3.6 Tab *Optionen*, Abschnitt *E-Mail-Auswahl*
Felder in diesem Abschnitt

- *Alle E-Mails archivieren*: Aktiviert die E-Mail-Archivierung, unabhängig von Sender- oder Empfänger-Domain.

- *Sender-Domains*: Aktiviert die Archivierung für E-Mails, die von den ausgewählten Domains gesendet wurden.
- *Empfänger-Domains*: Aktiviert die Archivierung für E-Mails, die an die ausgewählten Domains gesendet wurden. Hinweis: Wenn hier eine lokal verwaltete Maildomain ausgewählt wird, werden E-Mails auch an andere, nicht ausgewählte, aber lokal verwaltete Maildomains archiviert.
- *Interne Domains*: Aktiviert die Archivierung von E-Mails, deren Absender- und Empfängerdomain identisch mit einer der ausgewählten Domains ist.

13.8.3.7 Tab *Optionen*, Abschnitt *Indexierung*

Felder in diesem Abschnitt

- *Indexierung von*: Hier wird gewählt, ob die vollständige E-Mail, oder ob nur die Kopfzeilen der E-Mail indexiert werden soll.

13.8.3.8 Tab *Vier-Augen-Prinzip*, Abschnitt *Auditor-Zugriff erste Person*

Felder in diesem Abschnitt

- *Archivsuche*: Benutzer der markierten Gruppen dürfen das E-Mail-Archiv durchsuchen. Die Suchfunktion kann über den Benutzer-Web-Access aufgerufen werden und umfasst alle archivierten E-Mails des Systems. Die Suche kann nur nach Eingabe eines Kontrollpassworts, z.B. durch eine zweite Person, durchgeführt werden.

13.8.3.9 Tab *Vier-Augen-Prinzip*, Abschnitt *Auditor-Zugriff zweite Person* Felder in diesem Abschnitt

- *Kontrollpasswort für die Archivsuche*: Das Kontrollpasswort muss mindestens 12 Zeichen enthalten. Es können Sonderzeichen verwendet werden. Um das Vier-Augen-Prinzip durchzusetzen, ist an dieser Stelle die Vorgabe des Passworts durch eine weitere Person erforderlich.
- *Bestätigung Kontrollpasswort*: Da die Zeichen nicht im Klartext erscheinen, ist hier das Passwort zur Kontrolle durch die oben genannte Person nochmals einzugeben.
- *E-Mail-Benachrichtigung bei Archivsuche an*: Falls eine Suche in allen archivierten E-Mails gestartet wird, erhalten die angegebenen Adressen eine E-Mail-Nachricht. Es können mehrere Adressen, getrennt durch Zeilenumbruch, angegeben werden. Gültige Adressen sollen in der Form user@example.com eingegeben werden. Das Feld kann optional auch leergelassen werden.

13.8.3.10 Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten der E-Mail-Archivierung beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten der E-Mail-Archivierung beenden. Die Änderungen werden gespeichert.

13.8.4 *Archivstatus*

(Dieser Dialog befindet sich unter *Systembetrieb – E-Mail-Archivierung – Archivstatus*)

13.8.4.1 *Liste der Archiv-Volumes*

Spalten in der Tabelle

- *ID*: Die interne Identifikation eines Archiv-Volumes.
- *Status*: Beschreibt den aktuellen Status eines Archiv-Volumes.
  - Aktiv: Das Archiv-Volume wird zur Archivierung weiterhin beschrieben.
  - Inaktiv, kein ISO: Das Volume wird nicht mehr beschrieben. Aus diesem Volume wurde bisher noch kein ISO erstellt. Daher ist ein Löschen dieses Volumes noch nicht möglich.
  - Inaktiv, ISO erstellt: Das Volume wird nicht mehr beschrieben. Aus diesem Volume wurde bereits ein ISO erstellt. Dieses Volume kann gelöscht werden.
- *Plattenplatz (davon belegt)*: Beschreibt die eingestellte Größe des Volumes zum Erstellungszeitpunkt, mit Angabe des bisher verbrauchten Festplattenspeichers.
- *Angelegt*: Beschreibt den Erstellungszeitpunkt des Archiv-Volumes.
- *Name der ISO Datei*: Beschreibt den Namen unter dem die ISO-Datei erstellt wurde. Dieses Feld ist leer, wenn noch keine ISO-Datei existiert.

Aktionen für jeden Tabelleneintrag

- *Details*: Zeigt Detailinformationen zu einem Archiv-Volume an.
- *Volume deaktivieren*: Hier kann ein aktives Archiv-Volume deaktiviert werden, damit es nicht mehr beschrieben wird. Ein neues Archiv-Volume wird automatisch angelegt und aktiviert.
- *ISO erstellen*: Hier kann eine ISO-Datei aus einem deaktivierten Archiv-Volume erstellt werden. Die ISO-Datei wird unter dem angegebenen Namen in das Verzeichnis für ISO-Dateien abgelegt.
- *Volume entfernen*: Hier kann ein deaktiviertes Archiv-Volume, aus dem bereits eine ISO-Datei erstellt wurde, entgültig von der lokalen Festplatte gelöscht werden. Ein gelöschtes Volume kann nicht wiederhergestellt werden. Daher muss sichergestellt werden, dass die ISO-Datei erfolgreich auf dem gewählten Speichermedium gesichert wurde.

Aktionen für dieses Formular

- *Aktualisieren*: Mit dieser Aktion wird der aktuelle Archivstatus angezeigt.

13.8.4.2 *Details*

Felder in diesem Formular

- *ID*: Die interne Identifikation eines Archiv-Volumes.
- *Status*: Beschreibt den aktuellen Status eines Archiv-Volumes.
  - Aktiv: Das Archiv-Volume wird zur Archivierung weiterhin beschrieben.
  - Inaktiv, kein ISO: Das Archiv-Volume wird nicht mehr beschrieben. Aus diesem Archiv-Volume wurde bisher noch kein

ISO erstellt. Daher ist ein Löschen dieses Archiv-Volumes noch nicht möglich.
    - Inaktiv, ISO erstellt: Das Archiv-Volume wird nicht mehr beschrieben. Aus diesem Archiv-Volume wurde bereits ein ISO erstellt. Dieses Archiv-Volume kann gelöscht werden.
- *Angelegt am*: Beschreibt den Erstellungszeitpunkt des Archiv-Volumes.
- *Deaktiviert am*: Beschreibt den Zeitpunkt der Deaktivierung des Archiv-Volumes.
- *Geschlossen am*: Beschreibt den Zeitpunkt an dem die ISO-Datei erstellt wurde.
- *Plattenplatz (davon belegt)*: Beschreibt die eingestellte Größe des Archiv-Volumes zum Erstellungszeitpunkt, mit Angabe des bisher verbrauchten Festplattenspeichers.
- *Datum der ersten E-Mail*: Beschreibt den Zeitpunkt an dem die erste E-Mail in dieses Archiv-Volume geschrieben wurde.
- *Datum der letzten E-Mail*: Beschreibt den Zeitpunkt an dem die letzte E-Mail in dieses Archiv-Volume geschrieben wurde.
- *Anzahl E-Mails*: Beschreibt die Anzahl der E-Mails, die in dieses Archiv-Volume gespeichert wurden.

Aktionen für dieses Formular

- *Zurück*: Diese Aktion führt zurück zur Übersicht des Archivstatus.

13.8.4.3 ISO erstellen

Abschnitt *Details*

Felder in diesem Abschnitt

- *ID*: Die interne Identifikation eines Archiv-Volumes.
- *Angelegt am*: Beschreibt den Erstellungszeitpunkt des Archiv-Volumes.
- *Plattenplatz (davon belegt)*: Beschreibt die eingestellte Größe des Volumes zum Erstellungszeitpunkt, mit Angabe des bisher verbrauchten Festplattenspeichers.
- *Datum der ersten E-Mail*: Beschreibt den Zeitpunkt an dem die erste E-Mail in dieses Archiv-Volume geschrieben wurde.
- *Datum der letzten E-Mail*: Beschreibt den Zeitpunkt an dem die letzte E-Mail in dieses Archiv-Volume geschrieben wurde.
- *Anzahl E-Mails*: Beschreibt die Anzahl der E-Mails, die in dieses Archiv-Volume gespeichert wurden.

Abschnitt *Einstellungen*

Felder in diesem Abschnitt

- *Name der ISO-Datei*: In diesem Feld kann der Name der zu erstellenden ISO-Datei angegeben werden.
- *Volume nach Generierung löschen*: Hier kann gewählt werden, ob das Archiv-Volume automatisch nach der Erstellung der ISO-Datei gelöscht werden soll. Ein gelöschtes Archiv-Volume kann nicht wiederhergestellt werden. Daher muss sichergestellt werden, dass die ISO-Datei erfolgreich auf dem gewählten Speichermedium gesichert wurde.

Abschnitt *Log*
Felder in diesem Abschnitt

- *Fortschritt*: Hier wird der Prozess der Erstellung der ISO-Datei angezeigt.

Aktionen für dieses Formular

- *Generieren*: Mit dieser Aktion wird die Erstellung der ISO-Datei gestartet.
- *Zurück*: Diese Aktion führt zurück zur Übersicht des Archivstatus.

13.8.5 GUI-Referenz: *Volume laden*

(Dieser Dialog befindet sich unter *Systembetrieb – E-Mail-Archivierung – Volume laden*)

Archiv-Volumes können im ISO-Format gespeichert und dann auf entsprechende optische Volumes gebrannt werden. Um den Inhalt dieser gebrannten Archiv-Volumes für die Archivsuche verfügbar zu machen, wird dieses Formular benutzt.

13.8.5.1 *Liste der geladenen Archiv-Volumes*

Es können per Fernzugriff Archiv-Volumes als Windows-Freigabe geladen und daraufhin durchsucht werden. Ist die Archivsuche beendet, kann das geladene Archiv-Volume abgemeldet und damit aus der Liste entfernt werden. Es ist möglich gleichzeitig mehrere Archiv-Volumes zu laden.

Spalten in der Tabelle

- *ID*: Die interne Identifikation eines Archiv-Volumes.
- *Größe*: Beschreibt die Größe des geladenen Archiv-Volumes in MB.
- *Datum der ersten E-Mail*: Beschreibt den Zeitpunkt an dem die erste E-Mail in dieses Archiv-Volume geschrieben wurde.
- *Datum der letzten E-Mail*: Beschreibt den Zeitpunkt an dem die letzte E-Mail in dieses Volume geschrieben wurde.
- *Anzahl E-Mails*: Beschreibt die Anzahl der E-Mails, die in dieses Volume gespeichert wurden.

Aktionen für jeden Tabelleneintrag

- *Abmelden*: Mit dieser Aktion wird das geladene Archiv-Volume abgemeldet. Nach der Aktion wird das Volume aus der Liste entfernt.

Aktionen für dieses Formular

- *Volume-Quelle angeben*: Mit dieser Aktion werden die Quelldaten angegeben, um Archiv-Volumes über eine Windows-Freigabe zu laden.

13.8.5.2 *Volume-Quelle*

Um ein Archiv-Volume, aus dem zuvor ein ISO erstellt und anschließend auf einen optischen Datenträger gebrannt wurde, für die E-Mail-Archivsuche zu laden, kann einmal der Datenträger selbst im Netzwerk als Freigabe zur Verfügung gestellt werden. Zum Zweiten

kann auch der Inhalt des Datenträgers in ein Verzeichnis einer PC-Arbeitsstation kopiert und im Netzwerk als Freigabe zur Verfügung gestellt werden.

In diesem Formular werden die Daten der Windows-Freigabe angegeben, um den Inhalt des Archiv-Volumes in die E-Mail-Archivsuche einzubinden.

Quelldaten
Felder in diesem Abschnitt

- *Rechnername oder IP-Adresse*: Hier wird der DNS-Name oder die IP-Adresse des Zielrechners angegeben.
- *Name der Freigabe*: Angabe des Namens unter dem das Volume auf dem Zielrechner freigegeben wurde.
- *Login*: Ist auf die Freigabe nur durch bestimmte Benutzer zugreifbar, dann kann hier der entsprechende Login-Name angegeben werden. Das Feld ist optional und kann für uneingeschränkten Zugriff auch leergelassen werden. Login und Passwort werden nicht gespeichert, sondern nur für diese Aktion benutzt.
- *Passwort*: Hier wird das Passwort zum Login-Namen angegeben. Login und Passwort werden nicht gespeichert, sondern nur für diese Aktion benutzt.

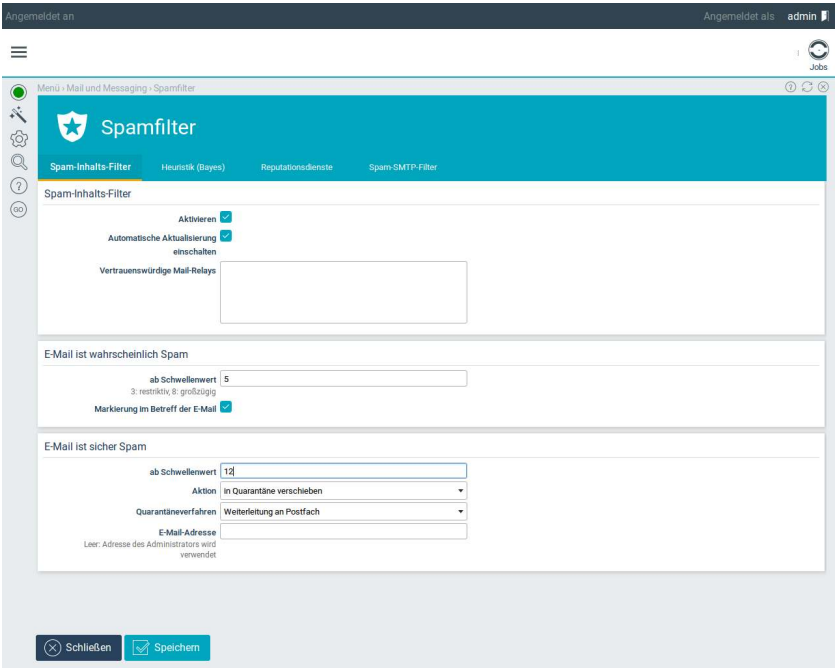
Aktionen für dieses Formular

- *Volume laden*: Mit dieser Aktion wird mit den angegebenen Daten das Archiv-Volume geladen und in der Liste der geladenen Volumes angezeigt. War der Ladeprozess erfolgreich, steht der Inhalt des geladenen Volumes für die Archivsuche zur Verfügung.
- *Zurück*: Führt zurück zur Liste der geladenen Archiv-Volumes, die angegebenen Daten werden verworfen.

Abschnitt *Ladeprozess*
Felder in diesem Abschnitt

- *Fortschritt*: Ist die Aktion Archiv-Volume laden ausgeführt, wird hier der Fortschritt des Ladeprozesses ausgegeben.

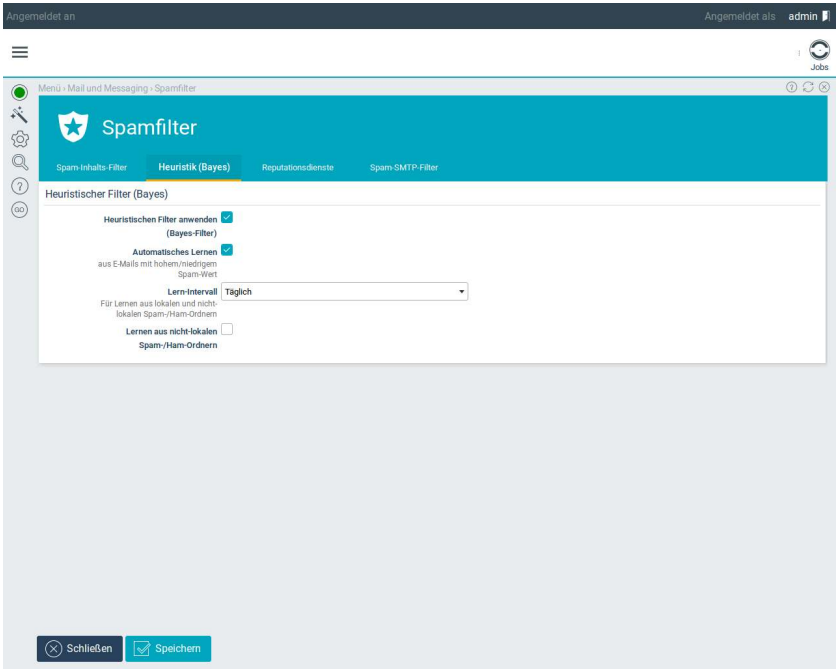
13.9 Schritt für Schritt: Spamfilter aktivieren



- Wechseln Sie zu *Mail und Messaging – Mail Security – Spam*.
- *Aktivieren* Sie den Spam-Filter.
- Die intern eingesetzte Software vergibt für bestimmte Kriterien Punkte. Je höher der Punktewert, desto größer ist auch die Wahrscheinlichkeit, dass eine E-Mail Spam ist. Unter *Spam-Schwellenwert* geben Sie die Grenze an, ab der eine E-Mail als Spam behandelt werden soll.
- Unter *Spam ab diesem Wert* legen Sie eine zweite Punktegrenze fest, bei deren Überschreiten die *Aktion* ausgelöst wird. Sie können dann die E-Mail *verwerfen* (also Löschen), in der Mailqueue

anhalten (in Quarantäne nehmen) oder in einem speziellen *IMAP-Ordner* ablegen.

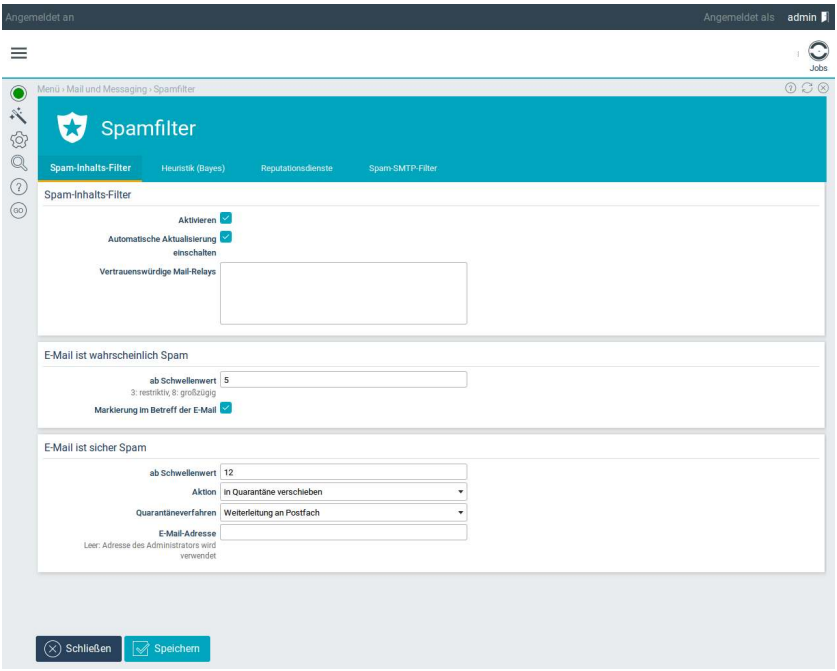
- Als Spam erkannte E-Mails können Sie auf verschiedene Arten weiterleiten. Wählen Sie hier *Als Textanhang weiterleiten*, damit eventuell enthaltene HTML-Formulare deaktiviert werden.
- Durch die *Markierung im Betreff der E-Mail* werden als Spam klassifizierte E-Mails markiert. Sie können diese Markierung dann nutzen, um in Ihrem Mailclient einen Filter einzurichten und solche Mails in einem eigenen Ordner abzulegen.



- Wechseln Sie auf den Reiter *Optionen*.
- Aktivieren Sie die *Automatische Whitelist* und setzen Sie den *Faktor der Whitelist* auf *50*. Über diese Whitelist bekommen Ab-

sender, die häufig E-Mails mit niedrigen Punktezahlen erreichen, einen Bonus.

- Aktivieren Sie *Automatisch trainieren*, um abhängig von der Punktezahl die Mails in „Spam-“ und „Ham-Ordner“ aufzuteilen.



- Wechseln Sie zum Reiter *Berechtigungen*.
- Aktivieren Sie den *Spam-/Ham-Ordner*.
- In diese IMAP-Ordner können Sie nun Spam und harmlose E-Mails („Ham“) sortieren. Ab einem Bestand von über 1000 E-Mails kann der Spamfilter dies als zusätzliche Wissensdatenbank heranziehen.
- Unter *Schreibrecht für* legen Sie fest, welche Gruppen in diese Ordner schreiben dürfen. Bedenken Sie, dass Mitglieder der

Gruppe Zugriff auf alle gespeicherten E-Mails haben und diese teilweise sensiblen Inhalts sein können.

13.10 GUI-Referenz: Mail Security

13.10.1 *Antivirus Mail-Filterung*

(Dieser Dialog befindet sich unter *Mail und Messaging – Mail Security – Antivirus Mail-Filterung*)

13.10.1.1 Tab *Grundeinstellungen*, Abschnitt *Filterung*

Felder in diesem Abschnitt

- *Aktivieren*: Diese Option schaltet die Filterung auf Viren für den E-Mail-Verkehr ein. Voraussetzung für die korrekte Filterung ist die Aktivierung mindestens eines Virenscanners.
- *E-Mail-Adresse des Virus-Administrators*: Hier wird eine E-Mail-Adresse für einen Administrator angegeben. Dieser Administrator erhält Statusinformationen vom Virenfilter.
- *Benutze*: Hier werden Scanner ausgewählt, die für Mailfilterung eingesetzt werden sollen.
- *Verdächtige Dateien blockieren*: Anhänge mit verdächtigem Namen werden blockiert. Dies betrifft hauptsächlich Dateien, deren Namen doppelte Extension-Bezeichnungen tragen. Alle Dateien, deren zweite Extension exe, vbs, pif, scr, bat, cmd, com, cpl oder dll enthalten werden als Virenmails behandelt.
- *Blockiere E-Mails, die Anhänge mit diesen Erweiterungen enthalten*: Anhänge mit bestimmten Datei-Extensions können hier ausge-

filtert werden. Die Datei-Extensions werden in dieser Textbox angegeben. Entsprechend werden die Emails blockiert, auch wenn die Dateien in Zip-Dateien oder in anderem Format gepackt sind. Es wird auch der „MIME content types“, der MIME-Name, oder der Dateityp berücksichtigt. Archivanhänge, die per ZIP komprimiert sind, wie beispielsweise .docx u.a., werden auch gefiltert, wenn hier zip angegeben wird.

13.10.1.2 Tab *Grundeinstellungen*, Abschnitt *Bei erkannten Viren*

Felder in diesem Abschnitt

- *Infizierte E-Mails*: Infizierte Nachrichten können durch unterschiedliche Methoden behandelt werden. Der Empfänger kann hierüber eine Warnung per E-Mail erhalten. Hierbei wird der infizierte Nachrichtenteil mit versendet. Alternativ können infizierte Nachrichten in Quarantäne geschoben und mit weiteren Methoden behandelt werden. Im einfachsten Fall können Nachrichten verworfen werden.
- *Benachrichtigung an*: Falls infizierte Nachrichten entdeckt werden kann hier gesteuert werden, an wen eine Benachrichtigung erfolgen soll.

13.10.1.3 Tab *Grundeinstellungen*, Abschnitt *Bei nicht überprüfbaren E-Mails ...*

Felder in diesem Abschnitt

- *Nicht überprüfbare E-Mails*: E-Mails können aufgrund von Verschlüsselung oder Passworschutz nicht bis in das letzte Detail geprüft werden. Mit dieser Option kann eingestellt werden, wie

mit solchen E-Mails verfahren wird. Der Empfänger kann hierüber eine Warnung per E-Mail erhalten. Hierbei wird der infizierte Nachrichtenteil mit versendet. Alternativ können infizierte Nachrichten in Quarantäne geschoben und mit weiteren Methoden behandelt werden. Im einfachsten Fall können Nachrichten verworfen werden.

- *Benachrichtigung an*: Falls infizierte Nachrichten entdeckt werden kann hier gesteuert werden, an wen eine Benachrichtigung erfolgen soll.

13.10.1.4 Tab *Grundeinstellungen*, Abschnitt *Quarantäne*

Felder in diesem Abschnitt

- *Quarantäneverfahren*: Es gibt verschiedene Quarantäneverfahren. E-Mails können in den administrativen IMAP-Ordner admin.virus zur Durchsicht abgelegt werden oder in der Mail-Queue des Mailservers vorgehalten werden. Alternativ können infizierte Nachrichten an ein bestimmtes Postfach weitergeleitet werden. Wenn die Zarafa Groupware installiert ist, können E-Mails auch in den administrativen Ordner der Groupware abgelegt werden.
- *E-Mail-Adresse*: Hier kann eine separate E-Mail-Adresse zu Quarantänezwecken angegeben werden.
- *Automatisch löschen nach (Tage)*: Im administrativen Ordner abgelegte E-Mails können nach Ablauf von den angegebenen Tagen automatisch gelöscht werden.

13.10.1.5 Tab *Berechtigungen*, Abschnitt *Administrativer IMAP-Ordner für infizierte E-Mails*

Felder in diesem Abschnitt

- *Administrative Rechte*: Hier wird festgelegt, welche Gruppenmitglieder Lese- und Schreibrechte auf den administrativen IMAP-Ordner erhalten.

13.10.1.6 Aktionen für dieses Formular

- *Speichern*: Beendet den Dialog, die Änderungen werden gespeichert.
- *Abbrechen*: Beendet den Dialog, die Änderungen werden verworfen.

13.10.2 *Spamfilter*

(Diese Option befindet sich im Zusatzmodul *Collax Mail Security*)
(Dieser Dialog befindet sich unter *Mail – Mail Security – Spam*)
In diesem Dialog wird der inhaltsbasierte Spamfilter für das Mailsystem konfiguriert.

13.10.2.1 Tab *Spam-Inhalts-Filter*, Abschnitt *Grundeinstellungen*

Felder in diesem Abschnitt

- *Aktivieren*: Diese Option schaltet den Spamfilter ein.
- *Automatische Aktualisierung*: Diese Option aktualisiert regelmäßig die Spam-Regeln für den Spam-Inhalts-Filter.

- *Vertrauenswürdige Mail-Relays*: Hier sollten die IP-Adressen der Mailserver angegeben werden, die für die eigene Domain E-Mails annehmen.

  Für bestimmte Tests („Received"-Zeilen im Mailheader) wird eine Liste aller Netze und Rechner benötigt, die als „vertrauenswürdig" betrachtet werden sollen. „Vertrauenswürdig" bedeutet dabei, dass diese Rechner nicht der Ausgangspunkt von Spam sind – es kann jedoch durchaus sein, dass diese Rechner Spam weiterleiten.

  Die Liste enthält automatisch alle Rechner und Netze, die über die Gruppenrichtlinien E-Mails über dieses System weiterleiten dürfen (Berechtigung: *Mail-Relay ohne Authentifizierung*).

  Zusätzlich müssen hier die Mailserver angegeben werden, die als MX („Mail-Exchanger") für die Domain zuständig sind. Diese sind per DNS ermittelbar, meist sind es ein oder mehrere Mailserver beim eigenen Provider.

13.10.2.2 Tab *Spam-Inhalts-Filter*, Abschnitt *E-Mail ist wahrscheinlich Spam*

Felder in diesem Abschnitt

- *ab Schwellenwert*: Jede E-Mail wird nach verschiedenen Kriterien bewertet. Für jedes zutreffende Kriterium erhält die E-Mail eine Anzahl Punkte, die aufsummiert werden.

  Mit diesem Parameter wird festgelegt, ab welcher Punktzahl eine E-Mail als Spam behandelt wird. Ein Wert von „5" ist die normale Einstellung. Bei diesem Wert ist die Negativerkennung schon extrem gering, die Effizienz beim Erkennen von Spam allerdings auch nicht optimal. Höhere Werte lassen mehr Kriterien zutreffen, bevor eine E-Mail als Spam markiert wird. In

Umgebungen, in denen hauptsächlich *Microsoft Outlook* verwendet wird, ist ein Grenzwert von „6“ oder „7“ eher sinnvoll. In anderen Fällen kann allerdings auch ein Grenzwert von nur „3“ ausreichend sein. Zunächst sollte mit einem hohen Grenzwert gestartet werden, der nach und nach heruntergesetzt wird. Durch die *Auto Whitelist-Funktion* verringert sich die Negativerkennung mit der Zeit zudem.

- *Markierung im Betreff der E-Mail*: Der Spamfilter legt in den Kopfzeilen einer E-Mail („Header“) einen Report über die erreichte Punktezahl und die zutreffenden Regeln ab. Durch das Ablegen im Header der Mail sieht die Mail auf den ersten Blick für den Benutzer unverändert aus. Mit Hilfe dieses Reports kann nachvollzogen werden, wie das System funktioniert und wie Grenzwerte angepasst werden sollten (indem bei jeder fälschlich als Spam markierten E-Mail untersucht wird, welche Punktezahl sie erhalten hat).

  Wird diese Option aktiviert, wird zusätzlich eine Markierung im Betreff der E-Mail eingefügt.

13.10.2.3 Tab *Spam-Inhalts-Filter*, Abschnitt *E-Mail ist sicher Spam* Felder in diesem Abschnitt

- *ab Schwellenwert*: Hier wird eingestellt, was mit E-Mails geschehen soll, die als Spam erkannt wurden. Spam kann gelöscht, in einem eigenen Ordner gespeichert oder angehalten werden („Quarantäne“). In diesem Feld wird ein ganzzahliger Wert als Grenzwert eingetragen. Bleibt dieses Feld leer, werden Spam-E-Mails nicht gesondert behandelt, sondern ganz normal in das entsprechende Postfach zugestellt.
- *Aktion*: Mit der Option *mit Warnung an Empfänger senden* wird

die E-Mail als einfacher Text zugestellt. Diese Einstellung ist notwendig, wenn verhindert werden soll, dass Benutzer oder die Mail-Applikationen die Anhänge öffnen und eventuelle Inhalte ausführen.

Durch die Aktion *in Quarantäne verschieben* kann die E-Mail mit weiteren Aktionen weiterverarbeitet werden.

Bei der Aktion *Verwerfen* wird die E-Mail sofort gelöscht, dem absendenden Mailserver wird jedoch bestätigt, dass die E-Mail zugestellt wurde. Für den Absender sieht es so aus, als ob die E-Mail zugestellt wurde.

Diese Aktion birgt die Gefahr, dass fälschlich auch erwünschte E-Mails einen hohen Punktewert bekommen und gelöscht werden („false positive“). Sie sollte daher erst aktiviert werden, wenn die festgelegten Punktgrenzen in der Praxis einige Zeit erfolgreich getestet wurden.

- *Quarantäneverfahren*: Die Aktion *in der Mail-Queue behalten* hält die E-Mail in der Warteschlange an. Sie muss vom Administrator explizit gelöscht oder freigegeben werden. Dazu kann er sie in der Mailqueue näher untersuchen.

  Die Aktion *Weiterleitung an Postfach* funktioniert so, dass die E-Mail an ein externes Postfach zur weiteren administrativen Bearbeitung zugestellt wird.

  Die Aktion *Kopano Ordner* funktioniert ähnlich. Hier wird die E-Mail an den Public Folder admin.spam in der Kopano Groupware zur weiteren administrativen Bearbeitung zugestellt.
- *E-Mail-Adresse*: Hier wird der Ort der Quarantäne angegeben. Dies geschieht in Form einer E-Mail-Adresse. Diese Adresse kann einem Benutzerpostfach, einem IMAP-Ordner, oder einem IMAP-Administrationsordner auf einem E-Mail-Server zugewiesen werden kann.

  Ein administrativer IMAP-Ordner für die Quarantäne kann als

öffentlicher Ordner definiert werden, die Lese- und Schreibberechtigungen sollten jedoch stark eingeschränkt sein. Zusätzlich sollte dieser Ordner direkt per E-Mail erreichbar sein.

Die Adresse für die direkte Zuordnung in einen IMAP-Ordner eines Benutzers kann die Form *Userid+Ordner@domain.tld* haben. Die Voraussetzung für das Sub-Addressing mit address extensions ist, dass der Mail-Server RFC 3598 unterstützt. Auf diesem Mailserver muss zudem das p-Flag für den Ordner gesetzt sein.

