

Astaro Security Gateway V7

(Version 7.500)

Administrationshandbuch

Datum: 2009-10-09 17:08 UTC

Die in dieser Dokumentation enthaltenen Angaben und Daten können ohne vorherige Ankündigung geändert werden. Die in den Beispielen verwendeten Namen und Daten sind frei erfunden, soweit nichts anderes angegeben ist. Ohne ausdrückliche schriftliche Erlaubnis der Astaro AG darf kein Teil dieser Unterlagen für irgendwelche Zwecke vervielfältigt oder übertragen werden, unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln, elektronisch oder mechanisch, dies geschieht.

© 2009 Astaro AG. Alle Rechte vorbehalten.

An der RaumFabrik 33a, 76227 Karlsruhe

<http://www.astaro.com>

Astaro Security Gateway und WebAdmin sind Markenzeichen der Astaro AG. Linux ist ein Markenzeichen von Linus Torvalds. Alle weiteren Markenzeichen stehen ausschließlich den jeweiligen Inhabern zu.

Einschränkung der Gewährleistung

Für die Richtigkeit des Inhalts dieses Handbuchs wird keine Garantie übernommen. Hinweise auf Fehler und Verbesserungen nehmen wir gerne unter der E-Mail-Adresse documentation@astaro.com entgegen.

Inhaltsverzeichnis

1	Installation	1
	Empfohlene Lektüre	1
	Hardware-Anforderungen	2
	USV-Unterstützung	3
	RAID-Unterstützung	4
	Installationsanleitung	4
	Grundkonfiguration	8
	Backup-Wiederherstellung	14
2	WebAdmin	15
	WebAdmin-Menü	16
	Symbolleiste	17
	Listen	17
	Dialogfenster	18
	Schaltflächen und Symbole	19
	Objektleisten	19
3	Dashboard	23
4	Verwaltung	27
	Systemeinstellungen	28
	Organisatorisches	28
	Rechnername	28
	Zeit und Datum	28
	Shell-Zugriff	31
	Zurücksetzung	31
	WebAdmin-Einstellungen	33
	Allgemein	33
	Zugriffskontrolle	33
	Sicherheit	34
	HTTPS-Zertifikat	35
	Benutzereinstellungen	36
	Lizenzen	37
	OnDemand Lizenzen	39
	Klassische Lizenzen	41
	Übersicht	42
	Installation	43
	Aktive IP-Adressen	44
	Up2Date	45

Übersicht	45
Konfiguration	48
Erweitert	49
Backups	50
Backup/Wiederherstellen	50
Automatische Backups	52
V6 Backup-Import	53
Benutzerportal	55
Allgemein	57
Erweitert	58
Benachrichtigungen	59
Allgemein	59
Benachrichtigungen	60
Erweitert	60
Anpassung	61
Allgemein	61
HTTP/S-Proxy	63
Download-Verwaltung	64
SMTP-/POP3-Proxy	64
SNMP	66
Anfrage	67
Traps	69
Zentralverwaltung	70
Astaro Command Center	70
Einrichtung von ACC V2.0	71
Einrichtung von ACC V1.4	72
ACC-Objekte	74
Live-Protokoll	76
Hochverfügbarkeit	76
Hardware- und Software-Anforderungen	78
Status	78
Systemstatus	80
Konfiguration	81
Ausschalten/Neustart	88
5 Benutzer	89
Benutzer	89
Gruppen	92
Authentifizierung	95
Allgemein	95
Server	97

	eDirectory	97
	Active Directory	100
	LDAP	103
	RADIUS	106
	TACACS	109
	Single Sign-On	110
	Erweitert	112
6	Definitionen	115
	Netzwerke	115
	Dienste	119
	Zeitereignisse	122
7	Netzwerk	125
	Schnittstellen	125
	Schnittstellen	126
	Automatische Netzwerkschnittstellen-Definitionen	127
	Arten von Schnittstellen	128
	Standard-Ethernet	129
	Ethernet-VLAN	131
	Kabelmodem (DHCP)	133
	DSL (PPPoE)	135
	DSL (PPPoA/PPTP)	137
	Modem (PPP)	139
	Zusätzliche Adressen	141
	Linkbündelung	142
	Uplink-Ausgleich	144
	Multipfadregeln	146
	Hardware	148
	Bridging	149
	Status	149
	Erweitert	151
	Statisches Routing	152
	Statische Routen	152
	Richtlinienrouten	154
	Dynamisches Routing (OSPF)	155
	Allgemein	156
	Schnittstellen	157
	Bereich	159
	Prüfsummen	161
	Fehlersuche	162

Erweitert	163
Dienstqualität (QoS)	163
Status	164
Verkehrskennzeichner	165
Bandbreiten-Pools	167
Multicast Routing (PIM-SM)	169
Allgemein	170
Schnittstellen	171
RP-Router	172
Routen	173
Erweitert	175
8 Netzwerkdienste	177
DNS	177
Allgemein	177
Weiterleitung	178
Anfragerouten	178
Statische Einträge	179
DynDNS	180
DHCP	182
Server	183
Relay	184
Statische MAC/IP-Zuordnungen	185
Lease-Tabelle	186
NTP	188
9 Network Security	189
Paketfilter	189
Regeln	190
ICMP	193
Erweitert	195
NAT	198
Maskierung	199
DNAT/SNAT	200
Angriffsschutz	203
Allgemein	203
Angriffsmuster	204
Anti-DoS/Flooding	207
Anti-Portscan	209
Ausnahmen	211
Erweitert	213

Server-Lastverteilung	215
Verteilungsregeln	215
Erweitert	217
Generischer Proxy	217
SOCKS-Proxy	218
IDENT-Reverse-Proxy	219
10 Web Security	221
HTTP/S	222
Allgemein	222
Antivirus/Schadsoftware	226
URL-Filterung	228
URL-Filterkategorien	231
Ausnahmen	232
Erweitert	235
HTTPS-CAs	238
HTTP/S-Profile	243
Übersicht	243
Proxy-Profile	244
Filterzuweisungen	249
Filteraktionen	250
FTP	253
Allgemein	253
Antivirus	255
Ausnahmen	256
Erweitert	257
11 Mail Security	259
SMTP	259
Allgemein	260
Routing	261
Antivirus	263
Antispam	268
Ausnahmen	275
Relaying	277
Erweitert	279
SMTP-Profile	282
POP3	288
Allgemein	288
Antivirus	289
Antispam	291

Ausnahmen	293
Erweitert	295
Verschlüsselung	299
Allgemein	303
Optionen	305
Interne Benutzer	306
S/MIME-Instanzen	309
S/MIME-Zertifikate	311
OpenPGP-Schlüssel	312
Quarantänebericht	314
Allgemein	316
Ausnahmen	317
Erweitert	319
Mail-Manager	321
Mail-Manager-Fenster	322
SMTP/POP3 Quarantine	322
SMTP Spool	325
SMTP Log	326
Allgemein	327
Konfiguration	330
12 VoIP-Sicherheit	331
SIP	331
H.323	332
13 IM/P2P	335
Einstellungen	335
Allgemein	336
Erweitert	336
Sofortnachrichten (IM)	338
Protokolle	338
Ausnahmen	340
Peer-to-Peer (P2P)	341
Protokolle	342
Ausnahmen	343
14 Site-to-Site-VPN	345
IPSec	346
Verbindungen	349
Entfernte Gateways	350
Richtlinien	353
Lokaler RSA-Schlüssel	357

Erweitert	358
Fehlersuche	361
SSL	362
Verbindungen	362
Einstellungen	366
Erweitert	367
Zertifikatverwaltung	369
Zertifikate	369
Zertifizierungsstelle	372
Sperrlisten (CRLs)	374
Erweitert	375
15 Fernzugriff	377
SSL	378
Allgemein	379
Einstellungen	380
Erweitert	382
PPTP	384
Allgemein	384
iPhone	387
Erweitert	388
L2TP über IPSec	388
Allgemein	389
iPhone	392
Erweitert	393
IPSec	394
Verbindungen	397
Richtlinien	399
Erweitert	403
Fehlersuche	406
Cisco VPN Client	406
Allgemein	406
iPhone	408
Fehlersuche	409
Erweitert	410
Zertifikatverwaltung	411
Zertifikate	411
Zertifizierungsstelle	411
Sperrlisten	411
Erweitert	411

16	Protokollierung	413
	Einstellungen	413
	Lokale Protokollierung	413
	Remote-Syslog-Server	415
	Ausgelagerte Protokollarchive	417
	Protokolldatei-Ansicht	419
	Heutige Protokolldateien	419
	Archivierte Protokolldateien	421
	Protokolldateien durchsuchen	422
17	Berichte	423
	Einstellungen	423
	Einstellungen	423
	Ausnahmen	425
	Anonymisierung	425
	Hardware	427
	Täglich	427
	Wöchentlich	428
	Monatlich	429
	Jährlich	429
	Netzwerknutzung	429
	Täglich	429
	Wöchentlich	430
	Monatlich	430
	Jährlich	430
	Netzwerkstatistik	431
	Network Security	432
	Täglich	432
	Wöchentlich	433
	Monatlich	433
	Jährlich	433
	Paketfilter	434
	IPS	434
	Web Security	435
	Internetnutzung	435
	Blockierungen	437
	IM	437
	P2P	437
	Entanonymisierung	438
	Mail Security	439
	Nutzungsdiagramme	439

Mail-Nutzung	439
Blockierte Mails	440
Entanonymisierung	440
Gesamtbericht	441
Bericht anzeigen	441
Archivierte Gesamtberichte	442
Konfiguration	442
18 Support	443
Handbuch	444
Support kontaktieren	444
Tools	445
Ping-Prüfung	445
Traceroute	446
DNS-Lookup	446
Erweitert	448
Prozessliste	448
Lokale Netzwerkverbindungen	448
Routen-Tabelle	448
Schnittstellen-Tabelle	449
Konfig-Abbild	449
REF_ auflösen	449
A Glossar	451
Abbildungsverzeichnis	461

Kapitel 1

Installation

Dieses Kapitel enthält Informationen über die Installation und Konfiguration des Astaro Security Gateways in Ihrem Netzwerk. Die Installation des Astaro Security Gateways erfolgt in zwei Schritten: Erstens, die Installation der Software; zweitens, die Konfiguration von grundlegenden Systemeinstellungen. Die Software-Installation wird mit Hilfe eines konsolen-gestützten Installationsmenüs durchgeführt. Die anschließende Konfiguration erfolgt vom Arbeitsplatzrechner aus über die web-basierte Benutzeroberfläche *WebAdmin*. Bevor Sie mit der Installation beginnen, überprüfen Sie bitte, ob Ihre Hardware den Mindestanforderungen entspricht.

Hinweis – Falls Sie eine Astaro Security Gateway Appliance verwenden, überspringen Sie die folgenden Abschnitte und fahren Sie direkt mit dem Abschnitt Grundkonfiguration fort. Die Astaro Security Gateway Software ist bereits auf allen Appliances vorinstalliert.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- Empfohlene Lektüre
- Hardware-Anforderungen
- Installationsanleitung
- Grundkonfiguration

Empfohlene Lektüre

Die folgenden Dokumente enthalten weitere Informationen zur Installation und Konfiguration der Astaro Security Gateway Appliances. Beide Dokumente sind der Astaro Security Gateway Appliance beigelegt und können alternativ von der Astaro Knowledgebase¹ heruntergeladen werden:

¹ <http://www.astaro.com/kb/>

- Getting Started Guide
- Operating Instructions

Hardware-Anforderungen

Für die Installation und den Betrieb von gelten die folgenden Hardware-Mindestanforderungen:

- **Prozessor:** Pentium 4 mit 1,5 GHz (oder vergleichbar)
- **Speicher:** 1 GB RAM
- **Festplatte:** 20 GB IDE- oder SCSI-Festplattenlaufwerk
- **CD-ROM:** Bootfähiges IDE- oder SCSI-CD-ROM-Laufwerk
- **Netzwerkkarte(n):** Zwei oder mehrere PCI-Ethernet-Netzwerkkarten
- **Netzwerkkarte (optional):** Eine heartbeat-fähige PCI Ethernet-Netzwerkkarte.
In einem hochverfügbaren System (HA) kommunizieren das Primärsystem und das Standby-System mittels eines sogenannten *Heartbeats* miteinander. Dabei handelt es sich um ein Signal, das über eine Netzwerkverbindung zwischen beiden Systemen zyklisch ausgetauscht wird. Falls Sie ein hochverfügbares System einsetzen möchten, stellen Sie sicher, dass beide Geräte mit heartbeat-fähigen Netzwerkkarten ausgestattet sind.
- **USB (optional):** Eine USB-Schnittstelle für die Kommunikation mit einem USV-Gerät, das für eine unterbrechungsfreie Stromversorgung sorgt.
- **Switch (optional):** Ein Gerät, das die Kommunikation in Computernetzwerken steuert.
Stellen Sie sicher, dass der Switch sogenannte *Jumbo Frames* unterstützt.

Astaro führt eine Liste aller Hardware-Produkte, die im Zusammenhang mit Software auf ihre Funktionalität hin getestet wurden. Diese Liste, kurz HCL (*Hardware Compatibility List*), befindet sich auf der Astaro Knowledgebase². Verwenden Sie nur Hardware die explizit dort aufgelistet ist. Die Hardware- und Software-Anforderungen an den Arbeitsplatzrechner für den Zugriff auf die web-basierte Benutzeroberfläche WebAdmin sind wie folgt:

² <http://www.astaro.com/kb/>

- **Prozessor:** Taktfrequenz 1 GHz oder höher
- **Browser:** Firefox 2 (empfohlen) oder Microsoft Internet Explorer 6 oder 7. JavaScript muss aktiviert sein. Darüber hinaus darf im Browser kein Proxy für die interne IP-Adresse (eth0) des konfiguriert sein.

Hinweis – Um Problemen beim Herunterladen von Dateien mit dem Internet Explorer 6 vorzubeugen, fügen Sie die URL der Firewall (z.B. <https://192.168.2.100>) und des Benutzerportals (z.B. <https://192.168.2.100/portal/>) den *Vertrauenswürdigen Sites* hinzu. Beim Internet Explorer 6 befinden sich diese Einstellungen im Menü *Extras >> Internetoptionen >> Sicherheit*. Beim Internet Explorer 7 aktivieren Sie zusätzlich im Fenster *Sicherheitseinstellungen* die Funktion *Automatische Eingabeaufforderung für Dateidownloads*.

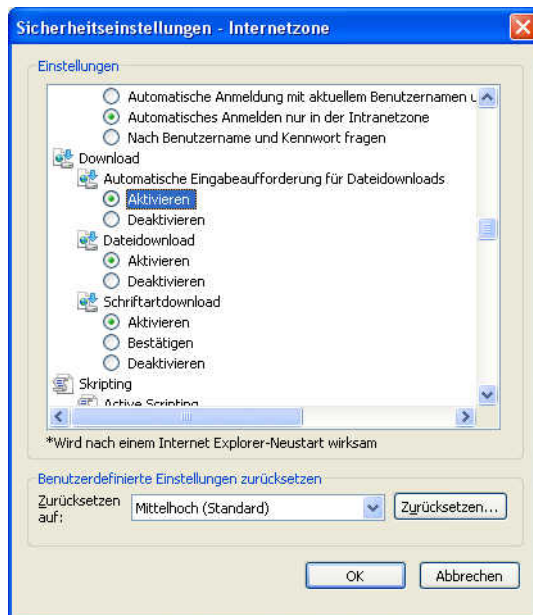


Figure 1.1 IE7 Sicherheitseinstellungen

USV-Unterstützung

Geräte zur unterbrechungsfreien Stromversorgung (USV) gewährleisten eine kontinuierliche Stromversorgung bei Störungen oder Schwankungen der

Stromzufuhr. Astaro Security Gateway unterstützt Geräte der Hersteller MGE UPS Systems und APC. Die Kommunikation zwischen dem USV-Gerät und Astaro Security Gateway erfolgt über die USB-Schnittstelle.

Sobald das USV-Gerät im Batteriebetrieb läuft, wird eine Nachricht an den Administrator geschickt. Falls die Stromunterbrechung für einen längeren Zeitraum andauert und der Batteriestatus des USV-Gerätes einen kritischen Wert erreicht, wird eine weitere Nachricht verschickt. Astaro Security Gateway fährt anschließend kontrolliert herunter und schaltet sich automatisch ab.

Hinweis – Informationen darüber wie Sie Astaro Security Gateway an Ihrem USV-Gerät anschließen können, erfahren Sie in der Bedienungsanleitung des USV-Gerätes. Astaro Security Gateway erkennt das an der USB-Schnittstelle angeschlossene USV-Gerät während des Systemstarts. Starten Sie das Astaro Security Gateway daher erst, nachdem Sie sie mit dem USV-Gerät verbunden haben.

RAID-Unterstützung

Ein RAID-System (*Redundant Array of Independent Disks*) ist ein Datenspeicherungsschema zwischen mehreren physikalischen Festplatten, die als ein einziges logisches Laufwerk organisiert sind. Um sicherzustellen, dass das RAID-System erkannt und korrekt auf dem *Dashboard* der Benutzeroberfläche WebAdmin angezeigt wird, benötigen Sie einen RAID-Controller, der von Astaro Security Gateway unterstützt wird. Auf der *Hardware Compatibility List* können Sie nachsehen welche RAID-Controller kompatibel sind. Die HCL befindet sich auf der Astaro Knowledgebase³ (verwenden Sie „HCL“ als Suchbegriff).

Installationsanleitung

In diesem Abschnitt wird die Installation der Astaro Security Gateway Software anhand einer Schritt-für-Schritt-Anleitung beschrieben. Bevor Sie mit der Installation beginnen, halten Sie die folgenden Komponenten bereit:

- Astaro Security Gateway Installations-CD
- Astaro Security Gateway Lizenz

³ <http://www.astaro.com/kb/>

Das Installationsprogramm überprüft zunächst die Hardware und installiert dann die Software auf Ihrem System.

Warnung – Alle Daten auf der Festplatte werden gelöscht.

1. Booten Sie den PC von der CD-ROM:

Wählen Sie den passenden Installationsmodus für Ihren Rechner aus. Es stehen drei vorkompilierte Kernel-Varianten zur Auswahl:

- **default:** Kernel für Systeme mit einem oder mehreren Prozessoren (SMP – *Symmetric Multiprocessing*).
- **nosmp:** Kernel für Systeme mit einem Prozessor – bootet ohne SMP-Unterstützung, d.h. mehrere CPUs werden nicht unterstützt.
- **classic:** Kernel für Systeme mit einem Prozessor, bei dem die Unterstützung für SMP, APIC (*Advanced Programmable Interrupt Controller*) und ACPI (*Advanced Configuration and Power Interface*) deaktiviert ist. Da in älteren Hardware-Komponenten APIC und ACPI häufig nicht unterstützt werden, empfehlen wir in diesem Fall die Verwendung des Classic-Kernels.

2. Tastenfunktionen während der Installation:

Die Navigation im Installationsmenü erfolgt über die nachfolgenden Tasten. Beachten Sie während der Installation auch die zusätzlichen Tastenfunktionen, die in der türkisfarbenen Fußleiste angezeigt werden:

- **Esc-Taste:** Abbruch der Installation.
- **Pfeiltasten:** Navigation in den Texten, z. B. in den Lizenzbestimmungen und zur Auswahl des Tastatur-Layouts.
- **Tabulator-Taste:** Wechseln zwischen den Text- und Eingabefeldern sowie den Schaltflächen.
- **Enter-Taste:** Die Eingabe wird bestätigt und es wird zum nächsten Punkt gesprungen.

Nachdem Sie eine Installationsart gewählt haben, bestätigen Sie die anschließende Sicherheitsabfrage durch einen Klick auf die F8-Taste.

3. Bestätigen Sie die Software-Installation.

Drücken Sie F8, um die mitgelieferte Software zu installieren, oder Esc, um die Installation abzubrechen.

4. Wählen Sie Ihr Tastatur-Layout:

Wählen Sie mit den Pfeiltasten das Tastatur-Layout aus und bestätigen Sie dies mit der Enter-Taste.

5. Bestätigen Sie die Hardware-Erkennung:

Die Software prüft die folgenden Hardware-Komponenten:

- Prozessor
- Fabrikat und Größe der Festplatte
- CD-ROM-Laufwerk
- Netzwerkkarten
- IDE- bzw. SCSI-Controller

Falls die vorhandenen Hardware-Ressourcen zur Installation der Software nicht ausreichen, wird die Installation mit einer entsprechenden Fehlermeldung abgebrochen.

6. Wählen Sie Ihre Region.

Wählen Sie mit den Pfeiltasten die Region aus und bestätigen Sie dies mit der Enter-Taste.

7. Wählen Sie Ihre Zeitzone.

Wählen Sie mit den Pfeiltasten die Zeitzone aus und bestätigen Sie dies mit der Enter-Taste.

8. Stellen Sie Datum und Uhrzeit ein.

Tragen Sie in die Eingabefelder das aktuelle Datum und die Uhrzeit ein. Sie können mit der Tabulator-Taste und den Pfeiltasten zwischen den Eingabefeldern wechseln. Ungültige Eingaben werden nicht übernommen. Bestätigen Sie die Eingaben mit der Enter-Taste.

9. Wählen Sie eine interne Netzwerkkarte.

Damit Sie nach der Installation die Astaro Security Gateway mit der Benutzeroberfläche WebAdmin konfigurieren können, müssen Sie eine Netzwerkkarte als interne Netzwerkkarte definieren. Diese Netzwerkkarte ist später die Schnittstelle (eth0) zum internen Netzwerk (LAN). Wählen Sie aus der

verfügbaren Hardware eine Netzwerkkarte aus und bestätigen Sie die Auswahl mit der **Enter**-Taste.

10. Konfigurieren Sie die Netzwerkschnittstelle für die Administration.

Definieren Sie für die ausgewählte Netzwerkkarte eine IP-Adresse, die Netzmaske und das Standardgateway. Die Standardwerte sind:

IP-Adresse: 192.168.2.100

Netzmaske: 255.255.255.0

Gateway: none

Den Wert für das Standardgateway müssen Sie nur ändern, wenn Sie die WebAdmin-Schnittstelle von einem PC aus erreichen möchten, der außerhalb des Netzwerkbereichs liegt. Das Gateway muss dann innerhalb des Netzwerkbereichs liegen.⁴

Bestätigen Sie die Eingaben mit der **Enter**-Taste.

11. Akzeptieren Sie die Installation des *Enterprise Toolkits*.

Sie können beschließen, nur Open-Source-Software zu installieren. Um die volle Funktionalität von Astaro Security Gateway verwenden zu können, sollten Sie jedoch auch das Enterprise Toolkit installieren.

Drücken Sie **Enter**, um beide Softwarepakete zu installieren, oder **Esc**, um nur die Open-Source-Software zu installieren.

12. Bestätigen Sie den Warnhinweis, um die Installation zu starten.

Bitte lesen Sie den Warnhinweis sorgfältig. Nach der Bestätigung werden alle bestehenden Daten auf dem PC gelöscht.

Falls Sie Eingaben ändern möchten, können Sie mit der **F12**-Taste wieder zu Schritt 2 des Installationsmenüs gelangen. Andernfalls starten Sie die Installation der Software mit der **F8**-Taste.

Die Installation der Software kann nun einige Minuten dauern. Sie können den Installationsvorgang mit Hilfe von vier Konsolen verfolgen:

- Installationsroutine (**Alt+F1**)
- Interaktive Bash-Shell (**Alt+F2**)

⁴ Bei der Netzmaske 255.255.255.0 wird das Subnetz durch die ersten drei Werte definiert. In unserem Beispiel lautet der relevante Bereich 192.168.2. Wenn nun Ihr Administrations-PC z. B. die IP-Adresse 192.168.10.5 hat, liegt er nicht im selben Subnetz. In diesem Fall benötigen Sie ein Gateway. Das Gateway muss dann eine Schnittstelle im 192.168.2-Subnetz und eine Verbindung zum Administrations-PC haben. Für unser Beispiel nehmen wir die Adresse: 192.168.2.1

- Protokoll (engl. *Log*) der Installationsroutine (Alt+F3)
- Kernel-Protokoll (engl. *Log*) (Alt+F4)

13. Entnehmen Sie die CD-ROM, verbinden Sie das interne Netzwerk und starten Sie das System neu.

Sobald Sie dazu aufgefordert werden, entnehmen Sie die CD-ROM aus dem Laufwerk und verbinden die Netzwerkkarte `eth0` mit Ihrem lokalen Netzwerk. Mit Ausnahme der internen Netzwerkkarte (`eth0`) wird die Reihenfolge der Netzwerkkarten in erster Linie durch die PCI-ID und die Kernel-Treiber bestimmt. Die Reihenfolge der Netzwerkkartenbenennung kann sich auch später durch Änderung der Hardwarekonfiguration, z. B. durch das Hinzufügen oder Entfernen von Netzwerkkarten ändern. Starten Sie danach Astaro Security Gateway mit der Tastenkombination `Strg+Alt+Entf` oder durch Drücken des `Reset`-Schalters neu. Während des Neustarts werden die IP-Adressen der internen Netzwerkkarten neu gesetzt, daher kann auf der Installationsroutine-Konsole (Alt+F1) für kurze Zeit die Meldung „No IP on eth0“ stehen.

Nachdem Astaro Security Gateway neu gestartet ist (je nach Hardware-Leistung kann dies einige Minuten dauern), sollten Sie mit dem Programm *Ping* die IP-Adresse der internen Netzwerkkarte `eth0` erreichen. Falls keine Verbindung zustande kommt, prüfen Sie Ihr System auf die nachfolgenden möglichen Fehlerquellen:

- Die IP-Adresse von Astaro Security Gateway ist nicht korrekt gesetzt.
- Die IP-Adresse vom Administrations-PC ist nicht korrekt gesetzt.
- Das Standardgateway ist nicht korrekt gesetzt.
- Das Netzkabel ist mit der falschen Netzwerkkarte verbunden.
- Alle Netzwerkkarten sind an einem Hub angeschlossen.

Grundkonfiguration

Der zweite Teil der Installation erfolgt im *WebAdmin*, der web-basierten Benutzeroberfläche von Astaro Security Gateway. Bevor Sie die Grundkonfiguration durchführen, sollten Sie eine Vorstellung davon haben, wie Sie Astaro Security Gateway in Ihr Netzwerk integrieren möchten. Sie müssen entscheiden, welche Funktionen es bereitstellen soll, z. B. ob es im Bridge-Modus oder im

Standard-Modus (Routing) arbeiten soll, oder ob es den Datenpaketfluss zwischen seinen Schnittstellen überwachen soll. Sie können die Konfiguration von Astaro Security Gateway jedoch später jederzeit ändern. Für die nachfolgend beschriebene Grundkonfiguration müssen Sie sich noch nicht auf ein bestimmtes Einsatzszenario festlegen.

1. Starten Sie Ihren Browser und öffnen Sie WebAdmin.

Navigieren Sie zur URL von Astaro Security Gateway, d. h. zur IP-Adresse von eth0. Um bei unserer Beispielkonfiguration zu bleiben, dies ist die URL `https://192.168.2.100:4444` (beachten Sie das HTTPS-Protokoll und die Portnummer 4444).

Beachten Sie, dass abweichend von der betrachteten Beispielkonfiguration alle vorinstallierten Astaro Security Gateway Appliances mit den folgenden Voreinstellungen ausgeliefert werden:

- **Schnittstellen:** Interne Schnittstelle (LAN/eth0)
- **IP-Adresse:** 192.168.0.1
- **Netzmaske:** 255.255.255.0
- **Standardgateway:** none

Um die Benutzeroberfläche WebAdmin zu einer Astaro Security Gateway Appliance zu öffnen, starten Sie Ihren Browser und geben Sie die folgende Adresse ein:

`https://192.168.0.1:4444`

Um Authentifizierung und verschlüsselte Kommunikation zu gewährleisten, wird Astaro Security Gateway mit einem selbstsignierten Sicherheitszertifikat ausgeliefert. Dieses digitale Zertifikat wird dem Browser beim Aufbau der HTTPS-basierten Verbindung zum WebAdmin angeboten. Da der Browser die Gültigkeit dieses Zertifikats nicht überprüfen kann, wird eine Sicherheitswarnung angezeigt. Nachdem Sie das Zertifikat akzeptiert haben, erscheint die initiale Anmeldemaske des WebAdmin.

2. Füllen Sie das Anmeldeformular aus.

Geben Sie die entsprechenden Informationen Ihrer Firma in die Textfelder ein. Bestimmen Sie ein Kennwort und geben Sie eine gültige E-Mail-Adresse für den Administrator ein. Wenn Sie mit den Lizenzbestimmungen einverstanden sind, klicken Sie auf die Schaltfläche *Perform Basic System Setup* um mit dem Anmeldevorgang fortzufahren. Während dieses Vorganges werden einige digitale Zertifikate und CAs (*Certificate Authorities*) erzeugt (letztere werden im Microsoft-Jargon auch *Vertrauenswürdige Stammzertifizierungsstellen* genannt):

The screenshot shows the 'Willkommen im WebAdmin' (Welcome to WebAdmin) window. It contains a 'System-Grundkonfiguration' (System Basic Configuration) section with the following fields:

- Rechnername: [Text input]
- Name der Firma oder Organisation: [Text input]
- Stadt: [Text input]
- Land: [Dropdown menu, currently showing 'Please select']
- Kennwort des **admin**-Kontos: [Text input]
- Kennwort bestätigen: [Text input]
- E-Mail-Adresse des **admin**-Kontos: [Text input]

To the right of these fields, a warning message states: 'Diese Einstellungen müssen vor Inbetriebnahme vorgenommen werden. Bitte beachten Sie, dass ALLE Felder ausgefüllt werden müssen. Melden Sie sich nach Übernahme der Einstellungen mit dem Benutzernamen **admin** und dem unten eingegebenen Kennwort am System an.' (These settings must be made before start-up. Please note that ALL fields must be filled out. Log in after taking over the settings with the username **admin** and the password entered below.)

Below the configuration fields is a scrollable area containing the 'Astaro License Agreement'. It starts with 'IMPORTANT--READ CAREFULLY BEFORE OPERATING THIS SOFTWARE' and 'BY MARKING THE "ACCEPT"-CHECKBOX OR USING THIS SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT...'. It then details the terms of the license agreement between Astaro AG and the user.

At the bottom of the scrollable area, there is a button 'EULA ausdrucken' (Print EULA) and a checkbox 'Ich akzeptiere die Lizenzvereinbarung' (I accept the license agreement). Below the checkbox is a green button with a checkmark and the text 'Grundkonfiguration durchführen' (Perform basic configuration).

Figure 1.2 Initiale Anmeldemaske des WebAdmin

- **WebAdmin CA:** Die CA, mit der das WebAdmin-Zertifikat signiert wird (siehe *Verwaltung >> WebAdmin-Einstellungen >> HTTPS-Zertifikate*).
- **VPN Signing CA:** Die CA, mit der Zertifikate für VPN-Verbindungen signiert werden (siehe *Site-to-Site-VPN >> Zertifikatverwaltung >> Zertifizierungsstelle*).
- **WebAdmin Server-Zertifikat:** Das digitale Zertifikat des WebAdmin (siehe *Site-to-Site-VPN >> Zertifikatverwaltung >> Zertifikate*).
- **Lokales X.509-Zertifikat:** Das digitale Zertifikat der Astaro Security Gateway, das für VPN-Verbindungen verwendet werden kann (siehe *Site-to-Site-VPN >> Zertifikatverwaltung >> Zertifikate*).

Die Anmeldeseite erscheint. (Bei einigen Browsern kann es passieren, dass Sie eine weitere Sicherheitswarnung sehen, weil sich das Zertifikat entsprechend Ihren Angaben geändert hat.)

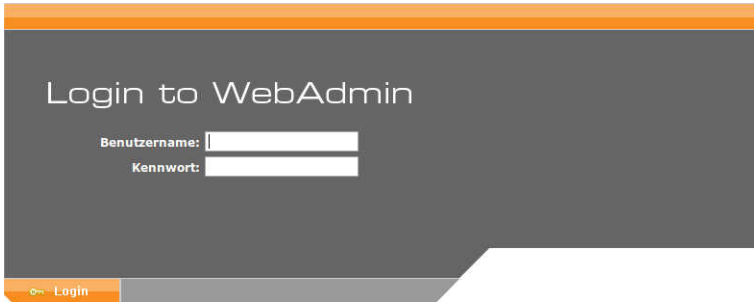


Figure 1.3 Reguläre Anmeldemaske des WebAdmin

3. Melden Sie sich am WebAdmin an.

Geben Sie in das Feld *Username* den String *admin* und in das Feld *Password* das Kennwort ein. Das Kennwort haben Sie in der vorherigen Maske festgelegt.

Ihnen wird nun ein Konfigurationsassistent angezeigt, der Sie durch den ersten Konfigurationsprozess leitet. Führen Sie die Schritte aus, um die Grundeinstellungen von Astaro Security Gateway vorzunehmen.

Falls Sie über eine Backupdatei verfügen, können Sie stattdessen auch das Backup wiederherstellen (lesen Sie dazu den Abschnitt Backup-Wiederherstellung). Alternativ können Sie auch bedenkenlos *Cancel* klicken (in jedem Schritt des Assistenten) und dadurch den Assistenten abbrechen, z. B. wenn Sie die Konfiguration des Astaro Security Gateway lieber direkt im WebAdmin vornehmen möchten. Sie können auch jederzeit *Finish* klicken, dann werden alle bis dahin vorgenommenen Einstellungen übernommen und der Assistent beendet.

4. Installieren Sie Ihre Lizenz.

Klicken Sie auf das Ordnersymbol um Ihre erworbene Lizenz (eine Textdatei) hochzuladen. Klicken Sie *Next*, um die Lizenz zu installieren.

Falls Sie keine Lizenz erworben haben, klicken Sie *Next*, um die 30-Tage-Evaluationslizenz zu verwenden, bei der alle Produktmerkmale aktiviert sind. Die Evaluationslizenz wird mit dem Astaro Security Gateway ausgeliefert.

5. Konfigurieren Sie die interne Netzwerkkarte.

Überprüfen Sie die Einstellungen für die interne Netzwerkkarte (*eth0*). Die vorliegenden Einstellungen resultieren aus den Informationen, die Sie während der Installation der Software eingegeben haben. Zusätzlich können Sie

das Astaro Security Gateway so einrichten, dass es auf der internen Netzwerkkarte als DHCP-Server fungiert. Markieren Sie dafür das entsprechende Auswahlkästchen.

Hinweis – Wenn Sie die IP-Adresse der internen Netzwerkkarte (eth0) ändern, müssen Sie sich mit der neuen IP-Adresse erneut am WebAdmin anmelden.

6. Wählen Sie den Uplink-Typ für die externe Netzwerkkarte.

Wählen Sie die Art der Verbindung Ihrer Uplink-/Internetverbindung, die die externe Netzwerkkarte verwenden wird. Die Art der Schnittstelle und ihre Konfiguration hängen davon ab, welche Art der Internetverbindung Sie verwenden werden. Klicken Sie danach *Next*.

Falls das Astaro Security Gateway über keinen Uplink verfügt oder Sie diesen jetzt noch nicht konfigurieren möchten, lassen Sie das Feld *Internet Uplink Type* leer. Falls Sie einen Internetuplink konfigurieren, wird IP-Maskierung automatisch für alle Verbindungen aus dem internen Netzwerk ins Internet konfiguriert.

Wenn Sie *Standard Ethernet Interface with Static IP Address* (Standard-Ethernetschnittstelle mit statischer IP-Adresse) auswählen, ist ein *Default Gateway* (Standardgateway) nur optional anzugeben. Wenn Sie das Textfeld leer lassen, bleibt Ihre Standardgateway-Einstellung aus der Installationsroutine erhalten.

Sie können jeden der folgenden Schritte überspringen, indem Sie *Next* klicken. Diese übergangenen Einstellungen können Sie dann später im WebAdmin vornehmen oder ändern.

7. Legen Sie die grundlegenden Firewallereinstellungen fest.

Hier können Sie auswählen, welche Arten von Diensten Sie für das Internet zulassen wollen. Klicken Sie *Next*, um Ihre Einstellungen zu bestätigen.

8. Legen Sie die grundlegenden Angriffsschutzeinstellungen fest.

Hier können Sie Einstellungen festlegen, die den Angriffsschutz verschiedener Betriebssysteme und Datenbanken betreffen. Klicken Sie *Next*, um Ihre Einstellungen zu bestätigen.

9. Legen Sie die Einstellungen für Sofortnachrichten und P2P fest.

Hier können Sie festlegen, welche Nachrichten- und Peer-to-Peer-Protokolle blockiert werden sollen. Klicken Sie *Next*, um Ihre Einstellungen zu bestätigen.

10. Legen Sie die Einstellungen zur Internetsicherheit fest.

Hier können Sie festlegen, ob Internetverkehr nach Viren und Spionagesoftware gescannt werden soll. Darüber hinaus können Sie Webseiten bestimmter Kategorien blockieren lassen. Klicken Sie *Next*, um Ihre Einstellungen zu bestätigen.

11. Legen Sie die Einstellungen zur E-Mail-Sicherheit fest.

Hier können Sie das erste Auswahlkästchen markieren, um den POP3-Proxy zu aktivieren. Wenn Sie das zweite Auswahlkästchen markieren, fungiert das ASG als SMTP-Relay für eingehende Mails: Geben Sie die IP-Adresse Ihres internen Mailservers an und fügen Sie SMTP-Domänen hinzu, die geroutet werden sollen. Klicken Sie *Next*, um Ihre Einstellungen zu bestätigen.

12. Bestätigen Sie Ihre Einstellungen.

Es wird Ihnen eine Aufstellung der vorgenommenen Einstellungen angezeigt. Klicken Sie *Finish*, um sie zu bestätigen oder *Back*, um sie zu ändern. Sie können die Einstellungen jedoch auch später im WebAdmin ändern. Nachdem Sie *Finish* geklickt haben, erscheint das Dashboard von WebAdmin, das Sie auf einen Blick über den aktuellen Systemstatus des Astaro Security Gateway informiert.

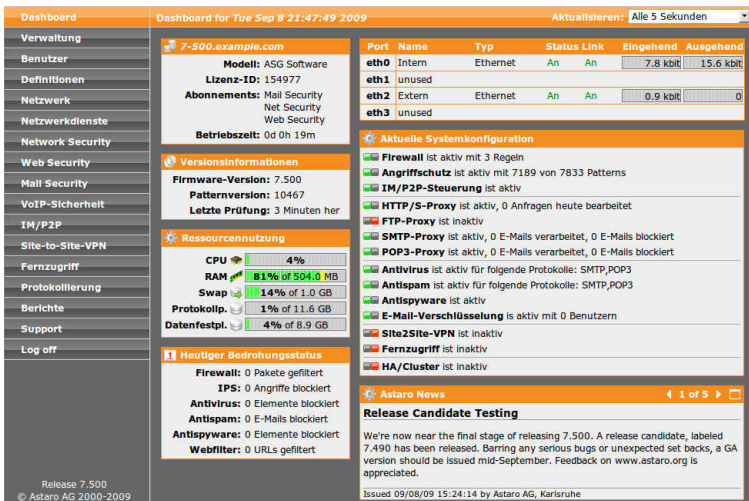


Figure 1.4 WebAdmin-Dashboard

Falls Sie bei einzelnen Schritten des Assistenten auf Probleme stoßen, wenden Sie sich bitte an die Support-Abteilung Ihres Astaro-Vertriebspartners. Weitergehende Informationen finden Sie auf den folgenden Webseiten:

- Astaro Bulletin Board⁵
- Astaro Knowledgebase⁶

Backup-Wiederherstellung

Der Konfigurationsassistent von WebAdmin (siehe Grundkonfiguration) ermöglicht es Ihnen, eine vorhandene Backupdatei wiederherzustellen, anstatt die Grundkonfiguration durchzuführen. Gehen Sie dazu folgendermaßen vor:

1. **Wählen Sie *Restore existing backup file* im Konfigurationsassistenten.**
Wählen Sie *Restore existing backup file* im Konfigurationsassistenten und klicken Sie *Next*.
Sie werden zu der Seite weitergeleitet, wo Sie die Datei hochladen können.
2. **Laden Sie das Backup hoch.**
Klicken Sie auf das Ordnersymbol, wählen Sie die Backupdatei aus, die Sie wiederherstellen möchten, und klicken Sie *Start Upload*.
3. **Stellen Sie das Backup wieder her.**
Klicken Sie *Finish*, um das Backup wiederherzustellen.

Wichtiger Hinweis – Danach ist es nicht mehr möglich, den Konfigurationsassistenten erneut aufzurufen.

Sobald das Backup wiederhergestellt wurde, werden Sie auf die Anmeldeseite weitergeleitet.

⁵ <http://www.astaro.org/>

⁶ <http://www.astaro.com/kb/>

WebAdmin

WebAdmin ist die web-basierte grafische Benutzeroberfläche zur vollständigen Administration von Astaro Security Gateway. WebAdmin besteht aus einem Menü und mehreren Seiten, von denen manche wiederum mehrere Registerkarten (engl. *tabs*) besitzen. Das Menü auf der linken Seite orientiert sich an den Produktmerkmalen von Astaro Security Gateway. Sobald Sie auf einen Menüpunkt wie z. B. *Netzwerk* klicken, öffnet sich ein Untermenü und die entsprechende Seite wird angezeigt. Beachten Sie, dass für einige Menüpunkte keine eigene Seite vorhanden ist. In diesem Fall wird weiterhin die zuvor ausgewählte Seite angezeigt. Erst wenn Sie ein Untermenü anklicken, öffnet sich die dazugehörige Seite, und zwar mit der ersten Registerkarte.

Die Anleitungen in diesem Administrationshandbuch leiten Sie zu einer Seite durch die Angabe des Menüs, Untermenüs, und der Registerkarte, z. B.: Auf der Registerkarte *Netzwerk* >> *Schnittstellen* >> *Hardware* werden ...

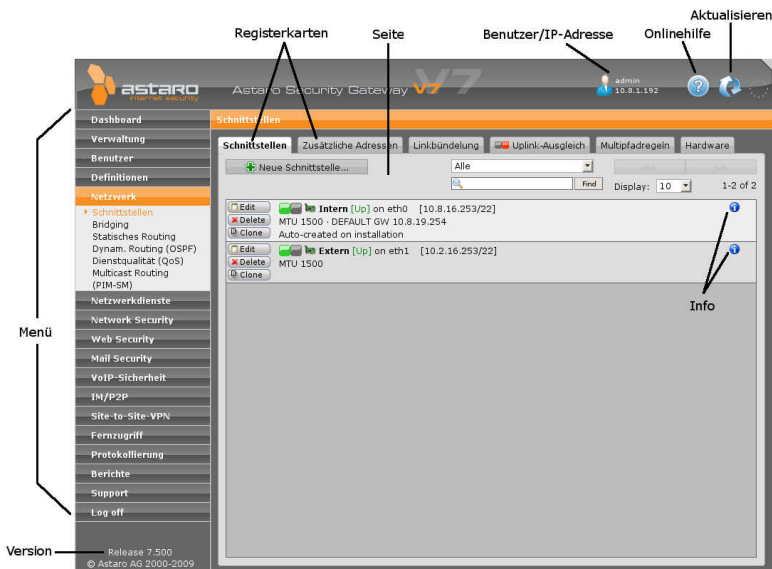


Figure 2.1 WebAdmin: Übersicht

WebAdmin-Menü

Das WebAdmin-Menü gibt Ihnen Zugriff auf alle Konfigurationsoptionen von Astaro Security Gateway. Die Verwendung einer Kommandozeile zur Konfiguration ist daher nicht erforderlich.

- **Dashboard:** Das Dashboard zeigt eine grafische Momentaufnahme des Betriebsstatus' von Astaro Security Gateway.
- **Verwaltung:** In diesem Menü werden grundlegende Einstellungen für das Gesamtsystem und den WebAdmin vorgenommen.
- **Benutzer:** Neben der Konfiguration von Benutzern und Benutzergruppen werden in diesem Menü externe Authentifizierungsserver angelegt.
- **Definitionen:** Hier werden Netzwerk- und Dienst-Definitionen sowie einzelne oder periodisch wiederkehrende Zeitereignisse (engl. *time events*) angelegt.
- **Netzwerk:** Dieses Menü enthält u.a. die Konfiguration von Netzwerkkarten und Routing-Optionen.
- **Netzwerkdienste:** Konfiguration von Netzwerkdiensten wie DNS und DHCP.
- **Network Security:** Konfiguration von grundlegenden Netzwerksicherheitsmerkmalen wie zum Beispiel Paketfilterregeln sowie Einstellungen für das Angriffsschutzsystem (engl. *intrusion protection*).
- **Web Security:** Konfiguration des HTTP/S- und FTP-Proxy von Astaro Security Gateway.
- **Mail Security:** Konfiguration des SMTP- und POP3-Proxy von Astaro Security Gateway sowie E-Mail-Verschlüsselung.
- **VoIP-Sicherheit:** Mithilfe dieses Menüs können Sie den VoIP-Datenverkehr kontrollieren.
- **IM/P2P:** Mithilfe dieses Menüs können Sie Sofortnachricht- (engl. *Instant Messaging*) und P2P-Datenverkehr kontrollieren.
- **Site-to-Site-VPN:** Konfiguration von Site-to-Site Virtual Private Networks (virtuelle private Netzwerke).

- **Fernzugriff:** In diesem Menü wird Astaro Security Gateway für den Einsatz in VPNs mit Fernzugriff (engl. *remote access*) konfiguriert.
- **Protokollierung:** Hier werden Einstellungen zur Protokollierung (engl. *logging*) vorgenommen. Darüber hinaus können Sie einzelne Protokollmeldungen verfolgen.
- **Berichte:** Anzeige von Nutzungsstatistiken.
- **Support:** Hier finden Sie verschiedene Hilfsmittel zur Fehlersuche.
- **Abmelden:** Abmelden vom WebAdmin.

Symbolleiste

Die Symbole in oberen rechten Ecke des WebAdmin haben folgende Bedeutung:

- **Benutzer/IP-Adresse:** Zeigt den aktuell angemeldeten Benutzer und die IP-Adresse an, von der aus auf den WebAdmin zugegriffen wird.
- **Onlinehilfe:** Jedes Menü, Untermenü, und jede Registerkarte verfügt über eine kontext-sensitive Onlinehilfe, die Informationen und Anleitungen zu der jeweils geöffneten Seite im WebAdmin enthält.

Hinweis – Die Onlinehilfe wird mithilfe von sogenannten Pattern-Updates aktualisiert und beschreibt stets die aktuelle Version von Astaro Security Gateway. Dies kann zu kleineren Abweichungen zwischen der Onlinehilfe und der tatsächlich installierten Firmware führen.

- **Aktualisieren:** Klicken Sie stets auf das Aktualisieren-Symbol, um eine Seite im WebAdmin zu aktualisieren.
-

Hinweis – Verwenden Sie nicht die Neuladen-Funktion des Browsers, da Sie in diesem Fall automatisch vom WebAdmin abgemeldet werden.

Listen

Viele Seiten im WebAdmin bestehen aus Listen. Mit den Schaltflächen *Bearbeiten* und *Löschen* können Sie einen Listeneintrag bearbeiten oder löschen.

Zum Erzeugen eines neuen Listeneintrags klicken Sie die Schaltfläche *Neue ...* (wobei „...“ als Platzhalter für das zu erstellende Listenobjekt steht, z. B. Schnittstelle). Dies öffnet ein Dialogfenster, in welchem Sie die Eigenschaften des Objektes festlegen können.

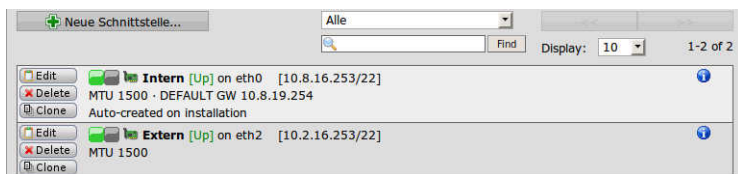


Figure 2.2 WebAdmin: Beispiel einer Liste

In jeder Liste können Sie die einzelnen Einträge nach ihrem Typ sortieren. Mit der Suchfunktion können Sie darüber hinaus gezielt nach Einträgen suchen. Geben Sie dazu einen Suchbegriff ein und klicken Sie auf *Finden*.

Beachten Sie, dass Listen mit mehr als zehn Einträgen auf mehrere Seiten aufgeteilt sind. Mit den Schaltflächen *Nächste* (>>) und *Vorherige* (<<) können Sie zwischen den Seiten hin- und herschalten.

Tipp – Wenn Sie auf das Info-Symbol eines Listeneintrags klicken, können Sie sehen, in welchen Konfigurationen das Objekt noch verwendet wird.

Dialogfenster

Dialogfenster sind spezielle Eingabemasken. Das Beispiel zeigt ein Dialogfenster für das Erzeugen einer statischen Route im Menü *Netzwerk >> Statisches Routing*.

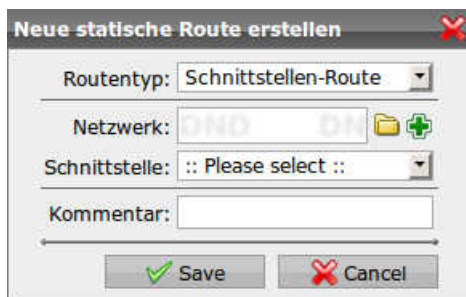


Figure 2.3 WebAdmin: Beispiel eines Dialogfensters

Jedes Dialogfenster kann aus verschiedenen Kontrollelementen (engl. *widgets*) wie zum Beispiel Textfeldern oder Auswahlkästchen (engl. *checkboxes*) bestehen. Viele Dialogfenster bieten darüber hinaus eine *Drag&Drop*-Funktionalität, die durch einen speziellen Hintergrund mit dem Schriftzug „DND“ gekennzeichnet sind. Immer dann, wenn Sie ein solches Feld vorfinden, können Sie ein Objekt durch Ziehen und Fallenlassen mit der Maus (*drag and drop*) in dieses Feld ziehen. Um das Fenster zu öffnen, von dem aus Sie das Objekt in das Feld ziehen möchten, klicken Sie auf das gelbe Ordnersymbol oben rechts am Eingabefeld. Abhängig von der jeweiligen Konfigurationsoption öffnet sich die Liste der verfügbaren Netzwerk-, Dienst- oder Zeitereignisdefinitionen. Ein Klick auf das grüne Plussymbol öffnet ein zweites Dialogfenster, in welchem Sie eine neue Definition anlegen können. Einige Kontrollelemente, die für eine bestimmte Konfiguration nicht benötigt werden, erscheinen ausgegraut. In manchen Fällen können diese durchaus editiert werden, haben dann allerdings keinen Effekt.

Note – Im WebAdmin gibt es u.a. die Schaltflächen *Speichern* und *Übernehmen*. Die Schaltfläche *Speichern* wird immer dann angezeigt, wenn Sie ein Objekt im WebAdmin erzeugen, zum Beispiel, wenn Sie eine neue statische Route anlegen oder eine Netzwerk-Definition bearbeiten. Jede Schaltfläche *Speichern* wird von einer Schaltfläche *Abbrechen* begleitet. *Übernehmen*-Schaltflächen hingegen dienen dazu, Ihre Einstellungen in das Backend zu übertragen und somit wirksam werden zu lassen.

Schaltflächen und Symbole

WebAdmin verfügt über einige Schaltflächen und Symbole mit hinterlegter Funktion, deren Nutzung hier beschrieben wird.

Objektleisten

Eine Objektleiste (auch *Group Tooltip*) ist eine Liste von Objekten die gelegentlich auf der linken Seite von WebAdmin eingeblendet wird und dabei vorübergehend das Hauptmenü verdeckt. Aus dieser Objektleiste können mittels „Drag and Drop“ (Ziehen und Loslassen) Objekte ausgewählt werden.

Die Objektleiste wird automatisch geöffnet, wenn Sie auf das Ordnersymbol klicken (siehe Abschnitt oben). Sie kann auch manuell über ein Tastaturkürzel

Schaltflächen

-  **View** Zeigt ein Dialogfenster mit detaillierten Informationen zu dem Objekt.
-  **Edit** Öffnet ein Dialogfenster, wo die Eigenschaften des Objekts bearbeitet werden können.
-  **Delete** Löscht das Objekt. Es wird eine Warnung ausgegeben, wenn ein Objekt noch irgendwo anders benutzt wird. Nicht alle Objekte können gelöscht werden, wenn sie in Benutzung sind.
-  **Clone** Öffnet ein Dialogfenster, um ein Objekt mit identischen Einstellungen/Eigenschaften anzulegen. Klonen dient dazu, ähnliche Objekte anzulegen ohne alle identischen Einstellungen erneut eingeben zu müssen.

geöffnet werden (siehe *Verwaltung >> WebAdmin-Einstellungen >> Benutzereinstellungen*).

Die Objektleisten ermöglichen einen schnellen Zugriff auf WebAdmin-Objekte wie Benutzer/Gruppen, Schnittstellen, Netzwerke und Dienste, um sie für Konfigurationszwecke auswählen zu können. Objekte werden ausgewählt, indem sie einfach zur aktuellen Konfiguration gezogen und dort über dem entsprechenden Feld fallen gelassen werden (Drag and Drop).

Es gibt fünf verschiedene Arten von Objektleisten, entsprechend zu den Objekttypen, die es gibt. Bei einem Klick auf das Ordnersymbol wird immer die Objektleiste geöffnet, deren Typ von der aktuellen Konfiguration benötigt wird.

Symbole mit Funktion

-  **Info:** Zeigt alle Konfigurationen an, in denen das Objekt benutzt wird.
-  **Statusampel:** Aktiviert oder deaktiviert eine Funktion. Sie zeigt grün, wenn die Funktion aktiv ist, rot, wenn die Funktion deaktiviert ist, und gelb, wenn eine Konfigurierung nötig ist, bevor die Funktion aktiviert werden kann.
-  **Ordner:** Dieses Symbol hat zwei Funktionen: (1) Öffnet eine Objektleiste (siehe Abschnitt unten) auf der linken Seite, aus der Sie passende Objekte auswählen können. (2) Öffnet ein Dialogfenster, um eine Datei hochzuladen.
-  **Plus:** Öffnet ein Dialogfenster, um ein neues Objekt des erforderlichen Typs hinzufügen.
-  **Papierkorb:** Entfernt ein Objekt aus der aktuellen Konfiguration, ohne das Objekt selbst zu löschen.
-  **Import:** Öffnet ein Dialogfenster, um Text mit mehr als einem Eintrag bzw. mehr als einer Zeile zu importieren. Diese Funktion erleichtert das Hinzufügen von mehreren Einträgen auf einmal ohne diese einzeln eingeben zu müssen, z. B. einer langen Blacklist zur URL-Blacklist. Kopieren Sie den Text dazu einfach von irgendwoher und fügen Sie ihn mittels CTRL+V ein.
-  **Export:** Opens a dialog window to export all existing items. You can select a delimiter to separate the items, which can either be new line, colon, or comma. To export the items as text, mark the whole text in the *Exported Text* field and press CTRL+C to copy it. You can then paste it into all common applications using CTRL+V, for example a text editor.
-  **Sortieren:** Verwenden Sie diese beiden Pfeile, um Listenelemente zu sortieren, indem Sie sie durch Klicken auf den jeweiligen Pfeil nach oben bzw. unten verschieben.
-  **PDF:** Speichert die aktuelle Ansicht der Daten in einer PDF-Datei ab und öffnet anschließend ein Dialogfenster, um die erzeugte Datei herunterzuladen.
-  **CSV:** Speichert die aktuelle Ansicht der Daten in einer CSV-Datei (komma-separierte Werte) ab und öffnet anschließend ein Dialogfenster, um die erzeugte Datei herunterzuladen.

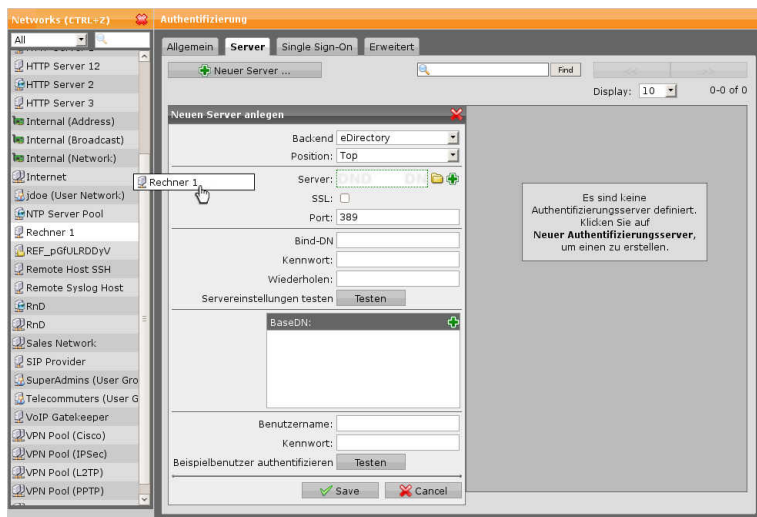


Figure 2.4 WebAdmin: Ziehen eines Objekts aus der Objektleiste *Networks*

Dashboard

Das Dashboard von Astaro Security Gateway ist eine grafisch aufbereitete Momentaufnahme von wichtigen Systemparametern. In der Voreinstellung wird das Dashboard alle fünf Sekunden aktualisiert. Das Zeitintervall für die Aktualisierung kann von *Nie* (keine Aktualisierung) bis zu 60 Sekunden eingestellt werden.

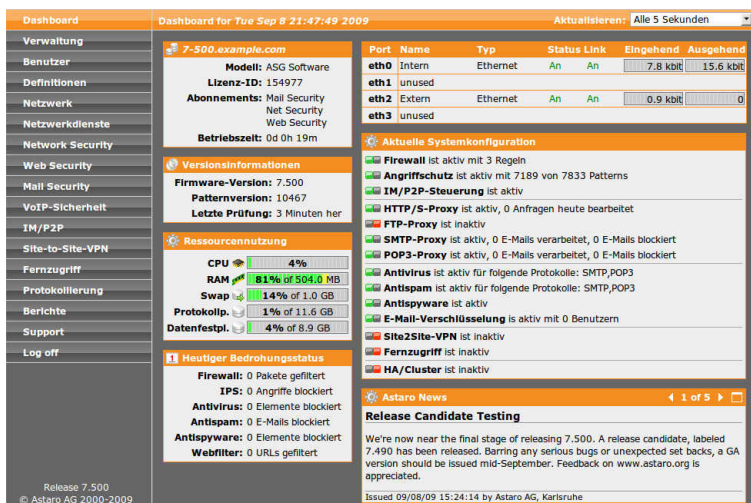


Figure 3.1 WebAdmin: Beispielhafte Dashboard-Anzeige der ASG Software V7 WebAdmin

Das Dashboard erscheint standardmäßig nach der Anmeldung am WebAdmin und stellt die folgenden Informationen zur Verfügung:

- **Allgemeine Informationen:** Rechnernamen, Modell, Lizenz-ID und die Zeitspanne, die das Gerät in Betrieb ist.
- **Versionsinformationen:** Versionsnummern der aktuell installierten Firmware und Patterns sowie verfügbare Updates.
- **Ressourcennutzung:** Aktuelle Systemauslastung, insbesondere der folgenden Komponenten:

- Prozessorauslastung in Prozent
- Speicherauslastung in Prozent
- Der von der Swap-Partition verbrauchte Festplattenplatz in Prozent
- Der von der Protokoll-Partition (engl. *log partition*) verbrauchte Festplattenplatz in Prozent
- Der von der Daten-Partition verbrauchte Festplattenplatz in Prozent
- Der Status des USV-Gerätes (falls vorhanden)
- **Heutiger Bedrohungsstatus:** Ein Zähler für die wichtigsten registrierten Bedrohungen seit Mitternacht:
 - Die Summe an Datenpaketen, die vom Paketfilter verworfen (engl. *drop*) oder abgelehnt (engl. *reject*) wurden und für die Protokollierung aktiviert ist
 - Die Gesamtanzahl der blockierten Angriffe und Eindringversuche (engl. *intrusion*) in das Netzwerk
 - Die Gesamtanzahl der blockierten Viren (alle Proxies)
 - Die Gesamtanzahl der blockierten Spam-Nachrichten (SMTP/POP3)
 - Die Gesamtanzahl blockierter Spyware-Kommunikation
 - Die Gesamtanzahl an blockierten URLs (HTTP)
- **Netzwerkarten:** Name und Status von konfigurierten Netzwerkkarten. Darüber hinaus wird für jede Schnittstelle die durchschnittliche Datenübertragungsrate der letzten 75 Sekunden angezeigt. Die Werte resultieren aus Durchschnittswerten, die in Intervallen von 15 Sekunden gewonnen wurden. Ein Klick auf die Verbindungssymbole einer Schnittstelle öffnet einen Verkehrsmonitor. Weitere Informationen finden Sie unter *Network Security* >> *Paketfilter* >> *Erweitert*.
- **Aktuelle Systemkonfiguration:** Anzeige der wichtigsten Sicherheitsfunktionen und deren Aktivitätsstatus:
 - **Firewall:** Paketfilter (inklusive der Gesamtanzahl aktiver Regeln)
 - **Angriffsschutz:** Das Angriffsschutzsystem (engl. *Intrusion Protection System*) (IPS) erkennt Angriffe und Eindringversuche in das Netzwerk mithilfe eines signaturbasierten Regelsatzes.

- **HTTP-Proxy:** Ein Proxydienst der Anwendungsschicht für das HTTP-Protokoll mit einer Vielzahl von Webfiltertechniken.
- **FTP-Proxy:** Ein Proxydienst der Anwendungsschicht für das FTP-Protokoll.
- **SMTP-Proxy:** Ein Proxydienst der Anwendungsschicht für das SMTP-Protokoll.
- **POP3-Proxy:** Ein Proxydienst der Anwendungsschicht für das POP3-Protokoll.
- **Antivirus:** Schutz Ihres Netzwerkes vor Viren, Würmern und anderer Schadsoftware.
- **Antispam:** Erkennung von unerwünschten E-Mails.
- **Antispyware:** Schutz vor Spyware-Infektionen durch zwei voneinander unabhängig operierende Virens Scanner, deren Virensignaturen regelmäßig aktualisiert werden.
- **E-Mail-Verschlüsselung:** Verschlüsselung, Entschlüsselung und digitale Signaturen von E-Mails mithilfe des S/MIME- und OpenPGP-Protokolls.
- **Site2Site-VPN:** Konfiguration von Punkt-zu-Punkt-VPN-Verbindungen (engl. *site-to-site*).
- **Fernzugriff:** Konfiguration von Fernzugriff-VPN-Verbindungen (auch *site-to-end* genannt).
- **HA/Cluster:** Ausfallsicherheit und Cluster-Technologie, d.h. die Verteilung von rechenintensiven Aufgaben wie z. B. Virens Scans oder Angriffsschutz auf mehrere Computer.

Kapitel 4

Verwaltung

Dieses Kapitel beschreibt allgemeine Systemeinstellungen sowie Einstellungen, die das Konfigurationstool *WebAdmin* des Astaro Security Gateway selbst betreffen. Die Verwaltung-Übersichtsseite zeigt eine Statistik der letzten zehn Anmeldeversuche.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- Systemeinstellungen
- WebAdmin-Einstellungen
- Lizenzen
- Up2Date
- Backups
- Benutzerportal
- Benachrichtigungen
- Anpassung
- SNMP
- Zentralverwaltung
- Hochverfügbarkeit
- Ausschalten/Neustart

Systemeinstellungen

Mit den Registerkarten im Menü *Systemeinstellungen* können Sie grundlegende Einstellungen der Firewall vornehmen, u.a. den Rechnernamen, Datum und Zeit.

Organisatorisches

Geben Sie den Namen, den Ort Ihrer Organisation und eine E-Mail-Adresse ein, über die eine Person oder Gruppe erreicht werden kann, die die technische Verantwortung für Ihre Astaro Security Gateway trägt. Diese Informationen werden auch in digitalen Zertifikaten für IPSec, E-Mail-Verschlüsselung und den WebAdmin verwendet.

Rechnername

Geben Sie den Rechnernamen (engl. *hostname*) der Firewall ein. Verwenden Sie hierzu das FQDN-Format (*Fully Qualified Domain Name*), z. B. `firewall.example.com`. Ein Rechnername darf aus alphanumerischen Zeichen, Punkten und Bindestrichen bestehen. Am Ende des Rechnernamens muss ein spezieller Bezeichner wie z. B. `com`, `org`, oder `de` stehen. Der Rechnername wird u.a. in Benachrichtigungs-E-Mails verwendet, um die Firewall zu identifizieren. Der Rechnername erscheint auch in Statusmeldungen des SMTP- und HTTP-Proxy. Beachten Sie, dass der Rechnername nicht in der DNS-Zone Ihrer Domäne registriert sein muss.

Zeit und Datum

Damit die Protokolldateien der Firewall bezüglich Datum und Zeit genau sind, sollten Sie die Uhrzeit und Zeitzone einstellen. Alternativ dazu können Sie die lokale Zeit der Firewall mit einem externen NTP-Server (*Network Time Protocol*) synchronisieren. Beachten Sie, dass die Zeitsynchronisation einmal pro Stunde stattfindet. Signifikante Änderungen der Uhrzeit erscheinen als Lücken in Protokoll- und Berichtsdaten.

Falls Sie mehrere miteinander verbundene Firewalls betreiben, die über verschiedene Zeitzonen reichen, wählen Sie eine gemeinsame Zeitzone, z. B. UTC (*Coordinated Universal Time*). Damit lassen sich Protokolleinträge sehr viel einfacher vergleichen.

Beachten Sie, dass Änderungen an der Zeiteinstellung unerwünschte Nebeneffekte nach sich ziehen können:

- **Uhrzeit vorstellen**

Zum Beispiel, wenn Sie die Uhr von der normalen Zeit (Winterzeit) auf Sommerzeit vorstellen.

- Die Zeitbeschränkung (engl. *timeout period*) des WebAdmin wird überschritten und die Sitzung ist nicht mehr gültig.
- In den zeitbasierten Berichten fehlen Daten für die entsprechende Zeitspanne. Die meisten Diagramme stellen diesen Zeitraum als gerade Linie in Höhe des alten Wertes dar.
- Für den Netzwerkverkehr (engl. *Accounting*) betragen alle Werte in dieser Zeitspanne 0.

- **Uhrzeit zurückstellen**

Zum Beispiel, wenn Sie die Uhrzeit von Sommer- auf Winterzeit umstellen.

- In den zeitbasierten Berichten gibt es für den entsprechenden Zeitraum bereits Protokolldaten (die aus Sicht des Systems aber aus der Zukunft kommen).
- Die meisten Diagramme stellen die Werte dieser Zeitspanne komprimiert dar.
- Die im Dashboard angezeigte verstrichene Zeit seit der letzten Pattern-Prüfung zeigt den Wert *nie*, obwohl die letzte Prüfung erst wenige Minuten zurückliegt.
- Automatisch erzeugte digitale Zertifikate können ungültig werden, da der Beginn ihrer Gültigkeit aus Sicht des Systems in der Zukunft liegt.
- Für den Netzwerkverkehr behalten die bereits erfassten Daten ihre Gültigkeit. Die Netzwerkverkehr-Dateien werden weitergeschrieben, wenn der Zurücksetzungszeitpunkt wieder erreicht ist.

Aufgrund dieser Nachteile sollten Sie die Systemzeit bei der Erstkonfiguration einmalig setzen und später nur geringfügig anpassen. Dies gilt insbesondere dann, wenn die gesammelten Netzwerkverkehrs- und Berichtsdaten weiterverarbeitet werden und die Genauigkeit der Daten wichtig ist.

Zeit und Datum einstellen

Zur manuellen Konfiguration der Systemzeit wählen Sie Datum und Zeit aus den entsprechenden Auswahllisten aus. Klicken Sie *Übernehmen*, um Ihre Einstellungen zu speichern.

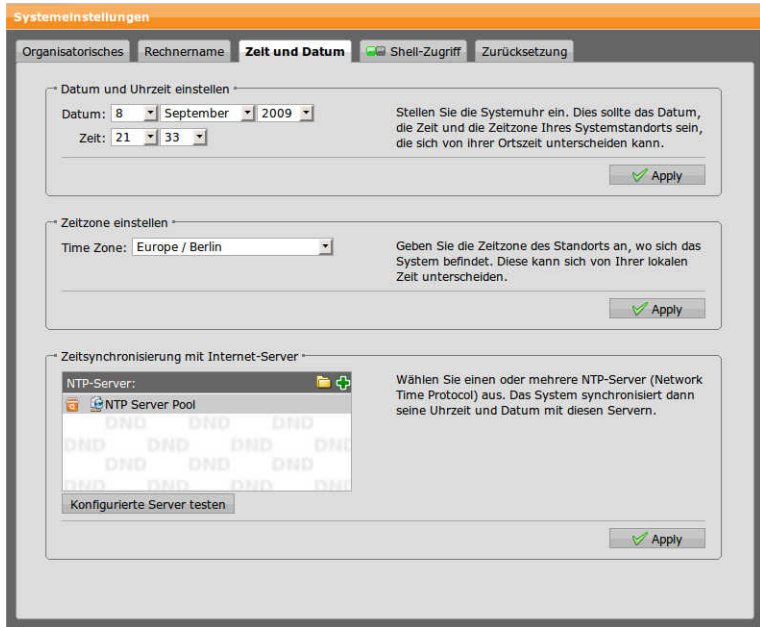


Figure 4.1 Systemeinstellungen: Einstellung von Datum und Uhrzeit

Zeitzone einstellen

Um die Zeitzone des Systems zu ändern, wählen Sie ein Gebiet oder eine Zeitzone aus der Auswahlliste aus. Klicken Sie *Übernehmen*, um Ihre Einstellungen zu speichern.

Synchronisation der Systemzeit mit NTP

Zur Synchronisation der Systemzeit mithilfe eines Zeitserver wählen Sie einen oder mehrere NTP-Server aus. Klicken Sie *Übernehmen*, nachdem Sie die Konfiguration abgeschlossen haben, damit Ihre Änderungen gespeichert werden.

NTP-Server: Der *NTP Server Pool* ist vorausgewählt. Diese Netzwerkdefinition bezieht sich auf einen Zusammenschluss von öffentlichen Zeitservern des *pool.ntp.org*-Projekts. Alternativ dazu können Sie andere NTP-Server-Definitionen wählen oder neue anlegen.

Das Hinzufügen von mehreren Zeitservern vermindert die Gefahr, dass Ihr System durch einen fehlerhaft funktionierenden NTP-Server beeinträchtigt wird – und bedeutet für das System nur eine unwesentliche Mehrbelastung.

Konfigurierte Server testen: Klicken Sie auf diese Schaltfläche, um zu testen, ob mit den gewählten NTP-Servern eine Verbindung von Ihrem Gerät aus aufgebaut werden kann und ob verwendbare Zeitdaten zurückgeliefert werden. Dabei wird der Zeitunterschied zwischen Ihrem System und den Servern

ermittelt. Verschiebungen sollten normalerweise weit unter einer Sekunde liegen, wenn Ihr System korrekt konfiguriert ist. Als Testergebnis wird eine Information über den Verbindungsstatus angezeigt.

Shell-Zugriff

Secure Shell (SSH) ist ein Netzwerkprotokoll, mit dessen Hilfe man sich über eine verschlüsselte Netzwerkverbindung auf der Firewall anmelden kann. Es wird typischerweise für Wartungsarbeiten und zur Fehlersuche verwendet. Um sich auf der Shell von Astaro Security Gateway anzumelden, benötigen Sie ein SSH-Programm, welches in den meisten Linux-Distributionen enthalten ist.

Zugelassene Netzwerke: Verwenden Sie das Feld *Zugelassene Netzwerke*, um den SSH-Zugang auf bestimmte Netzwerke einzuschränken. SSH-Programme aus hier eingetragenen Netzwerken können sich per SSH an der Firewall anmelden.

Shell-Benutzerkennwörter: Setzen Sie Kennwörter für die Standard-Zugangsberechtigten *root* und *loginuser*.

Hinweis – Um SSH-Zugriff zu ermöglichen, müssen die Kennwörter initial gesetzt sein. Darüber hinaus können Sie nur Kennwörter vergeben, die den Sicherheitseinstellungen entsprechen, die Sie auf der Registerkarte *Benutzer* >> *Authentifizierung* >> *Erweitert* konfiguriert haben. Mit anderen Worten, wenn Sie die Verwendung von komplexen Kennwörtern ausgewählt haben, dann können Sie hier nur Kennwörter eingeben, die diesen Sicherheitsanforderungen entsprechen.

SSH-Daemon-Listen-Port: Mit dieser Option können Sie den TCP-Port für das SSH-Protokoll ändern. Der standardmäßige Port für SSH ist 22. Um den Port zu ändern, geben Sie einen geeigneten Wert zwischen 1024 und 65535 in das Feld *Portnummer* ein und klicken Sie *Übernehmen*.

Zurücksetzung

Mit den Optionen auf der Registerkarte *Zurücksetzung* können Sie die Kennwörter der Shell-Benutzer löschen. Darüber hinaus können Sie Astaro Security Gateway durch Ausführen eines *Werkszurücksetzung* in den Auslieferungszustand zurückversetzen.

Systemkennwörter zurücksetzen: Das Ausführen dieser Funktion setzt die Kennwörter der folgenden Benutzer zurück:

- root (Shell-Benutzer)
- loginuser (Shell-Benutzer)
- admin (vordefiniertes Benutzerkonto des Administrators)

Um das Gerät nach dem Zurücksetzen der Kennwörter herunterzufahren, wählen Sie die Option *System anschließend herunterfahren*.

Sicherheitshinweis – Der nächsten Person, die sich mit dem WebAdmin verbindet, wird ein Kennwort-Dialogfenster angezeigt. Deshalb sollten Sie sich nach einer Kennwortzurücksetzung sofort abmelden, die Webseite neu laden und ein neues Administratorkennwort setzen.

Des Weiteren wird der Shell-Zugriff nicht mehr möglich sein, bis Sie neue Shell-Kennwörter auf der Registerkarte *Verwaltung >> Systemeinstellungen >> Shell-Zugriff* angeben.

Werkszurücksetzung: Diese Funktion setzt Astaro Security Gateway in den Auslieferungszustand zurück. Die folgenden Daten werden dabei gelöscht:

- Systemkonfiguration
- Zwischenspeicher des HTTP-Proxy
- Protokoll- und Netzwerkverkehrsdaten
- Datenbanken
- Update-Pakete
- Lizenzen
- Kennwörter
- Hochverfügbarkeitsstatus

Die Versionsnummer der Astaro Security Gateway Software bleibt unverändert. Das bedeutet, alle installierten Firmware- und Pattern-Updates werden beibehalten.

Hinweis – Astaro Security Gateway wird heruntergefahren, nachdem Sie eine Werkzurücksetzung veranlasst haben.

WebAdmin-Einstellungen

Im Menü *Verwaltung* >> *WebAdmin-Einstellungen* werden die Einstellungen für die Benutzeroberfläche WebAdmin wie der TCP-Port oder die Sprache durchgeführt.

Allgemein

WebAdmin-Sprache

Wählen Sie die Sprache des WebAdmin. Beachten Sie, dass sich dies nur auf das aktuelle Benutzerprofil auswirkt.

WebAdmin-Leerlauf-Zeitabschaltung

In der Textbox *Abmelden nach* geben Sie die Zeitspanne in Sekunden an, nach der Sie automatisch vom WebAdmin abgemeldet werden, wenn keine Aktionen stattfinden. Nach der Installation sind standardmäßig 300 Sekunden eingestellt. Sie können Werte von 60 bis 86.400 Sekunden eintragen.

Hinweis – Änderungen an der WebAdmin-Zeitabschaltung werden erst nach einer erneuten Anmeldung wirksam. Übrigens ist die automatische Abmeldung deaktiviert, wenn die Dashboard-Seite im WebAdmin geöffnet ist.

WebAdmin-TCP-Port

Standardmäßig erreicht man den WebAdmin unter Port 4444. Im Textfeld *TCP-Port* ist eine Eingabe von 1024 bis 65535 erlaubt. Allerdings sind einige Ports bereits von anderen Diensten belegt. Insbesondere können Sie nie den Port 10443, den Port des Benutzerportals oder des Fernzugriffs verwenden. Beachten Sie, dass Sie die Portnummer mit angeben müssen (abgetrennt durch einem Doppelpunkt), wenn Sie auf den WebAdmin zugreifen möchten, z. B. `https://192.168.0.1:1443`. Klicken Sie *Übernehmen*, um Ihre Änderungen zu speichern.

Zugriffskontrolle

Zugelassene Administratoren: Astaro Security Gateway kann von mehreren Administratoren gleichzeitig verwaltet werden. Im Feld *Zugelassene Administratoren* können Sie angeben, welche Benutzer oder Benutzergruppen unbeschränkten Lese- und Schreibzugriff auf die WebAdmin-Schnittstelle haben dürfen. Standardmäßig ist dies die Gruppe der *SuperAdmins*.

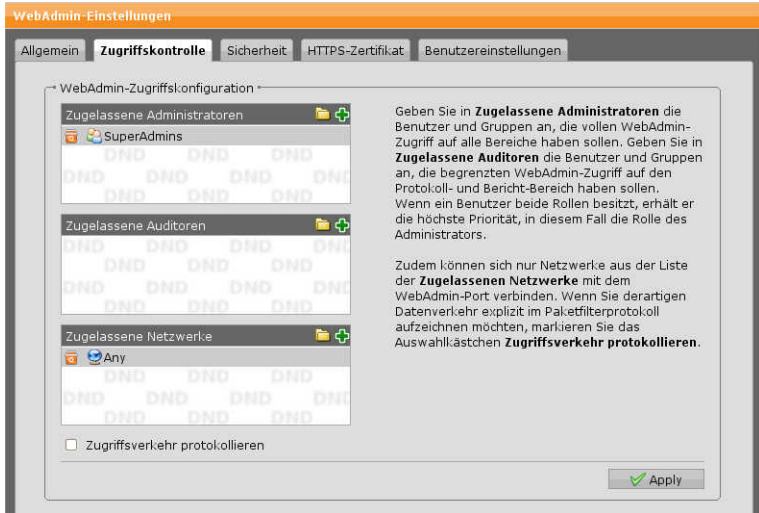


Figure 4.2 WebAdmin-Einstellungen: Konfiguration der WebAdmin-Zugriffskontrolle

Zugelassene Auditoren: Astaro Security Gateway ermöglicht auch beschränkten Zugriff für Auditoren, welche Protokolldateien und Berichtsdaten lesen können, ansonsten aber keine Änderungen vornehmen dürfen. Im Feld *Zugelassene Auditoren* können Sie angeben, welche Benutzer oder Gruppen diesen beschränkten Zugriff auf die WebAdmin-Schnittstelle haben dürfen. Standardmäßig ist das Textfeld leer.

Zugelassene Netzwerke: In diesem Eingabefeld können Sie festlegen, aus welchen Netzwerken Zugriff auf den WebAdmin möglich sein soll. Zum Zweck einer reibungslosen Installation ist hier standardmäßig *Any* (alle) ausgewählt. Dies bedeutet, dass auf den WebAdmin von überall her zugegriffen werden darf. Ändern Sie diese Einstellung so schnell wie möglich auf Ihre internen Netze. Die sicherste Methode besteht darin, den Zugriff per HTTPS auf einen einzigen Computer zu beschränken.

Zugriffsverkehr protokollieren: Wenn Sie alle Aktivitäten bezüglich des WebAdmin-Zugriffs in der Paketfilter-Protokolldatei aufgeführt haben möchten, wählen Sie diese Option.

Sicherheit

Erraten von Kennwörtern verhindern: Mit dieser Funktion können die Versuche, sich am WebAdmin anzumelden, begrenzt werden, z. B. Versuche, das

Kennwort zu erraten. Nach einer bestimmten Anzahl an Versuchen (standardmäßig drei) wird der Zugang von dieser IP-Adresse aus für eine bestimmte Zeit (standardmäßig 600 Sekunden) verweigert. Netzwerke, die im Feld *Netzwerke nie blockieren* stehen, sind vom Blockierschutz ausgenommen.

HTTPS-Zertifikat

Von der Registerkarte *Verwaltung >> WebAdmin-Einstellungen >> HTTPS-Zertifikat* aus können Sie das WebAdmin-CA-Zertifikat in Ihrem Browser installieren.

Während der initialen Einrichtung des WebAdmin-Zugriffs wurde automatisch eine lokale WebAdmin-CA erzeugt. Der öffentliche Schlüssel dieses CA-Zertifikats kann in Ihrem Browser installiert werden. Dadurch vermeiden Sie den Sicherheitshinweis während der Anmeldung am WebAdmin.

Hinweis – Um Problemen beim Herunterladen von Dateien mit dem Internet Explorer 6 vorzubeugen, fügen Sie die URL der Firewall (z.B. <https://192.168.2.100>) und des Benutzerportals (z.B. <https://192.168.2.100>) den *Vertrauenswürdigen Sites* hinzu. Beim Internet Explorer 6 befinden sich diese Einstellungen im Menü *Extras >> Internetoptionen >> Sicherheit*. Beim Internet Explorer 7 aktivieren Sie zusätzlich im Fenster *Sicherheitseinstellungen* die Funktion *Automatische Eingabeaufforderung für Dateidownloads*.

Um das Zertifikat der WebAdmin-CA zu importieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *HTTPS-Zertifikat auf CA-Zertifikat importieren*.**

Der öffentliche Schlüssel des CA-Zertifikats wird exportiert.

Sie können das Zertifikat entweder auf der Festplatte abspeichern oder es in Ihrem Browser installieren.

2. **Installieren Sie das Zertifikat (optional).**

Es öffnet sich ein Dialogfenster, mit dessen Hilfe das Zertifikat installiert werden kann.

Hinweis – Beachten Sie, dass infolge von unterschiedlichen Systemzeiten und den weltweit versetzten Zeitzonen das Zertifikat nicht sofort gültig sein muss.

Viele Browser geben in diesem Fall die Meldung aus, dass das Zertifikat abgelaufen sei. Diese Meldung ist nicht richtig. Das Zertifikat wird aber nach maximal 24 Stunden gültig und bleibt dies für einen Zeitraum von 27 Jahren.