- *Automatisch löschen nach (Tage)*: Im administrativen Ordner abgelegte Dateien können nach Ablauf von den angegebenen Tagen automatisch gelöscht werden.
- *Administrative Rechte für IMAP-Ordner admin.spam*: Hier werden die Gruppen angegeben, die ausgefilterte Spam-E-Mails begutachten und verwalten sollen.

13.10.2.4 Tab *Kaspersky™ Anti-Spam*, Abschnitt *Collax Spam Protection powered by Kaspersky™*

Felder in diesem Abschnitt

- *Aktivieren*: Die Collax Spam Protection powered by Kaspersky™ verwendet einen hybriden Ansatz (in der Cloud und on-premise), um Spam und Phishing zu erkennen. Einige der Methoden sind Cloud-basiert und erfordern eine Verbindung zu Kaspersky-Lab-Diensten. Andere Methoden arbeiten vor Ort. Diese Methoden verwenden Datenbanken und benötigen keine Verbindung zu Kaspersky-Lab-Diensten. Beachten Sie, dass die verwendeten Datenbanken regelmäßig aktualisiert werden. Hier wird der zusätzliche Anti-Spam-Filter mit zusätzlichen Filtermethoden aktiviert.
- *Gewichtung für Zwischenergebnis*: Mit dieser Option wird die

Gewichtung des originalen Kaspersky™-Ratings eingestellt. Damit kann das Kaspersky™-Rating an das Bewertungssystem und die deklarierten Schwellenwerten des Collax Spamfiltersystems angepasst werden.

Von Kaspersky™ geprüfte Nachrichten erhalten einen der folgenden Zustände: *Spam, Clean oder Blacklisted*. Als zusätzliches Ergebnis wird ein originales Rating zwischen 0 und 100 Punkten für eine Nachricht vergeben. Nachrichten, die durch die Kaspersky™ Anti-Spam-Engine als *Spam* oder als *Blacklisted* erkannt wurden, erhalten in der Regel 100 originale Punkte. Ist der Zustand *Clean* wird ein Wert zwischen 0 und 99 vergeben.

Als Standardwert der Gewichtung kann 10% eingestellt werden. Somit erhält eine durch die Kaspersky™ Anti-Spam-Engine geprüfte Spam-Nachricht original 100 Punkte, welche darauffolgend nach der Gewichtung mit 10 Punkten in das Collax Spamfiltersystem zusätzlich einfließen. Falls dieser Wert zu mehr False-Positives führt, sollte der Wert einen Prozentpunkt nach unten korrigiert werden.

13.10.2.5 Tab *Kaspersky™ Anti-Spam*,Abschnitt *Methoden zur Spam- und Phishing-Erkennung*

Felder in diesem Abschnitt

- *Linguistische Analyse (Heuristik)*: Diese Methode analysiert die Bedeutung und Kategorisierung von Text. Es durchsucht Nachrichten nach Wörtern, Ausdrücken und Begriffen, die auf Spam-Nachrichten hindeuten. Im Gegensatz zu einer einfachen Stichwortsuche sucht die linguistische Analyse nicht nur nach einzelnen Stichwörtern, sondern behandelt den gesamten Text als eine Einheit. Standardmäßig ist diese Option aktiviert.

- *DNS Analyse (Heuristik)*: Diese Methode verwendet auf DNS basierende Techniken zur Entdeckung von Spam. Standardmäßig ist diese Option aktiviert.
- *DMARC-Spezifikation*: Die Technik DMARC ist die weitergehende Prüfung auf Spam, basierend auf SPF und DKIM. Standardmäßig ist diese Option aktiviert.
- *Anti-Phishing Technologie*: Die Anti-Phishing-Komponente verhindert betrügerische Versuche eines Angreifers, sensible Informationen über die privaten Daten der Nachrichtenempfänger zu sammeln. Die Collax Spam Protection prüft Nachrichten auf häufige Attribute von Phishing-E-Mails, zu denen unter anderem aufmerksame und dringende Wort- und Phishing-Links gehören, und markiert solche Nachrichten wie Spam. Standardmäßig ist diese Option aktiviert.
- *Cloud-basierte Erkennung*: Hier werden Cloud-basierende Methoden, wie UDS, SURBL und URL Reputation zur Spam-Erkennung benutzt. Standardmäßig ist diese Option aktiviert.

  Der Cloud-Dienst wird extern auf Port 443 kontaktiert. Bei Verwendung dieser Methode ist deshalb zu beachten, dass die Verbindung zum Cloud-Dienst über einen WebProxy mit Entschlüsselung durch SSL-Interception *nicht* aufgebaut werden kann. Entweder ist für den Verkehr über HTTPS die SNI-Technik auf dem Webproxy einzuschalten, oder der Netzwerktraffic von Servers ins Internet auf Port 443 wird generell ungefiltert erlaubt.
- *Grafik-Analyse*: Diese Methode analysiert grafische Inhalte in Nachrichten mithilfe der proprietären Bildverarbeitungstechnologie von Kaspersky. Dank fortschrittlicher Bildverarbeitungsalgorithmen überlastet diese Technologie nicht die Rechenressourcen im Gegensatz zu häufig verwendeten OCR-Technologien (Optical Character Recognition).
- *Obszöne Sprache filtern*: Diese Option analysiert Nachrichten, ob

obszöne Sprache verwendet wird. Solche Nachrichten sind mit einem speziellen Service-Header gekennzeichnet. Standardmäßig ist diese Option aktiviert.

- *Östliche Sprachkodierungen akzeptieren*: Östliche Sprach-Kodierung wird beachtet, analysiert und akzeptiert. Diese Option ist sinnvoll, wenn geschäftliche Kontakte hierzu bestehen. Ist die Option deaktiviert erhöhen Nachrichten in diesen Sprachen die Spam-Bewertung. Standardmäßig ist diese Option deaktiviert.
- *Kyrillischen Sprachkodierungen akzeptieren*: Kyrillische Sprach-Kodierung wird beachtet, analysiert und akzeptiert. Diese Option ist sinnvoll, wenn geschäftliche Kontakte hierzu bestehen. Ist die Option deaktiviert erhöhen Nachrichten in diesen Sprachen die Spam-Bewertung. Standardmäßig ist diese Option deaktiviert.
- *Enforced Anti-Spam Updates Service (EASUS)*: Diese Methode stellt eine dauerhafte Verbindung mit den Kaspersky Lab Servern her. Updates für einige der Datenbank-Komponenten können so im Intervall von wenigen Sekunden ausgeliefert werden. Informationen über neue Spam-Bedrohungen werden durch diese Technik ausgeliefert, bevor eine regelmäßige Datenbank-Aktualisierung stattfindet. Dies geschieht in der Regel mehrere Minuten nachdem Kaspersky Lab Spam-Analysten eine neue Spam-Bedrohung entdeckten. Beachten Sie, dass EASUS nicht den vorhandenen Mechanismus zur Aktualisierung der Datenbank ersetzt, sondern ihn ergänzt.

  Der Cloud-Dienst wird extern auf Port 443 kontaktiert. Bei Verwendung dieser Methode ist deshalb zu beachten, dass die Verbindung zum Cloud-Dienst über einen WebProxy mit Entschlüsselung durch SSL-Interception *nicht* aufgebaut werden kann. Entweder ist für den Verkehr über HTTPS die SNI-Technik auf dem Webproxy einzuschalten, oder der Netzwerktraffic von Servers ins Internet auf Port 443 wird generell ungefiltert erlaubt.

- *Benutzerdefinierte Phrasen-Listen verwenden*: Hier besteht die Möglichkeit benutzerdefinierte Blacklists und Whitelists für Phrasen zu verwenden. Einträge werden mittels Zeilenumbruch getrennt.

13.10.2.6 Tab *Kaspersky™ Anti-Spam*,Abschnitt *Phrasenlisten* Felder in diesem Abschnitt

- *Whitelist*: Hier werden Phrasen eingetragen, die nicht als Spam erkannt werden sollen.
- *Blacklist*: Hier werden Phrasen eingetragen, die als Spam erkannt werden sollen. Beispielsweise *I sent this mail praying*

13.10.2.7 Tab *Heuristik (Bayes)*, Abschnitt *Heuristischer Filter (Bayes)*

Obwohl die Bewertungen des Spamfilters recht zuverlässig sind, kann es dennoch vorkommen, dass E-Mails falsch klassifiziert werden. Ein anderer Ansatz zur Spamerkennung verwendet keinen festen Regelsatz mit einem Punktesystem, sondern versucht, über eine Wissensdatenbank eine Entscheidung zu treffen. Zum Aufbau dieser Datenbank muss der Benutzer jeweils eine bestimmte Menge an unerwünschten („Spam“) und erwünschten („Ham“) E-Mails bereitstellen. Der Vorteil dieses Verfahrens liegt darin, dass sich ein solches System den individuellen Anforderungen des Benutzers anpasst. Der Nachteil ist, dass für die Bereitstellung der Spam/Ham-Ordner eine gewisse Disziplin erforderlich ist.

Felder in diesem Abschnitt

- *Heuristischen Filter anwenden (Bayes-Filter)*: Mit dieser Option wird über den wahrscheinlichkeitsbasierten Filter eine Erkennung vorgenommen.
- *Automatisches Lernen*: Abhängig von der Bayes-Datenbank werden die E-Mails automatisch nach „Ham“ oder „Spam“ klassifiziert und in der Datenbank des Spam-Filters hinterlegt.
- *Lern-Intervall*: Hier wird das Zeitintervall für das automatische Trainieren ausgewählt. Diese Einstellung gilt für das Trainieren aus lokalen und entfernten Spam-/Ham-Ordnern.
- *Lernen aus lokalen Spam-/Ham-Ordnern*: Durch das Aktivieren dieser Option werden die gemeinsam nutzbaren Ordner zur Ablage von Spam- und Ham-E-Mails angelegt. In diese Ordner sollen durch Benutzer qualifizierte E-Mails abgelegt werden. Der Spamfilter lernt aus diesen Ordnern dann automatisch.
- *Lernen aus nicht-lokalen Spam-/Ham-Ordnern*: Mit dieser Option kann der Spamfilter mit Hilfe eines externen IMAP-Postfachs trainiert werden. Das Postfach sollte hierzu auf einem Mailserver definiert sein und zwei Ordner enhalten, die jeweils mit Ham- und mit Spam-E-Mails bestückt werden können. Der Lernvorgang geschieht durch Auslesen der E-Mails im Postfach, getrennt für Ham und Spam.

Abschnitt *Einstellungen für nicht-lokalen Spam-/Ham-Ordner*
Felder in diesem Abschnitt

- *IMAP-Server*: Hier wird der Remote-Server definiert, auf dem das IMAP-Postfach mit den Spam- und Ham-Ordnern liegt.
- *Benutzername*: Mit dieser Benutzerkennung meldet sich der Collax Security Gateway an dem definierten externen Server mit IMAP-Postfach an.

- *Passwort*: Hier wird das Passwort zur Anmeldung eingegeben.
- *Spam-IMAP-Ordner*: Hier wird der Ordner definiert, den der Collax Security Gateway zum Lernen von Spam-E-Mails verwenden soll. Die Ordner müssen in IMAP-Schreibweise, mit Punkten getrennt, angegeben werden.

  Beispiel: Inbox.misc.spam, Inbox.spam, Public.spam
- *Ham-IMAP-Ordner*: Hier wird der Ordner definiert, den der Collax Security Gateway zum Lernen von Ham-E-Mails verwenden soll. Die Ordner müssen in IMAP-Schreibweise, mit Punkten getrennt, angegeben werden.

  Beispiel: Inbox.misc.ham, Inbox.ham, Public.ham
- *E-Mails nach Lernen auf Server löschen*: Mit Aktivieren dieser Option werden die Spam-/Ham-E-Mails, die bereits gelernt wurden, aus den entsprechenden Ordnern auf dem Remote-Server gelöscht.

13.10.2.8 Tab *Heuristik (Bayes)*, Abschnitt *Filter aus Kopano trainieren* Felder in diesem Abschnitt

- : Diese Funktion kann genutzt werden, wenn das Zarafa IMAP-Gateway aktiviert ist.
- *Aktivieren*: Mit dieser Option kann der Spam-Filter durch die Public Folder LearnAsHam und LearnAsSpam der Zarafa Groupware trainiert werden. Berechtiungen für die Ordner werden entweder über die Administrations-GUI oder durch einen Zarafa Groupware-Administrator gesetzt.
- *Intervall*: Der Filter kann entweder stündlich oder täglich aus den Ordnern lernen.
- *E-Mails nach Lernen auf Server löschen*: Mit dieser Option können die E-Mails der Public Folder nach dem Lernen entfernt werden.

13.10.2.9 Tab *Reputationsdienste*, Abschnitt *Online-Blacklists für SMTP-Reject*

Felder in diesem Abschnitt

- *Blacklists verwenden*: Wird diese Option aktiviert, prüft das System bei jeder einkommenden E-Mail, ob die einliefernde IP-Nummer in einer dieser schwarzen Listen erfasst ist.
- *Vordefinierte Blacklists verwenden*: In dieser Liste werden die Blacklist-Server eingetragen, die abgefragt werden sollen. Die Grundkonfiguration enthält eine Liste von frei zugänglichen DNS-Blacklists. Eine Anmeldung o. ä. ist nicht notwendig, um diese Listen nutzen zu dürfen.
- *Manuell Blacklists eintragen*: Hier können weitere Blacklists manuell eingetragen werden. Bestimmte Anbieter bieten kommerzielle Blacklists oder dynamische online Blacklists, die eine Anmeldung erfordern.

13.10.2.10 Tab *Reputationsdienste*, Abschnitt *Online-Blacklists für Inhaltsbewertung*

Felder in diesem Abschnitt

- *Verwenden*: Diese Option aktiviert die Abfrage von Spam-Block-Listen, die im DNS-System abgelegt sind. Diese Tests können die Erkennungsrate von Spam deutlich erhöhen – auf Kosten zusätzlicher Netzwerkanfragen.

  Wird diese Option aktiviert, werden die „Received“-Zeilen im Mailheader ausgewertet. Für jede Station auf diesem Weg wird ermittelt, ob diese als mögliche Quelle für Spam-E-Mails bekannt ist.

  Diese Option ähnelt derjenigen im Abschnitt *Online-Blacklists*

für SMTP-Reject. Während dort allerdings die Annahme einer E-Mail verweigert wird, wird hier nur eine zusätzliche Bewertungsmöglichkeit zur Bestimmung der Spam-Punktezahl aktiviert. Dadurch wird eine E-Mail nicht zwangsläufig abgelehnt, wenn der einliefernde Mailserver auf einer Blacklist erfasst ist.

Wenn der SMTP-Server oder der Provider bereits DNS-Blocklists auswerten, kann diese Option ohne den Verlust der Bewertungsmöglichkeit deaktiviert werden.

Die voreingestellten Blocklisten umfassen verschiedene unentgeltlich verwendbare Dienste. Diese Liste und die zugehörige Bewertung kann nicht geändert werden.

- *SenderBase verwenden*: SenderBase® ist ein weltweites Überwachungsnetzwerk für E-Mail, durch das Spam-E-Mails zuverlässig identifiziert werden können.
- *Gewichtung für SenderBase-Eintrag*: Hier kann zusätzlich eine Gewichtung zwischen 10% und 200% für den Wert eingegeben werden, welchen die E-Mail durch SenderBase® erhalten hat.
- *NiX-Spamfilter verwenden*: NiX Spam ist ein Spamfilter-Projekt der Zeitschrift iX. Es bildet Prüfsummen über den E-Mail-Body inklusive Anhänge und vergleicht diese Prüfsummen in einer laufend aktualisierten, per DNS abfragbaren Blacklist (DNSBL).

  Mit dieser Option werden eingehende E-Mails per DNS auf die Platzierung innerhalb des NiX-Spamfilter geprüft.
- *NiX Spam-Wert*: Ist eine Absender-IP-Adresse einer E-Mail in der NiX Spamfilter-Datenbank gelistet, wird der hier eingetragene Wert zur Spambewertung addiert.
- *Razor verwenden*: Durch Aktivieren dieser Option wird jede E-Mail anhand der Signaturen des Razor-Onlinechecks untersucht. Eine durch Razor als Spam klassifizierte E-Mail bekommt in der SpamAssassin-Auswertung mehr Punkte.

13.10.2.11 Tab *Reputationsdienste*, Abschnitt *DomainKeys Identified Mail (DKIM)*

DomainKeys Identified Mail (DKIM) ist ein von Yahoo entwickeltes Verfahren, E-Mails mit einer Signatur zu versehen, die es dem Empfänger ermöglicht, eindeutig festzustellen, ob eine E-Mail wirklich vom angeblichen Absender kommt. Bei der Verwendung von DKIM signiert der Absender seine E-Mails und stellt den öffentlichen Schlüssel über den TXT-Record der gleichen Domain bereit. Der Empfänger kann anschließend beim Empfang der E-Mails über die Signatur und den Schlüssel im DNS die Echtheit der E-Mail verifizieren.

Felder in diesem Abschnitt

- *DKIM E-Mail-Überprüfung verwenden*: Eingehende E-Mails können auf eine DKIM-Signature getestet werden.
- *Bonuspunkte für Absender in der DKIM-Whitelist*: Falls der Absender in der Whitelist vorhanden ist, werden die angegebenen Punkte von der Spam-Bewertung abgezogen.
- *Bonuspunkte für E-Mails mit einer gültigen DKIM-Signatur*: Falls die eingehende E-Mail eine gültige DKIM-Signatur enthält, werden die hier angegebenen Punkte von der Spam-Bewertung abgezogen.

13.10.2.12 Tab *Reputationsdienste*, Abschnitt *Sender Policy Framework (SPF)*

Felder in diesem Abschnitt

- *SPF verwenden*: Durch Aktivieren dieser Option wird bei jeder E-Mail eine Sender Policy Framework-Überprüfung durchgeführt, die das Fälschen des Absenders einer E-Mail auf SMTP-Ebene erschwert.

13.10.2.13 Tab *Spam-SMTP-Filter*, Abschnitt *Greylisting*

Felder in diesem Abschnitt

- *Greylisting verwenden*: Durch Aktivieren dieser Option wird Greylisting aktiviert. Dabei wird jede per SMTP neu eingelieferte E-Mail von Systemen, die nicht die Berechtigung *Mail Relay* haben, zunächst mit einer temporären Fehlermeldung abgewiesen. Nach Ablauf einer bestimmten Sperrfrist wird die E-Mail angenommen. Damit wird verhindert, dass E-Mail von Programmen angenommen wird, die über keine Mailqueue verfügen (und damit keine richtigen Mailserver sind).
- *Verzögerungsdauer (in Sekunden)*: Mit diesem Wert wird festgelegt, wie lange die Sperrfrist dauern soll. Voreinstellung sind 300 Sekunden, also 5 Minuten. Verbindet sich ein Mailserver nach der ersten Ablehnung innerhalb der Sperrfrist erneut, wird er wieder mit einer temporären Fehlermeldung abgewiesen.
- *Maximales Alter der Einträge (in Tagen)*: Intern werden alle Greylisting-Tupel in einer Datenbank gespeichert. Nach Ablauf der in diesem Feld gesetzten Haltezeit werden die Einträge gelöscht, sofern sie nicht zwischenzeitlich neu genutzt wurden.
- *Zeitfenster für erneuten Versuch (in Stunden)*: Innerhalb dieses Zeitfensters muss der einliefernde Mailserver sich erneut verbinden. Geschieht das nicht, wird das Tupel gelöscht, und die Greylisting-Sperre beginnt erneut.
- *Anzahl der E-Mails für automatische Whitelist*: Liefert ein Mailserver eine größere Anzahl E-Mails ein, kann dessen IP-Adresse zukünftig als vertrauenswürdig klassifiziert werden. In diesem Feld wird eingestellt, wie viele E-Mails erforderlich sind, damit Greylisting für dieses System deaktiviert wird.
- *Nachricht*: Der in diesem Feld gesetzte Text wird als temporäre Fehlermeldung an den einliefernden Mailserver ausgegeben. Im

Text sollte ein Hinweis auf die Nutzung der Greylisting-Technik stehen, damit der Administrator der Gegenseite dies im Logfile nachvollziehen kann.

In diesem Feld können die Variablen „%s“ zur Angabe der verbleibenden Wartezeit und „%r“ zur Anzeige der Empfängeradresse verwendet werden.

13.10.2.14 Tab *Spam-SMTP-Filter*, Abschnitt *Teergrube*

Felder in diesem Abschnitt

- *Teergrube emulieren*: (Diese Option befindet sich im Zusatzmodul *Collax Mail Security*)

  Mit dieser Option wird die Funktion Teergrube zur zusätzlichen Abwehr von Spam-E-Mails und der Verbreitung von Würmern eingeschaltet. Durch die Aktivierung wird die Kommunikation innerhalb von zwei Verbindungsstufen, zwischen dem Collax Server und dem verbindenden SMTP-Server, verzögert.

  Es ist zu beachten, dass durch diese Option der eingehende E-Mail-Server für den Zeitraum der Verzögerung von Stufe 1 und Stufe 2 blockiert wird.
- *Verzögerung Stufe 1*: Die Verzögerung der Stufe 1 bewirkt, dass der Begrüßungsbanner vom Collax Server 220 csg.example.com ESMTP (Postfix) bei einem Verbindungsversuch erst nach den angegebenen Sekunden dem eingehenden Server übermittelt wird.
- *Verzögerung Stufe 2*: Die Verzögerung der Stufe 2 bewirkt, dass die Antwort auf die Helo-Verbindung vom Collax Server erst nach den angegebenen Sekunden dem eingehenden Server übermittelt wird.

13.10.3 *Spam White-/Blacklist*

(Dieser Dialog befindet sich unter *Mail – Mail Security – Spam White-/Blacklist*)

In diesem Dialog wird eine Liste von Absenderadressen verwaltet, für die keine Spamfilterung durchgeführt wird. Technisch wird zwar eine Filterung durchgeführt, der Absender erhält jedoch einen so hohen Bonus für die Spam-Bewertung, dass seine E-Mails nie als Spam klassifiziert werden.

Analog zur Whitelist wird hier eine Liste von Absenderadressen verwaltet, deren E-Mails durch eine hohe Spam-Punktezahl immer als Spam klassifiziert werden.

Ebenso wird in diesem Dialog eine Liste von Absenderadressen für DKIM verwaltet, für die keine Spamfilterung durchgeführt wird. Technisch wird zwar eine Filterung durchgeführt, der Absender erhält jedoch einen so hohen Bonus für die Spam-Bewertung, dass seine E-Mails nie als Spam klassifiziert werden.

13.10.3.1 Tab *Spamfilter-Whitelist*, Abschnitt *Spamfilter-Whitelist*

Felder in diesem Abschnitt

- *Adressen*: In diesem Eingabefeld werden die Absenderadressen eingetragen. Die einzelnen Adressen werden mit Leerzeichen, Zeilenumbruch oder Komma getrennt.

  Die beiden Teile der Adresse (Empfänger und Domain) werden als Muster verwendet. Es ist möglich, *Wildcards* zu verwenden: Ein Fragezeichen steht für ein einzelnes und ein Stern (*) für beliebig viele beliebige Zeichen (hier werden keine regulären Ausdrücke eingesetzt).

13.10.3.2 Tab *Spamfilter-Blacklist*, Abschnitt *Spamfilter-Blacklist* Felder in diesem Abschnitt

- *Adressen*: In diesem Eingabefeld werden die Absenderadressen eingetragen. Die einzelnen Adressen werden mit Leerzeichen, Zeilenumbruch oder Komma getrennt.

  Die beiden Teile der Adresse (Emfänger und Domain) werden als Muster verwendet. Es ist möglich, *Wildcards* zu verwenden: Ein Fragezeichen steht für ein einzelnes und ein Stern (*) für beliebig viele beliebige Zeichen (hier werden keine regulären Ausdrücke eingesetzt).

13.10.3.3 Tab *DKIM-Whitelist*, Abschnitt *DKIM-Whitelist* Felder in diesem Abschnitt

- *Adressen*: In diesem Eingabefeld werden die Absenderadressen eingetragen. Die einzelnen Adressen werden mit Leerzeichen, Zeilenumbruch oder Komma getrennt.

  Die beiden Teile der Adresse (Absender und Domain) werden als Muster verwendet. Es ist möglich, Wildcards zu verwenden: Ein Fragezeichen steht für ein einzelnes und ein Stern (*) für beliebig viele beliebige Zeichen (hier werden keine regulären Ausdrücke eingesetzt).

13.10.3.4 Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten der White-/Blacklist beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten der White-/Blacklist beenden. Die Änderungen werden gespeichert.

13.10.4 GUI-Referenz: *Kopfzeilen/MIME-Filter*

(Dieser Dialog befindet sich unter *Mail – Mail Security – Kopfzeilen/MIME-Filter*)

In diesen Dialogen können eigene Regeln zum Filtern von E-Mail-Anhängen erstellt werden. Dabei kann sowohl auf die Dateiendung als auch auf den MIME-Content-Type gefiltert werden.

Ebenso werden in diesen Dialogen Filter für Zeilen im Header der E-Mail („Kopfzeilen“) verwaltet. Mit diesen Filtern können Muster im Betreff, im Absenderfeld u. ä. erkannt werden.

Die hier angegebenen Filter sind für alle E-Mails wirksam, die das Mailsystem durchlaufen.

13.10.4.1 *Tabelle*
Tab *Kopfzeilen*

Mit diesem Filter lassen sich Regeln für bestimmte Kopfzeilen definieren. Neben dem Blocken oder Zurückweisen von E-Mails mit bestimmten Betreffs oder von bestimmten Absendern lassen sich beispielsweise auch die Anforderungen für eine Lesebestätigung unterdrücken.

Spalten in der Tabelle

- *Bezeichnung*: Hier wird der Name der Regel angezeigt.
- *Kommentar*: Hier steht der Kommentartext zu dieser Regel.
- *Aktion*: Hier wird die Aktion angezeigt, die bei passendem Muster auf die E-Mail angewendet wird.

Tab *MIME*

E-Mails enthalten oft unerwünschte oder gefährliche Inhalte, die nicht an die Benutzer ausgeliefert werden sollten. In diesem Dialog werden Regeln für das Filtern von Anhängen bearbeitet.

Spalten in der Tabelle

- *Bezeichnung*: Hier wird eine Bezeichnung für die Regel angegeben.
- *Kommentar*: Hier steht ein kurzer Kommentartext zu dieser Regel.
- *Aktion*: Hier wird die Aktion angezeigt, die bei passendem Muster auf die E-Mail angewendet wird.

13.10.4.2 *Kopfzeilenfilter bearbeiten*

Felder in diesem Formular

- *Bezeichnung*: Hier wird eine Bezeichnung für die Regel angegeben. Wird eine bereits angelegte Regel bearbeitet, kann der Name nicht mehr geändert werden. Er wird dann nur in diesem Feld angezeigt.
- *Kommentar*: Hier kann ein kurzer Kommentartext zu dieser Regel angegeben werden.
- *Name der Kopfzeile*: In diesem Feld wird der Name der Kopfzeile angegeben, in der gefiltert werden soll. Der Doppelpunkt am Ende des Namens der Kopfzeile wird automatisch eingefügt, wenn er nicht eingegeben wird. Kopfzeilennamen werden unabhängig von Groß- und Kleinschreibung verarbeitet.
- *Inhalt der Kopfzeile*: Hier kann das Suchmuster angegeben werden, welches auch als Wert in der Kopfzeile auftauchen muss.

Bleibt das Feld leer, wird nur die Existenz der Kopfzeile geprüft.

In diesem Feld werden reguläre Ausdrücke ausgewertet. Beispiel: Kopfzeile „From“ und als Inhalt „user.*“. sorgen dafür, dass sämtliche E-Mails von einer Absenderadresse mit der Zeichenkette „user“ am Anfang, gefolgt von beliebigen (oder gar keinen) Zeichen, gefiltert werden („.*“ steht für beliebige Zeichen (.) beliebig oft (*)).

In der erzeugten E-Mail bzw. in dem eingefügten Text kann auf gefilterte Bestandteile zurückgegriffen werden: Dazu wird ein Verweis auf den passenden Teilausdruck in der Form „${n}“ eingefügt. Dabei steht „n“ für den n-ten Teilausdruck.

Beispiel: Kopfzeile „From“, als Inhalt „(.*)“ und als Text „Hallo ${1}, die E-Mail wurde gefiltert.“

- *Aktion*: Aus dieser Liste wird ausgewählt, was mit einer E-Mail geschehen soll, auf die die Filterregel passt.

  Wird *Warnen* ausgewählt, wird nur eine Warnung in die Logdatei geschrieben. Dies ist nützlich, wenn die Regeln zunächst einmal getestet werden.

  Die Aktion *Anhalten* behält die E-Mail in der Warteschlange, ohne sie zuzustellen („Quarantäne“). Der Administrator muss die E-Mail dann näher untersuchen und abschließend löschen oder zur Zustellung freigeben.

  Mit der Einstellung *Zurückweisen* wird die E-Mail abgelehnt, und der Sender erhält den zusätzlich angegebenen Text als Fehlermeldung. Diese Option kann zu Problemen führen, wenn E-Mails per POP3 oder Multidrop abgeholt werden.

  Wird hier *Verwerfen* ausgewählt, wird die E-Mail gelöscht; dem absendenden MTA wird jedoch bestätigt, dass die E-Mail akzeptiert wurde. Für den Absender sieht es so aus, als sei die E-Mail zugestellt worden.

  Die Auswahl von *Entfernen* löscht die gesamte Kopfzeile aus der E-Mail. Die E-Mail wird anschließend zugestellt.

Es können auch neue Kopfzeilen *eingefügt* werden. Wird diese Option ausgewählt, kann in einem weiteren Feld der gewünschte Text zum Einfügen angegeben werden.

Mit *Ersetzen* wird die gefundene Kopfzeile entfernt und durch eine neue ersetzt.

Wenn *Umleiten* gewählt wird, kann die gefilterte E-Mail an eine individuelle E-Mail-Adresse umgeleitet werden.

- *Einfügung/Ersetzung*: Wird als Aktion *Einfügen* gewählt, kann hier die einzufügende Kopfzeile angegeben werden.

  Wird *Ersetzen* als Aktion gewählt, wird die aktuelle Zeile aus dem Mailheader entfernt und statt dessen der Text in diesem Feld eingefügt.

  Um eine Kopfzeile einzufügen, muss sie vollständig eingegeben werden, z. B. „X-Inserted: Yes!“. Der Text darf nur aus 7-Bit-ASCII-Zeichen bestehen. Enthält die einzufügende Kopfzeile Umlaute u. ä., werden diese automatisch als „Quoted Printable“ kodiert. Wichtig ist der Doppelpunkt zur Trennung von Schlüsselwort und Inhalt.
- *Nachricht an Absender*: Der hier angegebene Text wird in die Logdatei geschrieben und bei der Aktion *Zurückweisen* an den Absender übermittelt, wenn eines der Muster für diese Regel zutrifft.
- *E-Mail Adresse für Umleitung*: An die hier angegebene Adresse wird die ausgefilterte E-Mail umgeleitet.

13.10.4.3 *MIME-Filter bearbeiten*

Felder in diesem Formular

- *Bezeichnung*: Hier wird eine Bezeichnung für die Regel angegeben. Wird eine bereits angelegte Regel bearbeitet, kann der

Name nicht mehr geändert werden. Er wird dann nur in diesem Feld angezeigt.

- *Kommentar*: Hier kann ein kurzer Kommentartext zu dieser Regel angegeben werden.
- *Aktion*: In dieser Liste wird ausgewählt, was mit einer entsprechenden E-Mail geschehen soll:

  Wird *Warnen* ausgewählt, wird nur eine Warnung in die Logdatei geschrieben. Dies ist nützlich, wenn die Regeln zunächst einmal getestet werden.

  Die Aktion *Anhalten* behält die E-Mail in der Warteschlange, ohne sie zuzustellen („Quarantäne“). Der Administrator muss die E-Mail dann näher untersuchen und abschließend löschen oder zur Zustellung freigeben.

  Mit der Einstellung *Zurückweisen* wird die E-Mail abgelehnt, und der Sender erhält den zusätzlich angegebenen Text als Fehlermeldung. Diese Option kann zu Problemen führen, wenn E-Mails per POP3 oder Multidrop abgeholt werden.

  Wird hier *Verwerfen* ausgewählt, wird die E-Mail gelöscht. Dem absendenden MTA wird jedoch bestätigt, dass die E-Mail akzeptiert wurde. Für den Absender sieht es so aus, als ob die E-Mail zugestellt wurde.
- *Information für Absender*: Der hier angegebene Text wird in die Logdatei geschrieben und eventuell an den Absender übermittelt, wenn eines der Muster für diese Regel zutrifft.
- *Dateiendung*: In diesem Eingabefeld werden die Endungen für Dateinamen angegeben, für die diese Regel zutreffen soll, z. B. „vbs“ für Visual-Basic-Macros.

  Hinweis: Manche Endungen sind nicht eindeutig. Nicht jede Datei mit der Endung „.doc“ ist eine Microsoft-Word-Datei, und nicht jeder „MIME“-Anhang hat einen Dateinamen. In jedem Fall sollte zusätzlich der „MIME-Content-Type“ für das Dokument angegeben werden.

- *MIME-Content-Type*: In diesem Feld wird der zu filternde Inhaltstyp („MIME-Content-Types“) angegeben. Der „MIME-Content-Type“ hat die Form „typ/subtyp“, z. B. „audio/wav“ oder „application/msword“.

  Der „MIME-Content-Type“ ist zwar die genauere Angabe, manche Mailprogramme (z. B. *Microsoft Outlook*) verlassen sich aber trotzdem eher auf die Endung des Dateinamens als auf diese Inhaltsangabe. Zudem kann die MIME-Angabe falsch gesetzt sein. Daher sollte zusätzlich für gefährliche Inhalte die Dateiendung angegeben werden.

  Hinweis: In diesem Feld werden reguläre Ausdrücke ausgewertet, z. B. trifft die Angabe „audio/.*“ auf alle Audioinhalte zu.

14 Webserver

14.1 Einführung

Über einen Webserver können Informationen für Besucher weltweit im WWW („World Wide Web“) bereitgestellt werden. WWW hat sich als Informationsmedium fest etabliert, da auf Webseiten Texte, Bilder und moderne Medien wie Filme und Animationen präsentiert werden können. Durch den Einsatz von Skriptsprachen und Datenbanken können Inhalte zum Zeitpunkt der Anfrage dynamisch erzeugt werden, Nachrichtenticker und Online-Shops sind typische Beispiele.

Oft wird ein Webserver auch genutzt, um Intranet-Anwendungen zu betreiben. Dabei handelt es sich um webbasierte Anwendungen, die nur innerhalb eines Unternehmens und nur für die eigenen Benutzer zugänglich sind.

Der Collax Security Gateway unterstützt all diese Möglichkeiten. Die Inhalte der Webseiten werden jeweils in einem Share abgelegt. Über den Webserver wird das Share per HTTP und HTTPS zugänglich. Andere Dienste können den gleichzeitigen Zugriff auf das Share über andere Protokolle ermöglichen, etwa zur Datenpflege über FTP oder Windows-Networking.

Der Webserver unterstützt populäre Skriptsprachen. Damit ist die Erstellung interaktiver Webseiten möglich. Die Verwendung der SQL-Datenbank im Collax Security Gateway eröffnet hier weitreichende Möglichkeiten für den Webserver.

Über die *Benutzungsrichtlinien* wird konfiguriert, aus welchen Netzen bzw. für welche Benutzer die Webseiten zugänglich sind. Über eigene Skripte bzw. Konfigurationsdateien im Share kann eine eigene Authentifizierung realisiert werden, auch gegen die interne

LDAP-Datenbank mit den im Collax Security Gateway angelegten Benutzern.

Über den Webserver im Collax Security Gateway wird zusätzlich eine Anwenderseite bereitgestellt („Webaccess“). Hier können Benutzer SSL-VPN-Anwendungen aufrufen sowie auf verschiedene andere Dienste im Collax Security Gateway zugreifen.

14.2 Verschlüsselung

Die Übertragung von Webseiten über HTTP erfolgt unverschlüsselt. Auch beim Ausfüllen von Formularen ist jede Information prinzipiell auf allen bei der Übertragung beteiligten Stationen abhörbar.

Mit HTTPS („S“ für „sicher“ bzw. „secure“) wird der Inhalt der Webseiten verschlüsselt übertragen. Es gibt die Verfahren SSL („Secure Socket Layer“) und das modernere TLS („Transport Layer Security“), die beim Verbindungsaufbau zwischen Browser und Webserver passend gewählt werden.

Bei allen Verfahren wird ein Zertifikat für den Webserver benötigt. Im Zertifikat muss der Name des Webservers (z. B. „www.example.com“) hinterlegt sein. Andernfalls wird die Browsersoftware auf Clientseite eine entsprechende Warnmeldung beim Verbindungsaufbau ausgeben. Der Browser generiert für sich selbst ebenfalls ein Zertifikat. Dieses wird aber nur zur Verschlüsselung, nicht zur Sicherstellung seiner Authentizität genutzt. Eine Authentifizierung der Person auf der Seite des Browsers erfolgt durch Login, Passwort, PIN oder TAN innerhalb der geschützten Web-Verbindung.

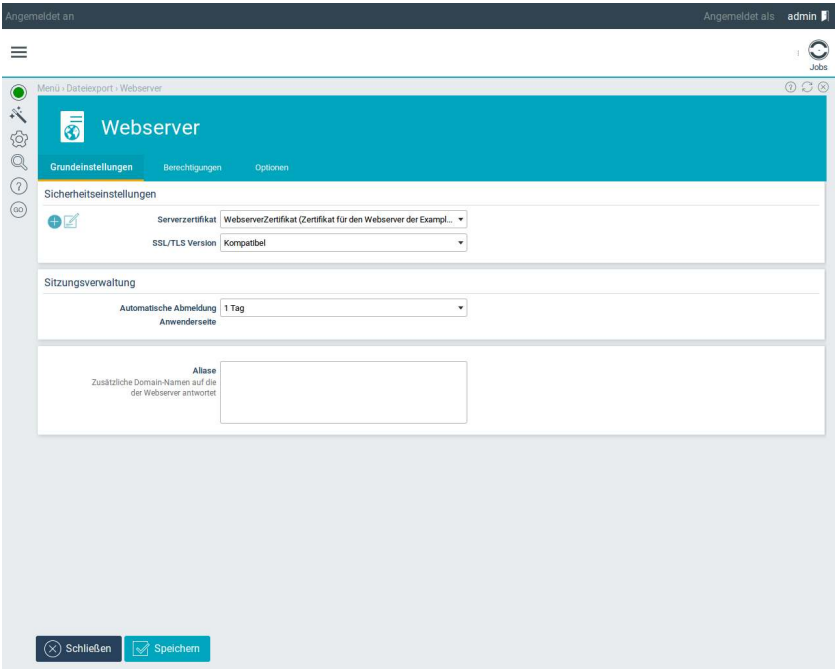
Beim Aufbau der Verbindung wird die Schlüssellänge zwischen Webserver und Browser ausgehandelt. Werte über 100 Bit Schlüssellänge gelten als sicher. Alte Browser unterstützen teilweise noch

40- oder 56-Bit-Schlüssel. In der Konfiguration des Collax Security Gateways kann festgelegt werden, ob mit solchen Gegenstellen eine Verbindung aufgebaut werden darf.

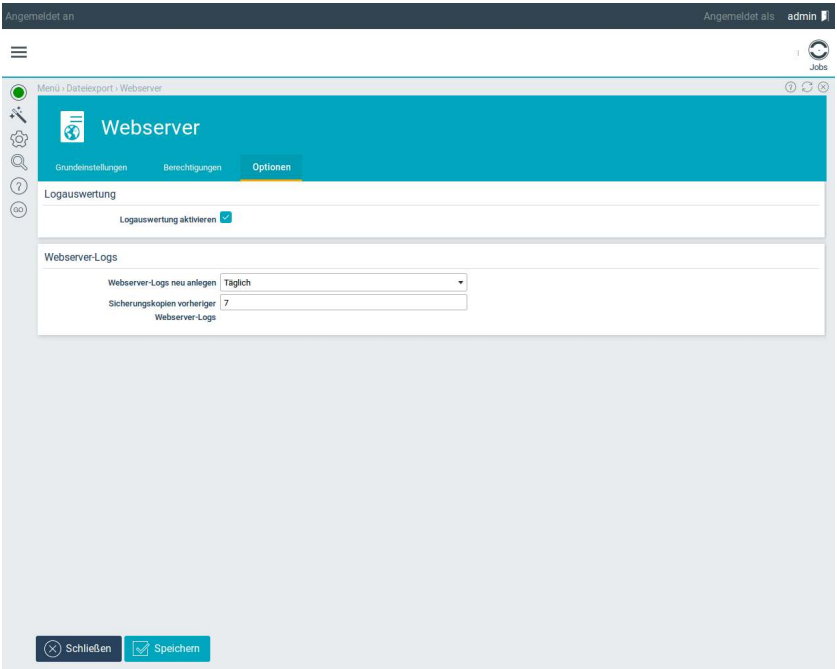
14.3 Schritt für Schritt: Aktivieren des Webservers

Um auf die im Collax Security Gateway integrierte Anwenderseite „Webaccess“ zugreifen zu können, muss zunächst der HTTPS-Webserver über die Angabe eines Zertifikats aktiviert werden. Dies ist erforderlich, da die gesamte Kommunikation verschlüsselt abläuft.

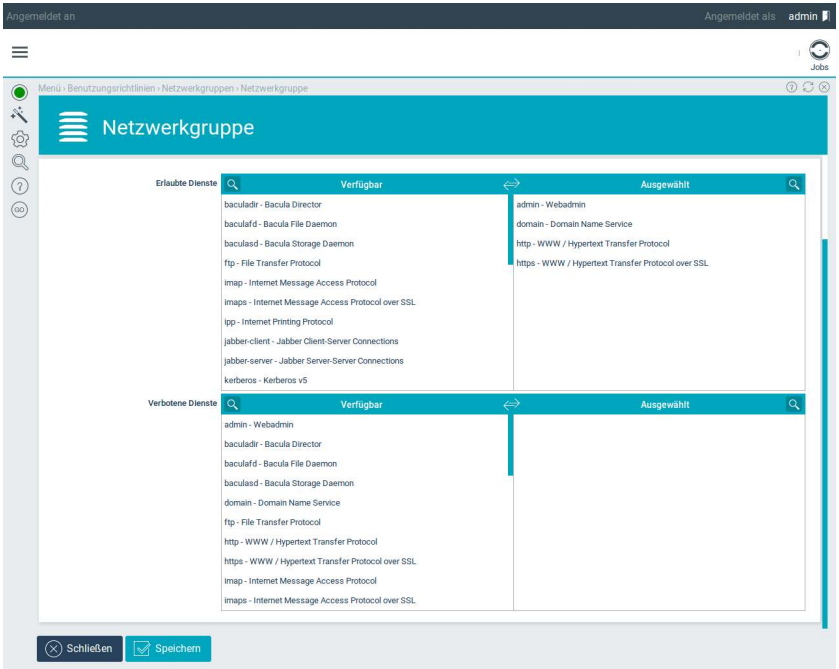
- Erstellen Sie zunächst wie im Kapitel „Zertifikate“ beschrieben, ein Zertifikat für Ihren Webserver. Beachten Sie, dass Sie für den „Common Name“ im Zertifikat den FQDN Ihres Webservers eintragen müssen.



- *Aktivieren* Sie den Webserver, indem Sie das entsprechende Zertifikat im Feld *Server-Zertifikat* selektieren.
- Setzen Sie die *Verschlüsselung mindestens* auf *128-Bit-Verfahren*. Diese Einstellung funktioniert mit gängigen Browsern und bietet im Vergleich zu 56- oder 48-Bit-Schlüsseln eine ausreichende Sicherheit.



- Wechseln Sie auf den Reiter *Optionen*.
- Aktivieren Sie die *Logauswertung*, um später unter *Überwachung/Auswertung – Auswertungen – Webserver* eine statistische Auswertung der Zugriffe auf den Webserver abrufen zu können.



- Wechseln Sie zu *Benutzungsrichtlinien – Richtlinien – Gruppen* .
- Wählen Sie die Gruppe aus, der Sie Zugriff auf den Webserver gestatten wollen. In der Abbildung ist es beispielhaft die Gruppe *Users*, die zum Bearbeiten geöffnet wird.
- Öffnen Sie in den *Berechtigungen* die Kategorie *Files*.
- Aktivieren Sie die Berechtigung *Zugriff auf Anwenderseite (HTTPS)*. Für die Anwenderseite ist dies ausreichend, da das Anmelden immer verschlüsselt abläuft.
- Falls Sie zusätzlich den Zugriff per HTTP ermöglichen wollen, öffnen Sie nun noch die Kategorie *Firewall* und wählen dort *HTTP-Connect* aus.

14.4 GUI-Referenz: *Webserver*

(Dieser Dialog befindet sich unter *Serverdienste – Webserver – Allgemein*)

In diesem Dialog werden die Konfigurationseinstellungen für den Webserver *Apache* vorgenommen.

14.4.1 Tab *Grundeinstellungen*, Abschnitt *Sicherheitseinstellungen*

14.4.1.1 Felder in diesem Abschnitt

- *Serverzertifikat*: Ist ein Zertifikat vorhanden, kann es für den Zugriff per HTTPS hier ausgewählt werden. In dieser Liste sind die Zertifikate enthalten, die für den Webserver geeignet sind (Serverzertifikate). Der Webserver-Dienst wird danach mit verfügbarer SSL-Verschlüsselung aktiviert. Mit der Aktivierung steht der Webserver mit der Anwenderseite für Zugriff per HTTPS zur Verfügung.

  Hinweis: Es sollte ein Zertifikat erstellt oder importiert werden, welches als Common Name (CN) den Hostnamen des Webservers enthält. Ansonsten geben einige Browser beim Aufbau der verschlüsselten Verbindung eine Warnung aus.
- *SSL/TLS Version*: Mit der Angabe der TLS-Version kann beeinflusst werden, welches Verschlüsselungsprotokoll der verbindende Client benutzen muss, um eine entsprechend sichere Verbindung mit dem Server herzustellen.

14.4.2 Tab *Grundeinstellungen*, Abschnitt *Sitzungsverwaltung*

14.4.2.1 Felder in diesem Abschnitt

- *Automatische Abmeldung Anwenderseite*: Aus Sicherheitsgründen werden Sitzungen auf der Anwenderseite nach einer bestimmten Leerlaufzeit unterbrochen. Mit diesem Feld wird eingestellt, wie lange diese Leerlaufzeit dauern darf.

14.4.3 Tab *Berechtigungen*, Abschnitt *Benutzerrechte*

14.4.3.1 Felder in diesem Abschnitt

- *Zugang zur Anwenderseite (HTTPS)*: Hier wird festgelegt, welche Benutzergruppe per HTTPS-Protokoll auf die Anwenderseite des Collax Security Gateway zugreifen darf.

14.4.4 Tab *Berechtigungen*,Abschnitt *Netzwerkzugang*

14.4.4.1 Felder in diesem Abschnitt

- *HTTP-Port*: Hier wird festgelegt, welche Netzwerkgruppe per HTTP-Protokoll auf den Collax Security Gateway zugreifen darf. Ist eine Berechtigung einer Netzwerkgruppe zugeteilt, wird der Webserverdienst mit den vorgenommenen Einstellungen
- *HTTPS-Port*: Hier wird festgelegt, welche Netzwerkgruppe per HTTPS-Protokoll auf den Collax Security Gateway zugreifen darf.

14.4.5 Tab *Optionen*, Abschnitt *Logauswertung*

14.4.5.1 Felder in diesem Abschnitt

- *Logauswertung aktivieren*: Durch das Aktivieren dieser Option wird die Logauswertung für den Webserver eingeschaltet. Mit der Logauswertung sind in der Systemüberwachung detaillierte Statistiken über die Nutzung des Webservers verfügbar.

14.4.6 Tab *Optionen*, Abschnitt *Webserver-Logs*

14.4.6.1 Felder in diesem Abschnitt

- *Webserver-Logs neu anlegen*: Analog zu den normalen Logdateien des Systems können hier Logdateien des Webservers nach einer gewissen Zeitspanne „rotiert“ werden.
- *Sicherungskopien vorheriger Webserver-Logs*: In diesem Feld wird eingestellt, wie viele alte Versionen der Logdatei aufbewahrt werden.

14.4.7 Tab *Extras*, Abschnitt *Extra*

14.4.7.1 Felder in diesem Abschnitt

- *Zusätzliche Optionen*: In diesem Eingabefeld können zusätzliche Einstellungen für den Webserver angegeben werden. Diese werden im globalen Abschnitt der Webserver-Konfiguration angegeben.

  Hinweis: Diese Angaben werden genau wie angegeben in die Konfigurationsdatei kopiert. Eventuelle Fehler können das Starten des Webservers verhindern oder zu Sicherheitslücken führen.

- *Datei*: Hier kann eine Datei hochgeladen werden, die Konfigurationseinstellungen beinhaltet. Diese werden in die Konfigurationsdatei des Webservers übernommen.

14.4.7.2 Aktionen für diesen Dialog

- *Importieren*: Mit dieser Aktion wird der Upload der Datei gestartet.

15 Datensicherung

15.1 Bacula Datensicherung - Einführung

Regelmäßige Datensicherung ist die einzige Möglichkeit, bei unvorhersehbaren Ereignissen wie Hardwareschäden abgesichert zu sein. Der Collax Security Gateway unterstützt u. a. die Sicherung auf externe Bandlaufwerke sowie auf Laufwerksfreigaben anderer Server.

Die eingesetzte Backuplösung besteht aus zwei Komponenten: einem Client und einem Server. Beide Komponenten können auf ein und demselben System parallel eingesetzt werden.

15.2 Schritt für Schritt: Datensicherung auf Windows-Freigabe einrichten

15.2.1 Grundeinstellungen und Sicherungsziel

- Unter *E-Mail-Adresse des Operators* tragen Sie die Adresse ein, an die Benachrichtigungen vom Backupsystem geschickt werden sollen. Wenn Sie ein Bandlaufwerk nutzen, wird eine Aufforderung zum Bandwechsel an diese Adresse geschickt.
- Wechseln Sie zu *Datensicherung – Sicherungsziele*.
- Öffnen Sie über *Hinzufügen* den Dialog zum Anlegen eines neuen Sicherungsziels.
- Geben Sie einen *Name* und einen *Kommentar* ein. Der Name kann später nicht mehr geändert werden.
- Wählen Sie als *Typ* das Windows-Netzwerkprotokoll *Entfernte SMB-/CIFS-Freigabe* aus.

- Unter *Sichern auf Rechner* geben Sie den Hostnamen oder die IP-Adresse des Zielservers an.
- Unter *Verzeichnis* müssen Sie den Namen der auf dem Zielserver exportierten Freigabe angeben.
- Geben Sie den *Login* und das passende *Passwort* ein, um auf die Freigabe zuzugreifen.
- Die Option *Spooling aktivieren* bleibt für *Entfernte SMB-/CIFS-Freigabe* ausgeschaltet.

15.2.2 Sicherungsvorgang

- Wechseln Sie zu *Datensicherung – Sicherungspläne*.
- Öffnen Sie mit der Aktion *Hinzufügen* den Dialog zum Anlegen eines neuen Sicherungsplans.
- Geben Sie eine *Bezeichnung* und einen *Kommentar* ein. Die Bezeichnung kann später nicht mehr geändert werden.
- Fügen sie mit Klick auf *Sicherungsvorgang hinzufügen* einen neuen Vorgang in den Sicherungsplan ein.
- Geben Sie eine Bezeichnung für den *Volume-Pool* ein, der ausschließlich für Vollsicherungen verwendet werden soll.
- Wählen Sie als *Sicherungs-Level Vollsicherung* aus und geben Sie als *Zyklus Wöchentlich* beginnend ab *Wochentag Samstags* an.
- Eine Vollsicherung soll vier Zyklen lang aufbewahrt werden, bevor sie überschrieben werden darf. Geben Sie als *Aufbewahrungsdauer (Tage)* 27 an.
- Die Sicherung kann *um:* Uhr 2:00 standardmäßig stattfinden.
- Fügen sie mit Klick auf *Sicherungsvorgang hinzufügen* einen zweiten Vorgang in den Sicherungsplan ein.
- Geben Sie eine andere Bezeichnung für den *Volume-Pool* ein, der ausschließlich für differenzielle Sicherungen verwendet werden soll.

- Wählen Sie als *Sicherungs-Level Differenzielle Sicherung* aus und geben Sie als *Zyklus Täglich* beginnend *Am: Ganze Woche (Mo-So)* an.
- Auch diese Sicherung kann *um:* Uhr 2:00 standardmäßig stattfinden.

15.2.3 Zuordnung

- Wechseln Sie ins Formular *Datensicherung Zuordnungen*.
- Öffnen Sie mit der Aktion *Hinzufügen* eine neue Zuordnung zur Bearbeitung.
- Wählen Sie als *Quelle/Client* den lokalen Rechner aus.
- Wählen Sie als *Zu sichernde Daten Alles*.
- Als *Sicherungsplan* wählen Sie den zuvor erstellten Ablaufplan aus und geben danach das definierte SMB-CIFS- *Ziel* an.

Speichern Sie die Einstellungen und aktivieren Sie anschließend die vorgenommene Konfiguration.

15.3 GUI-Referenz: Datensicherung *Allgemein*

(Dieser Dialog befindet sich unter *Datensicherung – Allgemein*

15.3.1 Tab *Grundeinstellungen*, Abschnitt *Operator*

15.3.1.1 Felder in diesem Abschnitt

- *E-Mail-Adresse des Operators*: Statusmeldungen der Datensicherung werden an die hier eingetragene E-Mail-Adresse gesendet.

15.3.2 Tab *Grundeinstellungen*, Abschnitt *Fremder Backup-Server*

15.3.2.1 Felder in diesem Abschnitt

- *Erlaube Zugriff von fremdem Backup-Server*: Übernimmt ein anderer Collax Server die Sicherung lokaler Daten muss der Zugriff hier erlaubt werden.
- *Identifikator des Backup-Servers*: Der entfernte Sicherungsservers muss sich mit dem Identifikator am lokalen System ausweisen, um die Datensicherung übernehmen zu können.
- *Internes Passwort des lokalen Backup-Systems*: Zeigt das Passwort des lokalen Sicherungssystems. Wird verwendet bei Kommunikation zwischen mehreren Sicherungssystemen.
- *Identifikator des lokalen Backup-Systems*: Zeigt den Identifikator des lokalen Sicherungssystem. Wird bei Kommunikation mehrerer Sicherungssysteme verwendet.

15.3.3 Tab *Grundeinstellungen*, Abschnitt *Einstellungen*

15.3.3.1 Felder in diesem Abschnitt

- *Verhalten bei Platzbedarf*: Hier wird eingestellt, ob bei einem Sicherungsvorgang mit weiterem Platzbedarf die Medien automatisch erweitert werden können, oder ob dies von Hand durchgeführt werden soll.
- *Quota des Backup-Systems (GB)*: Größenbegrenzung für lokale Sicherung. Beschreibt den maximal zu belegenden Platz auf der Platte.
- *Detaillierte Dateilisten nach Datenwiederherstellung*: Nach einer durchgeführten Datenwiederherstellung wird eine E-Mail mit Statusinformation an den Backup-Administrator versendet. Ist diese Option gesetzt, wird zusätzlich eine Liste aller wiederhergestellten Dateien versendet. Diese Liste ist potenziell sehr lang.
- *Dateilistenabgleich bei Datensicherung (Accurate mode)*: Standardmäßig wird bei Inkrementellen Backups anhand des Änderungszeitpunktes der Datei entschieden ob eine Datei gesichert werden muss. Dadurch lässt sich nicht feststellen, welche Dateien seit dem letzten Backup gelöscht worden oder mit einem älteren Änderungsdatum hinzugefügt worden sind. Ist diese Option gesetzt, so werden auch diese Dateien mitgesichert, indem mit einer Liste aller Dateien des letzten Backups verglichen wird. Dabei ist zu beachten, dass der Ressourcenbedarf (CPU und Arbeitsspeicher) steigt.
- *Ziel für Recovery-Informationen*: Falls eine Zuordnung die für eine Wiederherstellung von Bandlaufwerken nötigen Verwaltungsdaten der Sicherungsprozesse mitsichert, lässt sich dafür mit dieser Option ein weiteres, separates Sicherungsziel festlegen. Auf dieses werden dann die Informationen über Kataloge und dergleichen gesichert, so dass Sicherungen auch nach einem

Komplettausfall von einem Tapelaufwerk zurückgespielt werden können. Für diese Option stehen nur dateibasierte Sicherungsziele zur Auswahl.

15.3.4 Tab *Grundeinstellungen*, Abschnitt *Kompression und Verschlüsselung*

15.3.4.1 Felder in diesem Abschnitt

- *Datenkompression*: Ist diese Option aktiviert, so werden alle Dateien mit GNU ZIP komprimiert. Dies geschieht auf Dateibasis, das heißt falls eine der Dateien unlesbar wird, so ist tatsächlich nur diese Datei betroffen und nicht alle Dateien einer Sicherung. Diese Einstellung sollte nur dann aktiviert werden, wenn das Sicherungsziel keine Hardwarekompression unterstützt.
- *Kompressionsstärke*: Daten können unterschiedlich stark komprimiert werden, was sich in Speicherbedarf und Rechenaufwand auswirkt. Bei der schnellsten Kompression (Wert 1) erhält man größere Dateien als bei einer langsamen Kompression (Wert 9). Es wird prinzipiell nicht empfohlen eine Kompressionsstärke größer als 6 zu wählen, da der Rechenaufwand unverhältnismäßig zum Platzersparnis wächst.
- *Zertifikat für Datenverschlüsselung*: Falls es gewünscht ist, dass sämtliche Daten bei Sicherungsvorgängen verschlüsselt und damit für dritte unleserlich gemacht werden, kann hier ein Zertifikat ausgewählt werden, das als Schlüssel verwendet werden soll. Beim Wiederherstellen werden die Dateisignaturen überprüft und der Vorgang bei Unstimmigkeiten unterbrochen. Metadaten einer Datei wie Pfadname und Berechtigungen werden dabei nicht mitverschlüsselt.
- *Master-Zertifikat*: Bei der Verschlüsselung von Sicherungen gilt es

zu beachten, dass diese nicht wiederherstellbar sind, wenn die Schlüssel verloren gegangen sind. Um das Risiko, Sicherungen aufgrund verloren gegangener Zertifikate nicht wieder herstellen zu können, zu minimieren, kann mit einem zweiten sogenannten Master-Zertifikat verschlüsselt werden. Im Falle von Master-Zertifikaten ist es empfehlenswert, den privaten Schlüssel nicht auf dem Server zu lagern, sondern diesen nur zu importieren, wenn tatsächlich ein Zertifikat verloren gegangen ist und Sicherungen nicht mehr anders wiederherzustellen sind.

15.3.5 Tab *Laufzeitbeschränkung*, Abschnitt *Laufzeitbeschränkung für Jobs*

15.3.5.1 Felder in diesem Abschnitt

- *Max. Startverzögerung (Stunden)*: Die maximale Startverzögerung, gibt an wie lange sich ein Job eines geplanten Sicherungsjobs verzögern darf, weil beispielsweise noch ein vorhergehender Job läuft
- *Max. Laufzeit (Stunden)*: Die maximale Laufzeit gibt an, wie lange ein Job aktiv sein darf.
- *Max. Wartezeit (Stunden)*: Innerhalb eines Jobs gibt die maximale Wartezeit an, wie lange ein Job unterbrochen werden darf, um zum Beispiel ein Band zu wechseln.
- *Max. Dauer (Stunden)*: Die maximale Dauer gibt an, wie lange ein Job inklusive Startverzögerung, Lauf- und Wartezeit überhaupt dauern darf, damit Jobs zum Beispiel nicht während der Arbeitszeit durchgeführt werden.

15.3.6 Tab *Berechtigungen*, Abschnitt *Zugriff erlauben für ...*

15.3.6.1 Felder in diesem Abschnitt

- *Bacula-Netzwerkzugriff*: Beschreibt die Berechtigungen für den Netzwerkzugriff wenn mehrer Sicherungssysteme verwendet werden.

15.3.7 Aktionen für dieses Formular

- *Passwort zurücksetzen*: Diese Aktion ändert das angegebene Passwort des lokalen Sicherungssystems. Wenn das Passwort schon zur Kommunikation verwendet wird, können nach Ausführen dieser Aktion Probleme auftauchen.
- *Abbrechen*: Bearbeiten der Allgemeinen Sicherungseinstellungen beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten der Allgemeinen Sicherungseinstellungen beenden. Die Änderungen werden gespeichert.

15.4 GUI-Referenz: *Zuordnungen*

(Dieser Dialog befindet sich unter *Systembetrieb – Datensicherung – Zuordnungen* .)

Durch dieses Formular ist es möglich, sehr flexible Sicherungsabläufe zu definieren. Zuvor definierte Rechner, Ziele, Pläne und Datensätze können durch entsprechende Zuordnung auf die Anforderungen solcher Abläufe im lokalen Netzwerk angepasst werden. Eine Sicherung lokaler Daten auf entfernte Verzeichnisse wie auch die Sicherung von entfernten Arbeitsstationen auf lokal angeschlossene Bandlaufwerke sind möglich.

Zuordnungen sind zudem Voraussetzung, um Datenwiederherstellung, System-Recovery oder Monitor-Zugriff durchführen zu können.

15.4.1 Liste: *Zuordnungen*

In diesem Dialog werden alle angelegten Zuordnungen aufgelistet. Es können neue Zuordnungen hinzugefügt, editiert oder gelöscht werden.

15.4.1.1 Felder in diesem Formular

- *Bezeichnung*: Zeigt die Bezeichnung der Zuordnung.
- *Kommentar*: Weitere Beschreibung der Zuordnung.
- *Quelle*: Zeigt an, von welcher Quelle die Daten gesichert werden.
- *Ziel*: Zeigt an, wohin die Daten gesichert werden.

15.4.1.2 Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Durch Doppelklick oder Klick im Kontextmenü, kann ein ausgewählter Tabelleneintrag editiert werden.
- *Löschen*: Durch diese Aktion im Kontextmenü kann ein ausgewählter Tabelleneintrag gelöscht werden.

15.4.1.3 Aktionen für dieses Formular

- *Hinzufügen*: Mit dieser Aktion wird eine Zuordnung hinzugefügt.

15.4.2 *Zuordnung bearbeiten*

15.4.2.1 Abschnitt *Grundeinstellungen*

Felder in diesem Abschnitt

- *Bezeichnung*: Hier wird die Bezeichnung der Zuordnung eingegeben oder angezeigt.
- *Kommentar*: Weitere Beschreibungen können in diesem Feld hinzugefügt werden.

15.4.2.2 Abschnitt *Zuordnung*

Felder in diesem Abschnitt

- *Quelle/Client*: Hier wird ausgewählt, welcher Rechner gesichert werden soll.
- *Zu sichernde Daten*: Hier wird ausgewählt, welche Daten gesichert werden sollen. Wird der lokale Server gesichert, können einzelne Sicherungselemente unterschieden werden.
- *In die Sicherung aufnehmen*: Zeigt einzelne Sicherungselemente, die für die zu sichernden Daten ausgewählt werden können.
- *Sichere Zustand des Backup-Servers*: Verwaltungsdaten der Sicherungsprozesse können separat mit dieser Option gesichert werden.
- *Inhaltsliste*: Ist der zu sichernde Server oder Rechner kein Collax Security Gateway, ist eine zuvor zu definierende Inhaltsliste der zu sichernden Daten anzulegen. Diese spezielle Inhaltliste kann hier ausgewählt werden.
- *Sicherungsplan*: Ein zuvor erstellter Sicherungsplan kann hier verwendet werden, um festzulegen, wann über welchen Volume-Pool gesichert werden soll.
- *Ziel*: Hier wird ausgewählt, wohin gesichert werden soll.

- *Band nach Sicherung freigeben*: Wenn das Sicherungsziel ein Band ist, kann hier eingestellt werden, ob der Sicherungs-Job das Band automatisch freigibt, um es anschließend zurückzuspulen und auswerfen zu können. Wenn diese Option nicht gesetzt ist, kann das Band manuell unter *Datensicherung – Status und Betrieb* mit der Aktion *Aushängen* freigegeben werden.