WebAdmin-Zertifikat neu erstellen

Das WebAdmin Server-Zertifikat, mit dem sich Astaro Security Gateway gegenüber dem Browser authentifiziert, gilt für den Rechnernamen (engl. *hostname*), den Sie während der ersten Anmeldung angegeben haben. Wenn sich der Rechnername von Astaro Security Gateway in der Zwischenzeit geändert hat, so erscheint im Browser ein entsprechender Sicherheitshinweis. Um dies zu vermeiden, können Sie ein neues Server-Zertifikat mit einem neuen Rechnernamen erzeugen. Geben Sie zu diesem Zweck den gewünschten Rechnernamen an und klicken Sie *Übernehmen*. Um in WebAdmin weiterarbeiten zu können, müssen Sie wahrscheinlich – aufgrund der Änderung des Zertifikats – die Seite über Ihren Browser neu laden, das neue Zertifikat akzeptieren und sich an WebAdmin neu anmelden.

Benutzereinstellungen

Auf der Registerkarte *Verwaltung >> WebAdmin-Einstellungen >> Benutzereinstellungen* können Sie einige Benutzereinstellungen für den jeweils angemeldeten Benutzer vornehmen, wie globale Tastaturkürzel und die Anzahl von Elementen pro Seite bei längeren Tabellen oder Listen.

Konfiguration für WebAdmin-Tastaturkürzel

Hier können Sie Tastaturkürzel festlegen, um zwischen Objektleisten, dem Drag-and-Drop-Objektmenü, das für viele Konfigurationen benutzt wird, hin- und herzuschalten (weitere Informationen zu den Objektleisten finden Sie unter *WebAdmin >> Objektleisten*). Diese Funktion erlaubt Ihnen, Objektleisten einzublenden, ohne vorher etwas bearbeiten zu müssen. Verwenden Sie die Auswahlliste, um eine andere Umschalttaste auszuwählen, und das Textfeld, um ein anderes Zeichen einzugeben.

Wenn Sie die ursprünglichen Tastaturkürzel wiederherstellen wollen, klicken Sie auf die Schaltfläche *Auf Standard zurücksetzen*. Klicken Sie *Übernehmen*, um Ihre Änderungen zu speichern.

Optionen für Tabellen-Seitenumbruch

Hier können Sie global den Tabellenseiten-Umbruch festlegen, d. h. wie viele Elemente pro Seite angezeigt werden. Klicken Sie auf die Auswahlliste und wählen Sie einen Wert. Klicken Sie *Übernehmen*, um Ihre Änderungen zu speichern.

WebAdmin-Einstellungen

Allgemein | Zugriffskontrolle | Sicherheit | HTTPS-Zertifikat | **Benutzereinstellungen**

Konfiguration für WebAdmin-Tastaturkürzel

Hier können Sie die Tastaturkürzel für jede Objektleiste festlegen.

Users/Groups: CTRL V
 Interfaces: CTRL C
 Networks: CTRL Z
 Services: CTRL X

Auf Standard zurücksetzen

✓ Apply

Optionen für Tabellen-Seitenumbruch

Hier können Sie festlegen, wie viele Einträge pro Seite in den Tabellen angezeigt werden sollen.

Einträge pro Seite: 10

✓ Apply

Astaro News Feed

☐ Astaro News Feed deaktivieren

Hier können Sie den Astaro News Feed aktivieren oder deaktivieren, der auf dem Dashboard angezeigt wird.

✓ Apply

Figure 4.3 WebAdmin-Einstellungen: Konfiguration der Benutzereinstellungen

Astaro News Feed

Astaro News Feed ist, wenn er aktiviert ist, ein kleiner Bereich im Dashboard, wo Neuigkeiten über Astaro und seine Produkte bekannt gegeben werden. Standardmäßig ist der News Feed deaktiviert. Um ihn zu aktivieren, wählen Sie die Option *Astaro News Feed deaktivieren* ab und klicken Sie *Übernehmen*.

Lizenzen

Die Verfügbarkeit von bestimmten Funktionen auf Astaro Security Gateway, Astaro Mail Gateway und Astaro Web Gateway wird über Lizenzen und Abonnements (engl. *subscriptions*) geregelt, d. h. Lizenzen und Abonnements, die Sie mit Ihrer Firewall oder Ihrem Gateway erworben haben, ermöglichen Ihnen, bestimmte Funktionen zu verwenden und andere nicht.

Im Oktober 2009 wird Astaro ein neues Lizenzmodell einführen, genannt *On-Demand Licensing*, welches nach und nach das klassische, bisher gültige Lizenzmodell ablösen wird. Klassische Lizenzen, die Sie bereits erworben haben, bleiben unabhängig davon gültig!

Erwerb einer Lizenz

Nach dem Kauf einer Astaro Lizenz erhalten Sie per E-Mail Ihre Aktivierungsschlüssel. Diese Schlüssel benötigen Sie, um die eigentliche Lizenz zu erzeugen

bzw. eine bereits bestehende Lizenz zu aktualisieren. Dazu müssen Sie sich in MyAstaro anmelden. Gehen Sie dort auf die Seite für die Lizenzverwaltung. Oben auf der Seite befindet sich ein Formular, wo Sie den Aktivierungsschlüssel eintragen können. Kopieren Sie zu diesem Zweck den Aktivierungsschlüssel aus der E-Mail in das dafür vorgesehene Feld.

astaro
internet security

Simplifying Email, Web & Network Protection

Google Custom Search Search Language Worldwide

MyAstaro Login

Enter your credentials below. If you have forgotten your password, please click on the appropriate button and a new password will be mailed to your inbox.

Your email address:

Password:

Login to MyAstaro Forgot My Password

Sign up to MyAstaro - Free Membership

Join today and get instant FREE access to Astaro software downloads, license management, image and document downloads, online support and a personal home use license.

Join MyAstaro

Certified partners have exclusive access to the enhanced partner area. For partner access, please either contact your account manager or email myastaro@astaro.com. If you are interested in becoming an Astaro partner, then [contact us](#).

Our Products
Your Needs
References
Newsroom
Events
Support
Partners
Company
Contact
MyAstaro
Login

Webmaster Privacy Legal Sitemap © 2009 by Astaro AG

Figure 4.4 MyAstaro-Portal

Es erscheint ein neues Formular, in das Sie sowohl Informationen zu Ihrem Vertriebspartner als auch Ihre eigenen Kontaktdaten eintragen können. Aus den bereits gespeicherten Informationen versucht das Portal, so viele Felder wie möglich vorauszufüllen. Darüber hinaus können Sie Angaben zur Seriennummer Ihrer ASG machen. Nachdem Sie das Formular abgeschickt haben, wird Ihre Lizenz erzeugt und Sie werden auf die Lizenz-Detailseite weitergeleitet, von der aus Sie die Lizenz herunterladen können.

Um die Lizenz verwenden zu können, müssen Sie die erzeugte Lizenz-Datei herunterladen und lokal abspeichern. Melden Sie sich dann am WebAdmin an und öffnen Sie die Registerkarte *Verwaltung >> Lizenzen >> Installation*. Laden Sie nun die Lizenzdatei hoch. Der WebAdmin aktiviert nun alle Abonnements und anderen Einstellungen, die in der Lizenz enthalten sind.

Hinweis – Der Aktivierungsschlüssel, den Sie per E-Mail enthalten haben, kann nicht in den WebAdmin importiert werden. Dieser Schlüssel dient lediglich dazu, Ihre Lizenz in MyAstaro zu aktivieren. Nur die Lizenz-Datei kann im WebAdmin installiert werden.

OnDemand Lizenzen

Astaros OnDemand Lizenzmodell ist einfacher und wesentlich flexibler als das klassische Lizenzmodell.

Zunächst gibt es eine Basislizenz (*base license*), ähnlich der freien Home-User-Lizenz des klassischen Lizenzmodells, welche alle Basisfunktionalitäten kostenlos zur Verfügung stellt. Diese Basislizenz steht aber nicht mehr nur Privatanwendern zur kostenlosen Verfügung, sondern auch Geschäftskunden.

Des Weiteren gibt es drei Arten von kostenpflichtigen Abonnements:

- Net Security (Netzwerksicherheit)
- Web Security (Internetsicherheit)
- Mail Security (E-Mail-Sicherheit)

Diese Abonnements können einzeln oder in Kombination erworben werden. Jedes der Abonnements aktiviert bestimmte Funktionen des Produkts. Die untenstehende Tabelle zeigt eine Übersicht darüber, welche Funktionen durch welches Abonnement freigeschaltet werden.

Für detailliertere Informationen zu Abonnements und ihrem Funktionsumfang wenden Sie sich bitte an Ihren zertifizierten Astaro Partner oder die Astaro Homepage⁷.

Up2Dates

Jedes Abonnement aktiviert die vollständige Unterstützung automatischer Updates, das bedeutet, dass Sie automatisch über neue Firmware-Updates informiert werden. Darüber hinaus können Firmware- und Pattern-Updates automatisch heruntergeladen (und installiert) werden.

Eine Basislizenz ohne Abonnement besitzt nur eine eingeschränkte Unterstützung automatischer Updates: lediglich Pattern-Updates, wie z. B. Aktualisierungen der Onlinehilfe, werden weiterhin automatisch heruntergeladen und

⁷ <http://www.astaro.com/>

Funktion	Basislizenz	Net	Web	Mail
Verwaltung (Backups, Benachrichtigungen, SNMP, ACC, ...)	✓			
Lokale Auth. (Benutzer, Gruppen)	✓			
Grundlegende Netzwerkfunkt. (Stat. Routing, DHCP, DNS, Auto QoS, NTP, ...)	✓			
Firewall/NAT (Paketfilter, DNAT, SNAT, ...)	✓			
PPTP- & L2TP-Fernzugriff	✓			
Lokale Protokollierung, Standardberichte	✓			
Angriffsschutz (IPS) (Patterns, DoS, Flood, Portscan ...)		✓		
IPSec- & SSL-Site-to-Site-VPN, IPSec- & SSL-Fernzugriff		✓		
Erweiterte Netzwerkfunkt. (Linkbündelung, Uplink-Ausgleich, Richtlinien-Routing, OSPF, Multicast, angepasstes QoS, Serverlastausgleich, Generischer Proxy ...)		✓	(✓)	(✓)
Benutzerportal		✓	✓	✓
Hochverfügbarkeit		✓	✓	✓
Entfernte Auth. (AD, eDir, RADIUS, ...)		✓	✓	✓
Ausgelagerte Protokollierung, erweiterte Berichte (Archivierung, Konfiguration)		✓	✓	✓
Grundlegender HTTP/S- & FTP-Proxy			✓	
HTTP/S- & FTP-Schadsoftware-Filterung			✓	
Grundlegender SMTP-Proxy, Quarantänebericht, Mail-Manager				✓
SMTP- & POP3-Schadsoftware-Filterung				✓

Table 4.1 Lizenzen: Abonnements und Funktionen

installiert. Sie werden jedoch nicht über verfügbare Firmware-Updates informiert, und die Firmware-Updates müssen manuell heruntergeladen werden. Die Verfügbarkeit neuer Firmware-Updates wird im Astaro Up2Date-Blog⁸ bekannt gegeben.

⁸ <http://up2date.astaro.com/>

Support und Wartung

Mit der Basislizenz können Sie den *Web-Support* verwenden: das Astaro Support-Forum⁹ und Astaros Knowledgebase¹⁰ (Wissensdatenbank).

Sobald Sie eines der drei Abonnements erwerben, werden Sie automatisch auf *Standard-Support* umgestellt. Bei dieser Supportstufe können Sie zusätzlich einen Supportfall im MyAstaro Portal¹¹ eröffnen oder Ihren zertifizierten Astaro Partner kontaktieren.

Darüber hinaus gibt es die Möglichkeit, einen *Premium-Support*-Vertrag abzuschließen. Dieser bietet Ihnen 24/7-Support mit einem Astaro Engineer als Ansprechpartner.

Klassische Lizenzen

Das klassische Lizenzmodell wird von dem oben beschriebenen OnDemand-Lizenzmodell ersetzt werden. Das klassische Lizenzmodell ist hier dennoch aus Gründen der Kompatibilität beschrieben und weil es nicht von heute auf morgen abgelöst werden wird, sondern nach und nach.

Astaro Security Gateway wird standardmäßig mit einer 30-Tage-Testlizenz ausgeliefert, mit der Sie alle Leistungsmerkmale und Funktionen uneingeschränkt nutzen können. Nach Ablauf der 30 Tage müssen Sie eine gültige Lizenz installieren, um Astaro Security Gateway weiterhin betreiben zu können. Lizenzen werden im Registrierungsportal von MyAstaro¹² erzeugt. Im Folgenden wird beschrieben, wie Sie eine gültige Lizenz beziehen können und wie diese im WebAdmin installiert wird.

Abonnements

Astaros Webfilter wird auf dem Astaro Security Gateway über ein optionales Abonnement (engl. *Subscription*) aktiviert. Der Funktionsumfang beinhaltet Inhaltsfilterung, Viren- und Spyware-Schutz für HTTP/S sowie Antiviren-Mechanismen und Dateierweiterungsprüfung für FTP.

Wenn das Abonnement Web Filtering nicht aktiviert ist, können im WebAdmin die folgenden Registerkarten nicht ausgewählt werden:

- *Web Security >> HTTP/S >> Antivirus/Schadsoftware*
- *Web Security >> HTTP/S >> URL-Filterung*

⁹ <http://www.astaro.org>

¹⁰ <http://www.astaro.com/kb>

¹¹ <http://my.astaro.com>

¹² <http://my.astaro.com>

- *Web Security >> HTTP/S >> URL-Filterkategorien*
- *Web Security >> HTTP/S Profile >> Filteraktionen*
- *Web Security >> FTP >> Antivirus*

Astaros Mail Security wird auf dem Astaro Security Gateway über ein optionales Abonnement (engl. *Subscription*) aktiviert. Der Funktionsumfang beinhaltet E-Mail-Sicherheit und E-Mail-Verschlüsselung. Die E-Mail-Verschlüsselung unterstützt OpenPGP und S/MIME sowie die digitale Signatur von SMTP-Mails. Wenn das Abonnement Mail Security nicht aktiviert ist, können im WebAdmin die folgenden Registerkarten nicht ausgewählt werden:

- *Mail Security >> SMTP >> Antivirus*
- *Mail Security >> SMTP >> Antispam*
- *Mail Security >> POP3 >> Antivirus*
- *Mail Security >> POP3 >> Antispam*
- Alle Registerkarten des Menüs *Mail Security >> Verschlüsselung*

Hinweis – Kunden, die in der Vergangenheit entweder das Mail-Filtering- oder das Mail-Encryption-Abonnement nutzten, profitieren nun von der Zusammenlegung dieser beiden Abonnements.

Zusätzlich sind die folgenden Registerkarten deaktiviert:

- *Mail Security >> SMTP >> Weiterleitungen >> Inhaltsscan*
- *Mail Security >> SMTP >> Erweitert >> BATV-Schlüssel*
- *Mail Security >> SMTP >> Erweitert >> Max. Nachrichtengröße*
- *Mail Security >> SMTP-Profile*

Falls eine Funktion nicht Bestandteil der aktuellen Lizenz ist, wird über der Registerkarte ein entsprechender Warnhinweis angezeigt.

Übersicht

Die Registerkarte *Übersicht* zeigt detaillierte Informationen zu Ihrer Lizenz und besteht aus mehreren Abschnitten:

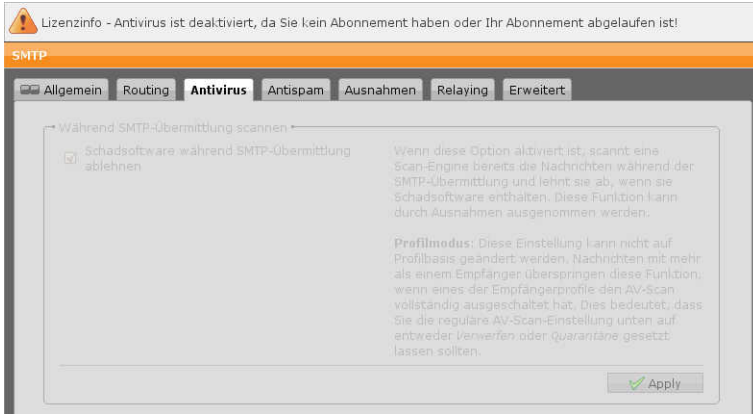


Figure 4.5 Lizenzen: Warnhinweis zur Lizenz

- **Lizenzinformationen:** Grundlegende Lizenzparameter, wie Besitzer, ID oder Ablaufdatum.
- **Wartung:** Support-Ebene sowie Gültigkeitsdatum
- **Abonnements:** Lizenzierte Abonnements
- **Hot-Standby/Cluster:** Lizenzoption für die Hot-Standby-/Cluster-Funktion.

Installation

Zum Installieren einer Lizenz gehen Sie folgendermaßen vor:

1. **Öffnen Sie das Dialogfenster *Upload File*.**
Klicken Sie auf das Ordnersymbol neben dem Eingabefeld *Lizenzdatei*. Das Dialogfenster *Upload File* öffnet sich.
2. **Wählen Sie die Lizenz-Datei.**
Wechseln Sie in das Verzeichnis, in dem sich Ihre Lizenz-Datei befindet. Wählen Sie die Lizenz-Datei, die Sie installieren möchten.
3. **Klicken Sie *Speichern*.**
Ihre Lizenz wird hochgeladen.
4. **Klicken Sie *Übernehmen*.**
Ihre Lizenz wird nun installiert. Beachten Sie, dass die neue Lizenz automatisch eine bereits installierte Lizenz ersetzt.
Die Installation der Lizenz dauert ca. 60 Sekunden.

Lizenzen

Übersicht | Installation | Aktive IP-Adressen

Lizenzinformationen

Inhaber: Astaro Karlsruhe
 Lizenz-ID: 154977
 Registrierungsdatum: 01 April 2008
 Ablaufdatum: Never
 Maximale gleichzeitige Verbindungen: Unbegrenzt
 Maximale Benutzerzahl: Unbegrenzt
 Software-Garantie-Ablaufdatum: 01 April 2013

Wartung

Ebene: Keine » Silber! » **Gold** » Platin » Platin Plus
 Startdatum: 01 April 2008
 Enddatum: 01 April 2013

Abonnements

Web Security: ✓ Lizenz gültig bis 01 April 2013
 Mail Security: ✓ Lizenz gültig bis 01 April 2013

Hot-Standby/Cluster

Hot-Standby: ✓ Aktiviert
 Cluster: ✓ Aktiviert (10 nodes)

Lizenz erwerben oder verlängern

In order to purchase additional Astaro capabilities, upgrades, renewals, or licenses for additional sites, please contact you Certified Astaro Reseller. They will be happy to help determine your needs and provide a quote. If you do not have an Astaro Reseller to contact, please click: [here](#) for more options.

Figure 4.6 Lizenzen: Lizenzübersicht (Klassisches Lizenzmodell)

Lizenzen

Übersicht | **Installation** | Aktive IP-Adressen

Hochladen der Lizenzdatei

Lizenzdatei:

Laden Sie die Lizenzdatei bitte hier hoch. Diese Lizenz ersetzt automatisch eine andere installierte Lizenz.

Figure 4.7 Lizenzen: Installation einer Lizenz

Aktive IP-Adressen

Falls Sie eine Lizenz erworben haben, die nicht uneingeschränkt viele Benutzer (IP-Adressen) erlaubt, zeigt Ihnen die Registerkarte *Aktive IP-Adressen* Informationen über die zulässige Anzahl an IP-Adressen, die von Ihrer Lizenz abgedeckt werden. IP-Adressen, die den Umfang Ihrer Lizenz überschreiten, werden gesondert aufgelistet. Falls Sie die zulässige Grenze überschritten haben, erhalten Sie regelmäßig eine Benachrichtigung per E-Mail.

Hinweis – IP-Adressen, die über einen Zeitraum von sieben Tagen inaktiv waren, werden nicht weiter gezählt.

Up2Date

Das Menü *Verwaltung >> Up2Date* enthält die Konfigurationsoptionen für Software-Updates von Astaro Security Gateway. Regelmäßige Updates sorgen dafür, dass die Firewall stets über die neuesten Fehlerbehebungen, Produktverbesserungen und aktuellen Virensignaturen verfügt. Jedes Update wird von Astaro digital signiert – unsignierte oder gefälschte Updates können so erkannt und Installationen von gefälschten Updates verhindert werden.

Es gibt zwei Typen von Software-Updates:

- **Firmware-Updates:** Firmware-Updates enthalten Fehlerbehebungen und Produktverbesserungen für Astaro Security Gateway.
- **Pattern-Updates:** Pattern-Updates halten Virus-, Spam-, und Angriffsschutz-Signaturen sowie die Onlinehilfe auf dem neuesten Stand.

Um Update-Pakete herunterzuladen, öffnet die Firewall eine TCP-Verbindung zu den Update-Servern auf Port 443. Hierzu müssen vom Administrator keinerlei Anpassungen vorgenommen werden. Falls Sie jedoch eine übergeordnete Firewall verwenden, so müssen Sie auf dieser die Kommunikation über TCP-Port 443 zu den Update-Servern explizit erlauben.

Übersicht

Die Registerkarte *Verwaltung >> Up2Date >> Übersicht* gibt Ihnen einen schnellen Überblick darüber, ob Ihr System auf dem neuesten Stand ist. Von hier aus können Sie neue Firmware- und Pattern-Updates installieren.

Up2Date-Fortschritt

Dieser Bereich ist nur sichtbar, wenn Sie einen Installationsvorgang angestoßen haben. Klicken Sie auf die Schaltfläche *Up2Date-Fortschritt in neuem Fenster anzeigen*, um den Update-Fortschritt zu verfolgen. Wenn Ihr Browser Pop-up-Fenster nicht unterdrückt, wird ein neues Fenster geöffnet, das den Update-Fortschritt anzeigt. Andernfalls müssen Sie Pop-up-Fenster zunächst explizit erlauben.



Figure 4.8 Up2Date: Übersicht

Hinweis – Bevor ein Installationsvorgang gestartet wird, wird ein Backup an den/die Standardempfänger für Backups versendet.

Firmware

Im Abschnitt *Firmware* sehen Sie die aktuell installierte Firmware-Version. Wenn ein Update-Paket verfügbar ist, erscheint eine Schaltfläche *Jetzt auf neueste Version aktualisieren*. Zusätzlich wird eine Nachricht im Abschnitt *Verfügbare Firmware-Up2Dates* angezeigt. Sie können von hier aus das neueste Update direkt herunterladen und installieren. Sobald Sie *Jetzt auf neueste Version aktualisieren* angeklickt haben, können Sie den Update-Fortschritt in einem neuen Fenster verfolgen. Klicken Sie dazu auf das Aktualisieren-Symbol von WebAdmin.

Verfügbare Firmware-Up2Dates

Wenn Sie *Manuell* auf der Registerkarte *Konfiguration* gewählt haben, sehen Sie hier eine Schaltfläche *Jetzt nach Up2Date-Paketen suchen*, mit der Sie Firmware-Up2Date-Pakete manuell herunterladen können. Wenn mehr als ein

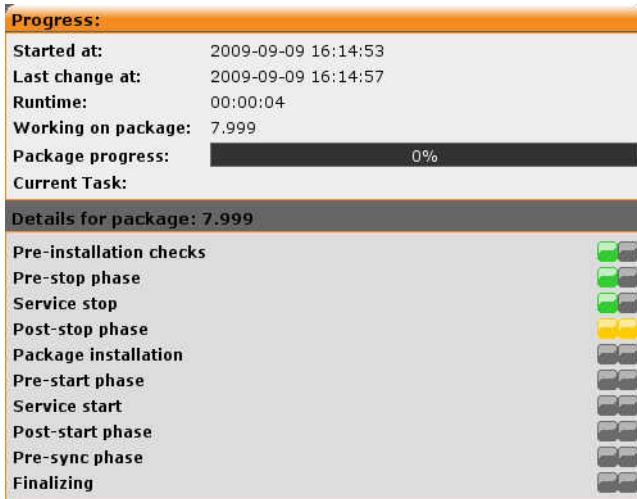


Figure 4.9 Up2Date: Fortschrittsbalken

Up2Date-Paket verfügbar ist, können Sie wählen, welches Sie installieren wollen. Sie können *Jetzt auf neueste Version aktualisieren* im Abschnitt *Firmware* verwenden, um die neueste Version zu installieren.

Es gibt außerdem eine Schaltfläche *Schedule* (dt. planen) für jedes Up2Date, mit dem Sie genaues Datum und Uhrzeit für eine automatische Installation bestimmen können. Um eine geplante Installation zu löschen, klicken Sie auf *Cancel* (dt. abbrechen).

Ein Hinweis zu Installationen, die „inbegriffen“ sind: Es kann Konstellationen geben, wo Sie die Installation eines Up2Date-Pakets planen, das die vorherige Installation eines älteren Up2Date-Pakets erfordert. Dieses Up2Date-Paket wird automatisch zur Installation eingeplant, und zwar vor dem eigentlichen Up2Date-Paket. Sie können jedoch auch für dieses Paket eine genaue Zeit einplanen, aber Sie können die Installation nicht verhindern.

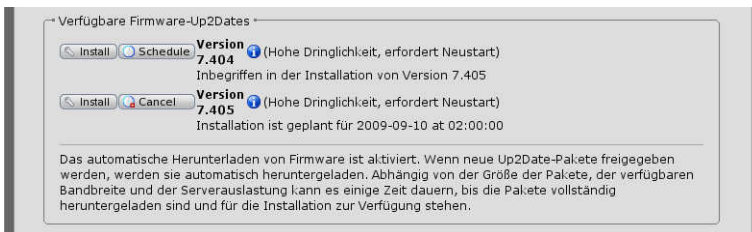


Figure 4.10 Up2Date: Installation von Up2Date-Paketen, die inbegriffen sind

Patterns

Im Abschnitt *Patterns* steht die Versionsnummer der aktuell installierten Patterns. Wenn Sie *Manuell* auf der Registerkarte *Konfiguration* gewählt haben, sehen Sie hier eine Schaltfläche *Patterns jetzt aktualisieren*, mit der sie neue verfügbare Patterns herunterladen und installieren können.

Hinweis – Die aktuell installierte Patternversion muss nicht mit der neuesten verfügbaren Patternversion übereinstimmen, damit Astaro Security Gateway korrekt funktioniert. Eine Abweichung zwischen der aktuell installierten und der aktuell erhältlichen Patternversion kann vorkommen, wenn neue Patterns vorliegen, die jedoch nicht zu dem Gerät passen, das Sie verwenden. Welche Patterns heruntergeladen werden, hängt von Ihren Einstellungen und Ihrer Hardwarekonfiguration ab. Wenn Sie zum Beispiel nicht den Angriffsschutzfunktion (IPS) des Astaro Security Gateway benutzen, werden neue IPS-Patterns nicht installiert, was den Abstand zwischen installierten und erhältlichen Patternversionen vergrößert.

Konfiguration

Neue Update-Pakete werden standardmäßig automatisch von der Firewall heruntergeladen.

Firmware-Download-Intervall

Diese Option steht in der Standardeinstellung auf 15 Minuten, das heißt, dass Astaro Security Gateway alle 15 Minuten nach verfügbaren Firmware-Updates sucht. Astaro Security Gateway lädt verfügbare Firmware-Update-Pakete automatisch herunter, ohne sie jedoch zu installieren. Der genaue Zeitpunkt hierfür liegt dabei beliebig in dem angegebenen Intervall. Sie können das Intervall auf bis zu *Monatlich* setzen, oder Sie können automatische Firmware-Downloads gänzlich deaktivieren, indem Sie *Manuell* in der Auswahlliste wählen. Wenn Sie *Manuell* wählen, erscheint eine Schaltfläche *Jetzt nach Up2Date-Paketen suchen* auf der Registerkarte *Übersicht*.

Intervall für Pattern-Download und -Installation

Diese Option steht in der Standardeinstellung auf 15 Minuten, das heißt, dass Astaro Security Gateway alle 15 Minuten nach verfügbaren Pattern-Updates sucht. Astaro Security Gateway lädt verfügbare Pattern-Updates automatisch herunter und installiert diese. Der genaue Zeitpunkt hierfür liegt dabei beliebig in dem angegebenen Intervall. Sie können das Intervall auf bis zu *Monatlich* setzen, oder Sie können automatische Pattern-Downloads und -Installationen

gänzlich deaktivieren, indem Sie *Manuell* in der Auswahlliste wählen. Wenn Sie *Manuell* wählen, erscheint eine Schaltfläche *Patterns jetzt aktualisieren* auf der Registerkarte *Übersicht*.

Erweitert

Die Registerkarte *Verwaltung* >> *Up2Date* >> *Erweitert* enthält weitere Konfigurationsmöglichkeiten für die Update-Funktionalität von Astaro Security Gateway, wie der Auswahl eines übergeordneten Proxy (engl. *parent proxy*) oder eines Up2Date-Zwischenspeichers.

Hinweis – Update-Pakete können vom Astaro FTP-Server unter dieser Adresse heruntergeladen werden: <ftp://ftp.astaro.com>.

Manuelles Hochladen von Up2Date-Paketen: Wenn die Firewall keinen direkten Zugang zum Internet oder einem Up2Date-Zwischenspeicher (engl. *Cache*) hat, um Update-Pakete herunterzuladen, so können Sie diese auch manuell auf die Firewall hochladen. Um Update-Pakete manuell hochzuladen, gehen Sie folgendermaßen vor:

1. **Öffnen Sie das Dialogfenster *Upload File*.**
Klicken Sie auf das Ordnersymbol neben dem Eingabefeld *Up2Date-Datei*. Das Dialogfenster *Upload File* öffnet sich.
2. **Wählen Sie das Update-Paket.**
Klicken Sie die Schaltfläche *Durchsuchen* im Dialogfenster *Upload File* und wählen Sie das Update-Paket aus, das Sie hochladen möchten.
3. **Klicken Sie *Save*.**
Das Update-Paket wird auf die Firewall kopiert.
4. **Klicken Sie *Übernehmen*.**
Ihre Einstellungen werden gespeichert.

Übergeordneter Proxy

Ein übergeordneter Proxy (auch *Parent* oder *Upstream* Proxy) wird in Ländern benötigt, in denen der Zugang zum Internet nur über einen staatlich kontrollierten Proxy erlaubt ist. Falls Ihre Sicherheitsbestimmungen die Nutzung eines übergeordneten Proxy erforderlich machen, so können Sie diesen hier durch Angabe einer Rechnerdefinition und eines Ports konfigurieren.

Übergeordneten Proxy verwenden: Wählen Sie diese Option, um einen übergeordneten Proxy zu verwenden. Geben Sie einen Rechnernamen und den Port des Proxy ein.

Dieser Proxy erfordert Authentifizierung: Falls der übergeordnete Proxy Authentifizierung erfordert, geben Sie den Benutzernamen und das Kennwort hier ein.

Falls Sie einen Parent Proxy eingerichtet haben, holt sich Astaro Security Gateway die Update-Pakete von diesem Proxy.

Backups

Mit der Backup-Funktion können Sie die Einstellungen der Firewall auf einer lokalen Festplatte sichern. Mithilfe der Backup-Datei sind Sie in der Lage, eine erprobte Konfiguration auf neu installierte oder fehlkonfigurierte Systeme zu übertragen.

Legen Sie nach jeder Änderung der Systemeinstellungen eine neue Backup-Datei an. Auf diese Weise haben Sie immer die aktuellen Einstellungen Ihres Systems gespeichert. Bewahren Sie dieses Backup an einem sicheren Ort auf, da sicherheitsrelevante Daten wie z. B. Zertifikate und kryptografische Schlüssel darin enthalten sind. Prüfen Sie die Backup-Datei nach der Generierung immer auf Lesbarkeit. Es ist außerdem ratsam, durch ein externes MD5-Programm eine Prüfsumme zu generieren, die es Ihnen auch später ermöglicht, die Integrität der Backup-Datei zu prüfen.

Backup/Wiederherstellen

Um ein Backup mit den aktuellen Systemeinstellungen zu erzeugen, gehen Sie folgendermaßen vor:

1. **Öffnen Sie die Registerkarte *Backup/Wiederherstellen*.**
2. **Geben Sie einen Kommentar an (optional).**
Fügen Sie dem Backup eine Beschreibung oder andere Informationen hinzu.
3. **Klicken Sie *Create Backup Now*.**
Das Backup erscheint in der Liste der verfügbaren Backups.

Die Liste enthält Informationen darüber, wann das Backup erstellt wurde, der Versionsnummer von Astaro Security Gateway Software sowie Informationen über den Benutzer, der das Backup erstellt hat.

Mit den Schaltflächen können Sie entweder einen Systemzustand wiederherstellen (*Restore*), eine Backup-Datei herunterladen (*Download*) oder löschen (*Delete*). Wenn Sie ein Backup herunterladen, geben Sie das Verzeichnis an, in dem das Backup abgespeichert werden soll.

Hinweis – Um Problemen beim Herunterladen von Dateien mit dem Internet Explorer 6 vorzubeugen, fügen Sie die URL der Firewall (z. B. <https://192.168.2.100>) und des Benutzerportals (z. B. <https://192.168.2.100>) den *Vertrauenswürdigen Sites* hinzu. Beim Internet Explorer 6 befinden sich diese Einstellungen im Menü *Extras >> Internetoptionen >> Sicherheit*. Beim Internet Explorer 7 aktivieren Sie zusätzlich im Fenster *Sicherheitseinstellungen* die Funktion *Automatische Eingabeaufforderung für Dateidownloads*.

Beim Herunterladen haben Sie außerdem die Möglichkeit, das Backup zu verschlüsseln (Triple-DES). Geben Sie zu diesem Zweck ein Kennwort an. Prägen Sie sich dieses Kennwort gut ein, da Sie beim Importieren des Backups danach gefragt werden (die Dateierweiterung von verschlüsselten Backups ist *ebf*).

Hinweis – Ein Backup enthält das Administrationskennwort sowie RSA-Schlüssel und X.509-Zertifikate. Da es sich dabei um vertrauliche Informationen handelt, ist eine Verschlüsselung von Backups ratsam.

Um ein Backup zu importieren, klicken Sie auf das Ordnersymbol neben dem Eingabefeld *Backup-Datei*. Wählen Sie die entsprechende Backup-Datei aus und klicken Sie *Save*. Wenn Sie ein verschlüsseltes Backup importieren möchten, geben das Kennwort ein. Beim Importieren des Backups wird Ihre aktuelle Konfiguration nicht überschrieben. Das Backup wird lediglich der Liste aller verfügbaren Backups hinzugefügt.

Darüber hinaus ist es auch möglich, unverschlüsselte Backup-Dateien von einem FAT-formatierten USB-Flashspeicher, wie z. B. einem USB-Stick. Um ein Backup von einem USB-Flashspeicher wiederherzustellen, kopieren Sie die Backup-Datei auf den USB-Flashspeicher und schließen Sie das Gerät an das Astaro Security Gateway an, bevor Sie Astaro Security Gateway hochfahren. Befinden sich mehrere Backup-Dateien auf dem Speichergerät, wird die lexikografisch erste Datei verwendet (Zahlen vor Buchstaben). Nehmen Sie z. B. an, die Backup-Dateien *Firewall_backup_2007-04-17.abf* und *2006-03-20_Firewall_backup.abf* befinden sich beide auf dem USB-Flashspeicher.

Beim Hochfahren wird die zweite Datei verwendet, weil sie mit einer Zahl beginnt, obwohl sie viel älter ist als die erste Datei.

Nach der erfolgreichen Wiederherstellung eines Backups wird eine Sperrdatei (engl. *lock file*) angelegt. Diese verhindert, dass ein- und dasselbe Backup immer wieder installiert wird, während der USB-Flashspeicher noch eingesteckt ist. Sollten Sie ein vorangegangenes Backup dennoch erneut installieren wollen, so müssen Sie den betreffenden Rechner zunächst ohne angeschlossenen USB-Flashspeicher neustarten. Dabei werden alle Sperrdateien gelöscht. Wenn Sie den Rechner nun erneut mit angeschlossenem USB-Flashspeicher hochfahren, kann dasselbe Backup installiert werden.

Automatische Backups

Auf der Registerkarte *Verwaltung >> Backups >> Automatische Backups* haben Sie die Möglichkeit, Backups automatisch erzeugen zu lassen. Gehen Sie dazu folgendermaßen vor:

1. **Aktivieren Sie die Option auf der Registerkarte *Automatische Backups*.**
Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche.
Die Statusampel wird grün und die Abschnitte *Optionen* sowie *Backups per E-Mail versenden* können nun bearbeitet werden.
2. **Legen Sie das Zeitintervall fest.**
Automatisch erzeugte Backups können in verschiedenen Zeitintervallen generiert werden.
Sie haben die Auswahl zwischen täglich, wöchentlich und monatlich.
3. **Legen Sie die maximale Anzahl der zu speichernden Backups fest.**
Backups können bis zu der hier angegebenen Anzahl gespeichert werden. Nachdem die maximale Anzahl erreicht worden ist, werden die ältesten Backup-Dateien gelöscht.
Beachten Sie, dass dies nur auf automatisch erzeugte Backup-Dateien zutrifft. Manuell erzeugte Backup-Dateien werden nicht gelöscht.
4. **Klicken Sie *Übernehmen*.**
Ihre Einstellungen werden gespeichert.

Um Ihnen die Arbeit abzunehmen, Backup-Dateien manuell zu speichern, können Sie sich Backup-Dateien an eine Liste von E-Mail-Adressen schicken lassen.

Empfänger: Automatisch erzeugte Backup-Dateien werden an diejenigen Empfänger geschickt, die im Eingabefeld *Empfänger* eingetragen sind. Es können

mehrere Empfänger eingegeben werden. Standardmäßig ist die E-Mail-Adresse des Administrators voreingestellt.

E-Mail-Backups verschlüsseln: Darüber hinaus können Sie die Backup-Datei verschlüsselt (Triple-DES) verschicken.

Kennwort: Nachdem Sie die Option *E-Mail-Backups verschlüsseln* gewählt haben, müssen Sie nun ein Kennwort angeben. Dieses Kennwort benötigen Sie, wenn Sie das Backup importieren möchten.

Automatisch erzeugte Backups erscheinen in der Liste der verfügbaren Backups auf der Registerkarte *Backup/Wiederherstellen* und sind mit dem Hinweis *System* in der Spalte *Creator* versehen. Von dort aus können sie genau wie manuell erzeugte Backup-Dateien installiert, heruntergeladen oder gelöscht werden.

V6 Backup-Import

Auf der Registerkarte *Verwaltung > > Backups > > V6 Backup-Import* können Sie Backups hochladen, die der Astaro Security Gateway Version 6 angehören.

Hinweis – Nur unverschlüsselte Backups der ASG Software Version 6.303 oder höher können importiert werden. Wenn Sie eine ältere Version installiert haben, aktualisieren Sie diese bitte auf 6.303 bevor Sie ein Backup anlegen, das Sie in ein Gerät mit Version 7 importieren möchten.

Bitte beachten Sie auch die folgenden Einschränkungen die gelten, wenn Sie ein Astaro Security Gateway V6-Backup importieren wollen:

- Nur Backups der Version 6.303 oder höher werden unterstützt.
- HA-Konfiguration wird nicht übernommen.
- Remote-Syslog wird nicht übernommen.
- Site-to-Site- und Fernzugriff-VPN: Nur PPTP-Einstellungen werden übernommen.
- Angriffsschutzeinstellungen werden nicht übernommen.
- Netzwerk- und Dienstgruppen: Gruppen, die andere Gruppen beinhalten, werden aufgespaltet.

- Paketfilter: QoS-Einstellungen der Paketfilterregeln werden nicht übernommen.
- DHCP auf Eth-VLAN wird in V7 nicht unterstützt.
- Konfigurierte, aber deaktivierte Ethernet-Aliasnamen werden nicht übernommen.
- E-Mail-Adressfelder aus V6 (wie z. B. *System >> Settings >> Administrator Contact*) werden nicht übernommen.
- Die HTTP-Proxy-Konfiguration wird nicht übernommen.
- Die SMTP-Proxy-Konfiguration wird nicht übernommen.
- Authentifizierungsdienste für entfernte Benutzer werden nicht übernommen.
- DHCP-Relay wird nicht übernommen.

Um ein ASG V6-Backup hochzuladen, gehen Sie folgendermaßen vor:

1. **Öffnen Sie die Registerkarte *V6-Backup-Import*.**
2. **Wählen Sie eine Backup-Datei aus.**
Klicken Sie auf das Ordnersymbol und wählen Sie eine Backup-Datei aus, die hochgeladen werden soll.
3. **Klicken Sie *Start Upload*.**
Die Backup-Datei wird importiert.

Beachten Sie, dass das Backup nicht sofort installiert wird, sondern der Liste verfügbarer Backups angehängt wird, die sich auf der Registerkarte *Verwaltung >> Backups >> Backup/Wiederherstellen* befindet. Von dort aus kann es wiederhergestellt, heruntergeladen oder gelöscht werden.

Warnung – Nachdem Sie ein Astaro-Security-Gateway-V6-Backup wiederhergestellt haben, überprüfen Sie sorgfältig alle Ihre Einstellungen, bevor Sie die Firewall in Betrieb nehmen.

Benutzerportal

Das Benutzerportal von Astaro Security Gateway ist eine besondere browser-basierte Anwendung in Astaro Security Gateway, die personalisierte Inhalte für den Fernzugriff (engl. *remote access*) bereitstellt und es autorisierten Benutzern ermöglicht, E-Mails zu verwalten. Das Portal ist erreichbar über die URL des Astaro Security Gateway, z. B. `https://192.168.2.100`. Beachten Sie das HTTPS-Protokoll und das Fehlen der Portnummer 4444, wie sie für den Zugriff auf den WebAdmin benötigt wird.

Das Benutzerportal enthält u.a. die sogenannte E-Mail-Quarantäne, die jene Nachrichten enthält, die aufgrund verschiedener Merkmale nicht an den Empfänger weitergeleitet wurden. Zu diesen Merkmalen zählt zum Beispiel, dass sie schädigende oder zweifelhafte Dateianhänge enthalten, als Spam identifiziert wurden, oder bestimmte Ausdrücke enthalten, die Sie explizit verboten haben.

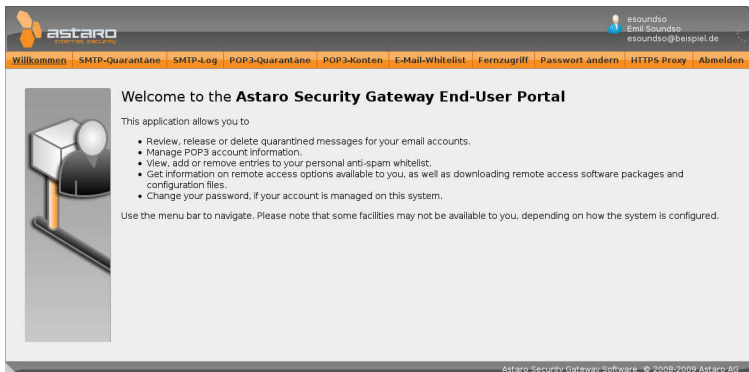


Figure 4.11 Benutzerportal: Benutzerportal von Astaro Security Gateway

Über das Benutzerportal haben Benutzer Zugriff auf die folgenden Dienste:

- **SMTP-Quarantäne:** Benutzer können sich Nachrichten in Quarantäne anschauen und gegebenenfalls freigeben. Welche Arten von Nachrichten sie freigeben dürfen, können Sie auf der Registerkarte *Mail Security >> Quarantänebericht >> Erweitert* festlegen.
- **SMTP-Protokoll:** Benutzer können hier Einblick in das SMTP-Protokoll (engl. *SMTP log*) ihres Mailverkehrs nehmen.
- **POP3-Quarantäne:** Benutzer können sich Nachrichten in Quarantäne anschauen und gegebenenfalls freigeben. Welche Arten von Nachrichten sie

freigegeben dürfen, können Sie auf der Registerkarte *Mail Security* >> *Quarantänebericht* >> *Erweitert* festlegen.

- **POP3-Konten:** Benutzer können hier Ihre Zugangsdaten für externe POP3-Konten eingeben, die sie verwenden. Es werden nur solche Spam-E-Mails im Benutzerportal zu sehen sein, für die POP3-Kontozugangsdaten hinterlegt sind. Benutzer, für die POP3-Kontozugangsdaten gespeichert sind, erhalten einen eigenständigen Quarantänebericht für jede E-Mail-Adresse. Beachten Sie, dass zugelassene POP3-Server auf der Registerkarte *Mail Security* >> *POP3* >> *Erweitert* eingetragen sein müssen.
- **E-Mail-Whitelist:** Nutzer können eine sogenannte Positivliste (engl. *whitelist*) für bestimmte Sender anlegen, dadurch werden Nachrichten von diesen Sendern nicht als Spam angesehen. In der Positivliste können sowohl einzelne gültige E-Mail-Adressen (z. B. *jdoe@example.com*) als auch Adressen einer spezifischen Domäne eingetragen werden, wobei ein Stern (Asterisk) als Platzhalter dient (z. B. **@example.com*).
- **Fernzugriff:** Benutzer können hier Client-Software für den Fernzugriff herunterladen sowie für sie bereitgestellte Konfigurationsdateien. Der Menüpunkt *Fernzugriff* ist allerdings nur zu sehen, wenn für diesen Benutzer der Fernzugriff aktiviert wurde.

Hinweis – Um Problemen beim Herunterladen von Dateien mit dem Internet Explorer 6 vorzubeugen, fügen Sie die URL der Firewall (z. B. *https://192.168.2.100*) und des Benutzerportals (z. B. *https://192.168.2.100*) den *Vertrauenswürdigen Sites* hinzu. Beim Internet Explorer 6 befinden sich diese Einstellungen im Menü *Extras* >> *Internetoptionen* >> *Sicherheit*. Beim Internet Explorer 7 aktivieren Sie zusätzlich im Fenster *Sicherheitseinstellungen* die Funktion *Automatische Eingabeaufforderung für Dateidownloads*.

- **Kennwort ändern:** Benutzer können hier Ihr Kennwort für den Zugang zum Benutzerportal ändern.
- **Abmelden:** Klicken Sie hier, um sich vom Benutzerportal abzumelden. Das ist allerdings nur nötig, wenn Sie *An meine Anmeldung erinnern* beim Anmelden markiert hatten — dabei wird ein sogenanntes Cookie angelegt —

und Sie sich nun explizit abmelden möchten. Dabei wird das Cookie gelöscht. Ansonsten gibt es keinen Grund, die Abmelden-Schaltfläche zu verwenden; es reicht aus, die Registerkarte des Browsers oder das Browserfenster zu schließen.

Allgemein

Über die Registerkarte *Verwaltung* >> *Benutzerportal* >> *Allgemein* legen Sie fest, von welchen Netzwerken aus Zugriff auf das Benutzerportal gewährt werden soll.

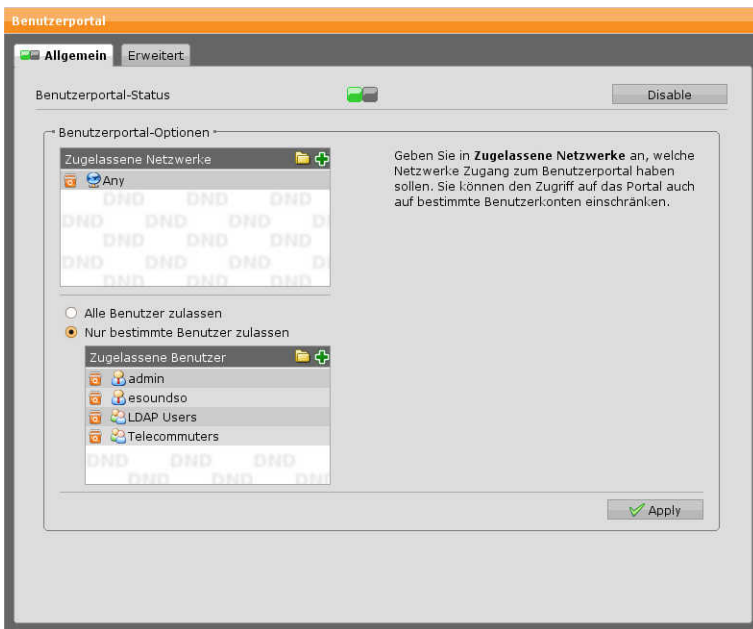


Figure 4.12 Benutzerportal: Zugriffskontrolle für das Benutzerportal

Um den Zugang zum Benutzerportal zu aktivieren, gehen Sie folgendermaßen vor:

1. Aktivieren Sie das Benutzerportal.

Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche.

Die Statusampel wird grün und der Abschnitt *Benutzerportal-Optionen* kann nun bearbeitet werden.

2. Wählen Sie die zugelassenen Netzwerke.

Wählen Sie diejenigen Netzwerke aus, von denen aus Zugriff auf das Benutzerportal möglich sein soll.

3. Wählen Sie die zugelassenen Benutzer.

Wählen Sie die Benutzer oder Benutzergruppen, die Zugriff auf das Benutzerportal haben sollen.

Wenn Sie nicht allen Nutzern aus den erlaubten Netzwerken den Zugriff gestatten möchten, wählen Sie die Option *Nur bestimmte Benutzer zulassen* und wählen Sie die Benutzer oder Benutzergruppen einzeln aus.

4. Klicken Sie Übernehmen.

Ihre Einstellungen werden gespeichert.

Erweitert

Auf der Registerkarte *Erweitert* können Sie einen alternativen Rechnernamen und Port für das Benutzerportal definieren sowie Sprach- und Sicherheitseinstellungen.

Sprache

Während der Anmeldung wertet das Benutzerportal die Spracheinstellungen des Webbrowsers aus und lädt das entsprechende Gebietsschema, um das Benutzerportal in derselben Sprache wie die Standardsprache des Browsers anzuzeigen. Sollte der Browser eine Sprache als Standardeinstellungen haben, die im Benutzerportal nicht verfügbar ist, können Sie hier angeben, welche Sprache als Ersatzsprache verwendet werden soll.

Sicherheit

Das Portal verwendet Cookies zur Sitzungsverwaltung. Dauerhafte Cookies ermöglichen dem Benutzer nach dem Schließen einer Sitzung später zurückzukehren ohne sich neu anmelden zu müssen. Cookies können jederzeit durch den Benutzer selbst gelöscht werden, indem dieser im Menü auf *Abmelden* klickt.

Portal-Einträge deaktivieren

Für die hier angegebenen Funktionen befindet sich ein Menüeintrag im Benutzerportal, wenn die entsprechende Funktion in WebAdmin aktiviert wurde. Sie können aber Menüeinträge bestimmen, die *nicht* im Benutzerportal angezeigt werden sollen. Wählen Sie hierzu die entsprechende(n) Option(en) aus und klicken Sie *Übernehmen*.

Rechnername and Port

Standardmäßig ist der Rechnername der Firewall voreingestellt, wie er auf der Registerkarte *Mail Security >> SMTP >> Erweitert* konfiguriert ist. Es ist jedoch möglich, hier einen anderen Rechnernamen einzutragen.

Der HTTPS-Port ist standardmäßig 443. Sie können die Portnummer jedoch entweder auf 80 oder auf jeden beliebigen Wert zwischen 1024 und 65535 ändern. Beachten Sie, dass Sie weder den Port 10443 noch den Port für den WebAdmin-Zugriff (WebAdmin TCP-Port) auswählen können, wie er auf der Registerkarte *Verwaltung >> WebAdmin-Einstellungen >> Allgemein* konfiguriert ist.

Der Spam-Bericht, der täglich von der Firewall verschickt wird, enthält Hyperlinks, auf die der Benutzer klicken kann, um eine Nachricht aus der Quarantäne freizugeben. Standardmäßig zeigen diese Hyperlinks auf den Rechnernamen der Firewall. Wenn Sie allerdings Zugriff auf das Benutzerportal über das Internet gestatten möchten, so ist es sinnvoll, hier einen alternativen Rechnernamen einzutragen, der öffentlich aufgelöst werden kann.

Begrüßungstext

Sie können den Begrüßungstext des Benutzerportals anpassen. Einfache HTML-Befehle und Hyperlinks sind gestattet.

Benachrichtigungen

Astaro Security Gateway verfügt über eine Benachrichtigungsfunktion, die Sie sofort per E-Mail oder SNMP über alle sicherheitsrelevanten Vorgänge auf der Firewall informiert. Alle Ereignisse, die für einen Administrator von Interesse sein könnten, haben ihre eigene Fehler-, Warn- und Informations-Kodierung. Welche Benachrichtigungen verschickt werden, hängt von den Einstellungen ab, die Sie auf der Registerkarte *Benachrichtigungen* gemacht haben.

Allgemein

Auf der Registerkarte *Verwaltung >> Benachrichtigungen >> Allgemein* können Sie die Absenderadresse konfigurieren, die für das Versenden von Benachrichtigungen von der Firewall verwendet werden soll. Standardmäßig ist dies `do-not-reply@fw-notify.net`. Falls Sie diese Einstellung ändern möchten, ist es ratsam, eine E-Mail-Adresse aus Ihrer Domäne zu wählen, da manche Mail-Server überprüfen, ob die Absender-Adresse einer empfangenen Nachricht tatsächlich existiert.

Darüber hinaus können Sie einen oder mehrere Empfänger für die Benachrichtigungen der Firewall festlegen. Standardmäßig ist dies die E-Mail-Adresse des Administrators, die Sie während der ersten Einrichtung angegeben haben.

Benachrichtigungen begrenzen: Einige sicherheitsrelevante Ereignisse, z. B. erkannte Angriffsversuche, erzeugen eine Vielzahl von Benachrichtigungen, was schnell dazu führen kann, dass die Postfächer der Empfänger verstopfen. Zu diesem Zweck verfügt Astaro Security Gateway über angemessene Voreinstellungen, um die Anzahl der Benachrichtigungen, die pro Stunde verschickt werden, zu begrenzen. Falls Sie diese Option deaktivieren, erzeugt jedes sicherheitsrelevante Ereignis eine Benachrichtigung; vorausgesetzt natürlich, dieses Ereignis ist auf der Registerkarte *Verwaltung* >> *Benachrichtigungen* >> *Benachrichtigungen* entsprechend konfiguriert.

Gerätespezifischer Text

Hier können Sie eine Beschreibung von Astaro Security Gateway eingeben, z. B. seinen Standort. Diese wird dann in den Benachrichtigungen angezeigt, die verschickt werden.

Benachrichtigungen

Benachrichtigungen sind in drei Kategorien unterteilt:

- **CRIT:** Eine Nachricht über ein kritisches Ereignis, das den fehlerfreien Betrieb der Firewall gefährdet.
- **WARN:** Ein Warnhinweis über ein potenzielles Problem, das Ihre Aufmerksamkeit erfordert, z. B. das Überschreiten von Grenzwerten.
- **INFO:** Eine rein informative Benachrichtigung, z. B. bezüglich des Neustarts einer Systemkomponente.

Für jedes einzelne Ereignis können Sie bestimmen, ob eine Benachrichtigung als E-Mail oder SNMP-Trap verschickt werden soll.

Erweitert

Für den Fall, dass Ihre ASG E-Mails nicht direkt senden kann, können Sie einen Smarthost für den E-Mail-Versand einrichten. Gehen Sie dazu folgendermaßen vor:

1. **Aktivieren Sie den Externen SMTP-Server auf der Registerkarte *Verwaltung* >> *Benachrichtigungen* >> *Erweitert*.**

Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche.

2. Geben Sie Ihren Smarthost ein.

Sie können dafür Drag&Drop verwenden. Der Port wird auf den SMTP-Port 25 voreingestellt.

- **TLS verwenden:** Wählen Sie diese Option, wenn Sie TLS für den Versand von Benachrichtigungen erzwingen wollen.
Beachten Sie, dass Benachrichtigungen nicht versendet werden, wenn der Smarthost TLS nicht unterstützt.

3. Klicken Sie *Übernehmen*.

Ihre Einstellungen werden gespeichert.

Falls der Smarthost Authentifizierung erfordert, geben Sie den entsprechenden Benutzernamen und Kennwort für den Smarthost im Abschnitt *SMTP-Authentifizierung* ein. Klicken Sie *Übernehmen*, um Ihre Einstellungen zu speichern.

Anpassung

Über die Registerkarten im Menü *Verwaltung* >> *Anpassung* können verschiedene Vorlagen angepasst und lokalisiert werden, die von Astaro Security Gateway zur Erzeugung von Statusmeldungen und E-Mail-Benachrichtigungen verwendet werden. Damit sind Sie in der Lage, diverse Meldungen der Firewall Ihren Richtlinien oder Ihrer Unternehmensidentität (Corporate Identity) anzupassen.

Allgemein

Auf der Registerkarte *Verwaltung* >> *Anpassung* >> *Allgemein* können Sie allgemeine Einstellungen für Statusmeldungen vornehmen. Beachten Sie, dass UTF-8/Unicode unterstützt wird.

Company Logo: Hier können Sie Ihr eigenes Firmenlogo/-banner (im jpg-Format) hochladen. Dieses Logo wird in den folgenden Kontexten:

- HTTP-Statusmeldungen
- Blockierte POP3-E-Mails

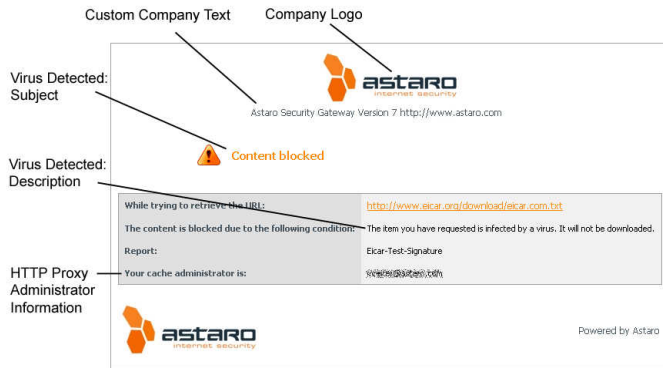


Figure 4.13 Anpassung: Beispiel einer blockierten Webseite mit Angabe der anpassbaren Elemente

- Freigabemeldungen von E-Mails aus der Quarantäne. Diese Meldungen erscheinen, nachdem eine Spam-E-Mail über den täglichen Quarantänebericht freigegeben wurde oder der Sender als vertrauenswürdig eingestuft wurde (durch Klick auf den Hyperlink *Whitelist*).
- Quarantänebericht

Begrenzen Sie die Auflösung des Logos auf einen angemessenen Wert (z. B. 100 x 200 Pixel).

Um ein Firmenlogo zu hochzuladen, gehen Sie folgendermaßen vor:

1. **Öffnen Sie das Dialogfenster *Upload File*.**
Klicken Sie dazu auf das Ordnersymbol neben dem Eingabfeld *Neues Logo hochladen*.
Das Dialogfenster *Upload File* wird geöffnet.
2. **Wählen Sie das Firmenlogo.**
Wechseln Sie in das Verzeichnis, wo sich das Firmenlogo befindet. Wählen Sie das Logo aus und klicken Sie anschließend auf die Schaltfläche *Save*.
3. **Klicken Sie *Übernehmen*.**
Das Firmenlogo wird hochgeladen und ersetzt die bereits vorhandene Datei.

Custom Company Text: Hierbei handelt es sich um den Text unterhalb des Firmenlogos auf der Standard-Fehlermeldungseite, die vom Browser angezeigt

wird, wenn ein Nutzer eine Website öffnet, die vom Virenschanner oder dem Inhaltsfilter blockiert wird. Sie können hier z. B. die Kontaktdaten des Administrators eintragen. Beachten Sie, dass eine Website aufgrund mehrerer Gründe blockiert werden kann, z. B. weil sie zu einer URL-Kategorie gehört, die explizit verboten ist, oder als Spyware (Spionagesoftware) eingestuft wurde, oder falls der Benutzer eine Datei herunterladen möchte, deren Erweiterung als kritisch eingestuft wird (z. B. ausführbare Dateien). Die Vorlagen für diese Vorkommnisse können auf der Registerkarte *Verwaltung >> Anpassung >> HTTP/S-Proxy* geändert werden.

HTTP/S-Proxy

Passen Sie hier die Vorlagen für Meldungen an, die vom HTTP/S-Proxy angezeigt werden, wenn versucht wird, auf blockierte Websites zuzugreifen. Die Meldungen beziehen sich dabei auf die jeweilige Ursache der Blockierung. Sie können die Vorlagen in andere Sprachen übersetzen oder sie zusätzlich um Kontaktinformationen erweitern, um nur einige Beispiele zu nennen. Die folgenden Vorlagen können angepasst werden:

- **HTTP-Proxy-Administratorangaben:** Hier können Sie Informationen über den Administrator des HTTP-Proxy eintragen. Zusätzlich können Sie die E-Mail-Adresse des Administrators angeben.
- **Inhalt blockiert von Surf Protection:** Diese Meldung wird angezeigt, wenn ein Benutzer versucht, eine blockierte Webseite zu öffnen.
- **Inhalt durch Blacklist blockiert:** Diese Meldung erscheint beim Öffnen einer Webseite, die auf der URL-Negativliste (engl. *Blacklist*) steht. Mehr Informationen zur Blacklist-Funktion finden Sie auf der Registerkarte *Web Security >> HTTP/S >> URL-Filterung*.
- **Virus gefunden:** Diese Meldung erscheint, wenn eine Datei entdeckt wurde, die einen Virus enthält.
- **Datei wird heruntergeladen:** Diese Meldung erscheint, wenn eine Datei gerade heruntergeladen wird.
- **Virenschan:** Diese Meldung erscheint, wenn eine Datei gerade auf Viren überprüft wird.

- **Herunterladen der Datei abgeschlossen:** Diese Meldung wird angezeigt, nachdem eine Datei komplett heruntergeladen und gescannt worden ist.
- **Transparenzmodus mit Authentifizierung:** Dieser Abschnitt ist nur von Bedeutung, wenn Sie den Proxy im *Transparenzmodus mit Authentifizierung* betreiben. Dieser Text wird auf der Authentifizierungsseite angezeigt, auf der jeder Benutzer sich anmelden muss, bevor er den Proxy verwenden kann. Das Feld *Nutzungsbedingungen* ist standardmäßig leer, das heißt, dass auf der Authentifizierungsseite keine Nutzungsbedingungen angezeigt werden. Wenn Sie Nutzungsbedingungen anzeigen wollen, die Benutzer akzeptieren müssen, geben Sie diese in diesem Feld an. Sie können die Nutzungsbedingungen auch wieder deaktivieren, indem Sie das Feld *Nutzungsbedingungen* leeren.

Download-Verwaltung

Wenn der HTTP/S-Proxy aktiviert ist, zeigt der Webbrowser die folgenden Statusmeldungen an, sobald ein Benutzer versucht, Inhalte von mehr als 1 MB Größe herunterzuladen, die kein Text oder Bild sind. Beachten Sie, dass keine Statusmeldungen angezeigt werden, wenn Video- oder Audio-Streams angefordert werden oder wenn mehr als 50% einer Datei innerhalb von fünf Sekunden heruntergeladen wurde.

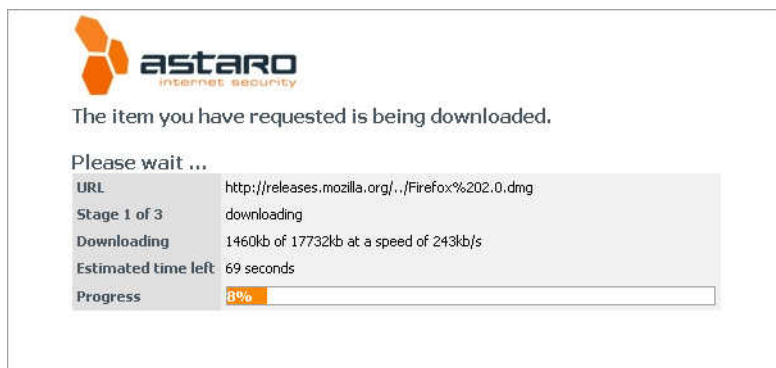


Figure 4.14 HTTP-Proxy: HTTP-Statusmeldung Schritt 1 von 3

SMTP-/POP3-Proxy

Passen Sie hier diejenigen Vorlagen an, die vom SMTP- und POP3-Proxy erzeugt werden. Sie können diese Vorlagen in andere Sprachen übersetzen oder

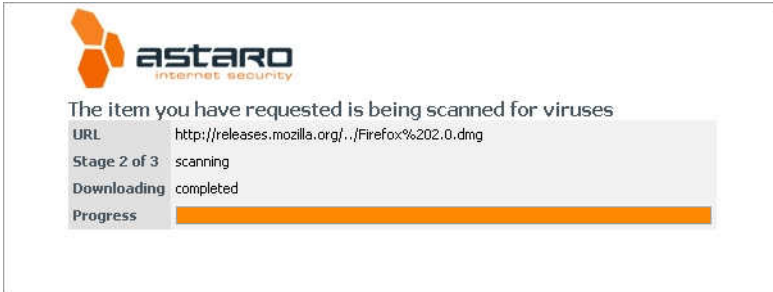


Figure 4.15 HTTP-Proxy: HTTP-Statusmeldung Schritt 2 von 3

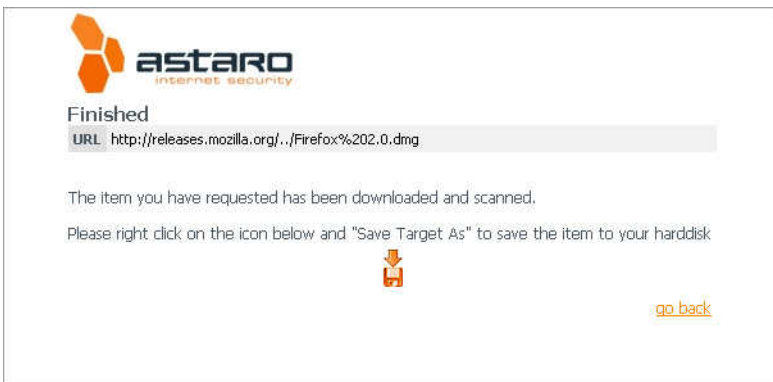


Figure 4.16 HTTP-Proxy: HTTP-Statusmeldung Schritt 3 von 3

sie zusätzlich um Kontaktinformationen erweitern, um nur einige Beispiele zu nennen. Die folgenden Vorlagen können angepasst werden:

- **Nachricht aus Quarantäne freigeben:** Diese Meldung wird angezeigt, wenn eine E-Mail erfolgreich aus der Quarantäne freigeben wurde.
- **Bei der Quarantäne-Freigabe der Nachricht ist ein Fehler aufgetreten:** Diese Meldung wird angezeigt, wenn ein Fehler während der Freigabe einer E-Mail aus der Quarantäne aufgetreten ist.
- **POP3-Nachricht blockiert:** Diese Meldung erscheint, wenn eine POP3-Nachricht blockiert wurde.



Figure 4.17 POP3-Proxy: Blockierte POP3-Nachricht

SNMP

Das *Simple Network Management Protocol* (SNMP) wird dazu benutzt, um Netzwerkelemente wie z. B. Router, Server oder Switches von einer zentralen Station aus überwachen und steuern zu können. SNMP ermöglicht es einem Administrator, sich schnell einen Überblick über den Zustand der überwachten Netzwerkgeräte zu verschaffen. Sie können Astaro Security Gateway dahingehend konfigurieren, SNMP-Anfragen zum Systemzustand zu beantworten oder SNMP-Traps an SNMP-Verwaltungswerkzeuge zu verschicken. Ersteres wird mit Hilfe von sogenannten *Management Information Bases* (MIBs) erreicht. Eine MIB definiert, welche Informationen zu welchen Netzwerkelementen abgerufen werden können. Astaro Security Gateway unterstützt die folgenden MIBs:

- **DISMAN-EVENT-MIB:** Event Management Information Base
- **HOST-RESOURCES-MIB:** Host Resources Management Information Base
- **IF-MIB:** Interfaces Group Management Information Base
- **IP-FORWARD-MIB:** IP Forwarding Table Management Information Base
- **IP-MIB:** Management Information Base for the Internet Protocol (IP)
- **NOTIFICATION-LOG-MIB:** Notification Log Management Information Base
- **RFC1213-MIB:** Management Information Base for Network Management of TCP/IP-based Internets: MIB II

- **SNMPv2-MIB:** Management Information Base for the Simple Network Management Protocol (SNMP)
- **TCP-MIB:** Management Information Base for the Transmission Control Protocol (TCP)
- **UDP-MIB:** Management Information Base for the User Datagram Protocol (UDP)

Um Systeminformationen von Astaro Security Gateway zu erhalten, müssen Sie einen SNMP-Manager verwenden, der zumindest gegen die RFC1213-MIB (MIB II) kompiliert ist.

Anfrage

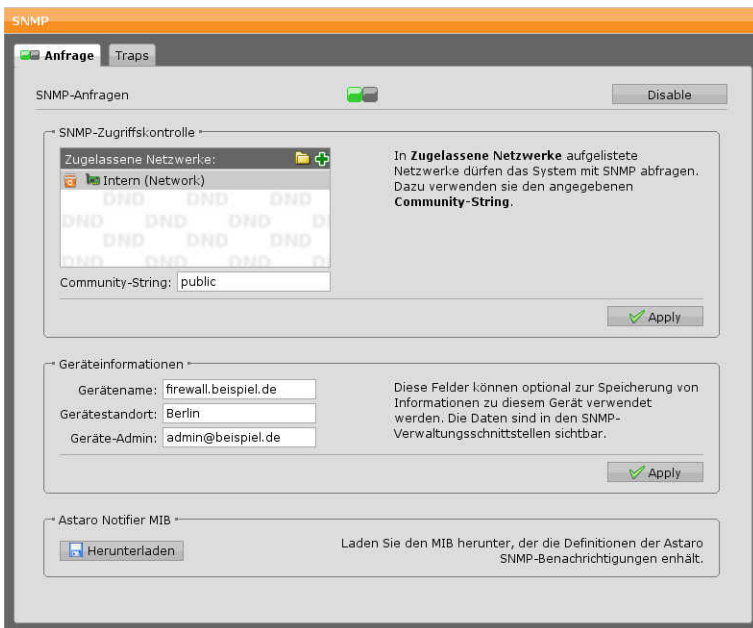


Figure 4.18 SNMP: Konfiguration von SNMP-Anfragen

SNMP-Anfragen konfigurieren:

1. **Aktivieren Sie SNMP-Anfragen.**

Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche.

2. **Wählen Sie Zugelassene Netzwerke aus.**

Netzwerke im Eingabefeld *Zugelassene Netzwerke* dürfen Anfragen an den SNMP-Agenten von Astaro Security Gateway stellen. Beachten Sie, dass der Zugriff nur lesend (engl. *read-only*) erfolgt.

3. **Geben Sie einen Community-String ein.**

Ein SNMP-Community-String dient als eine Art Kennwort für den Zugriff auf den SNMP-Agenten.

Standardmäßig ist „public“ als SNMP-Community-String voreingestellt. Sie können diesen Wert nach Ihren Bedürfnissen ändern.

Hinweis – Der Community-String darf aus folgenden Zeichen bestehen: (a-z), (A-Z), (0-9), (+), (_, (@), (.), (-), (Leerzeichen).

4. **Klicken Sie Übernehmen.**

Ihre Einstellungen werden gespeichert.

Darüber hinaus können Sie zusätzliche Informationen zu der Firewall angeben:

Geräteinformationen

Mit den Eingabefeldern im Abschnitt *Geräteinformationen* können Sie die Firewall weiter spezifizieren, z. B. durch Angabe eines Gerätenamens, des Ortes oder des zuständigen Administrators. Diese Informationen können von SNMP-Verwaltungswerkzeugen gelesen werden und helfen bei der Identifikation der Firewall.

Hinweis – Beachten Sie, dass der gesamte SNMP-Datenstrom (Protokollversion 2) zwischen der Firewall und den zulässigen Netzwerken unverschlüsselt erfolgt und bei einem Transfer über öffentliche Netze mitgelesen werden kann.

Astaro Notifier MIB

In diesem Abschnitt können Sie den Astaro „Notifier Management Information Base“ (MIB) herunterladen, der die Definitionen der Astaro SNMP-Benachrichtigungen enthält, die auf Ihren aktuellen Einstellungen für die Benachrichtigungs-Traps basiert.

Traps

Auf der Registerkarte *Traps* können Sie einen SNMP-Trap-Server auswählen, an den Benachrichtigungen über relevante Ereignisse auf der Firewall per SNMP-Trap verschickt werden können. Beachten Sie, dass spezielle SNMP-Überwachungssoftware benötigt wird, um die Traps anzeigen zu können.

Die als SNMP-Traps verschickten Nachrichten enthalten einen sogenannten *Object Identifier* (Objektidentifizierungsnummer) (OID), z. B. .1.3.6.1.4.1.9789. Diese OID setzt sich zusammen aus dem Präfix .1.3.6.1.4.1, das für `iso.org.dod.internet.private.enterprise` steht, sowie aus der privaten *Enterprise Number* (Unternehmensnummer) der Astaro AG. Unternehmen können jederzeit eine eigene Nummer unterhalb des erwähnten Präfixes bei der IANA¹³ beantragen. Die OID für Benachrichtigungen von Astaro Security Gateway ist 1500, an die wiederum die OID des Typs der Benachrichtigung und die der dazugehörigen Fehlerkodierung (000-999) angehängt wird. Die folgenden Benachrichtigungstypen sind verfügbar:

- DEBUG = 0
- INFO = 1
- WARN = 2
- CRIT = 3

Beispiel: Die Benachrichtigung „INFO-302: New firmware Up2Date installed“ verwendet die OID .1.3.6.1.4.1.9789.1500.1.302 und bekommt den folgenden Bezeichnung zugewiesen:

```
[<HOST>][INFO][302]
```

Beachten Sie, dass <HOST> ein Platzhalter für den Rechnernamen darstellt und dass nur Typ und Fehlercode aus der Betreffzeile der Benachrichtigung übermittelt werden.

Um einen SNMP-Trap-Server zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf *Neuer SNMP-Trap-Server*.**

Das Dialogfenster *Neuen SNMP-Trap-Server erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Rechner: Die Rechner-Definition für den SNMP-Trap-Server.

¹³ <http://www.iana.org>

Community: Ein SNMP-Community-String dient als eine Art Kennwort für den Zugriff auf den SNMP-Agenten. Standardmäßig ist „public“ als SNMP-Community-String voreingestellt. Tragen Sie hier den Community-String ein, der auf dem SNMP-Trap-Server konfiguriert ist.

Hinweis – Der Community-String darf aus folgenden Zeichen bestehen: (a–z), (A–Z), (0–9), (+), (_), (@), (.), (-), (Leerzeichen).

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über den SNMP-Trap-Server hinzu.

3. Klicken Sie **Save**.

Die neue SNMP-Trap-Server-Definition erscheint auf der Registerkarte *Traps*.

Zentralverwaltung

Über das Menü *Verwaltung* > *Zentralverwaltung* können Sie Schnittstellen zu Verwaltungswerkzeugen konfigurieren, die benutzt werden können, um die Firewall aus der Ferne zu verwalten.

Astaro Command Center

Astaro Command Center (ACC) ist Astaros Produkt zur zentralen Verwaltung und stellt die folgenden Funktionen für die von ihm verwalteten ASGs zur Verfügung: Überwachung, Konfiguration, Wartung und Inventarisierung. Dabei kann Astaro Command Center von mehreren Administratoren gleichzeitig bedient werden. Astaro Command Center gibt einen allgemeinen Überblick über den Zustand jeder verbundenen Astaro Gateway Appliance- und Software-Installation. Dazu gehören Informationen wie Versionsnummer, aktuelle Auslastung, Ablaufdatum der Lizenz sowie sicherheitsrelevante Ereignisse. Die Informationen werden über ein grafisches Web-Frontend präsentiert, das verschiedene Darstellungsmöglichkeiten für alle überwachten Geräte bietet. Das ACC-Inventarsystem behält dabei automatisch die Übersicht über jedes Gerät. Bei mehreren Administratoren können diesen unterschiedliche Zugriffsrechte zugewiesen werden – das macht den ACC zur perfekten Lösung für Astaro Partner und MSSPs (*Managed Security Service Provider*). Mehr Informationen zu Astaro Command Center finden Sie im ACC-Datenblatt, das Sie von der Astaro-Website¹⁴ herunterladen können.

¹⁴ http://www.astaro.com/our_products/management_tools/astaro_command_center

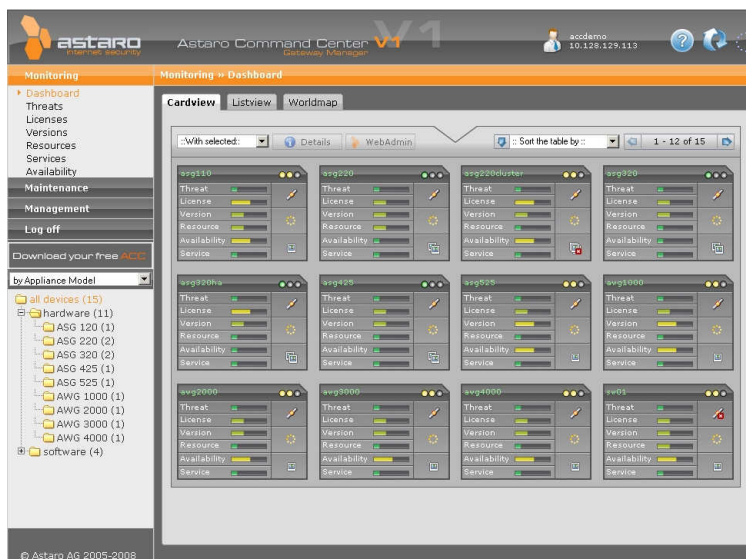


Figure 4.19 Zentralverwaltung: Dashboard von Astaro Command Center

Einrichtung von ACC V2.0

Damit Astaro Security Gateway von einem ACC Server überwacht werden kann, führen Sie die folgenden Schritte durch:

1. **Aktivieren Sie auf der Registerkarte *Astaro Command Center* die ACC-Funktion.**
Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche.
Die Statusampel wird gelb und der Abschnitt *ACC-Einstellungen* kann nun bearbeitet werden.
2. **Wählen Sie die Serverversion ACC V2.x aus (Standard).**
Alle Eingabefelder auf dieser Seite werden aktiviert.
3. **Geben Sie den ACC-Rechner an.**
Wählen oder legen Sie den ACC-Server an, zu dem sich Astaro Security Gateway verbinden soll.
4. **Klicken Sie *Übernehmen*.**
Ihre Einstellungen werden gespeichert und die Authentifizierungsfelder können bearbeitet werden.

Astaro Security Gateway kann nun über den ausgewählten ACC Server überwacht und verwaltet werden.

- **Geben Sie an, ob Ihr ACC-Server Authentifizierung erfordert (optional).**

Wählen Sie die Option *Authentifizierung* und geben Sie das Kennwort (*Vereinbarter Schlüssel*, engl. *Shared Secret*) ein, das auf dem ACC-Server festgelegt wurde.

- **Setzen Sie den ACC-Server als Up2Date-Zwischenspeicher (optional).**

Up2Date-Pakete können von einem Zwischenspeicher (engl. *cache*) geholt werden, der sich auf dem ACC-Server befindet. Wenn Sie diese Funktionalität für Ihre Firewall verwenden wollen, wählen Sie die Option *ACC-Server als Up2Date-Zwischenspeicher verwenden*. Bitte stellen Sie sicher, dass der Administrator des ACC, der Ihr Gerät verwaltet, die Up2Date-Zwischenspeicher-Funktionalität auf dem Server aktiviert hat. Beachten Sie, dass die Verwendung der Up2Date-Zwischenspeicher-Funktionalität und eines übergeordneten Proxy für Up2Date-Pakete sich gegenseitig ausschließen.

5. Klicken Sie **Übernehmen**.

Ihre Einstellungen werden gespeichert. Kurz darauf kann Astaro Security Gateway durch den angegebenen ACC-Server überwacht und verwaltet werden. Sie können den aktuellen Verbindungsstatus und Gesundheitszustand im Abschnitt *ACC-Zustand* sehen. Ein Neuladen der Seite aktualisiert diese Daten. Bitte verwenden Sie das *Live-Protokoll*, um weitere Informationen zu erhalten, falls es Verbindungsprobleme geben sollte.

Hinweis – Beachten Sie, dass die Firewall und der ACC-Server über Port 4433 miteinander kommunizieren, wohingegen der ACC-Server V1.9 mit einem Browser über das HTTPS-Protokoll auf Port 4444 (WebAdmin) bzw. auf Port 4422 (Gateway Manager) erreicht werden kann.

Einrichtung von ACC V1.4

Damit Astaro Security Gateway von einem ACC Server überwacht werden kann, führen Sie die folgenden Schritte durch:

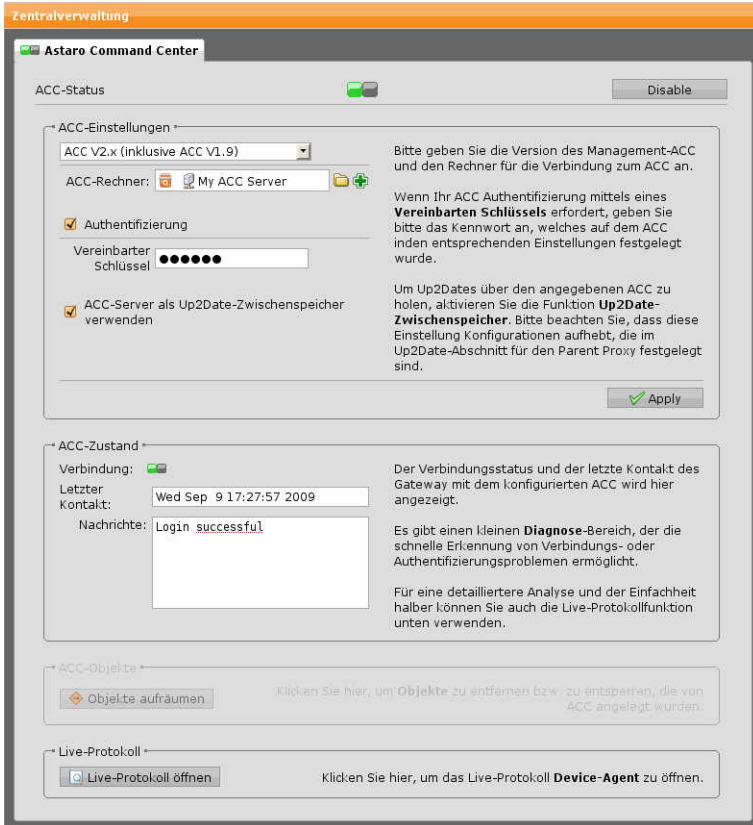


Figure 4.20 Zentralverwaltung: Konfiguration der zentralen Verwaltung durch einen ACC V1.9-Server

1. **Aktivieren Sie auf der Registerkarte *Astaro Command Center* die ACC-Funktion.**

Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche.