  Soll das Band auch automatisch zurück gespult und ausgeworfen werden, kann die Option *Band wird nach Freigabe zurückgespult/ausgeworfen* bei den Einstellungen zum Sicherungsziel aktiviert werden.
- *Vor Sicherung Slot-Belegung bestimmen*: Wenn Bandmagazine für Sicherungen gewechselt werden müssen, muss dem Sicherungssystem vor der Sicherung die Slot-Belegung bekannt gegeben werden. Dies kann manuell geschehen, in dem im Formular *Status und Betrieb* die Aktion *Slot-Belegung bestimmen* ausgeführt wird. Mit der hier angegeben Option kann die Slot-Belegung für die definierte Sicherungszuordnung auch automatisch vor Start der Sicherung bestimmt werden. Können Barcodes zur Identifizierung der Bänder verwendet werden, ist die Bestimmung der Slot-Belegung sehr schnell abgeschlossen. Ist kein Barcode-Reader vorhanden, muss zur Bestimmung zunächst jedes Band an den Anfang zurückgespult werden. Dies dauert entsprechend länger als die Bestimmung anhand von Barcodes.

  Hinweis: Um die Bestimmung zeitlich zu steuern, kann eine separate Zuordnung ohne zu sichernde Komponenten definiert werden, welche die Slot-Belegung automatisch bestimmt.

15.4.2.3 Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten der Zuordnung beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten der Zuordnung beenden. Die Änderungen werden gespeichert.

15.5 GUI-Referenz: *Sicherungsziele*

(Dieser Dialog befindet sich unter *Datensicherung – Ziele*)

15.5.1 Liste: *Sicherungsziele*

15.5.1.1 Felder in diesem Formular

- *Bezeichnung*: Hier wird die Bezeichnung des Ziels angezeigt.
- *Kommentar*: Weitere Beschreibung des Ziels.
- *Typ*: Zeigt den Typ des Sicherungziels an.
- *Details*: Je nach Typ des Sicherungziels wird in dieser Spalte der entsprechende Systempfad oder der UNC-Pfad angezeigt.

15.5.1.2 Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Durch Doppelklick oder Klick im Kontextmenü, kann ein ausgewählter Tabelleneintrag editiert werden.
- *Ziel überprüfen (nur CIFS/NFS)*: Durch diese Aktion im Kontextmenü kann ein Schreibtest für CIFS und NFS Ziele durchgeführt werden.

- *Medien-Initialisierung und -Status*: Durch diese Aktion können Wechselmedien für VTL Initialisiert werden, oder der Status der Medien abgerufen werden.
- *Löschen*: Durch diese Aktion im Kontextmenü kann ein ausgewählter Tabelleneintrag gelöscht werden.

15.5.1.3 Aktionen für dieses Formular

- *Hinzufügen*: Mit dieser Aktion wird ein Sicherungsziel hinzugefügt.

15.5.2 *Ziel bearbeiten*

15.5.2.1 Abschnitt *Sicherungsziel*

Felder in diesem Abschnitt

- *Bezeichnung*: Hier wird die Bezeichnung des Ziels eingegeben oder angezeigt.
- *Kommentar*: Weitere Beschreibungen können in diesem Feld hinzugefügt werden.
- *Typ*: Hier wird die Art des Sicherungsziels ausgewählt, entsprechende individuelle Einstellungen sind vorzunehmen.

15.5.2.2 Abschnitt *Grundeinstellungen*

Felder in diesem Abschnitt

- *Spooling aktivieren*: Um die Sicherung auf Bandlaufwerke zu optimieren, kann hier Spooling aktiviert werden. Dadurch werden Daten zunächst in ein Spool-Verzeichnis geschrieben, bevor die Daten auf Band geschrieben werden.

- *Spool-Größe (GB)*: Gibt die maximale Größe des Spool-Verzeichnisses an.
- *Automatisch neue Medien belegen*: Ist diese Option aktiviert, so werden bei einer Sicherung bisher ungenutzte Mediendefinitionen automatisch auf freie Medien dieses Sicherungsziels angewendet. Um also einen vollständig automatisierten Ablauf zu gewährleisten, muss diese Option aktiviert und in den Grundeinstellungen unter "Verhalten bei Platzbedarf" der Punkt "Automatisch neue Mediendefinitionen anlegen" gewählt werden.

15.5.2.3 Abschnitt *Model/Typ*
Felder in diesem Abschnitt

- *Gerätemodell/Gerätetyp*: Je nach Bandlaufwerk kann hier der entsprechende Typ ausgewählt werden. Im Normalfall kann die Einstellung *Standard-Laufwerk* unverändert bleiben. Falls das Bandlaufwerk weder mit den Standardeinstellungen noch mit den vorhandenen Laufwerkstypen korrekt funktioniert, können Feineinstellungen mit dem *Expertenmodus* vorgenommen werden.

15.5.2.4 Abschnitt *Einstellungen für Bandlaufwerk*
Felder in diesem Abschnitt

- *Linux-Device-Name des Bandlaufwerks*: Ist ein Bandlaufwerk angeschlossen, muss hier der Linux-Gerätename eingetragen werden.

15.5.2.5 Abschnitt *Bandlaufwerk Detaileinstellungen* Felder in diesem Abschnitt

- *Bandlaufwerk versteht "End of Medium"-Anfragen*: If No, the archive device is not required to support end of medium ioctl request, and the storage daemon will use the forward space file function to find the end of the recorded data. If Yes, the archive device must support the ioctl MTEOM call, which will position the tape to the end of the recorded data. In addition, your SCSI driver must keep track of the file number on the tape and report it back correctly by the MTIOCGET ioctl. Note, some SCSI drivers will correctly forward space to the end of the recorded data, but they do not keep track of the file number. Default setting for Hardware End of Medium is Yes. This function is used before appending to a tape to ensure that no previously written data is lost. We recommend if you have a non-standard or unusual tape drive that you use the btape program to test your drive to see whether or not it supports this function. All modern (after 1998) tape drives support this feature.
- *Bandlaufwerk kann schnell vorspulen*: If No, the archive device is not required to support keeping track of the file number (MTIOCGET ioctl) during forward space file. If Yes, the archive device must support the ioctl MTFSF call, which virtually all drivers support, but in addition, your SCSI driver must keep track of the file number on the tape and report it back correctly by the MTIOCGET ioctl. Note, some SCSI drivers will correctly forward space, but they do not keep track of the file number or more seriously, they do not report end of medium. Default setting for Fast Forward Space File is Yes.
- *Benutze MTIOCGET-Anfragen*: f No, the operating system is not required to support keeping track of the file number and repor-

ting it in the (MTIOCGET ioctl). The default is Yes. If you must set this to No, Bacula will do the proper file position determination, but it is very unfortunate because it means that tape movement is very inefficient.

- *BSF am Medienende*: If No, the default, no special action is taken by Bacula with the End of Medium (end of tape) is reached because the tape will be positioned after the last EOF tape mark, and Bacula can append to the tape as desired. However, on some systems, such as FreeBSD, when Bacula reads the End of Medium (end of tape), the tape will be positioned after the second EOF tape mark (two successive EOF marks indicated End of Medium). If Bacula appends from that point, all the appended data will be lost. The solution for such systems is to specify BSF at EOM which causes Bacula to backspace over the second EOF mark. Determination of whether or not you need this directive is done using the test command in the btape program.
- *Doppelte Medienende-Markierung*: If Yes, Bacula will write two end of file marks when terminating a tape -- i.e. after the last job or at the end of the medium. If No, the default, Bacula will only write one end of file to terminate the tape.
- *Laufwerk kann Records zurückspulen*: If Yes, the archive device supports the MTBSR ioctl to backspace records. If No, this call is not used and the device must be rewound and advanced forward to the desired position. Default is Yes for non random-access devices. This function if enabled is used at the end of a Volume after writing the end of file and any ANSI/IBM labels to determine whether or not the last block was written correctly. If you turn this function off, the test will not be done. This causes no harm as the re-read process is precautionary rather than required.
- *Laufwerk kann Dateien zurückspulen*: If Yes, the archive device

supports the MTBSF and MTBSF ioctls to backspace over an end of file mark and to the start of a file. If No, these calls are not used and the device must be rewound and advanced forward to the desired position. Default is Yes for non random-access devices.

- *Laufwerk kann Records vorspulen*: If Yes, the archive device must support the MTFSR ioctl to forward space over records. If No, data must be read in order to advance the position on the device. Default is Yes for non random-access devices.
- *Laufwerk kann Dateien vorspulen*: If Yes, the archive device must support the MTFSF ioctl to forward space by file marks. If No, data must be read to advance the position on the device. Default is Yes for non random-access devices.

15.5.2.6 Abschnitt *Einstellungen für Bandwechsler*

Felder in diesem Abschnitt

- *Gerät ist Bandwechsler*: Um einen Bandlaufwerk mit Bandwechsler korrekt anzusteuern, muss hier angegeben werden, dass das Gerät ein Bandwechsler ist.
- *Wechsler*: Hier ist der Geräte-Name des Bandwechslers auszuwählen.
- *Barcode-Leser*: Hier ist anzugeben, mit welcher Art Barcode-Leser das Bandwechselgerät ausgerüstet ist.
- *Forcierter Bandauswurf*: Für spezielle Bandwechselgeräte ist es erforderlich, das Band offline zu setzen, damit ein Wechselvorgang ausgeführt werden kann. Bandwechselgeräte des heutigen Standards benötigen diese Option üblicherweise nicht. Deshalb kann diese Option zuächst leergelassen werden.

15.5.2.7 Abschnitt *Band-Handhabung*
Felder in diesem Abschnitt

- *Band wird nach Freigabe zurückgespult/ausgeworfen*: Wenn das Laufwerk MTOFFL unterstützt, wird das Band mit dieser aktivierten Option nach abgeschlossenem Sicherungs-Job zurückgespult und ausgeworfen. Voraussetzung für den Auswurf des Bandes ist die gesetzte Option *Band nach Sicherung freigeben* in den Einstellungen einer Zuordnung.
- *Suche regelmäßig nach eingelegtem Band (in Sekunden)*: Der eingestellte Zeitwert gibt vor, in welchem Zyklus das Laufwerk nach einem neuen Band durchsucht wird. Mit dieser Option kann das neue Band eingelegt werden, der Sicherungsprozess erkennt dies und setzt die Sicherung automatisch fort.

15.5.2.8 Abschnitt *Einstellungen für CIFS-Sicherung*
Felder in diesem Abschnitt

- *Sichern auf Rechner*: Hier wird der Name oder die IP-Nummer des Systems angegeben, welches die Laufwerksfreigabe bereitstellt.
- *Verzeichnis*: Bei Sicherung per SMB/CIFS wird auf eine Freigabe des Zielrechners gesichert. Es kann Freigabe/Unterverzeichnis oder nur eine Freigabe hier angegeben werden. Auf dem Zielrechner wird das Unterverzeichnis automatisch angelegt.
- *Login*: Ist die Freigabe durch bestimmte Gruppenrechte geschützt, ist hier der passende Login-Name einzutragen, damit der Collax Security Gateway auf die Freigabe zugreifen kann.
- *Passwort*: Ist ein Login angegeben, sollte hier das entsprechende Passwort für einen korrekten Zugriff auf die Freigabe eingetragen werden.

- *Anmelde-Domain*: Geschieht der Zugriff mit einem Domänen-Benutzer in einer Domäne, wird hier die zugehörige Anmelde-Domain eingetragen.
- *Optionen*: Hier können spezifische Parameter zum Einhängen des Sicherungsziels angegeben werden. Die Parameter sind in Absprache mit dem Software-Hersteller einzutragen.

15.5.2.9 Abschnitt *Einstellungen für NFS-Sicherung*

Felder in diesem Abschnitt

- *Sichern auf Rechner*: Hier wird der Name oder die IP-Nummer des Systems angegeben, welches das NFS-Verzeichnis bereitstellt.
- *Verzeichnis*: Hier wird das NFS-Verzeichnis angegeben.

15.5.2.10 Abschnitt *Einstellungen für USB- und ähnliche Ziele*

Felder in diesem Abschnitt

- *Partition*: Hier kann die Partition eines vorhandenen Medium ausgewählt werden. Als Medien können hier USB-, iSCSI-, eSATA-Festplatten oder Logical Volumes erkannt werden.

15.5.2.11 Abschnitt *Einstellungen für Virtual Tape Libraries mit Wechselmedien*

Felder in diesem Abschnitt

- : Hier wird ein Hinweis zur Benutzung des Assistenten angezeigt, wenn eine neues ziel erstellt werden soll.

Abschnitt *Medium*
Felder in diesem Abschnitt

- *Partition*: Sind Medien definiert, kann hier die gewünschte Partition gewählt werden.

Aktionen für diesen Abschnitt

- *Entfernen*: Mit dieser Aktion wird das Element gelöscht.

Aktionen für diesen Abschnitt

- *Medium hinzufügen*: Hier können Laufwerke als Wechselmedium hinzugefügt werden. Falls die Laufwerke nicht über den Assistenten vorbereitet werden, muss nach dem Abspeichern die Aktion Medien initialisieren im Kontextmenü ausgeführt werden.

15.5.2.12 Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten des Sicherungsziels beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten des Sicherungsziels beenden. Die Änderungen werden gespeichert.

15.6 GUI-Referenz: *Pläne*

(Dieser Dialog befindet sich unter *Datensicherung – Pläne*)

In diesem Formular können Sicherungsvorgänge, Sicherungszeiten und Sicherungs-Level zu einem Plan verknüpft werden. Zudem ist es hier möglich, verschiedene Vorgänge auf verschiedene Volume-Pools sichern zu lassen. Dies ist letztendlich die Voraussetzung um das Vorhaben der Band-Rotation innerhalb einer Sicherungsstrategie umzusetzen, ebenso ist dadurch die Umsetzung von Sicherungsschemata, wie Türme-von-Hanoi, oder Großvater-Vater-Sohn, möglich.

Es wird empfohlen, zur Erstellung von Sicherungsplänen den Assistenten für Datensicherung zu benutzen. Die dort generierten Pläne können anschließend flexibel modifiziert werden.

15.6.1 Liste *Pläne*

Die Liste zeigt die definierten Sicherungspläne.

15.6.1.1 Felder in dieser Tabelle

- *Bezeichnung*: In dieser Spalte steht der Name des Sicherungsplans.
- *Kommentar*: Zeigt weitere Beschreibung des Plans.

15.6.1.2 Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion im Kontextmenü, oder mittels Doppel-Klick, kann der Eintrag bearbeitet werden.
- *Löschen*: Mit dieser Aktion im Kontextmenü kann der Eintrag gelöscht werden.

15.6.1.3 Aktionen für dieses Formular

- *Hinzufügen*: Das Formular für einen neuen Eintrag wird geöffnet.

15.6.2 *Plan bearbeiten*

15.6.2.1 *Plan bearbeiten*, Abschnitt *Grundeinstellungen*
Felder in diesem Abschnitt

- *Bezeichnung*: Hier wird der Name des Plans angezeigt oder eingegeben.
- *Kommentar*: Zusätzliche Informationen zu Plan können hier hinterlegt werden.

15.6.2.2 *Plan bearbeiten*, Abschnitt *Vorgang*
Felder in diesem Abschnitt

- *Volume-Pool*: Hier wird eine beliebige Bezeichnung für den Volume-Pool angegeben. Ein Volume-Pool ist eine Menge von Medien, die für die Sicherung in einem Vorgang verwendet wird. Es können verschiedene Volume-Pools über mehrere Sicherungsvorgänge definiert werden. Im einfachsten Fall wird ausschließlich ein Volume-Pool für alle Sicherungsvorgänge benutzt.

- *Aufbewahrungsdauer*: Dieser ganzzahlige Wert kennzeichnet die minimale Aufbewahrungsdauer in Tagen, bevor die gesicherten Daten überschrieben werden. Im einfachen Fall ist die Aufbewahrungsdauer genau der Zyklusdauer abzüglich einem Tag. Es besteht ein Datansatz, der innerhalb des nächsten Vorgangs überschrieben wird. Ist die Aufbewahrungsdauer zweimal so lange wie die Zyklusdauer, abzüglich einem Tag, so bestehen immer zwei Datensätze dieses Sicherungsvorgangs. Um einen Datensatz über 26 Wochen zu erhalten, wäre der Wert 181 in Verbindung mit einem wöchentlichen Zyklus zu setzen.

  Ein Wert der kleiner ist, als die Zyklusdauer, bedeutet, dass der Datensatz vor dem nächsten Vorgang zum Überschreiben freigegeben wird. Der Vorgang wird, wie vorgegeben, zum nächsten Zyklus ausgeführt.
- *Sicherungs-Level*: Es werden 3 Sicherungs-Level unterschieden.
  - Vollsicherung: Hier werden alle Daten gesichert, unabhängig vom Datum der letzten Sicherung innerhalb desselben Sicherungsplans.
  - Inkrementelle Sicherung: Bei der inkrementellen Sicherung werden alle Daten gesichert, die sich seit der letzten durchgeführten Sicherung innerhalb desselben Sicherungsplans verändert haben, oder die seit der letzten durchgeführten Sicherung innerhalb desselben Sicherungsplans neu hinzu gekommen sind.
  - Differenzielle Sicherung: Hier werden alle Daten gesichert, die sich seit der letzten Vollsicherung innerhalb desselben Sicherungsplan geänderten haben oder neu hinzugekommen sind.
- *Zyklus*: Hier wird die regelmäßige Wiederholung eines Sicherungsvorgangs festgelegt. Die längste Dauer eines Zyklus' beträgt ein Jahr, die kürzeste Dauer beträgt einen Tag.

- *Im:*: Angabe des Monats in dem der Vorgang ausgeführt werden soll, wenn die Zyklusdauer ein Jahr beträgt.
- *Am:*: Bestimmt den Tag der Durchführung, entweder absolut am ersten Tag des gewählten Monats, oder ein Wochentag einer bestimmten Woche innerhalb des gewählten Monats.
- *Für:*: Hier wird eine bestimmte Woche für die Durchführung gesetzt, wenn als Zyklus *In bestimmten Wochen* angegeben ist. Die Angabe der Wochen beziehen sich auf das laufende Kalenderjahr.
- *Wochentag*: Verwendung bei jährlichem, monatlichem oder wöchentlichem Zyklus.
- *Am:*: Der Vorgang kann Werktags oder jeden Tag der Woche durchgeführt werden.
- *Um:*: Gibt die Uhrzeit der Durchführung an.

Aktionen für diesen Abschnitt

- *Löschen*: Mit dieser Aktion wird ein Sicherungsvorgang innerhalb eines Plans gelöscht.

15.6.2.3 Aktionen für dieses Formular

- *Sicherungsvorgang hinzufügen*: Hier wird ein Vorgang zu dem geöffneten Plan hinzugefügt.
- *Abbrechen*: Die Bearbeitung des Formulars wird beendet. Änderungen werden verworfen.
- *Speichern*: Die Bearbeitung des Formulars wird beendet. Änderungen werden gespeichert.

15.7 GUI-Referenz: *Status und Betrieb*

(Dieser Dialog befindet sich unter *Datensicherung – Status und Betrieb*)

Über diesen Dialog können Statusinformationen des Datensicherungssystems abgerufen sowie administrative Aufgaben erledigt werden.

15.7.1 Abschnitt Anzeigen

15.7.1.1 Aktionen in diesem Abschnitt

- *Alle Jobs anzeigen*: Mit dieser Aktion werden alle Sicherungs- und Restore-Jobs des Systems angezeigt. In der Detailansicht sind unter Anderem der Umfang und Inhalt von Sicherungen sowie der Status von Jobs ersichtlich.
- *Laufende Jobs anzeigen*: Mit dieser Aktion werden alle Sicherungs- und Restore-Jobs angezeigt, die aktuell noch nicht beendet sind.
- *Erfolgreiche Jobs anzeigen*: Mit dieser Aktion werden alle Sicherungs- und Restore-Jobs angezeigt, die erfolgreich beendet worden sind.
- *Nicht erfolgreiche Jobs anzeigen*: Mit dieser Aktion werden alle Sicherungs- und Restore-Jobs angezeigt, die mit einem Fehler oder einem schweren Fehler beendet worden sind.

15.7.2 Abschnitt Anzeigen

15.7.2.1 Aktionen in diesem Abschnitt

- *Pools anzeigen*: Die in den Sicherungsvorgängen verwendeten Volume-Pools können hier aufgelistet werden. Weitere Informationen über die Volume-Pools können über das Kontext-Menü eines Pools, Rechter-Maus-Klick, aufgerufen werden.
- *Medien anzeigen*: Die über einen Sicherungs-Job erzeugten Medien können über diese Aktion angezeigt werden. Die Bearbeitung oder Veränderung von Medien sollte nur im Notfall erfolgen.

15.7.3 Abschnitt Definierte Jobs starten

15.7.3.1 Felder in diesem Abschnitt

- *Quelle/Client*: Hier wird die entsprechende Quelle, oder ein Client ausgewählt, der manuell gesichert werden soll.
- *File-Set*: Hier wird angegeben, welche Daten manuell gesichert werden sollen. Es kann nur ein einzelner Datensatz ausgewählt werden. Sollen mehrere Datensätze von Hand gesichert werden, kann dies seriell durchgeführt werden.
- *Volume-Pool*: Hier wird ausgewählt in welchen Volume-Pool gesichert werden soll.
- *Sicherungs-Level*: Hier kann zwischen verschiedenen Sicherungstypen gewählt werden.
- *Ziel*: Die manuelle Sicherung erfolgt beim Start auf das hier angegebene Sicherungsziel.

15.7.3.2 Aktionen in diesem Abschnitt

- *Start*: Mit dieser Aktion wird die eingestellte manuelle Sicherung gestartet. Der Status des gestarteten Sicherungs-Jobs kann anschließend über die Anzeige der Jobs eingesehen werden.

15.7.4 Abschnitt Datenträger hinzufügen/beschriften...

15.7.4.1 Felder in diesem Abschnitt

- *Ziel/Gerät*: Hier wird ein Ziel oder ein Gerät gewählt, für das ein neues Medium hinzugefügt oder beschriftet werden soll.
- *Name*: Hier wird die Bezeichnung des neuen Mediums angegeben, das erzeugt oder beschriftet werden soll.

15.7.4.2 Aktionen in diesem Abschnitt

- *Hinzufügen*: Mit dieser Aktion wird ein Medium/Datenträger mit dem angegebenen Namen innerhalb des ausgewählten Ziels angelegt. Die angelegten Informationen sind Meta-Daten, es wird entsprechend kein physikalisches Medium beschriftet. Diese Aktion ist im Allgemeinen nur sinnvoll, wenn für das Ziel die Option *Automatisch neue Medien belegen* aktiviert ist.
- *Beschriften*: Mit dieser Aktion wird ein Medium mit dem angegebenen Namen beschriftet. Die Aktion führt zum physikalischen Beschriften, des Mediums, es werden damit Informationen auf das Band oder die Festplatte übertragen. Diese Aktion ist sinnvoll, wenn Bänder mit bestimmten Namen belegt werden sollen.

15.7.5 Abschnitt Storage-Geräte verwalten

15.7.5.1 Felder in diesem Abschnitt

- *Storage-Geräte*: In diesem Feld kann ein Sicherungsgerät gewählt werden, welches verwaltet werden soll.
- *Laufwerk Nummer (falls vorhanden)*: Falls vorhanden, kann hier die Laufwerksnummer angegeben werden. Diese Angabe ist nur für Bandwechsler mit mehreren Laufwerken erforderlich.

15.7.5.2 Aktionen in diesem Abschnitt

- *Einhängen*: Das gewählte Sicherungsgerät wird eingehängt.
- *Aushängen*: Das gewählte Sicherungsgerät wird ausgehängt.
- *Freigeben*: Das gewählte Sicherungsgerät wird freigegeben.
- *Status*: Hier wird der Status des gewählten Geräts abgefragt und in der Ausgabe dargestellt.
- *Slot-Belegung bestimmen*: Wird ein Bandwechsler benutzt, muss mit dieser Aktion nach einem Magazin-Wechsel das System dazu veranlasst werden, die Bänder in den Magazinen zu erkennen. Diese Aktion kann zeitaufwendig sein.
- *Mit Barcodes beschriften*: Wird ein Bandwechsler mit Barcode-Unterstützung benutzt, können mit dieser Aktion die eingelegten Bänder automatisch mit ihrem jeweiligen Barcode beschriftet werden. Der Vorgang entspricht dem Schritt *Beschriften*, wobei für jedes Band der entsprechende Barcode als Name benutzt wird. Im Allgemeinen sollte diese Aktion nur mit neuen Medien durchgeführt werden. Diese Aktion kann zeitaufwendig sein.

15.8 GUI-Referenz: *Datenwiederherstellung*

(Dieser Dialog befindet sich unter *Datensicherung – Datenwiederherstellung*)

In diesem Formular können einzelne Elemente zurückgesichert werden. Zusätzlich können Status- und Detailinformationen einzelner Jobs eingesehen werden.

Im Menü Media können der aktuelle Zustand der verwendeten Sicherungsziel abgerufen werden.

15.8.1 Felder in diesem Formular

- *Hinweis*: Für eine Datenrücksicherung muss eine funktionierende Sicherung durch Zuordnung definiert sein. Ansonsten erscheint ein entsprechende Hinweis.

15.9 GUI-Referenz: *Katalog-Wiederherstellung*

(Dieser Dialog befindet sich unter *Datensicherung – Katalog-Wiederherstellung*)

Das Inhaltsverzeichnis (Katalog) aller Sicherungsdaten ist im Normalbetrieb dem System bekannt. Der Katalog wird für Datenwiederherstellung benutzt und ist in dem Formular *Datensicherung – Datenwiederherstellung* in einer Baumstruktur abgebildet. Wenn alle Daten gesichert werden, wird dieser Katalog üblicherweise ebenso auf einem Ziel gesichert.

Ist der Zustand dieser Informationen auf einem laufenden System

nicht mehr korrekt, kann über dieses Formular der Katalog aus gesicherten Daten auf einem Sicherungsziel wieder hergestellt werden.

Für das Auffinden des auf einem Sicherungsziel gespeicherten Katalogs ist eine Datei BackupCatalog*.bsr erforderlich. Diese wird nach jeder Sicherung dem Administrator per E-Mail zugestellt oder ist, je nach Einstellung, ebenso auf dem Sicherungsziel gespeichert.

15.9.1 Abschnitt *Hinweis*

15.9.1.1 Felder in diesem Abschnitt

- *Hinweis*: Erläutert den Zweck einer Katalog-Wiederherstellung. Auf einem funktionierenden System muss üblicherweise eine Katalog-Wiederherstellung nicht durchgeführt werden.

15.9.2 Abschnitt *Katalog-Wiederherstellung*

15.9.2.1 Felder in diesem Abschnitt

- *Bootstrap-Datei (BackupCatalog_XXX-XXX.bsr)*: Hier wird die Bootstrap-Datei gewählt, die Informationen enthält, wie der Katalog wieder hergestellt werden kann. Die Bootstrap-Datei wird bei erfolgreicher Datensicherung per E-Mail an den Backup-Operator gesendet.
- *Lese Katalog von Sicherungsziel*: Der Katalog (Inhaltverzeichnis aller gesicherten Daten) befindet sich auf einem Sicherungsziel. Hier wird angegeben, von welchem Sicherungsziel der Katalog gelesen und auf dem Server wieder hergestellt werden soll.

15.9.3 Abschnitt *Hinweis*

15.9.3.1 Felder in diesem Abschnitt

- : Statusmeldung des Prozesses.

15.9.4 Abschnitt *Ausgabe*

15.9.4.1 Felder in diesem Abschnitt

- *Ausgabe*: Ausgabe des Prozesses.

15.9.5 Aktionen für dieses Formular

- *Bootstrap-Datei laden*: Die Bootstrap-Datei wird mit dieser Aktion hochgeladen.
- *Zurück*: Beendet die Eingabe ins Formular. Änderungen werden verworfen.

16 Verschiedene Dienste

16.1 *Datum und Zeit*

Eine möglichst exakte Systemzeit ist wichtig, um beispielsweise Logdateien zwischen verschiedenen Servern vergleichen zu können. Daher kann die Systemzeit des Collax Security Gateways über NTP mit Zeitservern abgeglichen werden. Alternativ kann ein DCF77-Funkempfänger angeschlossen werden.

Seine eigene Systemzeit kann der Collax Security Gateway wiederum für andere Systeme per NTP im Netzwerk bereitstellen.

Intern wird die Uhrzeit als GMT, also Greenwich-Standardzeit, gespeichert. Diese wird dann unter Kenntnis des Standorts (Kontinent und Ort) in die lokale Zeit konvertiert; dabei wird auch die Umstellung mit Sommer- und Winterzeit berücksichtigt.

NTP („Network Time Protocol“) wird genutzt, um eine Zeitinformation im Internet zu übertragen. Üblicherweise werden mehrere Server per NTP befragt, da so eine genauere Uhrzeit ermittelt werden kann. Dies ist möglich, da die übertragene Uhrzeit durch die Laufzeit der IP-Pakete verfälscht wird. NTP besitzt Mechanismen, um diesen Fehler zu ermitteln und zu korrigieren. Je mehr Zeitserver zur Verfügung stehen, desto genauer wird die Uhrzeit. Über Internetabgleich ist eine minimale Abweichung von 10 Millisekunden erreichbar.

Eine noch genauere Uhrzeit lässt sich mit einem Empfänger erreichen, der ein von einer zuständigen Einrichtung übertragenes Funksignal auswertet. In Deutschland geschieht dies durch die Physikalisch-Technische Bundesanstalt (PTB), die den DCF77-Sender bei Frankfurt betreibt. Dieses Signal wird von Funkuhren und -Weckern ausgewertet. Es existiert verschiedene Hardware, mit der

ein Computer dieses Signal auswerten kann. Der Collax Security Gateway unterstützt ein solches Gerät zum Anschluss an die serielle Schnittstelle.

16.1.1 GUI-Referenz: Konfiguration

(Dieser Dialog befindet sich unter *Zeit – Konfiguration*)

In diesem Dialog kann die Systemzeit geändert und die Zeitzone angegeben werden. Die Systemzeit kann auch über eine Synchronisationsquelle gesetzt werden.

16.1.1.1 Abschnitt *Zeitzone*

Felder in diesem Abschnitt

- *Kontinent*: Hier wird der Kontinent ausgewählt. Damit wird die Auswahl der Einträge im Feld *Region/Ort* angepasst.
- *Region/Ort*: Hier wird die Region oder ein Ort in der Nähe ausgewählt.

16.1.1.2 Abschnitt *Synchronisationsquelle*

Über eine Synchronisationsquelle kann die Systemuhr automatisch gesetzt werden.

Wird hier die *Systemuhr* ausgewählt, wird ausschließlich die interne Uhr des Systems genutzt. Diese gehen meist allerdings nicht sehr genau. Bei einem Abgleich von Logdateiinformationen sind exakte Uhrzeiten jedoch unerlässlich. Daher sollte eine andere Quelle gewählt werden.

Wenn das System über eine Standleitung ans Internet angeschlossen ist oder im lokalen Netz ein NTP-Server betrieben wird, kann mit „NTP“ die Uhrzeit permanent synchronisiert werden.

Eine andere Möglichkeit ist, einen „DCF-77-Funkempfänger“ an das System anzuschließen und darüber permanent die Uhrzeit zu synchronisieren.

Felder in diesem Abschnitt

- *Typ*: Hier wird die Synchronisationsquelle ausgewählt.
- *Zeitserver*: Wird *NTP* als Quelle ausgewählt, muss hier ein Zeitserver angegeben werden, der über NTP ansprechbar ist.
- *Alternativer Zeitserver*: Hier kann ein zweiter Zeitserver angegeben werden, um eine bessere Qualität der ermittelten Uhrzeit zu erreichen.
- *Empfänger*: In dieser Liste sind alle unterstützten DCF-77-Empfänger aufgelistet.
- *Schnittstelle*: Hier wird die serielle Schnittstelle ausgewählt, an die der Empfänger angeschlossen ist. Es sind nur die Schnittstellen verfügbar, die weder mit serieller Konsole oder Modem noch einer USV belegt sind.
- *Datum*: Wird die interne Hardwareuhr des Rechners als Zeitquelle ausgewählt, kann hier das aktuelle Datum korrigiert werden.
- *Zeit*: Wird die interne Hardwareuhr des Rechners als Zeitquelle ausgewählt, kann hier die aktuelle Zeit korrigiert werden.