Die Statusampel wird gelb und der Abschnitt *ACC-Einstellungen* kann nun bearbeitet werden.

2. **Wählen Sie die Serverversion *ACC V1.4* aus (Standard).**

Eingabefelder auf dieser Seite, die nicht benötigt werden, werden deaktiviert.

3. Geben Sie den ACC-Rechner an.

Wählen oder legen Sie den ACC-Server an, zu dem sich Astaro Security Gateway verbinden soll.

- **Geben Sie an, ob Ihr ACC-Server Authentifizierung erfordert (optional).**

Wählen Sie die Option *Authentifizierung* und geben Sie das Kennwort (*Vereinbarter Schlüssel*, engl. *Shared Secret*) ein, das auf dem ACC-Server festgelegt wurde.

- **Setzen Sie den ACC-Server als Up2Date-Zwischenspeicher (optional).**

Up2Date-Pakete können von einem Zwischenspeicher (engl. *cache*) geholt werden, der sich auf dem ACC-Server befindet. Wenn Sie diese Funktionalität für Ihre Firewall verwenden wollen, wählen Sie die Option *ACC-Server als Up2Date-Zwischenspeicher verwenden*. Bitte stellen Sie sicher, dass der Administrator des ACC, der Ihr Gerät verwaltet, die Up2Date-Zwischenspeicher-Funktionalität auf dem Server aktiviert hat. Beachten Sie, dass die Verwendung der Up2Date-Zwischenspeicher-Funktionalität und eines übergeordneten Proxy für Up2Date-Pakete sich gegenseitig ausschließen.

4. Klicken Sie *Übernehmen*.

Ihre Einstellungen werden gespeichert. Kurz darauf kann Astaro Security Gateway durch den angegebenen ACC-Server überwacht und verwaltet werden. Bitte verwenden Sie das *Live-Protokoll*, um weitere Informationen zu erhalten, falls es Verbindungsprobleme geben sollte.

Hinweis – Beachten Sie, dass die Firewall und der ACC-Server über Port 4433 miteinander kommunizieren, wohingegen der ACC-Server V1.4 mit einem Browser über das HTTPS-Protokoll auf Port 443 erreicht werden kann.

ACC-Objekte

Der Abschnitt *ACC-Objekte* ist deaktiviert (ausgegraut), es sei denn es gibt Objekte, die von einem ACC aus angelegt wurden und dieser ACC ist nun von Astaro Security Gateway getrennt. ACC-erzeugte Objekte können Netzwerkdefinitionen, Definitionen entfernter Rechner, IPSec-VPN-Tunnel und Ähnliches sein.

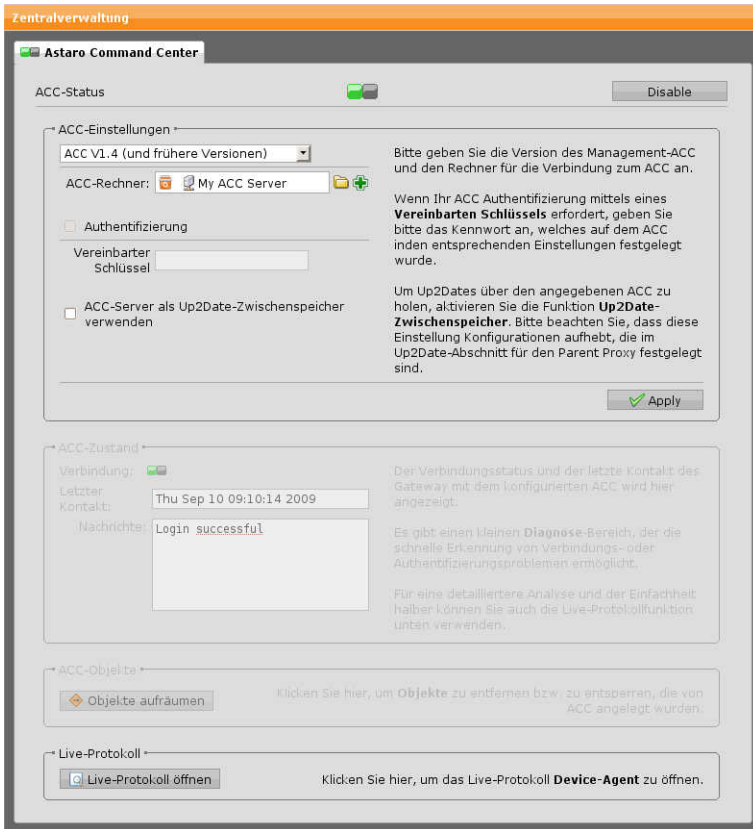


Figure 4.21 Zentralverwaltung: Konfiguration der zentralen Verwaltung durch einen ACC V1.4-Server

Die Schaltfläche *Objekte aufräumen* kann angeklickt werden, um alle Objekte freizugeben, die vom ACC angelegt wurden, mit dem das Gerät ehemals verwaltet wurde. Diese Objekte sind normalerweise gesperrt und können nur auf dem lokalen Gerät eingesehen werden. Nach Betätigung der Schaltfläche werden die Objekte voll zugänglich und können vom lokalen Administrator wiederverwendet oder gelöscht werden.

Hinweis – Wenn ehemalige ACC-erzeugte Objekte aufgeräumt wurden, können sie nicht zurückgewandelt werden, wenn das Gerät wieder mit demselben ACC verbunden wird. Das bedeutet, wenn ein entfernter ACC noch Objektdefinitionen für ein Gerät bereithält, das sich später mit ihm wiederverbindet, so

werden diese Objekte erneut auf das Gerät übertragen – obwohl dann bereits lokale Kopien existieren.

Live-Protokoll

Sie können das Live-Protokoll verwenden, um die Verbindung zwischen Ihrem Astaro Security Gateway und dem ACC zu beobachten. Klicken Sie *Live-Protokoll öffnen*, um das Live-Protokoll in einem neuen Fenster zu öffnen.

Hochverfügbarkeit

In den allermeisten Fällen ist ein Hardware-Fehler für den Ausfall eines Internetsicherheitssystems verantwortlich. Die Fähigkeit eines Systems, bei Ausfall einer seiner Komponenten einen uneingeschränkten Betrieb zu gewährleisten, wird auch Failover bzw. Hochverfügbarkeit genannt (abgekürzt HA, abgeleitet von engl. *High-Availability*). Astaro Security Gateway bietet Hochverfügbarkeit, indem es ermöglicht, ein redundantes *Hot-Standby*-System zu konfigurieren, das im Falle eines technischen Versagens des Primärsystems dessen Aufgaben übernimmt (active-passive). Alternativ dazu können Sie Astaro Security Gateway als *Cluster* konfigurieren, welcher speziellen Datenverkehr auf mehrere Maschinen verteilt (active-active), wie man es von konventionellen Lösungen zur Lastverteilung kennt. Das führt zu optimaler Ressourcenauslastung und verringert Rechenzeit.

Die Konzepte *Hochverfügbarkeit* und *Cluster* sind von der Implementierung her in Astaro Security Gateway eng miteinander verwandt. So kann z. B. ein hochverfügbares System als ein Zwei-Knoten-Cluster angesehen werden, was die Mindestanforderung an ein redundantes System darstellt.

Jeder Knoten innerhalb eines Clusters kann eine der folgenden Rollen annehmen:

- **Master:** Das Primärsystem in einem Hot-Standby-/Cluster-Aufbau. Innerhalb eines Clusters sorgt der Master für die Synchronisation und Verteilung der Daten.
- **Slave:** Das Sekundärsystem in einem Hot-Standby-/Cluster-Aufbau, das den Betrieb sicherstellt, falls das Primärsystem ausfällt.
- **Worker:** Ein einfacher Cluster-Knoten zur Datenverarbeitung.

Alle Knoten überwachen sich gegenseitig mithilfe eines sogenannten Heartbeat-Signals, ein in periodischen Abständen verschicktes Multicast-UDP-Datenpaket. Über diese Verbindung benachrichtigen sich alle Knoten gegenseitig, dass sie noch betriebsbereit, sprich „am Leben“ sind (daher der Begriff *Heartbeat*, dt. Herzschlag). Falls aufgrund eines technischen Defekts einer der Knoten kein Heartbeat-Signal mehr aussenden kann, wird er für „tot“ erklärt. Abhängig von der Rolle, die der Knoten innehatte, ändert sich die Konfiguration des Aufbaus wie folgt:

- Falls der Master-Knoten ausfällt, übernimmt der Slave-Knoten seinen Platz und der Worker-Knoten mit der höchsten ID wird Slave.
- Falls der Slave-Knoten ausfällt, wird der Worker-Knoten mit der höchsten ID zum Slave.
- Falls ein Worker-Knoten ausfällt, bemerken Sie im Höchstfall Leistungseinbußen aufgrund der verringerten Rechenleistung. Die Ausfallsicherheit ist nicht beeinträchtigt.

Berichte

Alle Berichtsdaten werden auf dem Master-Knoten konsolidiert und in Abständen von fünf Minuten auf die anderen Knoten übertragen. Im Falle einer Übernahme durch das Sekundärsystem verlieren Sie daher höchstens fünf Minuten an Daten. Es gibt allerdings einen Unterschied in Bezug auf die Akkumulation von Daten. Die Graphen auf der Registerkarte *Berichte >> Hardware* repräsentieren lediglich Daten des Knotens, der gerade Master ist. Netzwerkverkehrsdaten wiederum, wie sie beispielsweise auf der Seite *Netzwerknutzung* erscheinen, repräsentieren Daten von allen beteiligten Knoten. So zeigt z. B. das Histogramm der heutigen CPU-Auslastung die aktuelle Prozessorauslastung des Master-Knotens. Im Falle einer Übernahme durch den Slave wären dies dann die Daten des Slave. Im Gegensatz dazu sind z. B. die Informationen *Häufigste Netzwerkdienste* im Menü *Netzwerk* eine Akkumulation von Daten aller Knoten, die bei der verteilten Verarbeitung des Datenverkehrs involviert waren.

Hinweise

- Typen von Schnittstellen mit dynamischer IP-Adresszuweisung wie PPPoE und Kabelmodem (DHCP) werden im Cluster-Modus nicht unterstützt.
- Das *Address Resolution Protocol* (ARP) wird nur vom aktuellen Master benutzt, d. h. Slave- und Worker-Knoten senden und beantworten keine ARP-Anfragen.

- Im Falle eines Übernahmeereignisses, führt die Einheit, die die Aufgaben übernimmt, eine ARP-Bekanntgabe (auch bekannt als *gratuitous ARP*) durch. Das ist gewöhnlich eine ARP-Anfrage, die dazu dient, die ARP-Zwischenspeicher (Cache) der anderen Rechner zu aktualisieren, die diese Anfrage erhalten. Die ARP-Bekanntgabe wird dazu benutzt, bekannt zu geben, dass die IP-Adresse des Master auf den Slave übertragen wurde.
- Linkbündelung kann nicht dazu verwendet werden, den Durchsatz der Schnittstellen zu erhöhen, die für HA-/Cluster-Zwecke benutzt werden.
- Wenn die E-Mail-Verschlüsselung aktiv ist, wird SMTP-Verkehr nicht auf Cluster-Knoten verteilt.
- Alle Schnittstellen, die auf dem Master konfiguriert sind, müssen eine physikalische Verbindung haben, das heißt, der Port muss korrekt mit einem Netzwerkgerät verbunden sein.

Hardware- und Software-Anforderungen

Die folgenden Hardware- und Software-Anforderungen müssen die für HA- und Cluster-Funktionalität erfüllt sein:

- Gültige Lizenz mit aktivierter HA-Option (für das Standby-Gerät benötigen Sie lediglich eine zusätzliche Basislizenz).
- Zwei ASG-Geräte mit identischer Software-Version und identischer Hardware oder zwei ASG Appliances des gleichen Modells.
- Heartbeat-fähige Ethernet-Netzwerkkarten. Die *Hardware Compatibility List* (HCL) enthält alle Netzwerkkarten, die im Zusammenhang mit Astaro Security Gateway auf ihre Funktionalität hin getestet wurden. Sie finden die HCL in der Astaro Knowledgebase¹⁵ (verwenden Sie „HCL“ als Suchbegriff).
- Ethernet-Crosskabel (für die Verbindung zwischen Master und Slave in einem Hot-Standby-System). ASG Appliances der Modelle 320, 425 und 525, deren dedizierte HA-Schnittstelle eine Gigabit-auto-MDX-Schnittstelle ist, können auch durch ein Standard-Ethernetkabel der IEEE-Norm 802.3 miteinander verbunden werden.
- Netzwerk-Switch (um Cluster-Knoten miteinander zu verbinden).

Status

¹⁵ <http://www.astaro.com/kb/>

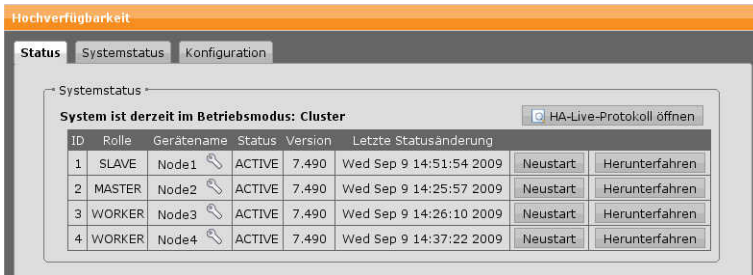


Figure 4.22 Hochverfügbarkeit: Statusseite

Die Registerkarte *Verwaltung >> Hochverfügbarkeit >> Status* führt alle Geräte auf, die zu einem Hot-Standby-System bzw. Cluster gehören und zeigt die folgenden Informationen an:

- **ID:** Die ID des Knotens. In einem Hot-Standby-System ist die ID entweder 1 (Master) oder 2 (Slave).
Die ID in einem Cluster reicht von 1 – 10, da ein Cluster aus maximal zehn Knoten bestehen kann.
- **Rolle:** Jeder Knoten in einem Cluster kann eine der folgenden Rollen annehmen:
 - **MASTER:** Das Primärsystem in einem Hot-Standby-/Cluster-Aufbau. Innerhalb eines Clusters sorgt der Master für die Synchronisation und Verteilung der Daten.
 - **SLAVE:** Das Sekundärsystem in einem Hot-Standby-/Cluster-Aufbau, das den Betrieb sicherstellt, falls das Primärsystem ausfällt.
 - **WORKER:** Ein einfacher Cluster-Knoten zur Datenverarbeitung.
- **Gerätename:** Der Name des Gerätes.
- **Status:** HA-Status des Knotens. Die folgenden Werte sind möglich:
 - **AKTIV:** Der Knoten ist einsatzbereit.
 - **NICHT VERBUNDEN:** Ein oder mehrere Schnittstellen sind nicht verbunden.
 - **UP2DATE:** Auf dem Knoten wird gerade ein Up2Date ausgeführt.
 - **UP2DATE FEHLGESCHLAGEN:** Auf dem Knoten wird gerade ein Up2Date ausgeführt.

- TOT: Der Knoten ist nicht erreichbar.
- SYNCING: Die Datensynchronisierung läuft. Dieser Status wird angezeigt, wenn ein Übernahmevorgang stattfindet. Die anfängliche Synchronisierungszeit beträgt mindestens fünf Minuten. Sie kann jedoch durch alle an der Synchronisierung beteiligten Programme verlängert werden. Während ein SLAVE synchronisiert und sich im Zustand SYNCING befindet, findet keine geplante Übernahme statt, z. B. wegen einem Linkausfall auf dem Master-Knoten.
- **Version:** Versionsnummer der auf dem Knoten installierten Astaro Security Gateway Software.
- **Letzte Statusänderung:** Zeitpunkt der letzten Statusänderung.

Reboot/Shutdown: (Neustarten/Herunterfahren) Mit diesen Schaltflächen kann ein Gerät manuell neu gestartet oder heruntergefahren werden.

Remove Node: (Knoten entfernen) Verwenden Sie diese Schaltfläche, um einen toten Cluster-Knoten über WebAdmin zu entfernen. Alle knotenspezifischen Daten wie Mailquarantäne und Spool werden dann vom Master übernommen.

Klicken Sie auf die Schaltfläche *Open HA Live-Log* in der rechten oberen Ecke, um das *Hochverfügbarkeits-Live-Protokoll* in einem separaten Fenster zu öffnen.

Systemstatus

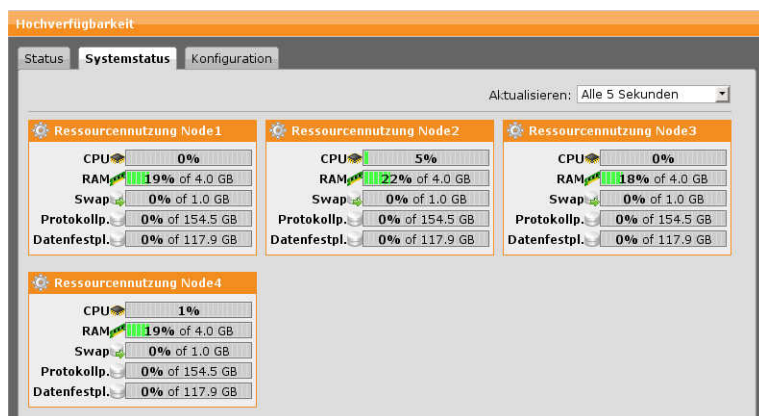


Figure 4.23 Hochverfügbarkeit: Ressourcennutzung der einzelnen HA- oder Cluster-Geräte

Die Registerkarte *Verwaltung* >> *Hochverfügbarkeit* >> *Systemstatus* führt alle Geräte auf, die zu einem Hot-Standby-System bzw. Cluster gehören und zeigt Informationen über die Ressourcennutzung jedes einzelnen Gerätes an:

- Die CPU-Nutzung in Prozent
- Die RAM-Nutzung in Prozent
- Die Swap-Nutzung in Prozent
- Die Menge des benutzten Festplattenspeicherplatzes der Protokollpartition (engl. *log partition*) in Prozent
- Die Menge des benutzten Festplattenspeicherplatzes der Systempartition (engl. *root partition*) in Prozent

Konfiguration

Die HA-Funktionalität von Astaro Security Gateway umfasst drei Grundeinstellungen:

- Automatische Konfiguration
- Hot-Standby (active-passive)
- Cluster (active-active)

Automatische Konfiguration: Astaro Security Gateway verfügt über eine *Plug-and-Play*-Option speziell für ASG Appliances, die es ermöglicht, ein Hot-Standby-System bzw. einen Cluster aufzubauen, ohne jedes Gerät einzeln konfigurieren zu müssen. Dazu verbindet man einfach die HA-Schnittstellen (in der Regel `eth3`) der ASG Appliances miteinander (im Falle eines Clusters mithilfe eines Switches) und wählt auf allen Geräten jeweils die Option *Automatische Konfiguration*.

Hinweis – Beachten Sie, dass die *Automatische Konfiguration* nur mit ASG Hardware Appliances des gleichen Modells funktioniert. Sie können z. B. nur zwei ASG 320 Hardware Appliances zum Aufbau eines HA-Systems verwenden; eine ASG 220 kann hingegen nicht mit einer ASG 320 kombiniert werden.

Wenn Sie zwei ASG Appliances über die entsprechende Schnittstelle miteinander verbinden, so erkennen sich beide Geräte gegenseitig und konfigurieren

sich selbstständig als HA-System. Das Gerät mit der längeren Betriebszeit wird Master. Im unwahrscheinlichen Fall, dass die Betriebszeit identisch ist, wird die Entscheidung, welches Gerät Master werden soll, anhand der MAC-Adresse getroffen.

Auf Geräten mit installierter ASG Software dient die Option *Automatische Konfiguration* auf dedizierten Slave-Systemen dazu, automatisch einem HA-System oder Cluster beizutreten. Aus diesem Grund ist die *Automatische Konfiguration* eher als Übergangsmodus zu verstehen denn als eigenständiger HA-Betriebsmodus. Denn der HA-Betriebsmodus ändert sich in *Hot-Standby* oder *Cluster*, sobald das Gerät mit der Einstellung *Automatische Konfiguration* einem Hot-Standby System bzw. Cluster beitrifft. Voraussetzung dafür allerdings ist, dass die Option *Autojoin* auf dem Master aktiviert ist. Die Autojoin-Funktion (dt. *automatisch beitreten*) sorgt dafür, dass genau diese Geräte automatisch einem Hot-Standby-System bzw. Cluster hinzugefügt werden, deren HA-Betriebsmodus auf *Automatische Konfiguration* steht.

Hot-Standby (active-passive): Astaro Security Gateway kann als Hot-Standby-System, bestehend aus zwei Knoten, konfiguriert werden, was die Mindestvoraussetzung für ein redundantes System ist. Eine der größten technischen Verbesserungen von Astaro Security Gateway Software V7 ist, dass die Latenzzeit für eine Übernahme durch das Standby-Gerät auf weniger als zwei Sekunden verringert werden konnte. Zusätzlich zur Paketfilter-Synchronisation werden im Falle einer HA-Übernahme auch bestehende IPSec-Verbindungen synchronisiert. Dies bedeutet, dass IPSec-Verbindungen nach einer Übernahme nicht neu aufgebaut werden müssen. Ebenfalls synchronisiert werden Objekte in der Quarantäne, die auch nach einem Ausfall des Primärsystems noch verfügbar sind.

Cluster (active-active): Um der gestiegenen Nachfrage nach der Verarbeitung von großen Mengen an Internetverkehr in Echtzeit gerecht zu werden, kann Astaro Security Gateway als Cluster konfiguriert werden. Ein Cluster besteht aus mehreren Knoten, auf die rechenintensive Aufgaben wie z. B. Inhaltsfilterung, Virencans, Einbruchschutz und Entschlüsselung gleichmäßig verteilt werden können. Ohne die Notwendigkeit eines speziellen Lastenausgleichsprogramms wird so die Gesamtleistung der Firewall deutlich erhöht.

Hinweis – Wenn Sie einen Cluster konfigurieren, stellen Sie sicher, dass Sie den Master zuerst konfigurieren, bevor Sie die anderen Geräten mit dem Switch verbinden.

Figure 4.24 Hochverfügbarkeit: Konfiguration eines Clusters

Um einen Master in einem Hot-Standby bzw. Cluster zu konfigurieren, gehen Sie folgendermaßen vor:

1. Wählen Sie einen HA-Betriebsmodus.

Standardmäßig ist die HA-Funktion deaktiviert.

Sie können zwischen den folgenden Betriebsarten auswählen:

- Automatische Konfiguration
- Hot-Standby (active-passive)
- Cluster (active-active)

Wählen Sie entweder *Hot-Standby* oder *Cluster* aus.

Hinweis – Falls Sie die Betriebsart später ändern möchten, müssen Sie vorher den Modus auf *Aus* stellen. Erst danach können Sie eine der Betriebsarten *Automatische Konfiguration*, *Hot-Standby* oder *Cluster* wählen.

- 2. Sync-NIC:** Wählen Sie die Netzwerkkarte aus, über die Master- und Slave-Systeme miteinander kommunizieren. Wenn Linkbündelung aktiviert ist, können Sie hier auch eine Linkbündelungsschnittstelle sehen.

Hinweis – Beachten Sie, dass nur jene Netzwerkkarten angezeigt werden, die noch nicht konfiguriert wurden.

Die folgenden Optionen können erst konfiguriert werden, nachdem entweder *Hot-Standby* oder *Cluster* als Betriebsart ausgewählt wurden.

Gerätename: Geben Sie dem Gerät einen aussagekräftigen Namen.

Geräteknoten-ID: Weisen Sie dem Gerät eine Knoten-ID zu. Im Falle eines Versagens des Primärsystems wird der Knoten mit der höchsten ID Master.

Verschlüsselungsschlüssel: Das Kennwort mit dem die Kommunikation zwischen Master und Slave verschlüsselt wird (zur Sicherheit müssen Sie das Kennwort zweimal eingeben). Der Schlüssel darf maximal 16 Zeichen lang sein.

3. Klicken Sie **Übernehmen**.

Die Konfiguration der HA-Ausfallsicherheit auf dem Master ist damit abgeschlossen.

Hinweis – Für einen Zeitraum von 15 Minuten ist die Übernahmefunktion (takeover) gesperrt, um sicherzustellen, dass die Synchronisierung der Konfiguration abgeschlossen ist. Zu Testzwecken können Sie diese Sperre umgehen, indem Sie den Master ausschalten, bevor Sie den Slave anschalten oder verbinden.

4. Optional können Sie folgende Einstellungen vornehmen:

Autojoin: Diese Option sorgt dafür, dass diejenigen Geräte automatisch zu einem Hot-Standby-System bzw. Cluster hinzugefügt werden, deren HA-Betriebsmodus auf *Automatische Konfiguration* eingestellt ist.

Backup-Schnittstelle: Ein Versagen der HA-Synchronisierungsschnittstelle oder ein ausgestecktes Netzkabel, beispielsweise, können dazu führen, dass sowohl Master als auch Slave gleichzeitig Master werden (Master-Master-Situationen). Um das zu verhindern, kann eine heartbeat-fähige Backup-Schnittstelle ausgewählt werden, welche irgendeine von den konfigurierten und aktiven Ethernet-Schnittstellen sein kann. Wenn eine Backup-Schnittstelle ausgewählt ist, wird ein zusätzliches Heartbeat-Signal über diese Schnittstelle in einer Richtung vom Master zum Slave gesendet, um sicherzustellen, dass die Master-Slave-Konfiguration intakt bleibt. Wenn die Master-Slave-Verbindung deaktiviert wird und das Backup-Schnittstelle in

Anspruch genommen wird, erhält der Administrator eine Benachrichtigung darüber, dass einer der Cluster-Knoten tot ist.

Hinweis – In dem Fall, dass die HA-Synchronisierungsschnittstelle ausfällt, wird keine Konfiguration mehr synchronisiert. Die Backup-Schnittstelle verhindert lediglich Master-Master-Situationen.

5. **Klicken Sie Übernehmen.**

Ihre Einstellungen werden gespeichert.

Fahren Sie nun mit der Konfiguration des Slave-Systems fort:

1. **Wählen Sie einen HA-Betriebsmodus.**

Standardmäßig ist die HA-Funktion deaktiviert.

Sie können zwischen den folgenden Betriebsarten auswählen:

- Automatische Konfiguration
- Hot-Standby (active-passive)
- Cluster (active-active)

Wenn Sie *Automatische Konfiguration* auswählen, brauchen Sie nur die Schnittstelle zur Kommunikation zwischen Master und Slave auszuwählen.

- ### 2. **Sync-NIC:** Wählen Sie die Netzwerkkarte aus, über die Master- und Slave-Systeme miteinander kommunizieren. Wenn Linkbündelung aktiviert ist, können Sie hier auch eine Linkbündelungsschnittstelle sehen. Die folgenden Optionen können erst konfiguriert werden, nachdem entweder *Hot-Standby* oder *Cluster* als Betriebsart ausgewählt wurden.

Geräteiname: Geben Sie dem Gerät einen aussagekräftigen Namen.

Geräteknotten-ID: Weisen Sie dem Gerät eine Knoten-ID zu. Im Falle eines Versagens des Primärsystems wird der Knoten mit der höchsten ID Master.

Verschlüsselungsschlüssel: Das Kennwort mit dem die Kommunikation zwischen Master und Slave verschlüsselt wird (geben Sie das Kennwort ein, das auf dem Master konfiguriert wurde). Der Schlüssel darf maximal 16 Zeichen lang sein.

3. **Klicken Sie Übernehmen.**

Die Konfiguration der HA-Ausfallsicherheit auf dem Master ist damit abgeschlossen.

Hinweis – Für einen Zeitraum von 15 Minuten ist die Übernahmefunktion (takeover) gesperrt, um sicherzustellen, dass die Synchronisierung der Konfiguration abgeschlossen ist. Zu Testzwecken können Sie diese Sperre umgehen, indem Sie den Master ausschalten, bevor Sie den Slave anschalten oder verbinden.

4. **Optional können Sie folgende Einstellungen vornehmen:**

Autojoin: Diese Option sorgt dafür, dass diejenigen Geräte automatisch zu einem Hot-Standby-System bzw. Cluster hinzugefügt werden, deren HA-Betriebsmodus auf *Automatische Konfiguration* eingestellt ist. Da diese Option jedoch keinen Effekt auf Slave-Systemen hat, können Sie die Option aktiviert lassen, was der Standardeinstellung entspricht.

Backup-Schnittstelle: Ein Versagen der HA-Synchronisierungsschnittstelle oder ein ausgestecktes Netzkabel, beispielsweise, können dazu führen, dass sowohl Master als auch Slave gleichzeitig Master werden (Master-Master-Situationen). Um das zu verhindern, kann eine heartbeat-fähige Backup-Schnittstelle ausgewählt werden, welche irgendeine von den konfigurierten und aktiven Ethernet-Schnittstellen sein kann. Wenn eine Backup-Schnittstelle ausgewählt ist, wird ein zusätzliches Heartbeat-Signal über diese Schnittstelle in einer Richtung vom Master zum Slave gesendet, um sicherzustellen, dass die Master-Slave-Konfiguration intakt bleibt. Da diese Option keinen Effekt auf Slave-Systemen hat, können Sie sie unkonfiguriert lassen.

Hinweis – In dem Fall, dass die HA-Synchronisierungsschnittstelle ausfällt, wird keine Konfiguration mehr synchronisiert. Die Backup-Schnittstelle verhindert lediglich Master-Master-Situationen.

5. **Klicken Sie Übernehmen.**

Ihre Einstellungen werden gespeichert.

Das Hot-Standby-System wird in regelmäßigen Abständen über das Sync-NIC (Synchronisierungsschnittstelle) aktualisiert. Sollte das Primärsystem ausfallen, übernimmt das Sekundärsystem unmittelbar und automatisch die Aufgaben des Master.

Hinweis – Wenn Sie ein Hot-Standby-System bzw. Cluster deaktivieren, führen der Slave und alle Worker-Knoten eine Werksrücksetzung (engl. *Factory Reset*) durch und fahren herunter.

Nähere Information zu diesem Thema (insbesondere Anwendungsfälle) erfahren Sie in der Astaro Knowledgebase¹⁶ (Wissensdatenbank) im HA/Cluster Guide.

Konfiguration

Es ist möglich, die Synchronisierungsschnittstelle in einer laufenden Konfiguration zu ändern. Beachten Sie, dass danach alle Knoten einen Neustart durchführen werden.

Erweitert

In diesem Abschnitt können Sie einige erweiterte Einstellungen vornehmen.

Automatische Konfiguration neuer Geräte aktivieren: Diese Option ist standardmäßig aktiviert und sorgt dafür, dass neu angeschlossene Geräte automatisch konfiguriert werden.

Preferred Master: (Erwünschter Master) Hier können Sie bestimmen, welcher Master-Knoten der erwünschte sein soll, indem Sie einen Knoten von der Auswahlliste wählen. Im Falle eines Failover wird der gewählte Knoten nicht im Slave-Modus bleiben, nachdem die Verbindung wiederhergestellt ist, sondern in den Master-Modus zurückkehren.

Backup-Schnittstelle: Ein Versagen der HA-Synchronisierungsschnittstelle oder ein ausgestecktes Netzkabel, beispielsweise, können dazu führen, dass sowohl Master als auch Slave gleichzeitig Master werden (Master-Master-Situationen). Um das zu verhindern, kann eine heartbeat-fähige Backup-Schnittstelle ausgewählt werden, welche irgendeine von den konfigurierten und aktiven Ethernet-Schnittstellen sein kann. Wenn eine Backup-Schnittstelle ausgewählt ist, wird ein zusätzliches Heartbeat-Signal über diese Schnittstelle in einer Richtung vom Master zum Slave gesendet, um sicherzustellen, dass die Master-Slave-Konfiguration intakt bleibt. Wenn die Master-Slave-Verbindung deaktiviert ist und die Backup-Schnittstelle in Aktion tritt, erhält der Administrator eine Benachrichtigung, die ihn darüber informiert, dass einer der Cluster-Knoten tot ist. Diese Option hat jedoch keinen Effekt auf Slave-Systemen, deshalb können Sie sie unkonfiguriert lassen.

¹⁶ <http://www.astaro.com/kb/>

Ausschalten/Neustart

Mit den Funktionen auf der Seite *Verwaltung* >> *Ausschalten/Neustart* können Sie Astaro Security Gateway herunterfahren bzw. neu starten.

Herunterfahren: Mit dieser Aktion können Sie das System herunterfahren und alle Dienste ordnungsgemäß stoppen. Falls Sie keinen Monitor oder LCD-Display angeschlossen haben, wird das erfolgreiche Herunterfahren durch eine endlose Reihe von Pieptönen im Abstand von einer Sekunde signalisiert.

Um Astaro Security Gateway herunterzufahren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf die Schaltfläche *System jetzt herunterfahren*.**

2. **Bestätigen Sie den Warnhinweis.**

Bestätigen Sie die Sicherheitsabfrage „System wirklich herunterfahren?“ mit *OK*.

Das System fährt anschließend herunter.

Abhängig von der verwendeten Hardware und Konfiguration kann dieser Prozess mehrere Minuten dauern. Sie sollten das Gerät erst dann abschalten, nachdem es vollständig heruntergefahren ist. Wenn Sie das Gerät vorher ausschalten, wird das System beim nächsten Start den Zustand des Dateisystems überprüfen, was den Startvorgang erheblich verzögert. Im schlimmsten Fall können Daten verloren gehen.

Einen erfolgreichen Systemstart signalisiert das Gerät mit fünf aufeinanderfolgenden Pieptönen.

Neustart: Mit dieser Aktion können Sie das System neu starten. Abhängig von der verwendeten Hardware und Konfiguration kann dieser Prozess mehrere Minuten dauern.

Um Astaro Security Gateway neu zu starten, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf die Schaltfläche *System jetzt neu starten*.**

2. **Bestätigen Sie den Warnhinweis.**

Bestätigen Sie die Sicherheitsabfrage „System wirklich neu starten?“ mit *OK*.

Das System fährt herunter und startet anschließend neu.

Kapitel 5

Benutzer

Dieses Kapitel beschreibt die Konfiguration von Benutzerkonten, Benutzergruppen, und die von Astaro Security Gateway unterstützten externen Authentifizierungsdienste.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- Benutzer
- Gruppen
- Authentifizierung

Benutzer

Auf der Registerkarte *Benutzer >> Benutzer* können Sie Benutzerkonten zu der Firewall hinzufügen. In der Werkseinstellung besitzt Astaro Security Gateway einen vorkonfigurierten Administrator namens *admin*.

Tipp – Durch einen Klick auf eine Benutzerdefinition in der Liste *Benutzer* werden Ihnen alle Konfigurationsoptionen angezeigt, in denen diese Benutzerdefinition benutzt wird.

Wenn Sie eine E-Mail-Adresse im Dialogfenster *Neuer Benutzer* angeben, wird parallel zum Anlegen der Benutzerdefinition ein X.509-Zertifikat generiert. Dabei wird die E-Mail-Adresse als VPN-ID für das Zertifikat benutzt. Andernfalls, wenn keine E-Mail-Adresse angegeben ist, wird ein Zertifikat generiert, dass den *Distinguished Name* (DN) des Benutzers als VPN-ID verwendet. Wenn sich ein Benutzer über eine Backend-Gruppe wie z. B. eDirectory authentifiziert, wird dadurch ein Zertifikat angelegt, selbst wenn keine E-Mail-Adresse in der entsprechenden Backend-Benutzerdefinition angegeben ist.

Da die VPN-ID jedes Zertifikats einzigartig sein muss, muss jede Benutzerdefinition eine unterschiedliche und einzigartige E-Mail-Adresse besitzen. Das Anlegen einer Benutzerdefinition mit einer bereits vorhandenen E-Mail-Adresse ist nicht möglich. Die Zertifikate können für verschiedene Fernzugriff-Methoden verwendet werden, die von Astaro Security Gateway unterstützt werden – mit

Ausnahme von PPTP, L2TP over IPSec mit vorvereinbarten Schlüsseln (engl. *preshared keys*) und nativem IPSec mit RSA oder PSK.

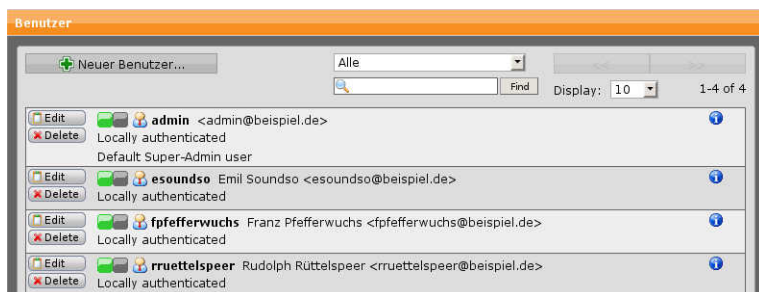


Figure 5.1 Benutzer: Benutzerkonten

Um ein Benutzerkonto hinzuzufügen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Benutzer* auf *Neuer Benutzer*.**
Das Dialogfenster *Neuen Benutzer erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Benutzername: Tragen Sie einen aussagekräftigen Namen für den Benutzer ein (z. B. Esoundso).

Echter Name: Tragen Sie den echten Namen des Benutzers ein (z. B. Emil Soundso).

E-Mail-Adresse: Tragen Sie die primäre E-Mail-Adresse des Benutzers ein.

Zusätzliche E-Mail-Adressen (optional): Hier können Sie zusätzliche E-Mail-Adressen des Benutzers eintragen. Alle als Spam eingestuft E-Mails an diese Adressen werden in einem individuellen Spambericht gesondert aufgeführt. Dieser Spambericht wird an die primäre E-Mail-Adresse geschickt.

Authentifizierung: Wählen Sie die Authentifizierungsmethode. Die folgenden Methoden sind verfügbar:

- **Lokal:** Der Benutzer authentifiziert sich lokal auf der Firewall.
- **Entfernt:** Der Benutzer authentifiziert sich über eine externe Authentifizierungsmethode, die von Astaro Security Gateway unterstützt wird. Weitere Informationen dazu finden Sie unter *Benutzer >> Authentifizierung*.
- **Keine:** Wählen Sie diese Methode, um zu verhindern, dass der Benutzer sich authentifizieren kann. Diese Option ist hilfreich, wenn ein Benutzerkonto vorübergehend deaktiviert, aber nicht ganz gelöscht werden soll.

Kennwort: Tragen Sie das Kennwort für den Benutzer ein (ein zweites Mal zur Bestätigung). Diese Option ist nur verfügbar, wenn Sie die Authentifizierungsmethode *Lokal* gewählt haben.

Backend-Sync.: Einige Grundeinstellungen, wie der echte Name und die E-Mail-Adresse des Benutzers werden automatisch durch Synchronisation mit dem externen Backend-Authentifizierungsserver aktualisiert (diese Option ist nur verfügbar, wenn Sie als Authentifizierungsmethode *Entfernt* gewählt haben).

Hinweis – Augenblicklich können Daten nur mit Active-Directory- und eDirectory-Servern synchronisiert werden.

X.509-Zertifikat: Sobald die Benutzerdefinition angelegt wurde, können Sie diesem Benutzer ein X.509-Zertifikat zuweisen, wenn Sie die Benutzerdefinition bearbeiten. Standardmäßig handelt es sich dabei um jenes Zertifikat, das beim Anlegen der Benutzerdefinition erzeugt wurde. Dennoch können Sie auch ein Zertifikat eines Drittanbieters zuweisen, welches Sie auf der Registerkarte *Fernzugriff >> Zertifikatverwaltung >> Zertifikate* hochladen können.

Statische Fernzugriffs-IP verwenden (optional): Wählen Sie diese Option aus, wenn Sie einem Benutzer, der Fernzugriff verwendet, eine statische IP-Adresse zuweisen möchten anstelle einer dynamischen IP-Adresse aus einem IP-Adressen-Pool. Für IPSec-Benutzer hinter einem NAT-Router ist es beispielsweise zwingend erforderlich, eine statische IP-Adresse zu verwenden.

Hinweis – Die statische IP-Adresszuweisung (engl. *static remote access IP*) kann nur für den Fernzugriff via PPTP, L2TP und IPSec genutzt werden, jedoch nicht für Fernzugriff via SSL.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über das Benutzerkonto hinzu.

3. Klicken Sie *Speichern*.

Das neue Benutzerkonto wird anschließend in der Liste *Benutzer* angezeigt.

Wenn Sie diesem Benutzer reguläre Administrationsrechte geben wollen, mit Zugriff auf die web-basierte Administrationsschnittstelle WebAdmin, fügen Sie den Benutzer zur Gruppe *SuperAdmins* hinzu. Die Benutzergruppen werden auf der Registerkarte *Benutzer >> Gruppen* verwaltet.

Hinweis – Wenn Sie ein Benutzerkonto gelöscht haben und ein Benutzerkonto mit demselben Namen anlegen wollen, stellen Sie sicher, dass Sie auch das zugehörige Zertifikat auf der Registerkarte *Fernzugriff* >> *Zertifikatverwaltung* >> *Zertifikate* entfernt haben. Andernfalls erhalten Sie eine Fehlermeldung, dass ein Benutzerkonto mit diesem Namen bereits existiert.

Gruppen

Auf der Seite *Benutzer* >> *Gruppen* können Sie Benutzergruppen zu der Firewall hinzufügen. In der Werkseinstellung besitzt Astaro Security Gateway bereits eine vordefinierte Gruppe namens *SuperAdmins*. Wenn Sie einem Benutzer administrative Rechte geben wollen, d. h. Zugriffsrechte auf WebAdmin, fügen Sie ihn der Gruppe *SuperAdmins* hinzu; diese Gruppe sollte nicht gelöscht werden.

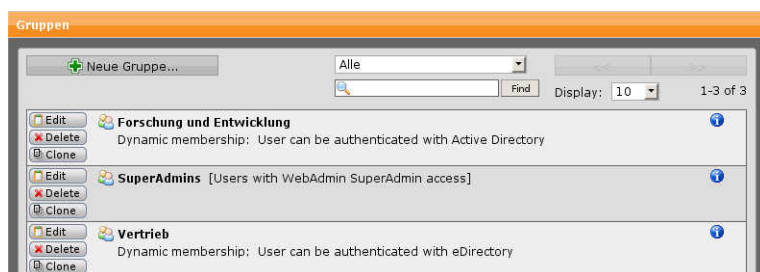


Figure 5.2 Gruppen: Gruppenliste

Tipp – Durch einen Klick auf eine Gruppenseite in der Liste *Gruppen* werden Ihnen alle Konfigurationsoptionen angezeigt, in denen die Gruppenseite verwendet wird.

Um eine Benutzergruppe hinzuzufügen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Gruppen* auf *Neue Gruppe*.**
Das Dialogfenster *Neue Gruppe erstellen* wird geöffnet.
2. **Nehmen Sie die folgenden Einstellungen vor:**
Gruppenname: Tragen Sie einen aussagekräftigen Gruppennamen ein. Der Gruppenname muss nicht mit dem Gruppennamen Ihrer Backend-Gruppen

übereinstimmen.

Gruppentyp: Wählen Sie den Gruppen-Typ aus. Sie können zwischen einer Gruppe mit statischen Mitgliedern und zwei Gruppen mit dynamischer Mitgliedschaft wählen.

- **Statische Mitglieder:** Wählen Sie die lokalen Benutzer aus, die Mitglied in dieser Gruppe werden sollen.
- **IPSec-X.509-DN-Maske:** Benutzer werden dynamisch zu einer IPSec-X.509-DN-Gruppengröße hinzugefügt, sobald sie sich erfolgreich über eine IPSec-Verbindung an der Firewall angemeldet haben und spezifische Parameter ihres Distinguished Name mit dem Wert im Feld *DN-Maske* übereinstimmen.
- **Backend-Mitgliedschaft:** Benutzer werden dynamisch zur einer Gruppengröße hinzugefügt, wenn sie sich erfolgreich an einem der unterstützten Authentifizierungsdienste angemeldet haben. Um fortzufahren, wählen Sie den entsprechenden Authentifizierungsdienst aus:
 - **Active Directory:** Eine Active-Directory-Benutzergruppe der Firewall stellt die Gruppenmitgliedschaft bereit für Mitglieder einer Active-Directory-Server-Benutzergruppe, die in einem Windows-Netzwerk konfiguriert ist. Geben Sie den Namen der Active-Directory-Server-Benutzergruppe ein, der dieser Benutzer angehört. Weitere Informationen finden Sie im Menü *Benutzer >> Authentifizierung >> Server*.
 - **eDirectory:** Eine eDirectory-Benutzergruppe der Firewall stellt die Gruppenmitgliedschaft bereit für Mitglieder einer eDirectory-Server-Benutzergruppe, die in einem eDirectory-Netzwerk konfiguriert ist. Geben Sie den Namen der eDirectory-Gruppe ein, der dieser Benutzer angehört. Weitere Informationen finden Sie im Menü *Benutzer >> Authentifizierung >> Server*.
 - **RADIUS:** Die Benutzer werden automatisch einer RADIUS-Backend-Gruppe hinzugefügt, wenn sie erfolgreich durch die Methode RADIUS authentifiziert wurden.
 - **TACACS+:** Die Benutzer werden automatisch einer TACACS+-Backend-Gruppe hinzugefügt, wenn sie erfolgreich durch die Methode TACACS+ authentifiziert wurden.
 - **LDAP:** Die Benutzer werden automatisch einer LDAP-Backend-Gruppe hinzugefügt, wenn sie erfolgreich durch die Methode LDAP authentifiziert wurden.

Auf Backend-Gruppenmitglieder beschränken (optional): In Netzwerken mit einem X.500-Verzeichnisdienst kann die Mitgliedschaft auf bestimmte Gruppen in der Datenbank begrenzt werden, wenn Sie nicht alle Benutzer des gewählten Backend-Servers in diese Gruppensdefinition einschließen wollen. Wenn Sie diese Option wählen müssen die hier angegebene(n) Gruppe(n) einen Vergleich mit dem *Common Name* bestehen, der auf Ihrem Backend-Server konfiguriert ist. Beachten Sie, dass Sie das CN=-Präfix weglassen können, wenn Sie diese Option für Active Directory einschalten. Wenn Sie diese Option für ein eDirectory-Backend einschalten, können Sie entweder den eDirectory-Browser verwenden, um bequem die eDirectory-Gruppen auszuwählen, die in diese Gruppensdefinition aufgenommen werden sollen. Falls Sie den eDirectory-Browser nicht verwenden, stellen Sie jedoch sicher, dass das CN=-Präfix vorhanden ist, wenn Sie die Gruppencontainer eingeben.

Ein LDAP-Attribut überprüfen (optional): In Netzwerken mit einem LDAP-Verzeichnisdienst kann die Mitgliedschaft auf bestimmte Gruppen in der Datenbank begrenzt werden, die ein bestimmtes LDAP-Attribut Ihres Backend-Servers aufweisen, wenn Sie nicht alle Benutzer eines gewählten LDAP-Backend-Servers in diese Gruppensdefinition einschließen wollen. Dieses Attribut wird dann als LDAP-Filterkriterium verwendet. Beispiel: Sie könnten `groupMembership` als Attribut mit dem Wert `CN=Sales, O=Example` angeben. Dadurch würden alle Benutzer aus der Sales-Abteilung Ihrer Firma zur Gruppensdefinition hinzugefügt werden.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die Benutzergruppe hinzu.

3. Klicken Sie *Speichern*.

Die neue Benutzergruppe wird anschließend in der Liste *Gruppen* angezeigt.

Um eine Benutzergruppe zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

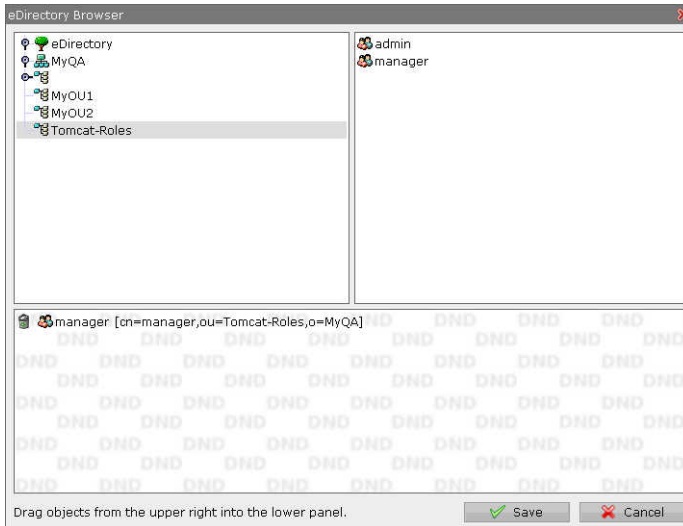


Figure 5.3 Gruppen: eDirectory Browser of Astaro Security Gateway

Authentifizierung

Im Menü *Benutzer >> Authentifizierung* werden die Datenbanken und Verzeichnisdienste für die externe Authentifizierung von Benutzern verwaltet. Externe Benutzerauthentifizierung ermöglicht es Ihnen, Benutzerkonten gegen vorhandene Benutzerdatenbanken oder Verzeichnisdienste zu validieren, die sich auf anderen Servern in Ihrem Netzwerk befinden. Momentan werden folgende Authentifizierungsdienste unterstützt:

- Novell eDirectory
- Microsoft Active Directory
- RADIUS
- TACACS+
- LDAP

Allgemein

Auf der Registerkarte *Benutzer >> Authentifizierung >> Allgemein* werden die Grundeinstellungen für die externe Authentifizierung durchgeführt. Folgende Funktionen sind verfügbar:

Benutzer automatisch erstellen: Wenn diese Option gewählt ist, legt Astaro Security Gateway automatisch ein Benutzerkonto an, sobald sich ein unbekannter Benutzer, der in einer Backend-Gruppe konfiguriert ist, erfolgreich über einen der angebundenen externen Authentifizierungsdienste anmeldet, der von Astaro Security Gateway unterstützt wird. Beispiel: Wenn Sie eine RADIUS-Backend-Gruppe konfigurieren und diese Gruppe im Feld *Zugelassene Auditoren* auf der Registerkarte *Verwaltung* > > *WebAdmin-Einstellungen* > > *Zugriffskontrolle* ausgewählt haben, wird Astaro Security Gateway automatisch eine Benutzerdefinition für denjenigen RADIUS-Benutzer erzeugen, der sich erfolgreich an WebAdmin angemeldet hat.

- **Automatische Benutzererstellung für Funktionen:** Für bestimmte Funktionen kann eine automatische Benutzererstellung aktiviert werden. Die Benutzer werden dabei nur für die ausgewählten Funktionen angelegt. Diese Funktionalität ist nicht verfügbar – und automatische Benutzererstellung ist für alle Funktionen deaktiviert – wenn die Option *Benutzer automatisch erstellen* nicht ausgewählt ist.

Hinweis – Diese Funktion ist nicht möglich mit Active Directory *Single Sign-On* (SSO).

Diese Benutzerdefinitionen werden auch benötigt, um Zugang zum Benutzerportal von Astaro Security Gateway zu gewähren. Darüber hinaus wird für alle Benutzerdefinitionen automatisch ein SSL-Zertifikat erzeugt. Beachten Sie jedoch, dass die automatische Benutzererstellung fehl schlägt, wenn es zu einem E-Mail-Adressenkonflikt kommt, da die zu erstellende Benutzerdefinition keine E-Mail-Adresse besitzen darf, die auf dem System bereits vorhanden ist. Alle E-Mail-Adressen müssen innerhalb des Systems einzigartig sein, da sie zur Identifizierung für die SSL-Zertifikate dienen.

Wichtiger Hinweis: Authentifizierung (das Herausfinden, wer ein Benutzer ist) und Autorisierung (das Herausfinden, was ein Benutzer darf) für einen Benutzer, dessen Benutzerdefinition automatisch erzeugt wurde, geschieht immer auf dem entfernten Backend-Server bzw. Verzeichnisdienst. Aus diesem Grund sind automatisch erzeugte Benutzerdefinitionen in Astaro Security Gateway nutzlos, wenn der entsprechende Backend-Server nicht erreichbar ist oder die Benutzerdefinition auf der entfernten Maschine gelöscht wurde.

Beachten Sie auch, dass Astaro Security Gateway (außer für Active Directory *Single Sign-On* (SSO)) Benutzerauthentifizierungsdaten, die es von einem entfernten Authentifizierungsserver geholt hat, für 300 Sekunden zwischenspeichert. Deshalb werden sich Änderungen an den entfernten Benutzereinstellungen erst auswirken, wenn der Speicherzeitraum abgelaufen ist.

Authentifizierungs-Zwischenspeicher

Jedes Mal, wenn Astaro Security Gateway eine Benutzeranfrage von einem noch unbekannten Benutzer erreicht, z. B. http, und Authentifizierung erforderlich ist, schreibt die *Astaro User Authentication* (AUA) einen Eintrag in den Authentifizierungs-Zwischenspeicher. Mit der Zeit kann es in Umgebungen mit häufig wechselnden Benutzern sinnvoll sein, den Zwischenspeicher von Zeit zu Zeit zu leeren. Eine Leerung kann auch angebracht sein, wenn Sie für alle Benutzer eine sofortige neue Authentifizierung erzwingen wollen. Verwenden Sie die Schaltfläche *Auth.-Zwischenspeicher leeren*, um den Authentifizierungs-Zwischenspeicher zu leeren.

Eine Authentifizierung ist 300 Sekunden lang gültig. In dieser Zeit werden neuerliche Authentifizierungsanfragen desselben Benutzers direkt im Zwischenspeicher nachgeschaut. Diese Methode entlastet die Backend-Authentifizierungsdienste wie eDirectory.

Hinweis – Ein Leeren des Speichers beeinträchtigt die Benutzer, die augenblicklich entfernt angemeldet sind, nicht.

Live-Protokoll: Durch einen Klick auf die Schaltfläche wird das Protokoll der *Astaro User Authentication* (AUA) in einem neuen Fenster angezeigt.

Server

Auf der Registerkarte *Benutzer >> Authentifizierung >> Server* können Sie einen oder mehrere Verzeichnisdienste anlegen, wie eDirectory, Active Directory, LDAP, RADIUS und TACACS+.

eDirectory

Novell eDirectory ist ein X.500-kompatibler Verzeichnisdienst zur zentralen Verwaltung von Zugriffsrechten auf Ressourcen auf mehreren Servern und Rechnern innerhalb eines bestimmten Netzwerks. Die hierarchische, objektorientierte Datenbank stellt alle Bestandteile einer Organisation in einer logischen

Baumstruktur dar. Diese Bestandteile können Menschen, Server, Workstations, Anwendungen, Drucker, Dienste, Gruppen usw. sein.

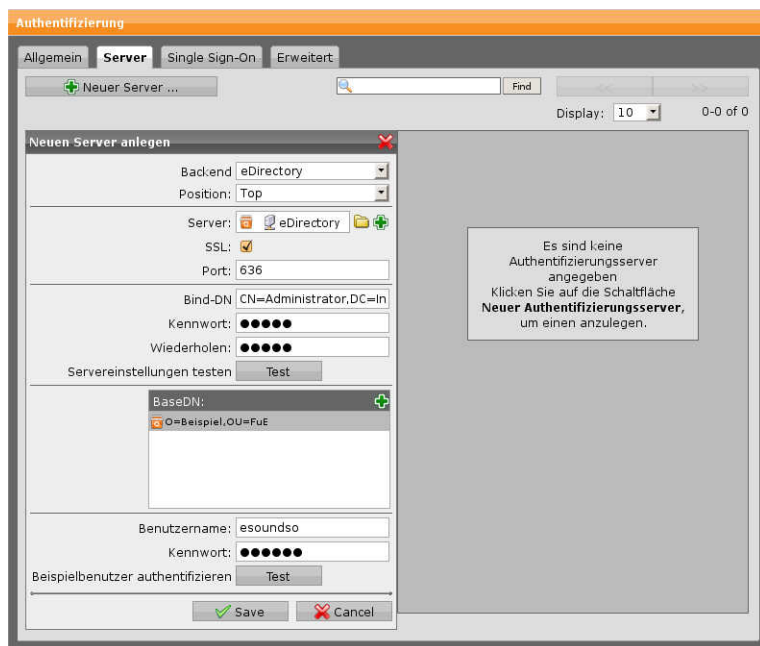


Figure 5.4 Authentifizierung: Benutzerauthentifizierung mit eDirectory

Um eine eDirectory-Authentifizierung zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte Server auf Neuer Server.**
Das Dialogfenster *Neuen Server anlegen* wird geöffnet.
2. **Nehmen Sie die folgenden Einstellungen vor:**
Backend: Wählen Sie *eDirectory* als Backend-Verzeichnisdienst.
Position: Wählen Sie eine Position für den Backend-Server. Backend-Server mit niedrigeren Nummern werden zuerst abgefragt. Stellen Sie für eine bessere Leistung sicher, dass der Backend-Server, der wahrscheinlich die meisten Anfragen erhält, ganz oben in der Liste steht.
Server: Wählen Sie einen eDirectory-Server (oder fügen Sie ihn hinzu).
SSL verwenden: Wählen Sie diese Option, um SSL-gesicherten Datentransfer zu aktivieren. Der Port ändert sich dann von 389 (LDAP) auf 636 (ldaps = LDAP over SSL).

Port: Wählen Sie den Port des eDirectory-Servers. Standardmäßig ist das Port 389.

Bind-DN: Der *Distinguished Name* (DN) des Benutzers, mit dem dieser am Server angemeldet werden soll. Dieser Benutzer wird benötigt, da anonyme Anfragen an den eDirectory-Server nicht erlaubt sind. Beachten Sie, dass der Benutzer genügend Privilegien besitzen muss, um alle relevanten Informationen zur Benutzerdefinition vom eDirectory-Server erhalten zu können, damit er Benutzer authentifizieren kann. eDirectory-Benutzer, -Gruppen und -Container können durch den vollen Distinguished Name in LDAP-Notation spezifiziert werden, wobei Kommas als Trennzeichen benutzt werden müssen (z. B. CN=administrator,DC=intranet,DC=beispiel,DC=de).

Kennwort: Geben Sie das Kennwort für den Bind-Benutzer ein (ein zweites Mal zur Bestätigung).

Servereinstellungen testen: Durch einen Klick auf diese Schaltfläche wird ein Bind-Test mit dem konfigurierten Server durchgeführt. Dadurch wird sichergestellt, dass die Einstellungen auf dieser Registerkarte richtig sind, und dass der Server eingeschaltet ist und Verbindungen entgegennimmt. Die Schaltfläche ist erst sichtbar, wenn die Servereinstellungen durch einen Klick auf *Übernehmen* gespeichert wurden.

BaseDN: Der Startpunkt, relativ gesehen zur Wurzel (engl. *root*) des LDAP-Baums, wo die Benutzer eingefügt sind, die authentifiziert werden sollen. Beachten Sie, dass der BaseDN über den vollen Distinguished Name (DN) in LDAP-Notation spezifiziert werden müssen, wobei Kommas als Trennzeichen verwendet werden müssen (z. B. O=Beispiel,OU=RnD). Der BaseDN kann leer sein. In diesem Fall wird der BaseDN automatisch aus dem Verzeichnis abgerufen.

Benutzername: Geben Sie den Benutzernamen eines Testbenutzers ein, um eine reguläre Authentifizierung durchzuführen.

Kennwort: Geben Sie das Kennwort des Testbenutzers ein.

Beispielbenutzer authentifizieren: Klicken Sie auf die Schaltfläche *Testen*, um den Authentifizierungstest für den Testbenutzer zu starten. Dies stellt sicher, dass alle Servereinstellungen korrekt sind, dass der Server eingeschaltet ist und Verbindungen akzeptiert, und dass Benutzer erfolgreich authentifiziert werden können.

3. Klicken Sie *Speichern*.

Der neue Server wird in der Liste *Server* angezeigt.

Active Directory

Microsoft Active Directory (AD) ist ein Verzeichnisdienst und eine zentrale Komponente der Windows 2000/2003 Server. Es speichert Informationen aus einem breiten Spektrum von Netzwerkressourcen, eingeschlossen Benutzer, Gruppen, Computer, Drucker, Anwendungen, Dienste und jede Art von benutzerdefinierten Objekten. Als solches ist es ein Mittel um diese Ressourcen zentral zu organisieren, zu verwalten und den Zugriff darauf zu kontrollieren.

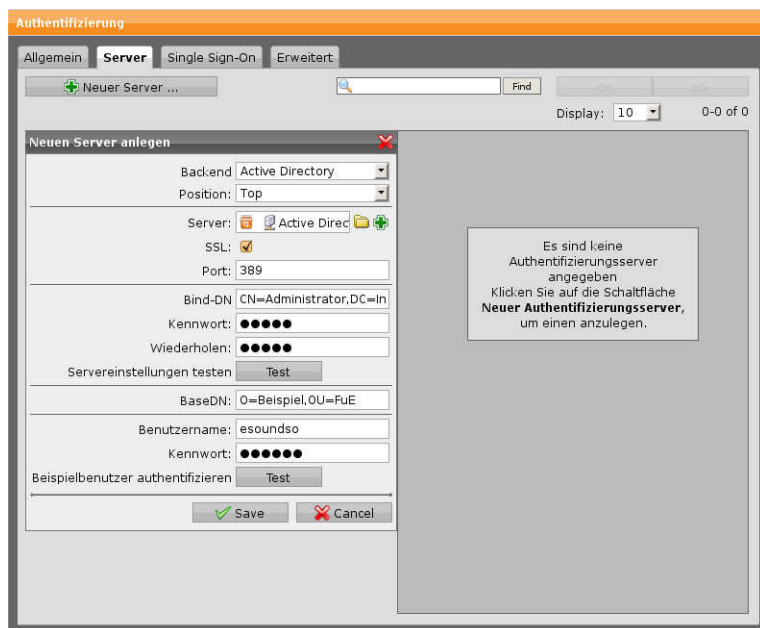


Figure 5.5 Authentifizierung: Benutzerauthentifizierung mit Active Directory

Die Implementierung der Active-Directory-Authentifizierung ermöglicht es, Astaro Security Gateway an einer Windows-Domäne zu registrieren, wodurch ein Objekt für Astaro Security Gateway auf dem primären Domänencontroller (DC) angelegt wird. Das Sicherheitssystem ist dann in der Lage, Benutzer- und Gruppeninformationen von der Domäne abzufragen.

Um eine Active-Directory-Authentifizierung zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Server* auf *Neuer Server*.**

Das Dialogfenster *Neuen Server anlegen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Backend: Wählen Sie *Active Directory* als Backend-Verzeichnisdienst.

Position: Wählen Sie eine Position für den Backend-Server. Backend-Server mit niedrigeren Nummern werden zuerst abgefragt. Stellen Sie für eine bessere Leistung sicher, dass der Backend-Server, der wahrscheinlich die meisten Anfragen erhält, ganz oben in der Liste steht.

Server: Wählen Sie einen Active Directory-Server (oder fügen Sie ihn hinzu).

SSL verwenden: Wählen Sie diese Option, um SSL-gesicherten Datentransfer zu aktivieren. Der Port ändert sich dann von 389 (LDAP) auf 636 (ldaps = LDAP over SSL).

Port: Wählen Sie den Port des eDirectory-Servers. Standardmäßig ist das Port 389.

Servereinstellungen testen: Durch einen Klick auf diese Schaltfläche wird ein Bind-Test mit dem konfigurierten Server durchgeführt. Dadurch wird sichergestellt, dass die Einstellungen auf dieser Registerkarte richtig sind, und dass der Server eingeschaltet ist und Verbindungen entgegennimmt. Die Schaltfläche ist erst sichtbar, wenn die Servereinstellungen durch einen Klick auf *Übernehmen* gespeichert wurden.

Bind-DN: Der volle *Distinguished Name* (DN) des Benutzers, mit dem dieser am Server angemeldet werden soll in LDAP-Notation. Dieser Benutzer wird benötigt, da anonyme Anfragen an den Active-Directory-Server gewöhnlich nicht erlaubt sind. Beachten Sie, dass der Bind-Benutzer genügend Privilegien besitzen muss, um alle relevanten Informationen zur Benutzerdefinition vom Active-Directory-Server erhalten zu können, damit er Benutzer authentifizieren kann – das ist eine Voraussetzung, die meistens vom Administrator der Domäne erfüllt wird.

Jeder DN besteht aus einem oder mehreren *Relative Distinguished Names* (RDN). Ein RDN setzt sich aus Attributen des Benutzerobjekts zusammen und umfasst seinem Benutzernamen, den Knoten wo es sich befindet und den höchsten DN des Servers. Die Definition erfolgt in der LDAP-Notation und als Trennzeichen wird das Komma verwendet.

- Der Benutzername muss der Name des Benutzers sein, der in der Lage ist, auf das Verzeichnis zuzugreifen und folgendermaßen spezifiziert ist: CN-Bezeichner (z. B. CN=Benutzer). Obwohl die Benutzung eines beliebigen Kontos mit Domänenberechtigungen, wie z. B. „admin“, möglich ist, wird als bessere Methode dringend empfohlen, einen Benutzer zu wählen, der keine Administrationsrechte besitzt, da es völlig ausreichend

für diesen Benutzer ist, Leserechte auf alle Objekte des angegebenen BaseDN zu besitzen.

- Die Information über den Knoten, an dem sich das Benutzerobjekt befindet, muss alle Unterknoten zwischen dem Wurzelknoten und dem Benutzerobjekt umfassen und besteht gewöhnlich aus Komponenten wie sogenannten Organisationseinheiten (engl. *organizational units*) und dem allgemeinen Namen (CN, engl. *common name*). Organisationseinheiten (dargestellt durch ein Verzeichnis-/Buchsymbol in der Microsoft Management-Konsole) werden durch den OU-Bezeichner spezifiziert. Beachten Sie, dass die Reihenfolge der Knoten vom untersten zum obersten verläuft, d. h. dass spezifischere Elemente zuerst angegeben werden (z. B. OU=Management_US, OU=Management). Andererseits werden Standardcontainer von Active Directory (dargestellt durch ein einfaches Verzeichnis-Symbol) wie z. B. der vordefinierte *Benutzer*-Knoten durch den CN-Bezeichner spezifiziert (z. B. CN=Users).
- Der oberste DN des Servers kann aus mehreren Domänenkomponenten (engl. *domain component*) bestehen, wobei jede durch den DC-Bezeichner spezifiziert wird. Beachten Sie, dass die Domänenkomponenten in der gleichen Reihenfolge angegeben werden wie der Domänenname. Beispiel: Wenn der Domänenname *beispiel.de* ist, dann ist der DN-Teil DC=beispiel,DC=de.

Ein Beispiel für einen Bind-Benutzer-DN wäre CN=administrator, CN=Users,DC=beispiel,DC=de, wenn der Benutzername *administrator* ist und sich das Benutzerobjekt im Container *Users* befindet in einer Domäne namens *beispiel.de*.

Nehmen wir nun an, Sie haben eine Organisationseinheit namens *Management* mit dem Unterknoten *Management_US* angelegt und verschieben das Benutzerobjekt „Administrator“ dorthin, dann ändert sich der DN wie folgt: CN=administrator,OU=Management_US,OU=Management,DC=beispiel,DC=de

Kennwort: Geben Sie das Kennwort für den Bind-Benutzer ein (ein zweites Mal zur Bestätigung).

Servereinstellungen testen: Durch einen Klick auf diese Schaltfläche wird ein Bind-Test mit dem konfigurierten Server durchgeführt. Dadurch wird sichergestellt, dass die Einstellungen auf dieser Registerkarte richtig sind, und dass der Server eingeschaltet ist und Verbindungen entgegennimmt. Die Schaltfläche ist erst sichtbar, wenn die Servereinstellungen durch einen Klick auf *Übernehmen* gespeichert wurden.

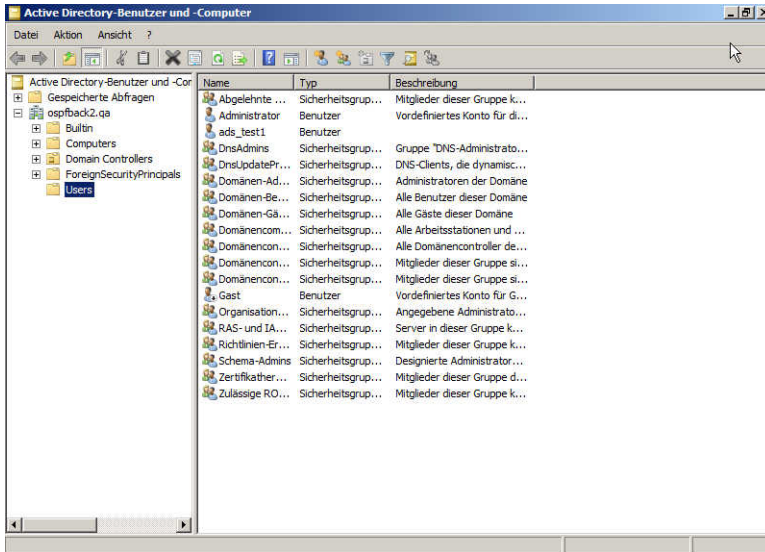


Figure 5.6 Authentifizierung: Microsoft Management-Konsole

BaseDN: Der Startpunkt, relativ gesehen zur Wurzel (engl. *root*) des LDAP-Baums, wo die Benutzer eingefügt sind, die authentifiziert werden sollen. Beachten Sie, dass der BaseDN über den vollen Distinguished Name (DN) in LDAP-Notation spezifiziert werden müssen, wobei Kommas als Trennzeichen verwendet werden müssen (z. B. `0=Beispiel,OU=RnD`). Der BaseDN kann leer sein. In diesem Fall wird der BaseDN automatisch aus dem Verzeichnis abgerufen.

Benutzername: Geben Sie den Benutzernamen eines Testbenutzers ein, um eine reguläre Authentifizierung durchzuführen.

Kennwort: Geben Sie das Kennwort des Testbenutzers ein.

Beispielbenutzer authentifizieren: Klicken Sie auf die Schaltfläche *Testen*, um den Authentifizierungstest für den Testbenutzer zu starten. Dies stellt sicher, dass alle Servereinstellungen korrekt sind, dass der Server eingeschaltet ist und Verbindungen akzeptiert, und dass Benutzer erfolgreich authentifiziert werden können.

3. Klicken Sie *Speichern*.

Der neue Server wird in der Liste *Server* angezeigt.

LDAP

LDAP steht für *Lightweight Directory Access Protocol* und ist ein Netzwerkprotokoll, um Verzeichnisdienste, die auf dem x.500-Standard basieren, zu modifizieren und Anfragen zu senden. Astaro Security Gateway benutzt das LDAP-Protokoll, um Benutzer für einige seiner Dienste zu authentifizieren, indem mit Hilfe von Attributen oder Gruppenzugehörigkeiten auf dem LDAP-Server festgestellt wird, ob Zugriff auf einen bestimmten Dienst gewährt wird oder nicht.

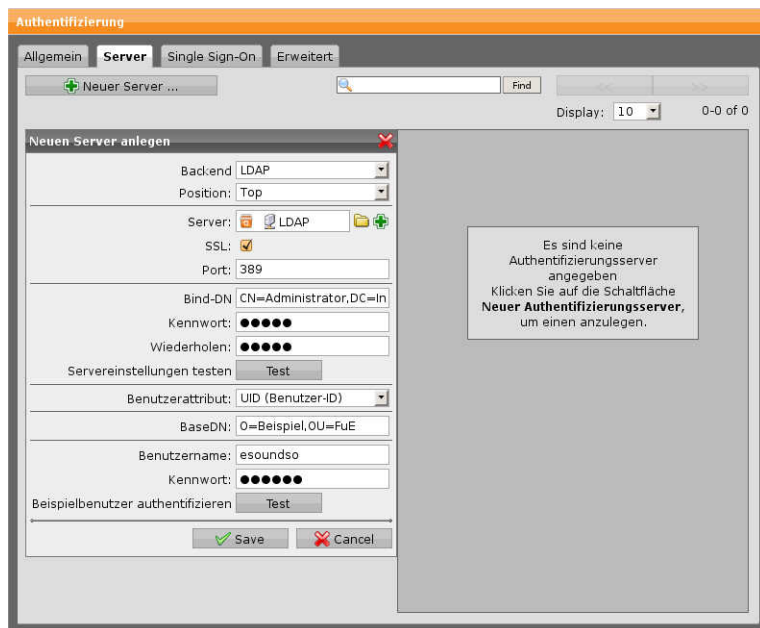


Figure 5.7 Authentifizierung: Benutzerauthentifizierung mit LDAP

Um eine LDAP-Authentifizierung zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Server* auf *Neuer Server*.**
Das Dialogfenster *Neuen Server anlegen* wird geöffnet.
2. **Nehmen Sie die folgenden Einstellungen vor:**
Backend: Wählen Sie *LDAP* als Backend-Verzeichnisdienst.
Position: Wählen Sie eine Position für den Backend-Server. Backend-Server mit niedrigeren Nummern werden zuerst abgefragt. Stellen Sie für eine bessere Leistung sicher, dass der Backend-Server, der wahrscheinlich die meisten Anfragen erhält, ganz oben in der Liste steht.

Server: Wählen Sie einen LDAP-Server (oder fügen Sie ihn hinzu).

SSL verwenden: Wählen Sie diese Option, um SSL-gesicherten Datentransfer zu aktivieren. Der Port ändert sich dann von 389 (LDAP) auf 636 (ldaps = LDAP over SSL).

Port: Tragen Sie den Port des LDAP-Servers ein. Der Port 389 ist voreingestellt.

Bind-DN: Der *Distinguished Name* (DN) des Benutzers, mit dem dieser am Server angemeldet werden soll. Dieser Benutzer ist zwingend. Aus Sicherheitsgründen werden anonyme Anfragen an den LDAP-Server nicht unterstützt. Beachten Sie, dass der Benutzer genügend Privilegien besitzen muss, um alle relevanten Informationen zur Benutzerdefinition vom LDAP-Server erhalten zu können, damit er Benutzer authentifizieren kann. LDAP-Benutzer, -Gruppen und -Container können durch den vollen Distinguished Name in LDAP-Notation spezifiziert werden, wobei Kommas als Trennzeichen benutzt werden müssen (z. B. CN=administrator,DC=intranet,DC=beispiel,DC=de).

Kennwort: Geben Sie das Kennwort für den Bind-Benutzer ein (ein zweites Mal zur Bestätigung).

Servereinstellungen testen: Durch einen Klick auf diese Schaltfläche wird ein Bind-Test mit dem konfigurierten Server durchgeführt. Dadurch wird sichergestellt, dass die Einstellungen auf dieser Registerkarte richtig sind, und dass der Server eingeschaltet ist und Verbindungen entgegennimmt. Die Schaltfläche ist erst sichtbar, wenn die Servereinstellungen durch einen Klick auf *Übernehmen* gespeichert wurden.

Benutzerattribut: Wählen Sie das Benutzerattribut, das als Filter für die Suche im LDAP-Verzeichnis benutzt werden soll. Das Benutzerattribut enthält den eigentlichen Anmeldenamen, nach dem jeder Benutzer von z. B. Fernzugriffsdiensten gefragt wird. Folgende Benutzerattribute stehen zur Auswahl:

- CN (allgemeiner Name, engl. *common name*)
- SN (Nachname)
- UID (Benutzer-ID)

Falls Benutzernamen in Ihrem LDAP-Verzeichnis nicht in Form dieser Attribute gespeichert werden, wählen Sie *<<Angepasst>>* aus der *Benutzerattribut*-Liste aus und geben Sie Ihr benutzerdefiniertes Attribut an. Beachten Sie, dass dieses Attribut in Ihrem LDAP-Verzeichnis konfiguriert sein muss.

BaseDN: Der Startpunkt, relativ gesehen zur Wurzel (engl. *root*) des LDAP-Baums, wo die Benutzer eingefügt sind, die authentifiziert werden sollen. Beachten Sie, dass der BaseDN über den vollen Distinguished Name (DN)

in LDAP-Notation spezifiziert werden müssen, wobei Kommas als Trennzeichen verwendet werden müssen (z.B. `0=Beispiel,0U=RnD`). Der BaseDN kann leer sein. In diesem Fall wird der BaseDN automatisch aus dem Verzeichnis abgerufen.

Benutzername: Geben Sie den Benutzernamen eines Testbenutzers ein, um eine reguläre Authentifizierung durchzuführen.

Kennwort: Geben Sie das Kennwort des Testbenutzers ein.

Beispielbenutzer authentifizieren: Klicken Sie auf die Schaltfläche *Testen*, um den Authentifizierungstest für den Testbenutzer zu starten. Dies stellt sicher, dass alle Servereinstellungen korrekt sind, dass der Server eingeschaltet ist und Verbindungen akzeptiert, und dass Benutzer erfolgreich authentifiziert werden können.

3. Klicken Sie *Speichern*.

Der neue Server wird in der Liste *Server* angezeigt.

RADIUS

RADIUS steht für *Remote Authentication Dial In User Service* und ist ein weit verbreitetes Protokoll, mit dem Netzwerkgeräte, wie z. B. Router, Informationen für die Benutzerauthentifizierung von einem zentralen Server abfragen können. Neben den reinen Benutzerinformationen für die Authentifizierung kann RADIUS auch technische Informationen verwalten, die von Netzwerkgeräten benutzt werden. Dazu gehören z. B. verwendete Protokolle, IP-Adressen, Routeninformationen etc. Zusammen bilden sie ein Benutzerprofil, das in einer Datei oder Datenbank auf dem RADIUS-Server gespeichert wird.

Das RADIUS-Protokoll ist sehr flexibel und es gibt Server für die meisten Betriebssysteme. Die Umsetzung von RADIUS auf diesem Sicherheitssystem ermöglicht es Ihnen, Zugriffsrechte basierend auf Proxies und Benutzern zu konfigurieren. Um die RADIUS-Authentifizierung verwenden zu können, benötigen Sie einen laufenden RADIUS-Server im Netzwerk. Da Kennwörter in Klartext (unverschlüsselt) übermittelt werden, platzieren Sie den RADIUS-Server in demselben Netzwerk wie Ihr Sicherheitssystem und stellen Sie sicher, dass das Sicherheitssystem und der Server am selben Switch hängen.

Um eine RADIUS-Authentifizierung zu konfigurieren, gehen Sie folgendermaßen vor:

1. Klicken Sie auf der Registerkarte *Server* auf *Neuer Server*.

Das Dialogfenster *Neuen Server anlegen* wird geöffnet.

2. Nehmen Sie die folgenden Einstellungen vor:

Backend: Wählen Sie *RADIUS* als Backend-Verzeichnisdienst.

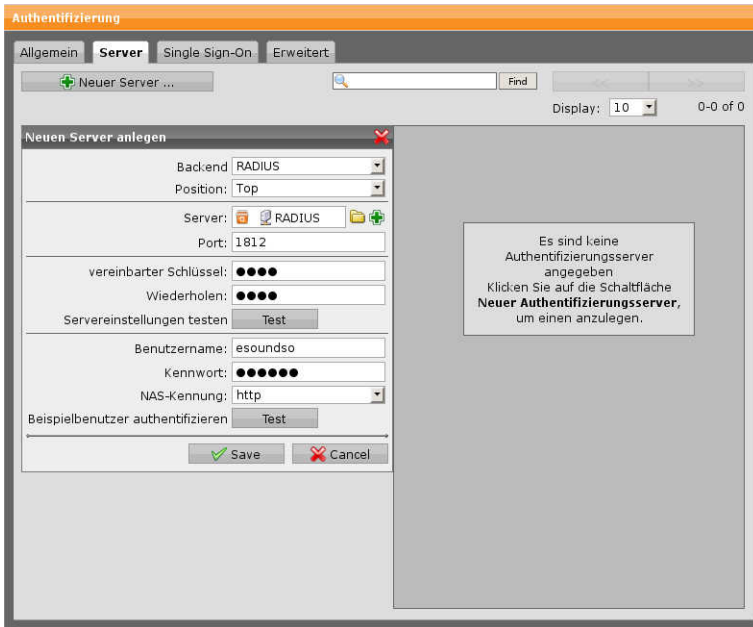


Figure 5.8 Authentifizierung: Benutzerauthentifizierung mit RADIUS

Position: Wählen Sie eine Position für den Backend-Server. Backend-Server mit niedrigeren Nummern werden zuerst abgefragt. Stellen Sie für eine bessere Leistung sicher, dass der Backend-Server, der wahrscheinlich die meisten Anfragen erhält, ganz oben in der Liste steht.

Server: Wählen Sie einen RADIUS-Server (oder fügen Sie ihn hinzu).

Port: Tragen Sie den Port des RADIUS-Servers ein. Der Port 1812 ist voreingestellt.

Vereinbarter Schlüssel: Dieser vereinbarte Schlüssel (engl. *Shared Secret*) ist eine Zeichenfolge, die als Kennwort zwischen dem RADIUS-Client und dem RADIUS-Server dient. Geben Sie den vereinbarten Schlüssel ein (ein zweites Mal zur Bestätigung).

Servereinstellungen testen: Durch einen Klick auf diese Schaltfläche wird ein Bind-Test mit dem konfigurierten Server durchgeführt. Dadurch wird sichergestellt, dass die Einstellungen auf dieser Registerkarte richtig sind, und dass der Server eingeschaltet ist und Verbindungen entgegennimmt. Die Schaltfläche ist erst sichtbar, wenn die Servereinstellungen durch einen Klick auf *Übernehmen* gespeichert wurden.

Benutzername: Geben Sie den Benutzernamen eines Testbenutzers ein, um eine reguläre Authentifizierung durchzuführen.

Kennwort: Geben Sie das Kennwort des Testbenutzers ein.

NAS-Kennung: Wählen Sie die entsprechende NAS-Kennung aus der Liste. Weitere Informationen entnehmen Sie bitte dem untenstehenden Hinweis und der Tabelle.

Beispielbenutzer authentifizieren: Klicken Sie auf die Schaltfläche *Testen*, um den Authentifizierungstest für den Testbenutzer zu starten. Dies stellt sicher, dass alle Servereinstellungen korrekt sind, dass der Server eingeschaltet ist und Verbindungen akzeptiert, und dass Benutzer erfolgreich authentifiziert werden können.

3. Klicken Sie *Speichern*.

Der neue Server wird in der Liste *Server* angezeigt.

Hinweis – Jeder Benutzerauthentifizierungsdienst von Astaro Security Gateway, wie z.B. PPTP oder L2TP, der Anfragen an den RADIUS-Server stellt, sendet eine andere Kennung (NAS-Kennung, engl. *NAS identifier*) an den RADIUS-Server. Beispiel: der PPTP-Dienst sendet die NAS-Kennung *pptp* an den RADIUS-Server, wenn er versucht, einen Benutzer zu authentifizieren. Dadurch können die verschiedenen Dienste auf dem RADIUS-Server auseinander gehalten werden. Das kommt den Autorisierungszwecken zugute, d. h. der Zugriffsgenehmigung für den Benutzer auf verschiedene Dienste. Unten finden Sie eine Liste der Benutzerauthentifizierungsdienste und ihrer NAS-Kennung.

Benutzerauthentifizierungsdienst	NAS-Kennung
SSL-VPN	ssl
PPTP	pptp
IPSec	ipsec
L2TP über IPSec	l2tp
SMTP-Proxy	smtp
Benutzerportal	portal
WebAdmin	webadmin
SOCKS-Proxy	socks
HTTP/S-Proxy	http

Table 5.1 RADIUS NAS-Kennungen

TACACS

TACACS+ steht für *Terminal Access Controller Access Control System* und ist ein proprietäres Protokoll von Cisco Systems Inc., das detaillierte Netzwerkverkehrsinformationen liefert und administrative Kontrolle über Authentifizierungs- und Autorisierungsprozesse ermöglicht.

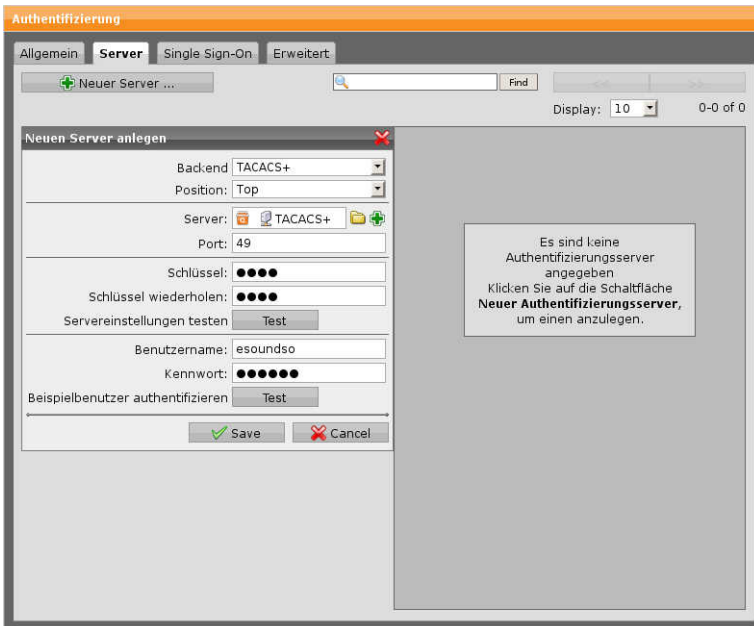


Figure 5.9 Authentifizierung: Benutzerauthentifizierung mit TACACS+

Um eine TACACS+-Authentifizierung zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Server* auf *Neuer Server*.**

Das Dialogfenster *Neuen Server anlegen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Backend: Wählen Sie *TACACS+* als Backend-Verzeichnisdienst.

Position: Wählen Sie eine Position für den Backend-Server. Backend-Server mit niedrigeren Nummern werden zuerst abgefragt. Stellen Sie für eine bessere Leistung sicher, dass der Backend-Server, der wahrscheinlich die meisten Anfragen erhält, ganz oben in der Liste steht.

Server: Wählen Sie einen TACACS+-Server (oder fügen Sie ihn hinzu).

Port: Tragen Sie den Port des TACACS+-Servers ein. Der Port 49 ist voreingestellt.

Schlüssel: Der Schlüssel für die Authentifizierung und die Verschlüsselung der gesamten TACACS+-Kommunikation zwischen Astaro Security Gateway und dem TACACS+-Server ein. Der hier eingegebene Wert des Schlüssels muss mit dem auf dem TACACS+-Server übereinstimmen. Tragen Sie den Schlüssel ein (ein zweites Mal zur Bestätigung).

Servereinstellungen testen: Durch einen Klick auf diese Schaltfläche wird ein Bind-Test mit dem konfigurierten Server durchgeführt. Dadurch wird sichergestellt, dass die Einstellungen auf dieser Registerkarte richtig sind, und dass der Server eingeschaltet ist und Verbindungen entgegennimmt. Die Schaltfläche ist erst sichtbar, wenn die Servereinstellungen durch einen Klick auf *Übernehmen* gespeichert wurden.

Benutzername: Geben Sie den Benutzernamen eines Testbenutzers ein, um eine reguläre Authentifizierung durchzuführen.

Kennwort: Geben Sie das Kennwort des Testbenutzers ein.

Beispielbenutzer authentifizieren: Klicken Sie auf die Schaltfläche *Testen*, um den Authentifizierungstest für den Testbenutzer zu starten. Dies stellt sicher, dass alle Servereinstellungen korrekt sind, dass der Server eingeschaltet ist und Verbindungen akzeptiert, und dass Benutzer erfolgreich authentifiziert werden können.

3. Klicken Sie *Speichern*.

Der neue Server wird in der Liste *Server* angezeigt.

Single Sign-On

Auf der Registerkarte *Benutzer >> Authentifizierung >> Single Sign-On* können Sie die Single-Sign-On-Funktionalität für Active Directory und/oder eDirectory konfigurieren.

Active Directory Single Sign-On (SSO)

Beachten Sie, dass die Active-Directory-SSO-Einrichtung augenblicklich nur mit dem HTTP/S-Proxy verwendet wird, um Single Sign-On für Browser bereitzustellen, die NTLMv2 oder Kerberos-Authentifizierung unterstützen.

Um die Single-Sign-On-Funktionalität zu aktivieren, muss das Sicherheitssystem der Active-Directory-Domäne beitreten. Damit dieser Domänenbeitritt funktioniert, müssen die folgenden Voraussetzungen erfüllt sein:

Authentifizierung

Allgemein | Server | **Single Sign-On** | Erweitert

Active Directory Single Sign-On (SSO)

Status: Domäne beigetreten
OSPFBACK2.QA.

Domäne:

Server:

Admin-Benutzername:

Kennwort:

Wiederholen:

Zur Aktivierung der Single-Sign-On-Funktionalität muss das System der Active-Directory-Domäne beitreten. Geben Sie den Domänennamen ein (z. B. 'intranet.IhreFirma.com'), der Sie beitreten wollen, sowie die Anmeldeangaben eines Administrators, der der Domäne Computer hinzufügen darf.

Active-Directory-SSO erfolgreich gespeichert ✓ Apply

eDirectory Single-Sign-On (SSO)

Status: SSO is not used in any http profiles.

Server:

Select here which eDirectory server should be used for SSO. eDirectory SSO uses a regularly defined eDirectory server. This server will be used when 'eDirectory SSO' is chosen as authentication method in Web Security -> HTTP/S.

Sync-Intervall:

Set the interval at which the user authentication daemon of Astaro Security Gateway synchronizes all currently logged-in users with the eDirectory server. Allowed values are 1-900 seconds. An interval of 20 seconds is recommended.

✓ Übernehmen

Figure 5.10 Authentifizierung: Konfiguration von Single Sign-On

- Die Zeitzone auf der Firewall und dem Domänencontroller (DC) müssen gleich sein.
- Der Zeitunterschied der Uhren darf NICHT mehr als fünf Minuten zwischen der Firewall und dem DC betragen.
- Der ASG-Rechnername muss im AD-DNS-System vorhanden sein.
- Die ASG muss das AD-DNS zur Weiterleitung (engl. *forwarder*) verwenden, oder es muss eine DNS-Anfrageroute zur AD-Domäne besitzen, die auf den AD-DNS-Server zeigt.

Um Active Directory SSO zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Legen Sie einen Active-Directory-Server auf der Registerkarte Server an.**
2. **Nehmen Sie die folgenden Einstellungen vor:**
Domäne: Tragen Sie hier den Namen der Domäne ein (z.B. `intranet.meinefirma.de`).
Admin-Benutzername: Tragen Sie den Benutzernamen ein, der auch die

Rechte für die Anbindung von Computern an diese Domäne besitzt (in der Regel ist dies der „Administrator“).

Kennwort: Tragen Sie das Kennwort für den Admin-Benutzer ein (ein zweites Mal zur Bestätigung).

3. Klicken Sie Übernehmen.

Ihre Einstellungen werden gespeichert.

Hinweis zur Unterstützung der Kerberos-Authentifizierung: Damit die opportunistische SSO-Kerberos-Unterstützung funktioniert, *müssen* die Clients den FQDN-Rechnernamen der ASG in ihren Proxyeinstellungen verwenden; die Benutzung der IP-Adresse wird nicht funktionieren. Der NTLMv2-Modus ist von dieser Voraussetzung nicht betroffen, und wird automatisch benutzt, wenn diese Voraussetzung nicht erfüllt ist oder wenn der Browser eine Kerberos-Authentifizierung nicht unterstützt.

eDirectory Single Sign-On (SSO)

Hier können Sie SSO für eDirectory konfigurieren. Wenn Sie eDirectory SSO als Konfigurationsmethode unter *Web Security* > *HTTP/S* eingerichtet haben, dann wird der hier gewählt eDirectory-Server benutzt.

Um eDirectory SSO zu konfigurieren, gehen Sie folgendermaßen vor:

1. Legen Sie einen eDirectory-Server auf der Registerkarte *Server* an.

2. Wählen Sie den eDirectory-Server aus.

Wählen Sie den eDirectory-Server aus der Auswahlliste aus, für den Sie SSO aktivieren wollen.

3. Klicken Sie Übernehmen.

Ihre Einstellungen werden gespeichert.

Erweitert

Kennwortkomplexität

Mit dieser Option können Sie festlegen, dass Administratoren oder lokal registrierte Benutzer mit administrativen Rechten sichere Kennwörter verwenden müssen. Die Kennwortkomplexität kann den folgenden Bedingungen unterliegen:

- Mindestlänge des Kennwortes (acht Zeichen ist voreingestellt)
- mindestens ein kleingeschriebener Buchstabe
- mindestens ein großgeschriebener Buchstabe
- mindestens eine Zahl
- mindestens ein nicht-alphanumerisches Zeichen

Um die ausgewählten Kennworteigenschaften einzuschalten, wählen Sie die Option *Komplexe Kennwörter verlangen* und klicken Sie *Übernehmen*.

Verzeichnis-Benutzer vorabholen

Benutzer von eDirectory oder Active Directory können mit der ASG synchronisiert werden. Das bedeutet, dass Benutzerdefinitionen vorab auf der ASG angelegt werden, so dass diese Benutzerdefinitionen bereits existieren, wenn sich ein Benutzer anmeldet. Der Synchronisationsprozess kann wöchentlich oder täglich stattfinden.

Um die Vorabholung (engl. *prefetching*) zu aktivieren, nehmen Sie die folgenden Einstellungen vor:

Server: Die Auswahlliste enthält Server, die auf der Registerkarte *Server* angelegt wurden. Wählen Sie einen Server aus, für den Sie Vorabholung aktivieren möchten.

Vorabholungsintervall: Wählen Sie ein Intervall, um Benutzer vorabzuholen. Um die Synchronisation wöchentlich stattfinden zu lassen, wählen Sie einen Wochentag, zu der die Synchronisation beginnen soll. Um die Synchronisation täglich stattfinden zu lassen, wählen Sie *Täglich*.

Vorabholungszeit: Wählen Sie eine Uhrzeit, zu der die Synchronisierung stattfinden soll.

eDirectory/Active-Directory-Gruppen: Geben Sie hier die Gruppen ein, die im Voraus angelegt werden sollen. Sie können den integrierten LDAP-Browser verwenden, um die Gruppen auszuwählen.

Aktiviere Backend-Synchronisierung bei Anmeldung (optional): Wählen Sie diese Option aus, wenn Sie wollen, dass Benutzerinformationen aus dem Verzeichnis geholt werden, sobald sich ein bislang unbekannter Benutzer anmeldet.

Klicken Sie *Übernehmen*.

Ihre Einstellungen werden gespeichert.

Jetzt vorabholen: Klicken Sie auf diese Schaltfläche, um den Vorabholungsprozess sofort zu starten.

Öffnen: Klicken Sie auf diese Schaltfläche, um das Live-Protokoll der Vorabholung zu öffnen.

Definitionen

Dieses Kapitel beschreibt die Konfiguration von Netzwerk- und Dienstdefinitionen sowie von sogenannten *Zeitereignissen*, die in Astaro Security Gateway verwendet werden. Die Seite *Definitionenübersicht* in WebAdmin zeigt die Anzahl aller Definitionen anhand ihres Typs und die Anzahl aller Dienste anhand ihres Protokolls.

Mit den Seiten des Menüs *Definitionen* können Sie zentral Netzwerke und Dienste definieren, die dann auch an anderen Stellen verwendet werden können. Dies erlaubt es Ihnen, überall mit einheitlichen Namen zu arbeiten statt mit unhandlichen IP-Adressen, Portnummern und Subnetzmasken. Ein weiterer Vorteil von Definitionen liegt darin, dass Sie individuelle Netzwerke und Dienste gruppieren und auf einmal konfigurieren können. Wenn Sie dann später Änderungen an den Einstellungen dieser Gruppe vornehmen, gelten diese für alle darin enthaltenen Netzwerke und Dienste.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- Netzwerke
- Dienste
- Zeitereignisse

Netzwerke

Auf der Seite *Definitionen* >> *Netzwerke* werden die Rechner (engl. *hosts*), Netzwerke und Netzwerkgruppen des Sicherheitssystems zentral definiert und verwaltet. Die hier angelegten Definitionen können an vielen anderen Stellen der WebAdmin-Konfigurationsmenüs verwendet werden.

Tipp – Wenn Sie auf das Info-Symbol einer Netzwerkdefinition in der Netzwerkliste klicken, können Sie alle Konfigurationsoptionen sehen, in denen diese Netzwerkdefinition verwendet wird.

Die Netzwerktabelle enthält auch statische Netzwerke, die automatisch vom System angelegt wurden und die weder bearbeitet noch gelöscht werden können:

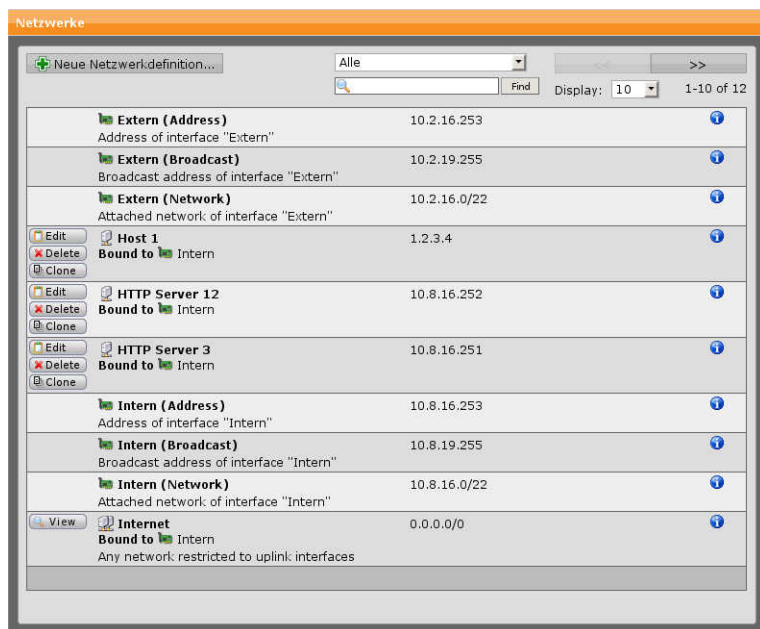


Figure 6.1 Definitionen: Liste der Netzwerkdefinitionen

- **Schnittstellen-Adresse:** Eine Definition dieser Art wird für jede Netzwerkkarte hinzugefügt. Sie enthält die aktuelle IP-Adresse der Schnittstelle. Ihr Name besteht aus dem Namen der Schnittstelle gefolgt von dem Zusatz „(Address)“.
- **Schnittstellen-Broadcast-Adresse:** Eine Definition dieser Art wird für jede Ethernet-artige Netzwerkschnittstelle hinzugefügt. Sie enthält die aktuelle IPv4-Broadcast-Adresse der Schnittstelle. Ihr Name besteht aus dem Namen der Schnittstelle gefolgt von dem Zusatz „(Broadcast)“.
- **Schnittstellen-Netzwerkadresse:** Eine Definition dieser Art wird für jede Ethernet-artige Netzwerkschnittstelle hinzugefügt. Sie enthält das aktuelle IPv4-Netzwerk der Schnittstelle. Ihr Name besteht aus dem Namen der Schnittstelle gefolgt von dem Zusatz „(Netzwerk)“.
- **Internet:** Eine Netzwerkdefinition, die an diejenige Schnittstelle gebunden ist, die als Standardgateway fungiert. Die Benutzung dieser Definition sollte Ihren Konfigurationsprozess erleichtern. Wenn *Uplink-Ausgleich* aktiviert ist, ist *Internet* an die *Uplink Interfaces* gebunden.

Um eine Netzwerkdefinition anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Netzwerke* auf *Neue Netzwerkdefinition*.**

Das Dialogfenster *Neue Netzwerkdefinition erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Name: Geben Sie einen aussagekräftigen Name für diese Definition ein.

Typ: Wählen Sie einen Netzwerkdefinitionstyp. Die folgenden Typen sind verfügbar:

- **Rechner:** Eine einzelne IPv4-Adresse eines Rechners (Host). Geben Sie die folgenden Informationen ein:
 - **Schnittstelle (optional):** Die Netzwerkdefinition kann an eine bestimmte Schnittstelle gebunden werden, so dass Verbindungen zu dieser Definition nur über diese Schnittstelle zustande kommen.
 - **Adresse:** Die IP-Adresse des Rechners (Sie können keine IP-Adresse einer bereits konfigurierten Schnittstelle eingeben).
 - **Kommentar (optional):** Fügen Sie eine Beschreibung oder sonstige Informationen über diesen Rechner hinzu.
- **DNS-Rechner:** Ein DNS-Rechnername, der dynamisch vom System aufgelöst wird, um eine IP-Adresse zu erhalten. DNS-Rechner sind nützlich, wenn es darum geht, mit dynamischen IP-Endpunkten zu arbeiten. Das System wird diese Definitionen periodisch immer wieder neu auflösen, wobei es sich an den TTL-Werten (Time To Live) orientiert, und die Definitionen nach Bedarf mit den neuen IP-Adressen aktualisieren. Geben Sie die folgenden Informationen ein:
 - **Schnittstelle (optional):** Die Netzwerkdefinition kann an eine bestimmte Schnittstelle gebunden werden, so dass Verbindungen zu dieser Definition nur über diese Schnittstelle zustande kommen.
 - **Rechnername:** Der Name des Rechners, der aufgelöst werden soll.
 - **Kommentar (optional):** Fügen Sie eine Beschreibung oder sonstige Informationen über diesen DNS-Rechner hinzu.
- **DNS-Gruppe:** Eine DNS-Gruppe ist ähnlich zu einem DNS-Rechner, aber sie kann mit mehreren RRs (Resource Records, dt. Ressourcen-Einträge) für einen einzelnen Rechner im DNS umgehen. Eine DNS-Gruppe ist nützlich für die Definition von Paketfilterregeln und für Ausnahmelisten in transparenten Proxies.

- **Netzwerk:** Ein Standard-IPv4-Netzwerk, das aus einer Netzwerkadresse und einer Netzmaske besteht. Geben Sie die folgenden Informationen ein:
 - **Schnittstelle (optional):** Die Netzwerkdefinition kann an eine bestimmte Schnittstelle gebunden werden, so dass Verbindungen zu dieser Definition nur über diese Schnittstelle zustande kommen.
 - **Adresse:** Die Netzwerkadresse des Netzwerks (Sie können keine IP-Adresse einer bereits konfigurierten Schnittstelle eingeben).
 - **Netzmaske:** Die Bitmaske, die angibt, wie viele Bits eines Oktetts das Subnetzwerk spezifizieren, und wie viele Bits Platz für Rechneradressen bieten.
 - **Kommentar (optional):** Fügen Sie eine Beschreibung oder sonstige Informationen über dieses Netzwerk hinzu.
- **Netzwerkgruppe:** Ein virtueller Behälter, der eine Liste anderer Netzwerkdefinitionen enthält. Sie können ihn verwenden, um Netzwerke und Rechner zusammenzufassen, damit Ihre Konfiguration übersichtlicher wird. Sobald Sie *Network Group* ausgewählt haben, erscheint das Feld *Mitglieder*, wo Sie die Gruppenmitglieder hinzufügen können.
- **Multicast-Gruppe:** Ein Netzwerk, das einen festgelegten Multicast-Netzwerkbereich umfasst.
 - **Adresse:** Die Netzwerkadresse des Multicast-Netzwerks, die im Bereich 224.0.0.0 bis 239.255.255.255 liegen muss.
 - **Schnittstelle (optional):** Die Netzwerkdefinition kann an eine bestimmte Schnittstelle gebunden werden, so dass Verbindungen zu dieser Definition nur über diese Schnittstelle zustande kommen.
 - **Netzmaske:** Die Bitmaske, die angibt, wie viele Bits eines Oktetts das Subnetzwerk spezifizieren, und wie viele Bits Platz für Rechneradressen bieten.
 - **Kommentar (optional):** Fügen Sie eine Beschreibung oder sonstige Informationen über dieses Netzwerk hinzu.
- **Verfügbarkeitsgruppe:** Eine Gruppe aus Rechnern und/oder DNS-Rechnern, die nach Priorität angeordnet sind. Die Verfügbarkeit aller Rechner wird in bestimmten Abständen durch ICMP-Pings überprüft.

Der (verfügbare) Rechner mit der höchsten Priorität und wird für die Konfiguration verwendet.

- **Mitglieder:** Fügen Sie die Gruppenmitglieder hinzu.
- **Prüfintervall:** Geben Sie eine Zeitspanne in Sekunden an, in der die Rechner per Ping überprüft werden.

3. Klicken Sie **Speichern**.

Die neue Definition erscheint in der Netzwerkdefinitionsliste.

Um eine Netzwerkdefinition zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Dienste

Auf der Seite *Definitionen* > > *Dienste* werden die Dienste und die Dienstgruppen zentral definiert und verwaltet. Dienste sind Definitionen bestimmter Arten von Netzwerkverkehr. Eine Dienstdefinition besteht aus einem Protokoll, z. B. TCP oder UDP, und protokoll-relevanten Optionen wie Portnummern. Mittels der Dienste können Sie bestimmen, welche Arten von Netzwerkverkehr von der Firewall angenommen oder abgelehnt werden.

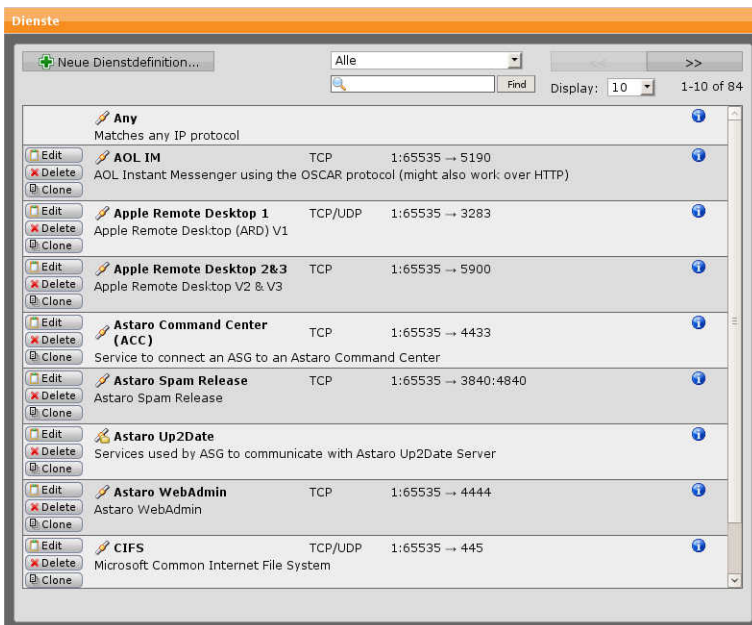


Figure 6.2 Dienste: Dienstdefinitionen

Tipp – Wenn Sie auf das Info-Symbol einer Dienstdefinition in der Liste *Dienste* klicken, werden Ihnen alle Konfigurationsoptionen angezeigt, in denen diese Dienstdefinition verwendet wird.

Um eine Dienstdefinition anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Definitionen* >> *Dienste* auf *Neue Dienstdefinition*.**

Das Dialogfenster *Neue Dienstdefinition erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

(Abhängig von dem gewählten Definitionstyp werden weitere Parameter der Netzwerkdefinition angezeigt.)

Name: Geben Sie einen aussagekräftigen Name für diese Definition ein.

Definitionstyp: Wählen Sie den Diensttyp aus. Die folgenden Typen sind verfügbar:

- **TCP:** TCP-Verbindungen (Transmission Control Protocol) verwenden Portnummern von 0 bis 65535. Verlorene Pakete werden von TCP erkannt und erneut abgefragt. Bei einer TCP-Verbindung informiert der Empfänger den Absender darüber, wenn er ein Paket erfolgreich erhalten hat (verbindungsbezogenes Protokoll). TCP-Sitzungen beginnen mit einem 3-Wege-Handshake und Verbindungen werden am Ende der Sitzung geschlossen. Geben Sie die folgenden Information an:
 - **Zielport:** Geben Sie den Zielport ein, entweder als einzelne Portnummer (z. B. 80) oder als Bereich (z. B. 1024:64000) mit einem Doppelpunkt als Trennzeichen.
 - **Quellport:** Geben Sie den Quellport ein, entweder als einzelne Portnummer (z. B. 80) oder als Bereich (z. B. 1024:64000) mit einem Doppelpunkt als Trennzeichen.
- **UDP:** Das UDP-Protokoll (User Datagram Protocol) verwendet Portnummern zwischen 0 und 65535 und ist ein zustandsloses (engl. *stateless*) Protokoll. Da UDP sich keine Zustände merkt, ist es schneller als TCP, besonders wenn es sich um das Versenden kleiner Datenmengen handelt. Diese Zustandslosigkeit bedeutet aber auch, dass UDP nicht erkennen kann, wenn Pakete verloren gehen oder verworfen (engl. *drop*) werden. Wenn Sie *UDP* gewählt haben, können Sie die gleichen Konfigurationsoptionen angeben wie bei TCP.

- **TCP/UDP:** Hierbei handelt es sich um eine Kombination von TCP und UDP, die sich besonders für Anwendungsprotokolle eignet, die beide Unterprotokolle verwenden, z. B. DNS. Wenn Sie *TCP/UDP* gewählt haben, können Sie die gleichen Konfigurationsoptionen angeben wie bei *TCP* oder *UDP*.
- **ICMP:** Das ICMP-Protokoll (Internet Control Message Protocol) wird, kurz gesagt, dazu verwendet, Fehlermeldungen zu versenden, die angeben, dass z. B. ein angeforderter Dienst nicht verfügbar ist oder dass ein Rechner oder Router nicht erreicht werden kann. Wenn Sie *ICMP* gewählt haben, geben Sie den ICMP-Typ/Code an.
- **IP:** Das Internet-Protokoll (Internet Protocol) ist ein Netzwerk- und Transportprotokoll für den Datenaustausch über das Internet. Wenn Sie *IP* gewählt haben, geben Sie die Nummer desjenigen Protokolls an, das in IP eingebettet werden soll, z. B. 121 (steht für das SMP-Protokoll).
- **ESP:** Das ESP-Protokoll (Encapsulating Security Payload) ist Teil des IPSec-Tunnelprotokoll-Pakets, welches Verschlüsselungsdienste für Daten bietet, die über VPN-Tunnel gesendet werden. Wenn Sie *ESP* oder *AH* gewählt haben, geben Sie den Sicherheitsparameterindex an, der in Verbindung mit der IP-Adresse die Sicherheitsassoziation identifiziert. Sie können entweder einen Wert zwischen 256 und 4.294.967.296 angeben, oder die Voreinstellung des Bereichs 256 bis 4.294.967.296 (Kommas als Trennzeichen!) beibehalten, insbesondere wenn Sie automatischen Schlüsselaustausch für IPSec verwenden. Beachten Sie, dass die Zahlen 1–255 von IANA (Internet Assigned Numbers Authority) reserviert sind.
- **AH:** Die Authentifizierungskopfzeile (Authentication Header) ist Teil des IPSec-Tunnelprotokoll-Pakets und befindet sich zwischen der IP-Kopfzeile (engl. *header*) und den Paket-Nutzdaten (engl. *payload*), um die Integrität der Daten zu verwalten – jedoch nicht deren Geheimhaltung.
- **Group:** (dt. Gruppe) Hierbei handelt es sich um eine Art Behälter, welcher eine Liste anderer Dienste enthält. Sie können ihn verwenden, um Dienstdefinitionen zusammenzufassen, damit Ihre Konfiguration übersichtlicher wird. Wenn Sie *Group* gewählt haben, erscheint das Feld *Mitglieder*, wo Sie Gruppenmitglieder hinzufügen können (d. h. andere Dienstdefinitionen).

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die Dienstdefinition hinzu.

3. Klicken Sie *Speichern*.

Die neue Dienstdefinition wird in der Dienstdefinitionenliste angezeigt.

Um eine Dienstdefinition zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Hinweis – Der Typ der Definition kann im Nachhinein nicht mehr geändert werden. Wenn Sie den Typ der Definition ändern wollen, müssen Sie die Dienstdefinition löschen und eine neue mit den gewünschten Einstellungen anlegen.

Zeitereignisse

Auf der Seite *Definitionen* >> *Zeitereignisse* werden einzelne (engl. *single*) oder wiederkehrende (engl. *recurring*) Zeitereignisse (engl. *time events*) definiert, die dann dazu verwendet werden können, Paketfilterregeln oder Inhaltsprofile auf bestimmte Zeiträume zu beschränken.

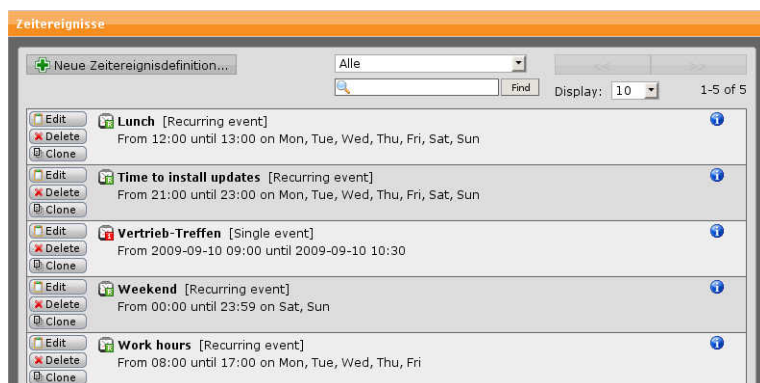


Figure 6.3 Zeitereignisse: Liste der Zeitereignisdefinitionen

Tipp – Wenn Sie auf das Info-Symbol einer Zeitereignisdefinition in der Liste *Zeitereignisse* klicken, werden Ihnen alle Konfigurationsoptionen angezeigt, in denen diese Zeitereignisdefinition verwendet wird.

Um eine Zeitereignisdefinition anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Definitionen* >> *Zeitereignisse* auf *Neue Zeitereignisdefinition*.**

Das Dialogfenster *Neue Zeitereignisdefinition erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Name: Geben Sie einen aussagekräftigen Name für dieses Zeitereignis ein.

Typ: Wählen Sie den Typ des Zeitereignisses aus. Die folgenden Zeitereignis-Typen sind verfügbar:

- **Wiederkehrendes Ereignis:** Diese Ereignisse kehren periodisch wieder. Sie können Startzeit, Endzeit und die Wochentage angeben, für die diese Zeitereignisdefinition gelten soll. Ein Start- oder Enddatum kann für diesen Typ nicht ausgewählt werden.
- **Einzelereignis:** Diese Ereignisse finden nur einmal statt. Sie können sowohl Startdatum und -zeit auswählen als auch ein Enddatum/-zeit. Da diese Ereignisse nicht wiederkehren, können Sie die Option *Wochentage* für diesen Typ nicht auswählen.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über das Zeitereignis hinzu.

3. **Klicken Sie *Speichern*.**

Die neue Zeitereignisdefinition wird in der Liste *Zeitereignisse* angezeigt.

Um eine Zeitereignisdefinition zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Hinweis – Sie können nur Zeitereignisse löschen, die nicht von einer Paketfilterregel oder innerhalb eines *Web Security* >> *HTTP/S-Profile* >> *Filterzuweisungen* verwendet werden.

Netzwerk

Dieses Kapitel beschreibt die Konfiguration der Schnittstellen und die netzwerkspezifischen Einstellungen in Astaro Security Gateway. Die Übersichtsseite *Netzwerkstatistik* zeigt eine Zusammenfassung über die zehn häufigsten am heutigen Tag benutzten Dienste, Quellrechner und gleichzeitigen Verbindungen. Jeder der Abschnitte enthält einen *Details*-Link. Ein Klick auf den Link leitet Sie zur entsprechenden Seite des Abschnitts *Berichte* von WebAdmin weiter, wo Sie weitere statistische Informationen finden können.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- Schnittstellen
- Bridging
- Statisches Routing
- Dynamisches Routing (OSPF)
- Dienstqualität (QoS)
- Multicast Routing (PIM-SM)

Schnittstellen

Eine Firewall benötigt mindestens zwei Netzwerkkarten um ein internes Netzwerk (LAN, engl. *Local Area Network*) mit einem externen Netzwerk (WAN, engl. *Wide Area Network*) zu verbinden. Bei den folgenden Beispielen ist die Netzwerkkarte `eth0` immer die interne Netzwerkschnittstelle. Die Netzwerkkarte `eth1` ist als externe Netzwerkschnittstelle vorgesehen (z. B. zum Internet). Diese beiden Seiten werden auch *Trusted* bzw. *Untrusted* genannt.

Während der Installation werden die Netzwerkkarten automatisch erkannt. Falls bei der Software Appliance später weitere Netzwerkkarten hinzugefügt werden, ist eine Neuinstallation des Sicherheitssystems notwendig. Nutzen Sie hierfür die Backup-Funktion, um nach der Neuinstallation Ihre aktuelle Systemkonfiguration einfach wieder einzuspielen.

Die Appliance muss die einzige Schnittstelle zwischen dem internem und dem externen Netzwerk sein. Alle Datenpakete müssen das Sicherheitssystem passieren. Wir raten dringend davon ab, die Schnittstellen der Firewall über einen Hub oder Switch physikalisch zusammen auf ein Netzwerksegment zu legen, es sei denn dieser ist als VLAN-Switch konfiguriert. Unter Umständen kann es sonst zu falschen ARP-Auflösungen (Address Resolution Protocol) kommen (ARP-Clash), die nicht alle Betriebssysteme (z. B. die von Microsoft) verwalten können. Pro Firewall-Netzwerkschnittstelle muss daher auch ein physikalisches Netzwerk-Segment verwendet werden.

Im Menü *Schnittstellen* können Sie alle auf dem Sicherheitssystem installierten Netzwerkkarten installieren und die Schnittstelle zum externen Netzwerk (WAN) und zu den internen Netzwerken (LAN, DMZ) konfigurieren.

Hinweis – Beachten Sie bei der Planung und Konfiguration Ihrer Netzwerktopologie, welche Netzwerkkarten Sie jeweils auf der Appliance auswählen. Für die Schnittstelle zum externen Netzwerk (WAN) ist die Netzwerkkarte mit der SysID `eth1` vorgesehen. Für die spätere Installation eines Hochverfügbarkeitssystems (HA) benötigen Sie auf beiden Appliances eine Netzwerkkarte mit gleicher SysID. Die Installation des HA-Systems wird auf der Seite Hochverfügbarkeit beschrieben.

In den nachfolgenden Abschnitten wird erklärt, wie die verschiedenen Arten von Schnittstellen (engl. *interface types*) über die Registerkarten *Schnittstellen*, *Zusätzliche Adressen*, *Linkbündelung*, *Uplink-Ausgleich*, *Multipfadregeln* und *Hardware* verwaltet und konfiguriert werden.

Schnittstellen

Auf der Registerkarte *Schnittstellen* können Sie die Netzwerkkarten und virtuellen Schnittstellen konfigurieren. In der Liste sind die bereits konfigurierten Netzwerkschnittstellen mit ihrem symbolischen Namen, Netzwerkkarte und aktueller Adresse aufgeführt. Ebenso wird der Status jeder Schnittstelle angezeigt. Durch Anklicken des Statussymbols können Sie Schnittstellen aktivieren und deaktivieren.

Tipp – Wenn Sie auf das Infosymbol einer Netzwerkschnittstelle in der Liste *Schnittstellen* klicken, werden Ihnen alle Konfigurationen angezeigt, in denen diese Schnittstelle benutzt wird.

Neu hinzugefügte Schnittstellen können am Anfang als *Aus* angezeigt werden, solange sich die Verbindung noch im Aufbau befindet. Sie können Schnittstellen bearbeiten oder löschen, indem Sie auf die entsprechenden Schaltflächen klicken.

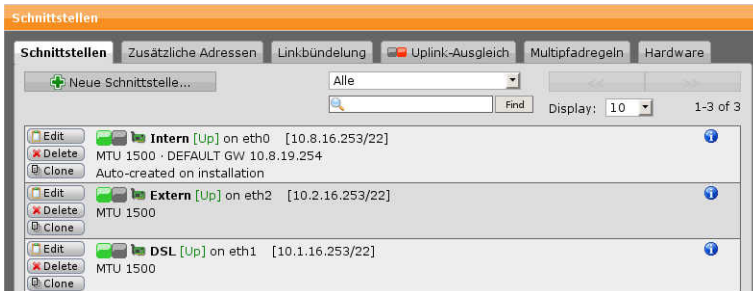


Figure 7.1 Schnittstellen: Konfiguration von Schnittstellen

Automatische Netzwerkschnittstellen-Definitionen

Jede Schnittstelle auf der Firewall besitzt einen symbolischen Namen und eine Netzwerkkarte, dem sie zugewiesen ist. Der symbolische Name wird verwendet, wenn Sie bei einer anderen Konfigurationseinstellung auf diese Schnittstelle Bezug nehmen. Für jede Schnittstelle wird automatisch eine passende Gruppe von Netzwerkdefinitionen von der Firewall angelegt:

- Eine Definition, die die aktuelle IP-Adresse der Schnittstelle enthält, und deren Name sich aus dem Schnittstellennamen und der Erweiterung (*Address*) zusammensetzt.
- Eine Definition, die das Netzwerk enthält, mit dem die Schnittstelle verbunden ist, und deren Name sich aus dem Schnittstellennamen und der Erweiterung (*Network*) zusammensetzt. Diese Definition wird nicht für *Point-to-Point*-Schnittstellen (PPP) angelegt.
- Eine Definition, die die Broadcast-Adresse der Schnittstelle enthält, und deren Name sich aus dem Schnittstellennamen und der Erweiterung (*Broadcast*) zusammensetzt. Diese Definition wird nicht für *Point-to-Point*-Schnittstellen (PPP, dt. *Punkt-zu-Punkt*) angelegt.

Wenn die Schnittstelle eine automatische Methode zur Adresszuweisung verwendet (wie z. B. DHCP oder dynamische Zuweisung), so werden diese Definitionen automatisch aktuell gehalten. Alle Einstellungen, die sich auf diese

Definitionen beziehen, z. B. Paketfilter- und NAT-Regeln, werden ebenfalls automatisch auf die geänderte Adresse aktualisiert. Eine Schnittstelle mit dem symbolischen Namen *Internal* ist bereits vordefiniert. Falls Sie sie umbenennen möchten, sollten Sie das direkt nach der Installation tun.

Arten von Schnittstellen

Die nachfolgende Liste gibt eine Übersicht darüber, welche Arten von Schnittstellen zu der Firewall hinzugefügt werden können, und welche Hardware dafür benötigt wird:

Standard-Ethernet: Dabei handelt es sich um eine normale Ethernet-Schnittstelle mit einer Bandbreite von 10, 100 oder 1000 Mbit/s.

Ethernet VLAN: VLAN (Virtual LAN) ist eine Methode, um mehrere schicht-2-getrennte Netzwerksegmente auf einer einzigen Hardwareschnittstelle zu ermöglichen. Jedes Segment wird durch eine VLAN-ID (auch engl. *tag* genannt) identifiziert, wobei es sich um eine einfache Ganzzahl (engl. *Integer*) handelt. Wenn Sie eine VLAN-Schnittstelle hinzufügen, erzeugen Sie damit ein Hardware-Gerät, das dazu verwendet werden kann, auch zusätzliche Schnittstellen (Aliase) hinzuzufügen. PPPoE- und PPPoA-Geräte können nicht über VLAN virtuelle Hardware betrieben werden.

Cable Modem (DHCP): Dabei handelt es sich um eine Standard-Ethernet-Schnittstelle mit DHCP.

DSL (PPPoE): PPP over Ethernet. Ein DSL-PPPoE-Gerät ermöglicht Ihnen, Ihre Firewall an *PPP-over-Ethernet*-kompatible DSL-Leitungen anzuschließen. Diese Geräte erfordern eine dedizierte Ethernet-Verbindung (sie können nicht mit anderen Schnittstellen auf derselben Hardware koexistieren). Sie müssen ein DSL-Modem an das Schnittstellennetzwerksegment anschließen. Die Netzwerkparameter für diese Gerätetypen können über eine entfernte Stelle zugewiesen werden (typischerweise Ihr Internetanbieter). Überdies müssen Sie einen Benutzernamen und Kennwort für Ihr Verbindungskonto angeben.

DSL (PPPoA/PPTP): PPP over ATM. Ein PPPoA-Gerät ermöglicht Ihnen, Ihre Firewall an *PPP-over-ATM*-kompatible DSL-Leitungen anzuschließen. Diese Geräte benutzen das PPT-Protokoll um IP-Pakete zu tunneln. Sie erfordern eine dedizierte Ethernet-Verbindung (sie können nicht mit anderen Schnittstellen auf derselben Hardware koexistieren). Die Netzwerkparameter für diese Gerätetypen können über eine entfernte Stelle zugewiesen werden (typischerweise Ihr Internetanbieter). Überdies müssen Sie einen Benutzernamen und Kennwort für Ihr Verbindungskonto angeben. Auch müssen Sie die IP-Adresse Ihres Modem angeben. Diese Adresse ist dem Modem normalerweise fest zugewiesen und kann nicht geändert werden. Um mit dem Modem kommunizieren zu

können, müssen Sie eine NIC-IP-Adresse und eine Netzmaske eingeben. Die IP-Adresse des Modems muss sich dabei innerhalb des durch diese Parameter definierten Netzwerks befinden. Die *Ping-Adresse* muss ein Rechner am anderen Ende der PPTP-Verbindung sein, der die ICMP-Pingabfragen beantwortet. Sie können versuchen, den DNS-Server Ihres Anbieters dafür zu verwenden. Falls diese Adresse nicht gepingt werden kann, wird angenommen, dass die Verbindung tot ist. Dann wird die Verbindung neu aufgebaut.

Modem (PPP): Diese Art der Schnittstelle ermöglicht Ihnen, das Sicherheitssystem über ein PPP-Modem mit dem Internet zu verbinden. Für die Konfiguration benötigen Sie eine serielle Schnittstelle und ein externes Modem auf dem Sicherheitssystem. Darüber hinaus benötigen Sie DSL-Zugangsdaten inklusive Kennwort. Diese Daten erhalten Sie von Ihrem Anbieter.

Standard-Ethernet

Um eine Netzwerkkarte für eine Standard-Ethernet-Verbindung zu einem internen oder externen Netzwerk zu konfigurieren, muss die Netzwerkkarte mit einer IP-Adresse und einer Netzmaske konfiguriert werden.

Um eine Standard-Ethernet-Schnittstelle zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Schnittstellen* auf *Neue Schnittstelle*.**
Das Dialogfenster *Neue Schnittstelle erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Name: Geben Sie einen aussagekräftigen Name für die Schnittstelle ein.

Art: Wählen Sie *Standard-Ethernet* aus der Auswahlliste aus.

Hardware: Wählen Sie aus der Auswahlliste *Hardware* eine Schnittstelle aus.

Tipp – Wählen Sie als primäre Schnittstelle zum externen Netzwerk (WAN) die Netzwerkkarte mit der SysID `eth1` aus. Bitte beachten Sie, dass eine Netzwerkkarte nicht gleichzeitig als *Standard-Ethernet*-Schnittstelle und als PPP over Ethernet (PPPoE-DSL) oder PPTP over Ethernet (PPPoA-DSL) genutzt werden kann.

Adresse: Tragen Sie die IP-Adresse der Schnittstelle ein.

Netzmaske: Wählen Sie eine Netzwerkmaste aus.

Standard-GW (optional): Falls Sie ein statisches Standardgateway definieren wollen, wählen Sie die Option *Standard-GW* aus.

Standard-GW IP (optional): Tragen Sie hier die IP-Adresse des Standard-gateway ein.

Proxy ARP: Wählen Sie diese Option aus, um die *Proxy-ARP*-Funktion zu aktivieren. Standardmäßig ist diese Option deaktiviert.

Diese Funktion ist für Schnittstellen vom Typ Broadcast verfügbar. Wenn diese Funktion aktiviert ist, wird die Firewall über diese Schnittstelle Datenverkehr stellvertretend für andere Rechner annehmen und diesen entsprechend weiterleiten. Diese Aufgabe übernimmt die Firewall für alle Rechner zu denen es eine direkte Schnittstellenroute besitzt. Das ermöglicht Ihnen, ein „transparentes“ Netzwerk-Bridging einzurichten ohne auf die Firewall-Eigenschaften zu verzichten. Ein anderer Anwendungsfall für diese Funktion ist, wenn der Router Ihres Anbieters Ihr „offizielles“ Netzwerk einfach auf seine Ethernetschnittstelle setzt, anstelle eine Rechnerroute zu verwenden.

MTU: Geben Sie die maximale Größe der Datenpakete (engl. *Maximum Transmission Unit*) für die Schnittstelle in Bytes an. Sie müssen einen Wert eingeben, der zur Art der Schnittstelle passt, wenn Sie Verkehrsverwaltung betreiben wollen. Der voreingestellte Wert ist ein sinnvoller Wert und sollte nur von technisch erfahrenen Benutzern geändert werden, da ein falscher Wert die Schnittstelle funktionsunfähig machen kann. Der MTU-Wert ist für den Schnittstellentyp *Standard-Ethernet* auf 1500 Bytes voreingestellt. Ein MTU-Wert, der größer als 1500 Bytes ist, muss vom Netzwerkbetreiber und der Netzwerkkarte (z. B. Gigabit-Netzwerkkarte) unterstützt werden.

Asymmetrisch (optional): Wählen Sie diese Option, falls die Bandbreite von Uplink und Downlink Ihrer Verbindung nicht identisch ist und Sie wollen, dass das Dashboard das widerspiegelt. Es werden zwei Textfelder angezeigt, in die Sie die Maximum-Bandbreite des Uplinks in entweder Mbps oder kbps angeben können. Wählen Sie die entsprechende Einheit aus der Auswahlliste aus.

Angezeigtes Max. (optional): Hier können Sie die maximale Downlink-Bandbreite Ihrer Verbindung angeben, wenn Sie wollen, dass das Dashboard sie widerspiegelt. Die Bandbreite kann entweder in Mbps oder kbps angegeben werden. Wählen Sie die entsprechende Einheit aus der Auswahlliste aus.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die Schnittstelle hinzu.

3. Klicken Sie *Speichern*.

Das System prüft die Einstellungen nun auf ihre Gültigkeit. Nach der erfolg-

reichen Prüfung erscheint die neue Schnittstelle in der Schnittstellen-Liste. Die Schnittstelle ist noch ausgeschaltet (Statusampel zeigt Rot).

4. Aktivieren Sie die Schnittstelle.

Aktivieren Sie die Schnittstelle durch einen Klick auf die Statusampel. Die Schnittstelle ist nun eingeschaltet (Statusampel zeigt Grün). Zu Beginn wird die Meldung *Down* angezeigt. Das System benötigt kurze Zeit, um die neue Schnittstelle zu konfigurieren und die Einstellungen zu laden. Die neue Schnittstelle ist in Betrieb, wenn die Meldung *Up* erscheint.

Um nur Schnittstellen einer bestimmten Art angezeigt zu bekommen, klicken Sie im Auswahlménú auf die entsprechende Art. Um eine Schnittstelle zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Ethernet-VLAN

Für die Verbindung zwischen dem Sicherheitssystem und den Virtual LANs benötigen Sie eine Netzwerkkarte mit tag-fähigem Treiber. Ein *Tag* ist ein kleiner 4-Byte-Header, der an den Ethernet-Header angefügt wird. Dieser angehängte Header enthält die VLAN-Nummer des VLAN, zu dem es gesendet werden soll: die VLAN-Nummer besteht aus 12 Bits. Es sind also 4095 verschiedene virtuelle LANs möglich. Diese VLAN-Nummer wird im WebAdmin als VLAN-Tag oder VLAN-ID bezeichnet.

Hinweis – Zur Konfiguration einer Ethernet-Virtual-LAN-Schnittstelle benötigen Sie eine Netzwerkkarte mit tag-fähigem Treiber. Die Hardware Compatibility List (HCL) befindet sich auf der Astaro Knowledgebase¹⁷. Benutzen Sie den Suchbegriff *HCL*, um schnell zur entsprechenden Seite zu gelangen.

Um eine Ethernet-VLAN-Schnittstelle zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Schnittstellen* auf *Neue Schnittstelle*.**
Das Dialogfenster *Neue Schnittstelle erstellen* wird geöffnet.
2. **Nehmen Sie die folgenden Einstellungen vor:**
 - Name:** Geben Sie einen aussagekräftigen Name für die Schnittstelle ein.
 - Art:** Wählen Sie *Ethernet-VLAN* aus der Auswahlliste aus.
 - Hardware:** Wählen Sie aus der Auswahlliste *Hardware* eine Schnittstelle

¹⁷ <http://www.astaro.com/kb/>

aus.

VLAN-Tag: Tragen Sie das Tag für das virtuelle Netzwerk ein.

Adresse: Tragen Sie die IP-Adresse der Schnittstelle ein.

Netzmaske: Wählen Sie eine Netzwerkmaske aus.

Standard-GW (optional): Falls Sie ein statisches Standardgateway definieren wollen, wählen Sie die Option *Standard-GW* aus.

Standard-GW IP (optional): Tragen Sie hier die IP-Adresse des Standardgateway ein.

MTU: Geben Sie die maximale Größe der Datenpakete (engl. *Maximum Transmission Unit*) für die Schnittstelle in Bytes an. Sie müssen einen Wert eingeben, der zur Art der Schnittstelle passt, wenn Sie Verkehrsverwaltung betreiben wollen. Der voreingestellte Wert ist ein sinnvoller Wert und sollte nur von technisch erfahrenen Benutzern geändert werden, da ein falscher Wert die Schnittstelle funktionsunfähig machen kann. Der MTU-Wert ist für den Schnittstellentyp *Ethernet-VLAN* auf 1500 Bytes voreingestellt. Ein MTU-Wert, der größer als 1500 Bytes ist, muss vom Netzwerkbetreiber und der Netzwerkkarte (z. B. Gigabit-Netzwerkkarte) unterstützt werden.

Asymmetrisch (optional): Wählen Sie diese Option, falls die Bandbreite von Uplink und Downlink Ihrer Verbindung nicht identisch ist und Sie wollen, dass das Dashboard das widerspiegelt. Es werden zwei Textfelder angezeigt, in die Sie die Maximum-Bandbreite des Uplinks in entweder Mbps oder kbps angeben können. Wählen Sie die entsprechende Einheit aus der Auswahlliste aus.

Angezeigtes Max. (optional): Hier können Sie die maximale Downlink-Bandbreite Ihrer Verbindung angeben, wenn Sie wollen, dass das Dashboard sie widerspiegelt. Die Bandbreite kann entweder in Mbps oder kbps angegeben werden. Wählen Sie die entsprechende Einheit aus der Auswahlliste aus.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die Schnittstelle hinzu.

3. Klicken Sie **Speichern**.

Das System prüft die Einstellungen nun auf ihre Gültigkeit. Nach der erfolgreichen Prüfung erscheint die neue Schnittstelle in der Schnittstellen-Liste. Die Schnittstelle ist noch ausgeschaltet (Statusampel zeigt Rot).

4. Aktivieren Sie die Schnittstelle.

Aktivieren Sie die Schnittstelle durch einen Klick auf die Statusampel. Die Schnittstelle ist nun eingeschaltet (Statusampel zeigt Grün). Zu Beginn wird die Meldung *Down* angezeigt. Das System benötigt kurze Zeit, um die neue Schnittstelle zu konfigurieren und die Einstellungen zu laden. Die neue Schnittstelle ist in Betrieb, wenn die Meldung *Up* erscheint.

Um nur Schnittstellen einer bestimmten Art angezeigt zu bekommen, klicken Sie im Auswahlmenü auf die entsprechende Art. Um eine Schnittstelle zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Kabelmodem (DHCP)

Um eine Kabelmodem-Schnittstelle (DHCP) zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Schnittstellen* auf *Neue Schnittstelle*.**
Das Dialogfenster *Neue Schnittstelle erstellen* wird geöffnet.
2. **Nehmen Sie die folgenden Einstellungen vor:**
Name: Geben Sie einen aussagekräftigen Name für die Schnittstelle ein.
Art: Wählen Sie *Kabelmodem (DHCP)* aus der Auswahlliste aus.
Hardware: Wählen Sie aus der Auswahlliste *Hardware* eine Schnittstelle aus.

Tipp – Wählen Sie als Schnittstelle zum externen Netzwerk (WAN) die Netzwerkkarte mit der SysID eth1 aus. Bitte beachten Sie, dass eine Netzwerkkarte nicht gleichzeitig als *Kabelmodem (DHCP)* und als PPP over Ethernet (PPPoE-DSL) oder PPPTP over Ethernet (PPPoA-DSL) genutzt werden kann.

Standard-GW (optional): Falls Sie ein statisches Standardgateway definieren wollen, wählen Sie die Option *Standard-GW* aus.

Standard-GW IP (optional): Tragen Sie hier die IP-Adresse des Standardgateway ein.

Proxy ARP: Wählen Sie diese Option aus, um die *Proxy-ARP*-Funktion zu aktivieren. Standardmäßig ist diese Option deaktiviert.

Diese Funktion ist für Schnittstellen vom Typ Broadcast verfügbar. Wenn diese Funktion aktiviert ist, wird die Firewall über diese Schnittstelle Datenverkehr stellvertretend für andere Rechner annehmen und diesen entsprechend weiterleiten. Diese Aufgabe übernimmt die Firewall für alle Rechner zu denen es eine direkte Schnittstellenroute besitzt. Das ermöglicht Ihnen, ein „transparentes“ Netzwerk-Bridging einzurichten ohne auf die Firewall-Eigenschaften zu verzichten. Ein anderer Anwendungsfall für diese Funktion ist, wenn der Router Ihres Anbieters Ihr „offizielles“ Netzwerk einfach auf seine Ethernetschnittstelle setzt, anstelle eine Rechnerroute zu verwenden.

MTU: Geben Sie die maximale Größe der Datenpakete (engl. *Maximum Transmission Unit*) für die Schnittstelle in Bytes an. Sie müssen einen Wert eingeben, der zur Art der Schnittstelle passt, wenn Sie Verkehrsverwaltung betreiben wollen. Der voreingestellte Wert ist ein sinnvoller Wert und sollte nur von technisch erfahrenen Benutzern geändert werden, da ein falscher Wert die Schnittstelle funktionsunfähig machen kann. Der MTU-Wert ist für den Schnittstellentyp *Kabelmodem* auf 1500 Bytes voreingestellt. Ein MTU-Wert, der größer als 1500 Bytes ist, muss vom Netzbetreiber und der Netzwerkkarte (z. B. Gigabit-Netzwerkkarte) unterstützt werden.

Rechnername (optional): Wenn Ihr ISP erfordert, dass Sie einen spezifischen Rechnername mit Ihrer DHCP-Anfrage übermitteln, geben Sie diesen in diesem Feld an. Geben Sie ihn aber nur an, wenn er wirklich gefordert ist.

Asymmetrisch (optional): Wählen Sie diese Option, falls die Bandbreite von Uplink und Downlink Ihrer Verbindung nicht identisch ist und Sie wollen, dass das Dashboard das widerspiegelt. Es werden zwei Textfelder angezeigt, in die Sie die Maximum-Bandbreite des Uplinks in entweder Mbps oder kbps angeben können. Wählen Sie die entsprechende Einheit aus der Auswahlliste aus.

Angezeigtes Max. (optional): Hier können Sie die maximale Downlink-Bandbreite Ihrer Verbindung angeben, wenn Sie wollen, dass das Dashboard sie widerspiegelt. Die Bandbreite kann entweder in Mbps oder kbps angegeben werden. Wählen Sie die entsprechende Einheit aus der Auswahlliste aus.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die Schnittstelle hinzu.

3. **Klicken Sie Speichern.**

Das System prüft die Einstellungen nun auf ihre Gültigkeit. Nach der erfolgreichen Prüfung erscheint die neue Schnittstelle in der Schnittstellen-Liste. Die Schnittstelle ist noch ausgeschaltet (Statusampel zeigt Rot).

4. **Aktivieren Sie die Schnittstelle.**

Aktivieren Sie die Schnittstelle durch einen Klick auf die Statusampel. Die Schnittstelle ist nun eingeschaltet (Statusampel zeigt Grün). Zu Beginn wird die Meldung *Down* angezeigt. Das System benötigt kurze Zeit, um die neue Schnittstelle zu konfigurieren und die Einstellungen zu laden. Die neue Schnittstelle ist in Betrieb, wenn die Meldung *Up* erscheint.

Um nur Schnittstellen einer bestimmten Art angezeigt zu bekommen, klicken Sie im Auswahlmenü auf die entsprechende Art. Um eine Schnittstelle zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

DSL (PPPoE)

Für diese Konfiguration benötigen Sie DSL-Zugangsdaten, inklusive Benutzername und Kennwort. Die Zugangsdaten erhalten Sie von Ihrem Internetanbieter (ISP). VDSL wird ebenfalls von dieser Schnittstellenart unterstützt.

Hinweis – Die Installation und spezifische Einstellungen für DSL-Verbindungen werden speziell für den Internet-Zugang mit T-DSL (Telekom Deutschland) im Leitfaden *Netzwerk mit T-DSL* erläutert. Beachten Sie auch, dass Ihr Sicherheitssystem 24 Stunden am Tag mit Ihrem Internetanbieter verbunden sein wird, wenn die DSL-Verbindung einmal aktiviert ist. Sie sollten deshalb sicherstellen, dass Ihr Anbieter die Verbindung als Flatrate oder bandbreiten-basiert abrechnet anstelle über die Verbindungsdauer. Der Leitfaden *Netzwerk mit T-DSL* ist in der Astaro Knowledgebase¹⁸ erhältlich.

Um eine DSL-(PPPoE)-Schnittstelle zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Schnittstellen auf Neue Schnittstelle*.**
Das Dialogfenster *Neue Schnittstelle erstellen* wird geöffnet.
2. **Nehmen Sie die folgenden Einstellungen vor:**
 - Name:** Geben Sie einen aussagekräftigen Name für die Schnittstelle ein.
 - Art:** Wählen Sie *DSL (PPPoE)* aus der Auswahlliste aus.
 - Hardware:** Wählen Sie aus der Auswahlliste *Hardware* eine Schnittstelle aus.
 - VDSL:** Wählen Sie diese Option (nur) aus, wenn es sich bei der Verbindung um eine VDSL-Verbindung handelt. Der *MTU*-Wert ändert sich auf 1476.
 - Standard-GW (optional):** Falls Sie ein statisches Standardgateway definieren wollen, wählen Sie die Option *Standard-GW* aus.
 - Standard-GW IP (optional):** Tragen Sie hier die IP-Adresse des Standardgateway ein.
 - Benutzername:** Tragen Sie den Benutzernamen ein, den Sie von Ihrem Anbieter erhalten haben.
 - Kennwort** Tragen sie das Kennwort ein, das Sie von Ihrem Anbieter haben.
 - Tägliche Wiedereinwahl:** Definieren Sie hier zu welcher Uhrzeit die Verbindung beendet und wieder neu aufgebaut werden soll. Sie können zwischen *Nie* und einer beliebigen Uhrzeit wählen.
 - Wiedereinwahl verzögern:** Definieren Sie hier die Zeitverzögerung für die

¹⁸ <http://www.astaro.com/kb/>

Wiedereinwahl. Standardmäßig beträgt sie *5 Sekunden*. Sollte Ihr Anbieter eine längere Verzögerung erfordern, dann können Sie den Wert auf *Eine Minute* oder *Fünfzehn Sekunden* setzen.

MTU: Geben Sie die maximale Größe der Datenpakete (engl. *Maximum Transmission Unit*) für die Schnittstelle in Bytes an. Sie müssen einen Wert eingeben, der zur Art der Schnittstelle passt, wenn Sie Verkehrsverwaltung betreiben wollen. Der voreingestellte Wert ist ein sinnvoller Wert und sollte nur von technisch erfahrenen Benutzern geändert werden, da ein falscher Wert die Schnittstelle funktionsunfähig machen kann. Der MTU-Wert ist für den Schnittstellentyp *DSL (PPPoE)* auf 1492 Bytes voreingestellt. Ein MTU-Wert, der größer als 1500 Bytes ist, muss vom Netzwerkbetreiber und der Netzwerkkarte (z. B. Gigabit-Netzwerkkarte) unterstützt werden.

Asymmetrisch (optional): Wählen Sie diese Option, falls die Bandbreite von Uplink und Downlink Ihrer Verbindung nicht identisch ist und Sie wollen, dass das Dashboard das widerspiegelt. Es werden zwei Textfelder angezeigt, in die Sie die Maximum-Bandbreite des Uplinks in entweder Mbps oder kbps angeben können. Wählen Sie die entsprechende Einheit aus der Auswahlliste aus.

Angezeigtes Max. (optional): Hier können Sie die maximale Downlink-Bandbreite Ihrer Verbindung angeben, wenn Sie wollen, dass das Dashboard sie widerspiegelt. Die Bandbreite kann entweder in Mbps oder kbps angegeben werden. Wählen Sie die entsprechende Einheit aus der Auswahlliste aus.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die Schnittstelle hinzu.

3. **Klicken Sie *Speichern*.**

Das System prüft die Einstellungen nun auf ihre Gültigkeit. Nach der erfolgreichen Prüfung erscheint die neue Schnittstelle in der Schnittstellen-Liste. Die Schnittstelle ist noch ausgeschaltet (Statusampel zeigt Rot).

4. **Aktivieren Sie die Schnittstelle.**

Aktivieren Sie die Schnittstelle durch einen Klick auf die Statusampel. Die Schnittstelle ist nun eingeschaltet (Statusampel zeigt Grün). Zu Beginn wird die Meldung *Down* angezeigt. Das System benötigt kurze Zeit, um die neue Schnittstelle zu konfigurieren und die Einstellungen zu laden. Die neue Schnittstelle ist in Betrieb, wenn die Meldung *Up* erscheint.

Um nur Schnittstellen einer bestimmten Art angezeigt zu bekommen, klicken Sie im Auswahlmenü auf die entsprechende Art. Um eine Schnittstelle zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

DSL (PPPoA/PPTP)

Für die Konfiguration einer *PPP over ATM*-Verbindung (PPPoA) benötigen Sie auf der Appliance eine freie Ethernet-Netzwerkkarte und ein externes ADSL-Modem mit Ethernet-Anschluss. Die Verbindung zum Internet erfolgt über zwei Teilstrecken. Zwischen der Appliance und dem ADSL-Modem erfolgt die Verbindung mit dem Protokoll *PPTP over Ethernet*. Die Verbindung vom ADSL-Modem zum Internetanbieter (ISP) erfolgt mit dem ADSL-Einwahlprotokoll *PPP over ATM*.

Die Konfiguration erfordert überdies DSL-Zugangsdaten inklusive Benutzername und Kennwort. Diese Informationen erhalten Sie von Ihrem Internetanbieter (ISP).

Hinweis – Die Installation und spezifische Einstellungen für DSL-Verbindungen werden speziell für den Internet-Zugang mit T-DSL (Telekom Deutschland) im Leitfaden *Netzwerk mit T-DSL* erläutert. Beachten Sie auch, dass Ihr Sicherheitssystem 24 Stunden am Tag mit Ihrem Internetanbieter verbunden sein wird, wenn die DSL-Verbindung einmal aktiviert ist. Sie sollten deshalb sicherstellen, dass Ihr Anbieter die Verbindung als Flatrate oder bandbreiten-basiert abrechnet anstelle über die Verbindungsdauer. Der Leitfaden *Netzwerk mit T-DSL* ist in der Astaro Knowledgebase¹⁹ erhältlich.

Um eine DSL-(PPPoA/PPTP)-Schnittstelle zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Schnittstellen* auf *Neue Schnittstelle*.**
Das Dialogfenster *Neue Schnittstelle erstellen* wird geöffnet.
2. **Nehmen Sie die folgenden Einstellungen vor:**
 - Name:** Geben Sie einen aussagekräftigen Name für die Schnittstelle ein.
 - Art:** Wählen Sie *Ethernet-VLAN* aus der Auswahlliste aus.
 - Hardware:** Wählen Sie aus der Auswahlliste *Hardware* eine Schnittstelle aus.
 - Standardgateway (optional):** Um das Standardgateway Ihres Internetanbieters zu verwenden, wählen Sie diese Option aus.
 - Modem-IP:** Tragen Sie die IP-Adresse des ADSL-Modems ein. Diese Adresse wird in der Regel vom Anbieter oder von der Hardware mitgeliefert und kann nicht geändert werden (z. B. 10.0.0.138 bei AonSpeed).

¹⁹ <http://www.astaro.com/kb/>

NIC-Adresse: Tragen Sie die IP-Adresse für die Netzwerkkarte auf der Appliance ein. Die Adresse muss im selben Subnetz liegen wie die IP-Adresse des Modems (z. B. 10.0.0.140 bei AonSpeed).

NIC-Netzmaske: Tragen Sie die Netzwerkmaske ein (z. B. 255.255.255.0 bei AonSpeed).

Ping-Adresse: Tragen Sie die IP-Adresse eines Rechners im Internet ein, der auf ICMP-Ping-Anfragen antwortet (z. B. der DNS-Server Ihres Internetanbieters). Um die Verbindung zwischen Ihrem Sicherheitssystem und dem externen Netzwerk zu testen, geben Sie eine IP-Adresse eines Rechners am anderen Ende des PPTP-Verbindung an. Sie können versuchen, den DNS-Server Ihres ISP zu verwenden. Das Sicherheitssystem sendet Ping-Anfragen zu diesem Rechner: falls das System von diese Rechner keine Antwort erhält, wird der Verbindungsaufbau abgebrochen.

Benutzername: Tragen Sie den Benutzernamen ein, den Sie von Ihrem Anbieter erhalten haben.

Kennwort: Tragen sie das Kennwort ein, das Sie von Ihrem Anbieter erhalten haben.

Tägliche Wiedereinwahl: Definieren Sie hier zu welcher Uhrzeit die Verbindung beendet und wieder neu aufgebaut werden soll. Sie können zwischen *Nie* und einer beliebigen Uhrzeit wählen.

MTU: Geben Sie die maximale Größe der Datenpakete (engl. *Maximum Transmission Unit*) für die Schnittstelle in Bytes an. Sie müssen einen Wert eingeben, der zur Art der Schnittstelle passt, wenn Sie Verkehrsverwaltung betreiben wollen. Der voreingestellte Wert ist ein sinnvoller Wert und sollte nur von technisch erfahrenen Benutzern geändert werden, da ein falscher Wert die Schnittstelle funktionsunfähig machen kann. Der MTU-Wert ist für den Schnittstellentyp *DSL (PPPoA)* auf 1492 Bytes voreingestellt. Ein MTU-Wert, der größer als 1500 Bytes ist, muss vom Netzwerkbetreiber und der Netzwerkkarte (z. B. Gigabit-Netzwerkkarte) unterstützt werden.

Asymmetrisch (optional): Wählen Sie diese Option, falls die Bandbreite von Uplink und Downlink Ihrer Verbindung nicht identisch ist und Sie wollen, dass das Dashboard das widerspiegelt. Es werden zwei Textfelder angezeigt, in die Sie die Maximum-Bandbreite des Uplinks in entweder Mbps oder kbps angeben können. Wählen Sie die entsprechende Einheit aus der Auswahlliste aus.

Angezeigtes Max. (optional): Hier können Sie die maximale Downlink-Bandbreite Ihrer Verbindung angeben, wenn Sie wollen, dass das Dashboard sie widerspiegelt. Die Bandbreite kann entweder in Mbps oder kbps angegeben werden. Wählen Sie die entsprechende Einheit aus der Auswahlliste aus.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die Schnittstelle hinzu.

3. Klicken Sie *Speichern*.

Das System prüft die Einstellungen nun auf ihre Gültigkeit. Nach der erfolgreichen Prüfung erscheint die neue Schnittstelle in der Schnittstellen-Liste. Die Schnittstelle ist noch ausgeschaltet (Statusampel zeigt Rot).

4. Aktivieren Sie die Schnittstelle.

Aktivieren Sie die Schnittstelle durch einen Klick auf die Statusampel. Die Schnittstelle ist nun eingeschaltet (Statusampel zeigt Grün). Zu Beginn wird die Meldung *Down* angezeigt. Das System benötigt kurze Zeit, um die neue Schnittstelle zu konfigurieren und die Einstellungen zu laden. Die neue Schnittstelle ist in Betrieb, wenn die Meldung *Up* erscheint.

Um nur Schnittstellen einer bestimmten Art angezeigt zu bekommen, klicken Sie im Auswahlmenü auf die entsprechende Art. Um eine Schnittstelle zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Modem (PPP)

Für diese Konfiguration benötigen Sie auf der Appliance eine serielle Schnittstelle und ein externes PPP-Modem. Darüberhinaus benötigen Sie die DSL-Zugangsdaten inklusive Benutzername und Kennwort. Die Zugangsdaten erhalten Sie von Ihrem Internetanbieter (ISP).

Um eine Modem-(PPP)-Schnittstelle zu konfigurieren, gehen Sie folgendermaßen vor:

1. Klicken Sie auf der Registerkarte *Schnittstellen* auf *Neue Schnittstelle*.

Das Dialogfenster *Neue Schnittstelle erstellen* wird geöffnet.

2. Nehmen Sie die folgenden Einstellungen vor:

Name: Geben Sie einen aussagekräftigen Name für die Schnittstelle ein.

Art: Wählen Sie *Ethernet-VLAN* aus der Auswahlliste aus.

Hardware: Wählen Sie aus der Auswahlliste *Hardware* eine Schnittstelle aus.

Standardgateway (optional): Um das Standardgateway Ihres Internetanbieters zu verwenden, wählen Sie diese Option aus.

Benutzername: Tragen Sie den Benutzernamen ein, den Sie von Ihrem Anbieter erhalten haben.

Kennwort: Tragen Sie das Kennwort ein, das Sie von Ihrem Anbieter erhalten haben.

Geschwindigkeit: Stellen Sie hier die Geschwindigkeit in Bits pro Sekunde für die Verbindung zwischen der Appliance und dem Modem ein. Übliche Werte sind 57.600 Bits/s und 115.200 Bits/s.

Datenflusskontrolle: Stellen Sie die Methode zur Kontrolle des Datenflusses ein.

Wenn die Daten über die serielle Verbindung laufen, kann es vorkommen, dass das System die ankommenden Daten nicht schnell genug verarbeiten kann. Um sicherzustellen, dass keine Daten verloren gehen, ist eine Methode zur Kontrolle des Datenflusses notwendig. Bei der seriellen Verbindung stehen zwei Methoden zur Auswahl:

- *Hardware-Signale*
- *Software-Signale*

Da bei einer PPP-Verbindung alle acht Bits der Leitung verwendet werden, und sich in den übertragenen Daten die Bytes der Steuerzeichen *Control S* und *Control Q* befinden, empfehlen wir, die Voreinstellung *Hardware* beizubehalten und ein entsprechendes serielles Verbindungskabel zu verwenden.

Init-Kennung: Tragen Sie in das Eingabefeld die Kennung zur Initialisierung des Modems ein. Beachten Sie, dass die *Init-Kennung* (init string) eventuell dem Modem angepasst werden muss. In diesem Fall entnehmen Sie die Init-Kennung dem zugehörigen Modem-Handbuch. Falls Sie keine entsprechende Dokumentation zur Verfügung haben, tragen Sie in das Eingabefeld *ATZ* ein.

Einwahlkennung: Tragen Sie in das Eingabefeld *ATDT* gefolgt von der Telefonnummer ein (z. B. *ATDT55512345*).

Rückstellung: Tragen Sie in das Eingabefeld die Rückstellungskennung (reset string) für das Modem ein. Beachten Sie auch hier, dass die Rückstellungskennung eventuell dem Modem angepasst werden muss. In diesem Fall entnehmen Sie diese dem zugehörigen Modem-Handbuch. Falls Sie keine entsprechende Dokumentation zur Verfügung haben, behalten Sie die voreingestellte Kennung *ATZ* bei.

MTU: Geben Sie die maximale Größe der Datenpakete (engl. *Maximum Transmission Unit*) für die Schnittstelle in Bytes an. Sie müssen einen Wert eingeben, der zur Art der Schnittstelle passt, wenn Sie Verkehrsverwaltung betreiben wollen. Der voreingestellte Wert ist ein sinnvoller Wert und sollte nur von technisch erfahrenen Benutzern geändert werden, da ein falscher Wert die Schnittstelle funktionsunfähig machen kann. Der MTU-Wert ist für den Schnittstellentyp *Modem (PPP)* auf 1492 Bytes voreingestellt. Ein MTU-Wert, der größer als 1500 Bytes ist, muss vom Netzwerkbetreiber und

der Netzwerkkarte (z. B. Gigabit-Netzwerkkarte) unterstützt werden.

Asymmetrisch (optional): Wählen Sie diese Option, falls die Bandbreite von Uplink und Downlink Ihrer Verbindung nicht identisch ist und Sie wollen, dass das Dashboard das widerspiegelt. Es werden zwei Textfelder angezeigt, in die Sie die Maximum-Bandbreite des Uplinks in entweder Mbps oder kbps angeben können. Wählen Sie die entsprechende Einheit aus der Auswahlliste aus.

Angezeigtes Max. (optional): Hier können Sie die maximale Downlink-Bandbreite Ihrer Verbindung angeben, wenn Sie wollen, dass das Dashboard sie widerspiegelt. Die Bandbreite kann entweder in Mbps oder kbps angegeben werden. Wählen Sie die entsprechende Einheit aus der Auswahlliste aus.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die Schnittstelle hinzu.

3. Klicken Sie *Speichern*.

Das System prüft die Einstellungen nun auf ihre Gültigkeit. Nach der erfolgreichen Prüfung erscheint die neue Schnittstelle in der Schnittstellen-Liste. Die Schnittstelle ist noch ausgeschaltet (Statusampel zeigt Rot).

4. Aktivieren Sie die Schnittstelle.

Aktivieren Sie die Schnittstelle durch einen Klick auf die Statusampel.

Die Schnittstelle ist nun eingeschaltet (Statusampel zeigt Grün). Zu Beginn wird die Meldung *Down* angezeigt. Das System benötigt kurze Zeit, um die neue Schnittstelle zu konfigurieren und die Einstellungen zu laden. Die neue Schnittstelle ist in Betrieb, wenn die Meldung *Up* erscheint.

Um nur Schnittstellen einer bestimmten Art angezeigt zu bekommen, klicken Sie im Auswahlmenü auf die entsprechende Art. Um eine Schnittstelle zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Zusätzliche Adressen

Einer Standard-Ethernet-Netzwerkkarte können mehrere zusätzliche IP-Adressen zugeordnet werden (IP-Aliase). Diese Funktion wird benötigt, um auf einer Netzwerkkarte mehrere logische Netzwerke zu verwalten. Sie kann auch im Zusammenhang mit der Funktion NAT (Network Address Translation) notwendig sein, um der Appliance zusätzliche Adressen zuzuweisen.

Um zusätzliche Adressen auf einer Netzwerkkarte zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Zusätzliche Adressen* auf *Neue zusätzliche Adresse*.**

Das Dialogfenster *Neue zusätzliche Adresse erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Name: Geben Sie einen aussagekräftigen Name für die neue zusätzliche Adresse ein.

Auf Schnittstelle: Wählen Sie im Auswahlménü die Netzwerkkarte aus, der die Adresse zugewiesen werden soll.

Adresse: Tragen Sie die zusätzliche IP-Adresse für die Schnittstelle ein.

Netzmaske: Wählen Sie eine Netzwerkmaske aus.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die Schnittstelle hinzu.

3. **Klicken Sie *Speichern*.**

Nach der erfolgreichen Prüfung erscheint die neue zusätzliche Adresse in der Liste. Die zusätzliche Adresse ist noch ausgeschaltet (Statusampel zeigt Rot).

4. **Aktivieren Sie die zusätzliche Adresse.**

Aktivieren Sie die zusätzliche Adresse durch einen Klick auf die Statusampel.

Die zusätzliche Adresse ist nun eingeschaltet (Statusampel zeigt Grün). Zu Beginn wird die Meldung *Down* angezeigt. Das System benötigt kurze Zeit, um die neue zusätzliche Adresse zu konfigurieren und die Einstellungen zu laden. Die neue zusätzliche Adresse ist in Betrieb, wenn die Meldung *Up* erscheint.

Um eine zusätzliche Adresse zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Linkbündelung

Linkbündelung (engl. Link Aggregation) (auch *Kanalbündelung port trunking* oder *NIC bonding*) fasst mehrere parallele Ethernet-Verbindungen zu einer logischen Verbindung mit einer IP-Adresse zusammen. Auf diese Weise lässt sich mit einfachen Mitteln die Bandbreite und somit die Datenrate vervielfachen. Fällt eine physikalische Verbindung aus, verläuft der Datenverkehr automatisch auf den restlichen Leitungen weiter. Ein solches Failover ist für das System, das diese Verbindung benutzt, völlig transparent.

Hinweis – Bei einer Hochverfügbarkeitsumgebung können die einzelnen Ethernet-Ports einer Linkbündelungsgruppe sogar auf verschiedenen HA-Einheiten enthalten sein.

Auf der Appliance können bis zu vier verschiedene Linkbündelungsgruppen (LAG) konfiguriert werden, wobei einer Gruppe bis zu vier Ethernet-Netzwerkkarten zugeteilt werden können. Zur Konfiguration einer Linkbündelungsgruppe benötigen Sie mindestens zwei freie Netzwerkkarten, wobei eine davon unkonfiguriert sein muss.

Um eine Linkbündelungsgruppe (LAG) zu konfigurieren, gehen Sie folgendermaßen vor:

1. Wählen Sie für jede LAG eine konfigurierte Netzwerkkarte aus.

Wählen Sie im Auswahlmenü *Schnittstelle umwandeln* der entsprechenden Gruppe #1 bis #4 die Schnittstelle aus, die in eine Linkbündelungsgruppe (LAG) konvertiert werden soll.

2. Wählen Sie für jede LAG eine weitere Netzwerkkarte aus.

Markieren Sie das entsprechende Auswahlkästchen einer unkonfigurierten Netzwerkkarte aus, um diese zur LAG hinzuzufügen.

3. Aktivieren Sie die LAG.

Aktivieren Sie die LAG durch einen Klick auf die Schaltfläche *Diese Gruppe aktivieren*.

Anschließend wird die LAG geladen und auf der Registerkarte *Netzwerk* >> *Schnittstellen* angezeigt (z. B. lag0). Mit einer LAG können die folgenden Schnittstellen-Typen konfiguriert werden:

- Ethernet-Standard
- Ethernet-VLAN
- Kabelmodem (DHCP)
- Alias-Schnittstellen

Um eine LAG auszuschalten, wählen Sie die entsprechende Schnittstelle ab, indem Sie das zugehörige Auswahlkästchen anklicken, und klicken Sie danach *Diese Gruppe aktualisieren*. Der aktuelle Status der aktiven Linkbündelungsgruppen wird auf der Registerkarte *Support* >> *Erweitert* >> *Schnittstellen-Tabelle* angezeigt.

Uplink-Ausgleich

Mit der Uplink-Ausgleich-Funktion können Sie mehrere Internetverbindungen zusammenfassen, entweder um Zusatzverbindungen bei einem Ausfall zu haben oder um die Last auf mehrere Verbindungen zu verteilen. Die Kombination von bis zu acht unterschiedlichen Internetverbindungen wird unterstützt.

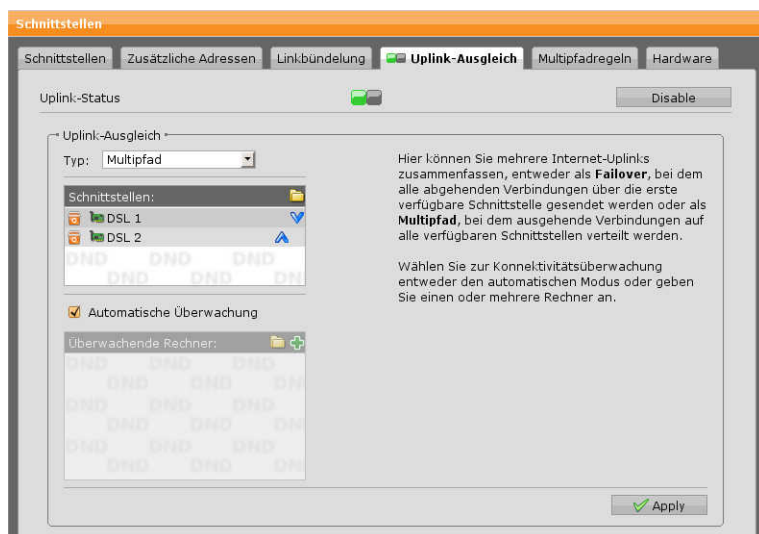


Figure 7.2 Schnittstellen: Konfiguration der Uplink-Ausgleich-Funktion

Um die Uplink-Ausgleich-Funktion zu verwenden, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie den Uplink-Ausgleich.**

Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche.