16.1.1.3 Aktionen für diesen Dialog

- *Datum/Zeit setzen*: Mit dieser Aktion wird die eingegebene Zeit mit Datum übernommen.

Hinweis: War vorher eine andere Synchronisationsquelle als die Systemuhr eingestellt, muss die Konfiguration zunächst aktiviert werden. Danach sollte die Uhrzeit kontrolliert und gesetzt werden.

16.1.2 GUI-Referenz: *NTP-Server*

(Dieser Dialog befindet sich unter *Serverdienste – NTP – Konfiguration*)

In diesem Dialog wird der NTP-Dienst konfiguriert. Über diesen können andere Systeme ihre Systemzeit abgleichen.

16.1.2.1 Tab *Grundeinstellungen*

Felder in diesem Abschnitt

- *Aktivieren*: Mit dieser Option wird auf diesem System der NTP-Zeitserver aktiviert.

16.1.2.2 Tab *Berechtigungen*

Felder in diesem Abschnitt

- *Zugang zu NTP-Port erlauben für*: Rechner und Netze, die zu einer der aktivierten Gruppen gehören, dürfen den NTP-Dienst abfragen. Für Benutzer in diesen Gruppen hat diese Einstellung keine direkten Auswirkungen.

16.1.2.3 Tab *Optionen*
Felder in diesem Abschnitt

- *Broadcast verwenden*: Wird diese Option aktiviert, sendet der Server seine aktuelle Systemzeit als Broadcast-Nachricht in das lokale Netz.

16.2 Netzwerküberwachung

In jedem Netzwerk ist die automatische Überwachung von wichtigen Komponenten empfohlen, um schnell auf Ausfälle reagieren zu können. Der Collax Security Gateway bietet die Möglichkeit, in ein bestehendes Überwachungssystem eingebunden zu werden. Dazu können mit SNMP („Simple Network Management Protocol“) wichtige Parameter ausgelesen werden. SNMP ist ein verbreitetes und einfaches Protokoll und wird von vielen Managementsystemen unterstützt. Um auf die Daten des Collax Security Gateways zuzugreifen, müssen SNMP aktiviert und die „SNMP-Community“ gesetzt werden.

Der Collax Security Gateway kann auch selbst das umliegende Netzwerk überwachen. Dazu stehen zwei unterschiedliche Mechanismen zur Verfügung. Bei der „passiven Überwachung“ steht mehr der Sicherheitsaspekt im Vordergrund, um neue, fremde Systeme im Netzwerk zu erkennen. Der Collax Security Gateway speichert dabei die IP- und MAC-Adressen aller Systeme, von denen er Datenpakete im Netzwerk „sieht“. Dies beschränkt sich auf die Netzwerksegmente, an die der Collax Security Gateway direkt mit einer Ethernetkarte angeschlossen ist (lokale Netze). Die passive Netzwerküberwachung ist notwendig, damit die Funktion *Hosts importieren* im Collax Security Gateway zur Verfügung steht.

Über die Option *Versende E-Mail bei Änderungen* wird beim Auftauchen von neuen Geräten im Netzwerk eine E-Mail verschickt. Damit werden fremde Geräte im Netzwerk schnell erkannt.

Bei der „aktiven Überwachung“ müssen hingegen die zu überwachenden Systeme vorher bekannt sein. Diese werden dann permanent überprüft und Ausfälle per E-Mail gemeldet.

Die zu überwachenden Systeme werden im Collax Security Gateway als *Hosts* angelegt. Dabei können die verschiedenen Dienste ausgewählt werden, die überwacht werden sollen. So ist es möglich, einen Mailserver zu überwachen, indem permanent die Dienste SMTP, POP3 und IMAP abgefragt werden. Der zu überwachende Server kann im lokalen Netz oder im Internet oder hinter einem VPN-Tunnel stehen. Er muss nur per IP-Adresse erreichbar sein, und der Collax Security Gateway muss auf die zu überwachenden Dienste zugreifen dürfen.

Die aktive Überwachung nutzt der Collax Security Gateway auch intern, um sich selbst zu überwachen und die betroffenen Dienste bei Ausfällen neu zu starten. In solchen Fällen wird keine Alarmierung vorgenommen.

16.2.1 Schritt für Schritt: Host überwachen

- Prüfen Sie, ob unter *Überwachung – Aktiv* die aktive Überwachung eingeschaltet ist. Falls nicht, aktivieren Sie diese.
- Bei einem Ausfall erhalten Sie *3 Meldungen* im *Abstand von 10 Minuten*. Sie können diese Werte auf Ihre Bedürfnisse anpassen.
- Wechseln Sie zu *Netzwerk – DNS – Hosts* und bearbeiten Sie den Host-Eintrag, den Sie überwachen möchten.
- Wenn noch kein Eintrag zu dem Host existiert, legen Sie zunächst einen neuen Eintrag (S. 355) an.
- Wechseln Sie im Host-Eintrag auf den Reiter *Netzwerk-Tests*.

- Hier können Sie verschiedene Tests aktivieren, die auf diesen Host angewendet werden. Um beispielsweise einen Mailserver zu überwachen, aktivieren Sie die Tests für *IMAP*, *POP3* und *SMTP*.
- Über den *Alarmierungszeitraum* können Sie festlegen, wann Alarme ausgelöst werden. Sie können eigene Zeiträume in den *Benutzungsrichtlinien* definieren. So kann die Überwachung von internen Servern auf die Arbeitszeit begrenzt werden.
- Wenn Sie eine komplexe Netzwerkstruktur administrieren, können Sie unter *Erreichbar über* den vorhergehenden Router (aus Sicht des Collax Security Gateways) angeben. Fällt dieser aus, wird für Systeme dahinter kein Alarm ausgelöst. Deren Zustand ist dann „unbestimmt“.
- Wechseln Sie zu den *Benutzungsrichtlinien* und bearbeiten Sie die Gruppe, über die Sie die Überwachungsberechtigung verwalten möchten. Legen Sie ggf. eine neue Gruppe zu diesem Zweck an. In den *Berechtigungen* der Gruppe unter dem Punkt *Monitor* können Sie den Zugriff auf die *aktive Überwachung* gewähren.
- Fügen Sie Benutzer als Mitglieder zu dieser Gruppe hinzu. Diese Benutzer haben nach Aktivierung der Konfiguration Zugriff auf die Nagios-Überwachungskonsole über das User-Webportal und können dort den Status des Netzwerkes einsehen. Diese Benutzer werden zudem bei einem Alarm über E-Mail benachrichtigt, vorausgesetzt, auf dem Collax Security Gateway ist ein E-Mail-System eingerichtet.

16.2.2 GUI-Referenz: *SNMP*

(Dieser Dialog befindet sich unter *Überwachung – SNMP*)

Über SNMP können verschiedene Daten dieses Systems mittels einer geeigneten Software über Netzwerk überwacht und aufgezeichnet werden.

16.2.2.1 Tab *Grundeinstellungen*

Felder in diesem Abschnitt

- *Aktivieren*: Wird diese Option aktiviert, ist der SNMP-Server über das Netzwerk erreichbar. Andernfalls ist das System so konfiguriert, dass nur Verbindungen vom lokalen System zulässig sind.
- *Community zum Lesen*: Hier wird der Name der „Community" für SNMPv1/SNMPv2c angegeben. Die Community ist eine Art Passwort für den Zugriff auf die SNMP-Daten. Der Name der Community wird im Allgemeinen als Klartext übermittelt und bietet daher nur minimalen Schutz.
- *Standort*: Hier kann der Standort des Systems angegeben werden.

16.2.2.2 Tab *Berechtigungen*

Felder in diesem Abschnitt

- *Zugriff auf SNMP-Port erlauben für*: Alle Rechner und Netze, die zu einer der aktivierten Gruppen gehören, bekommen Zugriff auf den SNMP-Dienst. Für Benutzer hat diese Einstellung keine Auswirkungen.

16.2.3 GUI-Referenz: *Netzwerk passiv überwachen*

(Dieser Dialog befindet sich unter *Überwachung – Passiv*)

Die passive Netzwerküberwachung überwacht die Netzwerkschnittstellen nach Datenpaketen und kann so IP-Adressen und MAC-Adressen von Systemen entdecken, die im gleichen Netzwerksegment kommunizieren.

Das Aktivieren dieser Option bietet die Möglichkeit, beim Anlegen von *Hosts* direkt alle Systeme zu importieren. Dabei wird deren jeweilige IP-Adresse und MAC-Adresse automatisch übernommen.

16.2.3.1 Felder in diesem Dialog

- *Aktivieren*: Hier kann die Überwachung aktiviert werden. Dabei werden Pakete auf allen oder gewählten Netzwerkschnittstellen überprüft und die MAC- sowie IP-Adressen der aktiven Computersysteme erkannt.
- *Versende E-Mail*: Mit dieser Option wird der Administrator per E-Mail benachrichtigt, wenn Änderungen im Netzwerk erkannt werden (neue Systeme erscheinen, vorhandene Systeme ändern ihre IP-Nummer, usw.).
- *Alle Ethernet-Links*: Mit dieser Option wird Überwachung auf allen angelegten Verbindungen vom Typs Ethernet aktiviert.
- *Ausgewählte Ethernet-Links*: Hier kann die Überwachung auf bestimmte Ethernet-Links beschränkt werden. Es ist möglich, mehrere Links auszuwählen.

16.2.3.2 Aktionen für diesen Dialog

- *Lösche bislang ermittelte Daten*: Hiermit werden alle bisher ermittelten Daten gelöscht.

  Dies ist nützlich, wenn viele alte oder unwichtige Systeme erkannt und in die Liste aufgenommen wurden.

  Hinweis: Der Collax Security Gateway wird nach dem Löschen sofort weiter Daten ermitteln.

16.2.4 *Fernüberwachung*

(Dieser Dialog befindet sich unter *Überwachung – Fernüberwachung (NRPE)*

In diesem Formular kann die Fernüberwachung des lokalen Servers ermöglicht werden. Technische Basis für die Fernüberwachung ist der NRPE-Dienst, Nagios Remote Plugin Execution. Um die Fernüberwachung in einem geschützten Netzwerk zu ermöglichen, muss darin Zugriff auf Port 5666 gewährt werden. Der Zugriff auf den Collax Server wird im Reiter Berechtigungen erlaubt.

16.2.4.1 Tab *Grundeinstellungen*

Felder in diesem Abschnitt

- *Aktiviert*: Hier wird die Möglichkeit zur Fernüberwachung dieses lokalen Servers eingeschaltet.

16.2.4.2 Tab *Berechtigungen*, Abschnitt *Netzwerkzugang* Felder in diesem Abschnitt

- *NRPE-Port*: Die Rechner der gewählten Netzwerkgruppen dürfen dieses System fernüberwachen. Der Zugriff erfolgt über Port 5666.

16.2.4.3 Aktionen für dieses Formular

- *Schließen*: Bearbeiten des Fernüberwachungs-Zugriff beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten des Fernüberwachungs-Zugriff beenden. Die Änderungen werden gespeichert.

16.2.5 GUI-Referenz: *Aktive Überwachung*

In diesen Dialogen wird die Konfiguration der aktiven Überwachung vorgenommen. Intern verwendet das System dazu *Nagios.* Primär wird Nagios zur Selbstüberwachung des Systems eingesetzt. Es können jedoch auch weitere Systeme im Netz überwacht werden.

In diesem Teil der Konfiguration wird angegeben, ob der aktive Monitor zur Überwachung gestartet werden soll sowie welche Gruppen beim Ausfall eines Dienstes alarmiert werden sollen und Zugang zum Web-Interface erhalten.

Die Konfiguration der einzelnen Hosts und der geprüften Dienste auf jedem Host wird in den Einstellungen des jeweiligen *Hosts* vorgenommen.

16.2.5.1 Tab *Grundeinstellungen*

Felder in diesem Abschnitt

- *Aktivieren*: Hier wird die Netzwerküberwachung der Systemdienste und von entsprechend konfigurierten Rechnern mittels Nagios aktiviert.
- *Anzahl der Meldungen*: Hier kann die Anzahl der Meldungen begrenzt werden, die für einen Vorfall versandt werden.

  Wird hier „1“ angegeben, wird eine E-Mail versandt, wenn ein Dienst oder ein Host ausfällt. Eine weitere E-Mail wird versandt, wenn das Problem behoben wurde.

  Wird ein Wert größer als „1“ angegeben, wird eine E-Mail bei Ausfall versandt und jeweils nach Ablauf des „Alarmintervalls“ eine weitere. Hinweis: Es wird keine E-Mail mehr versandt, wenn das Problem nach der maximalen Anzahl von Meldungen behoben wird.

  Bleibt der Wert leer oder wird eine „0“ angegeben, hängt das Verhalten vom Wert im Feld *Alarmintervall* ab. Wird dort ebenfalls eine „0“ eingetragen, werden keine Meldungen verschickt. Dann wird der Status der überwachten Dienste und Rechner nur in der Nagios-Web-Oberfläche angezeigt. Wird ein Wert größer 0 im Feld *Alarmintervall* angegeben, werden die Fehlermeldungen im angegebenen Intervall wiederholt.
- *Alarmintervall (Minuten)*: Hier wird das Intervall angegeben, in dem ein Alarm wiederholt werden soll. Dieser Wert steht in engem Zusammenhang mit der *Anzahl der Meldungen*.

16.2.5.2 Tab *Berechtigungen*

Felder in diesem Abschnitt

- *Benachrichtigung an Benutzer aus Gruppe*: Für alle aktivierten Benutzergruppen wird ein „contact"-Eintrag in der Nagios-Konfiguration erzeugt; jede aktivierte Gruppe erscheint als „contactgroup". Die Benutzer aus den Gruppen erhalten von Nagios automatisch E-Mail Benachrichtigungen.
- *Zugriff auf aktive Überwachung*: Alle Benutzer, die zu einer der aktivierten Gruppen gehören, bekommen über den URL „https://IP-Adresse:8001/nagios/" oder die Web-Access-Seite Zugriff auf die aktive Überwachung. Rechner und Netze sind von dieser Einstellung nicht betroffen.

16.2.6 *Watchdog-Timer*

Der Watchdog ist ein Timer, der einen Reset auslöst, wenn er abläuft. Im normalen Betriebszustand läuft der Watchdog-Timer nie ab, weil in bestimmten Zeitintervallen das System geprüft wird. Wenn die Datenpartition korrekt beschrieben werden kann, wird der Timer zurückgesetzt. Für diese Art der Systemüberwachung mit Fehlerkorrektur ist entsprechende Hardware erforderlich. Diese Watchdog-Überwachung unterstützt die Hardware des Intel 6300ESB Watchdog Timer.

Wurde ein Reset auf Grund eines schweren Systemfehlers ausgelöst, bleibt der Watchdog-Timer inaktiv, um eine Reset-Schleife zu verhindern. Der Watchdog-Timer kann im Betrieb über den Dialog *System – Überwachung/Auswertung – Status – Dienste* wieder gestartet werden.

16.2.6.1 Abschnitt *Hinweis*

Felder in diesem Abschnitt

- : Um die Watchdog-Überwachung zu aktivieren muss das Gerät Intel 6300ESB Watchdog Timer vorhanden sein.

16.2.6.2 Abschnitt *Einstellungen*

Felder in diesem Abschnitt

- *Aktivieren*: Hier wird die Watchdog-Überwachnung aktiviert.

Aktionen für diesen Abschnitt

- *Abbrechen*: Beendet den Dialog, die Änderungen werden verworfen.
- *Speichern*: Beendet den Dialog, die Änderungen werden gespeichert.

16.3 Server Management mit Spotlight

Collax Spotlight soll helfen den Überblick über mehrere Collax Server zu bewahren, die Administration von mehreren Server zu erleichtern und frühzeitig bei anbahnenden Problemen zu warnen.

Spotlight sammelt Informationen der Spotlight Agenten ein und visualisiert diese innerhalb des Web-Access. Über das Management im Web-Access können verschiedene Detailstufen eingesehen werden.

16.3.1 Schritt für Schritt: Spotlight und Spotlight Agent einrichten

16.3.1.1 Spotlight Server

- Wechseln Sie auf dem Spotlight Server ins Formular *Spotlight – Konfiguration* und aktivieren Sie Spotlight.
- Tragen sie im Feld *Servername* die IP-Adresse oder den DNS-Servernamen ein, den die Spotlight Agenten über das Netzwerk erreichen können.
- Vergeben Sie entsprechenden Benutzern über die Angabe einer Gruppen Berechtigung auf das Spotlight Management. Zusätzlich markieren Sie Gruppen mit Netzwerken, aus denen die Spotlight Agenten Zugriff erhalten sollen.
- Speichern Sie die Einstellungen.
- Laden Sie sich über den Knopf *Download Agent-Konfiguration* eine vorgefertigte Konfiguration für die Spotlight Agenten herunter.
- Aktivieren Sie die Einstellungen
- Wenn Sie den Collax Security Gateway hinter einer Firewall installiert haben, die keine direkten HTTPS-Zugriffe zulässt, muss ein port forwarding eingerichtet werden.

16.3.1.2 Spotlight Agent

- Wechseln Sie auf dem Spotlight Server ins Formular *Spotlight Agent – Konfiguration*.
- Geben Sie im Abschnitt *Upload* die vorweg gespeicherte Konfigurationsdatei ein und laden Sie die Datei hoch.
- Die Einstellungen für die Verbindung sind nun automatisch eingerichtet worden.
- Wechseln Sie auf den Reiter *Informationsbereiche* und wählen Sie

aus, welche Bereiche von Spotlight ausgewertet werden sollen.
- Wechseln Sie auf den Reiter *Kommandos* und definieren Sie, welche Befehle von Spotlight ausgeführt werden dürfen.
- Speichern und aktivieren Sie die Einstellungen. Der Spotlight Agent meldet sich automatisch bei Spotlight an.
- Wechseln Sie nun in den Web-Access.

16.3.2 Erste Schritte im Spotlight Management

Das Management-Interface von Spotlight wird über den Web Access aufgerufen oder kann direkt mit der URL https://spotlightserver/ak/spotlight/ aufgerufen werden. Dort haben Sie die Möglichkeit sich im linken Bereich eine Baumstruktur für die verwalteten Server aufzubauen. Hierzu können Sie per Rechtsklick oder über die Buttons am unteren Rand neue Ordner anlegen.

Im bereits vorhandenen Ordner „unsortiert“ finden Sie alle Server von denen der Spotlight Agent erfolgreich eine Verbindung zu Houston aufbauen konnte. Per Drag&Drop können Sie die Server in die Struktur ziehen.

Setzen Sie nun ein Häkchen in der Box neben einem Server oder einem Ordner. Die markierten Server werden nun im rechten Bereich angezeigt. Mit einem einfachen Klick werden durch Ausklappen weitere Informationen angezeigt.

Mit einem Doppelklick wird für den Server eine neue Registerkarte geöffnet, auf der Sie alle Detailinformationen zu diesem Server finden. Über die Buttons haben Sie die Möglichkeit zu diesem Server einen Kommentar zu hinterlegen oder eine Aufgabe zu definieren, die zu einem bestimmten Zeitpunkt ausgeführt werden soll. Mit dem Button „Start ssh“ können Sie eine ssh-Session über ein Browser-Applett starten. Über den Button „Administrationsoberfläche“ gelangen

Sie direkt zur Konfiguration des ausgewählten Servers. Wenn Sie die Credentials hinterlegt haben („Anmeldeinformationen hinterlegen“), werden Sie in beiden Fällen automatisch angemeldet.

Wenn Sie auf „Add Task“ klicken, erhalten Sie eine Auswahl der Aufgaben, die auf diesem Server durchgeführt werden dürfen. Es dürfen nur Befehle ausgeführt werden, die in der Konfiguration des Spotlight-Agenten explizit erlaubt wurden. Nachdem eine neue Aufgabe festgelegt wurde, erscheint sie in der Tabelle. Wurde die Aufgabe ausgeführt, können Sie hier die Ausgabe des Befehls abrufen. Einen Überblick über alle Aufgaben aller Server finden Sie in der Registerkarte „Aufgaben“.

Über der Baumstruktur finden Sie Filter mit der Sie die Auswahl der angezeigten Server einschränken können. Mit dem Plus-Button können Sie beliebige eigene Filter definieren und benutzen. Ist ein Filter aktiv, was zur Folge hat, dass einige Server in der Übersicht fehlen können, ist der Filter-Button rot. Es können auch mehrere Filter kombiniert werden. Mit dem Besen-Knopf können Sie alle Filter deaktivieren, so dass wieder alle Server angezeigt werden

16.3.3 GUI-Referenz: *Spotlight*

(Dieser Dialog befindet sich unter *Überwachung – Spotlight*

16.3.3.1 Abschnitt *Grundeinstellungen*

Felder in diesem Abschnitt

- *Aktiviert*: Diese Option aktiviert die zentrale Sammlung von Daten von Spotlight Agenten.
- *Servername*: Hier muss eine IP-Adresse oder ein DNS-Server-

namenn des Spotlight-Servers angegeben werden, den die Spotlight-Agenten netzwerktechnisch erreichen können.
- *Berechtigungen*: Spotlight-Agenten aus den gewählten Netzwerkgruppen dürfen auf den Spotlight-Server zugreifen. Zusätzlich erhalten Benutzer und Netzwerke der gewählten Gruppen Zugriff auf die Spotlight Web-Applikation im Collax Web Access.
- : Es erscheint ein Hinweis, falls kein Zertifikat hinterlegt wurde.

Aktionen für diesen Abschnitt

- *Download Agent-Konfiguration*: Um die Einstellungen für die Spotlight-Agenten zu vereinfachen, kann hier die passenden Konfigurationsdatei heruntergeladen werden. Diese kann auf allen Spotlight-Agenten, die über diesen Server verwaltet werden, hochgeladen und benutzt werden.

16.3.3.2 Aktionen für dieses Formular

- *Abbrechen*: Beendet den Dialog, Änderungen werden verworfen.
- *Speichern*: Beendet den Dialog, Änderungen werden gespeichert.

16.3.4 GUI-Referenz: *Spotlight Agent*

(Dieser Dialog befindet sich unter *Überwachung – Spotlight Agent*

16.3.4.1 Tab *Grundeinstellungen*, Abschnitt *Upload*
Aktionen für diesen Abschnitt

- *Upload*: Um die Verbindungskonfiguration zwischen dem Spotlight-Agenten und dem Spotlight-Server zu vereinfachen, kann hier die Konfiguration von Spotlight hochgeladen werden. Die Konfigurationsdatei „ spotlight.token“ enthält entsprechende Zertifikate und die IP-Adresse oder DNS-Namen des Spotlight-Servers.

16.3.4.2 Abschnitt *Grundeinstellungen*
Felder in diesem Abschnitt

- *Aktiviert*: Hier kann der Spotlight-Agent aktiviert werden.
- *Zertifikat*: Dieses Zertifikat wird verwendet, um Daten zwischen dem Spotlight-Server und dem Spotlight-Agenten zu verschlüsseln.
- *IP-Adresse Spotlight-Server*: Hier ist die IP-Adresse anzugeben, unter der der Spotlight-Server von den Spotlight-Agenten aus erreichbar ist.

16.3.4.3 Tab *Informationsbereiche*
Felder in diesem Abschnitt

- *Folgende Informationen übertragen*: Informationen der gewählten Dienste des laufenden Systems können vom Spotlight-Server über den Agenten abgefragt werden.

16.3.4.4 Tab *Kommandos*, Abschnitt *Globale Kommando-Optionen*

Felder in diesem Abschnitt

- *Administrations-GUI und SSH erlauben*: Mit dieser Option wird dem Spotlight-Server erlaubt Verbindungen zur Adminstrationsoberflache und zum SSH-Dienst des Spotlight-Agenten aufzubauen. Ist diese Option aktiviert, muss der Spotlight-Server auf den Ports 8892 und 8895 erreichbar sein.
- *Freie Kommandos erlauben*: Diese Option erlaubt es dem Spotlight-Server beliebige Systemkommandos auf dem Spotlight-Agenten auszuführen und deren Ergebnisse auszuwerten. Aus sicherheitstechnischen Gründen sollte dies nur in einzelnen Fällen erlaubt werden. Alternativ können frei definierbare Kommandos fest hinterlegt werden. Siehe Aktion *Neues Kommando*.

16.3.4.5 Tab *Kommandos*, Abschnitt *Kommando*

Felder in diesem Abschnitt

- *Name*: Zeigt oder deklariert den Namen des definierten Kommandos.
- *Kommando*: Zeigt oder deklariert das Systemkommando.
- *Parameteranzahl*: Zeigt oder definiert die Parameteranzahl des deklarierten Systemkommandos.
- *Kommentar*: Weitere Informationen über das Kommando.
- *Aktiviert*: Definiert, ob das Kommando vom Spotlight-Server ausgeführt werden darf.
- *Name*: Zeigt den Namen des vordefinierten Kommandos.
- *Kommentar*: Zeigt weitere Informationen über das vordefinierte Kommando.
- *Aktiviert*: Definiert, ob das vordefinierte Kommando vom Spotlight-Server ausgeführt werden darf.

Aktionen für diesen Abschnitt

- *Neues Kommando*: Diese Aktion öffnet einen Dialog um ein neues Systemkommando zu definieren. In der Verwaltungs-GUI des Spotlight-Servers wird dieses Kommando in die Liste der ausführbaren Kommandos eingetragen.
- *Löschen*: Diese Aktion löscht ein hinzugefügtes Kommando.

16.3.4.6 Aktionen für dieses Formular

- *Abbrechen*: Beendet den Dialog, die Änderungen werden verworfen.
- *Speichern*: Beendet den Dialog, die Änderungen werden gespeichert.

16.4 USV

16.4.1 GUI-Referenz: *USV-Geräte*

(Dieser Dialog befindet sich unter *USV – USV-Geräte*)

In diesem Dialog können USV-Geräte (Unterbrechungsfreie Stromversorgungen) eingerichtet werden. Das System, das direkt mit der USV kommuniziert, wird als *Master* bezeichnet. Der Status der USV kann über das Netzwerk an andere Systeme (*Clients*) weitergereicht werden, umso bei einem längeren Stromausfall alle Systeme geregelt herunterzufahren.

Bei einem Stromausfall laufen die angeschlossenen Systeme zunächst auf Batteriebetrieb weiter. Wenn der Ladezustand der

Batterien einen kritischen Wert erreicht, schickt der Master den Clients ein Kommando zum Herunterfahren. Anschließend fährt er selbst herunter und sendet als letztes Kommando der USV den Befehl zum Abschalten. Manche USVs können bei Rückkehr des Stroms eine Zeitlang warten und die Batterien bis über die kritische Grenze laden, bevor sie die Systeme wieder einschalten. Dann kann ein zweiter folgender Stromausfall ebenfalls abgefangen werden.

Weitere Informationen zur Technik und möglichen Anschlussstrategien sind auf der Projektseite dieser Software zu finden: <http://www.networkupstools.org/>.

Eine Kompatibilitätsliste ist unter dieser Adresse abrufbar: <http://www.networkupstools.org/stable-hcl.html>.

16.4.1.1 *Geräte*

(Dieser Dialog befindet sich unter *USV – USV-Geräte*)

Felder in diesem Dialog

- *Name*: Hier wird der Name der USV angezeigt.
- *Kommentar*: Hier steht der Kommentartext zu der USV.
- *Netzwerk*: Hier wird angezeigt, ob es sich um eine „Netzwerk-USV“ handelt. Eine solche USV ist nicht direkt angeschlossen, sondern der Status wird von einem anderen System über das Netzwerk erfragt (vorausgesetzt, der Switch ist auch an einer USV angeschlossen).
- *Master*: Für jede USV muss im Netzwerk ein Master existieren, der die Kommunikation mit der USV übernimmt.
- *Versorgt dieses System*: Hier wird angezeigt, ob auf einen Stromausfall reagiert wird.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion werden die Einstellungen der USV bearbeitet.
- *Löschen*: Mit dieser Aktion wird die USV gelöscht.

Aktionen für diesen Dialog

- *Suche USB-USV*: Mit dieser Aktion kann nach, an USB angeschlossenen, USV-Geräten gesucht werden.
- *USV anlegen (seriell, NUT)*: Mit dieser Aktion wird eine neue USV angelegt.

16.4.1.2 *Bearbeiten*

(Dieser Dialog befindet sich unter *USV – USV-Geräte*)

Felder in diesem Dialog

- *Name*: Hier wird der Name der USV angegeben.
- *Kommentar*: Hier kann ein Kommentartext zur USV eingegeben werden.
- *Diese USV steuern*: Wenn die USV lokal angeschlossen ist, kann das System als *Master* mit der USV kommunizieren. Dann muss das Modell und die Schnittstelle der USV ausgewählt werden.
- *Versorgt dieses System*: Wird diese Option aktiviert, wird die USV beobachtet und es wird auf einen Ausfall der USV reagiert. Das deaktivieren dieser Option ist hilfreich, wenn die Stromversorgung des Systems nicht an die USV angeschlossen ist. Das deaktivieren dieser Option ist nur bei über Netzwerk abfragbaren USVs möglich.

- *Über Netzwerk abfragen*: Wird diese Option aktiviert, kann die USV über das Netzwerk abgefragt werden. Dazu muss auf der USV oder dem entsprechenden Steuerungssystem ein *Nut-USV-Daemon* ab Version 1.1.0 laufen.
- *Rechner*: Der Hostname oder die IP-Adresse des Rechners, an dem die USV angeschlossen ist.
- *Name der entfernten USV*: Wenn mehrere USVs angesteuert werden, kann hier ein Name als Identifikator hinterlegt werden. Damit können die USV-Geräte besser unterschieden werden.
- *Login*: Der Benutzername, der zur Authentifizierung gesendet wird.
- *Passwort*: Das Passwort zur Authentifizierung.
- *Klicken Sie, um herauszufinden welchen Treiber die USV benötigt*: Hier werden Sie auf eine externe Seite weitergeleitet, auf der Sie herausfinden können welchen Treiber die USV benötigt.
- *Verwendeter Treiber*: Hier wird der verwendete Treiber angezeigt.
- *Anschluss*: Hier wird der Port ausgewählt, an dem die USV angeschlossen ist, z. B. die erste serielle Schnittstelle COM1 (ttyS0). Die serielle Schnittstelle muss hierzu unter *Hardware* für die Verwendung *Sonstiges* konfiguriert sein.

16.4.2 GUI-Referenz: *USV-Benutzer*

(Dieser Dialog befindet sich unter *USV – USV-Benutzer*)

In diesem Dialog werden Benutzeraccounts verwaltet, die den USV-Status abfragen dürfen. Dabei handelt es sich nicht um vollwertige Benutzerkonten. Normale Benutzer können die USV nicht abfragen.

16.4.2.1 *USV-Benutzer wählen*

(Dieser Dialog befindet sich unter *USV – USV-Benutzer*)

Felder in diesem Dialog

- *Benutzer*: Der Name des USV-Benutzers.
- *Beschreibung*: Hier wird der Kommentartext zum Benutzer angezeigt.
- *Erlaube Master*: Hier wird angezeigt, ob der Benutzer die Berechtigung hat, als *Master* zu arbeiten.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird der ausgewählte USV-Benutzeraccount bearbeitet.
- *Löschen*: Mit dieser Aktion wird der angelegte Benutzeraccount gelöscht.

Aktionen für diesen Dialog

- *Anlegen*: Mit dieser Aktion wird ein neues USV-Benutzerkonto angelegt.

16.4.2.2 *USV-Benutzer bearbeiten*

(Dieser Dialog befindet sich unter *USV – USV-Benutzer*)

Felder in diesem Dialog

- *Name*: Hier wird der Name des USV-Benutzers eingegeben. Es handelt sich hierbei nicht um vollwertige Benutzeraccounts, sondern um eine Kombination aus Login und Passwort zur Authentifizierung am USV-Monitor-Dienst.
- *Name*: Hier wird der Name des USV-Benutzers angezeigt. Wird ein bestehendes Nutzerprofil bearbeitet, kann der Name nicht geändert werden.
- *Kommentar*: Hier kann ein Kommentartext zum Benutzer eingegeben werden.
- *Passwort*: Hier wird das Passwort für den Benutzer gesetzt.
- *Passwort (Wiederholung)*: Da das Passwort aus Sicherheitsgründen bei der Eingabe nicht lesbar ist, muss es hier wiederholt werden.
- *Darf die USV steuern*: Diese Option erlaubt dem Benutzer, Master einer USV zu sein. Ein Rechner pro USV muss immer Master sein. Es kann nur einen Master für eine USV geben. Der Master übernimmt Steueraufgaben bei der Koordination der Shutdowns und ist zudem derjenige, der USV-Steuerkommandos absenden darf (instcmd). Sinnvollerweise wird der Master auf dem System eingerichtet, welches direkt mit der USV verbunden ist.