Die Statusampel wird gelb und der Abschnitt *Uplink-Ausgleich* kann nun bearbeitet werden.

2. **Wählen Sie den Ausgleichstyp.**

Wählen Sie aus der Auswahlliste *Typ* den Ausgleichstyp, den Sie verwenden wollen:

- **Failover:** Zusätzlich zur ersten Internetschnittstelle können ein oder mehrere Backup-Internetverbindungen im Bereitschaftsmodus arbeiten.

Aller Verkehr wird über die erste aktive Schnittstelle gesendet. Im Falle eines Ausfalls wird die Internetverbindungsschnittstelle automatisch zur nächsten verfügbaren Schnittstelle gewechselt.

- **Multipfad:** (Multipath). Alle Schnittstellen arbeiten aktiv, und der Verkehr wird gleichmäßig über alle verfügbaren Schnittstellen verteilt. Im Falle eines Ausfalls wird die entsprechende Schnittstelle ausgeschlos- sen. Die Lastverteilung wird basierend auf der Quell-IP-Adresse durch- geführt und hat eine Beständigkeit von einer Stunde. Wenn das Intervall zwischen zwei Anfragen derselben Quell-IP-Adresse dieses Zeitintervall überschreitet, wird die Lastverteilung neu berechnet. Die Verkehrsver- teilung basiert auf einem einfachen Round-Robin-Algorithmus.
3. **Fügen Sie Schnittstellen hinzu.** Wählen oder fügen Sie Schnittstellen hin- zu, die für den Uplink-Ausgleich verwendet werden sollen.

Hinweis – Die Reihenfolge der Schnittstellen ist wichtig, insbesondere für Failover: Wenn ein Server nicht antwortet, wird die erste darauffolgende Schnittstelle ausgewählt. Sie können die Reihenfolge der Schnittstellen än- dern, indem Sie die blauen Pfeile im Feld *Schnittstellen* verwenden.

4. **Überwachung (optional):**

Automatische Überwachung ist standardmäßig aktiviert, um ein mögliches Versagen einer Schnittstelle zu entdecken. Das bedeutet, dass der Zustand aller Uplink-Ausgleich-Schnittstellen überwacht wird, indem ein zufälliger Rechner im Internet in einem Abstand von 15 Sekunden gepingt wird. Sobald ein Rechner keinen Ping mehr versendet, wird die entsprechende Schnittstelle als tot betrachtet und nicht mehr für die Verteilung verwen- det.

Sie können die Rechner, die vom Server gepingt werden, selbst bestimmen:

1. **Wählen Sie die Option *Automatische Überwachung* ab.**
Das Feld *Überwachende Rechner* wird zur Bearbeitung freigegeben.
 2. **Fügen Sie Rechner hinzu, die gepingt werden sollen.**
Wählen oder fügen Sie einen oder mehrere Rechner hinzu, die anstelle einer zufälligen Auswahl an Rechnern gepingt werden sollen.
5. **Klicken Sie *Übernehmen*.**
Ihre Einstellungen werden gespeichert.

Eine neue virtuelle Schnittstelle namens *Uplink Interfaces* wird automatisch angelegt und steht anderen Funktionen des Astaro Security Gateway zur Verfügung, z. B. IPSec-Regeln. Die virtuelle Netzwerkschnittstelle *Uplink Interfaces* umfasst alle Uplink-Schnittstellen, die der Schnittstellen-Liste hinzugefügt wurden.

Darüber hinaus wird eine neue Netzwerkgruppe namens *Uplink Primary Addresses* automatisch angelegt und steht anderen Funktionen des Astaro Security Gateway zur Verfügung, z. B. Paketfilterregeln. Es verweist auf die ersten Adressen aller *Uplink Interfaces*.

Im Falle des Versagens einer Schnittstelle können offene VPN-Tunnel automatisch über die nächste verfügbare Schnittstelle wiederhergestellt werden, vorausgesetzt, dass DynDNS verwendet wird oder der entfernte Server die IP-Adressen aller Internetschnittstellen akzeptiert. Voraussetzung dafür ist außerdem, dass die IPSec-Regel die *Uplink Interfaces* als *Lokale Schnittstelle* benutzt.

Multipfadregeln

Auf der Registerkarte *Netzwerk >> Schnittstellen >> Multipfadregeln* können Sie Regeln für Multipfad (engl. *Multipath*) angeben, wenn Sie den *Multipfad*-Modus für den Uplink-Ausgleich verwenden.

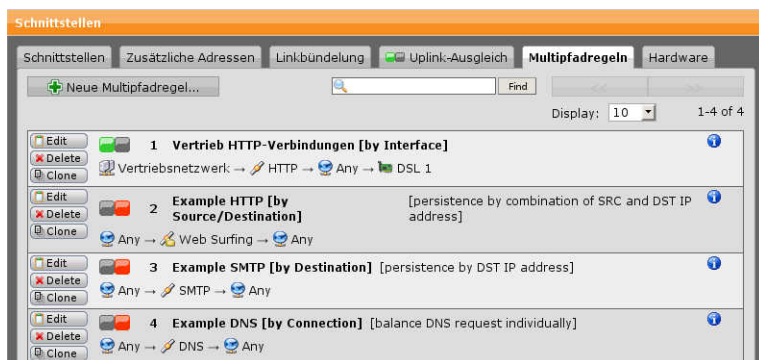


Figure 7.3 Schnittstellen: Multipfad-Regeln

Um eine Multipfadregel zu erstellen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Multipfadregeln* auf *Neue Multipfadregel*.**

Das Dialogfenster *Neue Multipfadregel erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Name: Geben Sie einen aussagekräftigen Name für die Multipfadregel ein.

Quelle: Wählen Sie eine Quell-IP-Adresse oder ein Quellnetzwerk aus, auf die oder das die Regel sich beziehen soll.

Dienst: Wählen Sie einen Netzwerkdienst aus, auf den die Regel sich beziehen soll.

Ziel: Wählen Sie eine Ziel-IP-Adresse oder ein Zielnetzwerk aus, die oder das für das Routen verwendet werden soll.

Schnittst.-Bindung: Die *Schnittstellenbindung* ist eine Methode, die sicherstellt, dass aufeinanderfolgende Verbindungen eines Clients immer über dieselbe Internetschnittstelle (Uplink) geroutet werden. Die Bindung hat eine Zeitbeschränkung von einer Stunde. Sie können bestimmen, was die Basis für die Bindung sein soll:

- **nach Verbindung:** Jede Verbindung wird unabhängig von anderen ausgeglichen.
- **nach Quelle (Standard):** Der Ausgleich erfolgt auf Basis der Quell-IP-Adresse.
- **nach Ziel:** Der Ausgleich erfolgt auf Basis der Ziel-IP-Adresse.
- **nach Quelle/Ziel** Der Ausgleich erfolgt auf Basis der Kombination von Quelle und Ziel.
- **nach Schnittstelle:** Wählen Sie eine Schnittstelle aus der Auswahlliste *BIND-Schnittstelle*. Der Verkehr, für den diese Regel zutrifft, wird über diese Schnittstelle geroutet. Im Falle des Versagens einer Schnittstelle oder wenn keine andere Regel zutrifft, wird für die Verbindung die Standardaktion angewendet.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die Multipfadregel hinzu.

3. **Klicken Sie *Speichern*.**

Die neue Multipfadregel erscheint in der Liste *Multipfadregeln*. Um eine Multipfadregel zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

4. **Aktivieren Sie die Regel.**

Die neue Multipfadregel ist standardmäßig ausgeschaltet. Klicken Sie auf

die Statusampel, um die Regel zu aktivieren.
Die Regel ist nun aktiv (Statusampel zeigt Grün).

Hardware

Auf der Registerkarte *Netzwerk >> Schnittstellen >> Hardware* sind alle konfigurierten Schnittstellen mit den entsprechenden Hardware-Informationen aufgelistet wie z. B. der Ethernet-Betriebsmodus und die MAC-Hardware-Adresse. Für jede Schnittstelle kann die Autonegotiation (engl. etwa *automatisches Aushandeln*) eingeschaltet oder ausgeschaltet werden.

Autonegotiation: Gewöhnlich wird der Ethernet-Betriebsmodus (10BaseT Full Duplex, 10BaseT Half Duplex usw.) zwischen zwei Netzwerkgeräte automatisch ausgehandelt, indem der beste Betriebsmodus gewählt wird, der von beiden Geräten unterstützt wird. Dabei wird eine höhere Geschwindigkeit (100 Mbit/s) vor niedrigerer Geschwindigkeit (10 Mbit/s) bevorzugt, und Full-Duplex wird Half-Duplex bei gleicher Geschwindigkeit vorgezogen.

Autonegotiation ist automatisch eingeschaltet bei Netzwerkkarten, deren Treiber die manuelle Auswahl einer Ethernet-Betriebsart nicht unterstützt oder für die die entsprechende Einstellung nicht bestimmt werden kann.

Um die Einstellung für Autonegotiation zu ändern, klicken Sie auf die Schaltfläche *Edit* der entsprechenden Netzwerkkarte und ändern Sie die Einstellung in dem erscheinenden Dialogfenster *NIC-Parameter bearbeiten*.

Warnung – Seien Sie vorsichtig, wenn Sie die Einstellung für *Autonegotiation* ändern, da die Leistung dieser Verbindung eingeschränkt oder sogar unterbrochen werden kann. Falls es sich bei der Netzwerkkarte um die Administrationschnittstelle handelt, wäre in diesem Fall kein Zugriff auf die Benutzeroberfläche mehr möglich!

Bridging

Das Bridging (engl. von „Brücke“) ist eine Methode zur Weiterleitung von Datenpaketen und wird hauptsächlich in Ethernet-Netzwerken eingesetzt. Im Gegensatz zum Routing trifft Bridging keine Annahmen darüber, wo sich in einem Netzwerk eine bestimmte Adresse befindet. Stattdessen benutzt es Broadcast um unbekannte Geräte zu lokalisieren.

Durch Bridging können zwei oder auch mehrere gleichartige Netzwerke oder Netzwerksegmente miteinander verbunden werden. Dabei werden die Datenpakete mittels Bridging-Tabellen weitergeleitet, welche MAC-Adressen einem Bridge-Port zuordnen. Die entstehende Bridge übermittelt den Verkehr dann transparent durch die Bridging-Schnittstellen.

Hinweis – Diese Art von Verkehr muss explizit durch entsprechende Paketfilterregeln erlaubt werden.

Status

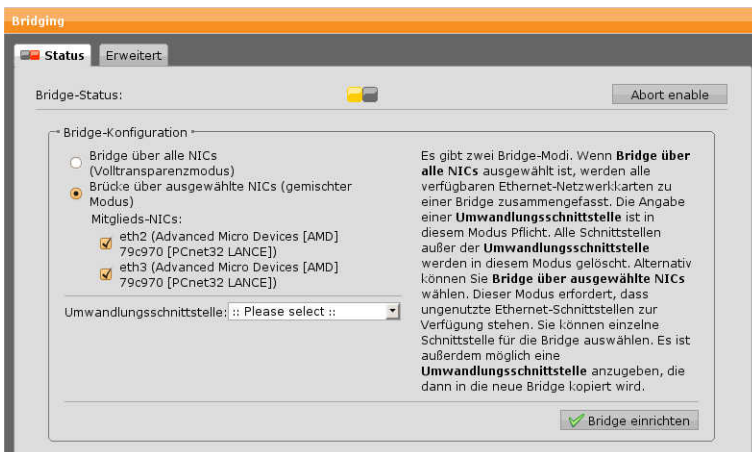


Figure 7.4 Bridging: Konfiguration einer Bridge

Um eine Bridge zu konfigurieren, gehen Sie folgendermaßen vor:

1. Aktivieren Sie Bridging.

Klicken Sie auf der Registerkarte *Netzwerk* >> *Bridging* >> *Status* entweder auf die Statusampel oder auf die Schaltfläche *Enable*.

Die Statusampel wird gelb und der Abschnitt *Bridge-Konfiguration* kann nun bearbeitet werden.

2. Wählen Sie die Bridging-Methode aus.

- **Bridge über alle NICs:** Bei dieser Methode werden alle konfigurierten Netzwerkkarten zu einer einzigen Bridge-Schnittstelle zusammengefasst. Die Angabe eines *Convert Interface* ist Pflicht. Alle Schnittstellen außer der konvertierten Schnittstelle werden bei dieser Methode gelöscht.
- **Bridge über ausgewählte NICs:** Bei dieser Methode können die Netzwerkkarten für die Bridge individuell zusammengestellt werden. Hierfür werden mindestens zwei unkonfigurierte Netzwerkkarten benötigt. Wählen Sie eine oder mehrere Netzwerkkarten aus, die Teil der Bridge werden sollen. Es ist überdies möglich, eine Umwandlungsschnittstelle zu bestimmen, d. h. eine Schnittstelle, die umgewandelt und die auf die neue Bridge kopiert wird.

3. Wählen Sie die Netzwerkkarten für die Bridge aus.

Für das Bridging kann nur eine bereits konfigurierte Netzwerkkarte ausgewählt werden. Die Bridge wird anschließend alle auf dieser Netzwerkkarte definierten Adresseinstellungen, sowie Alias-Adressen und VLAN-Einstellungen übernehmen.

4. Klicken Sie *Bridge einrichten*.

Die Netzwerkkarten werden nun zusammengefasst und die Bridge wird geladen (Statusampel zeigt Grün).

Um die Konfiguration abzubrechen, klicken Sie auf die Schaltfläche *Abort Enable* oder auf die gelbe Statusampel.

Sobald die Bridge konfiguriert ist, erscheint die umgewandelte Schnittstelle als ein Bridge-Gerät mit der SysID br0 auf der Registerkarte *Netzwerk >> Schnittstellen*. Alle Schnittstellen, die Teil der Bridge sind, werden im Abschnitt *Bridge-Konfiguration* angezeigt. Um eine Schnittstelle wieder aus der Bridge zu entfernen, wählen Sie die entsprechende Option ab und klicken Sie *Bridge aktualisieren*.

Um eine Bridge zu entfernen, gehen Sie folgendermaßen vor:

1. Klicken Sie auf der Registerkarte *Status auf Disable*.

Die Statusampel zeigt Gelb.

2. Klicken Sie auf die Schaltfläche *Entfernen der Bridge bestätigen*.

Die Statusampel zeigt Rot. Die Bridge wurde nun erfolgreich entfernt.

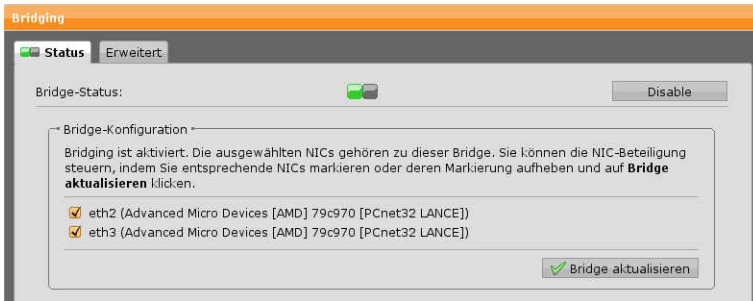


Figure 7.5 Bridging: Aktiviertes Bridging

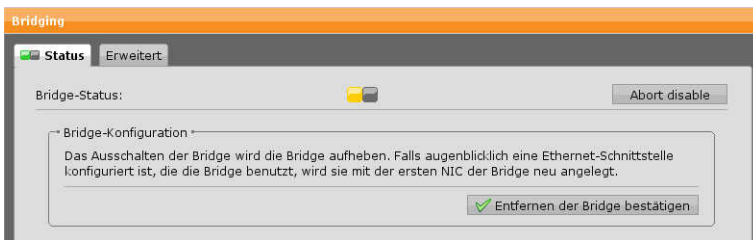


Figure 7.6 Bridging: Entfernen einer Bridge

Erweitert

Auf der Registerkarte *Netzwerk* >> *Bridging* >> *Erweitert* befinden sich die erweiterten Einstellungen zu Bridging.

ARP-Broadcasts zulassen: Mit dieser Funktion können Sie bestimmen, ob eingehende ARP-Broadcasts von der Bridge weitergeleitet werden. Im eingeschalteten Zustand erlaubt die Bridge Anfragen an die MAC-Zieladresse FF:FF:FF:FF:FF:FF. Dies kann eventuell von mutmaßlichen Angreifern genutzt werden, um Informationen über die Netzwerkkarten im entsprechenden Netzwerksegment oder sogar auf dem Gerät selbst zu sammeln. Im voreingestellten Zustand ist die Funktion *ARP-Broadcasts zulassen* daher ausgeschaltet.

Ablaufzeit: In diesem Eingabefeld stellen Sie ein, nach welcher Zeitspanne eine inaktive MAC-Adresse gelöscht wird. Die Funktion ist auf 300 Sekunden voreingestellt.

IPv6-Durchleitung zulassen: Aktivieren Sie diese Option, um die Durchleitung von IPv6-Verkehr über die Bridge ohne Kontrolle zuzulassen.

Statisches Routing

Jeder an ein Netzwerk angeschlossener Computer verwendet eine Routing-Tabelle, mit deren Hilfe er feststellt, welchen Weg ein ausgehendes Datenpaket nehmen muss, um sein Ziel zu erreichen. Die Routing-Tabelle enthält z. B. Informationen darüber, ob eine sich Zieladresse im lokalen Netzwerk befindet oder ob das Datenpaket über einen Router weitergeleitet werden muss. Falls ein Router beteiligt ist, enthält die Tabelle die Information, welcher Router für welches Netzwerk benutzt werden muss.

Astaro Security Gateway unterstützt zwei Routing-Arten: *Statische Routen* und *Richtlinienrouten*. Bei statischen Routen werden die Routingziele lediglich von der Zieladresse der Datenpakete bestimmt. Bei Richtlinienrouten ist es möglich, das Routing anhand der Absenderschnittstelle, der Absenderadresse, dem Dienst oder der Zieladresse zu bestimmen.

Hinweis – Sie brauchen für Netzwerke, die direkt an die Schnittstellen der Firewall angeschlossen sind, ebenso für Standardrouten, keine Routing-Einträge anzulegen. Diese Routing-Einträge werden vom System automatisch erstellt.

Statische Routen

Für die direkt angeschlossenen Netzwerke trägt das System die entsprechenden Routing-Einträge selbst ein. Weitere Einträge müssen manuell vorgenommen werden. Dies ist z. B. der Fall, wenn im lokalen Netzwerk ein weiterer Router existiert, über den ein bestimmtes Netzwerk erreicht werden soll. Routen für Netzwerke, die nicht direkt angeschlossen sind, aber über einen Befehl oder eine Konfigurationsdatei in die Routing-Tabelle eingetragen werden, bezeichnet man als statische Routen.

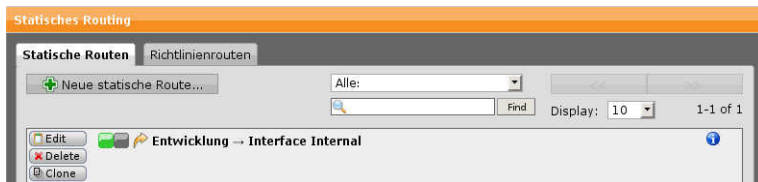


Figure 7.7 Statisches Routing: Tabelle der statischen Routen

Um eine statische Route hinzufügen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf die Schaltfläche *Neue statische Route*.**

Das Dialogfenster *Neue statische Route erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Routentyp: Die folgenden Routentypen stehen zur Verfügung:

- **Schnittstellen-Route:** Datenpakete werden an eine bestimmte Schnittstelle geschickt. Dieser Typ kann bei zwei Szenarien genutzt werden: Für Routing-Einträge zu dynamischen Schnittstellen (z. B. PPP), da in diesem Fall die IP-Adresse des Gateway nicht bekannt ist, oder für eine Standard-Route mit einem Gateway außerhalb der direkt angeschlossenen Netzwerke.
- **Gateway-Route:** Die Datenpakete werden an einen bestimmten Rechner (Gateway) geschickt.
- **Blackhole-Route:** Die Datenpakete werden verworfen, das heißt es werden keine ICMP-Nachrichten an den Absender geschickt. Bei Verbindungen mit dynamischen Routing-Protokollen (z. B. OSPF) können dadurch unter Anderem „Routing Loops“ (Schleifen) oder „Route Flapping“ („Flattern“, schnelles Wechseln von Routen) verhindert werden.

Netzwerk: Wählen Sie die Zielnetzwerke der Datenpakete, die die Firewall auffangen soll.

Schnittstelle: Wählen Sie die Schnittstelle, durch die die Datenpakete die Firewall verlassen (nur verfügbar, wenn Sie *Schnittstellen-Route* als Routentyp gewählt haben).

Gateway: Wählen Sie das Gateway/den Router aus, an das oder den die Firewall die Datenpakete weiterleiten soll (nur verfügbar, wenn Sie *Gateway-Route* als Routentyp gewählt haben).

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die Route hinzu.

3. **Klicken Sie *Speichern*.**

Die neue Route erscheint in der Liste *Statische Routen*.

4. **Aktivieren Sie die Route.**

Klicken Sie auf die Statusampel, um die Route zu aktivieren.

Um eine Route zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Richtlinienrouten

Normalerweise entscheidet ein Router darüber, wohin ein bestimmtes Paket geschickt werden muss, indem er die Zieladresse im Paket selbst ausliest und den entsprechenden Eintrag in einer Routing-Tabelle nachschaut. Manchmal jedoch ist es notwendig ein Paket basierend auf anderen Kriterien weiterzuleiten. Das richtlinienbasierte Routing ermöglicht die Weiterleitung bzw. das Routen von Datenpaketen nach eigenen Sicherheitsrichtlinien.

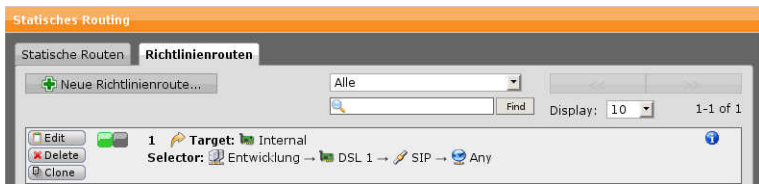


Figure 7.8 Statisches Routing: Tabelle der Richtlinienrouten

Um eine Richtlinienroute hinzuzufügen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf die Schaltfläche *Neue Richtlinienroute*.**

Das Dialogfenster *Neue Richtlinienroute erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Position: Die Positionsnummer, die die Priorität der Richtlinienroute festlegt. Niedrigere Nummern haben eine höhere Priorität. Routen werden in aufsteigender Reihenfolge abgeglichen. Wenn eine Route zutrifft, werden Routen mit einer höheren Nummer nicht mehr abgeglichen.

Routentyp: Die folgenden *Routentypen* stehen zur Verfügung:

- **Schnittstellen-Route:** Datenpakete werden an eine bestimmte Schnittstelle geschickt. Dieser Typ kann bei zwei Szenarien genutzt werden: Für Routing-Einträge zu dynamischen Schnittstellen (z. B. PPP), da in diesem Fall die IP-Adresse des Gateway nicht bekannt ist, oder für eine Standard-Route mit einem Gateway außerhalb der direkt angeschlossenen Netzwerke.
- **Gateway-Route:** Die Datenpakete werden an einen bestimmten Rechner (Gateway) geschickt.

Quellschnittstelle: Die Schnittstelle, auf der das zu routende Datenpaket ankommt. Mit der Einstellung *Any* werden alle Schnittstellen geprüft.

Quellnetzwerk: Das Quellnetzwerk des zu routenden Datenpakets. Mit der Einstellung *Any* werden alle Netzwerke geprüft.

Dienst: Datenpakete dieses Diensts werden auf passende Route-Regeln geprüft. Die Auswahlhilfe enthält sowohl die vordefinierten als auch Ihre selbst definierten Dienste. Mit Hilfe dieser Dienste lässt sich präzise definieren, welche Art von Datenverkehr verarbeitet werden soll. Die Einstellung *Any* steht hier für alle Kombinationen aus Protokollen und Quell- bzw. Zielports.

Zielnetzwerk: Das Zielnetzwerk des zu routenden Datenpakets. Mit der Einstellung *Any* werden alle Netzwerke geprüft.

Zielschnittstelle: Die Schnittstelle, an die die Datenpakete gesendet werden (nur verfügbar, wenn Sie als Routentyp *Schnittstellen-Route* gewählt haben).

Gateway: Wählen Sie das Gateway/den Router aus, an das oder den die Firewall die Datenpakete weiterleiten soll (nur verfügbar, wenn Sie *Gateway-Route* als Routentyp gewählt haben).

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die Route hinzu.

3. Klicken Sie **Speichern**.

Die neue Route erscheint in der Liste *Statische Routen*.

4. Aktivieren Sie die Route.

Klicken Sie auf die Statusampel, um die Route zu aktivieren.

Um eine Route zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Dynamisches Routing (OSPF)

Das Protokoll *Open Shortest Path First* (OSPF) ist ein dynamisches Link-State-Routing-Protokoll, das hauptsächlich innerhalb von großen autonomen Systemnetzwerken genutzt wird. Astaro Security Gateway unterstützt OSPF Version 2. Im Gegensatz zu anderen Protokollen, nutzt OSPF die Kosten für die Pfade als Routing-Metrik. Die Kosten für die Übermittlung von Datenpaketen über eine Schnittstelle mit eingeschaltetem OSPF wird aus der verfügbaren Bandbreite berechnet. Dabei sind die Kosten umgekehrt proportional zu der verfügbaren Bandbreite der Schnittstelle – eine größere Bandbreite hat somit geringere Kosten zur Folge. Die Kosten und die entstehende Zeitverzögerung sind z. B. bei einer seriellen Schnittstelle mit 56 Kbit/s höher als bei einer Ethernet-Schnittstelle mit 10 Mbit/s.

Die OSPF-Spezifikation enthält keine Angaben darüber, wie die Kosten für ein angeschlossenes Netzwerk berechnet werden – dies wird dem Anbieter überlassen. Daher können Sie eine eigene Berechnungsformel für die Kosten definieren. Wenn das OSPF-Netzwerk jedoch an ein anderes Netzwerk angrenzt, bei dem bereits eine Formel definiert wurde, muss diese hier ebenfalls als Basis für die Kostenberechnung verwendet werden.

Die Kosten werden standardmäßig bandbreitenbasiert berechnet. Cisco z. B. verwendet für die Kostenberechnung die folgende Formel: 10^8 dividiert durch die Bandbreite in Bits pro Sekunde. Mit dieser Formel kostet es $10^8/10\,000\,000 = 10$, um eine 10-Mbit/s-Ethernet-Schnittstelle zu benutzen, und $10^8/1\,544\,000 = 64$, um eine 1,544 Mbit/s-Schnittstelle (T1) zu benutzen (ungerade Ergebnisse werden auf einen geraden Wert abgerundet).

Allgemein

Auf der Registerkarte *Netzwerk >> Dynamisches Routing (OSPF) >> Allgemein* werden die Grundeinstellungen durchgeführt. Bevor die Registerkarte *Allgemein* aktiviert werden kann, muss auf der Registerkarte *Bereich* mindestens eine OSPF-Bereich (engl. *OSPF Area*) konfiguriert sein.

Warnung – Die Einstellungen für die OSPF-Funktion sollten nur von einem technisch erfahrenen Administrator durchgeführt werden, der mit dem Protokoll OSPF vertraut ist. Die Konfigurationsanleitung in diesem Kapitel umfasst nicht genügend Aspekte von OSPF, um ein vollständiges Verständnis des OSPF-Protokolls zu erreichen. Verwenden Sie diese Funktion deshalb mit Vorsicht, da eine fehlerhafte Konfiguration das Netzwerk betriebsunfähig machen kann.



Figure 7.9 OSPF: Konfiguration von OSPF

Um OSPF zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Konfigurieren Sie auf der Registerkarte *Bereich* mindestens einen OSPF-Bereich.**
2. **Aktivieren Sie OSPF auf der Registerkarte *Allgemein*.**
 Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche.
 Die Statusampel wird gelb und der Abschnitt *Router* kann nun bearbeitet werden.
3. **Geben Sie die Router-ID ein.**
 Tragen Sie eine eindeutige ID ein, über die sich Astaro Security Gateway gegenüber den anderen OSPF-Routern identifiziert.
4. **Klicken Sie *Übernehmen*.**
 Ihre Einstellungen werden gespeichert.

Um die OSPF-Funktion auszuschalten, klicken Sie auf Statusampel oder *Disable*.

Schnittstellen

Auf der Registerkarte *Netzwerk* > > *Dynamisches Routing (OSPF)* > > *Schnittstellen* werden die Schnittstellen konfiguriert, die innerhalb eines OSPF-Bereichs genutzt werden sollen. Jede Definition enthält verschiedene Parameter, die spezifisch für OSPF-Schnittstellen sind.

Um eine OSPF-Schnittstelle zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Schnittstellen* auf *Neue OSPF-Schnittstelle*.**
 Das Dialogfenster *Neue OSPF-Schnittstelle erstellen* wird geöffnet.
2. **Nehmen Sie die folgenden Einstellungen vor:**
Name: Geben Sie einen aussagekräftigen Name für die Schnittstelle ein.
Schnittstelle: Wählen Sie die Schnittstelle aus, die zum OSPF-Bereich hinzugefügt werden soll.
Auth.-Art: Wählen Sie für alle OSPF-Pakete, die über diese Schnittstelle gesendet und empfangen werden, die Authentifizierungsmethode aus.
 Die folgenden Authentifizierungsmethoden stehen zur Verfügung:

- **MD5:** MD5-Authentifizierung. MD5 (Message-Digest Algorithm 5) ist eine weit verbreitete kryptografische Hash-Funktion, die einen 128-Bit-Hashwert benutzt.
- **Klartext:** Klartext-Authentifizierung. Tragen Sie das Kennwort in das Eingabefeld *Auth.-Schlüssel* ein. Das Kennwort wird als Klartext durch das Netzwerk geschickt.
- **Aus:** Es erfolgt keine Authentifizierung.

Prüfsumme: Wählen Sie die Prüfsumme (MD, von engl. *message digest*), um die MD5-Authentifizierung für OSPF festzulegen. Beachten Sie, dass für die MD5-Authentifizierung auf der Registerkarte *Prüfsummen* zuerst ein Schlüssel erzeugt werden muss.

Kosten: Der Kosten-Faktor für die Übermittlung der Datenpakete über diese Schnittstelle. Ein gültiger Wert liegt im Bereich 1 bis 65535.

Erweiterte Optionen (optional): Durch die Auswahl der Option *Erweiterte Optionen* werden weitere Konfigurationsoptionen angezeigt:

- **Grußpaketintervall:** Legen Sie das Zeitintervall fest (in Sekunden), das Astaro Security Gateway wartet, bevor es Grußpakete (engl. *Hello packets*) über die Schnittstelle sendet. Es ist ein Zeitintervall von zehn Sekunden voreingestellt.
- **Wiederübertragungsint.:** (Wiederübertragungsintervall) Legen Sie das Zeitintervall (in Sekunden) fest, nach dem ein LSA (engl. *link state advertisement*) für die Schnittstelle nochmals übertragen wird, wenn keine Bestätigung eingegangen ist. Es ist ein Zeitintervall von fünf Sekunden voreingestellt.
- **Totes Intervall:** Legen Sie das Zeitintervall (in Sekunden) fest, die Astaro Security Gateway auf Grußpakete wartet, die über die Schnittstelle eintreffen. Es ist ein Zeitintervall von 40 Sekunden voreingestellt. Der Wert sollte grundsätzlich vier mal größer sein als der Wert des *Grußpaketintervalls*.
- **Priorität:** Legen Sie die Router-Priorität fest, bei der es sich um eine 8-Bit-Nummer von 1 bis 255 handelt, die hauptsächlich dafür genutzt wird, um in einem Netzwerk den designierten Router (DR) (engl. *Designated Router*) zu bestimmen. Der Standardwert ist 1.
- **Übertragungsverzögerung:** Legen Sie das geschätzte Zeitintervall (in Sekunden) fest, das benötigt wird, um ein Link-State-Update-Paket über die Schnittstelle zu senden. Ein gültiger Wert liegt im Bereich 1 bis

65535; das Zeitintervall 1 ist voreingestellt.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die OSPF-Schnittstelle hinzu.

3. Klicken Sie *Speichern*.

Anschließend wird die neue OSPF-Schnittstelle in der Liste *Schnittstellen* angezeigt.

Um eine OSPF-Schnittstelle zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Live-Protokoll öffnen: Im OSPF-Live-Protokoll werden die Aktivitäten auf der OSPF-Schnittstelle protokolliert. Durch einen Klick auf die Schaltfläche wird das Live-Protokoll in einem neuen Fenster geöffnet.

Bereich

Ein OSPF-Netzwerk ist in Bereiche unterteilt. Dies sind logische Gruppierungen von Routern, deren Informationen für das restliche Netzwerk zusammengefasst werden können. Die einzelnen Bereiche werden durch eine 32-Bit-ID in der Punkt-Dezimalschreibweise festgelegt – ähnlich der Schreibweise bei IP-Adressen.

Es gibt insgesamt sechs OSPF-Bereichstypen:

- **Backbone:** Die Bereich mit der ID 0 (oder 0.0.0.0) ist für das Backbone-Netzwerk des OSPF-Netzwerks reserviert, welches das Kernnetz eines OSPF-Netzwerks bildet – alle anderen Bereiche sind damit verbunden.
- **Normal:** Eine normaler oder regulärer Bereich (engl. *Regular Area*) erhält eine eindeutige ID im Bereich 1 (oder 0.0.0.1) bis 4.294.967.295 (oder 255.255.255.255). In normalen Bereichen werden die Datenpakete von externen Routen bidirektional durch den Area Border Router (ABR) (dt. Grenzrouter) geflutet (engl. *Flooding*). Beachten Sie, dass externe Routen als Routen definiert werden, die im OSPF von einem anderen Routing-Protokoll verteilt werden.
- **Stub:** Ein Stub-Bereich (Stub-Bereich) hat üblicherweise keine direkte Verbindung zu irgendeinem externen Netzwerk. Es ist unnötig externe Routen in eine Stub-Bereich einzuspeisen, da der gesamte Datenverkehr zu einem externen Netzwerk durch einen Area Border Router (ABR) geleitet werden muss. Daher ersetzt der Stub-Bereich eine vorgegebene Route durch externe Routen, um Daten an externe Netzwerke zu senden.

- **Stub No-Summary:** Dieser Bereich (auch *Totally-Stubby-Area*) ist vergleichbar mit dem Stub-Bereich, allerdings werden keine sogenannten *Summary Routes* erlaubt. Das bedeutet, dass die Flutung von Summary-Link-State-Advertismments (LSAs) des Typs 3 in dem Bereich damit eingeschränkt wird.
- **NSSA:** Dieser Bereich (*Not-So-Stubby-Area*) ist vergleichbar mit dem Stub-Bereich, allerdings können auch externe Verbindungen unterstützt werden. Beachten Sie dabei, dass keine virtuellen Links unterstützt werden.
- **NSSA No-Summary:** Dieser Bereich (*NSSA No-Summary-Area*) ist vergleichbar mit NSSA, allerdings werden keine sogenannten *Summary Routes* erlaubt. Das bedeutet, dass die Flutung von Summary-Link-State-Advertismments (LSAs) des Typs 3 in dem Bereich damit eingeschränkt wird.

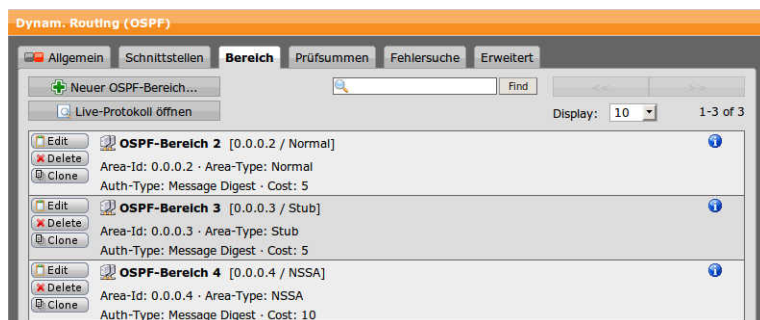


Figure 7.10 OSPF: Übersicht mit konfigurierten Bereichen

Um einen OSPF-Bereich zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Bereich* auf *Neuer OSPF-Bereich*.**
Das Dialogfenster *Neuen OSPF-Bereich erstellen* wird geöffnet.
2. **Nehmen Sie die folgenden Einstellungen vor:**
 - Name:** Geben Sie einen aussagekräftigen Name für den Bereich ein.
 - Bereichs-ID:** Tragen Sie die ID für die Bereich in der Punkt-Dezimalschreibweise ein (z. B. 0.0.0.1).
 - Bereichstyp:** Wählen Sie einen Bereichstyp aus.
Die Beschreibungen der verschiedenen OSPF-Bereiche befinden sich in der Einleitung.
 - Auth.-Art:** Wählen Sie für die Pakete, die über die Schnittstelle die OSPF-Bereich erreichen, die Authentifizierungsmethode aus.
Die folgenden Authentifizierungsmethoden stehen zur Verfügung:

- **MD5:** MD5-Authentifizierung. MD5 (Message-Digest Algorithm 5) ist eine weit verbreitete kryptografische Hash-Funktion, die einen 128-Bit-Hashwert benutzt.
- **Klartext:** Klartext-Authentifizierung. Tragen Sie das Kennwort in das Eingabefeld *Auth.-Schlüssel* ein. Das Kennwort wird als Klartext durch das Netzwerk geschickt.
- **Aus:** Es erfolgt keine Authentifizierung.

Verbinden über Schnittstelle: Wählen Sie für den Bereich eine OSPF-Schnittstelle aus. Im Feld *Verbinden über Schnittstelle* werden nur OSPF-Schnittstellen angezeigt, die zuvor auf der Registerkarte *Netzwerk >> Dynamisches Routing (OSPF) >> Schnittstellen* konfiguriert wurden.

Virtuelle Links verbinden: Alle Bereiche in einem autonomen OSPF-System (AS) müssen physikalisch mit dem Backbone-Bereich verbunden sein. In manchen Fällen ist eine physikalische Verbindung nicht möglich. In diesem Fall können Sie einen virtuellen Link verwenden, um den Backbone-Bereich mit einem Nicht-Backbone-Bereich zu verbinden. Tragen Sie in das Feld *Virtuelle Link verbinden* die Router-ID, die dem virtuellen Link-Nachbarn zugeordnet ist, in der Punkt-Dezimalschreibweise ein (z. B. 10.0.0.8).

Kosten: Der Kosten-Faktor für das Senden und Empfangen von Datenpaketen in diesem Bereich. Ein gültiger Wert liegt im Bereich 1 bis 65535.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über den OSPF-Bereich hinzu.

3. Klicken Sie *Speichern*.

Anschließend wird der neue OSPF-Bereich in der Liste *Bereich* angezeigt.

Um eine OSPF-Schnittstelle zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Live-Protokoll öffnen: Im OSPF-Live-Protokoll werden die Aktivitäten auf der OSPF-Schnittstelle protokolliert. Durch einen Klick auf die Schaltfläche wird das Live-Protokoll in einem neuen Fenster geöffnet.

Prüfsummen

Auf der Registerkarte *Netzwerk >> Dynamisches Routing (OSPF) >> Prüfsummen* werden die Prüfsummenschlüssel generiert. Prüfsummenschlüssel werden benötigt, um MD5-Authentifizierung mit OSPF zu ermöglichen. Die MD5-Authentifizierung nutzt das Kennwort um eine Prüfsumme zu generieren.

Dabei handelt es sich um eine 128-Bit-Prüfsumme aus dem Datenpaket und dem Kennwort. Die Prüfsumme wird mit dem Datenpaket und einer Schlüssel-ID verschickt. Die Schlüssel-ID ist dem Kennwort zugeordnet.

Hinweis – Auf allen empfangenden Routern muss derselbe Prüfsummenschlüssel konfiguriert sein.

Um einen Prüfsummenschlüssel zu generieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Prüfsummen* auf *Neuer Prüfsummenschlüssel*.**

Das Dialogfenster *Neuen Prüfsummenschlüssel erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

ID: Tragen Sie die Schlüssel-Identifikationsnummer für diesen Prüfsummenschlüssel ein. Ein gültiger Wert liegt im Bereich 1 bis 255.

MD5-Schlüssel: Tragen Sie das Kennwort ein. Es kann bis zu 16 alphanumerische Zeichen enthalten.

3. **Klicken Sie *Speichern*.**

Anschließend wird der neue Schlüssel in der Liste *Prüfsummen* angezeigt.

Um einen Schlüssel zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Fehlersuche

Auf der Registerkarte *Netzwerk >> Dynamisches Routing (OSPF) >> Fehlersuche* werden detaillierte Informationen zu den relevanten OSPF-Parametern in separaten Browser-Fenstern dargestellt. Die folgenden Informationen werden dargestellt:

- **IP des OSPF-Nachbarn anzeigen:** Es werden zu den OSPF-Nachbarn schnittstellenbezogene Informationen angezeigt.
- **IP der OSPF-Routen anzeigen:** Es wird der aktuelle Stand der Routing-Tabelle angezeigt.
- **IP der OSPF-Schnittstelle anzeigen:** Es werden OSPF-bezogene Schnittstelleninformationen angezeigt.

- **IP der OSPF-Datenbank anzeigen:** Es werden zu einem bestimmten Router OSPF-datenbankbezogene Informationen angezeigt.
- **IP der OSPF-Grenzrouter anzeigen:** Es werden die internen Einträge aus der OSPF-Routing-Tabelle zum *Area Border Router* (ABR) und zum *Autonomous System Boundary Router* (ASBR) angezeigt.

Erweitert

Auf der Registerkarte *Netzwerk >> Dynamisches Routing (OSPF) >> Erweitert* befinden sich die erweiterten Einstellungen. Die Funktionen beziehen sich dabei auf die Einspeisung (Neuverteilung) von Routing-Informationen von einer Nicht-OSPF-Domäne zu der OSPF-Domäne.

Hinweis – Richtlinienrouten können nicht neu verteilt werden.

Verbundene neuverteilen: Um die Routen von direkt verbundenen Netzwerken neu zu verteilen, wählen Sie diese Option aus. Der Metrikwert (Kostenfaktor) 10 ist voreingestellt.

Statische neuverteilen: Um die statischen Routen neu zu verteilen, wählen Sie diese Option aus. Der Metrikwert (Kostenfaktor) 10 ist voreingestellt.

Standardroute bekanntgeben: Um eine vorgegebene Route zur OSPF-Domäne neu zu verteilen, wählen Sie diese Option aus.

Hinweis – Eine vorgegebene Route wird in der OSPF-Domäne angezeigt, ungeachtet dessen, ob sie eine Route zu 0.0.0.0/0 enthält.

Dienstqualität (QoS)

Im Allgemeinen bezeichnet *Dienstqualität* (QoS, engl. *Quality of Service*) Kontrollmechanismen, die dafür sorgen, dass ausgewählter Netzwerkverkehr bevorzugt behandelt wird. Im Besonderen heißt das, dass diesem eine Mindestbandbreite zugesichert wird. Bei Astaro Security Gateway wird zu priorisierender Verkehr im Menü *Netzwerk >> Dienstqualität* konfiguriert. Hier können Sie für bestimmte Arten von ausgehendem Verkehr, der zwei Punkte im Netzwerk passiert, eine garantierte Bandbreite reservieren. Dahingegen wird die Optimierung von Kapazitäten (engl. *traffic shaping*) für eingehenden Verkehr

intern durch verschiedene Techniken umgesetzt, z. B. durch *Stochastic Fairness Queuing* (SFQ) oder *Random Early Detection* (RED).

Status

Auf der Registerkarte *Netzwerk* >> *Dienstqualität* >> *Status* sind die Netzwerkkarten aufgelistet für die QoS konfiguriert werden kann. Standardmäßig ist QoS für alle Schnittstellen ausgeschaltet.

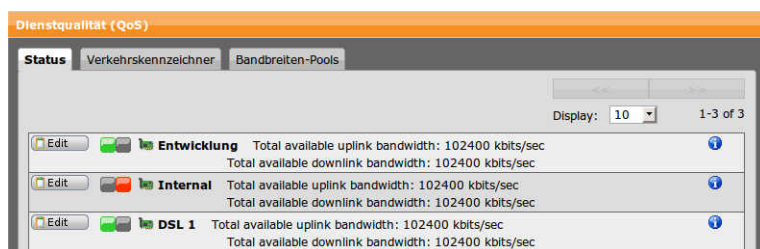


Figure 7.11 QoS: Status

Um die Bandbreiten, die von Ihrem ISP bereitgestellt werden, für Down- und Uplink zu konfigurieren (in Kbit/s), klicken Sie die Schaltfläche *Edit* der jeweiligen Schnittstelle. Geben Sie beispielsweise für eine 5 Mbit/s-Internetverbindung bei Up- und Downlink 5120 ein.

Sollte Ihre Bandbreite variieren, geben Sie den niedrigsten garantierten Wert an, der von Ihrem ISP zugesichert wird. Wenn Sie beispielsweise eine Internetverbindung mit 5 Mbit/s für Up- und Downlink mit einer Variation von 0,8 Mbit/s haben, geben Sie 4300 Kbit/s an. Beachten Sie, dass die Firewall eine veränderte Bandbreite berücksichtigt, wenn die verfügbare Bandbreite temporär höher ausfällt als der konfigurierte tiefste zugesicherte Wert. Dabei wird der prozentuale Anteil an der Bandbreite für zu priorisierenden Verkehr entsprechend erhöht; umgekehrt funktioniert das jedoch leider nicht.

Uplink begrenzen: Die Funktion QoS nutzt die oben eingetragenen Bandbreitenwerte als Basis für die Kalkulation des priorisierten Datenverkehrs. Die Funktion *Limit Uplink* ist standardmäßig ausgewählt und sollte bei folgenden Schnittstellen-Typen verwendet werden:

- Standard-Ethernet-Schnittstelle: Zwischen der Firewall und Internet ist ein Router installiert und die vom Router bereitgestellte Bandbreite ist bekannt.
- Ethernet-VLAN-Schnittstelle: Zwischen der Firewall und Internet ist ein Router installiert und die vom Router bereitgestellte Bandbreite ist bekannt.

- DSL (PPPoE)
- DSL (PPPoA)
- Modem (PPP)

Die Option *Uplink begrenzen* sollte grundsätzlich ausgewählt werden, wenn die maximale Bandbreite der Schnittstelle die Ausführung des Bandbreiten-Managements behindert. Dies betrifft hauptsächlich die folgenden Schnittstellen-Typen:

- Standard-Ethernet-Schnittstelle: Direkt mit dem Internet verbunden.
- Ethernet-VLAN-Schnittstelle: Direkt mit dem Internet verbunden.
- Kabelmodem (DHCP)

Bei Schnittstellen ohne eine Uplink-Grenze verteilt die QoS-Funktion den gesamten Datenverkehr proportional. Wenn Sie beispielsweise auf einer Kabelmodem-Schnittstelle 512 Kbit/s für VoIP-Verkehr reserviert haben und sich die verfügbare Bandbreite halbiert, dann würden 256 Kbit/s für diesen Datenverkehr verwendet werden (im Gegensatz zu Schnittstellen mit einer festen Obergrenze funktioniert proportionale Verteilung in beiden Richtungen).

Download Equalizer: (Download-Ausgleich) Wenn diese Option aktiviert ist, verhindern die beiden Warteschlangen-Algorithmen *Stochastic Fairness Queuing* (SFQ) und *Random Early Detection* (RED), dass es zu Netzwerkstaus kommt. Im Falle dass die konfigurierte Download-Geschwindigkeit erreicht ist, werden Pakete jener Verbindung verworfen, die den meisten Downlink in Anspruch nimmt.

Upload Optimizer: (Upload-Optimierung) Wenn diese Option aktiviert ist, werden ausgehende TCP-Pakete, die eine Verbindung aufbauen, priorisiert (TCP-Pakete mit SYN-Flag) ebenso wie TCP-Bestätigungspakete (TCP-Pakete mit ACK-Flag und einer Paketlänge zwischen 40 und 60 Bytes) und DNS-Lookups (UDP-Pakete auf Port 53).

Verkehrskennzeichner

Ein Verkehrskennzeichner (engl. *traffic selector*) kann als eine QoS-Definition angesehen werden, die bestimmte Arten von Netzwerkverkehr beschreibt, die von QoS behandelt werden. Diese Definitionen werden später innerhalb der Bandbreiten-Pool-Definition verwendet. Dort können Sie festlegen, wie dieser Verkehr von QoS behandelt wird, indem Sie z. B. die komplette Bandbreite begrenzen oder dem Verkehr einen gewissen Mindestanteil der Bandbreite zusichern.

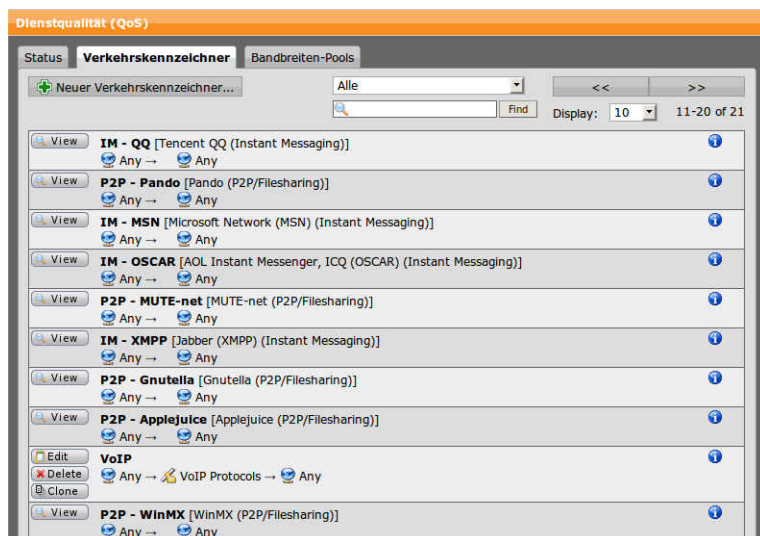


Figure 7.12 QoS: Verkehrskennzeichner

Um einen Verkehrskennzeichner zu definieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Verkehrskennzeichner* auf *Neuer Verkehrskennzeichner*.**

Das Dialogfenster *Neuen Verkehrskennzeichner erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Name: Geben Sie einen aussagekräftigen Name für den Verkehrskennzeichner ein.

Kennzeichnertyp: Sie können einen einzelnen Verkehrskennzeichner definieren oder eine Verkehrskennzeichnergruppe. Für eine Gruppe müssen bereits einzelne Verkehrskennzeichner definiert sein.

Quelle: Wählen Sie das Quellnetzwerk aus, für das QoS aktiviert werden soll.

Dienst: Wählen Sie den Netzwerkdienst aus, für den QoS aktiviert werden soll. Sie können zwischen verschiedenen vordefinierten Diensten und Dienstgruppen auswählen. Wenn Sie z. B. für VoIP-Verbindungen eine bestimmte Bandbreite reservieren möchten, wählen Sie die Protokolle SIP und H.323 aus.

Ziel: Wählen Sie das Zielnetzwerk aus, für das QoS aktiviert werden soll.

TOS/DSCP: Wählen Sie diese Option aus, wenn Sie das TOS/DSCP-Feld im IP-Header zur Kennzeichnung des zu priorisierenden Datenverkehrs nutzen wollen. In großen VoIP-Umgebungen wird der TOS/DSCP Flag oft zur

Kennzeichnung von VoIP-Datenverbindungen genutzt. Wenn Sie eine feste Bandbreite für VoIP-Verbindungen nicht auf der Basis von VoIP-Protokollen reservieren wollen, wählen Sie ToS-Bits oder DSCP-Bits, die in Ihrer VoIP-Umgebung verwendet werden.

- **ToS-Bits:** Wenn Sie ToS-Bits wählen, stehen die folgenden Optionen zur Verfügung:
 - Normaler Dienst
 - Kosten minimieren
 - Zuverlässigkeit maximieren
 - Durchsatz maximieren
 - Verzögerung minimieren
- **DSCP-Bits:** Wenn Sie DSCP-Bits (Differentiated Services Code Point) wählen, können Sie einfach einen einzelnen *DSCP-Wert* festlegen (eine Ganzzahl im Bereich 0 bis 63). Oder Sie wählen einen vordefinierten Wert aus der Liste *DSCP-Klasse* (z. B. *BE default dscp (000000)*).

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über den Verkehrskennzeichner hinzu.

3. Klicken Sie *Speichern*.

Der neue Verkehrskennzeichner wird in der Liste *Verkehrskennzeichner* angezeigt.

Wenn Sie viele Verkehrskennzeichner definiert haben, können Sie mehrere Kennzeichner zu einer einzigen Verkehrskennzeichnergruppe zusammenfügen, um die Konfiguration angenehmer zu gestalten.

Der Verkehrskennzeichner oder die Verkehrskennzeichnergruppe kann nun für jeden Bandbreiten-Pool verwendet werden. Diese Pools können auf der Registerkarte *Schnittstellen* definiert werden.

Bandbreiten-Pools

Auf der Registerkarte *Netzwerk >> Dienstqualität >> Bandbreiten-Pools* werden die Pools für das Bandbreiten-Management definiert und verwaltet.

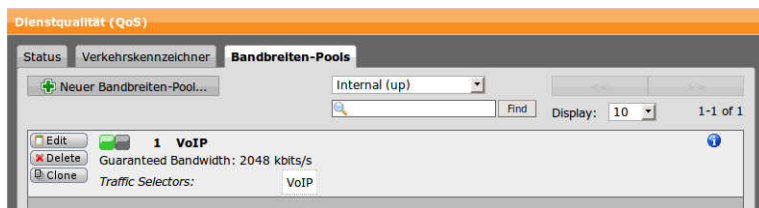


Figure 7.13 QoS: Bandbreiten-Pools

Um einen Bandbreiten-Pool zu definieren, gehen Sie folgendermaßen vor:

1. Wählen Sie auf der Registerkarte **Bandbreiten-Pools** eine Schnittstelle aus.

Wählen Sie aus der Auswahlliste diejenige Schnittstelle aus, für die Sie einen Bandbreiten-Pool definieren möchten.

2. Klicken Sie auf die Schaltfläche **Neuer Bandbreiten-Pool**.

Das Dialogfenster *Neuen Bandbreiten-Pool erstellen* wird geöffnet.

3. Nehmen Sie die folgenden Einstellungen vor:

Name: Geben Sie einen aussagekräftigen Name für den Bandbreiten-Pool ein.

Position: Die Positionsnummer, die die Priorität des Bandbreiten-Pools festlegt. Niedrigere Nummern haben eine höhere Priorität. Bandbreiten-Pools werden in aufsteigender Reihenfolge abgeglichen. Wenn ein Bandbreiten-Pool zutrifft, werden Bandbreiten-Pools mit einer höheren Nummer nicht mehr abgeglichen. Platzieren Sie Bandbreiten-Pools mit den genauer definierten Verkehrskennzeichnern an der Spitze der Tabelle, um sicher zu gehen, dass unpräzisere Profile zuletzt abgeglichen werden.

Beispiel: Sie haben einen Bandbreiten-Pool für HTTP-Datenverkehr im allgemeinen und einen weiteren Pool für den Datenverkehr zu einem bestimmten Webserver definiert. Dann sollte der Bandbreiten-Pool mit dem spezifischen Webserver vorrangig positioniert, d. h. auf Position 1 gesetzt werden. Beachten Sie allerdings, dass die Prioritäten keine Wirkung haben, wenn die darin enthaltenen Verkehrskennzeichner verschiedenen Schnittstellen zugeordnet sind, auf denen QoS aktiv ist.

Bandbreite: Tragen Sie die Uplink-Bandbreite (in Kbit) ein, die für diesen Bandbreiten-Pool reserviert werden soll. Beispiel: Sie möchten 1 Mbit/s für diesen Pool reservieren, dann tragen Sie den Wert 1024 ein.

Hinweis – Es können für einen Bandbreiten-Pool lediglich bis zu 90 % der zur Verfügung stehenden Gesamtbandbreite reserviert werden. Die Firewall

reserviert grundsätzlich 10 % für den vom Bandbreiten-Management unberücksichtigten Datenverkehr. Beispiel: Wenn der Uplink 5 Mbit/s beträgt, und Sie möchten VoIP soviel Bandbreite wie möglich zuweisen, können Sie für den VoIP-Datenverkehr eine Bandbreite von maximal 4608 Kbit/s reservieren.

Obere Bandbreitengrenze angeben: Der Wert, den Sie oben im Feld *Bandbreite* angegeben haben, stellt die zugesicherte Bandbreite dar, die für einen speziellen Verkehrstyp reserviert ist. Ein Bandbreiten-Pool beansprucht jedoch immer mehr Bandbreite für seinen Verkehr als verfügbar ist. Wenn Sie für einen bestimmten Verkehrstyp verhindern wollen, dass er mehr als eine bestimmte Menge Ihrer Bandbreite verbraucht, wählen Sie diese Option aus. Damit beschränken Sie die Bandbreitennutzung dieses Pools auf eine Obergrenze.

Verkehrskennzeichner: Wählen Sie den *Verkehrskennzeichner* für diesen Bandbreiten-Pool aus.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über den Bandbreiten-Pool hinzu.

4. Klicken Sie *Speichern*.

Anschließend wird der neue Bandbreiten-Pool in der Liste *Bandbreiten-Pools* angezeigt.

Multicast Routing (PIM-SM)

Das Menü *Netzwerk >> Multicast Routing (PIM-SM)* ermöglicht die Konfiguration von *Protocol Independent Multicast Sparse Mode* (PIM-SM) zur Benutzung in Ihrem Netzwerk. PIM ist ein Protokoll, um dynamisch Multicast-Pakete in Netzwerk zu routen. Multicast ist eine Methode, Pakete, die von mehr als einem Client empfangen werden sollen, effizient auszuliefern, indem so wenig Verkehr wie möglich verursacht wird. Normalerweise werden Pakete für mehr als einen Client einfach kopiert und jedem Client individuell zugestellt. Dabei steigt die benötigte Bandbreite mit der Anzahl der Benutzer. Dadurch benötigen Server, die viele Clients haben, die die gleichen Pakete zur gleichen Zeit erfragen, sehr viel Bandbreite, so z. B. Server für Streaming-Inhalte.

Multicast hingegen spart Bandbreite, indem es Pakete nur einmal über jeden Netzwerkknoten sendet. Um das zu erreichen, beteiligt Multicast entsprechend konfigurierte Router an der Entscheidung, wann Kopien erstellt werden müssen auf dem Weg vom Server (Sender) zum Client (Empfänger). Die Router benutzen PIM-SM, um die aktiven Multicast-Empfänger im Auge zu behalten,

und benutzen diese Information, um das Routen zu konfigurieren.

Ein grobes Schema der PIM-SM-Kommunikation sieht wie folgt aus: Ein Sender beginnt damit, seine Multicast-Daten zu übermitteln. Der Multicast-Router für den Sender registriert sich über PIM-SM am RP-Router, welcher wiederum eine Teilnahmemeldung (join message) an den Router des Senders schickt. Multicast-Pakete fließen nun vom Sender zum RP-Router. Ein Empfänger registriert sich über einen IGMP-Broadcast für diese Multicast-Gruppe bei seinem lokalen PIM-SM-Router. Dieser Router sendet daraufhin eine Teilnahmemeldung für den Empfänger in Richtung RP-Router, welcher im Gegenzug den Multicast-Verkehr an den Empfänger weiterleitet.

Multicast besitzt seinen eigenen IP-Adressbereich, welcher 224.0.0.0/4 ist.

Allgemein

Auf der Registerkarte *Netzwerk >> Multicast Routing (PIM-SM) >> Allgemein* können Sie PIM aktivieren und deaktivieren. Der Abschnitt *Routing-Daemon-Einstellungen* zeigt den Status der Schnittstellen und beteiligten Router an.



Figure 7.14 Beispielkonfiguration PIM-SM

Bevor Sie PIM aktivieren können, müssen Sie zunächst auf der Registerkarte *Schnittstellen* mindestens zwei Schnittstellen definieren, die als PIM-Schnittstellen dienen sollen, und auf der Registerkarte *RP-Router* einen Router. Um PIM-SM zu aktivieren, gehen Sie folgendermaßen vor:

1. Aktivieren Sie PIM-SM auf der Registerkarte *Allgemein*.

Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche.

Die Statusampel wird gelb und der Abschnitt *Routing-Daemon-Einstellungen* kann nun bearbeitet werden.

2. Nehmen Sie die folgenden Einstellungen vor:

Aktive PIM-SM-Schnittstellen: Wählen Sie mindestens zwei Schnittstellen für die Benutzung von PIM-SM aus. Schnittstellen können auf der Registerkarte *Schnittstellen* konfiguriert werden.

Aktive PIM-SM-RP-Router: Wählen Sie mindestens einen RP-Router für die Benutzung von PIM-SM aus. RP-Router können auf der Registerkarte *RP-Router* definiert werden.

3. Klicken Sie *Übernehmen*.

Ihre Einstellungen werden gespeichert.

PIM-SM-Kommunikation in Ihrem Netzwerk ist nun aktiviert.

Um die Konfiguration abzubrechen, klicken Sie auf die Schaltfläche *Abort Enable* oder auf die gelbe Statusampel. Um PIM-SM zu deaktivieren, klicken Sie auf die Statusampel oder die Schaltfläche *Disable*.

Live-Protokoll

Klicken Sie auf die Schaltfläche *Live-Protokoll öffnen*, um das PIM-Live-Protokoll in einem neuen Fenster zu öffnen.

Schnittstellen

Auf der Registerkarte *Netzwerk >> Multicast Routing (PIM-SM) >> Schnittstellen* können Sie festlegen, über welche Schnittstellen von Astaro Security Gateway Multicast-Kommunikation stattfinden soll.



Figure 7.15 PIM-SM: Schnittstellenliste

Um eine neue PIM-SM-Schnittstelle anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Schnittstellen* auf *Neue PIM-SM-Schnittstelle*.**

Das Dialogfenster *Neue PIM-SM-Schnittstelle anlegen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Name: Geben Sie einen aussagekräftigen Name für die PIM-SM-Schnittstelle ein.

Schnittstelle: Wählen Sie eine Schnittstelle aus, die PIM- und IGMP-Netzwerkverkehr annehmen soll.

DR-Priorität (optional): Geben Sie eine Zahl ein, die die designierte Router-Priorität (DR) für diese Schnittstelle festlegt. Der Router mit der niedrigsten Zahl nimmt IGMP-Anfragen an, wenn mehr als ein PIM-SM-Router im selben Netzwerksegment präsent ist. Zahlen von 0 bis 2^{32} sind erlaubt. Wenn Sie keine Priorität angeben, wird die Zahl 0 gesetzt.

IGMP: Wählen Sie die Version des Internet-Group-Management-Protokolls (*Internet Group Management Protocol*), die unterstützt werden soll. IGMP wird von Empfängern benutzt, um einer Multicast-Gruppe beizutreten.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die PIM-SM-Schnittstelle hinzu.

3. **Klicken Sie *Speichern*.**

Die neue PIM-SM-Schnittstelle wird zur Schnittstellenliste hinzugefügt.

Um eine PIM-SM-Schnittstelle zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

RP-Router

Um Multicast in Ihrem Netzwerk verwenden zu können, müssen Sie einen oder mehrere Rendezvous-Point-Router (RP-Router) konfigurieren. Ein RP-Router nimmt Registrierungen sowohl von Multicast-Empfängern als auch -Sendern an. Ein RP-Router ist ein regulärer PIM-SM-Router, der dazu auserkoren wurde, außerdem der RP-Router für bestimmte Multicast-Gruppen zu sein. Alle PIM-SM-Router müssen darin übereinstimmen, welcher Router der RP-Router ist.

Um einen RP-Router anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *RP-Router* auf *Neuer Rendezvous-Point-Router*.**

Das Dialogfenster *Neuen RP-Router anlegen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Name: Geben Sie einen aussagekräftigen Name für den RP-Router ein.

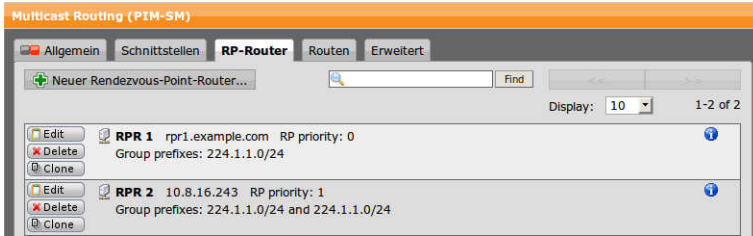


Figure 7.16 PIM-SM: Liste der Rendezvous-Point-Router

Rechner: Legen Sie einen Rechner an (oder wählen Sie einen aus), der als Rendezvous-Point-Router agieren soll.

Priorität: Geben Sie eine Zahl an, die die Priorität des RP-Routers festlegt. Teilnahmemeldungen werden zu dem RP-Router mit der niedrigsten Priorität gesendet. Zahlen von 0 bis 255 sind erlaubt. Wenn Sie keine Priorität angeben, wird die Zahl 0 gesetzt.

Multicast-Gruppenpräfixe: Geben Sie die Multicast-Gruppe ein, für die der RP-Router verantwortlich ist. Sie können Gruppenpräfixe wie 224.1.1.0/24 festlegen, falls der RP für mehr als eine Multicast-Gruppe verantwortlich ist. Die Multicast-Gruppe oder Gruppenpräfixe muss/müssen sich innerhalb des Multicast-Adressbereichs befinden, der 224.0.0.0/4 ist.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über den RP-Router hinzu.

3. Klicken Sie *Speichern*.

Der neue RP-Router wird zur Routerliste hinzugefügt.

Um einen RP-Router zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Routen

Sie müssen zwischen Sender(n) und Empfängern eine durchgängige Kommunikationsroute einrichten. Wenn Empfänger, Sender und/oder RP-Router sich nicht im selben Netzwerksegment befinden, werden Sie eine Route anlegen müssen, um die Kommunikation zwischen ihnen zu gewährleisten.

Um eine PIM-SM-Route anzulegen, gehen Sie folgendermaßen vor:



Figure 7.17 PIM-SM: Routen-Liste

1. Klicken Sie auf der Registerkarte **Routen** auf **Neue PIM-SM-Route**. Das Dialogfenster *Neue PIM-SM-Route anlegen* wird geöffnet.

2. Nehmen Sie die folgenden Einstellungen vor:

Routentyp: Die folgenden Routentypen sind verfügbar:

- **Schnittstellen-Route:** Datenpakete werden an eine bestimmte Schnittstelle geschickt. Dieser Typ kann bei zwei Szenarien genutzt werden: Für Routing-Einträge zu dynamischen Schnittstellen (z. B. PPP), da in diesem Fall die IP-Adresse des Gateway nicht bekannt ist, oder für eine Standard-Route mit einem Gateway außerhalb der direkt angeschlossenen Netzwerke.
- **Gateway-Route:** Die Datenpakete werden an einen bestimmten Rechner (Gateway) geschickt.

Netzwerk: Wählen Sie den Zieladressbereich aus, wohin der PIM-Verkehr geroutet werden soll.

Gateway: Wählen Sie das Gateway/den Router aus, an das oder den die Firewall die Datenpakete weiterleiten soll (nur verfügbar, wenn Sie *Gateway-Route* als Routentyp gewählt haben).

Schnittstelle: Wählen Sie die Schnittstelle aus, zu der die Firewall die Datenpakete weiterleiten soll (nur verfügbar, wenn Sie *Schnittstellenroute* als Routentyp ausgewählt haben).

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die Route hinzu.

3. Klicken Sie **Speichern**.

Die neue PIM-SM-Route wird zur Routen-Listen hinzugefügt.

Um eine PIM-SM-Route zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Erweitert

Auf der Registerkarte *Netzwerk >> Multicast Routing (PIM-SM) >> Erweitert* können Sie erweiterte Einstellungen konfigurieren.

Shortest-Path-Tree-Einstellungen

In einigen Netzwerken ist die PIM-Kommunikationsroute zwischen Sender, RP und Empfänger nicht der kürzestmögliche Netzwerkpfad. Die Option *Wechsel zu Shortest-Path-Tree ermöglichen* erlaubt es, eine bestehende Kommunikation zwischen Sender und Empfänger auf den kürzestmöglichen verfügbaren Pfad zu verlegen, wenn ein gewisser Schwellenwert erreicht ist, wobei der RP dann als Vermittler ausgelassen wird.

Auto-Paketfilter-Einstellungen

Wenn Sie diese Option auswählen, wird das System automatisch alle notwendigen Paketfilterregeln anlegen, die benötigt werden, um Multicast-Verkehr für die angegebenen Multicast-Gruppen weiterzuleiten.

Fehlersuche-Einstellungen

Wählen Sie die Option *Fehlersuche-Modus aktivieren* um zusätzliche Information für die Fehlersuche im PIM-SM Routing-Daemon-Protokoll zu sehen.

Kapitel 8

Netzwerkdienste

Dieses Kapitel beschreibt die Konfiguration einiger Netzwerkdienste von Astaro Security Gateway für Ihr Netzwerk.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- DNS
- DHCP
- NTP

DNS

Die Registerkarten des Menüs *Netzwerkdienste >> DNS* enthalten eine Reihe von Konfigurationsmöglichkeiten, die sich auf den Dienst *Domain Name System* (DNS) beziehen. Die Hauptaufgabe von DNS ist die Übersetzung von Domännennamen (Rechnernamen) in die zugehörigen IP-Adressen.

Allgemein

Auf der Registerkarte *Netzwerkdienste >> DNS >> Allgemein* kann den angeschlossenen Netzwerken erlaubt werden, die Firewall für die rekursive DNS-Auflösung (engl. *DNS resolving*) zu nutzen. Üblicherweise wird dies nur den internen Netzwerken (LAN) gestattet.

Hinweis – Wenn Sie bereits einen internen DNS-Server nutzen, z. B. in Verbindung mit Active Directory, dann sollten Sie das Eingabefeld *Zugelassene Netzwerke* leer lassen.

DNS-Speicher leeren

Der DNS-Proxy benutzt einen Zwischenspeicher (Cache) für seine Einträge. Jeder Eintrag hat ein Ablaufdatum (TTL, time-to-live), an dem er gelöscht wird. Die TTL beträgt normalerweise einen Tag. Sie können den Zwischenspeicher jedoch manuell leeren, wenn Sie z. B. wollen, dass jüngste Änderungen in DNS-Einträgen sofort berücksichtigt werden, ohne darauf warten zu müssen, dass

die TTL abläuft. Um den Zwischenspeicher zu leeren, klicken Sie *DNS-Speicher jetzt leeren*.

Weiterleitung

Auf der Registerkarte *Netzwerkdienste >> DNS >> Weiterleitung* können Sie sogenannte *DNS-Forwarders* definieren. Ein Forwarder (von engl. *forward* für weiterleiten) leitet DNS-Anfragen für externe DNS-Namen an DNS-Sever außerhalb des Netzwerks weiter. Fügen Sie möglichst einen DNS-Forwarder Ihrer Konfiguration hinzu. Dies sollte ein lokaler Rechner oder idealerweise ein Server sein, der von Ihrem Internetanbieter (ISP) betrieben wird. Dieser wird dann als übergeordneter Zwischenspeicher (engl. *parent cache*) verwendet und Ihre DNS-Anfragen um einiges beschleunigen. Wenn Sie keinen Weiterleitungs-Namensserver angeben, werden stattdessen die Basis-DNS-Server (engl. *root DNS server*) gefragt, die zunächst einmal Zoneninformationen einholen und deshalb eine längere Beantwortungszeit benötigen.

Um einen DNS-Forwarder hinzuzufügen, gehen Sie folgendermaßen vor:

1. **Wählen Sie einen DNS-Forwarder aus.**

Wählen Sie einen DNS-Forwarder aus oder fügen Sie einen hinzu.

2. **Wählen Sie Forwarders Ihres ISP aus (optional).**

Wählen Sie die Option *Use Forwarders Assigned by ISP* aus, um DNS-Anfragen an DNS-Server Ihres ISP weiterzuleiten.

Wenn diese Option ausgewählt ist, werden alle Forwarders, die automatisch von Ihrem ISP zugewiesen werden, in der Zeile unter dem Feld aufgelistet.

3. **Klicken Sie *Übernehmen*.**

Ihre Einstellungen werden gespeichert.

Anfragerouten

Angenommen, Sie betreiben Ihren eigenen internen DNS-Server, dann kann dieser Server dazu verwendet werden, als alternativer Server DNS-Anfragen für Domänen aufzulösen, die Sie nicht von DNS-Forwarders auflösen lassen wollen. Auf der Registerkarte *Netzwerkdienste >> DNS >> Anfragerouten* können Sie Routen zu eigenen DNS-Servern definieren.

Um eine DNS-Anfrageroute hinzuzufügen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Anfragerouten* auf *Neue DNS-Anfrageroute*.**

Das Dialogfenster *Neue DNS-Anfrageroute erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Domäne: Tragen Sie die Domäne ein, für die der alternative DNS-Server genutzt werden soll.

Target Servers: Wählen Sie einen oder mehrere alternative Server aus.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die DNS-Anfrageroute hinzu.

3. **Klicken Sie *Speichern*.**

Die neue Route wird anschließend in der Liste *DNS-Anfragerouten* angezeigt und ist sofort aktiv.

Um eine DNS-Anfrageroute zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Statische Einträge

Wenn Sie keinen eigenen DNS-Server einrichten wollen, aber eine statische DNS-Zuordnung für einige Rechner benötigen, können Sie diese Zuordnung hier angeben. Bedenken Sie, dass diese Lösung sich nur für eine begrenzte Anzahl von Einträgen eignet und in keiner Weise als Ersatz für einen richtigen DNS-Server dienen kann.

Um einen statischen Eintrag hinzuzufügen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Statische Einträge* auf *Neue statische DNS-Zuordnung*.**

Das Dialogfenster *Neue statische DNS-Zuordnung erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Rechnername: Tragen Sie den Namen des Rechners ein, für den die statische DNS-Zuordnung erfolgen soll.

IP-Adresse: Tragen Sie die IP-Adresse des Rechners ein.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über den statischen DNS-Eintrag hinzu.

3. **Klicken Sie *Speichern*.**

Die neue statische DNS-Zuordnung wird anschließend in der Liste *Statische Einträge* angezeigt und ist sofort aktiv.

Um einen statischen DNS-Eintrag zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

DynDNS

Dynamic DNS, oder kurz DynDNS, ist ein Domännennamensdienst, der es ermöglicht, statische Internetdomännennamen eines Computers einer variierenden IP-Adresse zuzuordnen. Beim DynDNS-Dienst können Sie über die DynDNS-Website²⁰ ein DNS-Alias beantragen, das automatisch aktualisiert wird, sobald sich Ihre Internet-IP-Adresse ändert. Wenn Sie sich bei diesem Dienst registriert haben, erhalten Sie einen Rechnernamen, einen Benutzernamen und ein Kennwort, welche für die Konfiguration benötigt werden.

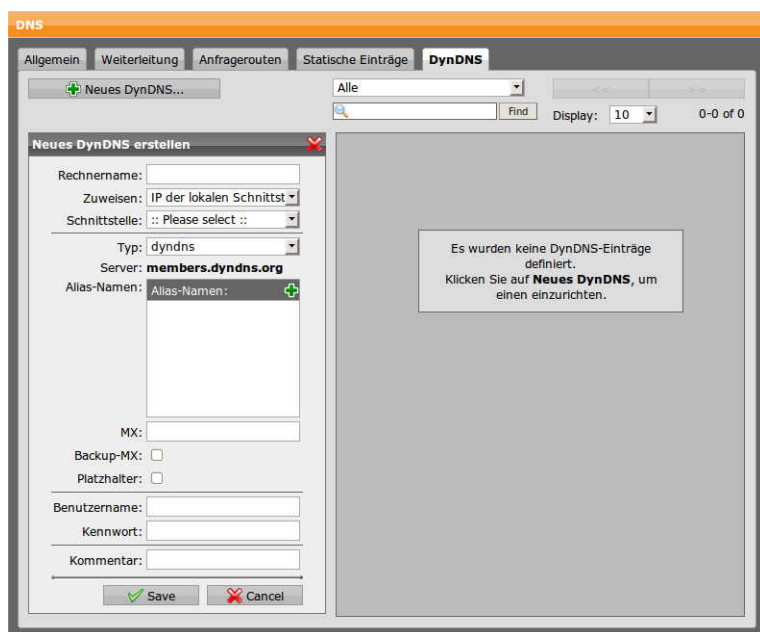


Figure 8.1 DNS: Konfiguration von DynDNS

Um DynDNS zu konfigurieren, gehen Sie folgendermaßen vor:

²⁰ <http://www.dyndns.com/>

1. Klicken Sie auf der Registerkarte *DynDNS* auf *Neues DynDNS*.

Das Dialogfenster *Neues DynDNS erstellen* wird geöffnet.

2. Nehmen Sie die folgenden Einstellungen vor:

Rechnername: Tragen Sie die Domäne ein, die Sie von Ihrem Internetanbieter erhalten haben (z. B. `firewall.domain.dynalias.org`). Sie müssen dabei keine spezielle Syntax einhalten, sondern nur das eingeben, was ihr DynDNS-Anbieter erfordert. Überdies können Sie optional Ihren DynDNS-Rechnernamen auch als den Hauptrechnernamen für Ihre Firewall verwenden.

Zuweisen: Legen Sie die IP-Adresse fest, der der DynDNS-Name zugeordnet werden soll. Wählen Sie *IP der lokalen Schnittstelle*, wenn die betreffende Schnittstelle eine öffentliche IP-Adresse hat. Üblicherweise werden Sie diese Option für Ihre DSL-Internetverbindung verwenden. Bei der Option *Erste öffentliche IP auf der Standardroute* müssen keine Schnittstellen spezifiziert werden. Ihre ASG wird stattdessen eine WWW-Anfrage zu einem öffentlichen DynDNS-Server senden, der im Gegenzug mit der öffentlichen IP-Adresse antwortet, die Sie gerade verwenden. Diese Option ist nützlich, wenn Ihre ASG keine öffentliche IP-Adresse besitzt, sondern sich in einem privaten Netzwerk befindet und sich über einen maskierenden Router mit dem Internet verbindet.

Schnittstelle: Wählen Sie die Netzwerkkarte aus, die für den DynDNS-Dienst genutzt werden soll. In der Regel ist dies die externe Schnittstelle zum Internet.

Typ: Die folgenden DynDNS-Typen stehen zur Verfügung:

- **DynDNS:** Für den Standarddienst von DynDNS.
- **DynDNS-custom:** Für den Dienst *Custom DNS* von DynDNS. Dieser Dienst ist hauptsächlich für Benutzer, die ihre Domäne selbst besitzen oder selbst registriert haben.

Alias-Namen (optional): In dieses Dialogfenster können zusätzliche Rechnernamen eingetragen werden (z. B. `mail.example.com`, `example.com`). Diese Alias-Namen verweisen dann auf die gleiche IP-Adresse wie der Name im Eingabefeld *Rechnername*.

MX (optional): Tragen Sie in das Eingabefeld den Mailserver ein (z. B. `mail.example.com`) (nur mit dem Typ *DynDNS* möglich). Ein Mailserver wird benötigt, um Mails an einen bestimmten Server umzuleiten. MX-Einträge (engl. *MX records*) ermöglichen, dass Mails an eine bestimmte Domäne zu einem bestimmten Server geleitet werden. Beispiel: Wenn im Eingabefeld des Mailservers `mail.example.com` eingetragen ist, dann wird eine Mail mit der Adresse `user@example.com` an den Rechner

mail.example.com geliefert.

Backup-MX (optional): Wählen Sie diese Option nur aus, wenn der Rechnername im Feld *Rechnername* als Hauptmailserver dienen soll. Dann wird der Rechnername im Feld *MX* nur als Backup-Mailserver eingesetzt.

Platzhalter (optional): Wählen Sie diese Option aus, wenn Sie wollen, dass Subdomänen auf dieselbe IP-Adresse verweisen wie Ihre registrierte Domäne (nur mit dem Typ *DynDNS* möglich). Bei Verwendung dieser Option wird Ihrer Domäne ein Stern (*) angefügt, der als Platzhalter dient (z. B. *.example.dyndns.org). Das stellt sicher, dass z. B. www.example.dyndns.org auf dieselbe Adresse verweist wie example.dyndns.org.

Benutzername: Tragen Sie den Benutzernamen ein, den Sie vom DynDNS-Anbieter erhalten haben.

Kennwort: Tragen Sie das Kennwort ein, das Sie vom DynDNS-Anbieter erhalten haben.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über den DynDNS-Eintrag hinzu.

3. Klicken Sie *Speichern*.

Der neue DynDNS-Dienst wird in der Liste *DynDNS* angezeigt. Der Dienst ist noch ausgeschaltet (Statusampel zeigt Rot).

4. Aktivieren Sie den DynDNS-Dienst.

Aktivieren Sie die Schnittstelle durch einen Klick auf die Statusampel. Der Dienst ist nun eingeschaltet (Statusampel zeigt Grün).

Um einen DynDNS-Dienst zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Sie können mehrere DynDNS-Einträge gleichzeitig haben. Wenn alle Einstellungen für zwei Rechnernamen identisch sind, empfiehlt es sich, die Option *Alias-Namen* zu verwenden anstatt zwei Einzel-Einträge zu erstellen.

DHCP

Das *Dynamic Host Configuration Protocol* (DHCP) (dynamisches Rechnerkonfigurationsprotokoll) weist angeschlossenen Rechnern (Clients) aus einem festgelegten Adressbereich automatisch IP-Adressen zu. Dies spart bei größeren Netzwerken viel Konfigurationsaufwand und beugt Adresskonflikten vor. DHCP verteilt an seine Clients IP-Adressen und Informationen zum Standardgateway (Router) und zur DNS-Konfiguration.

Zusätzlich zur vereinfachten Konfiguration von Clientrechnern und der einfachen Bewegung von mobilen Computern zwischen verschiedenen Netzwerken, lassen sich in einem DHCP-Netzwerk Fehler einfacher lokalisieren und beheben, da die Konfiguration der IP-Adressen primär von den Einstellungen des DHCP-Server abhängen. Außerdem lassen sich Adressbereiche effektiver nutzen, vor allem wenn nicht alle Rechner gleichzeitig im Netzwerk aktiv sind. Die IP-Adressen können so je nach Bedarf vergeben und wiederverwendet werden.

Server

Auf der Registerkarte *Netzwerkdienste* >> *DHCP* >> *Server* wird der DHCP-Server konfiguriert. Astaro Security Gateway fungiert dann als DHCP-Server, stellt die Adressbereiche für die angeschlossenen Netzwerke bereit und weist den Clients weitere Parameter zur Netzwerkkonfiguration zu. Der DHCP-Dienst kann für jedes angeschlossene Netzwerk individuell konfiguriert werden.

Um einen DHCP-Server zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Server* auf *Neuer DHCP-Server*.**

Das Dialogfenster *Neuen DHCP-Server erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Schnittstelle: Wählen Sie die Netzwerkkarte aus, von der aus den Clients die IP-Adressen zugewiesen werden. Es kann nur eine bereits konfigurierte Schnittstelle ausgewählt werden.

Bereichsbeginn/-ende: Der IP-Adressbereich, der als Kontingent für diese Schnittstelle verwendet wird. Ein möglicher Adressbereich für diese Schnittstelle ist bereits voreingestellt. Der Adressbereich muss innerhalb des Netzwerks sein, das mit der Schnittstelle verbunden ist.

DNS-Server 1/2: Tragen Sie die IP-Adressen der Namensserver ein.

Standardgateway: Tragen Sie die IP-Adresse des Standardgateway ein.

Domäne (optional): Tragen Sie die Domäne ein, die an die Clients übermittelt werden soll (z. B. `intranet.example.com`).

Lease-Zeit: Jede IP-Adresse, die vom DHCP-Server zugewiesen wird, läuft nach einer bestimmten Zeitdauer ab. Hier können Sie diese Dauer in Sekunden festlegen. Der Standard ist 86400 Sekunden (ein Tag). Das Minimum beträgt 600 Sekunden (10 Minuten) und das Maximum beträgt 2592000 Sekunden (ein Monat).

Nur Clients mit statischer Zuordnung (optional): Wählen Sie diese Option aus, damit der DHCP-Server IP-Adressen nur an Clients vergibt, die einen Eintrag auf der Registerkarte *Statische MAC/IP-Zuordnungen* haben.

WINS-Knotentyp: Der *Windows Internet Naming Service* (WINS) ist Microsofts Implementation des *NetBIOS Name Server* (NBNS) unter Windows. Dabei handelt es sich um einen Namensserver und -dienst für NetBIOS-Computernamen. Ein WINS-Server verhält sich wie eine Datenbank, die Rechnernamen mit IP-Adressen vergleicht. Dadurch ermöglicht er Computern, die NetBIOS verwenden, das TCP/IP-Protokoll zu nutzen. Die folgenden WINS-Knotentypen sind verfügbar:

- **Nicht festlegen:** Der WINS-Knotentyp ist nicht festgelegt und wird vom Client selbst bestimmt.
- **B-Knoten (kein WINS):** Verwendet ausschließlich Broadcast.
- **P-Knoten (nur WINS):** Verwendet nur Punkt-zu-Punkt-Namensanfragen für einen Windows-Namensserver (WINS) .
- **M-Knoten (Broadcast, dann WINS):** Zuerst erfolgt ein Broadcast, dann wird der Namensserver angefragt.
- **H-Knoten (WINS, dann Broadcast):** Zuerst wird der Namensserver angefragt, dann erfolgt ein Broadcast.

WINS-Server: Tragen Sie hier die IP-Adresse des WINS-Servers ein (Textfeld erscheint nur bei den Knotentypen mit WINS).

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über den DHCP-Server hinzu.

3. Klicken Sie **Speichern**.

Der neue DHCP-Server wird anschließend in der DHCP-Server-Liste angezeigt und ist sofort aktiv.

Um einen DHCP-Server zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Relay

Auf der Registerkarte *Netzwerkdienste* >> *DHCP* >> *Relay* können Sie ein DHCP-Relay konfigurieren. Der DHCP-Dienst wird von einem separaten DHCP-Server bereitgestellt und das Sicherheitssystem fungiert als Relay (auch *Relais*) und leitet die DHCP-Anfragen und -Antworten durch die Netzwerksegmente weiter. Bevor die Einstellungen für das DHCP Relay durchgeführt werden können, muss der separate DHCP-Server konfiguriert sein.

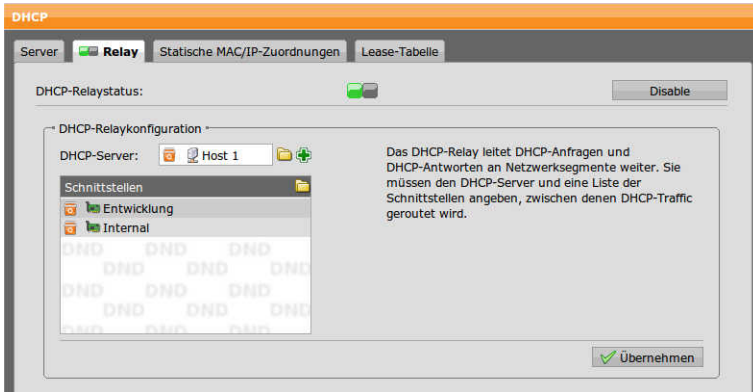


Figure 8.2 DHCP: Konfiguration eines DHCP-Relay

Um ein DHCP-Relay zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie *DHCP-Relay* auf der Registerkarte *Relay*.**
 Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche.
 Die Statusampel wird gelb und der Abschnitt *DHCP-Relaykonfiguration* kann nun bearbeitet werden.
2. **Wählen Sie den DNS-Server aus.**
3. **Wählen Sie eine Schnittstelle aus.**
 DHCP-Anfragen, die über diese Schnittstelle ankommen, werden an den gewählten DHCP-Server weitergeleitet.
4. **Klicken Sie *Übernehmen*.**
 Ihre Einstellungen werden gespeichert.

Um die Konfiguration abzubrechen, klicken Sie auf die Schaltfläche *Abort Enable* oder auf die gelbe Statusampel.

Statische MAC/IP-Zuordnungen

Auf der Registerkarte *Netzwerkdienste >> DHCP >> Statische MAC/IP-Zuordnungen* wird den Clients eine bestimmte IP-Adresse statisch zugewiesen. Dafür benötigen Sie einen konfigurierten DHCP-Server und die MAC-Adresse der Netzwerkkarte dieses Clients. MAC-Adressen werden typischerweise als eine Folge von sechs Gruppen aus zwei hexadezimalen Zeichen dargestellt, die durch Doppelpunkt getrennt sind (z. B. 00:04:76:16:EA:62).

Note – Um Adresskonflikte vorzubeugen, vermeiden Sie eine Adressüberschneidung zwischen einem definierten DHCP-Kontingent mit einer statisch zugewiesenen IP-Adresse. Beispielsweise kann eine statische Zuordnung von 192.168.0.200 darin resultieren, dass zwei Systeme dieselbe IP-Adresse erhalten, wenn das DHCP-Kontingent 192.168.0.100–192.168.0.210 umfasst.

Um eine statische MAC/IP-Zuordnung zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Statische MAC/IP-Zuordnungen* auf *Neue MAC/IP-Zuordnung*.**

Das Dialogfenster *Neue MAC/IP-Zuordnung erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

DHCP-Server: Wählen Sie den DHCP-Server aus, von dem der Client die statische IP-Adresse bezieht.

MAC-Adresse: Tragen Sie die MAC-Adresse der Client-Netzwerkkarte ein.

IP-Adresse: Tragen Sie die statische IP-Adresse für den Client ein. Die IP-Adresse muss im Netzwerkbereich der internen Netzwerkkarte liegen.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die statische MAC/IP-Zuordnung hinzu.

3. **Klicken Sie *Speichern*.**

Die neue statische MAC/IP-Zuordnung wird anschließend in der MAC/IP-Zuordnungsliste angezeigt.

Um eine statische MAC/IP-Zuordnung zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Lease-Tabelle

Wenn der DHCP-Dienst genutzt wird, besitzt ein Client keine eigene IP-Adresse mehr, sondern „borgt“ (engl. *lease*) sich diese vom DHCP-Server. Dieser gibt dem Client das Recht, die IP-Adresse für einen gewissen Zeitraum zu verwenden.

Die Lease-Tabelle auf der Registerkarte *Netzwerkdienste >> DHCP >> Lease-Tabelle* zeigt die aktuellen IP-Adresszuweisungen des DHCP-Servers. Das schließt Informationen über Beginn der Zuweisung und Ablaufzeit der IP-Adresse mit ein.

Rechnername	MAC-Adresse	IP-Adresse	Lease-Start	Lease-Ablauf	Statische Zuordnung hinzufügen
[unknown]	00:10:f3:09:cd:df	10.8.10.255	2009/09/11 11:32:23 UTC	2009/09/12 11:32:23 UTC	Neue Zuordnung
[unknown]	00:10:f3:0b:94:2f	10.8.8.170	2009/09/11 11:32:52 UTC	2009/09/12 11:32:52 UTC	Neue Zuordnung

Figure 8.3 DHCP: Lease-Tabelle

Statische Zuordnung hinzufügen

Sie können einen vorhandenen Lease als Vorlage für eine neue statische MAC/IP-Zuordnung, indem Sie die Schaltfläche *Neue Zuordnung* in der Spalte *Statische Zuordnung hinzufügen* benutzen. Gehen Sie folgendermaßen vor:

1. **Klicken Sie auf die Schaltfläche *Neue Zuordnung*.**

Das Dialogfenster *Neue Zuordnung* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

MAC-Adresse (optional): Ändern Sie die MAC-Adresse nur, wenn Sie die statische Zuordnung einem anderen Rechner als dem gewählten zuweisen wollen.

IP-Adresse: Ändern Sie die IP-Adresse auf eine Adresse außerhalb des DHCP-Pool-Bereichs um.

DNS-Zuordnung erstellen (optional): Wählen Sie die Option, um automatisch eine statische DNS-Zuordnung für den Rechner zu erstellen (siehe *Netzwerkdienste >> DNS >> Statische Einträge*). Wenn Sie einen Rechnernamen eingeben, wird die Zuordnung ihn verwenden.

Netzwerkrechnerobjekt anlegen (optional): Wählen Sie diese Option, um automatisch ein Rechnerobjekt anzulegen (siehe *Definitionen >> Netzwerke*). Wenn Sie einen *Rechnernamen* angeben, wird dieser der Name des Objekts.

Rechnername (optional): Der Übersichtlichkeit halber sollten Sie einen Namen für den Rechner angeben. Andernfalls wird das Objekt als „[unknown]“ aufgeführt.

3. **Klicken Sie *Speichern*.**

Ihre Einstellungen werden gespeichert.

Hinweis – Wenn ein Lease in eine statische Zuordnung umgewandelt wird, sollten Sie die IP-Adresse ändern, so dass sie nicht mehr im DHCP-Pool-Bereich

liegt. Wenn Sie die IP-Adresse ändern, wird sich die IP-Adresse des Clients jedoch nicht sofort ändern, sondern erst, wenn er das nächste Mal versucht, seinen Lease zu erneuern.

NTP

Im Menü *Netzwerkdienste* >> *NTP* wird der NTP-Server für die angeschlossenen Netzwerke konfiguriert. Das *Network Time Protocol* (NTP) ist ein Protokoll, das Uhren von Computer-Systemen über IP-Netzwerke synchronisiert. Anstatt nur die Zeit von Astaro Security Gateway zu synchronisieren – diese Funktion wird auf der Registerkarte *Verwaltung* >> *Systemeinstellungen* >> *Zeit und Datum* eingestellt – können Sie bestimmten Netzwerken explizit erlauben, diesen Synchronisierungsdienst ebenfalls zu verwenden.

Um die Benutzung von NTP-Zeitsynchronisierung zu ermöglichen, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie den NTP-Server.**

Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche.

2. **Wählen Sie Zugelassene Netzwerke aus.**

Wählen Sie die Netzwerke aus, die Zugriff auf den NTP-Server haben sollen.

3. **Klicken Sie Übernehmen.**

Ihre Einstellungen werden gespeichert.

Network Security

Dieses Kapitel beschreibt die Konfiguration der grundlegenden Netzwerksicherheitsfunktionen von Astaro Security Gateway. Die Übersichtsseite *Network-Security-Statistik* zeigt eine Zusammenfassung über Ereignisse im Angriffsschutzsystem sowie über verworfene Datenpakete sowohl für Quell- als auch Zielrechner. Jeder der Abschnitte enthält einen *Details*-Link. Ein Klick auf den Link leitet Sie zur entsprechenden Seite des Abschnitts *Berichte* von WebAdmin weiter, wo Sie weitere statistische Informationen finden können.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- Paketfilter
- Netzwerkadressumsetzung (NAT)
- Angriffsschutz
- Server-Lastverteilung
- Erweiterte Einstellungen

Paketfilter

Im Menü *Network Security* > > *Paketfilter* werden die Paketfilterregeln der Firewall definiert und verwaltet. Im Allgemeinen ist der Paketfilter ein zentraler Teil der Firewall und dient in einem Netzwerk dazu, Verbindungen zu verhindern, die von der Sicherheitspolitik her verboten sind. Die Voreinstellung der Astaro Security Gateway Sicherheitspolitik sieht vor, dass aller Netzwerkverkehr blockiert und protokolliert werden soll. Ausnahmen bilden automatisch generierte Regelwerke, die andere Softwarekomponenten benötigen, um funktionieren zu können. Diese automatisch generierten Regeln werden jedoch auf der Registerkarte *Paketfilter* > > *Regeln* nicht angezeigt. Diese Art der Sicherheitspolitik erfordert, dass Sie explizite Regeln für Netzwerkverkehr anlegen, der die Firewall passieren darf.

Regeln

Auf der Registerkarte *Network Security >> Paketfilter >> Regeln* wird das Paketfilterregelwerk verwaltet. Alle neu definierten Paketfilterregeln sind direkt nach der Erstellung deaktiviert. Aktivierte Regeln werden der Reihe nach angewandt, bis die erste Regel zutrifft. Die Reihenfolge der Abarbeitung richtet sich dabei nach der Positionsnummer, d. h. wenn Sie die Reihenfolge der Regeln ändern, ändern Sie gleichzeitig die Reihenfolge der Abarbeitung.

Warnung – Wenn eine Regel zutrifft, werden die nachfolgenden Regeln nicht mehr beachtet! Die Reihenfolge ist daher sehr wichtig. Setzen Sie nie eine Regel mit den Einträgen *Any (Quelle)* – *Any (Dienst)* – *Any (Ziel)* – *Zulassen (Aktion)* an den Beginn Ihres Regelwerks.

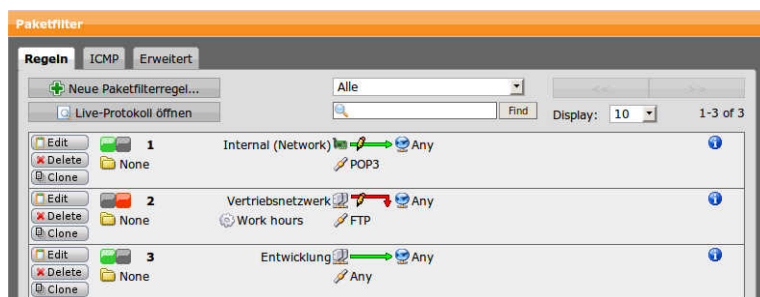


Figure 9.1 Paketfilter: Regelsatz

Um eine Paketfilterregel zu erstellen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Regeln* auf *Neue Paketfilterregel*.**
Das Dialogfenster *Neue Regel erstellen* wird geöffnet.
2. **Nehmen Sie die folgenden Einstellungen vor:**
 - Gruppe:** Zur einfacheren Administration des Regelwerks können Paketfilterregeln zu Gruppen zusammengefasst werden. Die Zugehörigkeit zu einer Gruppe hat nur Auswirkungen auf die Darstellung, aber keinen Einfluss auf die Abarbeitung der Regel im Regelwerk.
 - Position:** Die Positionsnummer, die die Priorität der Regel festlegt. Niedrigere Nummern haben eine höhere Priorität. Regeln werden in aufsteigender Reihenfolge abgeglichen. Wenn eine Regel zutrifft, werden Regeln mit einer höheren Nummer nicht mehr abgeglichen.
 - Quelle:** Die Netzwerkdefinition der Quelle, die angibt, von welche(m/n)

Rechner(n) oder Netzwerk(en) die Pakete stammen.

Dienst: Die Dienstdefinition, die das Protokoll angibt, und bei TCP oder UDP die Quell- und Zielpports der Pakete.

Ziel: Die Netzwerkdefinition des Ziels, die angibt, wer der/die Zielrechner oder das/die Zielnetzwerk(e) der Pakete ist/sind.

Aktion: Dies ist die Aktion, die der Paketfilter durchführt, wenn Datenverkehr dieser Regel entspricht. Die folgenden Aktionen stehen zur Auswahl:

- **Zulassen:** Die Verbindung wird zugelassen und Datenverkehr wird weitergeleitet.
- **Verwerfen:** Alle Pakete, die diese Bedingung erfüllen, werden ohne Rückmeldung an den Absender verworfen (engl. *drop silently*).
- **Ablehnen:** Verbindungsanfragen, die diese Bedingung erfüllen, werden abgewiesen. Der Absender erhält eine entsprechende ICMP-Nachricht.

Zeitereignis: Standardmäßig ist kein Zeitereignis ausgewählt, das bedeutet, die Regel ist gültig. Wenn Sie ein Zeitereignis auswählen, wird die Regel nur innerhalb der Zeitspanne gültig, die durch dieses Zeitereignis definiert ist. Weitere Informationen hierzu finden Sie unter Zeitereignisse.

Verkehr protokollieren: Wenn Sie diese Option wählen, wird die Protokollierung aktiviert und Pakete, die auf Regeln zutreffen werden im Paketfilterprotokoll mitgeschrieben.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die Paketfilterregel hinzu.

3. Klicken Sie **Speichern**.

Anschließend wird die neue Paketfilterregel in der Paketfilterliste angezeigt.

4. Aktivieren Sie die **Paketfilterregel**.

Klicken Sie auf die Statusampel, um die Paketfilterregel zu aktivieren.

Um eine Regel zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Live-Protokoll öffnen: Über diese Schaltfläche wird ein neues Fenster mit dem Live-Protokoll des Paketfilters geöffnet. Dieses enthält ein Echtzeit-Protokoll der gefilterten Pakete, und das sich selbstständig aktualisierende Fenster zeigt die aktuelle Netzwerkaktivität. Anhand der Hintergrundfarbe wird angezeigt, welche Aktion ausgeführt wurde:

- Rot: Das Paket wurde verworfen (drop).
- Gelb: Das Paket wurde abgelehnt (reject).
- Grün: Das Paket wurde zugelassen (allow).
- Grau: Die Aktion konnte nicht bestimmt werden.

Das Live-Protokoll enthält auch Informationen dazu, welche Paketfilterregel dafür gesorgt hat, dass ein Paket abgelehnt wurde. Solche Informationen sind wichtig für die Fehlersuche im Regelwerk.

Mit der Suchfunktion können Sie das Paketfilter-Protokoll nach spezifischen Einträgen durchsuchen. Die Suchfunktion erlaubt es sogar Ausdrücke zu negativieren, indem Sie ein Minus vor den Ausdruck schreiben, z. -WebAdmin, wodurch alle Zeilen ausgeblendet werden, die diesen Ausdruck enthalten.

Live-Protokoll: Paketfilter		Filter:	☒ Autoscroll
09:14:16	WebAdmin connection	TCP	192.168.2.182:1401 → 10.8.0.28:4444
09:14:16	WebAdmin connection	TCP	192.168.2.182:1402 → 10.8.0.28:4444
09:14:17	WebAdmin connection	TCP	192.168.2.182:1403 → 10.8.0.28:4444
09:15:01	Paketfilter rule #1	TCP	10.8.0.8:45070 → 10.8.0.28:21
09:15:02	Paketfilter rule #1	TCP	10.8.0.8:45071 → 10.8.0.28:21
09:15:04	WebAdmin connection	TCP	10.8.0.11:4885 → 10.8.0.28:4444
09:15:06	Default DROP	TCP	10.8.0.8:44828 → 10.8.0.28:12345
09:15:09	Default DROP	TCP	10.8.0.8:44828 → 10.8.0.28:12345
09:15:11	Default DROP	TCP	10.8.0.8:44829 → 10.8.0.28:12345
09:15:13	Paketfilter rule #1	TCP	10.8.0.8:45074 → 10.8.0.28:21
09:15:22	Paketfilter rule #1	TCP	10.8.0.8:45075 → 10.8.0.28:21
09:15:25	Default DROP	TCP	10.8.0.8:44832 → 10.8.0.28:12345
09:15:33	WebAdmin connection	TCP	10.8.0.11:4886 → 10.8.0.28:4444
09:15:34	WebAdmin connection	TCP	10.8.0.11:4887 → 10.8.0.28:4444
09:15:39	Default DROP	TCP	10.8.0.8:44833 → 10.8.0.28:12345
09:15:42	Paketfilter rule #1	TCP	10.8.0.8:45078 → 10.8.0.28:21

Figure 9.2 Paketfilter: Live-Protokoll

Durch die Funktion *Autoscroll* rücken die Zeilen auf, wenn neue hinzukommen, wodurch im Fenster immer die jüngste Regelverletzung sichtbar wird ohne manuell blättern zu müssen.

Hier finden Sie noch ein paar grundlegende Hinweise zur Konfiguration der Regelwerktafel:

- **Verworfen Broadcasts:** Alle Broadcasts werden von der Firewall standardmäßig verworfen. Diese Aktion wird auch nicht protokolliert (weitere Informationen hierzu unter Erweitert). Dies ist für NetBIOS-Netzwerke (z. B. Microsoft Windows Betriebssysteme) mit vielen Computern hilfreich, da die Broadcasts das Paketfilter-Protokoll schnell volllaufen lassen. Um eine Regel für das Verwerfen von Broadcasts manuell zu definieren, gruppieren Sie die Definitionen der Broadcast-Adressen aller angeschlossenen

Netzwerke zusammen und fügen Sie eine Definition „globaler_broadcast“ von 55.255.255.255/255.255.255.255 hinzu. Fügen Sie dann eine Regel hinzu, die allen Verkehr dieser Adressen verwirft, und platzieren Sie die Regel ganz oben in Ihrer Paketfilterkonfiguration. In Netzwerken mit einer hohen Broadcast-Belastung wirkt sich das überdies positiv auf die Leistung des Systems aus.

- **IDENT-Verkehr ablehnen:** Wenn Sie den IDENT-Reverse-Proxy nicht nutzen möchten, können Sie Datenpakete an den Port 113 (IDENT) des internen Netzwerks ablehnen. Dies kann bei Diensten, die IDENT verwenden (z. B. FTP, SMTP und IRC) längere Zeitüberschreitungen verhindern.

Hinweis – Bei der Nutzung von Maskierung (engl. *masquerading*) werden die IDENT-Anfragen für die maskierten Netzwerke auf den Maskierungs-Schnittstellen ankommen.

- NAT verändert die Adressen der Datenpakete und hat damit Auswirkungen auf die Funktionalität des Paketfilters.
 - DNAT wird vor dem Paketfilter ausgeführt – der Paketfilter bearbeitet daher die bereits umgeschriebenen Datenpakete.
 - SNAT und Maskierung werden nach dem Paketfilter ausgeführt – der Paketfilter bearbeitet daher noch die Datenpakete mit der originalen Quelladresse.

Mit den Funktionen im Kopfbereich der Tabelle können Paketfilterregeln nach bestimmten Kriterien gefiltert werden und so übersichtlich dargestellt werden. Wenn Sie Gruppen angelegt haben, können Sie eine Gruppe über die Auswahlliste wählen und sehen so alle Regeln, die zu dieser Gruppe gehören. Mit dem Suchfeld können Sie nach Stichworten oder auch nur Wortteilen suchen, zu denen die Regeln angezeigt werden sollen. Die Suche umfasst Quelle, Ziel, Dienst, Gruppenname und Kommentar einer Regel.

ICMP

Auf der Registerkarte *Network Security >> Paketfilter >> ICMP* werden die Einstellungen für das Protokoll namens *Internet Control Message Protocol* (ICMP) vorgenommen. ICMP dient dazu verbindungsrelevante Statusinformationen zwischen Rechner auszutauschen. Darüber hinaus ist es wichtig um die

Erreichbarkeit des Netzwerks zu testen und zur Fehlerbehebung bei Netzwerkproblemen.

Das Erlauben von allem ICMP-Verkehr auf dieser Registerkarte hebt eventuelle ICMP-Einstellungen im Paketfilter auf. Wenn Sie ICMP-Verkehr nur für bestimmte Rechner oder Netzwerke erlauben wollen, sollten Sie besser die Registerkarte *Paketfilter* >> *Regeln* verwenden.

Globale ICMP-Einstellungen

Die folgenden globalen ICMP-Funktionen sind verfügbar:

- **ICMP auf Firewall zulassen:** Die Firewall antwortet auf alle ICMP-Pakete.
- **ICMP über Firewall zulassen:** Alle ICMP-Pakete werden durch die Firewall weitergeleitet.
- **ICMP-Umleitungen protokollieren:** Die *ICMP-Umleitungen* (engl. *redirects*) werden von Routern gegenseitig verschickt, um eine bessere Route zu einem Paketziel zu finden. Router ändern daraufhin ihre Routing-Tabellen und leiten das Paket auf der vermeintlich besseren Route zum gleichen Ziel weiter. Wenn Sie diese Option wählen, werden die ICMP-Umleitungen im Paketfilter-Protokoll protokolliert.

Ping-Einstellungen

Das Programm *Ping* ist ein Computer-Netzwerkwerkzeug mit dem man testen kann, ob ein bestimmter Rechner über ein IP-Netzwerk erreichbar ist. Ping arbeitet indem es ICMP-Echo-Anfragen an den Zielrechner schickt und auf Antworten in Form von ICMP-Echo-Antworten lauscht. Aus Zeitintervallen und Antworthäufigkeiten schätzt Ping die Dauer des Paketumlaufs und die Paketverlustrate zwischen den Rechnern.

Die folgenden Ping-Funktionen sind verfügbar:

- **Firewall ist Ping-sichtbar:** Die Firewall antwortet auf ICMP-Echo-Pakete. Die Funktion ist standardmäßig eingeschaltet.
- **Von Firewall pingen:** Der Ping-Befehl kann auf der Firewall verwendet werden. Die Funktion ist standardmäßig eingeschaltet.
- **Firewall leitet Pings weiter:** Die Firewall leitet ICMP-Echo-Anfragen und ICMP-Echo-Antworten weiter.

Traceroute-Einstellungen

Das Programm *Traceroute* ist ein Computer-Netzwerkwerkzeug zur Bestimmung der Route, die von Paketen in einem IP-Netzwerk genommen werden.

Es listet die IP-Adressen der Router auf, über die das versendete Paket transportiert wurde. Sollte der Pfad der Datenpakete kurzfristig nicht nachweisbar sein, wird ein Stern (*) an Stelle der IP-Adresse angezeigt. Nach einer bestimmten Menge an Fehlversuchen wird die Überprüfung abgebrochen. Der Abbruch einer Überprüfung kann viele Gründe haben, der wahrscheinlichste ist jedoch, dass ein Paketfilter im Netzwerkpfad Traceroute-Pakete blockiert.

Die folgenden Traceroute-Funktionen sind verfügbar:

- **Firewall ist Traceroute-sichtbar:** Die Firewall antwortet auf Traceroute-Pakete.
- **Traceroute von Firewall aus:** Der Traceroute-Befehl kann auf der Firewall verwendet werden. Die Funktion ist standardmäßig eingeschaltet.
- **Firewall leitet Traceroute weiter:** Die Firewall leitet Traceroute-Pakete weiter.

Hinweis – Darüber hinaus werden auch die UDP-Ports für UNIX-Traceroute-Anwendungen geöffnet.

Erweitert

Die Registerkarte *Network Security >> Paketfilter >> Advanced* enthält die erweiterten Einstellung zu den Paketfilter- und NAT-Regeln.

Helfer für Verbindungsverfolgung

Sogenannte „Helfer für die Verbindungsverfolgung“ (engl. *connection tracking helpers*) aktivieren Protokolle, die mehrere Netzwerkverbindungen benutzen, um mit Paketfilterregeln oder NAT-Regeln zu arbeiten. Alle Verbindungen, die über den Paketfilter abgewickelt werden, werden durch das Kernelmodul *Conntrack* mitverfolgt: ein Prozess der besser als *Connection Tracking* bekannt ist. Einige Protokolle, wie FTP oder IRC, benötigen mehrere offene Ports und benötigen deshalb spezielle Verbindungsverfolgungshelfer, damit sie korrekt funktionieren. Diese Helfer sind spezielle Kernelmodule, die dabei helfen, zusätzliche Verbindungen zu identifizieren, indem sie sie als zur Eingangsverbindung zugehörig markieren. Das tun sie, indem sie verwandte Adressen aus dem Datenstrom auslesen.

Damit z. B. eine FTP-Verbindung korrekt funktioniert, muss ein FTP-Conntrack-Helfer ausgewählt werden. Der Grund hierfür liegt in den Eigenheiten

des FTP-Protokolls, welches zunächst eine einzelne Verbindung, die FTP-Kontrollverbindung, aufbaut. Sobald Befehle über diese Verbindung laufen, werden andere Ports geöffnet, um den Rest der Daten zu transportieren, die zu dem jeweiligen Befehl gehören (z. B. Downloads oder Uploads). Das Problem hierbei ist, dass die Firewall nichts von den Extraports weiß, weil sie dynamisch ausgehandelt wurden. Aus diesem Grund ist die Firewall kann die Firewall auch nicht wissen, dass sie dem Server erlauben soll, sich mit dem Client über diese spezifischen Ports (aktive FTP-Verbindungen) zu verbinden, oder dass sie Clients aus dem Internet erlauben soll, sich mit dem FTP-Server zu verbinden (passive FTP-Verbindungen).

Hier greift der FTP-Conntrack-Helfer ein. Dieser spezielle Helfer wird zur Verbindungsverfolgung hinzugefügt und durchsucht dann die Kontrollverbindung (normalerweise auf Port 21) nach spezifischen Informationen. Wenn er auf korrekte Informationen stößt, fügt er diese spezifischen Informationen zu einer Liste erwarteter Verbindungen hinzu, so dass sie als zugehörig zur Kontrollverbindung gelten. Das wiederum ermöglicht der Firewall sowohl die FTP-Eingangsverbindung als auch die zugehörigen Verbindungen richtig zu verfolgen.

Verbindungsverfolgungshelfer stehen für die folgenden Protokolle zur Verfügung:

- FTP
- IRC (für DCC)
- PPTP
- TFTP

Hinweis – Das Helfer-Modul PPTP wird benötigt, wenn Sie PPTP-VPN-Dienste auf der Firewall anbieten wollen. PPTP-Verbindungen können sonst nicht aufgebaut werden. Der Grund dafür ist, dass das Protokoll PPTP zuerst eine Verbindung auf TCP-Port 1732 aufbaut, bevor es zur Verbindung mit dem Protokoll *Generic Routing Encapsulation* (GRE) wechselt, welches ein eigenständiges IP-Protokoll ist. Wenn das Helper-Modul *PPTP* nicht geladen ist, werden alle GRE-Pakete von der Firewall blockiert. Falls Sie aber das Helper-Modul *PPTP* nicht laden möchten, können Sie für die GRE-Pakete auch entsprechende Paketfilterregeln anlegen.

Protokollhandhabung

TCP-Fensterskalierung ermöglichen: Das *TCP Receive Window* (RWin) gibt

vor (in Bytes), welche Datenmenge ein System während einer Verbindung puffern kann. Der Absender kann nur diese Datenmenge versenden, danach muss er auf eine Bestätigung und eine Fensteraktualisierung des Empfängers warten. Für eine effizientere Nutzung von Netzwerken mit hoher Bandbreite kann allerdings eine größere Fenstergröße verwendet werden. Allerdings kontrolliert das TCP-Fenstergrößenfeld den Datenfluss und ist auf zwei Bytes beschränkt bzw. eine Fenstergröße von 65535 Bytes. Da das Größenfeld nicht erweitert werden kann, wird ein Skalierungsfaktor verwendet. *TCP window scaling* (TCP-Fensterskalierung) ist eine Kerneloption des TCP/IP-Stacks und kann dazu verwendet werden, die maximale Fenstergröße von 65535 Bytes auf ein Gigabyte zu erweitern. Da viele Netzwerkgeräte wie Router, Lastverteiler, Firewalls usw. die Fensterskalierung immer noch nicht durchgehend unterstützen, ist diese Funktion standardmäßig ausgeschaltet.

Strikte TCP-Sitzungsverwaltung verwenden: Das System kann standardmäßig vorhandene TCP-Verbindungen aufsammeln, die in der Verbindungsverfolgungstabelle aufgrund eines Neustarts nicht verwaltet werden. Interaktive Sitzungen, wie z. B. Secure Shell (SSH) und Telnet werden daher nicht unterbrochen, wenn eine Schnittstelle vorübergehend nicht erreichbar ist. Sobald diese Option aktiviert ist, wird immer ein neuer 3-Wege-Handshake notwendig sein, um solche Sitzungen zu reaktivieren. Es wird empfohlen, diese Option ausgeschaltet zu lassen.

Paketlänge validieren: Der Paketfilter prüft die Datenpakete auf die minimale Länge, wenn das Protokoll ICMP, TCP oder UDP verwendet wird. Wenn die Datenpakete kürzer als die Minimalwerte sind, werden sie blockiert und es wird ein Eintrag im Paketfilterprotokoll angelegt.

Täuschungsschutz: Die Option *Täuschungsschutz* (engl. *spoof protection*) ist standardmäßig ausgeschaltet. Die folgenden Einstellungen stehen zur Verfügung:

- **Normal:** Die Firewall verwirft und protokolliert alle Datenpakete, die als Absenderadresse (source IP) entweder die gleiche IP-Adresse enthalten wie die Firewall, oder Datenpakete, die auf einer Schnittstelle ankommen, welche eine Quell-IP-Adresse eines Netzwerks besitzt, die einem Netzwerk auf einer anderen Schnittstelle zugeordnet ist.
- **Strikt:** Mit dieser Einstellung werden darüber hinaus alle Datenpakete verworfen und protokolliert, die zwar die richtige Zieladresse (destination IP) für eine bestimmte Schnittstelle im Netzwerk enthalten, allerdings über eine Schnittstelle, der sie nicht zugeordnet sind, im Netzwerk eintreffen. Beispielsweise werden Pakete verworfen, die von einem externen Netzwerk an eine IP-Adresse der internen Schnittstelle geschickt wurden, die aber nur

dafür vorgesehen ist, Pakete aus dem internen Netzwerk entgegenzunehmen.

Protokollierungsoptionen

FTP-Datenverbindungen protokollieren: Die Firewall protokolliert alle Datenübertragungen mit FTP-Datei- und Verzeichnisauflistungen. Die Protokolleinträge werden mit dem Ausdruck „FTP data“ versehen.

Einzelne, eindeutige DNS-Anfragen protokollieren: Die Firewall protokolliert alle ausgehenden Anfragen an DNS-Server sowie deren Ergebnis. Die Protokolleinträge werden mit dem Ausdruck „DNS request“ versehen.

Verworfen Broadcasts protokollieren: Standardmäßig verwirft der Paketfilter alle Broadcasts, die darüber hinaus auch nicht protokolliert werden. Wenn Sie allerdings Broadcasts im Paketfilterprotokoll protokollieren lassen möchten, z. B. für Prüfungszwecke, wählen Sie die Option aus.

Datenverkehrsmonitor

In diesem Abschnitt können Sie einen Datenverkehrsmonitor starten, auf dem Sie den Bandbreitenverbrauch aller Netzwerkkarten sehen können. Der Verkehrsmonitor wird in einem neuen Fenster geöffnet, wenn Sie auf die Schaltfläche *Verkehrsmonitor starten* klicken. Der Verkehrsmonitor aktualisiert sich selbst in kurzen Abständen. Sie können die Schaltfläche *Pause* verwenden, um die Aktualisierung zu unterbrechen.

Tipp – Der Verkehrsmonitor kann für bestimmte Netzwerkkarten auch über das Dashboard geöffnet werden, durch einen Klick auf die *Ein-/Ausgehend*-Grafiken.

NAT

Im Menü *Network Security >> NAT* werden die NAT-Regeln der Firewall definiert und verwaltet. Network Address Translation (NAT) ist ein Verfahren mit dem die Quell- und/oder Zieladressen von IP-Paketen umgeschrieben werden, wenn sie einen Router oder eine Firewall passieren. Die meisten Systeme benutzen NAT, damit mehrere Rechner in einem privaten Netzwerk den Internetzugang über eine einzige öffentliche IP-Adresse nutzen können. Wenn ein Client ein IP-Paket an den Router schickt, wandelt NAT die Absenderadresse in eine andere, öffentliche IP-Adresse um, bevor es das Paket ins Internet weiterleitet. Kommt von der entfernten Station eine Antwort auf dieses Paket zurück, wandelt NAT die öffentliche Adresse wieder in die ursprüngliche IP-Adresse um

und leitet das Paket an den Client weiter. Je nach den vorhandenen Systemressourcen ist NAT in der Lage, beliebig große interne Netzwerke zu verwalten.

Maskierung

Maskierung (engl. *masquerading*) ist eine Sonderform der Quellnetzwerkadress-Umsetzung (engl. *Source Network Address Translation*) (SNAT), bei der viele private IP-Adressen (typischerweise Ihr LAN mit privatem Adressraum) auf eine einzige öffentliche IP-Adresse (typischerweise Ihre externe Schnittstelle zum Internet) umgeschrieben werden, d. h. Sie verbergen interne IP-Adressen und Netzwerkinformationen nach außen. SNAT ist allgemeiner, da es ermöglicht, mehrere Quelladressen mehreren Zieladressen zuzuordnen.

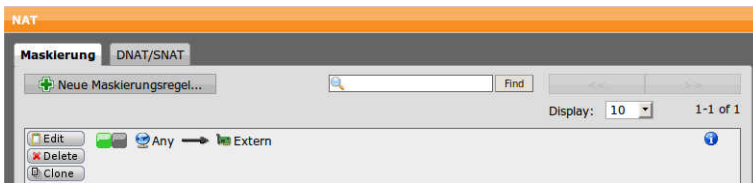


Figure 9.3 NAT: Maskierungsregeln

Hinweis – Die Quelladresse wird nur umgesetzt, wenn das Paket die Firewall über die angegebene Schnittstelle verlässt. Des Weiteren ist die Quelladresse immer die aktuelle IP-Adresse dieser Schnittstelle, d. h. diese Adresse kann dynamisch sein.

Um eine Maskierungsregel anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Maskierung* auf *Neue Maskierungsregel*.**

Das Dialogfenster *Neue Maskierungsregel erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Netzwerk: Wählen Sie das zu maskierende (interne) Netzwerk aus.

Schnittstelle: Wählen Sie die (externe) Netzwerkkarte aus, die mit dem Internet verbunden ist.

Benutze Adresse: Wenn der Schnittstelle, die Sie gewählt haben, mehr als eine IP-Adresse zugewiesen ist (siehe *Netzwerk >> Schnittstellen >> Zusätzliche Adressen*), können Sie hier bestimmen, welche IP-Adresse für die Maskierung verwendet werden soll.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über Maskierungsregel hinzu.

3. Klicken Sie *Speichern*.

Anschließend wird die neue Maskierungsregel in der Liste der Maskierungsregeln angezeigt.

4. Aktivieren Sie die Maskierungsregel.

Klicken Sie auf die Statusampel, um die Maskierungsregel zu aktivieren.

Um eine Maskierungsregel zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Hinweis – Damit von den Clients aus dem internen Netzwerk eine Verbindung zum Internet aufgebaut werden kann, müssen Sie für den Paketfilter entsprechende Regeln anlegen.

DNAT/SNAT

DNAT (*Destination Network Address Translation*, Zielnetzwerkadressumsetzung) und SNAT (*Source Network Address Translation*, Quellnetzwerkadressumsetzung) sind zwei spezielle Fälle von NAT. Mit SNAT wird die IP-Adresse des Rechners umgeschrieben, der die Verbindung initiiert hat. Das Gegenstück hierzu ist DNAT, das die Zieladresse der Datenpakete umschreibt. DNAT ist besonders nützlich, wenn ein internes Netzwerk private IP-Adressen verwendet und der Administrator einige Dienste von außen zugänglich machen will.

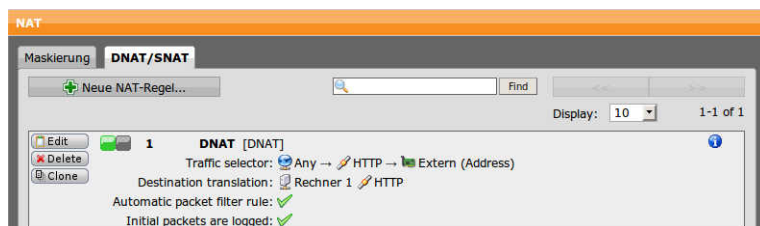


Figure 9.4 NAT: Regeln

Das lässt sich am besten anhand eines Beispiels verdeutlichen: Ein Webserver mit der IP-Adresse 192.168.0.20, 80, der in einem privaten Netzwerk mit dem Adressraum 192.168.0.0/255.255.255.0 steht, soll für Clients aus dem Internet erreichbar sein. Da der 192.168.-Adressraum privat ist, können Clients aus

dem Internet Pakete nicht direkt an den Webserver schicken. Sie können aber mit der externen (öffentlichen) Adresse der Firewall kommunizieren. DNAT kann in diesem Fall Pakete an Port 80 der Firewall annehmen und diese zum internen Webserver weiterleiten.

Hinweis – *PPTP-VPN-Zugang* ist nicht kompatibel mit DNAT.

Im Gegensatz zur Maskierung, welche dynamisch ist, verwendet SNAT statische Adressumsetzung, d. h. dass jede interne Adresse zu einer eigenen, extern sichtbaren IP-Adresse umgesetzt wird.

Hinweis – Der Port 443 (HTTPS) wird standardmäßig für das Benutzerportal genutzt. Wenn Sie diesen Port umleiten möchten, müssen Sie den TCP-Port für das Benutzerportal auf einen anderen Wert setzen (z. B. 1443). Das können Sie unter *Verwaltung >> Benutzerportal >> Erweitert* tun.

Da DNAT vor dem Paketfilter angewendet wird, müssen Sie sicherstellen, dass entsprechende Paketfilterregeln gesetzt sind. Weitere Informationen finden Sie unter *Network Security >> Paketfilter >> Regeln*.

Um eine DNAT/SNAT-Regel anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *DNAT/SNAT* auf *Neue NAT-Regel*.**

Das Dialogfenster *Neue NAT-Regel erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Name: Geben Sie einen aussagekräftigen Name für die NAT-Regel ein.

Gruppe: Sie können verschiedene NAT-Regeln zu Gruppen zusammenfassen. Dadurch erhöhen Sie die Übersichtlichkeit der NAT-Regeln. Eine Gruppe kann aus einer beliebigen Zeichenfolge bestehen.

Position: Die Positionsnummer, die die Priorität der Regel festlegt. Niedrigere Nummern haben eine höhere Priorität. Regeln werden in aufsteigender Reihenfolge abgeglichen. Wenn eine Regel zutrifft, werden Regeln mit einer höheren Nummer nicht mehr abgeglichen.

Datenverkehrsquelle: Die originale Quelladresse des Pakets. Dabei kann es sich entweder um einen einzelnen Rechner oder ein gesamtes Netzwerk handeln.

Datenverkehrsdienst: Der originale Dienstyp des Pakets, der aus Quell- und Zielpports der Pakete oder einem Protokoll besteht.

Hinweis – Ein Datenverkehrsdienst kann nur umgesetzt werden, wenn auch die entsprechenden Adressen umgesetzt werden. Des Weiteren kann ein Dienst nur in einen Dienst mit dem gleichen Protokoll umgesetzt werden.

Datenverkehrsziel: Die originale Zieladresse des Pakets. Dabei kann es sich entweder um einen einzelnen Rechner oder ein gesamtes Netzwerk handeln.

NAT-Modus: Wählen Sie die NAT-Methode aus:

- DNAT (Ziel)
- SNAT (Quelle)
- Volles NAT

Je nach der gewählten Methode werden verschiedene Optionen angezeigt:

- Wenn Sie *DNAT* gewählt haben, wählen Sie eine neue Zielrechner/-netzwerk und einen neuen Zieldienst aus, d. h. die neue Zieladresse und -dienst für das Datenpaket.
- Wenn Sie *SNAT* gewählt haben, wählen Sie eine neue Quellrechner/-netzwerk und einen neuen Quelldienst aus, d. h. die neue Quelladresse und -dienst für das Datenpaket.
- Wenn Sie *Volles NAT* gewählt haben, wählen Sie einen Zielrechner/-netzwerk aus, einen Zieldienst, einen Quellrechner/-netzwerk und einen Quelldienst.

Initpakete protokollieren (optional): Wählen Sie diese Option, um Initialisierungspakete einer Kommunikation ins Paketfilter-Protokoll zu schreiben. Wann immer eine NAT-Regel verwendet wird, werden Sie eine Meldung im Paketfilter-Protokoll mit folgendem Inhalt finden: „Connection using NAT“ (dt. Verbindung benutzt NAT). Diese Option funktioniert sowohl für zustandsbehaftete (stateful) als auch zustandlose (stateless) Protokolle.

Automatische Paketfilterregeln (optional): Wählen Sie diese Option, um automatisch Paketfilterregeln anlegen zu lassen.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die NAT-Regel hinzu.

3. Klicken Sie **Speichern**.

Anschließend wird die neue NAT-Regel in der NAT-Liste angezeigt.

4. Aktivieren Sie die NAT-Regel.

Klicken Sie auf die Statusampel, um die Regel zu aktivieren.

Um eine NAT-Regel zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Angriffschutz

Im Menü *Network Security* > > *Angriffschutz* werden die IPS-Regeln der Firewall definiert und verwaltet. Das Angriffschutzsystem (IPS, engl. *Intrusion Prevention*) erkennt Angriffsversuche anhand eines signaturbasierten Regelwerks zur Angreiferkennung. Das System analysiert den gesamten Datenverkehr und blockiert Attacken automatisch, bevor diese das lokale Netzwerk erreichen. Das bereits vorhandene Regelwerk und die Angriffssignaturen werden durch die Pattern-Updates-Funktion aktualisiert. Neue IPS-Angriffssignaturen werden automatisch als IPS-Regeln in das IPS-Regelwerk importiert.

Allgemein

Auf der Registerkarte *Network Security* > > *Angriffschutz* > > *Allgemein* können Sie das Angriffschutzsystem (IPS) von Astaro Security Gateway aktivieren.

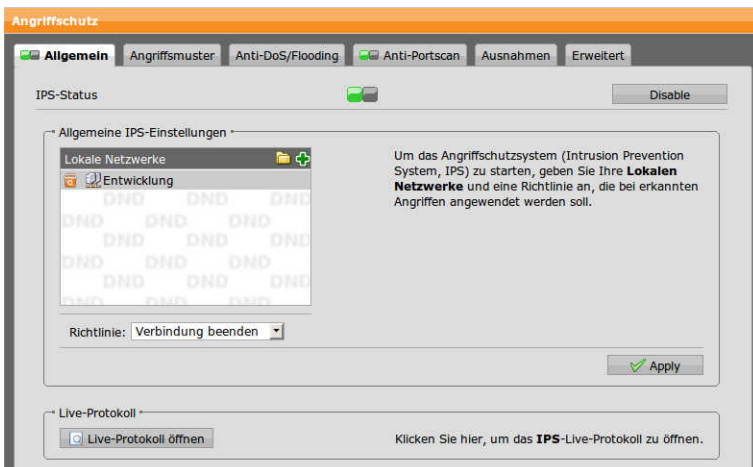


Figure 9.5 Angriffschutz: Aktivierung des Angriffschutzsystems

Um IPS zu aktivieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie das Angriffschutzsystem.**

Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche. Die Statusampel wird gelb und der Abschnitt *Allgemeine IPS-Einstellungen* kann nun bearbeitet werden.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Lokale Netzwerke: Wählen Sie die Netzwerke aus, die vom Angriffschutzsystem überwacht werden sollen. Falls kein Netzwerk ausgewählt ist, wird IPS automatisch wieder ausgeschaltet und kein Netzwerkverkehr überwacht.

Richtlinie: Wählen Sie die Sicherheitsrichtlinie aus, die von IPS verwendet werden soll, wenn eine IPS-Regel eine Angriffsignatur erkennt:

- **Unbemerkt verwerfen:** Die Datenpakete werden ohne weitere Maßnahmen verworfen.
- **Verbindung beenden:** An beide Verbindungspartner wird ein Paket geschickt, das die Verbindung beendet (*RST* bei TCP-Verbindungen und *ICMP Port Unreachable* für UDP-Verbindungen).

Hinweis – Die Maßnahme *Unbemerkt verwerfen* ist voreingestellt. Diese Einstellung sollte in der Regel nicht verändert werden, vor allem da aus Paketen zur Verbindungsbeendigung mutmaßliche Angreifer auch Informationen über die Firewall ziehen können.

3. **Klicken Sie Übernehmen.**

Ihre Einstellungen werden gespeichert.

Live-Protokoll: Das Angriffschutz-Live-Protokoll dient zur Überwachung der gesetzten IPS-Regeln. Durch einen Klick auf die Schaltfläche wird das Fenster geöffnet.

Angriffsmuster

Die Registerkarte *Network Security >> Angriffschutz >> Angriffsmuster* enthält das IPS-Regelwerk, gruppiert nach allgemeinen Angriffssignaturen. Die IPS-Angriffssignaturen sind in folgende Gruppen unterteilt:

- **Operating system specific attacks:** Angriffe auf Betriebssystem-spezifische Schwächen.
- **Attacks against servers:** Angriffe auf alle Arten von Servern, z. B. Webserver, Mailserver usw.
- **Attacks against client software:** Angriffe auf Client-Software, z. B. Webbrowser, Multimedia-Player usw.
- **Protocol Anomaly:** Signaturen sind auf Netzwerkanomalien ausgerichtet.
- **Malware:** Software, die darauf ausgelegt ist, in ein Computersystem einzudringen und ihm zu schaden, ohne dass der Besitzer davon Kenntnis hat, z. B. Trojaner, DoS-Kommunikationswerkzeuge usw.

Um die Leistungsfähigkeit der Firewall zu erhöhen, sollten Sie IPS-Angriffssignaturen deaktivieren, die sich auf Dienste oder Software beziehen, welche nicht in Ihrem lokalen Netzwerk vorkommen. Wenn sich in Ihrem lokalen Netzwerk z. B. kein Webserver im Einsatz befindet, können Sie die Auswahl *HTTP Servers* aufheben.

Für jede Gruppe stehen die folgenden Einstellungen zur Verfügung:

Action: Jede Regel einer Gruppe besitzt eine ihm zugewiesene Maßnahme. Sie können zwischen den folgenden Maßnahmen wählen:

- **Drop:** Standardeinstellung. Wenn ein vermeintlicher Angriff festgestellt wird, wird das kritische Datenpaket verworfen.
- **Alert:** Im Gegensatz zu *Drop* wird das kritische Datenpaket durch die Firewall gelassen, aber es wird eine Warnmeldung in das IPS-Protokoll geschrieben.

Hinweis – Um die Einstellungen für individuell erstellte IPS-Regeln zu ändern, verwenden Sie auf der Registerkarte *Angriffsschutz >> Erweitert* das Feld *Modified Rules*. Eine detaillierte Liste mit allen IPS-Regeln, die in Astaro Security Gateway Version 7 enthalten sind, finden Sie auf der Astaro-Website²¹.

Add Extra Warnings: Wenn Sie diese Option wählen, werden jeder IPS-Regel zusätzliche Regeln hinzugefügt, die die IPS-Erkennungsrate erhöhen. Beachten Sie dabei, dass diese zusätzlichen Regeln allgemeiner gefasst und vager sind als

²¹ <http://www.astaro.com/lists/ASGV7-IPS-rules.html>

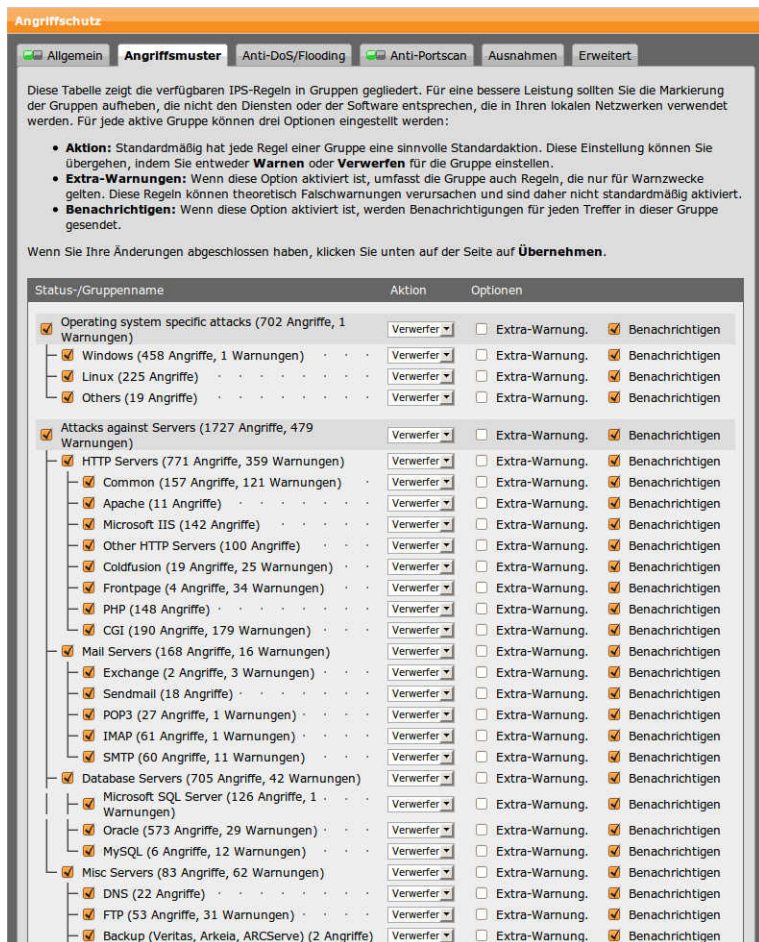


Figure 9.6 Angriffsschutz: IPS-Regelwerk

die expliziten IPS-Angriffssignaturen und dadurch sicherlich häufiger Alarme auslösen. Aus diesem Grund ist die voreingestellte Aktion *Alert*, welche nicht geändert werden kann.

Notify: Wenn Sie diese Option wählen, wird für jedes IPS-Ereignis, das zu dieser Gruppe gehört, eine Meldung an den Administrator geschickt. Beachten Sie, dass die Nachricht nur abgeschickt wird, wenn Sie die Funktion *Benachrichtigungen* im Menü *Management >> Benachrichtigungen* eingeschaltet und entsprechend konfiguriert haben. Darüber hinaus hängt es ebenfalls von den Einstellungen dort ab, ob es sich bei der Benachrichtigung um eine E-Mail oder

SNMP-Trap handelt. Dabei kann es bis zu fünf Minuten dauern, bevor die Änderungen an den Benachrichtigungseinstellungen wirksam werden.

Anti-DoS/Flooding

Auf der Registerkarte *Network Security >> Angriffsschutz >> Anti-DoS/Flooding* können Sie die Konfiguration für den Schutz vor Denial-of-Service- (DoS, dt. etwa *Dienstblockierung*) und Distributed-Denial-of-Service-Angriffe (DDoS, dt. etwa *Verteilte Dienstblockierung*) vornehmen.

The screenshot shows the 'Angriffsschutz' (Attack Protection) configuration window with the 'Anti-DoS/Flooding' tab selected. The window is divided into three main sections for configuring flood protection:

- TCP-SYN-Flood-Schutz:**
 - ☒ Verwende TCP-SYN-Flood-Schutz
 - TCP-SYN-Flood-Schutz erkennt und blockiert TCP-SYN-Paketfluten.
 - Modus: Quell- und Zieladressen
 - Protokollierung: Begrenzt
 - Quellpaketrate (Pakete/Sekunde): 100
 - Zielpaketrate (Pakete/Sekunde): 200
 - Apply
- UDP-Flood-Schutz:**
 - ☒ Verwende UDP-Flood-Schutz
 - UDP-Flood-Schutz erkennt und blockiert UDP-Paketfluten.
 - Modus: Quell- und Zieladressen
 - Protokollierung: Begrenzt
 - Quellpaketrate (Pakete/Sekunde): 200
 - Zielpaketrate (Pakete/Sekunde): 300
 - Apply
- ICMP-Flood-Schutz:**
 - ☒ Verwende ICMP-Flood-Schutz
 - ICMP-Flood-Schutz erkennt und blockiert ICMP-Paketfluten.
 - Modus: Quell- und Zieladressen
 - Protokollierung: Begrenzt
 - Quellpaketrate (Pakete/Sekunde): 10
 - Zielpaketrate (Pakete/Sekunde): 20
 - Apply

Figure 9.7 Angriffsschutz: Konfiguration des Flood-Schutzes

Die Denial-of-Service-Angriffe (DoS) auf Server zielen darauf ab, ein Computersystem für legitime Zugriffe un erreichbar zu machen. Im einfachsten Fall überflutet der Angreifer den Server mit sinnlosen Paketen, um seine Leitung zu überlasten. Da für diese Angriffe eine große Bandbreite erforderlich ist, verlegen sich immer mehr Angreifer auf sogenannte *SYN-Flood*-Attacken, die nicht

darauf abzielen, die Bandbreite auszulasten, sondern die Systemressourcen des Servers zu blockieren. Zu diesem Zweck werden sogenannte SYN-Pakete mit einer oftmals gefälschten Quelladresse an den TCP-Port des Dienstes geschickt. Auf diese Weise wird der Server veranlasst, die Verbindung zur Hälfte zu öffnen, indem er TCP/SYN-ACK-Pakete an die gefälschte Adresse zurücksendet und auf ein Antwort-TCP/ACK-Paket des Absenders wartet – dieses wird von der falschen Adresse niemals abgeschickt. Diese halboffenen Verbindungen sättigen die Anzahl der verfügbaren Verbindungen, die der Server eingehen kann, und hindert ihn somit daran, auf legitime Anfrage zu reagieren.

Solche Angriffe können abgewehrt werden, indem die Menge der SYN- (TCP), UDP- und ICMP-Pakete, die in das Netzwerk geschickt werden, über eine bestimmte Zeit begrenzt werden.

TCP-SYN-Flood-Schutz

Um den TCP-SYN-Flood-Schutz zu konfigurieren, gehen Sie folgendermaßen vor:

1. Wählen Sie auf der Registerkarte **TCP-SYN-Flood-Schutz** die Option **Verwende TCP-SYN-Flood-Schutz**.

2. Nehmen Sie die folgenden Einstellungen vor:

Modus: Die folgenden Modi stehen zur Auswahl:

- **Quell- und Zieladressen:** In diesem Modus werden TCP-SYN-Pakete zurückgewiesen, die sowohl die Quell-IP-Adresse als auch die Ziel-IP-Adresse betreffen. Zuerst werden die SYN-Pakete nach der Quelladresse gefiltert. Wenn dann noch zu viele Anfragen vorhanden sind, werden zusätzlich die SYN-Pakete nach der Zieladresse gefiltert. Der Modus ist voreingestellt.
- **Nur Zieladresse:** In diesem Modus werden die TCP-SYN-Pakete abhängig nur von der Ziel-IP-Adresse zurückgewiesen.
- **Nur Quelladresse:** In diesem Modus werden die TCP-SYN-Pakete abhängig nur von der Quell-IP-Adresse zurückgewiesen.

Protokollierung: Mit dieser Option können Sie den Protokollumfang einstellen. Die folgenden Einstellungen sind möglich:

- **Aus:** Wählen Sie diese Option, wenn keine Protokolle erstellt werden sollen.
- **Begrenzt:** Wählen Sie diese Option, um pro Sekunde maximal fünf Pakete zu protokollieren. Dieser Protokollumfang ist voreingestellt.
- **Alles:** Wählen Sie diese Option, um alle TCP-SYN-Verbindungsversuche zu protokollieren. Beachten Sie, dass TCP-SYN-Flood-Angriffe schnell zu einer sehr umfangreichen Protokollierung führen können.

Quellpaketrate (Pakete/Sekunde): Tragen Sie in das Eingabefeld die maximale Anzahl der Datenpakete pro Sekunde ein, die für Quell-IP-Adressen erlaubt sind.

Zielpaketrate (Pakete/Sekunde): Tragen Sie in das Eingabefeld die maximale Anzahl der Datenpakete pro Sekunde ein, die für Ziel-IP-Adressen erlaubt sind.

Hinweis – Es ist wichtig, dass Sie in die Eingabefelder angemessene Werte eintragen. Wenn Sie die Werte zu hoch definieren, kann es passieren, dass der Webserver den Dienst versagt, weil er eine derart große Menge an TCP-SYN-Paketen nicht bewältigen kann. Wenn Sie andererseits die Rate zu gering definieren, kann es passieren, dass die Firewall unvorhersehbar reagiert und reguläre Anfragen blockiert. Die Einstellungen für die Werte hängen hauptsächlich von Ihrer Hardware ab. Ersetzen Sie daher die Standardeinstellungen durch für Ihr System geeignete Werte.

3. Klicken Sie **Übernehmen**.

Ihre Einstellungen werden gespeichert.

UDP-Flood-Schutz

Der UDP-Flood-Schutz erkennt und blockiert UDP-Paketfluten.

Die Konfiguration des *UDP-Flood-Schutzes* ist identisch zu der des *TCP-SYN-Flood-Schutzes*.

ICMP-Flood-Schutz

Der ICMP-Flood-Schutz erkennt und blockiert ICMP-Paketfluten.

Die Konfiguration des *ICMP-Flood-Schutzes* ist identisch zu der des *TCP-SYN-Flood-Schutzes*.

Anti-Portscan

Auf der Registerkarte *Network Security >> Angriffsschutz >> Anti-Portscan* werden die Einstellungen für Portscan-Erkennung durchgeführt.

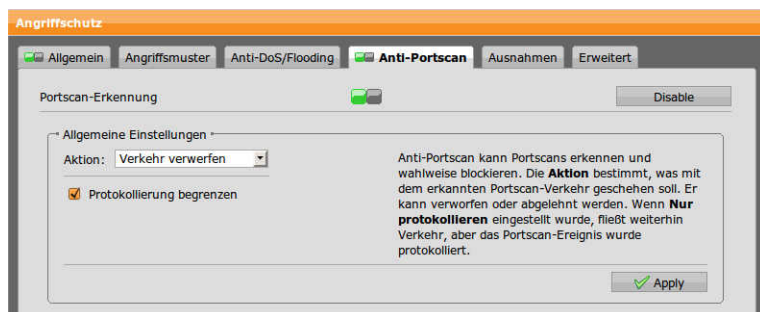


Figure 9.8 Angriffsschutz: Konfiguration des Portscan-Schutzes

Die Portscans werden meist von Hackern durchgeführt, um in gesicherten Netzwerken nach erreichbaren Diensten zu suchen. Um in ein System einzudringen bzw. eine Denial-of-Service-Attacke (DoS) zu starten, benötigen Angreifer Informationen zu den Netzwerk-Diensten. Wenn solche Informationen vorliegen, sind Angreifer möglicherweise in der Lage, gezielt die Sicherheitslücken dieser Dienste auszunutzen. Netzwerkdienste, die die Internet-Protokolle TCP und UDP verwenden, sind über bestimmte Ports erreichbar und diese Port-Zuordnung ist im Allgemeinen bekannt, z. B. ist der Dienst SMTP in der Regel dem TCP-Port 25 zugeordnet. Die von Diensten verwendeten Ports werden als „offen“ bezeichnet, da es möglich ist, eine Verbindung zu ihnen aufzubauen. Die unbenutzten Ports werden hingegen als „geschlossen“ bezeichnet – Versuche, eine Verbindung zu ihnen aufzubauen, scheitern. Damit Angreifer herausfinden können, welche Ports offen sind, verwenden sie ein spezielles Software-Tool, den Portscanner. Dieses Programm versucht mit mehreren Ports auf dem Zielrechner eine Verbindung aufzubauen. Falls dies gelingt, zeigt es die entsprechenden Ports als offen an und die Angreifer haben die nötigen Informationen, welche Netzwerkdienste auf dem Zielrechner verfügbar sind.

Da den Internetprotokollen TCP und UDP je 65535 Ports zur Verfügung stehen, werden die Ports in sehr kurzen Zeitabständen gescannt. Wenn nun von derselben Quell-IP-Adresse mehrere Versuche registriert werden, mit immer anderen Ports Ihres Systems Verbindung aufzunehmen bzw. Informationen an diese zu senden, dann handelt es sich mit ziemlicher Sicherheit um einen Portscan. Wenn ein vermeintlicher Angreifer Rechner oder Dienste in Ihrem Netzwerk scannt, wird dies von der Portscan-Erkennung entdeckt. Eine Möglichkeit dagegen vorzugehen ist, weitere Portscans von derselben Quell-IP-Adresse automatisch zu blockieren.

Technisch gesehen liegt ein Portscan vor, wenn für eine einzelne Quell-IP-Adresse innerhalb von 300 ms eine Erkennungsrate (engl. *Detection Score*)

von 21 Punkten erreicht wird. Diese Erkennungsrate setzt sich folgendermaßen zusammen:

- Scan eines TCP-Zielports unter 1024 = 3 Punkte
- Scan eines TCP-Zielports gleich oder höher 1024 = 1 Punkt
- Scan der Ports 11, 12, 13, 2000 = 10 Punkte

Um die Portscan-Erkennung einzuschalten, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie auf der Registerkarte *Anti-Portscan* die *Portscan-Erkennung*.**

Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche. Die Statusampel wird grün und der Abschnitt *Allgemeine Einstellungen* kann nun bearbeitet werden.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Aktion: Die folgenden Aktionen stehen zur Auswahl:

- **Ereignis nur protokollieren:** Es wird keine Maßnahme gegen den Portscanner ergriffen – es erfolgt nur eine Meldung.
- **Verkehr verwerfen:** Die nachfolgenden Pakete einer Portscansequenz werden verworfen und es kommt keine Verbindung zustande. Der Portscanner wird diesen Port als „gefiltert“ melden.
- **Verkehr ablehnen:** Die Verbindungsanfragen des Angreifers werden zurückgewiesen und eine ICMP-Antwort „destination unreachable/port unreachable“ wird an den Initiator geschickt. Dadurch wird der Port als „geschlossen“ melden.

Protokollierung begrenzen: Aktivieren Sie diese Option, um die Menge der Protokollnachrichten zu minimieren. Die Portscan-Erkennung kann während eines Portscans viele Einträge erzeugen. So wird z. B. jedes SYN-Paket, das als Teil eines Portscans angesehen wird im Paketfilter-Protokoll aufgeführt. Durch Aktivierung dieser Funktion wird der Protokollumfang auf fünf Zeilen pro Sekunde reduziert.

3. **Klicken Sie *Übernehmen*.**

Ihre Einstellungen werden gespeichert.

Ausnahmen

Auf der Registerkarte *Network Security >> Angriffsschutz >> Ausnahmen* können Sie Quell- und Ziernetzwerke definieren, die vom Angriffsschutzsystem (IPS) ausgenommen werden.

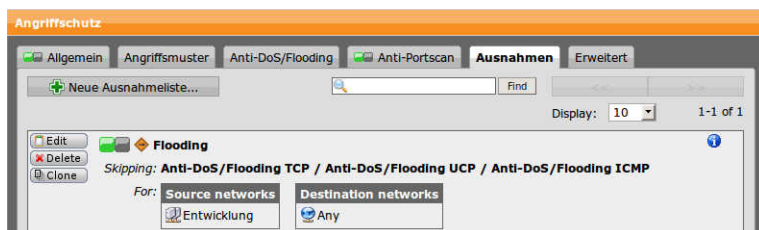


Figure 9.9 Angriffsschutz: Ausnahmenliste

Um eine Ausnahmeliste zu definieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Ausnahmen* auf *Neue Ausnahmeliste*.**
Das Dialogfenster *Ausnahmeliste erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Name: Geben Sie einen aussagekräftigen Name für diese Ausnahme ein.

Diese Kontrollen überspringen: Die Verbindung kann von den folgenden Sicherheitsfunktionen ausgenommen werden:

- **Angriffsschutz:** Wenn Sie diese Option aktivieren, wird IPS ausgeschaltet.
- **Anti-Portscan:** Wenn Sie diese Option aktivieren, verlieren Sie den Schutz vor Portscans.
- **Anti-DoS/Flooding TCP:** Wenn Sie diese Option aktivieren, wird der TCP-SYN-Flood-Schutz ausgeschaltet.
- **Anti-DoS/Flooding UDP:** Wenn Sie diese Option aktivieren, wird der UDP-Flood-Schutz ausgeschaltet.
- **Anti-DoS/Flooding ICMP:** Wenn Sie diese Option aktivieren, wird der ICMP-Flood-Schutz ausgeschaltet.

Quellnetzwerke: Wählen Sie die Quellnetzwerke aus, für die die Sicherheitsprüfungen nicht durchgeführt werden sollen.

Wenn Sie diese Option aktivieren, wird das Feld *Quellnetzwerke* geöffnet.

Zielnetzwerke: Wählen Sie die Zielnetzwerke aus, für die die Sicherheitsprüfungen nicht durchgeführt werden sollen.

Wenn Sie diese Option aktivieren, wird das Feld *Zielnetzwerke* geöffnet.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die Ausnahme hinzu.

3. Klicken Sie *Speichern*.

Anschließend wird die neue Ausnahmeliste in der Liste aller Ausnahmen angezeigt.

Um eine Ausnahme zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Hinweis – Wenn Sie den Angriffsschutz für Pakete mit der Zieladresse der Firewall ausschalten wollen, wird die Wahl *Any* im Feld *Zielnetzwerke* nicht den gewünschten Effekt haben. Wählen Sie stattdessen eine Schnittstellendefinition der Firewall, die die IP-Adresse der Firewall enthält, z. B. *Internal (Address)*, wenn Sie den Angriffsschutz für die interne Adresse der Firewall ausschalten wollen.

Erweitert

Auf der Registerkarte *Network Security >> Angriffsschutz >> Erweitert* können Sie IPS-Regeln manuell modifizieren. Dabei wird die Standardrichtlinie, die aus den Gruppen unter *Angriffsmuster* stammt, für die jeweilige Regel überschrieben. Solche Änderungen sollten nur erfahrene Benutzer vornehmen.

Um eine modifizierte IPS-Regel anzulegen, gehen Sie folgendermaßen vor:

1. Klicken Sie im Feld *Geänderte Regeln* auf das Plusymbol.

Das Dialogfenster *Modify Rule* wird geöffnet.

2. Nehmen Sie die folgenden Einstellungen vor:

Regel-ID: Tragen Sie die ID der IPS-Regel ein, die Sie ändern wollen. Die Regel-IDs sind in der IPS-Regelliste auf der Astaro Website aufgeführt, in den Formaten HTML²² und XML²³. Darüber hinaus können Sie auch über das IPS-Protokoll oder den IPS-Bericht bestimmt werden.

Diese Regel deaktivieren: Wenn Sie diese Option wählen, wird die IPS-Regel mit der entsprechenden ID ausgeschaltet.

Wenn Sie diese Option *nicht* wählen, stehen die folgenden Einstellungen zur Verfügung:

²² <http://www.astaro.com/lists/ASGV7-IPS-rules.html>

²³ <http://www.astaro.com/lists/ASGV7-IPS-rules.xml>

- **Benachrichtigungen ausschalten:** Wenn Sie diese Option wählen, werden keine Benachrichtigungen mehr versendet, wenn diese Regel angewendet wird.
- **Aktion:** Hierbei handelt es sich um die Maßnahmen, die ausgeführt werden, wenn eine Regel zutrifft. Die folgenden Maßnahmen stehen zur Auswahl:
 - **Verwerfen:** Wenn ein vermeintlicher Angriff festgestellt wird, werden die betroffenen Datenpakete verworfen.
 - **Warnung:** Im Gegensatz zur Option *Verwerfen*, wird kritischen Datenpaketen gestattet, die Firewall zu passieren. Es wird allerdings eine Meldung in das IPS-Protokoll eingetragen.

3. Klicken Sie *Speichern*.

Anschließend wird die neue IPS-Regel im Feld *Geänderte Regeln* angezeigt. Bitte beachten Sie, dass Sie auch unten auf der Seite *Übernehmen* klicken müssen, damit die Änderungen wirksam werden.

Hinweis – Wenn Sie eine Regel-ID zum Feld *Geänderte Regeln* hinzufügen und die Aktion zum Beispiel auf *Warnung* setzen, wird diese Änderung nur eine Auswirkung haben, wenn die Gruppe, zu der diese Regel gehört, auf der Registerkarte *Angriffsmuster* auch aktiviert ist. Sollte diese Angriffsmustergruppe jedoch deaktiviert sein, haben Änderungen an einzelnen Regeln keine Auswirkung.

Leistungssteigerung

Um die Leistung des Angriffsschutzsystems zu verbessern und die Menge falscher Alarme zu minimieren, können Sie hier den Bereich der IPS-Regeln auf einzelne Ihrer internen Server begrenzen. Beispiel: Auf der Registerkarte *Angriffsmuster* ist die Gruppe *HTTP Servers* eingeschaltet und hier ist der interne HTTP-Server eingestellt. Wenn nun das Angriffsschutzsystem einen Angriff auf einen HTTP-Server feststellt, dann wird die eingestellte Aktion (*Verwerfen* oder *Warnung*) nur ausgeführt, wenn die IP-Adresse des betroffenen Servers mit der IP-Adresse des hier eingestellten HTTP-Servers übereinstimmt.

Der Einsatzbereich der IPS-Regeln kann für die folgenden Servertypen begrenzt werden:

- **HTTP:** Alle Untergruppen in der Angriffsmustergruppe *HTTP Servers*
- **DNS:** Die Angriffsmustergruppe *DNS*
- **SMTP:** Die Angriffsmustergruppen *Exchange* und *Sendmail*
- **SQL:** Alle Untergruppen in der Angriffsmustergruppe *Database Servers*

Server-Lastverteilung

Mit der Server-Lastverteilung-Funktion (engl. *server load balancing*) können Sie eingehende Verbindungen (z. B. SMTP- oder HTTP-Verkehr) auf verschiedene Server hinter der Firewall verteilen. Die Verteilung basiert auf der Quell-IP-Adresse mit einer Bindungsdauer von einer Stunde. Falls das Intervall zwischen zwei Anfragen derselben Quell-IP-Adresse diesen Zeitraum überschreitet, wird die Verteilung neu ausgehandelt. Die Verteilung des Datenverkehrs basiert auf einem einfachen Round-Robin-Algorithmus.

Alle Server des Serverpools werden entweder durch ICMP-Ping, TCP-Verbindungsaufbau oder HTTP/S-Anfragen überwacht. Bei einem Ausfall wird der betroffene Server nicht weiter verwendet, wobei jede eventuelle Quell-IP-Bindungsdauer aufgehoben wird.

Hinweis – Der Rückgabewert einer HTTP/S-Anfrage muss entweder 1xx Information, 2xx Success, 3xx Redirection oder 4xx Client Error sein.

Verteilungsregeln

Auf der Registerkarte *Network Security >> Server-Lastverteilung >> Verteilungsregeln* können Sie Lastverteilungsregeln für die Astaro Security Gateway Software setzen.

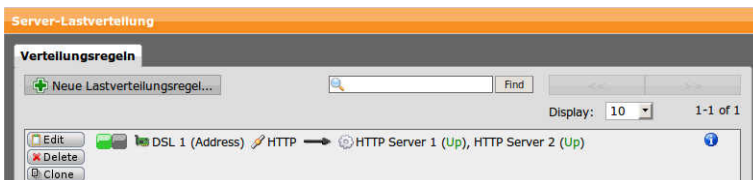


Figure 9.10 Server-Lastverteilung: Lastverteilungsregeln

Um eine Lastverteilungsregel zu setzen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Verteilungsregeln* auf *Neue Lastverteilungsregel*.**

Das Dialogfenster *Neue Lastverteilungsregel erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Dienst: Wählen Sie den Netzwerkdienst aus, den Sie verteilen wollen.

Virtueller Server: Der ursprüngliche Zielrechner des eingehenden Datenverkehrs. Üblicherweise entspricht die Adresse der externen Adresse der Firewall.

Echte Server: Die Rechner, die abwechselnd den Datenverkehr für diesen Dienst akzeptieren.

Typ prüfen: Wählen Sie für die Dienstüberwachung entweder *Ping* (ICMP-Ping), *TCP* (TCP-Verbindungsaufbau), *HTTP-Rechner* (HTTP-Anfragen) oder *HTTPS-Rechner* (HTTPS-Anfragen). Für HTTP- und HTTPS-Anfragen müssen Sie zusätzlich eine URL im Feld *URL prüfen* angeben, welche mit oder ohne Domänenname sein kann, z.B. `index.html` oder `www.beispiel.de/index.html`.

Prüfintervall: Geben Sie einen Prüfintervall in Sekunden ein. 15 Sekunden sind voreingestellt, d. h. alle 15 Sekunden werden alle echten Server auf ihre Funktionsfähigkeit überprüft.

Automatische Paketfilterregeln: Wählen Sie diese Option, um automatische Paketfilterregeln anlegen zu lassen. Diese Regeln erlauben die Weiterleitung von Datenverkehr von beliebigen Rechnern zu den echten Servern.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die Lastverteilungsregel hinzu.

3. **Klicken Sie *Speichern*.**

Anschließend wird die neue Lastverteilungsregel in der Liste angezeigt. Die Regel ist noch ausgeschaltet (Statusampel zeigt Rot).

4. **Aktivieren Sie die Lastverteilungsregel.**

Aktivieren Sie die Regel durch einen Klick auf die Statusampel.

Die Lastverteilungsregel ist nun eingeschaltet (Statusampel zeigt Grün).

Um eine Verteilungsregel zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Beispiel: Angenommen Sie besitzen in Ihrer DMZ zwei HTTP-Server mit den IP-Adressen 192.168.66.10 und 192.168.66.20. Nun wollen Sie den HTTP-Verkehr, der auf der externen Schnittstelle der Firewall ankommt, gleichmäßig auf beide Server verteilen. Um eine Lastverteilungsregel zu erstellen, wählen Sie eine Rechnerdefinition oder legen Sie eine Rechnerdefinition für jeden Server an. Sie könnten Sie `http_server_1` und `http_server_2` nennen. Wählen

Sie dann im Dialogfenster *Neue Lastverteilungsregel erstellen* HTTP als Dienst aus. Wählen Sie außerdem die externe Adresse der Firewall als *Virtuellen Server* aus und fügen Sie zuletzt die Rechnerdefinitionen dem Feld *Echte Server* hinzu.

Erweitert

Im Menü *Network Security >> Erweitert* können Sie zusätzliche Funktionen für die Netzwerksicherheit konfigurieren: einen generischen Proxy, SOCKS-Proxy und IDENT-Reverse-Proxy.

Generischer Proxy

Der generische Proxy, auch bekannt als *Port Forwarder*, ist eine Kombination von DNAT und Maskierung (engl. *masquerading*) und leitet allen eingehenden Datenverkehr für einen bestimmten Dienst weiter zu einem beliebigen Server. Der Unterschied zum normalen DNAT ist jedoch, dass der generische Proxy auch die Quelladresse eines Anfragepakets mit der IP-Adresse der Schnittstelle für ausgehenden Datenverkehr ersetzt. Zusätzlich kann noch der Ziel-Port umgeschrieben werden.

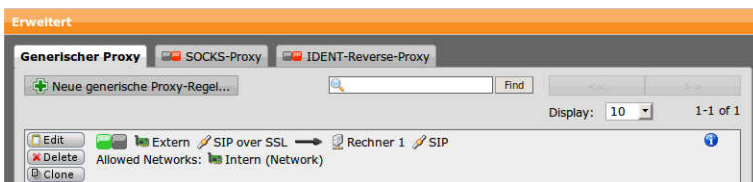


Figure 9.11 Generischer Proxy: Regelliste

Um einen generischen Proxy zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Generischer Proxy* auf *Neue generische Proxy-Regel*.**

Das Dialogfenster *Neue generische Proxy-Regel erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Schnittstelle: Wählen Sie die Schnittstelle für den eingehenden Datenverkehr aus.

Dienst: Wählen Sie die Dienst für den Verkehr aus, der weitergeleitet werden soll.

Rechner: Wählen Sie den Zielrechner aus, zu dem der Datenverkehr weitergeleitet werden soll.

Dienst: Wählen Sie den Zieldienst für den Verkehr aus, der weitergeleitet werden soll.

Zugelassene Netzwerke: Wählen Sie die Netzwerke aus, zu denen die Weiterleitung erfolgen soll.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über diese generische Proxy-Regel hinzu.

3. Klicken Sie *Speichern*.

Anschließend wird die neue generische Proxy-Regel in der Liste angezeigt.

4. Aktivieren Sie die Regel.

Aktivieren Sie die Regel durch einen Klick auf die Statusampel.

Die Regel ist nun eingeschaltet (Statusampel zeigt Grün).

Um eine Regel zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

SOCKS-Proxy

SOCKS ist ein universeller Internet-Protokoll, durch den Client-Server-Anwendungen transparent die Dienste der Netzwerk-Firewall nutzen können. Der Proxy wird von vielen Client-Anwendungen hinter einer Firewall genutzt, um mit Rechnern im Internet zu kommunizieren. Einige Beispiele dafür sind IRC-/Sofortnachrichten-Clients, FTP-Clients und Windows SSH-/Telnet-Clients. Clients hinter einer Firewall, die auf einen externen Server zugreifen wollen, verbinden sich stattdessen mit einem SOCKS-Proxy-Server. Dieser Proxy-Server überprüft dann die Berechtigung des Clients, eine Verbindung zu dem externen Server aufzubauen, und leitet die Anfrage zu dem Server weiter. Ihre Client-Anwendung muss explizit die Protokollversion SOCKS 4 or SOCKS 5 unterstützen.