16.4.3 *USV-Dienst*

In diesem Formular kann die Zugriffsberechtigung auf den USV-Verwaltungsdienst für Netzwerkgruppen gesetzt werden. Ein Zugriff auf den USV-Dienst ist dann sinnvoll, wenn am Server eine USV lokal angeschlossen ist und wenn die Information eines Stromausfalls an andere Rechner im Netzwerk weitergegeben werden soll.

16.4.3.1 Felder in diesem Formular

- *NUT-Port*: Mit dieser Berechtigung wird der entsprechende Firewall-Port geöffnet. Hosts in den aktivierten Netzwerkgruppen dürfen dann auf den USV-Dienst zugreifen. Der Zugriff ist über das Network UPS Tool (NUT) oder einfach über weitere Collax Server möglich.

  Zugriff auf den USV-Dienst ist dann möglich, wenn mindestens ein USV-Gerät an einem seriellen oder an einem USB-Anschluss konfiguriert ist.

16.4.3.2 Aktionen für dieses Formular

- *Schließen*: Bearbeiten des USV-Dienstes beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten des USV-Dienstes beenden. Die Änderungen werden gespeichert.

17 Lizenzierung, Update und Softwaremodule

17.1 Lizenz

Die Lizenz eines Collax Security Gateway legt fest, wie viele Benutzeraccounts, Netzwerklinks und Maildomains maximal verwendet werden dürfen. Lizenzen ohne Beschränkungen sind dabei ebenfalls erhältlich.

Die Lizenz wird in Form einen Lizenzcodes geliefert und muss in der Weboberfläche eingegeben werden. Nach Eingabe des Lizenzcodes wird die Lizenz online geprüft und im Anschluss auf dem Collax Security Gateway freigeschaltet.

Eine Lizenz ist immer mit der Subscription kombiniert. Diese berechtigt innerhalb der Laufzeit zum Zugriff auf den Updateserver, um Softwareaktualisierungen durchzuführen und zusätzliche Softwaremodule zu installieren.

Ein nicht registriertes System erlaubt nur eine minimale Anzahl von Benutzern und Netzwerklinks. Damit ist es möglich, eine Internetverbindung aufzubauen und die Registrierung durchzuführen.

In der Weboberfläche wird die aktuell zulässige sowie die bereits genutze Anzahl angezeigt. Bei Änderungen an der Lizenz muss ggf. der Lizenzstatus online aktualisiert werden, um die korrekte Ausgabe zu erhalten. Über das Collax Web Account kann eine Übersicht über die einzelnen Lizenzen abgefragt werden, etwa die Laufzeit. Bei der Lizenzaktivierung können mehrere Systeme unter einem Account in Collax Web Account aufgenommen werden.

17.1.1 GUI-Referenz: *Lizenzen und Module*

(Dieser Dialog befindet sich unter *System – Systembetrieb – Software – Lizenzen und Module*)

17.1.1.1 Tab *Status*, Abschnitt *Systemlizenz*

Felder in diesem Abschnitt

- *Unregistriert*: Dieser Informationstext weist darauf hin, dass das System noch nicht registriert ist. Damit ist es nicht möglich, Updates durchzuführen oder weitere Softwaremodule zu installieren.
- *Lizenznummer*: Hier wird die auf diesem System verwendete Lizenznummer angezeigt.
- *Collax Web Account*: Dieser Link verweist direkt in das Collax Web Account. Dort sind weitere Informationen zu der Lizenz abrufbar, etwa über die Laufzeit.
- *Support-Übersicht und Dokumente*: Dieser Link verweist auf die Supportinformationen auf der Collax-Website. Hier sind u. a. die Release-Notes zu den einzelnen Versionsständen abrufbar.
- *Lizenzstatus ungültig*: Dieser Text wird angezeigt, wenn eine ungültige Lizenz für das System vorliegt.

Dieses System ist nicht registriert. Bitte registrieren Sie zuerst Ihre Software, um alle Funktionen nutzen zu können.

Solange das System unregistriert ist, gelten die unten dargestellten Limitierungen.

Diese Lizenz ist nur für nichtkommerziellen Einsatz zugelassen.

Sie haben die Möglichkeit, die Lizenz dieser Maschine zu löschen, um eine neue Lizenz zu registrieren. Drücken Sie dazu den Knopf „Lizenz freigeben“.

Lizenzen können nur einmal registriert werden. Damit sie ein weiteres Mal verwendet werden können, müssen sie vom Collax-Support freigeschaltet werden. Dies dient zu Ihrem Schutz, damit Dritte Ihre Lizenz nicht ebenfalls verwenden können.

Geben Sie Lizenzen nur frei, wenn es erforderlich ist.

Diese Lizenz ist nur für Händler zugelassen und darf nicht weiterverkauft werden.

17.1.1.2 Tab *Status*, Abschnitt *Nur für nichtkommerzielle Nutzung*

Felder in diesem Abschnitt

- *Hinweis*: Bei der Verwendung einer Lizenz für nichtkommerzielle, private Nutzung wird dieser Hinweistext angezeigt.

17.1.1.3 Tab *Status*, Abschnitt *Nicht für Wiederverkauf*

Felder in diesem Abschnitt

- *Not for resale*: Bei einer Lizenz, die nicht für den Wiederverkauf bestimmt ist, wird dieser Hinweistext angezeigt.

17.1.1.4 Tab *Status*, Abschnitt *Berechtigungen*

In dieser Übersicht wird die derzeit benutzte und die erlaubte Anzahl von Benutzerkonten, Netzwerklinks, E-Maildomains von Modulen und Funktionen dargestellt.

Kann die benutzte Anzahl nicht genau ermittelt werden, weil beispielsweise der Collax Security Gateway als Mail-Relayserver eingesetzt wird und daher die Benutzer auf einem nachgeschalteten

Mailserver verwaltet werden, wird der Wert „Externe Benutzer“ angezeigt.

Spalten in der Tabelle

- *Limit*: In dieser Spalte werden die einzelnen Objekte bzw. Module aufgelistet, für die Beschränkungen existieren.
- *Benutzt*: In dieser Spalte wird für jedes Objekt die vom System ermittelte Anzahl aktuell genutzter Berechtigungen angezeigt.
- *Erlaubt*: In dieser Spalte wird die durch die Lizenz maximal zulässige Anzahl von Berechtigungen für das jeweilige Objekt angezeigt.

17.1.1.5 Tab *Status*, Abschnitt *Zusatzmodule*

In dieser Tabelle werden die verfügbaren Zusatzmodule angezeigt. Für jedes Modul wird aufgelistet, welcher Lizenz es unterliegt und ob es auf dem Collax Security Gateway bereits installiert ist.

Spalten in der Tabelle

- *Paket*: In dieser Spalte wird die Bezeichnung des Softwaremoduls ausgegeben.
- *Beschreibung*: Hier wird eine kurze Beschreibung zu jedem Modul angezeigt, die den genauen Einsatzzweck erläutert.
- *Status*: In dieser Spalte wird angezeigt, ob das Modul bereits installiert ist oder nicht.
- *Lizenz*: Hier wird der Lizenztyp des jeweiligen Softwaremoduls angezeigt. Es gibt kostenlose Module, für die keine weitere Lizenz erworben werden muss, kostenpflichtige Module, für die ein Ak-

tivierungsschlüssel erworben werden muss, und kostenpflichtige Module, für die eine Hersteller-Lizenz erhältlich ist.

Eine solche Hersteller-Lizenz ist eine Lizenzdatei, die im Gegensatz zu den hier verwalteten Lizenzschlüsseln in der Weboberfläche bei der Konfiguration des Softwaremoduls selbst eingespielt wird.

Aktionen für jeden Tabelleneintrag

- *Installieren*: Mit dieser Aktion wird das Softwaremodul installiert. Dabei werden entsprechende Pakete vom Updateserver heruntergeladen und in das System integriert.

  Eine Installation kann im Regelfall dann erfolgen, wenn das betreffende Produkt oder Zusatzmodul mit einem Lizenzschlüssel aktiviert wurde.
- *Entfernen*: Mit dieser Aktion wird ein Softwaremodul wieder aus dem System entfernt.

17.1.1.6 Tab *Lizenz-Verwaltung*, Abschnitt *Zusätzliche Lizenzen*

Felder in diesem Abschnitt

- *Zusätzliche Lizenzen*: Um weitere Benutzer oder zusätzliche Softwaremodule zu lizenzieren, können hier weitere Lizenzen dem System hinzugefügt werden.
- *Lizenzschlüssel*: In diesem Feld muss der Aktivierungsschlüssel angegeben werden.

Aktionen für diesen Abschnitt

- *Aktivieren*: Mit dieser Aktion wird der Aktivierungsschlüssel in das System übernommen und online überprüft.

17.1.1.7 Tab *Lizenz-Verwaltung*, Abschnitt *Lizenz freigeben*

Felder in diesem Abschnitt

- *Lizenz freigeben*: Bei einem Wechsel der Lizenz oder bei einem Verkauf des Systems oder aus sonstigem Grund kann die Lizenz auf dieser Seite von dem System entfernt werden.

  Nach diesem Vorgang ist der Collax Security Gateway bezüglich der Lizenzierung wieder im Auslieferungszustand, d. h., er ist eine lizenzlose, unregistrierte, im Funktionsumfang eingeschränkte Testversion.

Aktionen für diesen Abschnitt

- *Lizenz freigeben*: Mit dieser Aktion wird die Lizenz freigegeben.

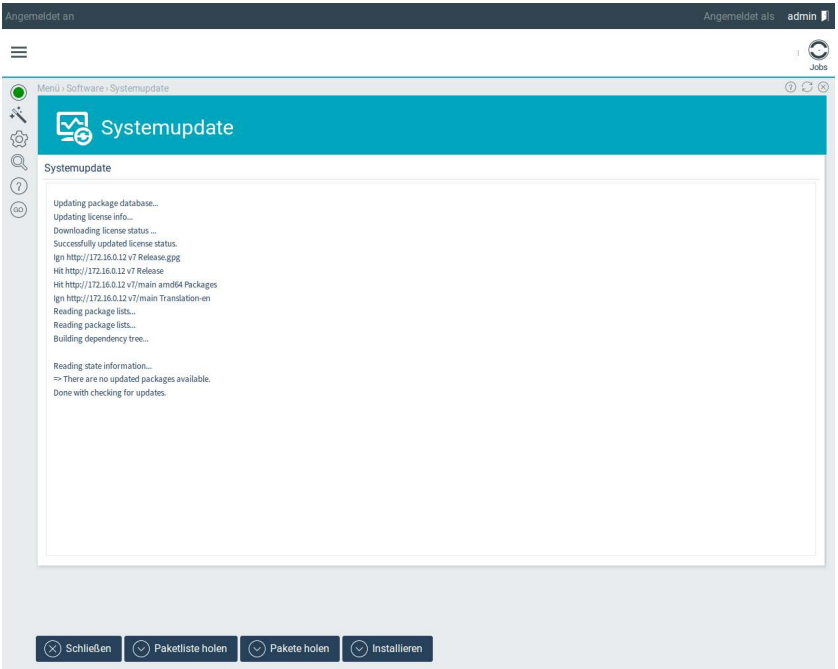
17.1.1.8 Aktionen für dieses Formular

- *Zurück*: Diese Aktion führt zurück zur Hauptansicht.
- *Lizenzstatus aktualisieren*: Mit dieser Aktion wird der angezeigte Lizenzstatus mit dem Registrierungsserver abgeglichen. Dies kann in seltenen Fällen notwendig sein, wenn Änderungen an der Lizenz durchgeführt wurden.

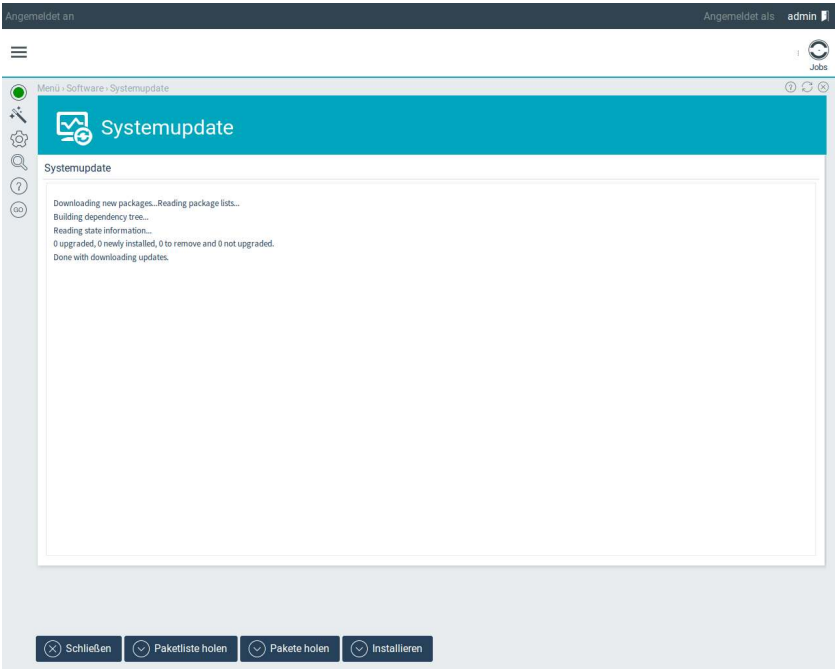
17.2 Systemsoftware

17.2.1 Schritt für Schritt: System aktualisieren

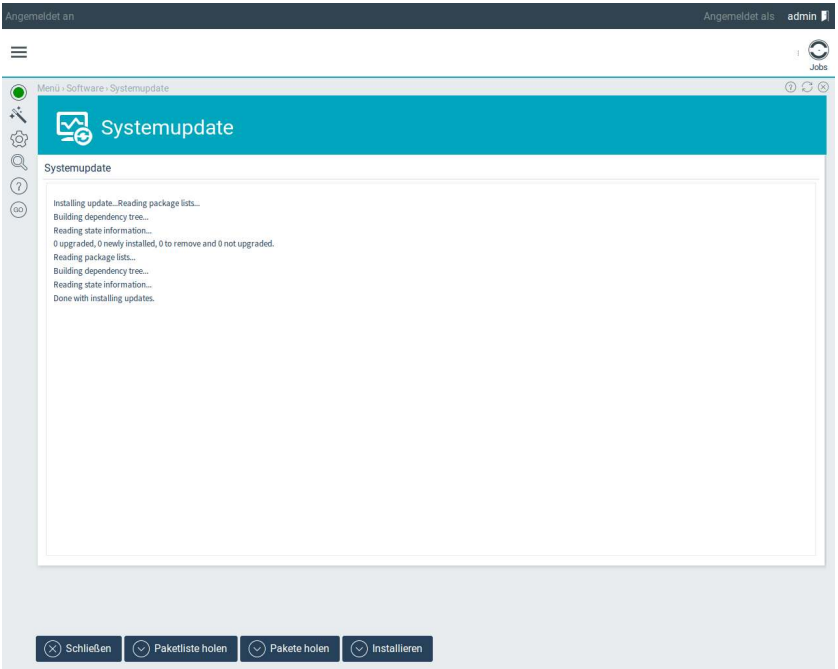
- Wechseln Sie auf den Reiter *System* links vom Hauptmenü.
- Rufen Sie dort unter *Systembetrieb – Software* die Seite *Systemupdate* auf.
- Am unteren Rand sind drei Schalter. Klicken Sie auf *Paketliste holen*. Nun wird die aktuelle Paketliste vom Update-Server heruntergeladen.
- Wenn Sie den Collax Security Gateway hinter einer Firewall installiert haben, die keine direkten HTTPS-Zugriffe nach außen lässt, müssen Sie unter *Einstellungen – Systembetrieb – Softwareupdate – Konfiguration* einen *Proxy-Server* einstellen.



- Während des Ladens der Paketliste erscheint eine Animation. Wenn Sie auf die Animation klicken, sehen Sie ein Terminalfenster mit detaillierteren Ausgaben.
- Wenn auf dem Update-Server neue Pakete vorhanden sind, sehen Sie eine Zeile diesen oder ähnlichen Inhalts: *25 packages upgraded, 1 newly installed, 0 to remove and 0 not upgraded*. Hier werden 25 Pakete aktualisiert und ein neues Paket wird dem System hinzugefügt.



- Um den Download der Pakete zu starten, klicken Sie auf *Pakete holen*.



- Durch *Installieren* starten Sie die Installation der heruntergeladenen Pakete.
- Auch hier können Sie das Terminalfenster für eine detaillierte Ausgabe öffnen. In diesem Fall wird durch das Update der Kernel ausgetauscht, dazu muss der Collax Security Gateway neu gestartet werden. Ein entsprechender Hinweis findet sich am Ende der Ausgabe.

17.2.2 GUI-Referenz: *Systemupdate*

(Dieser Dialog befindet sich unter *Systembetrieb – Software – Systemupdate*)

In diesem Dialog werden Softwareupdates heruntergeladen und installiert. Die Updates werden von einem Update-Server heruntergeladen, dazu muss das System registriert sein und über einen gültigen Subscriptionvertrag verfügen. Releasenotes und weitere Hinweise zu den Updates sind auf der Webseite des Herstellers verfügbar.

Beim Download von Dateien wird das HTTPS-Zertifikat des Update-Servers überprüft. Dadurch wird gewährleistet, dass die Updates nicht durch Dritte verfälscht wurden.

17.2.2.1 Felder in diesem Dialog

- *Release-Notes*: Neuerungen und Änderungen eines Systemupdates sind für Collax-Server in Release-Notes festgehalten. An dieser Stelle können die aktuellen Release-Notes eingesehen werden.
- *Ausgabe*: In diesem Feld werden die Ausgaben der Updateaktionen angezeigt. Es sollte auf jeden Fall bis zur Ausgabe der Zeile *done* abgewartet werden, bevor weitere Konfigurationen o. ä. vorgenommen werden.

17.2.2.2 Aktionen für diesen Dialog

- *Paketliste holen*: Hier wird eine aktuelle Paketliste vom Updateserver heruntergeladen. Sind neue Pakete auf dem Server verfügbar, wird dies mit ausgegeben.
- *Pakete holen*: Hier wird der Download der aktualisierten Pakete gestartet. Im Anschluss wird keine Installation durchgeführt.

- *Installieren*: Hier wird die Installation der Pakete gestartet. Wurden vorher keine Pakete heruntergeladen, wird zunächst der Download durchgeführt.

17.2.3 GUI-Referenz: *Manueller Upload*

(Dieser Dialog befindet sich unter *Systembetrieb – Software – Manueller Upload*)

In seltenen Fällen besteht die Möglichkeit, spezielle Updatedateien manuell einzuspielen. Pakete aus nicht vertrauenswürdigen Quellen können die Integrität des Systems gefährden. Hier sollten also nur Pakete in Absprache mit dem Support des Herstellers eingespielt werden.

17.2.3.1 Felder in diesem Dialog

- *Datei*: Hier wird die Datei ausgewählt, die eingespielt werden soll. Es muss sich dabei um ein gültiges Collax Security Gateway-Softwarepaket handeln.
- *Ergebnis*: Nach der Installation werden hier die Ausgaben der Installation angezeigt.

17.2.3.2 Aktionen für diesen Dialog

- *Update einspielen*: Mit dieser Aktion wird der Upload gestartet.

17.2.4 *Endbenutzer-Lizenzvertrag*

(Dieser Dialog befindet sich unter *Systembetrieb – Software – Endbenutzer-Lizenzvertrag*)

In diesem Formular wird der Endbenutzer-Lizenzvertrag der erworbenen Software angezeigt.

17.2.5 *Registrierung des Servers*

(Dieser Dialog befindet sich unter *System – Systembetrieb – Software – Registrierung*)

Mit Hilfe dieses Assistenten wird der Collax Security Gateway registriert. Dieser Assistent gleicht die beim Hersteller hinterlegten Daten des Fachhandelspartner ab und bietet die Möglichkeit diese Daten falls erforderlich, zu korrigieren.

17.2.5.1 Ablauf

Im ersten Schritt wird die Erreichbarkeit des Collax Lizenzierungs-Server getestet. Anschließend kann die erhaltene Lizenznummer eingegeben werden.

Nachfolgend werden die hinterlegten Daten des Fachhandelspartner zur Überprüfung angezeigt. Änderungen können vorgenommen werden. Im Anschluss werden die Endbenutzerdaten zur Kontrolle angezeigt.

Handelt es sich bei der eingetragenen Lizenz um eine NFR-Lizenz (nicht für den Wiederverkauf bestimmt), kann die Registrierung fertiggestellt werden. Wird eine Lizenz für die private Nutzung registriert, entfällt die Anzeige des Fachhandelspartner. Es werden nur die Endbenutzerdaten angezeigt.

Der Server wird nach der Zusammenfassung registriert. Durch die Registrierung kann die Software-Update-Funktionen des Servers und der registrierten Software-Module für die Dauer der Laufzeit genutzt werden. Detailinformationen über die Lizenz können über das Collax Web Account unter http://www.collax.com abgerufen werden

17.3 Anwendungen

Sie können auf dem Collax Security Gateway Anwendungen anderer Hersteller installieren. Dazu benötigen Sie ein *Anwendungs-Cabinet*; dies ist eine Datei, die Sie über den jeweiligen Hersteller beziehen können. Sie enthält neben einer allgemeinen Beschreibung des Produktes technische Informationen darüber, welche Schritte der Collax Security Gateway zum Installieren der Anwendung ausführen muss und von woher das System Updates beziehen kann. Das Anwendungs-Cabinet speichern Sie zunächst auf Ihrer Workstation. Von dort aus können Sie es auf den Collax Security Gateway hochladen.

Normalerweise enthält das Anwendungs-Cabinet jedoch nicht die Pakete, aus denen die eigentliche Software besteht. Diese werden vom Collax Security Gateway stattdessen von den Updateservern anhand der in der Cabinet-Datei enthaltenen Informationen heruntergeladen und anschließend direkt installiert. Das gilt auch für weitere Pakete, die aufgrund von Abhängigkeiten der Anwendung nachinstalliert werden müssen. Daher muss der Collax Security Gateway während der Installation normalerweise eine funktionsfähige Verbindung ins Internet haben. Für Spezialfälle kann ein Anwendungs-Cabinet jedoch auch direkt die Pakete enthalten; kontaktieren Sie diesbezüglich den Hersteller.

Zum Installieren eines Anwendungs-Cabinets folgen Sie der Anleitung (S. 605).

Ein Update des Systems (S. 597) bezieht im Regelfall ein Update der installierten Anwendungen mit ein. Ob und wann solche Updates für die bei Ihnen installierten Anwendungen zur Verfügung stehen, erfahren Sie beim jeweiligen Hersteller.

17.3.1 Schritt für Schritt: Anwendungen verschiedener Hersteller installieren

- Voraussetzung ist, dass Sie ein Anwendungs-Cabinet vom Hersteller erhalten und auf Ihrer Workstation abgespeichert haben.
- Wechseln Sie auf den Reiter *System* links vom Hauptmenü.
- Rufen Sie dort unter *Systembetrieb – Software* die Seite *Anwendungen* auf.
- Klicken Sie auf *Ein Anwendungs-Cabinet installieren*.
- Wählen Sie das Anwendungs-Cabinet, das sie installieren wollen, mit Hilfe von *Browse* aus und klicken Sie anschließend auf *Upload*.
- Nach dem Hochladen sehen Sie Informationen über die in der Cabinet-Datei enthaltene Anwendung: den Namen des Herstellers, die Bezeichnung des Produkts und eine Beschreibung. Vergewissern Sie sich, dass dies tatsächlich die Anwendung ist, die Sie installieren wollen.
- Um die Anwendung zu installieren, klicken Sie auf *Installieren*. Nach erfolgreich durchgeführter Installation wird die Anwendung im Dialog *Anwendungen* aufgelistet.
- Wo sich die soeben installierte Anwendung im Hauptmenü befindet und wie sie konfiguriert wird, entnehmen Sie der dazugehörigen Dokumentation. Diese ist über das Hilfesymbol (Fragezeichen) auf der rechten Seite der dunkelblauen Leiste oberhalb des Hauptmenüs erreichbar. Wählen Sie über den

Menübaum der Online-Dokumentation den zur Anwendung gehörenden Eintrag aus und folgen Sie den entsprechenden Anweisungen.

17.3.2 GUI-Referenz: *Anwendungen*

(Dieser Dialog befindet sich unter *Systembetrieb* – *Software* – *Anwendungen*)

17.3.2.1 Abschnitt*Installierte Anwendungen*

Spalten in der Tabelle

- *Hersteller*: Hier wird der Hersteller der Anwendung angezeigt.
- *Produkt*: Hier wird der Produktname der Anwendung angezeigt.
- *Beschreibung*: Hier erscheint ein Kurzbeschreibung der Anwendung.

Aktionen für jeden Tabelleneintrag

- *Entfernen*: Hier kann eine Anwendung deinstalliert werden.

Aktionen für diesen Abschnitt

- *Ein Anwendungs-Cabinet installieren*: Mit dieser Aktion wird in das Formular gewechselt, in dem Anwendungs-Cabinet-Dateien installiert werden können.

17.3.2.2 Abschnitt*Ausgabe*
Felder in diesem Abschnitt

- : In diesem Fenster erscheint die Ausgabe der durchgeführten Aktion. Ansonsten ist das Fenster nicht sichtbar.

17.3.2.3 Aktionen für dieses Formular

- *Zurück*: Diese Aktion führt zurück ins Hauptformular.

17.3.3 GUI-Referenz: *Anwendung installieren*

(Dieser Dialog befindet sich unter *Systembetrieb – Software – Anwendungen installieren*)

17.3.3.1 Abschnitt*Anwendungs-Cabinet installieren*
Felder in diesem Abschnitt

- *Hersteller*: Wurde eine Anwendungs-Cabinet-Datei hochgeladen, wird hier der Hersteller angezeigt.
- *Produkt*: Nach dem Hochladen der Anwendungs-Cabinet-Datei wird hier der Name des Produktes angezeigt.
- *Beschreibung*: Hier wird die Beschreibung der Anwendung angezeigt.

17.3.3.2 Abschnitt*Ausgabe*
Felder in diesem Abschnitt

- *Ausgabe*: In diesem Fenster erscheint die Ausgabe der durchgeführten Aktion. Ansonsten ist das Fenster nicht sichtbar.

17.3.3.3 Aktionen für dieses Formular

- *Upload*: Mit dieser Aktion wird die über *Browse* ausgewählte Datei auf den Collax Security Gateway hochgeladen.
- *Installieren*: Wurde eine Cabinet-Datei hochgeladen, kann die Anwendung anschließend über diese Aktion installiert werden.
- *Zurück*: Diese Aktion führt zurück ins Hauptformular.

17.4 GUI-Referenz: *Update-Konfiguration*

(Dieser Dialog befindet sich unter *Softwareupdate – Konfiguration*)

In diesem Dialog kann ein Proxy für den Download von Systemupdates konfiguriert werden. Dies kann notwendig sein, wenn der Collax Security Gateway hinter einer Firewall betrieben wird und keine direkte Internetverbindung aufbauen kann. Der Proxyserver muss allerdings HTTPS unterstützen.

17.4.1 Felder in diesem Dialog

- *Proxy für Updates benutzen*: Durch das Aktivieren dieser Option werden Updates über einen Proxyserver heruntergeladen.
- *Typ des Proxys*: Da die Verbindung zum Updateserver verschlüsselt ist, sollte hier bei Verwendung eines zwischengeschaltetem Proxy, das Systemupdate mittels CONNECT-Methode angefordert werden. Falls diese Methode nicht zum Erfolg führt, weil der Proxy diese nicht unterstützt, kann hier optional auch die GET-Methode verwendet werden.
- *Proxy*: Hier wird der Hostname oder die IP-Adresse des Proxyservers angegeben, der verwendet werden soll.
- *Proxy-Port*: Der Port des Proxyservers muss hier angegeben werden. Ein Standard-Squid-Proxy benutzt meist den Port 3128.
- *Proxy-Authentifizierung benutzen*: Falls der Proxy einen Benutzernamen und ein Passwort zur Authentifizierung verlangt, muss diese Option aktiviert werden.
- *Proxy-Benutzername*: Hier wird der Benutzername zur Nutzung des Proxyservers angegeben.
- *Proxy-Passwort*: Hier wird das zugehörige Passwort angegeben.

18 Systembetrieb

18.1 GUI-Referenz: *Netzwerk-Tools*

(Dieser Dialog befindet sich unter *Systembetrieb – Werkzeugkasten – Netzwerk-Tools*)

Der Werkzeugkasten bietet die Möglichkeit, vom Collax Security Gateway aus verschiedene Netzwerktests durchzuführen. Hier können DNS-Anfragen durchgeführt, Ping-Anfragen verschickt und Routen untersucht werden.

18.1.1 Abschnitt *Netzwerktest*

18.1.1.1 Felder in diesem Abschnitt

- *Name oder IP-Adresse*: Hier wird die IP-Adresse oder der Host- bzw. Domainname angegeben, der abgefragt und überprüft werden soll.
- *Aktion*: Hier wird die Aktion ausgewählt, die für die Adresse bzw. den Namen durchgeführt werden soll. Es können mehrere Aktionen ausgewählt werden, diese werden nacheinander durchgeführt.

  Die Aktion *dns* befragt einen DNS-Server nach dem angegebenen Namen oder der Adresse. Welche Informationen abgefragt werden und welcher DNS-Server befragt wird, kann angegeben werden, wenn die *dns*-Option aktiviert wurde.

  Mit der Aktion *whois* kann abgefragt werden, wem eine Internetdomain oder eine IP-Adresse gehört. Leider funktioniert der Dienst nicht (mehr) mit allen Top-Level-Domains, insbesondere

nicht mit Namen unterhalb von „.de“. Hier wurde die Veröffentlichung der Informationen aus Datenschutzgründen eingestellt.

Die Aktion *route* ermittelt, über welchen Link ein Zielrechner derzeit erreicht werden könnte. Diese Aktion nutzt die Routingtabellen des Systems, es werden keine Daten verschickt. Wenn hier ein Name eingegeben wurde, muss dieser Name zunächst per DNS-Anfrage in eine IP-Adresse aufgelöst werden. Ist der DNS-Server nicht erreichbar oder nicht konfiguriert, kann die Route nicht ermittelt werden.

Die Aktion *ping* sendet ICMP Echo-Request-Pakete an den Zielrechner und prüft, ob und mit welcher Laufzeit ICMP Echo-Reply-Pakete empfangen werden. Wenn als Ziel ein Hostname angegeben wird, muss der Name zuerst auf eine IP-Adresse aufgelöst werden. Ist der DNS-Server nicht erreichbar oder nicht konfiguriert, kann das Ping nicht verschickt werden.

- *Frage DNS nach*: Wird *dns* als Aktion ausgewählt, kann hier angegeben werden, welche Informationen im DNS abgefragt werden.
- *Nameserver*: Hier kann ein Nameserver angegeben werden, der befragt werden soll. Bleibt das Feld leer, wird der aktuell im System konfigurierte DNS verwendet.

18.1.2 Abschnitt *Fernzugriff*

18.1.2.1 Felder in diesem Abschnitt

- *Konsolen*: Hier können zwei Konsolen für Fernzugriff ausgewählt werden. Die Konsolen werden in einem Browser-Pop-Up-Fenster geöffnet. Damit die Aktion korrekt gestartet werden kann, müssen Pop-Up-Fenster vom Browser erlaubt sein.

  Mit *SSH* wird ein Terminal über eine verschlüsselte Verbindung

geöffnet. Ein Benutzername für das Login muss angegeben werden.

Eine unverschlüsselte Verbindung kann mit der Wahl von *Telnet* gestartet werden. Hier kann der Ziel-Port angegeben werden, standardmäßig wird Port 23 benutzt.