Der Standardport für SOCKS ist 1080. Fast alle Clients verfügen über die Implementierung dieses Standardports, deshalb muss er normalerweise nicht konfiguriert werden. Der Unterschied zwischen SOCKS und NAT ist, dass SOCKS auch „bind“-Anfragen erlaubt (im Auftrag des Clients auf einem Port lauschen – eine Funktion, die nur sehr wenige Clients unterstützen) und dass SOCKS 5 Benutzerauthentifizierung zulässt.

Wenn der SOCKS-Proxy eingeschaltet wird, muss mindestens ein Netzwerk ausgewählt werden, das Zugang zum Proxy hat. Für eine Benutzerauthentifizierung können auch die entsprechenden Benutzer oder Gruppen ausgewählt werden.

Hinweis – Ohne Benutzerauthentifizierung kann der SOCKS-Proxy sowohl mit SOCKS 4 als auch mit SOCKS 5 genutzt werden. Für Benutzerauthentifizierung wird das Protokoll SOCKS 5 benötigt. Wenn Benutzerauthentifizierung ausgewählt ist, ist nur SOCKS 5 möglich. Damit im SOCKS-5-Modus auch Rechnernamensauflösung durchgeführt wird, müssen Sie auch den DNS-Proxy einschalten, andernfalls schlägt die DNS-Auflösung fehl.

Um den SOCKS-Proxy zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie den SOCKS-Proxy auf der Registerkarte *SOCKS-Proxy*.**
Sie können entweder auf die Statusampel klicken oder auf die *Enable-Schaltfläche*. Die Statusampel wird grün und der Abschnitt *SOCKS-Proxy-Optionen* kann nun bearbeitet werden.
2. **Nehmen Sie die folgenden Einstellungen vor:**
Zugelassene Netzwerke: Wählen Sie die zugelassenen Netzwerke aus, die den SOCKS-Proxy benutzen können sollen.
Benutzerauthentifizierung aktivieren: Wenn Sie diese Option wählen, müssen Benutzer einen Benutzernamen und ein Kennwort angeben, um sich am SOCKS-Proxy anmelden zu können. Da Benutzerauthentifizierung nur vom Protokoll SOCKS 5 unterstützt wird, wird SOCKS 4 automatisch ausgeschaltet.
Zugelassene Benutzer: Wählen Sie die Benutzer oder Gruppen aus, die den SOCKS-Proxy benutzen können sollen.
3. **Klicken Sie *Übernehmen*.**
Ihre Einstellungen werden gespeichert.

IDENT-Reverse-Proxy

Das IDENT-Protokoll wird von einigen Servern zur einfachen Identitätsüberprüfung der auf sie zugreifenden Clients verwendet. Obwohl dieses IDENT-Protokoll unverschlüsselt ist und leicht manipuliert werden kann, verwenden es noch viele Dienste und setzen es manchmal sogar voraus.

Um den IDENT-Reverse-Proxy zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie die IDENT-Weiterleitung auf der Registerkarte *IDENT-Reverse-Proxy*.**

Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche. Die Statusampel wird grün und der Abschnitt *Allgemeine Einstellungen* kann nun bearbeitet werden.

2. **Nehmen Sie die folgenden Einstellungen vor:**

An interne Rechner weiterleiten (optional): Da IDENT-Anfragen von der Verbindungsverfolgung der Firewall nicht verarbeitet werden, bleiben Sie „stecken“, wenn Maskierung (engl. *masquerading*) verwendet wird. Wählen Sie die Option *An interne Rechner weiterleiten*, um IDENT-Anfragen an maskierte Rechner hinter der Firewall weiterzuleiten. Beachten Sie dabei, dass die aktuelle IP-Verbindung nicht übergeben wird. Stattdessen wird die Firewall beim internen Client nach einer IDENT-Antwort fragen und diese Zeichenfolge an den anfragenden Server weiterleiten. Dieses Vorgehen wird von den meisten „Mini-IDENT“-Servern unterstützt, die meist Bestandteil der heute gängigen IRC- und FTP-Clients sind.

Standardantwort: Die Firewall bietet Unterstützung für die Beantwortung von IDENT-Anfragen, wenn Sie die IDENT-Weiterleitung aktivieren. Das System wird dann immer mit der Zeichenfolge antworten, den Sie als *Standardantwort* definiert haben, ungeachtet des lokalen Dienstes, der diese Verbindung initiiert hat.

3. **Klicken Sie Übernehmen.**

Ihre Einstellungen werden gespeichert.

Kapitel 10

Web Security

In diesem Kapitel wird die Konfiguration der grundlegenden Web-Security-Funktionen von Astaro Security Gateway beschrieben.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- HTTP/S-Proxy
- HTTP/S-Profile
- FTP-Proxy

Die Seite *Web-Security-Statistik* enthält eine Übersicht mit den meistaufgerufenen Internetadressen (URLs). Es wird angezeigt, wie lange eine Seite besucht wurde, welches Datenvolumen erzeugt wurde und welcher Benutzer die Website besucht hat. Des Weiteren werden die meistblockierten Kategorien für die Websites aufgelistet. Jeder der Abschnitte enthält einen *Details*-Link. Ein Klick auf den Link leitet Sie zur entsprechenden Seite des Abschnitts *Berichte* von WebAdmin weiter, wo Sie weitere statistische Informationen finden können.

Hinweis – Die Erfassung der Internet-Surf-Daten erfolgt sitzungsbasiert. Um aussagekräftige Näherungswerte zu bekommen, werden die Internetadressen und Benutzer folgendermaßen erfasst: Jede URL-Anfrage wird anhand des Datenvolumens und der Zeitspanne zwischen zwei Anfragen protokolliert. Wenn für eine Dauer von fünf Minuten keine Anfrage für einen Benutzer oder eine URL erfasst wurde, gilt die Sitzung als beendet. Damit im Näherungswert berücksichtigt wird, dass der Benutzer die Internetseite eventuell angeschaut hat, auch wenn die Verbindung inaktiv war, wird jeweils eine Minute beim Wert der Verweildauer (time spent) hinzugefügt. Die Berichtsdaten werden alle 15 Minuten aktualisiert.

Wenn Clients versuchen, ungültige URLs anzufragen, werden diese vom Proxy protokolliert, auch wenn er die Internetseite nicht liefern kann. Diese Links werden auf der Seite *Web-Security-Statistik* als Fehlermeldung (Error) angezeigt. Dies ist allerdings kein Fehler der Berichtsfunktion oder des HTTP/S-Proxy; in den meisten Fällen treten diese Fehler auf, wenn auf einer Internetseite ungültige oder unvollständige Links enthalten sind.

HTTP/S

Auf den Registerkarten des Menüs *Web Security* >> *HTTP/S* können Sie die Astaro Security Gateway Software als einen HTTP-Proxy konfigurieren. Dieser Proxy verfügt neben dem reinen Zwischenspeichern (engl. *Caching*) über zahlreiche Funktionen zur *Web-Filterung* für Netzwerke, die diesen Dienst verwenden dürfen. Das beinhaltet das Verhindern von Virus- und Spyware-Infektionen mithilfe von zwei unterschiedlichen Virenerkennungsmechanismen, deren Signaturdatenbanken laufend aktualisiert werden, und Spyware-Filtermechanismen, die sowohl eingehenden als auch ausgehenden Datenverkehr schützen. Darüberhinaus kann Astaro Security Gateway den Zugriff auf verschiedene Websites kontrollieren, indem es auf eine ausgeklügelte Website-Kategorisierung zurückgreift, und damit die weltgrößte Echtzeit-URL-Datenbank verwendet.

Allgemein

Auf der Registerkarte *Web Security* >> *HTTP/S* >> *Allgemein* werden die Grundeinstellungen für den HTTP-Proxy vorgenommen.

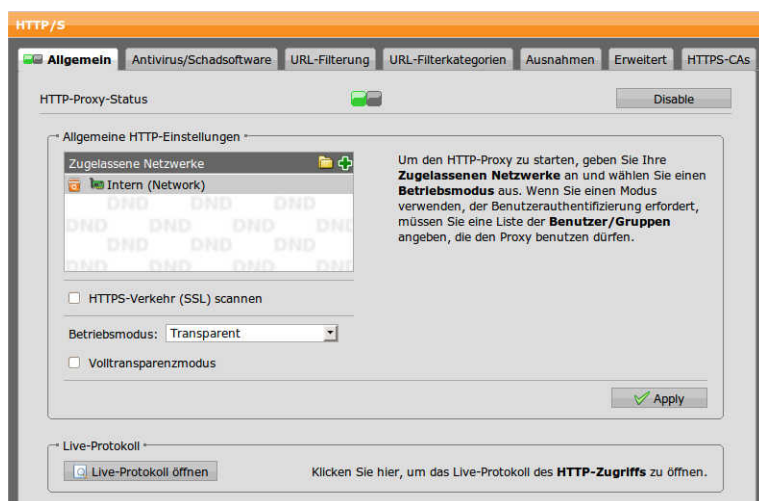


Figure 10.1 HTTP-Proxy: Allgemeine Einstellungen

Um den HTTP/S-Proxy zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie den HTTP-Proxy auf der Registerkarte *Allgemein*.**

Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche. Die Statusampel wird grün und der Abschnitt *Allgemeine HTTP-Einstellungen* kann nun bearbeitet werden.

2. **Wählen Sie die zugelassenen Netzwerke aus.**

Wählen Sie die Netzwerke aus, die für den HTTP-Proxy zugelassenen sind. Standardmäßig lauscht der HTTP-Proxy nach Client-Anfragen auf dem TCP-Port 8080 und lässt alle Clients zu, die aus dem/den Netzwerk(en) stammen, welche im Feld *Zugelassene Netzwerke* stehen.

3. **HTTPS-Verkehr (SSL) scannen**

Wählen Sie diese Option, um nicht nur HTTP-Verkehr sondern auch HTTPS-Verkehr zu scannen.

4. **Wählen Sie den Betriebsmodus aus.**

Falls Sie einen Betriebsmodus mit Benutzerauthentifizierung wählen, sollten Sie auch die Benutzer und Gruppen angeben, die auf den HTTP-Proxy zugreifen dürfen. Wenn keine Benutzer oder Gruppen ausgewählt sind, können alle den HTTP-Proxy nutzen, die sich erfolgreich am Verzeichnisdienst angemeldet haben.

Die folgenden Betriebsmodi stehen zu Verfügung:

- **Standard:** Im Standardmodus lauscht der Proxy nach Client-Anfragen standardmäßig auf Port 8080 und lässt jeden Client zu, der sich in einem Netzwerk befindet, das im Feld *Zugelassene Netzwerke* aufgeführt ist. In diesem Modus muss der HTTP-Proxy in der Browser-Konfiguration von jedem Client angegeben sein.
- **Active Directory SSO:** Wählen Sie diese Option, wenn Sie *Active Directory Single Sign-On* (SSO) auf der Registerkarte *Benutzer >> Authentifizierung >> Server* konfiguriert haben. Das hat den Effekt, dass NTLM-Benutzerauthentifizierung verwendet wird, um Clients zu authentifizieren. Beachten Sie, dass die Funktion nur mit Internet Explorer garantiert wird. In diesem Modus muss der HTTP-Proxy in der Browser-Konfiguration von jedem Client angegeben sein. Sie können Benutzer und/oder Gruppen auswählen oder anlegen, die den Proxy verwenden dürfen, und sie im Feld *Benutzer/Gruppen* hinzufügen.
- **Apple OpenDirectory SSO:** Wählen Sie diese Option, wenn Sie *LDAP* auf der Registerkarte *Benutzer >> Authentifizierung >> Server* konfiguriert haben und Sie Apple OpenDirectory verwenden. Damit der Proxy richtig funktioniert, müssen Sie zusätzlich eine MAC OS X Single

Sign-On Kerberos Schlüsseldatei auf der Registerkarte *Web Security >> HTTP/S >> Erweitert* hochladen. In diesem Modus muss der HTTP-Proxy in der Browser-Konfiguration von jedem Client angegeben sein. Sie können Benutzer und/oder Gruppen auswählen oder anlegen, die den Proxy verwenden dürfen, und sie im Feld *Benutzer/Gruppen* hinzufügen. Beachten Sie, dass der Safari-Browser SSO nicht unterstützt.

- **Einfache Benutzerauthentifizierung:** In diesem Modus muss sich jeder Client aus dem Netzwerk am HTTP-Proxy authentifizieren. Weitere Informationen zu den unterstützten Authentifizierungsmethoden finden Sie im Menü *Benutzer >> Authentifizierung* beschrieben. Beachten Sie, dass in den Browsern der Proxy für den Zugriff definiert werden muss. In diesem Modus muss der HTTP-Proxy in der Browser-Konfiguration von jedem Client angegeben sein. Sie können Benutzer und/oder Gruppen auswählen oder anlegen, die den Proxy verwenden dürfen, und sie im Feld *Benutzer/Gruppen* hinzufügen.
- **eDirectory SSO:** Wählen Sie diesen Modus, wenn Sie *eDirectory* auf der Registerkarte *Benutzer >> Authentifizierung >> Server* konfiguriert haben. In diesem Modus muss der HTTP-Proxy in der Browser-Konfiguration von jedem Client angegeben sein. Sie können Benutzer und/oder Gruppen auswählen oder anlegen, die den Proxy verwenden dürfen, und sie im Feld *Benutzer/Gruppen* hinzufügen.

Hinweis – Für die Modi *eDirectory* und *Active Directory Single Sign-On (SSO)*, speichert der Proxy die IP-Adressen und Berechtigungen der anfragenden Clients bis zu fünfzehn Minuten; für *Apple OpenDirectory SSO* speichert er nur die Gruppeninformationen. Das Zwischenspeichern reduziert die Last auf den Authentifizierungsservern, aber es bedeutet auch, dass es bis zu fünfzehn Minuten dauern kann, bis Änderungen an Benutzern, Gruppen oder dem Anmeldestatus der zugreifenden Benutzer vom Proxy berücksichtigt werden.

- **Transparent:** Im Transparenzmodus werden alle Verbindungen von Client-Browseranwendungen auf Port 80 (bzw. Port 443 wenn SSL aktiviert ist) abgefangen und an den Proxy weitergeleitet, ohne client-seitige Konfiguration. Der Vorteil dieses Modus' ist, dass keine zusätzliche Verwaltung oder client-seitige Konfiguration nötig ist, der Nachteil hingegen ist, dass nur HTTP-Anfragen (Port 80) verarbeitet werden

können. Deshalb werden die Proxy-Einstellungen im Client-Browser unwirksam, wenn Sie *Transparent* als Modus wählen.

Volltransparenzmodus (optional): Wählen Sie die Option *Volltransparenzmodus*, um die Quell-IP der Clients zu erhalten, anstatt sie durch die IP der Firewall zu ersetzen. Das ist nützlich, wenn Ihre Clients öffentliche IP-Adressen verwenden, die nicht durch den Proxy verschleiert werden sollen.

Hinweis – Im Transparenzmodus entfernt der Proxy NTLM-Authentifizierungsheader von HTTP-Anfragen. Darüberhinaus kann der Proxy keine FTP-Anfragen in diesem Modus verarbeiten. Wenn Ihre Clients auf solche Dienste zugreifen wollen, müssen Sie den Port (21) im Paketfilter öffnen. Beachten Sie auch, dass manche Webserver einige Daten über einen anderen Port als Port 80 übermitteln, im besonderen Streaming-Video- und -Audiodaten. Diese Anfragen werden nicht beachtet, wenn der Proxy im Transparenzmodus arbeitet. Um solchen Verkehr zu unterstützen, müssen Sie entweder einen anderen Modus wählen oder eine explizite Paketfilterregel anlegen, die diesen Verkehr erlaubt.

- **Transparent mit Authentifizierung:** Benutzen Sie diesen Modus, damit Benutzer sich authentifizieren müssen, während der Proxy transparent arbeitet. Wenn Benutzer eine Website zum ersten Mal öffnen, wird ihnen eine Webseite präsentiert, auf der sie Benutzername und Kennwort eingeben müssen. Dieser Modus ermöglicht benutzernamenbasierte Verfolgung (engl. *tracking*), Berichterstellung und Surfen ohne client-seitige Browserkonfiguration. Darüberhinaus können Sie Nutzungsbedingungen einrichten, die dann zusätzlich auf der Anmeldeseite angezeigt werden und von den Benutzern akzeptiert werden müssen, bevor sie fortfahren können. Weitere Informationen zu den Nutzungsbedingungen finden Sie im Kapitel *Verwaltung >> Anpassung >> HTTP/S-Proxy*. Sie können Benutzer und/oder Gruppen auswählen oder anlegen, die den Proxy verwenden dürfen, und sie im Feld *Benutzer/Gruppen* hinzufügen.

5. Klicken Sie **Übernehmen**.

Ihre Einstellungen werden gespeichert.

Wichtiger Hinweis – Wenn SSL-Scanning zusammen mit dem Transparenzmodus aktiviert ist, werden einige Verbindungen nicht zustande kommen, z. B.

SSL-VPN-Tunnel. Um SSL-VPN-Verbindungen zu ermöglichen, fügen Sie den entsprechenden Zielrechner zur *Transparenzmodus-Ausnahmen* hinzu (siehe *Web Security >> HTTP/S-Proxy >> Erweitert*).

Antivirus/Schadsoftware

Auf der Registerkarte *Web Security >> HTTP >> Antivirus/Schadsoftware* können Sie Optionen konfigurieren, die darauf abzielen, Ihr Netzwerk vor Internetverkehr zu schützen, der gefährlichen Inhalt wie Viren, Würmer oder andere Schadsoftware enthält.

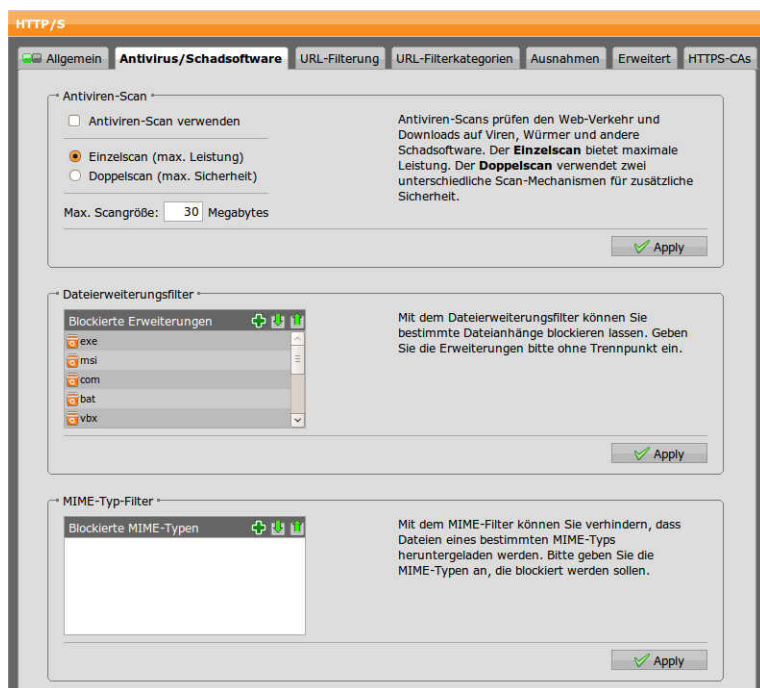


Figure 10.2 HTTP-Proxy: Konfiguration der Antiviren- und Schadsoftware-Einstellungen

Antiviren-Scan

Wählen Sie die Option *Antiviren-Scan verwenden*, um eingehenden und ausgehenden Datenverkehr zu scannen. Astaro Security Gateway bietet für höchstmöglichen Schutz mehrere Antivirus-Mechanismen:

- **Einzelscan:** Standardeinstellung, die maximale Leistung bietet.
- **Doppelscan:** Bietet maximale Erkennungsrate, indem aller Internetverkehr von zwei verschiedenen Virenscannern gescannt wird.

Max. Scangröße: Geben Sie die maximale Größe der Dateien an, die vom Antivirus-Mechanismus gescannt werden soll. Dateien, die größer sind als der angegebene Wert, werden nicht gescannt.

Klicken Sie *Übernehmen*, um Ihre Einstellungen zu speichern.

Dateierweiterungsfilter

Diese Funktion filtert bestimmte Dateitypen basierend auf Ihren Erweiterungen (z.B. ausführbare Binärdateien) aus dem Internetverkehr heraus, wenn diese eine Dateierweiterung besitzen, die in der Liste *Blockierte Erweiterungen* aufgeführt ist. Sie können weitere Dateierweiterungen hinzufügen oder solche Erweiterungen aus der Liste löschen, die nicht blockiert werden sollen. Um eine Dateierweiterung hinzuzufügen, klicken Sie auf das Plus-Symbol im Feld *Blockierte Erweiterungen* und geben Sie die Dateierweiterung ein, die blockiert werden soll, z. B. `exe` (ohne den Punkt als Trennzeichen). Klicken Sie *Übernehmen*, um Ihre Einstellungen zu speichern.

Hinweis – Verschlüsselte zip-Archive können nicht nach schädlichem Inhalt durchsucht werden und passieren den Virusscanner ungehindert. Um Ihr Netzwerk vor Schadsoftware aus verschlüsselten zip-Dateien zu schützen, sollten Sie in Betracht ziehen, zip-Dateien gänzlich zu blockieren.

MIME-Typ-Filter

Um einen MIME-Typ hinzuzufügen, der blockiert werden soll, klicken Sie auf das Plus-Symbol im Feld *Blockierte MIME-Typen* und geben Sie den MIME-Typ an (z. B. `image/gif`). Es ist möglich, Platzhalter (*) zu verwenden, z. B. `audio/*`.

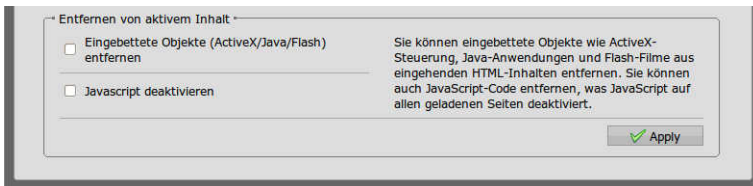


Figure 10.3 HTTP-Proxy: Konfiguration für das Entfernen von aktivem Inhalt

Entfernen von aktivem Inhalt

Im Abschnitt *Entfernen von aktivem Inhalt* können Sie einstellen, dass spezifischer Internetinhalt, wie eingebettete Objekte auf Webseiten, automatisch entfernt wird (z. B. Multimedia-Dateien). Sie können die folgenden Einstellungen vornehmen:

- **Eingebettete Objekte entfernen:** Wenn Sie diese Funktion wählen, werden alle <OBJECT>-Tags aus HTML-Seiten entfernt, wodurch dynamische Inhalte wie ActiveX, Flash oder Java aus dem eingehenden HTTP-Verkehr gelöscht wird.
- **Javascript deaktivieren:** Wenn Sie diese Funktion wählen, werden alle <SCRIPT>-Tags aus HTML-Seiten entfernt, wodurch Funktionen deaktiviert werden, die in HTML-Seiten eingebettet oder eingebunden sind.

URL-Filterung

Auf der Registerkarte *Web Security >> HTTP/S >> URL-Filterung* können Sie die Grundeinstellungen für die Zugriffskontrolle für bestimmte Arten von Websites vornehmen.

Sie können die folgenden Einstellungen vornehmen:

- **Zulassen/Blockieren-Auswahl:** Entscheiden Sie aus, ob Ihre ausgewählten Website-Kategorien zugelassen oder blockiert werden sollen. Die folgenden Varianten sind möglich:
 - **Inhalt zulassen, der die unten stehenden Kriterien nicht erfüllt:** Wenn Sie diese Option wählen, werden Ihre ausgewählten Website-Kategorien blockiert, während alle anderen Kategorien (die nicht ausgewählt) zugelassen werden.
 - **Inhalt blockieren, der die unten stehenden Kriterien nicht erfüllt:** Wenn Sie diese Option wählen, werden alle Website-Kategorien blockiert, außer jenen, die Sie ausgewählt haben.

Die Standardeinstellung ist *Zulassen*. Wenn Sie zu *Blockieren* wechseln, beachten Sie, dass dadurch die untenstehenden Optionen in ihrer Bedeutung „umgedreht“ werden, was sich daran zeigt, dass die Begriffe von *Blockieren* auf *Zulassen* wechseln und umgekehrt.

Hinweis – Um auf die Kategorisierungsdatenbank zugreifen zu können, müssen die TCP-Ports 6000 oder 80 in Upstream-Firewalls offen sein. Wenn

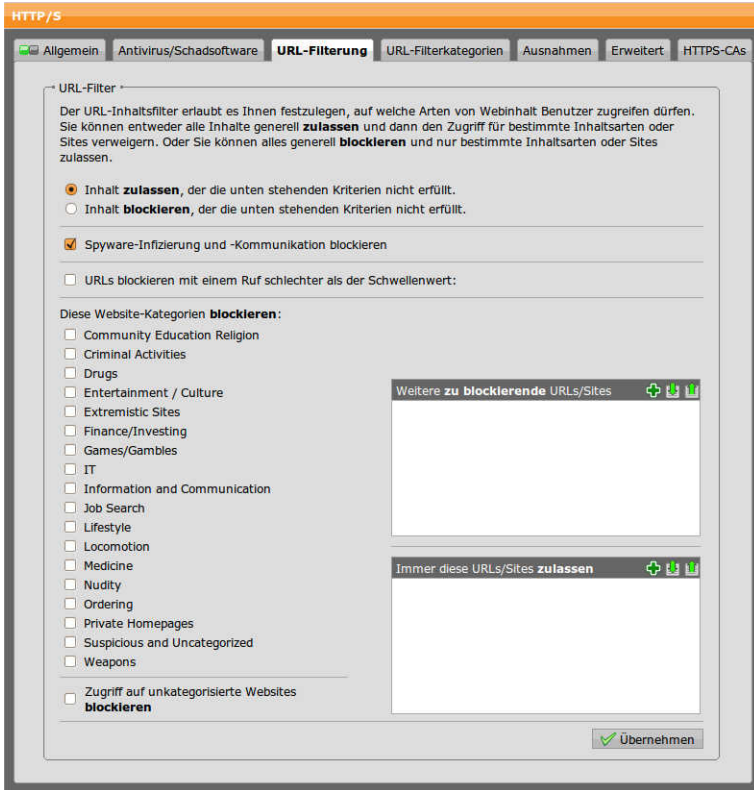


Figure 10.4 HTTP-Proxy: Konfiguration der URL-Filterung

ein übergeordneter Proxy (Parent-Proxy) konfiguriert ist, werden alle Anfragen an die Datenbank über den übergeordneten Proxy geleitet.

- **Spyware-Infizierung und -Kommunikation blockieren:** Bei Spyware handelt es sich um Software, die Systeme ausspionieren und Informationen über Benutzerverhalten an Unbefugte übermitteln kann, ohne dass der Benutzer davon erfährt. Diese Funktion entdeckt und blockiert Spyware, die vom Server auf den Client geladen wird. Dadurch wird verhindert, dass Computer in Ihrem Netzwerk mit neuer Spyware infiziert werden. Zusätzlich erkennt und unterbindet diese Funktion Datenverkehr von bereits auf einem Client installierter Spyware. Die Spyware ist somit nicht mehr in

der Lage, die von ihr gesammelten Informationen an das Internet weiterzuleiten. Beachten Sie, dass diese Option nur verfügbar ist, wenn die erste Option auf dieser Seite auf *Zulassen* gestellt ist.

Hinweis – Die Unterkategorie *Spyware* kann keiner der 18 verfügbaren Gruppen zugeordnet werden, deshalb kann sie nur durch die Option *Spyware-Infizierung und -Kommunikation blockieren* aktiviert werden.

- **URLs blockieren mit einem Ruf schlechter als der Schwellenwert:** Websites können in folgende Klassen unterteilt werden: *Vertrauenswürdig* (engl. *trusted*), *Neutral*, *Verdächtig* (engl. *Suspicious*) oder böseartig, wobei die letzte nicht aufgeführt ist (da dadurch alle Seiten zugelassen würden, was der Nichtverwendung der Schwellenwert-Option entspricht). Unklassifizierte Websites werden als *Unüberprüft* (engl. *Unverified*) eingestuft. Sie können bestimmen, welchen Ruf eine Website haben muss, um für Ihr Netzwerk erreichbar zu sein. Websites unterhalb dieses Schwellenwerts werden blockiert. Beachten Sie, dass diese Option nur verfügbar ist, wenn die erste Option auf dieser Seite auf *Zulassen* gestellt ist. Weitere Informationen zu dem Ruf von Websites finden Sie unter <http://www.trustedsource.org>.
- **Diese Website-Kategorien blockieren:** Wählen Sie die Website-Kategorien, die blockiert werden sollen. Beachten Sie, dass sich diese Option zu *Diese Website-Kategorien zulassen* ändert, wenn die erste Option auf dieser Seite auf *Blockieren* gestellt ist. Jede Kategorie enthält mehrere Unterkategorien. Die Kategorien können auf der Registerkarte *Web Security* >> *HTTP/S* >> *URL-Filterkategorien* editiert werden.

Hinweis – Wenn Sie der Meinung sind, dass eine Website falsch kategorisiert ist, dann können Sie in Astaros URL-Meldeformular²⁴ neue Kategorien vorschlagen.

- **Zugriff auf unkategorisierte Websites blockieren:** Verhindert, dass der Browser Internetseiten mit unbekanntem Inhalt öffnet. Diese Funktion kann als zusätzliche Sicherung verstanden werden, falls eine möglicherweise unzulässige Seite noch nicht als solche kategorisiert wurde. Diese Funktion bewahrt den Benutzer vor sogenannten Phishing-Angriffen.

²⁴ <http://www.astaro.com/tool/urlreport>

Phishing Mails enthalten in der Regel verdächtige Links zu gefälschten Websites, wo der Benutzer dazu gebracht wird, persönliche und vertrauliche Informationen preis zu geben. Falls diese Links noch nicht als schädlich klassifiziert wurden, werden sie entweder als *unkategorisiert* oder *verdächtig* eingestuft. Durch Aktivieren dieser Option werden diese Kategorien blockiert. Selbst wenn eine Phishing-Nachricht zugestellt wurde, können Benutzer dadurch eine betrügerische URL nicht öffnen. Beachten Sie, dass sich diese Option zu *Zugriff auf unkategorisierte Websites zulassen* ändert, wenn die erste Option auf dieser Seite auf *Blockieren* gestellt ist.

- Weitere zu blockierende URLs/Seiten:** Wenn Sie ein spezifische URL oder Website unabhängig von ihrer Kategorie blockieren wollen, geben Sie sie hier ein. Das bewirkt, dass hier aufgeführte Websites blockiert werden können, selbst wenn sie zu einer Kategorie gehören, die Sie zulassen. Reguläre Ausdrücke sind hier erlaubt (z.B. `^https?://.*wikipedia.org`). Um genau eine URL zu blockieren, geben Sie die komplette URL ein (z.B. `http://www.wikipedia.org`). Beachten Sie, dass Ausdrücke wie `wikipedia.org` nicht nur auf die URL passen sondern auch auf Suchergebnisse und Teile von ähnlichen URLs, was zu versehentlich blockierten Seiten führen kann.
Diese Option ändert sich zu *Weitere zugelassene URLs/Sites*, wenn die erste Option auf dieser Seite auf *Blockieren* gestellt ist.
- Immer diese URLs/Seiten zulassen:** Wenn Sie eine spezifische URL oder Website explizit zulassen wollen, unabhängig von ihrer Kategorie oder einem Eintrag in der Blockierungsliste, geben Sie sie hier ein. Beachten Sie, dass sich diese Option zu *Immer diese URLs/Seiten blockieren* ändert, wenn die erste Option auf dieser Seite auf *Blockieren* gestellt ist.

URL-Filterkategorien

Auf der Registerkarte *Web Security* >> *HTTP/S* >> *URL-Filterkategorien* können Sie die Zuordnung von den Kategoriengruppen, die auf der Registerkarte *Web Security* >> *HTTP/S* >> *URL-Filterung* verwendet werden, zu ihren Unterkategorien anpassen. Astaro Security Gateway kann 60 unterschiedliche Kategorien von Websites identifizieren und den Zugriff auf sie blockieren. Ausgeklügelte URL-Klassifizierungsmethoden stellen die Genauigkeit und Vollständigkeit bei der Einschätzung fragwürdiger Websites sicher. Wenn ein Benutzer eine Website aufruft, die nicht in der Datenbank vorliegt, wird die URL zu Webcrawlern gesendet und automatisch klassifiziert.

Hinweis – Wenn Sie der Meinung sind, dass eine Website falsch kategorisiert sind, dann können Sie über Astaros URL-Meldeformular²⁵ neue Kategorien vorschlagen.

Um Website-Kategorien einer Kategoriengruppe zuzuweisen, gehen Sie folgendermaßen vor:

1. **Klicken Sie *Edit* in der Kategoriengruppe, die Sie ändern wollen.**
Das Dialogfenster *Filterkategorie bearbeiten* wird geöffnet.
2. **Wählen Sie die Unterkategorien aus.**
Markieren Sie das Auswahlkästchen von Unterkategorien, die Sie hinzufügen möchten, oder entfernen Sie die Markierung von Unterkategorien, die aus der Gruppe entfernt werden soll.
3. **Klicken Sie *Speichern*.**
Die Gruppe wird mit Ihren Einstellungen aktualisiert.

Alternativ können Sie auch eine neue Filterkategorie anlegen. Gehen Sie folgendermaßen vor:

1. **Klicken Sie auf die Schaltfläche *Neue Filterkategorie* oben auf der Seite.**
Das Dialogfenster *Filterkategorie erstellen* wird geöffnet.
2. **Geben Sie einen Namen ein.**
Geben Sie einen aussagekräftigen Namen für die neue Filterkategorie ein.
3. **Wählen Sie die Kategorien.**
Markieren Sie die Auswahlkästchen der Kategorien, die Sie zur Gruppe hinzufügen wollen.
4. **Klicken Sie *Speichern*.**
Die Gruppe wird mit Ihren Einstellungen aktualisiert.

Ausnahmen

Auf der Registerkarte *Web Security* >> *HTTP/S* >> *Ausnahmen* können Sie Netzwerke, Benutzer/Gruppen und Domänen definieren, die nicht gefiltert/blockiert werden sollen, d. h. sie stehen auf der Whitelist (dt. weiße Liste, Positivliste). Alle Einträge in den Listen auf dieser Seite sind von bestimmten Web-Security-Diensten ausgenommen.

²⁵ <http://www.astaro.com/tool/urlreport>

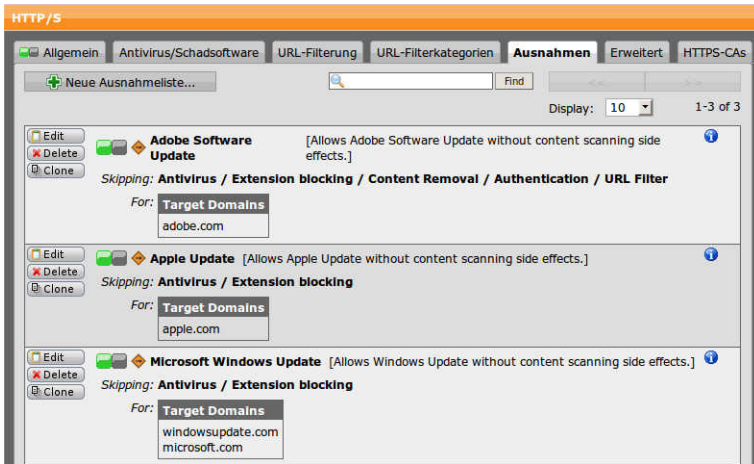


Figure 10.5 HTTP-Proxy: Ausnahmenliste

Um eine Ausnahme zu definieren, gehen Sie folgendermaßen vor:

1. Klicken Sie auf der Registerkarte **Ausnahmen** auf **Neue Ausnahmeliste**. Das Dialogfenster *Ausnahmeliste erstellen* wird geöffnet.
2. Nehmen Sie die folgenden Einstellungen vor:

Name: Geben Sie einen aussagekräftigen Name für diese Ausnahmeliste ein.

Diese Prüfungen ausnehmen: Wählen Sie die Sicherheitsprüfungen, von denen diese Liste ausgenommen werden soll:

 - **Authentifizierung:** Wenn der HTTP-Proxy im Authentifizierungsmodus läuft, dann können Sie die Authentifizierung für Quellrechner/-netzwerke, Zieldomänen oder Benutzer/Gruppen aussetzen.
 - **Zwischenspeichern:** Wählen Sie diese Option, um die Zwischenspeicherung für spezifische Domänen oder Quellrechner/-netzwerke zu deaktivieren.
 - **Antivirus:** Wählen Sie diese Option, um die Virenschannfunktion zu deaktivieren, die Nachrichten nach unerwünschten Inhalten wie Viren, Trojanischen Pferden und Ähnlichen durchsucht.
 - **Erweiterungsblockierung:** Wählen Sie diese Option, um den Dateierweiterungsfilter zu deaktivieren, der Inhalte blockiert, wenn sie bestimmte Dateierweiterungen enthalten.

- **MIME-Typ-Blockierung:** Wählen Sie diese Option, um den MIME-Typ-Filter zu deaktivieren, der Inhalte blockiert, die einen bestimmten MIME-Typ haben.
- **URL-Filter:** Wählen Sie diese Option, um den URL-Filter zu deaktivieren, der den Zugriff auf bestimmte Website kontrolliert.
- **Inhaltse Entfernung:** Wählen Sie diese Option, um die Entfernung von bestimmten Inhalten, wie eingebettete Objekte (z. B. Multimedia-Dateien) oder JavaScript, auf Webseiten auszulassen.
- **Zertifikat-Vertrauensprüfung (Trust Check):** Wählen Sie diese Option, um die Vertrauensprüfung für das HTTPS-Server-Zertifikat auszulassen.
- **Zertifikatsdatumsprüfung:** Wählen Sie diese Option, um die Überprüfung, ob das Zertifikatsdatum gültig ist, auszulassen.

Für diese Quellrechner/-netzwerke: Wählen Sie diese Option, um Quellrechner/-netzwerke hinzufügen, die von Sicherheitsprüfungen dieser Ausnahmeregel ausgenommen werden sollen. Geben Sie die entsprechenden Rechner oder Netzwerke in das Feld *Rechner/Netzwerke* ein, das nach Markierung des Auswahlkästchens geöffnet wird.

Diesen URLs entsprechend: Wählen Sie diese Option, um Zieldomänen hinzufügen, die von den Sicherheitsprüfungen dieser Ausnahmeregel ausgenommen werden sollen. Fügen Sie die entsprechenden Domänen zum Feld *Zieldomänen* hinzu, das nach Markierung des Auswahlkästchens geöffnet wird. Beispiel: `^https?/[^\.]*\.domain.com` deckt HTTP(S)-Verbindungen zu allen Subdomänen dieser Domäne ab.

Diese Benutzer/Gruppen: Wählen Sie diese Option, um Benutzer oder Benutzergruppen hinzufügen, die von den Sicherheitsprüfungen dieser Ausnahmeregel ausgenommen werden sollen. Geben Sie die entsprechenden Benutzer oder Gruppen im Feld *Benutzer/Gruppen* an, das nach Markierung des Auswahlkästchens geöffnet wird.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die Ausnahme hinzu.

3. Klicken Sie *Speichern*.

Anschließend wird die neue Ausnahmeliste zur Liste *Ausnahmen* hinzugefügt.

Um eine Ausnahmeliste zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Erweitert

Die Registerkarte *Web Security >> HTTP/S >> Erweitert* bietet zusätzliche Konfigurationsoptionen für den HTTP/S-Proxy wie z. B. Zwischenspeicherung (engl. *Caching*) oder Porteinstellungen.

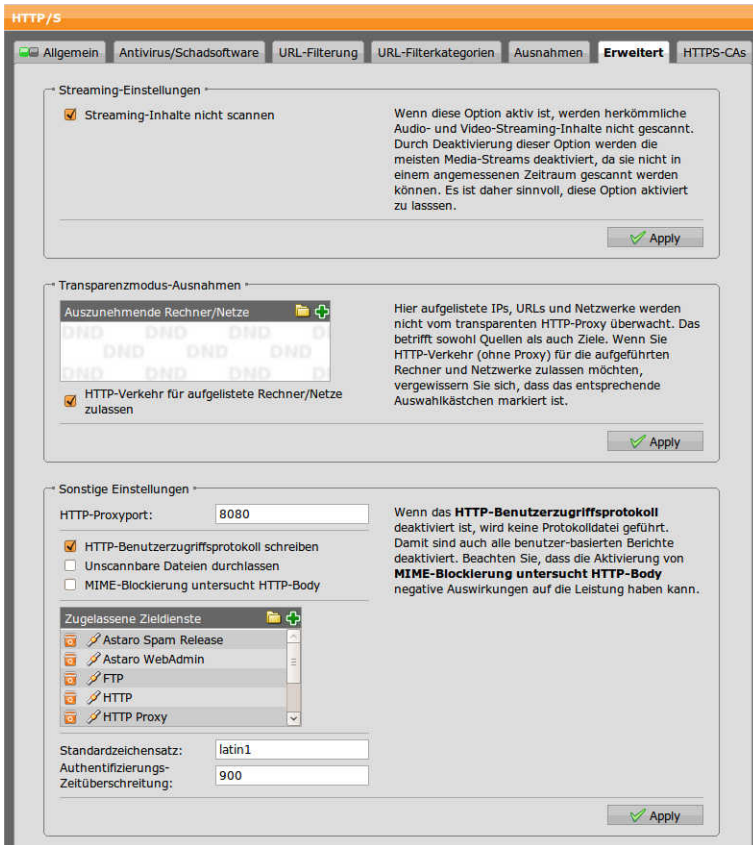


Figure 10.6 HTTP-Proxy: Erweiterte Einstellungen, Teil 1

Streaming-Einstellungen

Streaming-Inhalte nicht scannen: Wenn diese Option aktiviert ist, werden typische Audio- und Video-Streaminginhalte nicht auf ihren Inhalt hin gescannt. Das Abschalten dieser Option wird die meisten Mediastreams praktisch deaktivieren, da sie nicht in vertretbarer Zeit gescannt werden können. Daher wird empfohlen, diese Option eingeschaltet zu lassen.

Transparenzmodus-Ausnahmen

Diese Option ist nur von Bedeutung, wenn der HTTP-Proxy im Betriebsmodus *Transparent* läuft. Rechner und Netzwerke, die im Feld *Auszunehmende Rechner/Netze* aufgeführt sind, deren Netzwerkverkehr wird dann nicht vom HTTP/S-Proxy überwacht. Das betrifft sowohl Quell- als auch Zielrechner/-netzwerke. Um dennoch HTTP/S-Datenverkehr (ohne Proxy) für alle diese Rechner und Netzwerke zu erlauben, wählen Sie die Option *HTTP-Verkehr für aufgelistete Rechner/Netze zulassen*. Wenn Sie das Auswahlkästchen nicht markieren, müssen Sie spezifische Paketfilterregeln für die hier aufgeführten Rechner und Netzwerke definieren.

Sonstige Einstellungen

HTTP Proxy Port: In dem Eingabefeld wird die Portnummer für Clientanfragen an den HTTP-Proxy eingestellt. Standardmäßig ist der Port 8080 eingetragen.

Hinweis – Die Option ist nur gültig, wenn der Proxy nicht im Transparenzmodus arbeitet.

HTTP-Benutzerzugriffsprotokoll schreiben: Es werden Benutzerdaten protokolliert, unter anderem besuchte URLs, Benutzernamen und IP-Adressen von Clients. Wenn diese Funktion ausgeschaltet wird, werden die Benutzer-/IP-Informationen nur für blockierte Seiten ins HTTP-Proxy-Protokoll geschrieben.

Unscannbare Dateien durchlassen: Wählen Sie diese Option, um Dateien zum Empfänger durchzuleiten, obwohl sie nicht gescannt werden konnten.

MIME-Blockierung untersucht HTTP-Body: Der HTTP-Verkehr wird nach blockierten MIME-Typen durchsucht. Beachten Sie, dass das Einschalten dieser Funktion sich negativ auf die Leistung des Systems auswirken kann.

Zugelassene Zieldienste: In diesem Feld werden die Dienste eingestellt, auf die der HTTP-Proxy zugreifen darf. Standardmäßig sind bereits die Dienste mit Ports enthalten, zu denen eine Verbindung als sicher gilt und die in der Regel von Browsern genutzt werden: *HTTP* (port 80), *HTTPS* (port 443), *FTP* (port 21), *LDAP* (port 389), *LDAP-SSL* (port 636), *HTTP Proxy* (port 8080), *Astaro Spam Release* (ports 3840-4840) und *Astaro WebAdmin* (port 4444).

Standardzeichensatz: Diese Option wirkt sich darauf aus, wie der Proxy Dateinamen im Fenster *Download Manager* anzeigt. URLs (und Dateinamen, auf die sie vielleicht verweisen), die in ausländischen Zeichensätzen kodiert sind, werden von UTF-8 in den hier definierten Zeichensatz umgewandelt, es sei denn, der Server übermittelt einen anderen Zeichensatz. Wenn Sie sich in einem Land oder einer Region befinden, die einen Zwei-Byte-Zeichensatz verwendet, sollten Sie diese Option auf den „nativen“ Zeichensatz für dieses Land/diese Region setzen.

Übergeordneter HTTP-Proxy

☐ Übergeordneten Proxy verwenden

Rechner:  

Port:

☐ Proxy-Authentifizierung verwenden

Benutzer:

Kennwort:

Wiederholen:

Bei Verwendung eines übergeordneten Proxy (auch Parent oder Upstream Proxy) führt das System alle Anfragen über diesen Proxy durch. Wenn der übergeordnete Proxy Authentifizierung erfordert, geben Sie den erforderlichen Benutzernamen und das Kennwort ein.

 **Apply**

HTTP-Zwischenspeicherung

☒ Zwischenspeichern aktivieren

☐ SSL-Inhalte zwischenspeichern

☐ Zwischenspeicherinhalt der Cookies enthält

 **Zwischenspeicher leeren**

Bei aktivierter Zwischenspeicherung (Cache) speichert der Proxy heruntergeladene HTTP-Inhalte und legt diese in einem indizierten Zwischenspeicher zum schnelleren Abruf ab. Dieser Zwischenspeicher kann geleert werden, indem Sie auf **Zwischenspeicher leeren** klicken.

 **Apply**

MAC OS X Single Sign-On

Schlüsseldatei hochladen: 

Wenn Sie vorhaben, Apple OpenDirectory Single Sign-On zu verwenden, legen Sie bitte eine Kerberos Schlüsseldatei auf dem Server an und stellen Sie sie hier bereit.

 **Apply**

Figure 10.7 HTTP-Proxy: Erweiterte Einstellungen, Teil 2

Übergeordneter HTTPProxy

Ein übergeordneter Proxy (auch *Parent* oder *Upstream* Proxy) wird in Ländern benötigt, in denen der Zugang zum Internet nur über einen staatlich kontrollierten Proxy erlaubt ist. Falls Ihre Sicherheitsbestimmungen die Nutzung eines übergeordneten Proxy erforderlich machen, so können Sie diesen hier durch Angabe einer Rechnerdefinition und eines Ports konfigurieren.

Übergeordneten Proxy verwenden: Wählen Sie diese Option, um einen übergeordneten Proxy zu verwenden. Geben Sie einen Rechnernamen und den Port des Proxy ein.

Dieser Proxy erfordert Authentifizierung: Falls der übergeordnete Proxy Authentifizierung erfordert, geben Sie den Benutzernamen und das Kennwort hier ein.

HTTP-Zwischenspeicherung

Zwischenspeichern aktivieren: Wenn diese Option aktiviert ist, hält der HTTP-Proxy einen Zwischenspeicher auf Festplatte vor, um Anfragen zu häufig besuchten Webseiten schneller beantworten zu können.

SSL-Inhalte zwischenspeichern: Wählen Sie diese Option, um SSL-verschlüsselte Daten ebenfalls – unverschlüsselt – auf der Festplatte zu speichern.

Zwischenspeicherinhalt der Cookies enthält: Cookies werden oft für Authentifizierungszwecke verwendet. Wenn diese Option aktiviert ist, werden HTTP-Antworten, die Cookies enthalten, ebenfalls zwischengespeichert. Dieses Vorgehen kann aber zu Datenschutz-Problemen führen, da Benutzer, die auf die gleiche Seite zugreifen wollen, sehr wahrscheinlich die Seite aus dem Zwischenspeicher erhalten, welche dann den Cookie eines anderen Benutzers enthält.

Wichtiger Hinweis – Das Zwischenspeichern von SSL- oder Cookie-Inhalten stellt ein wichtiges Sicherheitsproblem dar, da die Inhalte von jedem Benutzer mit SuperAdmin-Rechten eingesehen werden kann.

Zwischenspeicher leeren: Sie können alle zwischengespeicherten Seiten löschen, indem Sie *Zwischenspeicher leeren* klicken.

MAC OS X Single Sign-On

Wenn Sie *Apple OpenDirectory SSO* als Authentifizierungsmethode benutzen, müssen eine MAC OS X Single Sign-On Kerberos Schlüsseldatei hochladen, damit die Authentifizierung funktioniert. Generieren Sie die Schlüsseldatei und laden Sie sie durch einen Klick auf *Schlüsseldatei hochladen* hoch. Für nähere Informationen dazu, wie Sie die Schlüsseldatei generieren können, lesen Sie bitte die Kerberos-Dokumentation.

HTTPS-CAs

Auf der Registerkarte *Web Security >> HTTP/S >> HTTPS-CAs* können Sie die Signierungs- und Verifizierungs-Zertifizierungsstellen (CAs, Certificate Authorities) für HTTPS-Verbindungen verwalten.

Signierungs-CA

In diesem Abschnitt können Sie Ihr Signierungs-CA-Zertifikat hochladen, das Signierungs-CA-Zertifikat neu erstellen oder das vorhandene Signierungs-CA-Zertifikat herunterladen. Standardmäßig wird das Signierungs-CA-Zertifikat aus den Informationen erzeugt, die während der Grundkonfiguration eingegeben wurden, d. h. es stimmt mit den Informationen auf der Registerkarte *Verwaltung >> Systemeinstellungen >> Organisatorisches* überein, es sei denn, es wurden inzwischen Änderungen vorgenommen.

Um ein neues Signierungs-CA-Zertifikat hochzuladen, gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Schaltfläche *Hochladen*.

Das Dialogfenster *Upload PKCS#12 Certificate File* wird geöffnet.

2. Gehen Sie zu der Datei, die Sie hochladen wollen.

Klicken Sie auf das Ordnersymbol neben dem *Datei*-Feld, klicken Sie *Durchsuchen* im erscheinenden Dialogfenster *Upload File*, wählen Sie das hochzuladende Zertifikat aus und klicken Sie *Save*.

Sie können nur Zertifikate im PKCS#12-Format hochladen, die kennwortgeschützt sind.

3. Geben Sie das Kennwort ein.

Geben Sie das Kennwort zweimal in die entsprechenden Felder ein und klicken Sie *Speichern*.

Das neue Signierungs-CA-Zertifikat wird installiert.

Um Ihr Signierungs-CA-Zertifikat neu zu erstellen, gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Schaltfläche *Neu erstellen*.

Das Dialogfenster *Create New Signing CA* wird geöffnet.

2. Ändern Sie die Informationen.

Ändern Sie die angegebenen Informationen nach Ihren Bedürfnissen und klicken Sie *Speichern*.

Das neue Signierungs-CA-Zertifikat wird erstellt. Die Informationen zur Signierungs-CA im *Signierungs-CA*-Bereich ändert sich entsprechend.

Um das Signierungs-CA-Zertifikat herunterzuladen, gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Schaltfläche *Herunterladen*.

Das Dialogfenster *Download Certificate File* wird geöffnet.

2. Wählen Sie das Dateiformat aus, das Sie herunterladen wollen.

Sie können zwischen zwei verschiedenen Formaten wählen:

- **PKCS#12:** Dieses Format ist verschlüsselt, deshalb geben Sie bitte ein Kennwort ein.
- **PEM:** Dieses Format ist unverschlüsselt.

3. Klicken Sie *Save*.

Klicken Sie *Save*, um die Datei zu speichern.

Wenn Sie für Ihre internen Webserver Zertifikate verwenden, die von einer eigenen CA signiert sind, ist es ratsam, dieses CA-Zertifikat in WebAdmin als Vertrauenswürdige Zertifizierungsstelle (Trusted Certificate Authority) hochzuladen. Andernfalls wird Benutzern eine Fehlermeldung vom HTTP-Proxy gezeigt, die ihnen mitteilt, dass das Serverzertifikat nicht vertrauenswürdig ist.

Um die Ausstattung der Clients mit dem Proxy-CA-Zertifikat zu vereinfachen, können Benutzer das Zertifikat selbst über <http://passthrough.fw-notify.net/cacert.pem> herunterladen und es in ihrem Browser installieren. Die Website-Anfrage wird direkt vom Proxy akzeptiert und verarbeitet. Deshalb ist es notwendig, zunächst den HTTPS-Proxy auf der Registerkarte *Web Security* >> *Allgemein* zu aktivieren.

Hinweis – Falls der Proxy nicht im Transparenzmodus arbeitet, muss der Proxy im Browser des Benutzers aktiviert werden. Sonst kann der Download-Link nicht erreicht werden.

Wenn das Benutzerportal aktiviert ist, können Benutzer alternativ das Proxy-CA-Zertifikat auch aus dem Benutzerportal, Registerkarte *HTTPS-Proxy*, herunterladen.

HTTPS-Problemen vorbeugen

Wenn Sie HTTPS verwenden, sind Windows-Systemprogramme wie Windows Update und Windows Defender nicht in der Lage, Verbindungen aufzubauen, weil sie mit Systembenutzer-Rechten laufen. Dieser Benutzer vertraut aber standardmäßig nicht der Proxy-CA. Deshalb ist es notwendig, das HTTPS-Proxy-CA-Zertifikat für den Systembenutzer zu importieren. Gehen Sie folgendermaßen vor:

1. **Öffnen Sie unter Windows die Microsoft Management Console (mmc).**
2. **Klicken Sie auf *Datei* im Menü und dann *Snap-In hinzufügen/entfernen*.**
Das Dialogfenster *Snap-In hinzufügen/entfernen* wird geöffnet.
3. **Klicken Sie unten *Hinzufügen*.**
Das Dialogfenster *Eigenständiges Snap-In hinzufügen* wird geöffnet.
4. **Wählen Sie aus der Liste *Zertifikate* und klicken Sie *Hinzufügen*.**
Ein Assistent wird geöffnet.
5. **Wählen Sie *Computerkonto* und klicken Sie *Weiter*.**

6. **Stellen Sie sicher, dass *Lokalen Computer* ausgewählt ist und klicken Sie *Fertigstellen* und dann *Schließen*.**

Das erste Dialogfenster enthält nun das Objekt *Zertifikate (Lokaler Computer)*.

7. **Klicken Sie *OK*.**

Das Dialogfenster wird geschlossen, und der Konsolenstamm enthält nun das Objekt *Zertifikate (Lokaler Computer)*.

8. **Öffnen Sie im *Konsolenstamm* links *Zertifikate >> Vertrauenswürdige Stammzertifizierungsstellen*, rechtsklicken Sie *Zertifikate* und wählen Sie *Alle Aufgaben >> Importieren* aus dem Kontextmenü.**

Der Import-Assistent wird geöffnet.

9. **Klicken Sie *Weiter*.**

Der nächste Schritt wird angezeigt.

10. **Wechseln Sie zu dem zuvor heruntergeladenen *HTTPS-Proxy-CA-Zertifikat*, klicken Sie *Öffnen* und dann *Weiter*.**

Der nächste Schritt wird angezeigt.

11. **Stellen Sie sicher, dass *Alle Zertifikate in folgendem Speicher speichern* ausgewählt ist und klicken Sie *Weiter* und *Fertigstellen*.**

Der Import-Assistent meldet, dass der Import erfolgreich war.

12. **Bestätigen Sie die Meldung des Import-Assistenten.**

Das Proxy-CA-Zertifikat wird nun unter den vertrauenswürdigen Zertifikaten aufgeführt.

13. **Speichern Sie die Änderung.**

Klicken Sie auf *Datei* im Menü und dann *Speichern*, um die Änderung am Konsolenstamm zu speichern.

Nach diesem Importvorgang wird der CA systemweit vertraut, und es sollten keine Verbindungsprobleme aufgrund des HTTPS-Proxys mehr auftreten.

Verifizierungs-CAs

In diesem Bereich können Sie Ihre Verifizierungs-CAs verwalten. Das sind Zertifizierungsstellen, denen Sie generell vertrauen, d. h. Websites, die gültige Zertifikate vorweisen, welche von diesen CAs signiert sind, werden vom HTTPS-Proxy als vertrauenswürdig eingestuft.

Lokale Verifizierungs-CAs: Sie können weitere Verifizierungs-CAs zur untenstehenden CA-Liste hinzufügen. Gehen Sie folgendermaßen vor:

1. **Klicken Sie auf das Ordner-Symbol neben dem Feld *Lokale CA hochladen*.**

Das Dialogfenster *Upload File* wird geöffnet.

2. **Wählen Sie das Zertifikat aus, das Sie hochladen wollen.**

Klicken Sie *Durchsuchen* und wählen Sie das CA-Zertifikat, das Sie hochladen wollen.

3. **Laden Sie das Zertifikat hoch.**

Klicken Sie *Hochladen*, um das gewählte Zertifikat hochzuladen.

Das Zertifikat wird installiert und im Abschnitt *Lokale Verifizierungs-CAs* angezeigt.

Globale Verifizierungs-CAs: Die Liste der hier aufgeführten Verifizierungs-CAs ist identisch zu den Verifizierungs-CAs, die in Mozilla Firefox vorinstalliert sind. Sie können jedoch einen oder alle Verifizierungs-CAs auf der Liste deaktivieren, wenn Sie sie nicht für vertrauenswürdig halten. Um das Zertifikat einer CA zurückzuziehen (engl. *revoke*), klicken Sie auf seine Statusampel. Die Statusampel wird daraufhin rot und der HTTPS-Proxy wird keine Websites mehr zulassen, die von dieser CA signiert sind.

Tipp – Klicken Sie auf das blaue Infosymbol, um den Fingerabdruck der CA zu sehen.

Der HTTPS-Proxy zeigt Clients eine Fehlerseite mit dem Hinweis „Blocked Content“, wenn die CA unbekannt oder deaktiviert ist. Sie können jedoch eine Ausnahme für solche Seiten anlegen: entweder über den Link *Ausnahme anlegen* auf der Fehlerseite des Proxys oder über die Registerkarte *Web Security* >> *HTTP/S* >> *Ausnahmen*.

Hinweis – Wenn Sie auf den Link *Ausnahme anlegen* auf der Fehlerseite des Proxys klicken, wird ein Dialogfenster zur Anmeldung präsentiert. Nur Benutzer mit Admin-Rechten können Ausnahmen anlegen.

HTTP/S-Profile

Astaro Security Gateway verfügt über einen HTTP/S-Proxy, der dafür ausgelegt und optimiert ist zu kontrollieren, welche Internetinhalte für welchen Teil des Netzwerks zugänglich sind. Dadurch hindert er Benutzer daran, Inhalte zu sehen, die Sie vielleicht ablehnen. Sie können den HTTP/S-Proxy so konfigurieren, dass ausgewählte Netzwerke global überwacht. Alternativ dazu können Sie individuelle Proxy-Profile anlegen, die verwendet werden können, um verschiedene Sicherheitsrichtlinien auf verschiedene Netzwerksegmente anzuwenden. Auf diese Weise können Sie unterschiedliche Inhaltsfilter-Richtlinien für die verschiedenen Abteilungen innerhalb Ihres Unternehmens definieren, sogar mit unterschiedlichen Benutzer-Authentifizierungsmethoden.

Querverweis – Weitere Informationen darüber, wie Sie HTTP/S-Profile konfigurieren können, finden Sie in der Astaro Knowledgebase²⁶ (navigieren Sie zu *ASG Version 7 > > Web Security*).

Dieses Kapitel beschreibt, wie Sie Filteraktionen hinzufügen und wie Sie diese im Rahmen der HTTP/S-Profile von Astaro Security Gateway verwenden. Es ist hierbei sinnvoll, die Registerkarten von *HTTP/S Profile* von hinten nach vorne zu konfigurieren. Das bedeutet, dass Sie damit beginnen sollten, Filteraktionen zu definieren, welche dann bestimmten Benutzern und Benutzergruppen in den sogenannten Filterzuweisungen zugewiesen werden. Diese wiederum verwenden Sie dann, um die Proxy-Profile zu konfigurieren.

Übersicht

Hinweis – Um HTTP-Profile konfigurieren zu können, muss der HTTP-Proxy eingeschaltet sein.

Das Flussdiagramm stellt schematisch dar, wie Filteraktionen, Filterzuweisungen und Proxy-Profile miteinander zusammenhängen. Wenn eine HTTP-Anfrage hereinkommt, bestimmt der HTTP-Proxy zunächst, welches Proxy-Profil angewendet werden muss. Das hängt gänzlich von der Quelladresse der Anfrage ab. Das erste Profil, das auf die Quelladresse der Anfrage zutrifft, wird

²⁶ <http://www.astaro.com/kb/>

verwendet. Alle anderen Proxy-Profile, die vielleicht noch vorhanden sind, werden ignoriert.

Intern werden alle Profile in einer einzigen Datei gespeichert, wobei sich das Standardprofil am Ende der Liste befindet. Solange noch kein anderes HTTP-Profil konfiguriert wurde, gibt es nur das Standardprofil. Wenn Sie beginnen, individuelle Proxy-Profile hinzuzufügen und sie mithilfe der Auswahlliste *Position* sortieren, bleibt das Standardprofil am Ende der Liste. Dabei stellt es sicher, dass es immer zuletzt angewendet wird.

Das Standardprofil ist jedoch kein Profil, das explizit über die Registerkarten unter *Web Security* >> *HTTP/S-Profile* konfiguriert werden kann. Stattdessen wird es vom System automatisch generiert, wenn Sie den HTTP-Proxy auf den Registerkarten *Web Security* >> *HTTP/S* konfigurieren. Die *Zugelassenen Netzwerke*, die auf der Registerkarte *Web Security* >> *HTTP/S* >> *Allgemein* konfiguriert werden, entsprechen den Quellnetzwerken eines Proxy-Profiles. Die Einstellungen im Feld *Benutzer/Gruppen* (Registerkarte *Web Security* >> *HTTP/S* >> *Allgemein*, wenn der Betriebsmodus *Einfache Benutzerauthentifizierung* ausgewählt ist) werden das Standardprofil. Dahingegen entsprechen die Einstellungen auf der Registerkarte *Web Security* >> *HTTP/S* >> *URL-Filterung* einer Filteraktion. Zuletzt, wenn nicht einmal das Standardprofil zutrifft, wird die HTTP-Anfrage blockiert.

Anschließend wird geprüft, welche Filterzuweisung mit diesem Profil verknüpft ist. Falls keine Filterzuweisung zutrifft, wird die Ersatzaktion (*Fallback Action*) für die Anfrage ausgeführt. Bei der Ersatzaktion handelt es sich um eine spezielle Filteraktion, die die Sicherheitspolitik Ihres Unternehmens widerspiegeln sollte. Im Falle einer sehr strengen Sicherheitspolitik sollten Sie eine Filteraktion anlegen, die allen Internetverkehr ohne Ausnahme blockiert.

Um den Benutzern innerhalb eines Netzwerksegments unterschiedliche Sicherheitsstufen zu bieten, brauchen Sie nur ein Profil zu konfigurieren, das mit unterschiedlichen Filterzuweisungen verknüpft ist. Die Zugriffsrechte für einen bestimmten Benutzer hängen dann von den Einstellungen in der ausgewählten Filterzuweisung ab. Aus diesem Grund macht es keinen Sinn, zwei Profile mit genau den gleichen Quellnetzwerken zu konfigurieren, da das zweite Profil in diesem Fall niemals aktiviert wird.

Proxy-Profile

Die Profile werden dazu genutzt, unterschiedliche Richtlinien für den Inhaltsfilter zu definieren, um anschließend verschiedene Richtlinien auf verschiedene Adressen Ihres Netzwerks anwenden zu können. Auf diese Weise können Sie unterschiedliche Richtlinien für die verschiedenen Abteilungen innerhalb Ihres

Unternehmens definieren. Zusätzlich kann jedem Profil seine eigene Methode zur Benutzerauthentifizierung zugewiesen werden.

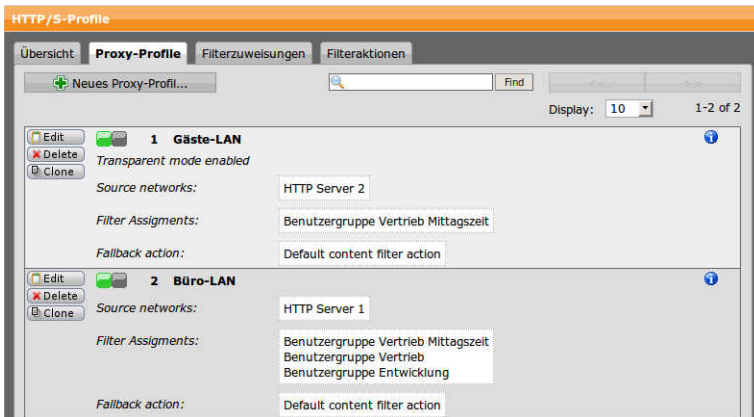


Figure 10.8 Proxy-Profil: Liste der Proxy-Profile

Um ein Proxy-Profil zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf die Schaltfläche *Neues Proxy-Profil*.**
Das Dialogfenster *Proxy-Profil erstellen* wird geöffnet.
2. **Nehmen Sie die folgenden Einstellungen vor:**
Name: Geben Sie einen aussagekräftigen Name für dieses Profil ein.
Position: Die Positionsnummer, die die Priorität des Profils festlegt. Niedrigere Nummern haben eine höhere Priorität. die Profile werden in aufsteigender Reihenfolge abgeglichen. Wenn ein Profil zutrifft, werden die Profile mit einer höheren Nummer nicht mehr abgeglichen. Platzieren Sie die spezifischeren Profile oben in der Liste, um sicherzustellen, dass weniger restriktive Profile zuletzt abgeglichen werden.
Quellnetzwerke: Wählen Sie die Netzwerke aus, die dieses Profil verwenden sollen (Pflichtfeld).

Warnung – Stellen Sie sicher, dass Sie keine Quellnetzwerke auswählen, die schon in anderen Profilen verwendet werden. Andernfalls kann es zu Unstimmigkeiten in der Zuordnung von Filteraktionen und Benutzer/Gruppen kommen, woraufhin vielleicht Benutzer eines bestimmten Netzwerksegments Websites öffnen können, auf die sie nicht zugreifen können sollen.

Filterzuweisungen: Wählen Sie eine Filterzuweisung aus. Eine Filterzuweisung ist eine Menge von Web-Security-Konfigurationseinstellungen, die verwendet werden können, um verschiedene Schutzstufen verschiedenen Benutzern/Gruppen zu beliebiger Zeit zuweisen zu können (weitere Informationen finden Sie unter *Web Security >> HTTP/S-Profile >> Filterzuweisungen*). Sie können auch mehrere Filterzuweisungen auswählen. Darüberhinaus können Sie festlegen, welche Filterzuweisung zuerst angewendet werden soll. Das ist zum Beispiel nützlich, wenn Sie verschiedene Filterzuweisungen demselben Benutzer oder derselben Benutzergruppe zu unterschiedlichen Zeiten zuweisen wollen. Generell sollten Sie die spezifischen Zuweisungen oben in der Liste platzieren, um sicherzustellen, dass die am wenigsten restriktiven Zuweisungen zuletzt abgeglichen werden. Benutzen Sie dafür die blauen Pfeile, die erscheinen, wenn Sie mindestens zwei Filter ausgewählt haben.

Hinweis – Es kann auch die Standard-Filterzuweisung auswählen, die die Standard-Filteraktion den Benutzern/Gruppen von der Registerkarte *HTTP/S >> Allgemein* zugewiesen hat, vorausgesetzt der HTTP/S-Proxy läuft in einem der drei Betriebsmodi: *Einfache Benutzerauthentifizierung*, *Active Directory SSO* oder *eDirectory SSO*. Beachten Sie außerdem, dass Sie eine Filterzuweisung verwenden können, die Benutzer und Gruppen beinhaltet, selbst wenn Sie den Betriebsmodus auf *Standard* oder *Transparent* setzen. Allerdings werden in diesem Fall die Benutzer und Gruppen ignoriert und nur Zeitereignisse, die in der Filterzuweisung definiert sind, werden im Proxy-Profil berücksichtigt.

Ersatzaktion: Bei der Ersatzaktion handelt es sich um eine spezielle Filteraktion, die die Sicherheitspolitik Ihres Unternehmens widerspiegeln sollte. Diese Filteraktion wird als letztes abgeglichen nachdem keine der anderen Filteraktionen zutreffen hat. Im Falle einer sehr strengen Sicherheitspolitik, können Sie einen speziellen Filter als Ersatzaktion anlegen, der den gesamten Internetdatenverkehr ohne Ausnahme blockiert. Übrigens entspricht die Standardfilteraktion hier den Einstellungen unter *Web Security >> HTTP/S >> URL-Filterung*.

Betriebsmodus: Für jedes Proxy-Profil können Sie zwischen mehreren Methoden zur Benutzerauthentifizierung wählen. Verschiedene Proxy-Profile können unterschiedliche Authentifizierungsmethoden haben, aber pro Proxy-Profil kann nur eine Benutzerauthentifizierungsmethode verwendet werden. Sie können sogar einen anderen Betriebsmodus auswählen

als den auf der Registerkarte *Web Security >> HTTP/S >> Allgemein* konfigurierten Betriebsmodus. Beachten Sie jedoch, dass die Authentifizierung nur wie vorgesehen funktioniert, wenn die hier gewählte Authentifizierungsmethode der Authentifizierungsmethode von allen Benutzer- und Gruppenobjekten entspricht, die in allen Filterzuweisungen verwendet werden. Die folgenden Betriebsmodi stehen zu Verfügung:

- **Standard:** Im Standardmodus lauscht der Proxy nach Client-Anfragen standardmäßig auf Port 8080 und lässt jeden Client zu, der sich in einem Netzwerk befindet, das im Feld *Zugelassene Netzwerke* aufgeführt ist. In diesem Modus muss der HTTP-Proxy in der Browser-Konfiguration von jedem Client angegeben sein.
- **Active Directory SSO:** Wählen Sie diese Option, wenn Sie *Active Directory Single Sign-On* (SSO) auf der Registerkarte *Benutzer >> Authentifizierung >> Server* konfiguriert haben. Das hat den Effekt, dass NTLM-Benutzerauthentifizierung verwendet wird, um Clients zu authentifizieren. Beachten Sie, dass die Funktion nur mit Internet Explorer garantiert wird. In diesem Modus muss der HTTP-Proxy in der Browser-Konfiguration von jedem Client angegeben sein.
- **Apple OpenDirectory SSO:** Wählen Sie diese Option, wenn Sie *LDAP* auf der Registerkarte *Benutzer >> Authentifizierung >> Server* konfiguriert haben und Sie Apple OpenDirectory verwenden. Damit der Proxy richtig funktioniert, müssen Sie zusätzlich eine MAC OS X Single Sign-On Kerberos Schlüsseldatei auf der Registerkarte *Web Security >> HTTP/S >> Erweitert* hochladen. In diesem Modus muss der HTTP-Proxy in der Browser-Konfiguration von jedem Client angegeben sein. Beachten Sie, dass der Safari-Browser SSO nicht unterstützt.
- **Einfache Benutzerauthentifizierung:** In diesem Modus muss sich jeder Client aus dem Netzwerk am HTTP-Proxy authentifizieren. Weitere Informationen zu den unterstützten Authentifizierungsmethoden finden Sie im Menü *Benutzer >> Authentifizierung* beschrieben. Beachten Sie, dass in den Browsern der Proxy für den Zugriff definiert werden muss. In diesem Modus muss der HTTP-Proxy in der Browser-Konfiguration von jedem Client angegeben sein.
- **eDirectory SSO:** Wählen Sie diesen Modus, wenn Sie *eDirectory* auf der Registerkarte *Benutzer >> Authentifizierung >> Server* konfigu-

riert haben. In diesem Modus muss der HTTP-Proxy in der Browser-Konfiguration von jedem Client angegeben sein.

- **Transparent:** Im Transparenzmodus werden alle Verbindungen von Client-Browseranwendungen auf Port 80 (bzw. Port 443 wenn SSL aktiviert ist) abgefangen und an den Proxy weitergeleitet, ohne client-seitige Konfiguration. Der Vorteil dieses Modus' ist, dass keine zusätzliche Verwaltung oder client-seitige Konfiguration nötig ist, der Nachteil hingegen ist, dass nur HTTP-Anfragen (Port 80) verarbeitet werden können. Deshalb werden die Proxy-Einstellungen im Client-Browser unwirksam, wenn Sie *Transparent* als Modus wählen.

Volltransparenzmodus (optional): Wählen Sie die Option *Volltransparenzmodus*, um die Quell-IP der Clients zu erhalten, anstatt sie durch die IP der Firewall zu ersetzen. Das ist nützlich, wenn Ihre Clients öffentliche IP-Adressen verwenden, die nicht durch den Proxy verschleiert werden sollen.

Hinweis – Im Transparenzmodus entfernt der Proxy NTLM-Authentifizierungsheader von HTTP-Anfragen. Darüberhinaus kann der Proxy keine FTP-Anfragen in diesem Modus verarbeiten. Wenn Ihre Clients auf solche Dienste zugreifen wollen, müssen Sie den Port (21) im Paketfilter öffnen. Beachten Sie auch, dass manche Webserver einige Daten über einen anderen Port als Port 80 übermitteln, im besonderen Streaming-Video- und -Audiodaten. Diese Anfragen werden nicht beachtet, wenn der Proxy im Transparenzmodus arbeitet. Um solchen Verkehr zu unterstützen, müssen Sie entweder einen anderen Modus wählen oder eine explizite Paketfilterregel anlegen, die diesen Verkehr erlaubt.

- **Transparent mit Authentifizierung:** Benutzen Sie diesen Modus, damit Benutzer sich authentifizieren müssen, während der Proxy transparent arbeitet. Wenn Benutzer eine Website zum ersten Mal öffnen, wird ihnen eine Webseite präsentiert, auf der sie Benutzername und Kennwort eingeben müssen. Dieser Modus ermöglicht benutzernamenbasierte Verfolgung (engl. *tracking*), Berichterstellung und Surfen ohne client-seitige Browserkonfiguration. Darüberhinaus können Sie Nutzungsbedingungen einrichten, die dann zusätzlich auf der Anmeldeseite angezeigt werden und von den Benutzern akzeptiert werden müssen, bevor sie fortfahren können. Weitere Informationen zu den Nutzungsbedingungen finden Sie im Kapitel *Verwaltung >> Anpassung >> HTTP/S-Proxy*.

HTTPS-Verkehr (SSL) scannen: Wählen Sie diese Option, um nicht nur HTTP-Verkehr sondern auch HTTPS-Verkehr zu scannen.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über das Proxy-Profil hinzu.

3. Klicken Sie *Speichern*.

Das neue Profil erscheint in der Liste *Proxy Profile*.

Um ein Proxy-Profil zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Filterzuweisungen

Auf der Registerkarte *HTTP/S-Profil* >> *Filterzuweisungen* können Sie Filteraktionen bestimmten Benutzern und Benutzergruppen zuweisen. Während eine Filteraktion sich auf das „Was“ bezieht, d. h. sie definiert, welche Websites oder Kategorien von Websites blockiert werden sollen, bezieht sich eine Filterzuweisung auf das „Wer“ und „Wann“, indem es diese Aktionen Benutzern und Benutzergruppen zu festgelegten Zeiten zuweist.

Hinweis – Die verschiedenen Einstellungen, die Sie auf der Registerkarte *Web Security* >> *HTTP/S* >> *Antivirus* konfiguriert haben (Antiviren-Scan, Dateierweiterungsfilter, MIME-Typ-Filter, Entfernung von Inhalt) und die Einstellungen auf der Registerkarte *HTTP/S* >> *URL-Filterung* (Kategorien, blockierte URLs) werden als Filteraktion *Standardfilteraktion* gespeichert, welche aus der Auswahlliste *Filteraktion* ausgewählt werden kann.

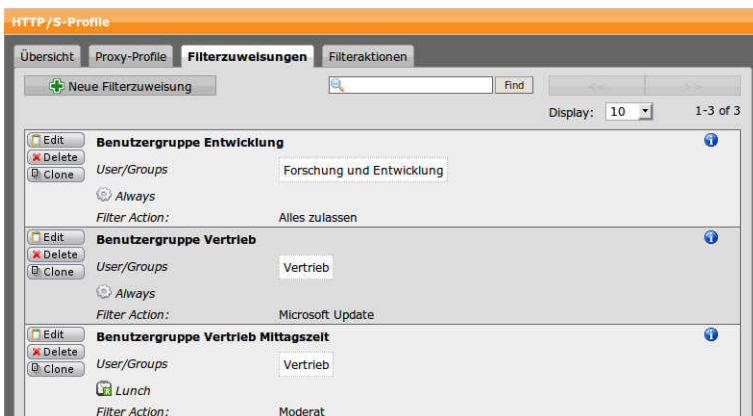


Figure 10.9 Proxy-Profil: Liste der Filterzuweisungen

Um eine Filterzuweisung zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf Neue Filterzuweisung.**

Das Dialogfenster *Neue Filterzuweisung erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Name: Geben Sie einen aussagekräftigen Name für die Filterzuweisung ein.

Benutzer/Gruppen: Wählen Sie die Benutzer und Gruppen aus, die eine bestimmte Filteraktion benutzen sollen. Achten Sie darauf, dass Ihre neue Filterzuweisung nur in Proxy-Profilen verwendet werden sollte, die die gleiche Authentifizierungsmethode verwenden wie die hier gewählten Benutzer und Gruppen.

Zeitereignis: Zeitereignisse sind einzelne oder wiederkehrende Zeitfenster, die Sie verwenden können, um Paketfilterregeln oder Filterprofile auf bestimmte Zeiträume zu begrenzen. Weitere Informationen finden Sie unter *Definitionen >> Zeitereignisse*.

Filteraktion: Wählen Sie die Filteraktion, die Sie den oben gewählten Benutzern und Benutzergruppen zuweisen wollen.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die Filterzuweisung hinzu.

3. **Klicken Sie Speichern.**

Die neue Filterzuweisung erscheint in der Liste *Filterzuweisungen*.

Um eine Filterzuweisung zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Jede Filterzuweisung kann gewählt werden, wenn Sie ein Proxy-Profil anlegen.

Filteraktionen

Auf der Registerkarte *HTTP/S-Profile >> Filteraktionen* können Sie einen Satz von Konfigurationseinstellungen zu Web Security anlegen und bearbeiten, mit dem verschiedene Schutzarten und Schutzstufen angepasst werden können. Filteraktionen können verschiedenen Benutzern und Benutzergruppen zugewiesen werden und bieten einen flexiblen Weg, den Internetzugriff zu kontrollieren.

Um eine Filteraktion zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf Neue Filteraktion.**

Das Dialogfenster *Neue Filteraktion erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Name: Geben Sie einen aussagekräftigen Name für die Filteraktion ein.

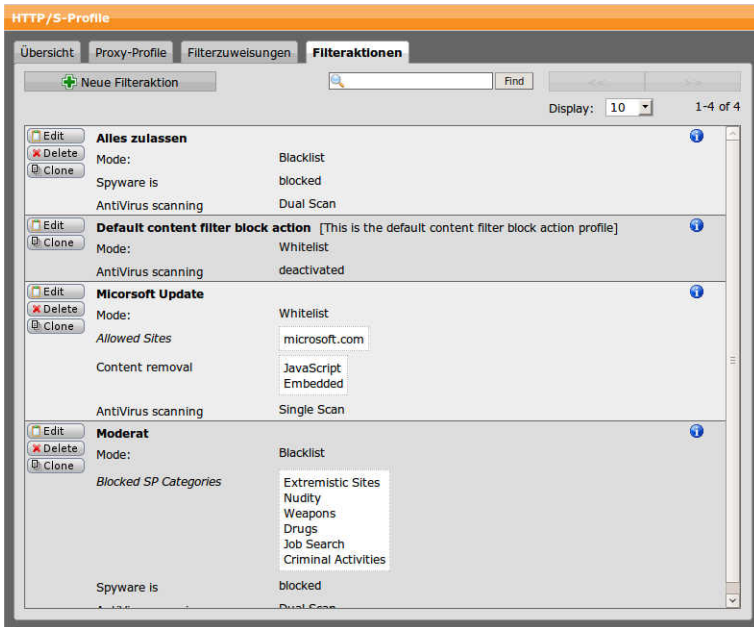


Figure 10.10 Proxy-Profil: Liste der Filteraktionen

Modus: Legen Sie fest, ob Ihre Auswahl an Website blockiert oder zugelassen werden soll. Die folgenden Optionen sind möglich:

- **Standardmäßig zulassen:** Wenn Sie diese Option wählen, werden alle Websites zugelassen außer denen, die Sie unten auswählen.
- **Standardmäßig blockieren:** Wenn Sie diese Option wählen, werden alle Websites blockiert außer denen, die Sie unten auswählen.

Schwellenwert: Websites können in folgende Klassen unterteilt werden: *Vertrauenswürdig* (engl. *trusted*), *Neutral* oder *Verdächtig* (engl. *Suspicious*). Unklassifizierte Websites werden als *Unüberprüft* (engl. *Unverified*) eingestuft. Sie können bestimmen, welchen Ruf eine Website haben muss, um für Ihr Netzwerk erreichbar zu sein. Websites unterhalb dieses Schwellenwerts werden blockiert.

Spyware-Kommunikation blockieren: Wählen Sie diese Option, um Spyware (Spionagesoftware) auf dem Weg vom Server zum Client zu entdecken und zu blockieren. Das verhindert, dass Computer in Ihrem Netzwerk mit neuer Spyware infiziert werden. Darüberhinaus entdeckt und blockiert diese Funktion Verkehr, der von bereits installierten Spyware-Programmen

ausgeht. Dadurch können bereits gewonnene Informationen über den Benutzer nicht länger an das Internet übermittelt werden. Beachten Sie, dass diese Option nicht verfügbar ist, wenn Sie den Modus *Standardmäßig blockieren* wählen.