- *SSH-Benutzername*: Hier wird der Benutzername für den Fernzugriff per SSH eingegeben.
- *Telnet-Port*: Hier wird der Ziel-Port für die Telnet-Verbindung angegeben. Der Telnet-Dienst benutzt als Standard Port 23. Für Tests anderer Dienste kann dieser Port verändert werden.

18.1.3 Abschnitt *Antworten*

Hier werden die ermittelten Informationen angezeigt.

18.1.4 Aktionen für diesen Dialog

- *Aktion starten*: Abfragen über die Toolbox starten.

18.1.5 GUI-Referenz: *Aufräumen*

(Dieser Dialog befindet sich unter *Systembetrieb – Werkzeugkasten – Aufräumen*)

Der Verbleib von benutzerbezogenen Daten im Collax System geschieht, um generell Datenverlust zu vermeiden. In diesem Dialog können Daten, die noch auf dem Collax Server gespeichert sind aber keine zugehörigen Benutzer oder Konfigurationsdaten enthalten, endgültig im System aufgeräumt werden. Die zu diesen Daten

gehörenden Elemente wie Verzeichnisse, Benutzer oder Datensicherungsaufgaben wurden zuvor über die Administrationsoberfläche entfernt.

Bei Sicherungen kann es auch bei ungewollten Unterbrechungen der Sicherungsarbeiten dazu kommen, dass verwaiste Datensätze (Medien) im System hinterbleiben. Diese Medien können ebenso über diesen Dialog aufgeräumt werden.

18.1.5.1 Tab *Verzeichnisse*
Felder in diesem Abschnitt

- *Verwaiste Verzeichnisse*: Hier wird eine Liste von File-Shares angezeigt, die aus der Collax Administration entfernt wurden.

18.1.5.2 Aktionen für diesen Dialog

- *Verzeichnisse löschen*: Die ausgewählten Verzeichnisse werden durch diese Aktion endgültig aus dem System gelöscht. Alle Inhaltsdaten der gewählten Ordner gehen dadurch verloren.

18.1.5.3 Tab *Persönliche Ordner*
Felder in diesem Abschnitt

- *Verwaiste Ordner*: Hier wird eine Liste von persönlichen Ordnern angezeigt, deren Besitzer nicht mehr auf dem Collax Server existieren.

18.1.5.4 Aktionen für diesen Dialog

- *Ordner löschen*: Durch diese Aktion werden die gewählten persönlichen Ordner endgültig aus dem System gelöscht. Alle Inhaltsdaten der gewählten Ordner gehen dadurch verloren.

18.1.5.5 Tab *Postfächer*
Felder in diesem Abschnitt

- *Verwaiste Postfächer*: Hier wird eine Liste von Postfächern angezeigt, deren Besitzer nicht mehr auf dem System existieren. Der Name des Postfach lautet identisch zu dem Login des nicht mehr existenten Benutzers.

18.1.5.6 Aktionen für diesen Dialog

- *Postfächer löschen*: Mit dieser Aktion werden die gewählten Postfächer aus dem Collax System gelöscht. Alle E-Mails der gewählten Postfächer gehen dadurch verloren.

18.1.5.7 Tab *Sicherungsdaten*
Felder in diesem Abschnitt

- *Verwaiste Sicherungsdaten*: Hier wird eine Liste von lokalen Sicherungsdaten angezeigt, bei denen referenzierende Informationen aus der Konfiguration entfernt wurden oder durch einen unterbrochenen Sicherungsdurchlauf verloren gingen.

18.1.5.8 Aktionen für diesen Dialog

- *Sicherungsdaten löschen*: Die ausgewählten lokalen Sicherungsdaten werden mit dieser Aktion bereinigt und aus dem Collax System entfernt.

18.2 *Festplattenverwaltung*

Über die Festplattenverwaltung ist es mit Hilfe des „Logical Volume Management“ (LVM) möglich, weitere Festplattenkapazitäten nachzurüsten und damit die Datenpartition des Collax Security Gateways zu vergrößern.

Der Collax Security Gateway behandelt dabei Festplatten und physikalische Partitionen als „physikalische Volumes“. Aus diesen physikalischen Volumes werden „Logical Volumes“ gebildet, diese werden vom System als Partitionen zum Speichern von Daten verwendet.

Mehrere „Logical Volumes“ gehören zu einer „Volume Group“, die durch Hinzufügen von „physikalischen Volumes“ erweitert werden kann.

18.2.1 GUI-Referenz: Festplattenverwaltung

(Dieser Dialog befindet sich unter *Systembetrieb – Hardware – Festplattenverwaltung*)

In diesem Dialog werden alle vorhandenen Volume-Gruppen verwaltet. Informationen zu angeschlossenen Festplatten können eingesehen werden.

18.2.1.1 Tab *Volume-Gruppen*, Abschnitt *Volume-Gruppe*

Felder im Abschnitt

- *Name*: Name der angezeigten Volume-Gruppe.
- *Größe*: Gesamte Größe des Speicherplatzes, die die Volume-Gruppe mit allen beinhalteten Logical Volumes einnimmt.
- *Benutzt*: Zeigt den Anteil des Speicherplatzes der Volume-Gruppe, der mit Daten gefüllt ist.
- *Verfügbar*: Zeigt den Anteil des Speicherplatzes der Volume-Gruppe, der noch zur Verfügung steht.

18.2.1.2 Tab *Volume-Gruppen*, Abschnitt *Physikalische Volumes*

Spalten in der Tabelle

- *Name*: Zeigt den Namen des physikalischen Volumes.
- *Gerät*: Zeigt den Gerätenamen des physikalischen Volumes.
- *Info*: Hier werden Details über den Geräteanschluss oder die Herstellerbezeichnung angezeigt.
- *Größe*: Hier wird die gesamte Größe des Geräts angezeigt.

Aktionen für jeden Tabelleneintrag

- *Entfernen*: Wird ein physikalisches Volume nicht von Logical Volumes benutzt und ist darauf kein Dateisystem vorhanden, kann das physikalische Volume mit dieser Aktion aus der Gruppe entfernt werden. Ein Detail-Formular wird geöffnet.

18.2.1.3 Tab *Volume-Gruppen*, Abschnitt *Logical Volumes*

Spalten in der Tabelle

- *Name*: Hier wird der Name der Logical Volumes angezeigt. Auf Collax Servern ist das Logical Volume „datavolume“ immer vorhanden.
- *Benutzt physikalisches Volume*: Zeigt an, auf welches physikalische Volume zugegriffen wird.
- *Verwendung*: Zeigt an, ob das Logical Volume vom System oder von einer virtuellen Maschine benutzt wird.
- *Größe*: Zeigt die gesamte Größe des Logical Volumes an. Maximal kann die Größe des benutzten physikalischen Volumes eingenommen werden.

Aktionen für jeden Tabelleneintrag

- *Erweitern*: Steht innerhalb der Volume-Gruppe noch Speicherplatz zur Verfügung, kann der Speicherplatz einzelner Logical Volumes erweitert werden. Maximal kann das Volume um den Speicherplatz erweitert werden, der in der zugehörigen Volume-Gruppe als *Verfügbar* bezeichnet ist.
- *Entfernen*: Wenn das Volume weder vom System noch von einer virtuellen Maschine verwendet wird, kann es mit dieser Aktion entfernt werden. Ein Detail-Formular wird geöffnet.

18.2.1.4 Aktionen für diesen Abschnitt

- *Logical Volume anlegen*: Steht weiterer Speicherplatz in der Volume-Gruppe zur Verfügung, kann mit dieser Aktion ein neues Logical Volume erzeugt werden.

18.2.1.5 Tab *Volume-Gruppe*, Abschnitt *Verfügbare Hardware*

Die Tabelle zeigt am Server angeschlossene Geräte, die zur Verwendung in Volume-Gruppen zur Verfügung stehen.

Spalten in der Tabelle

- *Name*: Hier wird der Name des Geräts angezeigt.
- *Gerät*: Zeigt die Systembezeichnung des Geräts an.
- *Info*: Zeigt weitere Informationen über das Gerät.
- *Größe*: Hier wird die gesamte Größe des Geräts angezeigt.

Aktionen für jeden Tabelleneintrag

- *Physikalisches Volume generieren*: Um das angezeigte Gerät im LVM-System verwenden zu können, kann hier ein physikalisches Volume generiert werden.

18.2.1.6 Tab *Festplatten*, Abschnitt *Blockgeräte*

Diese Tabelle zeigt alle dem Server vorhandenen blockorientierten Geräte.

Spalten in der Tabelle

- *Name*: Name des Geräts.
- *Gerät*: Zeigt die Systembezeichnung des Geräts an.
- *Typ*: Hier wird angezeigt, ob es sich bei dem Gerät um eine Partition, eine erweiterte Partition, ein Volume oder ein Gerät mit Dateisystem handelt. Ist das Feld leer, wurde kein darauf

vorhandenes Dateisystem erkannt, das Gerät wird dann in der Tabelle *Verfügbare Hardware* aufgelistet.
- *Info*: Detailinformation über das Gerät.
- *Größe*: Zeigt die Gesamtgröße des Geräts an.
- *Verwendung*: Hier wird angezeigt, ob das Gerät von einer Volume-Gruppe, vom Backup-System, von einer virtuellen Maschine oder vom Betriebssystem verwendet wird.

Aktionen für jeden Tabelleneintrag

- *Benutzen für ...*: Mit dieser Aktion kann das Gerät zu einer bestehender Volume-Gruppe hinzugefügt werden.
- *Initialisieren ...*: Wurde ein Gerät im System erkannt, das nicht verwendet wird und dessen Partitionen nicht verwendet werden, kann das Gerät mit dieser Aktion initialisiert werden. Nach der Initialisierung kann das Gerät von bestehenden Volume-Gruppen, vom Backup-System oder von virtuellen Maschinen verwendet werden.

  Hinweis: Diese Aktion löscht ohne Rückfrage jedwelche Daten, die auf dem Gerät vorhanden sind.
- *Aus Volume-Gruppe entfernen*: Wird das angezeigte Gerät als physikalisches Volume in einer Volume-Gruppe verwendet und besteht in der Volume-Gruppe ausreichend freier Speicherplatz, dann kann das Gerät aus der Volume-Gruppe entfernt werden. Bei dieser Aktion gehen keine Daten verloren. Der belegte Speicherplatz des ausgewählten Geräts wird bei dieser Aktion auf die anderen Geräte in der Volume-Gruppe verteilt.

18.2.1.7 Tab *Festplatten*, Abschnitt *Logical Volumes*

Diese Tabelle zeigt alle dem Server vorhandenen logischen Geräte an.

Spalten in der Tabelle

- *Gerät*: Systembezeichnung des Geräts.
- *Typ*: Zeigt an, ob es sich um ein Volumen mit erzeugtem Dateisystem handelt.
- *Info*: Detailinformation zum Logical Volume.
- *Größe*: Zeigt die Gesamtgröße des Volumes.

18.2.2 *Physikalisches Volume generieren*

In diesem Detailformular können Informationen kontrolliert, abschließend ein physikalisches Volume erzeugt oder der Dialog abgebrochen werden.

18.2.2.1 Abschnitt *Physikalisches Volume*
Felder in diesem Abschnitt

- *Gerätename*: Zeigt den Gerätenamen des ausgewählten Geräts zur Kontrolle.
- *Information*: Zeigt Detailinformationen zur Kontrolle.
- *Größe*: Zeigt die Gesamtgröße zur Kontrolle.
- *In Volume-Gruppe*: Zeigt zur Kontrolle die Volume-Gruppe, in der das physikalische Volume erzeugt werden soll.

18.2.2.2 Abschnitt *Hinweis*
Felder in diesem Abschnitt

- : Zeigt einen Hinweis zur Beachtung, bevor die Aktion ausgeführt wird.

18.2.2.3 Aktionen für dieses Formular

- *Abbrechen*: Beendet den Dialog, das physikalische Volume wird nicht erzeugt.
- *Generieren*: Beendet den Dialog, das physikalisch Volume wird erzeugt. Die Systemausgabe wird angezeigt.
- *Zurück*: Die Aktion führt zurück ins Hauptformular, die Systemausgabe wird beendet.

18.2.2.4 *Systemausgabe*
Felder in diesem Abschnitt

- : Zeigt die Ausgabe vom Systemprozess.

18.2.3 *Physikalisches Volume löschen*

In diesem Detailformular können Informationen kontrolliert, abschließend das physikalische Volume gelöscht oder der Dialog abgebrochen werden.

18.2.3.1 Abschnitt *Physikalisches Volume*
Felder in diesem Abschnitt

- *Gerät*: Zeigt den Gerätenamen zur Kontrolle.
- *Info*: Zeigt Detailinformationen zur Kontrolle.
- *Größe*: Zeigt die Gesamtgröße des Volumes.
- *Aus Volume-Gruppe*: Zeigt zur Kontrolle die Volume-Gruppe, aus der das physikalische Volume entfernt werden soll.

18.2.3.2 Abschnitt *Hinweis*
Felder in diesem Abschnitt

- : Zeigt einen Hinweis zur Beachtung, bevor die Aktion ausgeführt wird.

18.2.3.3 Aktionen für dieses Formular

- *Abbrechen*: Beendet den Dialog, das physikalische Volume wird nicht gelöscht.
- *Löschen*: Beendet den Dialog, das physikalische Volume wird gelöscht. Die Systemausgabe wird angezeigt.
- *Zurück*: Die Aktion führt zurück ins Hauptformular, die Systemausgabe wird beendet.

18.2.3.4 Abschnitt *Systemausgabe*
Felder in diesem Abschnitt

- : Zeigt die Ausgabe vom Systemprozess.

18.2.4 *Logical Volume anlegen*
18.2.4.1 Abschnitt *Logical Volume*
Felder in diesem Abschnitt

- *Name*: Hier wird der Name angegeben, unter dem das Volume intern verwaltet wird.
- *In Volume-Gruppe*: Zeigt zur Kontrolle die Volume-Gruppe, in der das Logical Volume erzeugt werden soll.
- *Maximale Volume-Größe*: Zeigt die Größe an, mit der das Volume maximal erzeugt werden kann.
- *Größe*: Hier wird angegeben, wie viel Speicherplatz das Volume einnehmen soll.
- *Dateisystem anlegen (ext3)*: Mit dieser Wahl wird angegeben, ob auf dem neuen Volume das Journaling-Dateisystem EXT3 angelegt werden soll.

18.2.4.2 Aktionen für dieses Formular

- *Abbrechen*: Beendet den Dialog, das Logical Volume wird nicht angelegt.
- *Anlegen*: Beendet den Dialog, das Logical Volume wird erzeugt. Die Systemausgabe wird angezeigt.
- *Zurück*: Die Aktion führt zurück ins Hauptformular, die Systemausgabe wird beendet.

18.2.4.3 Abschnitt *Systemausgabe*

Felder in diesem Abschnitt

- : Zeigt die Systemausgabe vom Systemprozess.

18.2.5 *Logical Volume erweitern*

18.2.5.1 Abschnitt *Logical Volume*

Felder in diesem Abschnitt

- *Name*: Zeigt den Gerätenamen zur Kontrolle.
- *In Volume-Gruppe*: Zeigt zur Kontrolle die zugehörige Volume-Gruppe.
- *Aktuelle Größe*: Zeigt die Größe an, die das Volume aktuell belegt.
- *Zusätzlich verfügbar*: Zeigt die Größe an, um die das Volume maximal erweitert werden kann.
- *Erweitern um*: Hier wird die Größe des Speicherplatzes eingetragen, um die das Volume erweitert werden soll.

18.2.5.2 Aktionen für dieses Formular

- *Abbrechen*: Beendet den Dialog, das Logical Volume wird nicht erweitert.
- *Erweitern*: Beendet den Dialog, das Logical Volume wird erweitert. Die Systemausgabe wird angezeigt.
- *Zurück*: Die Aktion führt zurück ins Hauptformular, die Systemausgabe wird beendet.

18.2.5.3 *Systemausgabe*
Felder in diesem Abschnitt

- : Zeigt die Ausgabe vom Systemprozess.

18.2.6 *Logical Volume entfernen*
18.2.6.1 Abschnitt *Logical Volume*
Felder in diesem Abschnitt

- *Name*: Zeigt den internen Namen des Volumes zur Kontrolle.
- *Volume-Gruppe*: Zeigt zur Kontrolle die Volume-Gruppe, aus der das Logical Volume entfernt werden soll.
- *Größe*: Zeigt den belegten Speicherplatz. Wird das Volume gelöscht, steht dieser Platz der Volume-Gruppe zur Verfügung.

18.2.6.2 Abschnitt *Hinweis*
Felder in diesem Abschnitt

- : Hinweis zur Beachtung, bevor das Volume entfernt wird.

18.2.6.3 Aktionen für dieses Formular

- *Abbrechen*: Beendet den Dialog, das Logical Volume wird nicht gelöscht.
- *Löschen*: Beendet den Dialog, das Logical Volume wird gelöscht. Die Systemausgabe wird angezeigt.
- *Zurück*: Die Aktion führt zurück ins Hauptformular, die Systemausgabe wird beendet.

18.2.6.4 Abschnitt *Systemausgabe*

Felder in diesem Abschnitt

- : Zeigt die Ausgabe vom Systemprozess.

18.3 GUI-Referenz: *Shutdown und Reboot*

(Dieser Dialog befindet sich unter *Systembetrieb – Shutdown/Reboot – Allgemein*)

In diesem Dialog kann das System heruntergefahren oder neu gestartet werden. Hier wird zusätzlich die „Uptime“ angezeigt, d. h. die Zeitspanne seit dem letzten Neustart.

Hinweis: Nach 497 Tagen gibt es einen „Wrap-around“; durch einen Überlauf fängt die Uptime wieder bei Null an.

18.3.1 Felder in diesem Dialog

- *Uptime*: Die Laufzeit des Systems seit dem letzten Neustart.

18.3.2 Aktionen für diesen Dialog

- *System herunterfahren*: Mit dieser Aktion wird das System heruntergefahren.
- *System neu starten*: Mit dieser Aktion wird das System heruntergefahren und anschließend neu gestartet.

18.4 GUI-Referenz: *Cache*

(Dieser Dialog befindet sich unter *Systembetrieb – Webproxy – Cache*)

In diesem Dialog kann der Cache des Webproxyservers auf der Festplatte gelöscht werden. Dabei wird der Proxyserver gestoppt und anschließend neu gestartet.

18.4.1 Felder in diesem Dialog

- *Ausgabe*: Hier werden die Meldungen angezeigt, die durch das Löschen des Proxy-Caches und den folgenden Neustart des Webproxyservers verursacht werden.

18.4.2 Aktionen für diesen Dialog

- *Cache löschen*: Mit dieser Aktion wird der Cache gelöscht.
- *Zurück*: Mit dieser Aktion kehren Sie in den Dialog zurück.

19 Systeminformationen

Der Collax Security Gateway bietet umfangreiche Möglichkeiten zur Analyse und Steuerung des gesamten Systems. Diese sind alle unter *System – Überwachung/Auswertung* zugänglich.

19.1 Systeminformationen

Unter *Status – Systeminformationen* ist die Auslastung von Prozessor, Hauptspeicher und Festplattenspeicher einsehbar. Wenn ein Collax Security Gateway sehr träge reagiert, sollte die Auslastung überprüft werden. Interessant ist die Angabe von *Load Average*. Hier wird die gemittelte Last des Systems in der letzten Minute, in den letzten 5 Minuten und in den letzten 15 Minuten angegeben. Diese Load gibt die Auslastung aller Kompontenten wieder. Ein Wert kleiner 1 besagt, dass das System zeitweise nicht ausgelastet war. Ein Wert größer 1 zeigt an, dass einzelne Prozesse auf die Zuteilung von Resourcen warten mussten. Der Betrieb ist bis zu einer Load von ca. 4 problemlos möglich. Liegt die Load darüber, müssen geeignete Maßnahmen ergriffen werden. Die Load selbst kann bis in den dreistelligen Bereich steigen, wobei dann die Antwortzeiten eines Systems sehr groß werden.

Eine Möglichkeit zur genaueren Untersuchung der Load findet sich unter *Auswertungen – Systemstatistik* . Hier können bis zu sechs Parameter des Systems grafisch dargestellt und verglichen werden. Dabei kann das Zeitfenster der Anzeige in verschiedenen Stufen von vier Stunden bis zu einem Jahr eingestellt werden. Durch die

Darstellung der Graphen übereinander lassen sich Zusammenhänge zwischen einzelnen Parametern herstellen.

19.2 Dienste

Alle im Collax Security Gateway vorhandenen Dienste sowie deren jeweiliger Zustand lassen sich unter *Status – Dienste* einsehen. Der Status jeden Dienstes wird zudem durch eine Ampel (rot bzw. grün für nicht laufend bzw. laufend) dargestellt.

Durch Anklicken dieser Ampel kann ein Dienst in den jeweils anderen Zustand geschaltet werden. Dienste, die noch nicht ausreichend konfiguriert sind, werden eventuell nicht starten. Diese Änderungen sind nur temporär und gehen mit dem Neustart des Systems verloren.

Wichtige Dienste, wie der Apache-Webserver (der die GUI bedient) oder der LDAP-Server (der die Benutzerkonten bereitstellt), sollten nicht grundlos deaktiviert werden, da dadurch der Zugriff auf den Collax Security Gateway erschwert wird.

Generell ist diese Seite als Übersicht gedacht, welche Dienste aktuell laufen. In seltenen Fällen können hier einzelne Dienste neu gestartet werden. Um Dienste dauerhaft zu (de-)aktivieren, muss in deren jeweiliger Konfiguration die Option *Aktivieren* entsprechend gesetzt werden.

19.3 Netzwerkstatus

Unter *Status – Link-Status* sind alle angelegten Links aufgelistet. Neben dem Typ und der gesetzten IP-Adresse werden die Zählerstände der ein- und ausgehenden Byte- und Paketzähler angezeigt. Durch Anklicken des *Namens* öffnet sich ein weiteres Fenster, in dem eine Byte-Statistik des jeweiligen Links grafisch angezeigt wird. Dabei werden Graphen für die letzte Stunde, den letzten Tag sowie die gesamte Woche angezeigt.

Zu jedem Link wird der *Status* angezeigt. Mögliche Werte sind „Ok“, „Disabled“ und „Broken“. Der Status „Broken“ zeigt eine Störung an, etwa wenn ein Netzwerkkabel keine Verbindung hat oder wenn die Einwahl zu einer Gegenseite fehlgeschlagen ist. Mit der Ampel können analog zu den Diensten einzelne Links deaktiviert und neu gestartet werden. Auch diese Änderungen sind nur temporär, d. h. bis zum nächsten Neustart gültig.

Für VPN-Links gibt es zudem unter *Status – IPsec* detailliertere Informationen über den Zustand der einzelnen Tunnel sowie die Anzeige der auf einem Tunnel genutzten Algorithmen für Verschlüsselung und Prüfsummen.

Wird der Collax Security Gateway als DHCP-Server eingesetzt, sind unter *Status – DHCP-Leases* alle per DHCP vergebenen IP-Adressen sowie deren Laufzeit einsehbar.

19.4 Mailqueue

Alle vom Collax Security Gateway erzeugten und empfangenen E-Mails werden vor der weiteren Zustellung in die Mailqueue aufgenommen. Wenn die Zustellung durch einen temporären Fehler fehlschlägt (wenn der Zielserver beispielsweise nicht erreichbar ist), verbleiben die E-Mails bis zu fünf Tage in der Mailqueue, bevor sie mit einer Fehlermeldung an den Absender zurückgeschickt werden.

Die Filtermechanismen für E-Mail im Collax Security Gateway werden auf alle neuen E-Mails in der Mailqueue angewandt. Ist eine E-Mail „sauber", wird sie weiter zugestellt. Erkennt ein Filter eine E-Mail als unerwünscht, wird sie abhängig von der Einstellung des Filters aus der Mailqueue gelöscht, in Form einer neuen E-Mail an den Absender zurückgeschickt oder in der Mailqueue angehalten.

Der aktuelle Inhalt der Mailqueue kann unter *Status – Mail-Queue* eingesehen werden. Für jede E-Mail wird die Message-ID, der Zeitpunkt, zu dem sie in die Mailqueue kam, der aktuelle Status sowie die Adressen von Absender und Empfänger angezeigt.

Die Message-ID ist wichtig, um in den Logdateien alle Meldungen zu dieser E-Mail aufzufinden. Durch Anklicken der Message-ID wird ein Fenster geöffnet, in dem alle relevanten Einträge in der Logdatei zu dieser Mail angezeigt werden.

Der Status einer E-Mail zeigt an, warum sich diese E-Mail noch in der Mailqueue befindet. „Verzögert" bedeutet, dass eine Zustellung aufgrund eines Fehlers nicht möglich war. Es erfolgen aber in wachsenden Zeitabständen erneute Zustellversuche. Wurde eine E-Mail beispielsweise durch einen Filter blockiert, ist der Zustand „Angehalten". In diesem Fall muss die E-Mail über *Auswahl* markiert und dann mit *Löschen* entfernt oder mit *Freigeben* zugestellt werden.

Ist der Collax Security Gateway so konfiguriert, dass E-Mails nicht

sofort ausgeliefert werden, kann über den Schalter *Jetzt versenden* eine Auslieferung allur E-Mails erzwungen werden. Analog werden mit *Jetzt abholen* alle Abholaufträge für externe Postfächer gestartet.

19.5 Auswertungen

Für die vier Dienste Webserver, Webproxy, E-Mail-Server und FTP-Server sind detaillierte Auswertungen abrufbar. Dazu muss unter *Auswertungen* der gewünschte Dienst ausgewählt werden. Diese Auswertungen stehen nur für die Dienste zur Verfügung, bei denen *Logauswertung aktiviert* ist. Beim Webproxy muss zudem noch das Protokollieren in eine Logdatei aktiviert werden.

Die Auswertungen werden nachts aus den Logdateien erstellt. Um eine manuelle Auswertung auszulösen, kann *Jetzt aktualisieren* angeklickt werden.

Abgesehen von dienstespezifischen Details zeigen die Auswertung die Verteilung des Datenvolumens über einzelne Zeiträume. Zudem sind die „Top 10“ der Anwender sowie der besuchten Adressen sichtbar. Dazu kann auch jeweils eine vollständige Liste abgerufen werden.

19.6 System-Logdateien

Viele wichtige Dienste im Collax Security Gateway protokollieren ihre Ereignisse in einer zentralen Logdatei, der Syslog-Datei. Auf die Inhalte dieser Datei kann über die Weboberfläche unter *Logdateien* zugegriffen werden. Verschiedene Filter stehen zur Verfügung, um die gesuchte Information zu erhalten.

Zunächst kann der Zeitraum ausgewählt werden, üblicherweise werden Einträge von heute oder gestern gesucht. Es kann aber auch ein konkretes Datum angegeben werden (vorausgesetzt, von dem Zeitpunkt existieren Logdatei-Einträge; dies hängt von der Haltezeit der Logdateien ab).

Als nächstes kann das „Subsystem“ ausgewählt werden, von dem die Einträge gezeigt werden sollen. Folgende Subsysteme existieren:

Kategorien der Logdateien

Kategorie	Details
mail	E-Mail-System mit SMTP-Server postfix und POP/IMAP-Server cyrus.
kernel	Meldungen des Betriebssystemkerns.
firewall	Abhängig von ihrer Einstellung protokolliert die Firewall verschiedene Pakete/Verbindungen.
daemon	Alle Dienste, die keine eigene Kategorie zugeteilt bekommen haben, protokollieren in dieser Kategorie.
auth	Alle Meldungen über Anmeldungen am Collax Security Gateway werden hier erfasst, auch fehlgeschlagene.
syslog	Meldungen über den Systemstatus.
cron	Cron ist die interne Zeitsteuerung des Collax Security Gateways. Hier werden alle Rückmeldungen dieses Dienstes ausgegeben.
ftp	Meldungen des FTP-Servers.

Über das Feld *Programm* können noch die Ausgaben eines einzelnen Dienstes gefiltert werden, etwa „fetchmail“ oder „pluto“.

Die Ausgabe kann entweder im *Textformat* oder in Form einer HTML-Tabelle erfolgen. In der HTML-Variante wird über die Farben grün, gelb und rot die Wichtigkeit der Meldung visualisiert.

19.7 GUI-Referenz: Status

19.7.1 *Systeminformationen*

(Dieser Dialog befindet sich unter *Überwachung/Auswertung – Status – Systeminformationen*)

19.7.1.1 Tab *Status/CPU*, Abschnitt *Status*

Felder in diesem Abschnitt

- *Uptime*: In diesem Feld wird von links nach rechts die aktuelle Systemzeit in der lokalen Zeitzone, die Laufzeit seit dem letzten Neustart des Systems, die Anzahl der über die Konsole angemeldeten Benutzer sowie die durchschnittliche Systemlast der letzten Minute, der letzten fünf Minuten und der letzten 15 Minuten angezeigt.

19.7.1.2 Tab *Status/CPU*, Abschnitt *Graphen*

In diesen Graphen werden CPU-Auslastungen dargestellt.

Felder in diesem Abschnitt

- *CPU-Graphen*: Auslastungen der CPU innerhalb der letzten vier Stunden werden hier in Bezug auf Systemprozesse, virtuellen Maschinen und Dienste dargestellt. Die Aktualisierung geschieht minütlich.

19.7.1.3 Tab *RAM*, Abschnitt *Graphen*

Felder in diesem Abschnitt

- *Speicherbelegung*: Hier wird die Systembenutzung des Hauptspeichers (RAM) der letzten vier Stunden angezeigt. Die Graphik wird minütlich aktualisiert.

19.7.1.4 Tab *Dateisystem*, Abschnitt *Graphen*

Felder in diesem Abschnitt

- *Dateisystem*: Hier wird die Benutzung der Wurzel- und der Datenpartition der letzten vier Stunden angezeigt. Ebenso wird anteilig die Benutzung der Datenpartition von Diensten grafisch dargestellt. Die Graphik wird minütlich aktualisiert.

19.7.1.5 Tab *Festplatten*, Abschnitt *Graphen*

Felder in diesem Abschnitt

- *Festplatten*: Hier werden die Ein- und Ausgabedetails angeschlossener Festplatten dargestellt. Die Graphik wird minütlich aktualisiert.

19.7.1.6 Tab *Netzwerk*, Abschnitt *Graphen*
Felder in diesem Abschnitt

- *Netzwerk*: Hier werden die Ein- und Ausgabedetails angeschlossener Netzwerkschnittstellen dargestellt. Dies betrifft physikalische Ethernet-Geräte aber auch Bridges. Die Graphik wird minütlich aktualisiert.

19.7.1.7 Tab *Virtuelle Maschinen*, Abschnitt *Graphen*
Felder in diesem Abschnitt

- *Virtuelle Maschinen*: Hier werden sämtliche Details angelegter virtueller Maschinen grafisch aufgezeichnet. Die Graphik wird minütlich aktualisiert.

19.7.2 *Dienste*

(Dieser Dialog befindet sich unter *Überwachung/Auswertung – Status – Dienste*)

Dieser Dialog zeigt alle wichtigen Dienste auf dem Collax Security Gateway und ihren aktuellen Status an. Die Dienste können hier gestoppt und gestartet werden.

19.7.2.1 Felder in diesem Dialog

- *Subsystem*: Hier wird das übergeordnete System angezeigt, zu dem der Dienst gehört.
- *Dienst*: Hier wird der Name des Dienstes angezeigt.

- *Status*: Hier wird der Status des Dienstes angezeigt. „Running“ bedeutet, dass der Dienst aktiviert ist und läuft, „stopped“ hingegen, dass der Dienst in der Konfiguration aktiviert ist, der Dienst jedoch aus unbestimmtem Grund gestopped wurde.
- *Test*: In dieser Spalte wird das Ergebnis aufgrund eines qualitativen Tests angezeigt. So kann hier z.B. als Ergebnis CRITICAL angezeigt werden, auch wenn der Status „Running“ ist. Das hier angezeigt Testergebnis entspricht dem der aktivien Überwachung.

19.7.2.2 Aktionen für jeden Tabelleneintrag

- *Start*: Um einen Dienst zu starten, muss über das Kontextmenü (rechter Mausklick) „Start“ angeklickt werden.
- *Stop*: Um einen Dienst zu beenden, muss über das Kontextmenü (rechter Mausklick) „Stop“ angeklickt werden.

19.7.3 *Link-Status*

(Dieser Dialog befindet sich unter *Status – Link-Status*)
Hier wird der Status der einzelnen Netzwerklinks angezeigt.

19.7.3.1 Felder in diesem Dialog

- *Name*: Hier steht der Name des Links.
- *Typ*: Hier steht der zugehörige Link-Typ.
- *Interface*: Hier wird das Interface angezeigt, auf dem der Link existiert.

- *IP-Adresse*: Hier wird die IP-Adresse des Systems angegeben, die auf dem jeweiligen Link gesetzt ist.
- *Gegenstelle*: Hier wird die Gegenstelle des Links angezeigt.
- *Status*: Hier wird der Status des Links angezeigt. Mögliche Zustände der Links sind „UP“, „Not established“ und „Disabled“.

19.7.3.2 Aktionen für jeden Tabelleneintrag

- *Deaktivieren*: Ist der Link aktiviert, wird ein grüner Schalter angezeigt. Über diesen kann der Link deaktiviert werden, so dass keine weiteren Daten übertragen werden.
- *Restart*: Mit dieser Aktion kann ein Link gestoppt werden. Der Neustart erfolgt im Anschluss automatisch.
- *Aktivieren*: Bei einem deaktivierten Link wird ein roter Schalter angezeigt. Über diesen kann der Link aktiviert werden.

19.7.4 *Ethernet-Status*

(Dieser Dialog befindet sich unter *Überwachung/Auswertung – Status – Ethernet-Status*)

In diesem Formular können Detailinformationen über den Ethernet-Status eingesehen werden. Zunächst kann im Graph eine schematische Abbildung der lokalen Schnittstellen und deren Verbindung zu den anliegenden Geräten eingesehen werden. Weitere Details können in der Liste für jedes einzelne Ethernet-Gerät abgerufen werden.

19.7.4.1 *Ethernet-Status*

Tab *Graph*

In diesem Schaubild sind die Netzwerkschnittstellen abgebildet. Zudem werden verbundene Geräte, wie Switch oder andere Server, gezeigt. Ist eine Schnittstelle rot umrandet, ist diese nicht verbunden oder wird nicht verwendet.

Tab *Liste*

Spalten in der Tabelle

- *Name*: Zeigt den Namen der Ethernet-Schnittstelle.
- *Art*: Zeigt die Art der Schnittstelle. Es gibt physikalische Schnittstellen und logische Schnittstellen. Zu den logischen Schnittstellen gehören VLAN, MAC-Vlan, Ethernet-Bond, Bridge oder die Loopback-Schnittstelle.
- *Status*: Zeigt den Status. Wird eine Schnittstelle verwendet hat diese den Status *up*. Bei *unknown* liegen momentan keine Informationen für die Schnittstelle vor.
- *MAC-Adresse*: Zeigt die Hardware-Adresse. Eine oder mehrere logischen Schnittstellen dürfen dieselbe MAC-Adresse besitzen, insofern keine spezielle konfiguriert wurde.

Aktionen für jeden Tabelleneintrag

- *Detail*: Per Doppelklick oder Rechter-Maus-Klick können die Details mit dieser Aktion abgerufen werden.

19.7.4.2 *Ethernet-Status (Detail)*

Tab *Grundlagen*

Hier werden die grundlegenden Informationen zur Schnittstelle angezeigt.

Tab *Grundlagen*, Abschnitt *VLAN*

Hier werden die grundlegenden Informationen zu VLAN angezeigt.

Tab *Grundlagen*, Abschnitt *Bündel*

Hier werden die grundlegenden Informationen zu einer Bonding-Schnittstelle angezeigt.

Tab *Grundlagen*, Abschnitt *Bridge Port*

Hier werden die grundlegenden Informationen zu einer Bridge angezeigt.

Tab *Grundlagen*, Abschnitt *IPv4 Adresse*

Hier werden die grundlegenden Informationen zu einer IPV4-Adresse angezeigt.

Tab *VLANs*, Abschnitt *VLAN*

Hier werden die grundlegenden Informationen zu VLAN angezeigt.

Tab *STP*

Hier werden die grundlegenden Informationen zu STP angezeigt.

Tab *Ports*, Abschnitt *Port* Abschnitt *MACs*

Hier werden die grundlegenden Informationen zu verwendeten Ports angezeigt.

Tab *Gegenstelle*, Abschnitt *Port*

Hier werden die grundlegenden Informationen zum Port der Gegenstelle angezeigt.

Tab *Gegenstelle*, Abschnitt *Gerät*

Hier werden die grundlegenden Informationen zum Gerät der Gegenstelle angezeigt.

Tab *Gegenstelle*, Abschnitt *Inventory*

Hier werden die grundlegenden Informationen zum Inventar der Gegenstelle angezeigt.

Aktionen für dieses Formular

- *Zurück*: Beendet den Dialog und führt zurück zur Übersicht.

19.7.5 *VPN-/IPsec-Status*

(Diese Option befindet sich im Zusatzmodul *Collax Gatekeeper*)

(Dieser Dialog befindet sich unter *Überwachung/Auswertung – Status – IPsec*)

Dieser Dialog zeigt eine Übersicht über die konfigurierten VPN-/IPsec-Verbindungen des Systems an. Für jeden IPsec-Link wird ein eigener Abschnitt angezeigt, der neben dem Namen des Links die Details für jede einzelne IPsec-Verbindung enthält.

Einem IPsec-Link können jeweils mehrere verschiedene Netzwerke als lokale und gegenüberliegende („remote“) Netze zugeordnet werden. Für jede dieser Verbindungsmöglichkeiten wird eine eigene Verbindung aufgebaut, die hier mit angezeigt wird. Es kann vorkommen, dass die verschiedenen Verbindungen einen unterschiedlichen Status haben. Bei Netz-zu-Netz-Verbindungen kann dies auf einen Konfigurationsfehler hindeuten.

Neben den einzelnen IP-Netzen wird mit *Eroute* und *Etabliert* der genaue Status angezeigt. *Eroute* steht für „encrypted Route“ und gibt an, dass Pakete in diese Netze tatsächlich verschlüsselt übertragen werden. Der Tunnel ist *etabliert*, wenn mit der Gegenseite eine Verbindung aufgebaut werden konnte. Bei aufgebautem Tunnel werden zusätzlich die aktuellen Verbindungsparameter (Verschlüsselungs- und Prüfsummenverfahren) angezeigt.

Hier wird der Status einzelner VPN-Links, die den IPsec-Standard benutzen, angezeigt.

19.7.5.1 Felder in diesem Abschnitt

- *Hinweis*: Wenn kein Status über VPN-Links verfügbar ist, wird hier ein entsprechender Hinweis angezeigt.

19.7.5.2 Felder in diesem Abschnitt

- *Link*: Dieses Feld zeigt den Namen des Links an.
- *Lokales Netz*: Dieses Feld zeigt die Adresse des lokalen Netzwerks an.
- *Lokale IP-Adresse*: Dieses Feld zeigt die lokal verwendete IP-Adresse des Links an.
- *Eigene ID*: Dieses Feld zeigt die eigene ID des VPN-Links an. Bei Authentifizierung mit Zertifikaten wird hier als ID der Common Name (cn) angezeigt. Bei Benutzung von einem PSK wird hier die angegebene lokale ID angezeigt.
- *Etabliert*: Dieses Feld zeigt an, ob der VPN-Link aufgebaut wurde. Ein rotes Kreuz symbolisiert „Nein“, ein grüner Haken symbolisiert „Ja“. Der Link ist dann vollständig aufgebaut, sobald auch „eroute“ gesetzt ist.
- *Eroute*: Dieses Feld zeigt an, ob der VPN-Link geroutet wird. Ein rotes Kreuz symbolisiert „Nein“, ein grüner Haken symbolisiert „Ja“. Wird das letztere Symbol angezeigt, ist der Link vollständig aufgebaut.
- *ESP*: Dieses Feld zeigt Details über die verwendeten Verschlüsselungs-Algorithmen des aufgebauten VPN-Links an.
- *Erreichbares Netz*: Dieses Feld zeigt die Adresse des erreichbaren Netzwerks an.
- *IP-Adresse der Gegenstelle*: Dieses Feld zeigt die IP-Adresse der VPN-Gegenstelle an.
- *ID der Gegenstelle*: Dieses Feld zeigt die ID der VPN-Gegenstelle an.

19.7.6 *DHCP-Leases*

(Dieser Dialog befindet sich unter *Überwachung/Auswertung – Status – DHCP-Leases*)

In diesem Dialog wird angezeigt, welche IP-Adressen per DHCP an welche Rechner vergeben wurden.

19.7.6.1 Felder in diesem Dialog

- *IP-Adresse*: Hier wird die vergebene IP-Adresse angezeigt.
- *Hostname*: Hier wird der Hostname des angemeldeten Rechners aufgeführt.
- *MAC-Adresse*: Hier ist die Ethernet-MAC-Adresse des Rechners aufgeführt, an den die IP-Adresse zuletzt vergeben wurde.
- *Vergeben seit*: Zeigt an, wann die IP-Adresse zugewiesen wurde.
- *Vergeben bis*: Zeigt an, bis wann die IP-Adresse vergeben ist. Der DHCP-Server behält bereits abgelaufene Leases auch dann noch, wenn der Rechner die IP-Adresse nicht mehr weiter benutzt. Daher kann hier ein Zeitpunkt in der Vergangenheit angezeigt werden.
- *Status*: Zeigt den Status der DHCP-Lease an. Eine IP-Adresse ist normalerweise entweder als *free* oder *active* markiert. *Active* bedeutet, dass die Adresse benutzt wird und daher nicht bei einer DHCP-Anfrage vergeben wird. Als *free* wird eine IP-Adresse markiert, die bei einer DHCP-Anfrage neu vergeben werden kann.

  Der Status *conflict* bedeutet, dass der Server diese Adresse per DHCP vergeben wollte, aber ein anderer Rechner im Netz diese IP-Adresse benutzt oder zum Zeitpunkt des Versuchs benutzt hat.

  In der Regel werden zunächst solange neue IP-Adressen aus dem Adresspool vergeben, bis keine weiteren Adressen mehr zur

Verfügung stehen. Erst danach beginnt der DHCP-Server, bereits benutzte IP-Adressen neu zu vergeben.

19.7.7 *USV-Status*

(Dieser Dialog befindet sich unter *Überwachung/Auswertung – Status – USV-Status*)

19.7.7.1 Abschnitt *Status*

Hier wird der Status einer angeschlossenen USV angezeigt.

Felder in diesem Abschnitt

Mit einem Klick auf den Namen der angelegten USV werden weitere Informationen zu dem Gerät angezeigt.

19.7.7.2 Abschnitt *Hinweis*

Felder in diesem Abschnitt

- *Auf diesem System ist noch keine USV eingerichtet. Daher ist hier kein Status abrufbar*: Hier werden detaillierte Informationen über die ausgewählte USV angezeigt. Mit der Aktion *Back to Overview* wird wieder die gesamte Liste angezeigt.

19.7.8 *Status Aktive Überwachung*

(Dieser Dialog befindet sich unter *Überwachung/Auswertung – Status – Aktive Überwachung*)

In diesem Dialog wird der Status der aktiven Überwachung angezeigt. Intern verwendet das System dazu *Nagios*, dessen Web-GUI hier eingeblendet wird. In dem Menü auf der linken Seite können verschiedene Informationen und Statistiken abgerufen werden.

Wichtig ist das *Tactical Overview*, welches auf einen Blick den Zustand der überwachten Computer (*Hosts*) und Dienste (*Services*) anzeigt. Interessant ist auch die *Status Map*, in der alle Hosts auf einen Blick erfasst werden können. Zudem visualisiert diese Übersicht die Abhängigkeiten der Systeme untereinander.

Die Konfiguration der einzelnen Hosts und der geprüften Dienste auf jedem Host wird in den Einstellungen des jeweiligen *Hosts* vorgenommen.

19.7.9 *Mail-Queue*

(Dieser Dialog befindet sich unter *Überwachung/Auswertung – Status – Mail-Queue*)

Alle eingehenden E-Mails werden in der Mailqueue, einer Warteschlange, zwischengespeichert. Sie sind vorweg durch eingeschaltete Filter geprüft worden. Von hier aus erfolgt die weitere Zustellung in einzelne Postfächer oder an andere Server. Ist eine *Wartezeit beim Versand* eingestellt, oder kommt es zu Problemen beim Versand, etwa weil ein anderer Mailserver nicht erreichbar ist, werden die E-Mails weiter in der Mail-Queue aufbewahrt. Das System unternimmt in regelmäßigen Abständen weitere Versuche, die E-Mails zuzustellen.

19.7.9.1 Spalten in der Tabelle

- *ID*: Dieses Feld enthält die Message-ID, unter der die E-Mail im Mailsystem verwaltet wird.

  Durch das Anklicken der Message-ID öffnet sich ein neues Fenster, welches alle Einträge zu dieser E-Mail aus der Logdatei anzeigt.
- *Empfangen*: Diese Spalte zeigt den Zeitpunkt an, an dem die E-Mail beim System eingeliefert wurde. Dies gilt auch für E-Mails, die auf dem System selbst erzeugt wurden.
- *Status*: In dieser Spalte wird der aktuelle Status der E-Mail angezeigt. Mögliche Werte sind:

  E-Mails im Zustand *Deferred* versucht das System noch zuzustellen. Entweder ist eine Wartezeit beim Versand eingestellt, oder der Mailserver des Empfängers bzw. der nächste Mailserver auf dem Weg dorthin kann die E-Mail im Moment nicht verarbeiten.

  E-Mails im Zustand *Active* werden momentan zugestellt. Eine E-Mail sollte sich eigentlich nur kurz in diesem Zustand befinden. Zu Zeitpunkten mit hohem Mailaufkommen kann es vorkommen, dass einige E-Mails mit diesem Zustand in der Mailqueue verweilen. Besteht dieser Zustand über einen längeren Zeitraum, liegt oft eine Störung im Mailsystem vor, und die Mail-Logdatei sollte auf mögliche Probleme hin untersucht werden.
- *Absender*: In dieser Spalte wird die die E-Mail-Adresse des Absenders angezeigt.
- *Absender-Domain*: In dieser Spalte wird die Domain des Absenders angezeigt.
- *Empfänger*: Hier werden die E-Mail-Adressen der Empfänger angezeigt. Mehrere Empfänger sind durch Kommata getrennt.
- *Empfänger-Domain*: In dieser Spalte werden die Domains der Empfänger angezeigt.

- *Kommentar*: Falls der Versand der E-Mail verzögert wurde, enthält dieses Feld die genaue Ursache der Verzögerung.

19.7.9.2 Aktionen für diesen Dialog

- *Aktualisieren*: Mit dieser Aktion wird der aktuelle Stand der Warteschlange angezeigt. Bisher als *aktiv* markierte E-Mails sollten dann aus der Warteschlange verschwunden (zugestellt) oder in einen anderen Status übergegangen sein.
- *Alle E-Mails löschen*: Mit dieser Aktion werden alle E-Mails aus der Mailqueue ohne Rückfrage gelöscht. Diese Aktion kann erforderlich sein, falls nach ausführen von *Zustellen* oder *Requeue* E-Mails in der Mail-Queue verbleiben, die aufgrund eines Fehlers nicht zustellbar sind.
- *Zustellen*: Mit dieser Aktion wird das Zustellen aller versandfertigen E-Mails veranlasst. E-Mails werden ohne Berücksichtigung der Wartezeit versendet.
- *Requeue*: Mit dieser Aktion wird ein erneuter Zustellversuch angestoßen und alle E-Mails durchlaufen nochmals die Filterkette. Es ist dadurch möglich, dass E-Mails nochmals ausgefiltert und somit angehalten werden. Zusätzlich werden Zähler des Mailsystems zurückgesetzt. Üblicherweise ist diese Aktion nur dann erforderlich, falls Einstellungen des Servers verändert wurden, um den E-Mail-Transport zu verbessern.
- *E-Mail anhalten*: Diese Aktion unterbricht die Zustellung der gewählten E-Mail und verschiebt diese in die Warteschlange für angehaltenen E-Mails. Danach kann die E-Mail, sofern erforderlich, gelöscht oder anderweitig verarbeitet werden.
- *E-Mails abholen*: Falls ein oder mehrere Abholaufträge zum Leeren von Postfächern auf fremden Servern eingerichtet sind, kann

deren Start mit dieser Aktion veranlasst werden. Normalerweise wird dies aber von der internen „Schaltuhr“ automatisch in festen Abständen durchgeführt.

19.7.10 *Angehaltene Mails*

(Diese Option befindet sich im Zusatzmodul *Collax Communication Server* und *Collax Mail Security*)

(Dieser Dialog befindet sich unter *Überwachung/Auswertung – Status – Angehaltene Mails*)

E-Mails, die durch einen Filter (Virenfilter usw.) identifiziert wurden, werden angehalten. Es erfolgt keine weitere Zustellung. Diese E-Mails befinden sich im Quarantänezustand, und der Administrator muss entscheiden, was mit ihnen weiter geschehen soll. Er kann die E-Mails dazu freigeben oder löschen.

19.7.10.1 Spalten in der Tabelle

- *Auswahl*: In dieser Spalte können Elemente für eine Aktion selektiv gewählt werden.
- *ID*: Dieses Feld enthält die Message-ID, unter der die E-Mail im Mailsystem verwaltet wird.

  Durch das Anklicken der Message-ID öffnet sich ein neues Fenster, welches alle Einträge zu dieser E-Mail aus der Logdatei anzeigt.
- *Empfangen*: Diese Spalte zeigt den Zeitpunkt an, an dem die E-Mail beim System eingeliefert wurde. Dies gilt auch für E-Mails, die auf dem System selbst erzeugt wurden.
- *Absender*: In dieser Spalte wird die die E-Mail-Adresse des Absenders angezeigt.

- *Absender-Domain*: In dieser Spalte wird die Domain des Absenders angezeigt.
- *Empfänger*: Hier werden die E-Mail-Adressen der Empfänger angezeigt. Mehrere Empfänger sind durch Kommata getrennt.
- *Empfänger-Domain*: In dieser Spalte werden die Domains der Empfänger angezeigt.
- *Kommentar*: In diesem Feld wird ein Hinweis angezeigt, weshalb die E-Mail ausgefiltert wurde.

19.7.10.2 Aktionen für jeden Tabelleneintrag

- *Anzeigen*: Die Kopfzeilen und der Inhalt angehaltener E-Mails kann in einem separaten Browser-Fenster angezeigt werden. Die Aktion wird durch rechten Mausklick auf die gewünschte E-Mail gewählt.
- *Alle markieren*: Diese Aktion markiert alle gehaltenen E-Mails.
- *Spam markieren*: Diese Aktion markiert alle gehaltenen E-Mails, die als Spam identifiziert wurden.
- *Viren markieren*: Diese Aktion markiert alle gehaltenen E-Mails, die als virenverseucht identifiziert wurden.
- *Header/MIME markieren*: Diese Aktion markiert alle E-Mails, die durch Kopfzeilen- oder Anhangsfilter angehalten wurden.
- *Markierung entfernen*: Alle Markierungen werden entfernt.
- *Löschen*: Alle markierten Elemente werden gelöscht.
- *Freigeben*: Alle markierten Elemente werden freigegeben und für die weitere Zustellung an die *Mail-Queue* übergeben.

19.7.10.3 Aktionen für dieses Formular

- *Aktualisieren*: Mit dieser Aktion wird die Liste der gehaltenen E-Mails aktualisiert.
- *E-Mails abholen*: Falls ein oder mehrere Abholaufträge zum Leeren von Postfächern auf fremden Servern eingerichtet sind, kann deren Start mit dieser Aktion veranlasst werden. Normalerweise wird dies aber von der internen „Schaltuhr“ automatisch in festen Abständen durchgeführt.

19.7.10.4 *E-Mail Inhalt*

Felder in diesem Formular

- *Inhalt*: In diesem Feld wird der Inhalt inklusive Kopfzeilen der E-Mail ausgegeben.

Aktionen für dieses Formular

- *Zurück*: Diese Aktion beendet die Anzeige und führt zurück zur Liste angehaltener E-Mails.

19.8 GUI-Referenz: Auswertungen

19.8.1 *Systeminformationen*

(Dieser Dialog befindet sich unter *Überwachung/Auswertung – Auswertungen – Systemstatistik*)

Das System ermittelt zur Laufzeit verschiedene statistische Angaben und speichert diese für einen Zeitraum von einem Jahr ab. Über diesen Dialog sind graphische Auswertungen dieser Daten abrufbar.

Zunächst muss unter *Zeige Daten für* ausgewählt werden, für welchen Zeitraum die Grafiken erstellt werden sollen. Wird *für eine Woche* oder *für einen Monat* gewählt, erscheint ein weiteres Feld, in dem die Woche oder der Monat festgelegt werden können.

Unter *Zeige Graphen für* wird das Subsystem ausgewählt, für welches die Grafik erstellt wird. Zum Vergleich können weitere Subsysteme ausgewählt werden.

19.8.1.1 Tab *Graphen*, Abschnitt *Graphen*
Felder in diesem Abschnitt

- *1. Graph*: Hier wird der Graph des ausgewählten Subsystems angezeigt. Es können bis zu sechs Graphen angezeigt und verglichen werden.

19.8.2 *Webserver*

(Dieser Dialog befindet sich unter *Überwachung/Auswertung – Auswertungen – Webserver*)

19.8.2.1 Abschnitt *Hinweis*
Felder in diesem Abschnitt

- *Die Logauswertung ist nicht aktiviert*: Die Logauswertung bietet für die Dienste HTTP, FTP, Mail und HTTP-Proxy eine statistische Auswertung über die Nutzung.

  Hinweis: Bei den einzelnen Diensten muss die Logauswertung jeweils aktiviert sein, damit die Statistikinformationen zur Verfügung stehen.

19.8.2.2 Abschnitt *Auswertungen für ...*
Felder in diesem Abschnitt

- *Auswertungen für ...*: Hier wird der Dienst ausgewählt, für den die Logauswertung angezeigt werden soll.

  Hinweis: Bei der FTP-Auswertung werden nur Transaktionen angezeigt. Anmeldungen am FTP-Server ohne Transaktionen werden nicht angezeigt.

19.8.2.3 Aktionen für diesen Dialog

- *Anzeigen*: Zeigt die Auswertung an.

19.8.3 *Webproxy*

(Dieser Dialog befindet sich unter *Überwachung/Auswertung – Auswertungen – Webproxy*)

Hier sind die Auswertungen für den Webproxyserver abrufbar.

19.8.3.1 Abschnitt *Hinweis*

Felder in diesem Abschnitt

- *Die Logauswertung ist nicht aktiviert*: Damit die Logauswertung genutzt werden kann, muss sie bei der Konfiguration der entsprechenden Dienste aktiviert werden. Die Logauswertung ist verfügbar für die Dienste HTTP, FTP, Mail und HTTP-Proxy.

19.8.3.2 Abschnitt *Auswertungen für ...*

Felder in diesem Abschnitt

- *Auswertungen für ...*: Hier wird der Dienst ausgewählt, für den die Logauswertung angezeigt werden soll.

  Hinweis: Bei der FTP-Auswertung werden nur Transaktionen angezeigt. Anmeldungen am FTP-Server ohne Transaktionen werden nicht angezeigt.

19.8.3.3 Aktionen für diesen Dialog

- *Anzeigen*: Zeigt die Auswertung der Webproxy-Logdatei an.

19.8.4 *Mail*

(Dieser Dialog befindet sich unter *Überwachung/Auswertung – Auswertungen – Mail*)

Hier sind die Auswertungen für den Mailserver abrufbar.

19.8.4.1 Abschnitt *Hinweis*

Felder in diesem Abschnitt

- *Die Logauswertung ist nicht aktiviert*: Damit die Logauswertung genutzt werden kann, muss sie bei der Konfiguration der entsprechenden Dienste aktiviert werden. Die Logauswertung ist verfügbar für die Dienste HTTP, FTP, Mail und HTTP-Proxy.

19.8.4.2 Abschnitt *Auswertungen für ...*

Felder in diesem Abschnitt

- *Auswertungen für ...*: Hier wird der Dienst ausgewählt, für den die Logauswertung angezeigt werden soll.

19.8.4.3 Aktionen für diesen Dialog

- *Anzeigen*: Zeigt die Auswertung an.

19.8.5 *System-Logdateien*

(Dieser Dialog befindet sich unter *Überwachung/Auswertung – Logdateien – System-Logdateien*)

19.8.6 Felder in diesem Dialog

- *Livelog*: Mit dieser Option kann die gewünschte Logdatei im Livelog-Modus angezeigt werden. Der „Follow-Mode“ ermöglicht es, die neuesten Systemmeldungen zu verfolgen.
- *Datum*: Hier wird eingestellt, aus welchem Zeitraum die Einträge aus der Logdatei angezeigt werden sollen. Über *andere* kann ein frei definierbarer Zeitraum angezeigt werden.
- *Stunde(n)*: Hier wird eingestellt, wie viele Stunden rückwirkend die angezeigte Logdatei reichen soll.
- *Ab Datum*: Hier kann ein Anfangsdatum für die Anzeige vorgegeben werden. Bleibt das Feld leer, startet die Anzeige mit dem ersten Eintrag in der Logdatei.
- *Ab Uhrzeit*: Hier kann eine Startzeit für die Anzeige vorgegeben werden. Bleibt das Feld leer, startet die Anzeige mit dem ersten Eintrag in der Logdatei.
- *Bis Datum*: Hier wird das Datum angegeben, bis zu dem Einträge angezeigt werden sollen. Bleibt das Feld leer, werden alle Einträge bis zum Ende der Logdatei angezeigt.
- *Bis Uhrzeit*: Hier kann die Zeit angegeben werden, bis zu der die Daten angezeigt werden.
- *Subsystem*: Die Anzeige der Logdateien kann auf einzelne *Subsysteme* beschränkt werden. Wird kein Subsystem ausgewählt, werden die Informationen von allen Subsystemen angezeigt.
- *Programm*: Mit diesem Feld kann auf die Logdatei ein Filter

angewandt werden, der nur Einträge von einer bestimmten Software anzeigt.

- *Message-ID*: Wenn als Subsystem *Mail* ausgewählt wurde, kann mit diesem Filter die Anzeige auf Einträge zu einer bestimmten Message-ID eingeschränkt werden.
- *Textformat benutzen*: Wird diese Option aktiviert, erfolgt die Ausgabe als Text und nicht als HTML-Tabelle. Manche Browser haben Probleme mit der Darstellung von großen Tabellen, in diesen Fällen sollte die Option aktiviert werden.

19.8.7 Aktionen für diesen Dialog

- *Anzeigen*: Zeigt die Einträge in der Logdatei an.
- *Download*: Startet einen Download der Logdateieinträge.

19.8.8 Logdateikonfiguration

Für die einzelnen Logdateien im System kann eingestellt werden, nach welcher Zeitspanne sie jeweils „rotiert“ werden. Dabei wird die aktuelle Logdatei umbenannt und eine neue, leere Logdatei erstellt. Durch entsprechende Umbenennung aller gespeicherten Logdateien bleibt eine Historie der letzten Tage oder Wochen zur Fehleranalyse vorhanden.

Dabei kann eingestellt werden, wie viele Logdateien aufbewahrt bleiben sollen. Wird beispielsweise wöchentlich rotiert und werden vier Dateien aufgehoben, sind neben der aktuellen Logdatei die Dateien der letzten vier Wochen vorhanden. Die älteste davon wird nach Ablauf einer weiteren Woche gelöscht.

19.8.8.1 *System-Log*

(Dieser Dialog befindet sich unter *Logkonfiguration – System-Logs*)

Felder in diesem Dialog

- *System-Log neu anlegen*: Hier wird eingestellt, nach welcher Zeitspanne die System-Logdateien „rotiert“ werden.
- *Sicherungskopien vorheriger System-Logs*: In diesem Feld wird eingestellt, wie viele alte Versionen der Logdatei aufbewahrt werden.
- *Über Netzwerk loggen*: Durch das Aktivieren dieser Option kann auf einen „Syslog-Server“ im Netzwerk protokolliert werden. Dies gewährleistet den Zugriff auf die Logdateien eines Systems, selbst wenn dieses System vollständig beschädigt ist (Festplattenschaden o. ä.).
- *Protokoll*: Hier wird das Protokoll (TCP/UDP) eingestellt, mit dem die Syslog-Meldungen im Netz verschickt werden.

  Normale Syslog-Server unterstützen nur UDP. Mit dem neuen „syslog-ng“ auf dem Syslog-Server kann auch TCP für eine zuverlässige Übertragung genutzt werden.
- *Log-Port*: Hier muss der Zielport des Syslog-Servers eingegeben werden. Normalerweise läuft Syslog auf Port 514.
- *Log-Host*: Hier wird die IP-Adresse des Syslog-Servers angegeben.

19.8.8.2 *Webserver-Logs*

(Dieser Dialog befindet sich unter *Serverdienste – Webserver – Webserver-Logs* sowie unter *Logkonfiguration – Webserver-Logs*)

Felder in diesem Dialog

- *Webserver-Logs neu anlegen*: Analog zu den normalen Logdateien des Systems können hier Logdateien des Webservers nach einer gewissen Zeitspanne „rotiert“ werden.
- *Sicherungskopien vorheriger Webserver-Logs*: In diesem Feld wird eingestellt, wie viele alte Versionen der Logdatei aufbewahrt werden.

19.8.8.3 *Webproxy-Logs*

(Dieser Dialog befindet sich unter *Netzwerk – Webproxy – Webproxy-Logs* sowie unter *Logkonfiguration – Webproxy-Logs*)

Felder in diesem Dialog

- *Webproxy-Logs neu anlegen*: Analog zu den normalen Logdateien des Systems können hier Logdateien des Webproxyservers nach einer gewissen Zeitspanne „rotiert“ werden.
- *Sicherungskopien vorheriger Webproxy-Logs*: In diesem Feld wird eingestellt, wie viele alte Versionen der Logdatei aufbewahrt werden.

19.8.8.4 *Ereignislog*

(Dieser Dialog befindet sich unter *Logkonfiguration – Ereignislog*)

Bei bestimmten Ereignissen kann das System selbständig eine E-Mail an den Administrator schicken. Dabei wird beispielsweise bei Zugriffen von anderen Systemen deren IP-Adresse sowie die Uhrzeit mitgeschickt.

Felder in diesem Dialog

- *Ereignis*: In dieser Liste müssen die Ereignisse ausgewählt werden, bei deren Auftreten eine E-Mail verschickt wird.
- *Benachrichtigen per E-Mail*: In dieser Liste müssen die Ereignisse ausgewählt werden, bei deren Auftreten eine E-Mail verschickt wird.

20 Software neu installieren oder Auslieferungszustand wiederherstellen

Das Betriebssystem des Collax Security Gateway kann bei Bedarf in kurzer Zeit neu installiert werden. So kann der Server sozusagen in den Auslieferungszustand zurückgesetzt werden.

20.1 Brennen der ISO-Datei

- Bevor Sie die Installation beginnen, brennen Sie das heruntergeladene ISO-Image als Disk-Image auf ihren leeren Datenträger (DVD-Rohling).
- Nach dem Brennen der DVD legen Sie diese bitte in ein Bootfähiges DVD-Laufwerk und rebooten die Maschine.
- Alternativ kann das ISO-Image auf einen USB-Stick kopiert werden, um mit diesem das System zu installieren. Die Vorgehensweise ist im Howto „Erstellen eines bootbaren USB-Sticks“ beschrieben.

20.2 Installation

WICHTIGER HINWEIS: Durch die Installation des Collax Servers werden ALLE AUF DEM SYSTEM BEFINDLICHEN DATEN GELÖSCHT. Verwenden Sie bitte eine dedizierte Maschine für Ihren Test bzw. für den späteren Betrieb.

- Legen Sie die DVD ein, booten Sie und folgen Sie den Anweisungen.
- Sie können die vorgeschlagene IP-Adresse akzeptieren oder eine IP-Adresse mit der entsprechenden Netzmaske aus Ihrem Netz vergeben.
- Nach der Installation erscheint die Meldung „Fertig“. Starten Sie den Rechner neu. Der erste Boot-Vorgangdauert etwas länger.
- Sobald die Login-Aufforderung kommt, können Sie Monitor und Tastatur abhängen.

Der Collax Server ist jetzt einsatzbereit.

20.3 Administration

- Verbinden Sie sich zum Collax Server über einen Browser.
- Folgen Sie den ersten Schritten hier (S. 11)

Index