Diese Website-Kategorien blockieren: Wählen Sie die Website-Kategorien aus, die blockiert werden sollen. Beachten Sie, dass sich diese Option zu *Diese Website-Kategorien zulassen* ändert, wenn Sie den Modus *Standardmäßig blockieren* wählen.

Unkategorisierte Seiten blockieren: Diese Funktion verhindert, dass der Browser Internetseiten mit unbekanntem Inhalt öffnet. Diese Funktion kann als zusätzliche Sicherung angesehen werden, falls eine potenziell unerwünschte Internetseite noch nicht als solche kategorisiert wurde. Beachten Sie, dass sich diese Option zu *Unkategorisierte Seiten zulassen* ändert, wenn Sie den Modus *Standardmäßig blockieren* wählen.

Diese URLs/Sites blockieren: Geben Sie die URL von Websites an, die blockiert werden sollen.

Immer diese URLs/Seiten zulassen: Geben Sie die URL von Websites an, die immer zugelassen werden sollen.

Blockierte Erweiterungen: Indem Sie in dieses Feld Dateierweiterungen eintragen, sorgen Sie dafür, dass Dateien mit diesem Dateityp blockiert werden (z. B. ausführbare Binärdateien). Um eine Dateierweiterung hinzuzufügen, klicken Sie auf das Plus-Symbol im Feld *Blockierte Erweiterungen* und geben Sie die Erweiterung ein, die blockiert werden soll, zum Beispiel *exe* (ohne den Punkt als Trennzeichen).

Blockierte MIME-Typen: Um einen MIME-Typ hinzuzufügen, der blockiert werden soll, klicken Sie auf das Plus-Symbol im Feld *Blockierte MIME-Typen* und geben Sie den MIME-Typ ein (z. B. *image/gif*).

Inhaltsentfernung: Wenn Sie dieses Auswahlkästchen markieren, erscheinen die beiden Optionen *JavaScript entfernen* und *Eingebettetes entfernen*. Mit diesen Optionen können Sie bestimmen, ob `<SCRIPT>`- und `<OBJECT>`-Tags aus HTML-Seiten entfernt werden sollen. Dabei werden einerseits Javascript-Funktionen deaktiviert, die in HTML-Seiten eingebettet oder eingebunden sind. Andererseits werden dynamische Inhalte aus dem eingehenden HTTP/S-Verkehr entfernt, wie etwa ActiveX, Flash oder Java-Applets.

Antiviren-Scan verwenden: Wenn Sie diese Option wählen, wird eingehender Datenverkehr nach schädigenden Inhalten gescannt. Astaro Security Gateway bietet mehrere Antiviren-Mechanismen für höchste Sicherheit.

Max. Scangröße: Legen Sie die Maximalgröße von Dateien fest, die von

den Antiviren-Mechanismen gescannt werden sollen. Dateien, die größer sind, werden nicht gescannt.

3. Klicken Sie *Speichern*.

Die neue Filteraktion erscheint in der Liste *Filteraktionen*.

Um eine Filteraktion zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Jede Filteraktion kann ausgewählt werden, wenn Sie eine Filterzuweisung oder ein Proxy-Profil anlegen.

Hinweis – Sie sehen hier auch die *Standardfilteraktion*, die standardmäßig alle HTTP/S-Anfragen blockiert, auf die keine andere Filteraktion oder die Einstellungen im Menü *HTTP/S* zutrifft.

FTP

Im Menü *Web Security >> FTP* wird der FTP-Proxy konfiguriert. Das *File Transfer Protocol* (FTP) ist ein weitverbreitetes Netzwerkprotokoll, um Dateien über das Internet auszutauschen. Astaro Security Gateway bietet einen Proxydienst, der als Zwischenstation für allen FTP-Verkehr in Ihrem Netzwerk agiert. Dabei bietet der FTP-Proxy nützliche Funktionen wie das Scannen von FTP-Verkehr nach Viren oder das Blockieren von bestimmten Dateitypen, die über das FTP-Protokoll übertragen werden.

Der FTP-Proxy kann transparent arbeiten, das heißt, alle FTP-Clients in Ihrem Netzwerk bauen eine Verbindung mit dem Proxy auf anstatt mit dem wirklichen Zielrechner. Der Proxy initiiert dann anhand der Anfrage eine neue Netzwerkverbindung, die für den Client unsichtbar bleibt. Der Vorteil dieser Vorgehensweise ist, dass kein weiterer Verwaltungsaufwand entsteht und clientseitig keine Konfiguration nötig ist.

Allgemein

Auf der Registerkarte *Web Security >> FTP >> Allgemein* können Sie die Grundeinstellungen für den FTP-Proxy konfigurieren.

Um den FTP-Proxy zu konfigurieren, gehen Sie folgendermaßen vor:



Figure 10.11 FTP-Proxy: Grundeinstellungen

1. **Aktivieren Sie den FTP-Proxy auf der Registerkarte *Allgemein***
 Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche. Die Statusampel wird gelb und der Abschnitt *FTP-Einstellungen* kann nun bearbeitet werden.
2. **Wählen Sie die *Zugelassenen Netzwerke* aus.**
 Wählen Sie die Netzwerke aus, die den FTP-Proxy verwenden dürfen.
3. **Wählen Sie einen Betriebsmodus aus.**
 Wählen Sie einen Betriebsmodus für den FTP-Proxy aus. Die folgenden Modi stehen zur Verfügung:
 - **Transparent:** Der Proxy leitet die Client-Anfragen an den Zielserver weiter und scannt den Inhalt. Es ist keine Konfiguration auf Client-Seite notwendig.
 - **Non-transparent:** Für diesen Modus müssen Sie die FTP-Clients konfigurieren. Benutzen Sie die IP-Adresse der Firewall und Port 2121.
 - **Beide:** Dieser Modus ermöglicht Ihnen, für einige Clients den Transparenzmodus zu verwenden und für andere den Non-Transparenzmodus. Konfigurieren Sie für die FTP-Clients, die im non-transparenten Modus arbeiten sollen, die Benutzung eines Proxys mit der IP-Adresse der Firewall und Port 2121.
4. **Klicken Sie *Übernehmen*.**
 Ihre Einstellungen werden gespeichert.

Hinweis – Der FTP-Proxy kann nicht mit FTP-Servern kommunizieren, bei denen Benutzerauthentifizierung via Active Directory durchgeführt wird. Um FTP-Clients die Kommunikation mit derartigen Servern zu ermöglichen, tragen Sie den FTP-Server auf der Registerkarte *Web Security >> FTP >> Erweitert* in das Feld *FTP-Proxy-Ausnahmen* ein.

Antivirus

Auf der Registerkarte *Web Security >> HTTP >> Antivirus* werden alle Maßnahmen betreffend FTP-Verkehr festgelegt, um schädlichen oder gefährlichen Inhalt wie Viren, Würmer oder andere Schadsoftware zu kontrollieren.

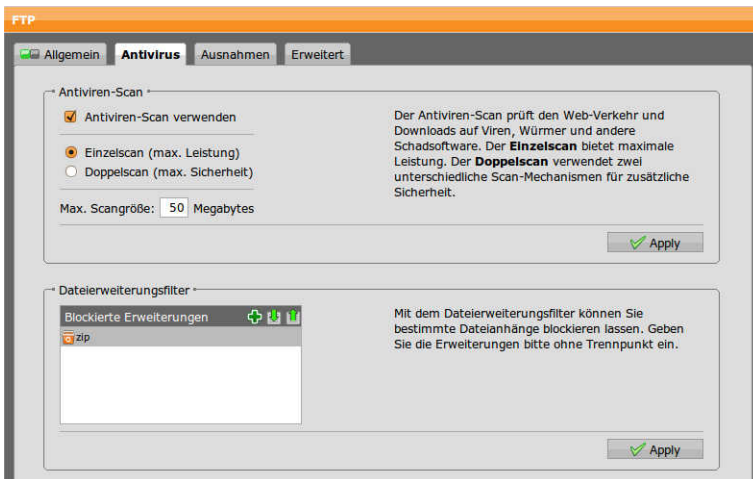


Figure 10.12 FTP-Proxy: Konfiguration von Antivirus für den FTP-Proxy

Antiviren-Scan verwenden: Wenn Sie diese Option wählen, wird der gesamte FTP-Verkehr gescannt. Astaro Security Gateway bietet für höchstmöglichen Schutz mehrere Antivirus-Mechanismen:

- **Einzelscan:** Standardeinstellung, die maximale Leistung bietet.
- **Doppelscan:** Bietet maximale Erkennungsrate, indem aller FTP-Verkehr von zwei verschiedenen Virensclannern gescannt wird.

Max. Scangröße: Geben Sie die maximale Größe der Dateien an, die vom Antivirus-Mechanismus gescannt werden soll. Dateien, die größer sind als der angegebene Wert, werden nicht gescannt.

Klicken Sie *Übernehmen*, um Ihre Einstellungen zu speichern.

Dateierweiterungsfilter

Diese Funktion filtert bestimmte FTP-Transfers basierend auf den übermittelten Dateiendungen (z. B. ausführbare Binärdateien) aus dem Internetverkehr heraus, wenn diese eine Dateierweiterung besitzen, die in der Liste *Blockierte Erweiterungen* aufgeführt ist. Sie können weitere Dateierweiterungen hinzufügen oder solche Erweiterungen aus der Liste löschen, die nicht blockiert werden sollen. Um eine Dateierweiterung hinzuzufügen, klicken Sie auf das Plus-Symbol im Feld *Blockierte Erweiterungen* und geben Sie die Dateierweiterung ein, die blockiert werden soll, z. B. *exe* (ohne den Punkt als Trennzeichen). Klicken Sie *Übernehmen*, um Ihre Einstellungen zu speichern.

Hinweis – Verschlüsselte zip-Archive können nicht nach schädlichem Inhalt durchsucht werden und passieren den Virusscanner ungehindert. Um Ihr Netzwerk vor Schadsoftware aus verschlüsselten zip-Dateien zu schützen, sollten Sie in Betracht ziehen, zip-Dateien gänzlich zu blockieren.

Ausnahmen

Auf der Registerkarte *FTP >> Ausnahmen* können Sie Rechner/Netzwerke definieren, die von bestimmten Sicherheitsoptionen ausgenommen sein sollen.

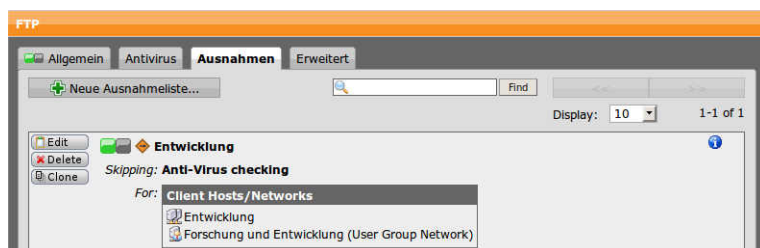


Figure 10.13 FTP-Proxy: Definition von Ausnahmen

Um eine Ausnahme zu definieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Ausnahmen auf Neue Ausnahmeliste*.**
Das Dialogfenster *Ausnahmeliste erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Name: Geben Sie einen aussagekräftigen Name für die Ausnahme ein.

Diese Prüfungen ausnehmen: Wählen Sie die Sicherheitsfunktionen, die ausgenommen werden sollen:

- **Antivirenprüfung:** Wählen Sie diese Option, um Virenskans auszuschalten, die den Verkehr auf unerwünschten Inhalt wie Viren, Trojanische Pferde, etc. überprüfen.
- **Blockierung von Dateierweiterungen:** Wählen Sie diese Option, um den Dateierweiterungsfilter zu deaktivieren, der benutzt werden kann, um Dateiübertragungen basierend auf Dateierweiterungen zu blockieren.
- **Zugelassene Server:** Wählen Sie diese Option um Prüfungen für zugelassene Server zu deaktivieren, die auf der Registerkarte *Erweitert* angegeben werden können.

Für diese Clientrechner/-Netzwerke: Wenn Sie diese Option wählen, wird das Feld *Clientrechner/-Netzwerke* geöffnet.

Wählen Sie die Clientrechner/-Netzwerke aus, die von den Sicherheitsprüfungen mit dieser Regel ausgenommen werden sollen.

Für diese Serverrechner/-netzwerke: Wenn Sie diese Option wählen, wird das Feld *Serverrechner/-netzwerke* geöffnet.

Wählen Sie die Server, die von den Sicherheitsprüfungen mit dieser Regel ausgenommen werden sollen.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die Ausnahme hinzu.

3. **Klicken Sie *Speichern*.**

Die neue Ausnahmeliste in der Liste *Ausnahmen* angezeigt.

Um eine Ausnahmeliste zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Erweitert

Auf der Registerkarte *FTP >> Erweitert* können Sie Rechner und Netzwerke angeben, die nicht vom Transparenzmodus des FTP-Proxys überwacht werden sollen.

Hinweis – Der FTP-Proxy kann nicht mit FTP-Servern kommunizieren, die Active Directory als Authentifizierungsmethode verwenden. Um FTP-Clients zu ermöglichen, sich mit einem solchen FTP-Server zu verbinden, fügen Sie den Server zur FTP-Proxy-Ausnahmen hinzu.

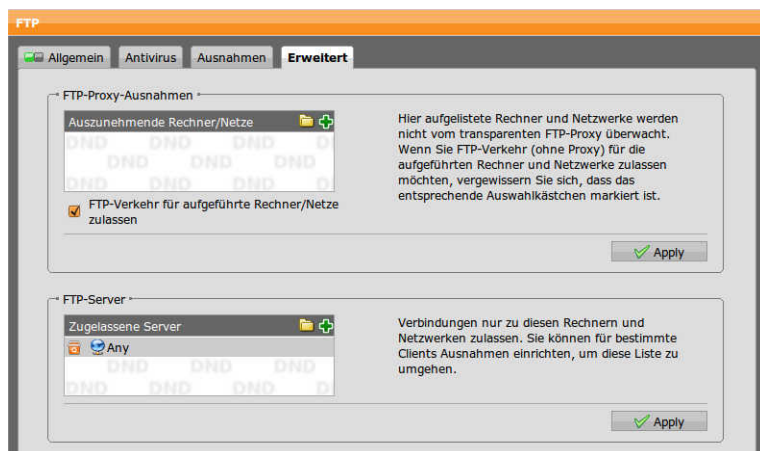


Figure 10.14 FTP-Proxy: Konfiguration der erweiterten Einstellungen

FTP-Proxy-Ausnahmen

Hier aufgeführte Rechner und Netzwerke sind von der transparenten Überwachung des FTP-Verkehrs ausgenommen. Um jedoch FTP-Verkehr für diese Rechner und Netzwerke zuzulassen, wählen Sie die Option *FTP-Verkehr für aufgeführte Rechner/Netze zulassen*. Wenn Sie diese Option nicht wählen, müssen Sie spezifische Paketfilterregeln für die hier aufgeführten Rechner und Netzwerke anlegen.

FTP-Server

Wählen Sie FTP-Server aus oder fügen Sie FTP-Server hinzu, auf die von Ihrem Netzwerk aus zugegriffen werden darf. Sie können Ausnahmen für einige Clients auf der Registerkarte *Ausnahmen* anlegen, um diese Liste zu umgehen.

Mail Security

In diesem Kapitel wird beschrieben, wie Sie grundlegende Sicherheitsfunktionen von Astaro Security Gateway für E-Mail konfigurieren. Die Seite *Mail-Security-Statistik* im WebAdmin gibt einen Überblick über die zehn aktivsten E-Mail-Versender, E-Mail-Empfänger, Spam-Versender (nach Land), erkannte Schadsoftware und gleichzeitige Verbindungen von heute. Jeder der Abschnitte enthält einen *Details*-Link. Ein Klick auf den Link leitet Sie zur entsprechenden Seite des Abschnitts *Berichte* von WebAdmin weiter, wo Sie weitere statistische Informationen finden können.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- SMTP
- SMTP-Profil
- POP3
- Verschlüsselung
- Quarantänebericht
- Mail-Manager

SMTP

Im Menü *Mail Security* >> *SMTP* können Sie den SMTP-Proxy konfigurieren. SMTP ist die Abkürzung für *Simple Mail Transfer Protocol*, ein Protokoll, das zum Ausliefern von E-Mails an einen Mail-Server verwendet wird. Astaro Security Gateway enthält ein Gateway auf Anwendungsebene für SMTP, das dazu genutzt werden kann, Ihren internen Mail-Server vor Angriffen aus dem Internet zu schützen. Des Weiteren bietet es effektive Dienste für Antivirenschans und E-Mail-Filterung.

Hinweis – Damit der SMTP-Proxy korrekt funktioniert, muss ein gültiger Namensserver (DNS) konfiguriert sein.

Allgemein

Auf der Registerkarte *Mail Security >> SMTP >> Allgemein* können Sie festlegen, ob Sie den *Einfachen Modus* oder den *Profilmodus* für die Konfiguration von SMTP verwenden wollen.

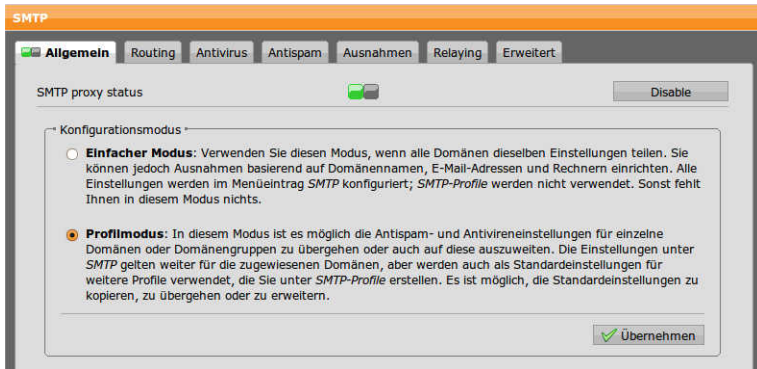


Figure 11.1 SMTP-Proxy: Grundeinstellungen

SMTP-Proxy konfigurieren:

1. Aktivieren Sie SMTP.

Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche. Die Statusampel wird grün und der Abschnitt *Konfigurationsmodus* kann nun bearbeitet werden.

2. Wählen Sie einen Konfigurationsmodus.

Einfacher Modus: Verwenden Sie diesen Modus, falls alle Domänen dieselben Einstellungen teilen. Dennoch können Sie Ausnahmen definieren, die auf dem Domännennamen, E-Mail-Adressen und Rechnern basieren. Es besteht keine Einschränkung in der Funktionalität im Vergleich zum *Profilmodus*.

Profilmodus: In diesem Modus können Sie globale Einstellungen überschreiben oder erweitern, z. B. für Antispam oder Antivirus, für individuelle Domänen oder Domänengruppen, indem Sie für diese Profile im Menü *SMTP-Profil* anlegen. Einstellungen, die im Menü *SMTP* vorgenommen wurden, gelten trotzdem noch für die ihnen zugeteilten Domänen und dienen außerdem als Standardeinstellungen für Profile. Im *Profilmodus* finden

Sie zusätzliche Hinweise zu einigen Einstellungen mit Hinblick auf Empfehlungen für den Profilmodus und das Verhalten von ASG.

3. Klicken Sie **Übernehmen**.

Ihre Einstellungen werden gespeichert. Der gewählte Modus wird aktiviert.

Routing

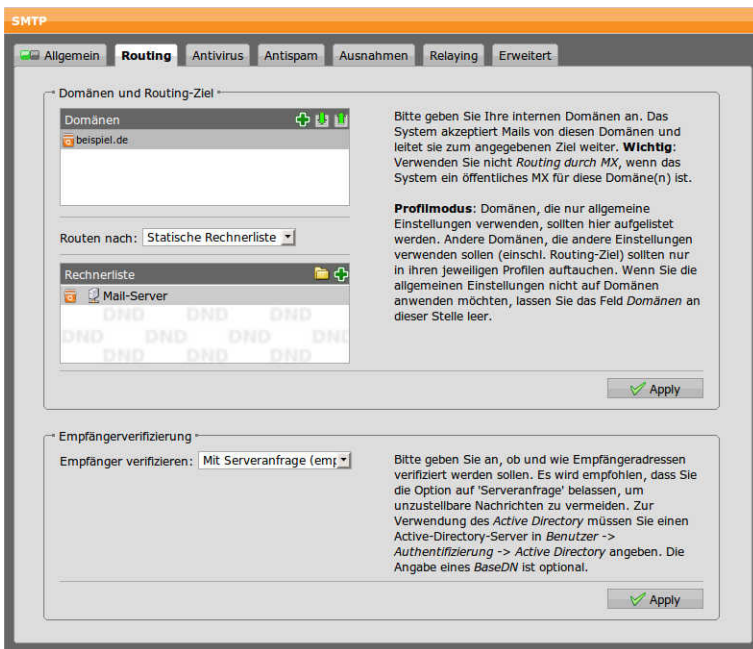


Figure 11.2 SMTP-Proxy: Konfiguration von Domänen und Routingzielen

Auf der Registerkarte *Routing* können Sie Domänen und Routingziele für den SMTP-Proxy konfigurieren und festlegen, wie Empfänger verifiziert werden sollen.

Um das SMTP-Routing zu konfigurieren, gehen Sie folgendermaßen vor:

1. Geben Sie Ihre interne(n) Domäne(n) ein.

Um E-Mail-Domänen einzugeben, klicken Sie auf das Plus-Symbol im Feld *Domänen*.

Geben Sie im erscheinenden Textfeld die Domäne in der Form `example.com`

ein und klicken Sie *Übernehmen*. Wiederholen Sie diesen Schritt bis alle Domänen aufgeführt sind.

Im Profilmodus: Geben Sie nur Domänen eine, die globale Einstellungen verwenden. Alle anderen Domänen sollten in ihren jeweiligen Profilen aufgeführt sein.

2. Geben Sie den internen Server an.

Wählen Sie aus der Auswahlliste *Routen nach* den Rechner aus, zu dem E-Mails für die aufgeführten Domänen weitergeleitet werden sollen. Ein üblicher Zielrechner wäre der Microsoft Exchange Server in Ihrem lokalen Netzwerk. Sie können zwischen verschiedenen Serverarten wählen:

- **Statische Rechnerliste:** Wählen Sie eine Rechnerdefinition der Zielroute aus dem Feld *Rechnerliste*. Beachten Sie, dass Sie mehrere Rechnerdefinitionen wählen können, um ein einfaches Failover gewährleisten zu können. Wenn die Zustellung an den ersten Rechner fehlschlägt, werden die Mails zum nächsten Rechner geroutet. Die (statische) Reihenfolge der Rechner kann in der aktuellen Version von Astaro Security Gateway jedoch nicht festgelegt werden und ist etwas zufällig. Um die Zustellung zufällig auf eine Gruppe von Rechnern zu verteilen, um zusätzlich einen einfachen Lastausgleich zu erlangen, verwenden Sie den Routentyp *DNS-Rechnername* und geben Sie einen Rechnernamen an, der mehrere A-Einträge (engl. *A Record*) besitzt (ein A-Eintrag oder *Address Resource Record* bildet im DNS einen Rechnernamen auf eine IP-Adresse ab.)
- **DNS-Rechnername:** Geben Sie den vollständigen Domännennamen (FQDN, *fully qualified domain name*) Ihrer Zielroute an (z.B. *exchange.example.com*). Beachten Sie, wenn Sie einen DNS-Namen mit mehreren A-Einträgen (engl. *A Record*) auswählen, werden die Mails an jeden Server beliebig verteilt. Wenn ein Server ausfällt, werden darüber hinaus alle Mails automatisch zu den verbleibenden Servern geroutet.
- **MX-Einträge:** Sie können Mails auch über MX-Einträge (engl. *MX Records*) zu Ihre(r/n) Domäne(n) routen. Wenn Sie diesen Routentyp auswählen, wird der Mail-Transfer-Agent von Astaro Security Gateway eine DNS-Anfrage starten, um den MX-Eintrag vom Domännennamen des Empfängers zu erfragen. Dieser ist der Teil der E-Mail-Adresse, die nach dem „@“-Zeichen steht. Wenn Sie diesen Routentyp wählen, stellen Sie

sicher, dass die Firewall nicht der primäre MX-Server für die oben angegebene Domäne ist, da er Mails nicht selbst zustellen wird.

3. Klicken Sie **Übernehmen**.

Ihre Einstellungen werden gespeichert.

Empfängerverifizierung

Empfänger verifizieren: Hier können Sie festlegen, ob und wie E-Mail-Empfänger verifiziert werden.

- **Mit Serveranfrage:** Es wird eine Anfrage an den Server geschickt, um den Empfänger zu verifizieren.
- **Im Active Directory:** Es wird eine Anfrage an den Active-Directory-Server geschickt, um den Empfänger zu verifizieren. Um Active Directory benutzen zu können, müssen Sie einen Active-Directory-Server unter *Benutzer >> Authentifizierung >> Server* angegeben haben. Geben Sie einen BaseDN im Feld *Alternativer BaseDN* ein.

Hinweis – Die Benutzung von Active-Directory-Empfängerverifizierung kann dazu führen, dass Nachrichten abgelehnt werden, im Fall dass der Server nicht antwortet.

- **Aus:** Sie können die Empfängerverifizierung vollständig ausschalten, aber das ist nicht empfehlenswert, da es zu einem höheren Spamaufkommen und Wörterbuchangriffen führt. Dadurch erhöhen Sie die Wahrscheinlichkeit, dass Ihre Quarantäne mit unerbetenen Nachrichten „überflutet“ wird.

Klicken Sie **Übernehmen**, um Ihre Einstellungen zu speichern.

Antivirus

Die Registerkarte *Antivirus* enthält verschiedene Maßnahmen gegen E-Mails, die einen schädlichen oder gefährlichen Inhalt enthalten wie Viren, Würmer oder andere Schadsoftware.

Während SMTP-Transaktion scannen

Wählen Sie die Option *Schadsoftware während SMTP-Transaktion ablehnen*, wenn Nachrichten bereits während der SMTP-Übermittlung gescannt werden und abgelehnt werden sollen, wenn Sie Schadsoftware enthalten.

Im Profilmodus: Diese Einstellung kann nicht für einzelne Profile geändert werden. Nachrichten mit mehr als einem Empfänger lassen diese Funktion aus,



Figure 11.3 SMTP-Proxy: Konfiguration der Antivirus-Einstellungen

wenn bei einem der Empfängerprofile *Antiviren-Scan* ausgeschaltet ist. Das bedeutet, dass es sinnvoll ist, die reguläre Antivirus-Einstellung unten auf entweder *Verwerfen* oder *Quarantäne* gestellt zu lassen.

Antiviren-Scan

Wenn Sie diese Option wählen, werden E-Mails nach unerwünschtem Inhalt gescannt wie z. B. Viren, Trojanische Pferde oder verdächtige Dateitypen. Nachrichten mit schädlichem Inhalt werden blockiert oder in der E-Mail-Quarantäne gespeichert. Benutzer können ihre unter Quarantäne stehenden E-Mails ansehen und freigeben, entweder über das Astaro Benutzerportal oder den täglichen Quarantänebericht. Nachrichten, die schädlichen Inhalt enthalten, können jedoch nur vom Administrator aus der Quarantäne freigegeben werden, über den Mail-Manager.

Antivirus: Hier können Sie festlegen, was mit Nachrichten geschieht, die schädlichen Inhalt enthalten. Die folgenden Aktionen sind möglich:

- **Aus:** Es werden keine Antiviren-Scans durchgeführt.
- **Verwerfen:** Die E-Mail wird angenommen und sofort gelöscht.
- **Quarantäne:** Die E-Mail wird blockiert und unter Quarantäne gestellt. Nachrichten unter Quarantäne können im Benutzerportal oder im täglichen

Quarantänebericht eingesehen werden. Beachten Sie, dass Nachrichten mit schädlichem Inhalt nur vom Administrator aus der Quarantäne freigegeben werden können.

Astaro Security Gateway bietet für höchstmöglichen Schutz mehrere Antivirus-Mechanismen:

- **Einzelscan:** Standardeinstellung, die maximale Leistung bietet.
- **Doppelscan:** Bietet maximale Erkennungsrate, indem aller E-Mails von zwei verschiedenen Virenscannern gescannt wird.

Unscannbaren Inhalt in Quarantäne: Wenn Sie diese Option wählen, werden E-Mails mit Inhalt, der nicht gescannt werden kann, unter Quarantäne gestellt. Unscannbarer Inhalt können verschlüsselte Archive oder sehr große Inhalte sein, oder es kann ein technischer Grund vorliegen wie z. B. der Ausfall eines Scanners.

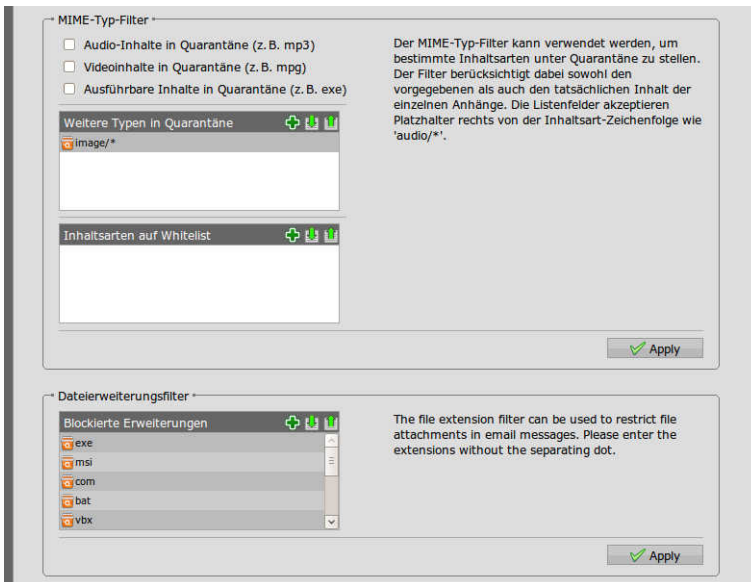


Figure 11.4 SMTP-Proxy: Dateierweiterungsfilter

MIME-Typ-Filter

Der MIME-Typ-Filter liest den Typ von E-Mail-Inhalten aus. Sie können festlegen, wie mit den verschiedenen MIME-Typen umgegangen werden soll.

- **Audio-Inhalte in Quarantäne:** Wenn Sie diese Option wählen, werden Audioinhalte wie mp3- oder wav-Dateien unter Quarantäne gestellt.
- **Videoinhalte in Quarantäne:** Wenn Sie diese Option wählen, werden Videoinhalte wie mpg- oder mov-Dateien unter Quarantäne gestellt.
- **Ausführbare Inhalte in Quarantäne:** Wenn Sie diese Option wählen, werden ausführbare Inhalte wie exe-Dateien unter Quarantäne gestellt.

Weitere Typen in Quarantäne: Um einen anderen MIME-Typ als die obigen hinzufügen, der unter Quarantäne gestellt werden soll, klicken Sie auf das Plus-Symbol im Feld *Weitere Typen in Quarantäne* und geben Sie den MIME-Typ an (z. B. image/gif). Sie können Platzhalter (*) auf der rechten Seite des Schrägstriches verwenden, z. B. application/*.

Inhaltsarten auf Whitelist: Sie können in dieses Feld MIME-Typen eintragen, die generell zugelassen sein sollen. Um einen MIME-Typ hinzuzufügen, klicken Sie auf das Plus-Symbol im Feld *Inhaltsarten auf Whitelist* und geben Sie den MIME-Typ ein.

MIME-Typ	MIME-Type-Klasse
audio/*	Audiodateien
video/*	Videodateien
application/x-dosexec	Anwendungen
application/x-msdownload	
application/exe	
application/x-exe	
application/dos-exe	
vms/exe	
application/x-winexe	
application/msdos-windows	
application/x-msdos-program	

Table 11.1 MIME-Typen, die dem MIME-Typ-Filter bekannt sind

Dateierweiterungsfilter: Mit dem Dateierweiterungsfilter können Sie E-Mails unter Quarantäne stellen (mit Warnung), die bestimmte Dateitypen enthalten,

basierend auf ihren Dateierweiterungen (z. B. ausführbare Dateien). Um Dateierweiterungen hinzuzufügen, klicken Sie auf das Plus-Symbol im Feld *Blockierte Erweiterungen* und geben Sie eine kritische Dateierweiterung ein, die gescannt werden soll, z. B. *exe* oder *jar* (ohne den Punkt als Trennzeichen).

Hinweis – Verschlüsselte zip-Archive können nicht auf schädliche Inhalte gescannt werden und werden ungeprüft durch den Virens Scanner geleitet. Um Ihr Netzwerk vor Schadsoftware zu schützen, die in verschlüsselten zip-Archiven enthalten ist, sollten Sie in Betracht ziehen, grundsätzlich alle zip-Anhänge zu blockieren.

Fußzeile über Antivirenprüfung: Für jede ausgehende Nachricht können Sie eine spezielle Fußzeile hinzufügen beziehungsweise eine Fußzeile anpassen, die Benutzer darüber informiert, dass die E-Mail auf schädliche Inhalte gescannt wurde. Die Antivirenprüfungsfußzeile wird nicht an die E-Mail angehängt, wenn die E-Mail eine Antwort ist (d. h. sie besitzt den Header *In-Reply-To*) oder wenn die Inhaltsart der E-Mail nicht bestimmt werden konnte.

Hinweis – Das Hinzufügen einer Fußzeile zu Nachrichten, die bereits signiert oder verschlüsselt sind, durch ein E-Mail-Programm (z. B. Microsoft Outlook oder Mozilla Thunderbird), wird ihre Signatur kaputt und damit ungültig machen. Wenn Sie digitale Zertifikate auf Client-Seite erzeugen wollen, deaktivieren Sie die Antivirenprüfungsfußzeilen-Option. Wenn Sie jedoch nicht auf Datenschutz und Authentifizierung in Ihrer E-Mail-Kommunikation verzichten möchten und dennoch eine allgemeine Antivirenprüfungsfußzeile verwenden wollen, dann sollten Sie in Betracht ziehen, die eingebaute Funktion von Astaro Security Gateway einzusetzen. E-Mail-Verschlüsselung, die auf dem Gateway durchgeführt wird, bedeutet, dass die Fußzeile zur Nachricht hinzugefügt wird, bevor die digitale Signatur erzeugt wird, wodurch die Signatur intakt bleibt.

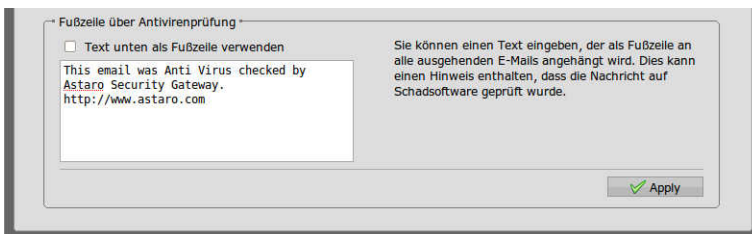


Figure 11.5 SMTP-Proxy: Fußzeile zur Antivirenprüfung

Antispam

Astaro Security Gateway kann so konfiguriert werden, dass es unerbetene Spam-E-Mails entdeckt und Spam-Übermittlungen von bekannten oder verdächtigen Spam-Verteilern identifiziert. Die Konfigurationsoptionen auf der Registerkarte *Antispam* ermöglichen die Konfiguration von SMTP-Sicherheitsfunktionen, die darauf ausgelegt sind, Ihr Netzwerk vor dem Empfang von unerbetenen kommerziellen E-Mails zu schützen.

SMTP

☒ Allgemein
 ☐ Routing
 ☐ Antivirus
 Antispam
☐ Ausnahmen
 ☐ Relaying
 ☐ Erweitert

Spam-Erkennung während SMTP-Übermittlung

Zur SMTP-Zeit ablehnen: Bestätigten Spam

Sie können Spam schon während der SMTP-Übermittlung ablehnen, indem Sie entweder allen Spam oder nur Bestätigten Spam ablehnen.

Profilmodus: Diese Einstellung kann nicht auf Profibasis geändert werden. Nachrichten mit mehr als einem Empfänger überspringen diese Funktion, wenn eines der Empfängerprofile den Spam-Scan vollständig ausgeschaltet hat. Dies bedeutet, dass Sie die reguläre Spam-Scan-Einstellung unten auf entweder Verwerfen oder Quarantäne gesetzt lassen sollten.

✓ Apply

RBLs (Echtzeit-Blackhole-Listen)

☒ Empfohlene RBLs verwenden
☒ Einwahl-/Privatrechner blockieren

Echtzeit-Blackhole-Listen (RBLs, auch 'DNS-Listen' genannt) stehen an erster Stelle in der Spam-Abwehr. Die RBL-Verarbeitung geht schnell und sollte daher am besten eingeschaltet bleiben.

Extra-RBL-Zonen

- 1 rbl.interserver.net
- 2 spam.rbl.msrbf.net

✓ Apply

Spamfilter

Spam-Aktion: Quarantäne

Aktion b. bestätigtem Spam: Quarantäne

Spam-Kennzeichner: *SPAM*

Dieser Spamfiltermechanismus bewertet Nachrichten nach ihrem Inhalt und SMTP-Envelope-Informationen.

✓ Apply

Figure 11.6 SMTP-Proxy: Konfiguration der Antispam-Einstellungen

Hinweis – Die Maximalgröße für Nachrichten, die vom Antispam-Mechanismus gescannt werden, beträgt 128 KB. Nachrichten, die diese Größe überschreiten, werden nicht nach Spam gescannt.

Spam-Erkennung während SMTP-Übermittlung

Sie haben die Möglichkeit, Spam bereits zum Zeitpunkt der SMTP-Übermittlung abzulehnen. Wählen Sie eine der folgenden Einstellungen für die Option *Zur SMTP-Zeit ablehnen*:

- **Aus:** Spam-Erkennung ist ausgeschaltet und es werden keine E-Mails aufgrund von Spamverdacht abgelehnt.
- **Bestätigten Spam:** Nur bestätigter Spam wird abgelehnt.
- **Spam:** Alle E-Mails, die das System für Spam hält, werden abgelehnt. Beachten Sie, dass hierbei die Rate der Fehlfunde (engl. *false positives*) steigen kann, da E-Mails, die als möglicher Spam betrachtet werden (wie z. B. Newsletter), abgelehnt werden.

Profilmodus: Diese Einstellung kann nicht für einzelne Profile geändert werden. Nachrichten mit mehr als einem Empfänger lassen diese Funktion aus, wenn bei einem der Empfängerprofile der Spam-Scan ausgeschaltet ist. Das bedeutet, dass es sinnvoll ist, die reguläre Einstellung zur Spam-Erkennung auf entweder *Spam* oder *Bestätigten Spam* gestellt zu lassen.

RBLs (Echtzeit-Blackhole-Listen)

Echtzeit-Blackhole-Listen (*Realtime Blackhole Lists*, RBL, *blackhole* = verwerfen) sind eine Methode, mit der Websites eine Liste von IP-Adressen bekannt geben, die mit Spam-Versand in Verbindung gebracht werden.

Empfohlene RBLs verwenden: Die Wahl dieser Option sorgt dafür, dass externe Datenbanken nach bekannten Spam-Versendern gefragt werden (sogenannte *Echtzeit-Blackhole-Listen*). Nachrichten, die von einer Domäne gesendet werden, die in einer oder mehrerer dieser Listen aufgeführt ist, können einfach abgelehnt werden. Es sind einige Dienste dieser Art im Internet verfügbar. Diese Funktion ist eine enorme Hilfe bei der Reduzierung des Spam-Aufkommens.

Standardmäßig werden die folgenden RBLs genutzt:

- sbl-xbl.spamhaus.org
- pbl.spamhaus.org
- cbl.abuseat.org

Hinweis – Die RBLs, die von Astaro Security Gateway genutzt werden, können sich ohne Ankündigung ändern. Astaro übernimmt keine Gewähr für den Inhalt dieser Datenbanken.

Sie können weitere RBL-Sites hinzufügen, um die Antispam-Fähigkeiten von Astaro Security Gateway zu verbessern. Klicken Sie dazu auf das Plus-Symbol im Feld *Extra-RBL-Zonen*. Geben Sie in das erscheinende Textfeld die RBL-Zone ein und klicken Sie anschließend *Übernehmen*.

Einwahl-/Privatrechner blockieren: Wählen Sie diese Option, um die Verwendung von Privatrechner-Blockierungslisten zu aktivieren. DSL-Privatkunden von ISPs (*Internet Service Providers*, Internetanbietern) erhalten eine IP-Adresse aus einem bestimmten Adressbereich, der vom ISP verwaltet wird. Diese IP-Adressen können entweder dynamisch oder statisch sein. Da Kunden mit privatengenenutzten IP-Adressen meistens den Mailserver ihres ISP verwenden und keinen eigenen Mailserver betreiben, veröffentlichen ISPs diese Privat-IP-Adresse der Kunden, damit andere ISPs Mails ablehnen können, die von diesen Adressen kommt. Wenn Sie diese Option wählen, werden deshalb alle Mails blockiert, die von einer dort aufgeführten IP-Adresse kommen. Klicken Sie *Übernehmen*, um Änderungen in diesem Abschnitt zu speichern.

Spamfilter

Astaro Security Gateway bietet eine heuristische Prüfung eingehender E-Mails auf Spam-Eigenschaften. Es benutzt dafür SMTP-Envelope-Informationen (*envelope* = Umschlag) und eine interne Datenbank mit heuristischen Tests und Eigenschaften. Die Spamfilter-Option bewertet Nachrichten basierend auf ihrem Inhalt und SMTP-Envelope-Informationen. Höhere Werte deuten auf eine höhere Spam-Wahrscheinlichkeit hin.

Mit den folgenden beiden Optionen können Sie festlegen, was mit Nachrichten geschehen soll, denen einen gewissen Spam-Wert zugewiesen bekommen haben. Das stellt sicher, dass potenzielle Spam-E-Mails von der Firewall anders behandelt werden.

- **Spam-Aktion:** Hier können Sie festlegen, was mit Nachrichten geschieht, die als möglicher Spam eingestuft wurden. Beachten Sie, dass es Fehlfunde geben kann, z. B. Newsletter, wodurch durch Verwerfen E-Mails verloren gehen können.
- **Aktion bei bestätigtem Spam:** Hier können Sie festlegen, was mit Nachrichten geschieht, die sicher Spam sind.

Sie können zwischen verschiedenen Aktionen für diese beiden Arten von Spam wählen:

- **Aus:** Es werden keine Nachrichten als Spam markiert oder ausgefiltert.
- **Warnen:** Es werden keine Nachrichten ausgefiltert. Stattdessen wird eine Spam-Markierung („Flag“) zum Header der Nachricht hinzugefügt und der Betreff der Nachricht erhält einen Spam-Kennzeichner.
- **Quarantäne:** Die Nachricht wird blockiert und in die E-Mail-Quarantäne verschoben. Nachrichten in Quarantäne können entweder über das Benutzerportal oder den täglichen Quarantänebericht eingesehen werden.
- **Verwerfen:** Die Nachricht wird akzeptiert und sofort gelöscht.

Spam-Kennzeichner: Mit dieser Option können Sie eine Kennzeichnung für Spam-Nachrichten festlegen, d. h. dass eine Zeichenkette zur Betreffzeile der Nachricht hinzugefügt wird, die es einfach macht, Spam-Nachrichten schnell als solche zu erkennen. Standardmäßig wird die Zeichenkette **SPAM** benutzt, um Nachrichten als Spam zu kennzeichnen.

Absender-Blacklist

Der Envelope-Sender (dt. Absender auf „Umschlag“) von eingehenden SMTP-Sitzungen wird mit den Adressen auf dieser Blacklist (dt. schwarze Liste) abgeglichen. Wenn der Envelope-Sender auf der Blacklist gefunden wird, wird die Nachricht verworfen.

Um ein neues Adressmuster zur Blacklist hinzuzufügen, klicken Sie auf das Plus-Symbol im Feld *Adressmuster auf Blacklist*, geben Sie eine (oder einen Teil einer) Adresse ein und klicken Sie *Übernehmen*. Sie können einen Asterisk (*) als Platzhalter verwenden, z. B. **@abbeybnknational.com*.

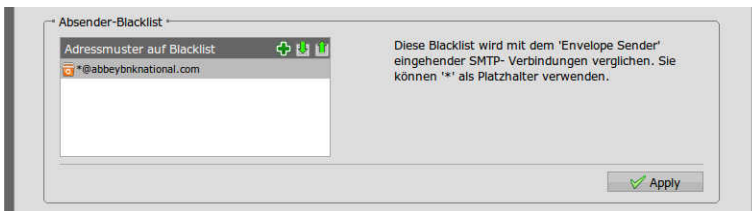


Figure 11.7 SMTP-Proxy: Erweiterung der Absender-Blacklist

Ausdruckfilter

Der Ausdruckfilter scannt den Inhalt von Nachrichten, die durch den SMTP-Proxy geleitet werden, auf spezifische Ausdrücke. Verdächtige E-Mails werden

blockiert. Ausdrücke können in Form von *Perl Compatible Regular Expressions* (Perl-kompatiblen regulären Ausdrücken) eingegeben werden. Einfache Zeichenfolgen wie „Online Dating“ werden ohne Berücksichtigung der Groß-/Kleinschreibung interpretiert.

Klicken Sie *Übernehmen*, um Änderungen zu speichern.

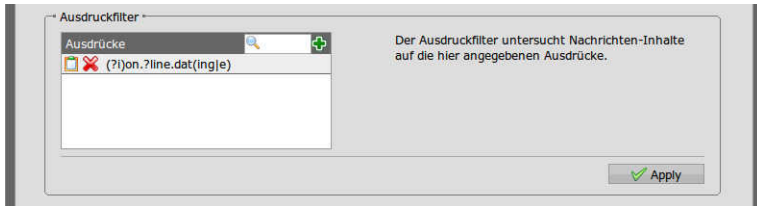


Figure 11.8 SMTP-Proxy: Hinzufügen von Ausdrücken zum Ausdruckfilter

Erweiterte Antispam-Funktionen

Dieser Abschnitt enthält weitere Optionen, die die Antispam-Fähigkeiten von Astaro Security Gateway verbessern.

Ungültige HELO/fehlende RDNS ablehnen: Wählen Sie diese Option, wenn Sie Rechner ablehnen wollen, die ungültige HELO-Einträge senden oder bei denen rDNS-Einträge fehlen. Wenn Sie Rechner von dieser Prüfung ausnehmen wollen, benutzen Sie die entsprechende Option auf der Registerkarte *Ausnahmen*.

Greylisting verwenden: Greylisting (dt. Verwendung grauer Listen) bedeutet, dass E-Mails für einen gewissen Zeitraum abgelehnt werden. Normalerweise zeichnet ein Mailserver, der Greylisting verwendet, die folgenden drei Informationen für alle eingehenden Nachrichten auf, auch bekannt als *Triplet* (engl. *triplet*):

- Die Absenderadresse
- Die IP-Adresse des Rechners, der die Nachricht verschickt hat
- Die Empfängeradresse

Das Triplet wird nun mit der internen Datenbank des SMTP-Proxy verglichen. Wenn dieses Triplet noch nicht vorhanden ist, wird ein Eintrag in die Datenbank geschrieben zusammen mit einem speziellen Zeitstempel, der das Triplet beschreibt. Aufgrund dieses Zeitstempels wird die E-Mail vom SMTP-Proxy für den Zeitraum von fünf Minuten abgelehnt. Nach dieser Zeitspanne ist das Triplet dem Proxy bekannt und die Nachricht wird beim nächsten Zustellversuch akzeptiert. Beachten Sie, dass das Triplet nach einer Woche verfällt, wenn es

innerhalb dieser Zeitspanne nicht aktualisiert wird.

Das Greylisting nutzt die Tatsache, dass die meisten Versender von Spam-Mails Software verwenden, die nach der „Fire-and-Forget“-Methode arbeiten: Versuche die E-Mail zuzustellen und wenn es nicht klappt, vergiss es! Das heißt, dass die Versender solcher Spam-Mails nicht wie RFC-konforme Mailserver versuchen, die Mail bei einem vorübergehenden Fehlschlag nochmals zu versenden. Die Annahme beruht darauf, dass ein legitimer Server bei einem vorübergehenden Fehlschlag E-Mails nochmal versenden wird, da dieses Verhalten in der RFC-Spezifikation vorgesehen ist, und zu diesem Zeitpunkt wird der Zielrechner die E-Mails annehmen.

BATV verwenden: Bei der Funktion *Bounce Address Tag Validation* (BATV) handelt es sich um einen Entwurf des Standardisierungsgremiums *Internet Engineering Task Force* (IETF), bei dem der Versuch unternommen wird, die legitime Benutzung von E-Mail-Adressen von unautorisierter Benutzung zu unterscheiden. BATV bietet eine Methode, den Envelope-Sender von ausgehenden Mails zu signieren, indem ein einfacher geteilter Schlüssel hinzugefügt wird, der einen Hash der Adresse und zeitvariante Informationen kodiert, sowie einige zufällige Daten. Alles zusammen soll beweisen, dass die Mail wirklich von Ihnen stammt. Prinzipiell wird es dazu benutzt, Ablehnungsnachrichten (engl. *bounce messages*) abzuweisen, die nicht von Ihnen versendet wurden. Durch BATV können Sie nun herausfinden, ob Ablehnungsnachrichten, die Sie erhalten, wirklich durch eine von Ihnen versendete Mail ausgelöst wurden und nicht durch einen Spammer, der eine E-Mail mit Ihrer Adresse gefälscht hat. Wenn eine Ablehnungsnachricht eintrifft und die E-Mail ist nicht nach BATV signiert, dann wird der SMTP-Proxy die Nachricht nicht annehmen. Beachten Sie, dass die BATV-Signatur nach sieben Tagen abläuft. Um den Schlüssel (auch *BATV-Secret* genannt) zu ändern, der für die Verschlüsselung des Hashes der Envelope-Adresse MAIL FROM verwendet wird, gehen Sie zur Registerkarte *Mail Security >> SMTP >> Erweitert*.

Hinweis – Einige Mail-Transfer-Programme (*Mail Transfer Agents*, MTA) könnten E-Mails zurückweisen, deren Envelope-Absenderadresse mittels BATV verändert wurde. In diesem Fall müssen Sie für die betroffenen Absenderadressen, Empfängeradressen oder Domänen eine entsprechende Ausnahmeregel definieren.

SPF-Prüfung durchführen: SPF (*Sender Policy Framework*) ist ein System bei dem Domäneninhaber Informationen über Ihre E-Mailserver für ausgehende Mails veröffentlichen können. Domänen benutzen öffentliche Einträge, um Anfragen nach verschiedenen Diensten (Web, E-Mail, usw.) an jene Rechner

weiterzuleiten, die diese Dienste anbieten. Alle Domänen veröffentlichen MX-Einträge für E-Mail-bezogene Dienste, damit andere wissen, welche Rechner Mails für die Domäne entgegennehmen. SPF funktioniert durch Domänen, die zusätzlich eine Art „Rückwärts-MX“ veröffentlichen, um der Welt mitzuteilen, welche Rechner Mails von der Domäne versenden. Wenn der Empfänger eine Nachricht von einer bestimmten Domäne erhält, dann kann er diese Einträge überprüfen, um sicherzustellen, dass die Mail wirklich daher kommt, woher sie kommen soll.

Querverweis – Weitere Informationen erhalten Sie auf der Internetseite zu Sender Policy Framework²⁷.

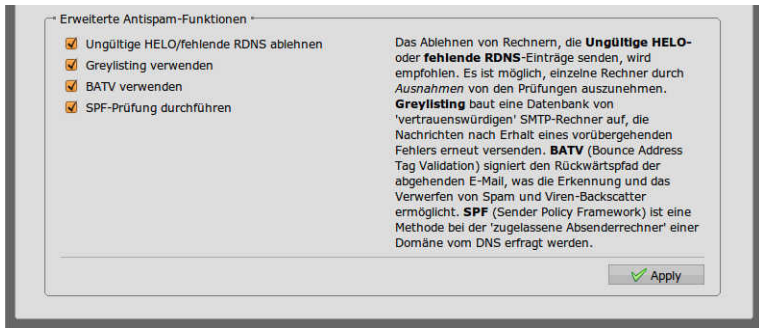


Figure 11.9 SMTP-Proxy: Erweiterte Antispam-Funktionen

Als zusätzliche Antispam-Funktion gleicht der SMTP-Proxy stillschweigend jede Empfängeradresse, die er erhält, mit Ihren Backend-Mailservern ab, bevor er die Mail für diese Adresse annimmt. E-Mails für ungültige Benutzeradressen werden nicht angenommen. Damit die Funktion greift, muss/müssen Ihr(e) Backend-Mailserver E-Mails von unbekannten Empfängern zur SMTP-Zeit ablehnen. Die Grundregel lautet: Wenn Ihr Backend-Server eine Nachricht ablehnt, lehnt sie der SMTP-Proxy ebenfalls ab.

Beachten Sie jedoch, dass die Empfängerüberprüfung *nicht* für vertrauenswürdige (authentifizierte) Rechner oder Relay-Rechner durchgeführt wird, da manche Benutzerprogramme (*User Agents*) ein Problem damit haben, wenn Empfänger während der SMTP-Übertragung abgelehnt werden. Gewöhnlich

²⁷ <http://www.openspf.org/>

(der Backend-Mailserver lehnt unbekannte Empfänger während der SMTP-Übertragung ab) wird Astaro Security Gateway Mails nur in den folgenden Fällen ablehnen (*bounce*):

- Wenn eine vertrauenswürdige Quelle oder ein Relay-Rechner eine Nachricht zu einem nicht verfügbaren Empfänger sendet.
- Wenn der Backen-Mailserver nicht erreichbar war, so dass Astaro Security Gateway den Empfänger nicht verifizieren konnte.

Astaro Security Gateway hindert Ihre(n) Backen-Mailserver jedoch nicht daran, NDRs (*non-delivery reports*, Berichte über Nicht-Auslieferung) oder Ablehnungen (*bounces*) zu versenden. Außerdem speichert Astaro Security Gateway positive Callout-Antworten des Mailservers 24 Stunden zwischen und negative zwei Stunden.

Ausnahmen

Auf der Registerkarte *SMTP >> Ausnahmen* können Sie vertrauenswürdige Rechner, Netzwerke, Absender und Empfänger definieren, die dann von Antivirus-, Antispam- und anderen Sicherheitsprüfungen ausgenommen werden.

Sicherheitshinweis – Da E-Mails mehrere Empfänger haben können und Astaro Security Gateway den Scan für das SMTP-Protokoll inline ausführt, wird die Überprüfung einer E-Mail gänzlich ausgesetzt, sobald einer von den Empfängern der E-Mail im Feld *Empfänger* aufgeführt ist.

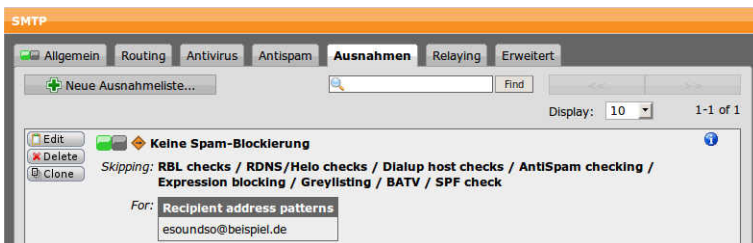


Figure 11.10 SMTP-Proxy: Ausnahmenliste

Um eine Ausnahmeregel anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Ausnahmen* auf *Neue Ausnahmeliste*.**
Das Dialogfenster *Ausnahmeliste erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Name: Geben Sie einen aussagekräftigen Name für diese Ausnahmeregel ein.

Diese Prüfungen ausnehmen: Wählen Sie die Sicherheitsprüfungen, von denen diese Liste ausgenommen werden soll. Weitere Information finden Sie unter *Mail Security >> SMTP >> Antivirus* und *Antispam*.

Für diese Quellrechner/-netzwerke: Wählen Sie die Quellrechner/-netzwerke (d.h. die Rechner oder Netzwerke, wo Nachrichten herkommen), die von den hier gewählten Sicherheitsprüfungen ausgenommen werden sollen.

Hinweis – Es muss keine Ausnahmeregel für Localhost angelegt werden, da lokale Nachrichten standardmäßig nicht gescannt werden.

Wenn Sie diese Option wählen, wird das Feld *Rechner/Netzwerke* geöffnet. Hier können Sie einen Rechner oder Netzwerk eingeben, indem Sie auf das Plus-Symbol oder das Ordnersymbol klicken.

Diese Absenderadressen: Wählen Sie die Absenderadressen, die von den gewählten Sicherheitsprüfungen ausgenommen werden sollen.

Wenn Sie diese Option wählen, wird das Feld *Absender* geöffnet. Sie können entweder eine vollständige E-Mailadresse eingeben (z. B. *esound-so@beispiel.de*) oder alle E-Mailadressen einer bestimmten Domäne, wobei Sie einen Asterisk (*) als Platzhalter verwenden (z. B. **@beispiel.de*).

Hinweis – Verwenden Sie die *Absender*-Option mit Bedacht, da Absenderadressen leicht gefälscht werden können.

Diese Empfängeradressen: Wählen Sie die Empfängeradressen, die von den gewählten Sicherheitsprüfungen ausgenommen werden sollen. Wenn Sie diese Option wählen, wird das Feld *Empfänger* geöffnet. Sie können entweder eine vollständige E-Mailadresse eingeben (z. B. *esound-so@beispiel.de*) oder alle E-Mailadressen einer bestimmten Domäne, wobei Sie einen Asterisk (*) als Platzhalter verwenden (z. B. **@beispiel.de*).

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die Ausnahmeregel hinzu.

3. Klicken Sie *Speichern*.

Die neue Ausnahmeregel wird in der Ausnahmeliste angezeigt.

Um eine Ausnahmeregel zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Relaying

Auf der Registerkarte *Mail Security >> SMTP >> Relaying* kann der SMTP-Proxy als Mail-Relay-Server konfiguriert werden. Ein Mail-Relay ist ein Server, der so konfiguriert ist, dass er bestimmten Benutzern, Benutzergruppen oder Rechnern erlaubt, Mails durch ihn hindurch zu leiten, an Domänen, die lokal nicht erreichbar sind.

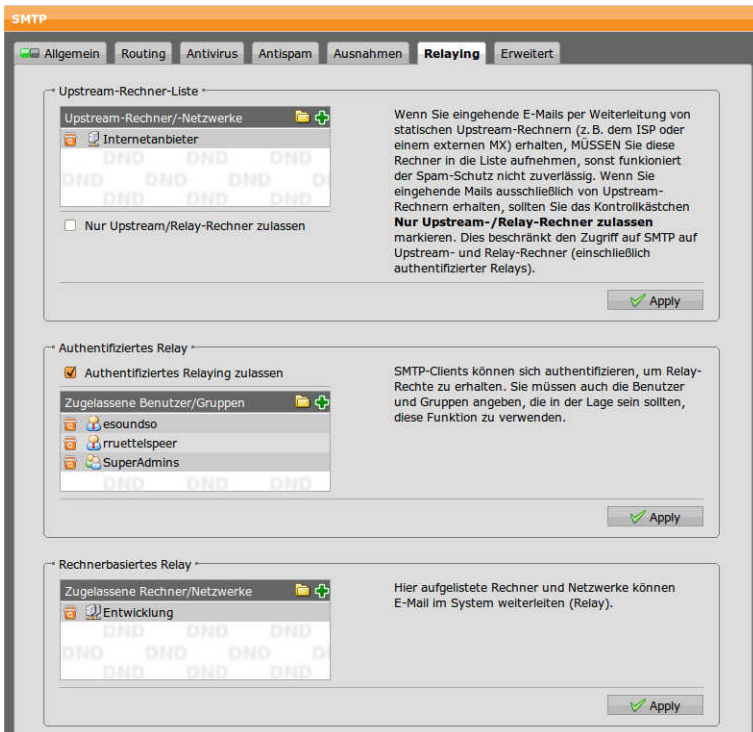


Figure 11.11 SMTP-Proxy: Konfiguration von Relaying

Upstream-Rechner-Liste

Ein Upstream-Rechner ist ein Rechner, der E-Mails an Sie weiterleitet, z. B. Ihr ISP oder externer MX. Wenn Sie eingehende E-Mails von statischen Upstream-Rechnern erhalten, ist es nötig, dass Sie diese Rechner hier eintragen. Andernfalls wird der Spamschutz nicht richtig funktionieren.

Um einen Upstream-Rechner hinzuzufügen, klicken Sie entweder auf das Plus-Symbol oder, um Rechner per Drag&Drop aus der *Networks*-Objektleiste zu holen, das Ordnersymbol. Wenn Sie ausschließlich Upstream-Rechner zulassen möchten, wählen Sie die Option *Nur Upstream/Relay-Rechner zulassen*. Der SMTP-Zugriff wird dann auf die definierten Upstream-Rechner (und authentifizierten Relays, siehe unten) begrenzt. Klicken Sie *Übernehmen*, um Ihre Änderungen zu speichern.

Authentifiziertes Relay

SMTP-Clients können sich authentifizieren, um Relaying-Rechte zu erlangen. Wählen Sie die Option *Authentifiziertes Relaying zulassen* und geben Sie die Benutzer oder Benutzergruppen an, die diese Funktion verwenden dürfen. Klicken Sie *Übernehmen*, um Ihre Änderungen zu speichern.

Rechnerbasiertes Relay

Mail-Relaying kann auch rechnerbasiert ablaufen. Wenn Ihr lokaler Mailserver oder Ihre Mail-Clients in der Lage sein sollen, den SMTP-Proxy als Mail-Relay zu verwenden, müssen Sie die Netzwerke und Rechner, die Mails über das Relay versenden dürfen, zum Feld *Zugelassene Rechner/Netzwerke* hinzufügen.

Warnung – Wählen Sie im Feld *Zugelassene Rechner/Netzwerke* niemals *Any* aus, denn das würde zu einem offenen Mail-Relay führen, welches es jedem aus dem Internet gestattet, Nachrichten über den SMTP-Proxy zu senden. Spam-Versender werden das schnell herausfinden und das wird zu erheblichem E-Mail-Aufkommen führen. Im schlimmsten Fall werden Sie auf Spam-Versender-Blacklists Dritter geführt. In den meisten Konfigurationen sind die einzigen Rechner, die als Mail-Relay agieren dürfen, die Mailserver in Ihrem Netzwerk.

Klicken Sie *Übernehmen*, um Ihre Änderungen zu speichern.

Rechner-/Netzwerk-Blacklist

Hier können Sie Rechner und Netzwerke bestimmen, die vom SMTP-Proxy blockiert werden sollen. Klicken Sie *Übernehmen*, um Ihre Änderungen zu speichern.



Figure 11.12 SMTP-Proxy: Aktivierung der Blacklist für Rechner/Netzwerke

Inhaltsscan für (ausgehende) Relay-Nachrichten

Wenn diese Option gewählt ist, werden auch Nachrichten auf bösartigen Inhalt gescannt, die entweder von authentifizierten oder rechnerbasierten Relays gesendet werden. Klicken Sie *Übernehmen*, um Ihre Änderungen zu speichern.

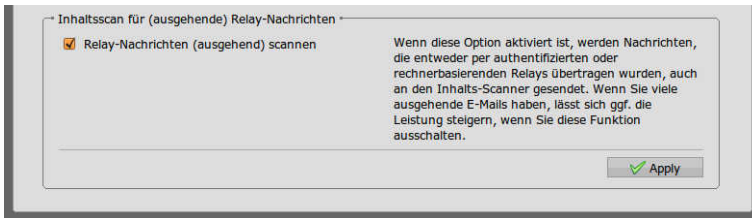


Figure 11.13 SMTP-Proxy: Aktivierung des Inhaltsscans für Relay-Nachrichten

Erweitert

Auf der Registerkarte *SMTP >> Erweitert* können Sie zusätzliche Sicherheitsoptionen für den SMTP-Proxy konfigurieren, wie z. B. Smarthost-Einstellungen oder die Ausnahmeliste für den Transparenzmodus.

Übergeordneter Proxy

Ein übergeordneter Proxy (auch *Parent* oder *Upstream* Proxy) wird in Ländern benötigt, in denen der Zugang zum Internet nur über einen staatlich kontrollierten Proxy erlaubt ist. Falls Ihre Sicherheitsbestimmungen die Nutzung eines übergeordneten Proxy erforderlich machen, so können Sie diesen hier durch Angabe einer Rechnerdefinition und eines Ports konfigurieren.

Übergeordneten Proxy verwenden: Wählen Sie diese Option, um einen übergeordneten Proxy zu verwenden. Geben Sie einen Rechnernamen und den Port des Proxy ein.

Dieser Proxy erfordert Authentifizierung: Falls der übergeordnete Proxy Authentifizierung erfordert, geben Sie den Benutzernamen und das Kennwort hier ein.

Transparenzmodus

Um den Transparenzmodus für SMTP zu aktivieren, markieren Sie das Auswahlkästchen und klicken Sie *Übernehmen*.

Rechner und Netzwerke, die im Feld *Auszunehmende Rechner/Netze* aufgeführt sind, werden im Gegensatz zum restlichen SMTP-Verkehr nicht transparent überwacht. Um jedoch SMTP-Verkehr für diese Rechner und Netzwerke zuzulassen, wählen Sie die Option *SMTP-Verkehr für aufgelistete Rechner/Netze zulassen*. Wenn Sie diese Option nicht wählen, müssen Sie spezielle Paketfilterregeln für die hier aufgeführten Rechner und Netzwerke anlegen.

TLS-Einstellungen

Das Sicherheitssystem handelt die TLS-Verschlüsselung mit allen Gegenstellen aus, die sie unterstützen. Falls ein bestimmter Rechner oder Netzwerk Probleme mit TLS-Verschlüsselung haben, können diese im Feld *TLS-Aushandlungsrechner/-netze ausnehmen* angegeben und das entsprechende TLS-Zertifikat aus der Auswahlliste auswählen. Damit wird dieser Rechner oder Netzwerk von der TLS-Verschlüsselung ausgenommen. Klicken Sie *Übernehmen*, um Ihre Änderungen zu speichern.

DomainKeys Identified Mail (DKIM)

DKIM ist eine Methode, um ausgehende Nachrichten kryptografisch zu signieren. Um DKIM-Signierung zu verwenden, geben Sie Ihren privaten RSA-Schlüssel und den dazugehörigen Schlüsselselektor (engl. *key selector*), den Schlüsselnamen, in die entsprechenden Felder ein. Fügen Sie dann die Domänen, für die Sie E-Mails signieren wollen, zum Feld *DKIM-Domänen* hinzu. Klicken Sie *Übernehmen*, um Ihre Änderungen zu speichern.

Vertraulichkeitsfußzeile

Sie können für jede ausgehende E-Mail eine Vertraulichkeitsfußzeile hinzufügen oder anpassen, die Benutzer zum Beispiel darüber informiert, dass die E-Mail vertrauliche oder privilegierte Informationen enthalten kann. Die Vertraulichkeitsfußzeile wird jedoch nicht angehängt, wenn die E-Mail eine Antwort-E-Mail ist (d. h. sie besitzt einen *In-Reply-To-Header*) oder wenn die Inhaltsart der E-Mail nicht bestimmt werden konnte.

Hinweis – Das Hinzufügen einer Fußzeile zu Nachrichten, die bereits signiert oder verschlüsselt sind, durch ein E-Mail-Programm (z. B. Microsoft Outlook oder Mozilla Thunderbird), wird ihre Signatur kaputt und damit ungültig machen. Wenn Sie digitale Zertifikate auf Client-Seite erzeugen wollen, deaktivieren Sie die Vertraulichkeitsfußzeilen-Option. Wenn Sie jedoch nicht auf Datenschutz und Authentifizierung in Ihrer E-Mail-Kommunikation verzichten möchten und dennoch eine allgemeine Vertraulichkeitsfußzeile verwenden wollen,

dann sollten Sie in Betracht ziehen, die eingebaute Funktion von Astaro Security Gateway einzusetzen. E-Mail-Verschlüsselung, die auf dem Gateway durchgeführt wird, bedeutet, dass die Fußzeile zur Nachricht hinzugefügt wird, bevor die digitale Signatur erzeugt wird, wodurch die Signatur intakt bleibt.

Erweiterte Einstellungen

Hier können Sie unter anderem den SMTP-Rechnernamen und die Postmaster-Adresse einstellen.

SMTP-Rechnername: Wenn ein *SMTP-Rechnername* definiert ist, wird der SMTP-Proxy diesen Namen in HELO- und in SMTP-Banner-Nachrichten verwenden. Standardmäßig ist der Rechnername des Systems angegeben.

Postmaster-Adresse: Tragen Sie die E-Mail-Adresse des Postmasters, des E-Mail-Verantwortlichen, für das Sicherheitssystem ein, an den die Nachrichten weitergeleitet werden, die in der Form `postmaster@[192.168.16.8]` gesendet werden, wobei die IP-Adresse eine der IP-Adressen des Sicherheitssystems ist. Die Annahme solcher Nachrichten ist ein Erfordernis des RFC.

BATV-Schlüssel: Hier können Sie den automatisch generierten BATV-Schlüssel (engl. *BATV secret*) ändern, der vom SMTP-Proxy benutzt wird. Der BATV-Schlüssel ist ein geteilter Schlüssel, der benutzt wird, um die Envelope-Adresse (dt. Umschlagadresse) `MailFrom` einer E-Mail zu signieren, wodurch die Erkennung ungültiger Absenderadressen von Ablehnungsnachrichten möglich wird. Wenn Sie mehrere MXs für Ihre Domänen verwenden, können Sie den BATV-Schlüssel ändern, damit er auf allen Systemen gleich ist.

Max. Nachrichtengröße: Die maximale Größe der E-Mails, die vom Proxy akzeptiert wird. Diese Einstellung bezieht sich sowohl auf eingehende als auch ausgehende E-Mails. Falls Ihr Backend-Server eine Begrenzung in Bezug auf die Größe von E-Mails hat, dann sollten Sie hier denselben oder einen niedrigeren Wert einstellen.

Max. Verbindungen: Die maximale Anzahl gleichzeitiger Verbindungen, die der Proxy zulässt. Der Standardwert ist 20.

Max. Verb./Rechner: Die maximale Anzahl von Rechnern pro Verbindung, die der Proxy zulässt. Der Standardwert ist 10.

Max. Mails/Verbindung: Die maximale Anzahl an Mails pro Verbindung, die der Proxy zulässt. Der Standardwert ist 1000.

Max. Empf./Mail: Die maximale Anzahl an Empfängern pro Mail, die der Proxy zulässt. Der Standardwert ist 500.

Fußzeilen-Modus: Hier können Sie bestimmen, wie Fußzeilen zu E-Mails hinzugefügt werden. *MIME-Teil* fügt die Fußzeile als Extra-MIME-Teil hinzu. Bereits vorhandene Teilkodierungen werden nicht geändert und nationale Sprachzeichen bleiben erhalten. Die andere Methode ist *Inline*, das bedeutet,

dass die Fußzeile von der eigentlichen Mail durch das Trennzeichen - getrennt ist. Bei diesem Modus können Sie wählen, ob die Fußzeile nach Unicode (UTF-8) konvertiert wird oder nicht. Eine Unicode-Umwandlung verändert die Nachricht dahingehend, dass nationale Sprachzeichen in der Fußzeile erhalten bleiben.

Smarthost-Einstellungen: Ein Smarthost ist eine Art Mail-Relay-Server, der es einem SMTP-Server erlaubt, Mails an einen Upstream-Mail-Server zu routen statt direkt an den Server des Empfängers. So ein Smarthost verlangt meistens, dass der Absender sich authentifiziert, um sicherzustellen, dass der Absender auch die Berechtigung besitzt, Mails durch den Smarthost weiterzuleiten.

Smarthost verwenden: Wenn Sie einen Smarthost für den Mailversand verwenden wollen, markieren Sie dieses Auswahlkästchen und geben Sie den Rechnernamen oder die IP-Adresse des Smarthost ein. Sie können auch eine Portnummer hinzufügen, die Sie von der IP-Adresse durch einen Doppelpunkt trennen, z. B. 195.99.144.85:443. In diesem Fall wird der Proxy Mails nie selbst zustellen, sondern diese immer an den Smarthost senden. Wenn der Smarthost Authentifizierung erfordert, wählen Sie die Option *Dieser Smarthost erfordert Authentifizierung* und geben Sie einen Benutzernamen und ein Kennwort in die entsprechenden Textfelder ein. Als Authentifizierungsmethode wird sowohl *Plain* als auch *Login* unterstützt.

SMTP-Profile

Der SMTP-Proxy von Astaro Security Gateway ermöglicht es Ihnen, alternative SMTP-Profile anzulegen, die dann verschiedenen Domänen zugeordnet werden können. Auf diese Weise können Sie Domänen bestimmen, die ein anderes Profil verwenden sollen als das Standardprofil, das unter *Mail Security >> SMTP* konfiguriert ist. Die Reihenfolge der Funktionen, die in Form von Registerkarten dargestellt sind, spiegelt die Abfolge einzelner Schritte während der SMTP-Zeit wider.

Um ein SMTP-Profil anzulegen, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie den SMTP-Profilmodus.**

Wählen Sie auf der Registerkarte *Mail Security >> SMTP >> Allgemein* die Option *Profilmodus* und klicken Sie *Übernehmen*. Das Anlegen von SMTP-Profilen im Menü *Mail Security >> SMTP-Profile* ist aktiviert.

2. **Klicken Sie auf der Registerkarte *SMTP-Profile* auf *Neues Profil erstellen*.**

Ein Dialogfenster wird geöffnet.

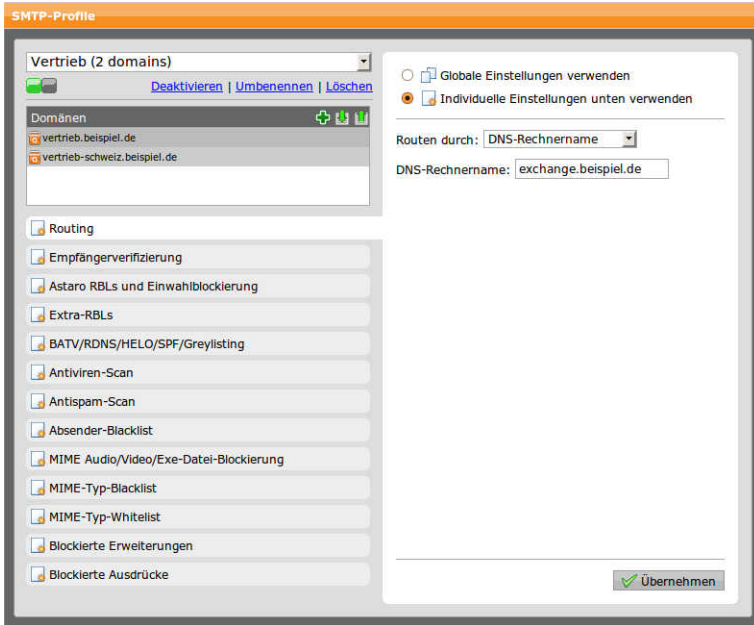


Figure 11.14 SMTP-Profil: Konfiguration eines SMTP-Profiles

3. **Geben Sie einen aussagekräftigen Namen für das Profil an und klicken Sie OK.**

Die Seite mit den Einstellungen für das Profil wird geöffnet.

4. **Fügen Sie eine oder mehrere Domänen hinzu.**

Geben Sie im Feld *Domänen* eine oder mehrere Domänen an.

Einstellungen in diesem Profil werden für diese Domänen gelten.

5. **Nehmen Sie die folgenden Einstellungen vor:**

Sie brauchen nur die Einstellungen für jene Funktionen vorzunehmen, die Sie verwenden wollen. Für jede der folgenden Funktionen können Sie entscheiden, ob die hier vorgenommenen individuellen Einstellungen verwendet werden sollen oder die globalen Einstellungen von *Mail Security* > > *SMTP*. Standardmäßig ist die individuelle Einstellung vorausgewählt. Die individuellen Einstellungen für jede Funktion sind unten beschrieben.

Hinweis – Verschlüsselte E-Mails, deren Absenderadressen einen Domänennamen beinhalten, welcher hier konfiguriert ist, können nicht entschlüsselt werden, wenn Sie die Ver-/Entschlüsselungsfunktion von Astaro Security

Gateway verwenden. Aus diesem Grund sollten Sie keine Profile für externe E-Mail-Domänen anlegen.

Alle Einstellungen, die Sie hier vornehmen können, können unter *Mail Security >> SMTP* auch global vorgenommen werden. Deshalb werden hier nur eine Liste der Einstellungsmöglichkeiten und die Unterschiede zu den globalen Einstellungen aufgeführt. Dazu gibt es Querverweise zu der jeweils entsprechenden globalen Einstellung, wo Sie detaillierte Informationen finden.

Die folgenden Einstellungen können vorgenommen werden:

- **Routing:** Auf der Registerkarte *Routing* können Sie Domänen- und Routingziele für den SMTP-Proxy konfigurieren. Außerdem können Sie festlegen, wie Empfänger verifiziert werden sollen.

- Statische Rechnerliste
- DNS-Rechnername
- MX-Einträge

Weitere Informationen finden Sie unter *Mail Security >> SMTP >> Routing*.

- **Empfängerverifizierung**

Empfänger verifizieren: Hier können Sie festlegen, ob und wie E-Mail-Empfänger verifiziert werden.

- **Mit Serveranfrage:** Es wird eine Anfrage an den Server geschickt, um den Empfänger zu verifizieren.
- **Im Active Directory:** Es wird eine Anfrage an den Active-Directory-Server geschickt, um den Empfänger zu verifizieren. Um Active Directory benutzen zu können, müssen Sie einen Active-Directory-Server unter *Benutzer >> Authentifizierung >> Server* angegeben haben. Geben Sie einen BaseDN im Feld *Alternativer BaseDN* ein.

Hinweis – Die Benutzung von Active-Directory-Empfängerverifizierung kann dazu führen, dass Nachrichten abgelehnt werden, im Fall dass der Server nicht antwortet.

- **Aus:** Sie können die Empfängerverifizierung vollständig ausschalten, aber das ist nicht empfehlenswert, da es zu einem höheren Spamaufkommen und Wörterbuchangriffen führt. Dadurch erhöhen Sie die Wahrscheinlichkeit, dass Ihre Quarantäne mit unerbetenen Nachrichten „überflutet“ wird.

Weitere Informationen finden Sie unter *Mail Security >> SMTP >> Routing*.

- **Astaro RBLs und Einwahlblockierung:** Hier können Sie IP-Adressen blockieren, die mit Spamversand in Verbindung gebracht werden.

- Empfohlene RBLs verwenden
- Einwahl-/Privatrechner blockieren

Weitere Informationen finden Sie unter *Mail Security >> SMTP >> Antispam*.

- **Extra-RBLs:** Sie können weitere RBL-Seiten hinzufügen, um die Antispam-Fähigkeiten von Astaro Security Gateway zu verbessern. Weitere Informationen finden Sie unter *Mail Security >> SMTP >> Antispam*. Beachten Sie, dass Sie als dritte Option die globalen Einstellungen zu Ihren individuellen Einstellungen hier hinzufügen können.

- **BATV/RDNS/HELO/SPF/Greylisting:** Auf dieser Registerkarte sind verschiedene erweiterte Optionen vereint, die die Antispam-Fähigkeiten von Astaro Security Gateway verbessern.

- Ungültige HELO/fehlende RDNS ablehnen
- Greylisting verwenden
- BATV verwenden
- SPF-Prüfung durchführen

Weitere Informationen finden Sie unter *Mail Security >> SMTP >> Antispam*.

- **Antiviren-Scan:** Sie können konfigurieren, wie mit Nachrichten verfahren wird, die bösartigen Inhalt besitzen. Die folgenden Aktionen sind möglich:

- Aus
- Quarantäne
- Verwerfen

Sie können zwischen den folgenden Antivirus-Scan-Optionen wählen:

- Einzelscan: bietet maximale Leistung.
- Doppelscan: bietet maximale Erkennungsrate.

Weitere Informationen finden Sie unter *Mail Security >> SMTP >> Antivirus*.

- **Antispam-Scan:** Hier können Sie konfigurieren, wie mit unerbetenen kommerziellen E-Mails verfahren werden soll. Sowohl für Spam als auch für bestätigten Spam können Sie zwischen den folgenden Optionen wählen:

- Aus
- Warnen
- Quarantäne
- Verwerfen

Weitere Informationen finden Sie unter *Mail Security >> SMTP >> Antispam*.

- **Absender-Blacklist:** Der Envelope-Absender eingehender SMTP-Sitzungen wird mit den Adressen auf dieser Blacklist verglichen. Wenn der Envelope-Absender auf der Blacklist gefunden wird, wird die Nachricht verworfen. Weitere Informationen finden Sie unter *Mail Security >> SMTP >> Antispam*. Beachten Sie, dass Sie als dritte Option die globalen Einstellungen zu Ihren individuellen Einstellungen hier hinzufügen können.
- **MIME Audio/Video/Exe-Datei-Blockierung:** Der MIME-Typ-Filter liest den MIME-Typ von E-Mail-Inhalten aus. Sie können wählen, welche Inhaltsarten Sie unter Quarantäne stellen wollen:
 - Audioinhalte
 - Videoinhalte
 - Ausführbare Dateien

Weitere Informationen finden Sie unter *Mail Security >> SMTP >> Antivirus*.

- **MIME-Typ-Blacklist:** Hier können Sie zusätzliche MIME-Typen hinzufügen, die unter Quarantäne gestellt werden sollen. Weitere Informationen finden Sie unter *Mail Security >> SMTP >> Antivirus*. Beachten Sie, dass Sie als dritte Option die globalen Einstellungen zu Ihren individuellen Einstellungen hier hinzufügen können.
- **MIME-Typ-Whitelist:** Hier können Sie MIME-Typen angeben, die nicht unter Quarantäne gestellt werden sollen. Weitere Informationen finden Sie unter *Mail Security >> SMTP >> Antivirus*. Beachten Sie, dass Sie als dritte Option die globalen Einstellungen zu Ihren individuellen Einstellungen hier hinzufügen können.
- **Blockierte Erweiterungen:** Mit dieser Funktion können Sie E-Mails unter Quarantäne stellen (eine Warnung wird ausgegeben), die bestimmte Dateitypen enthalten, basierend auf deren Dateiendung (z. B. ausführbare Dateien). Weitere Informationen finden Sie unter *Mail Security >> SMTP >> Antivirus*. Beachten Sie, dass Sie als dritte Option die globalen Einstellungen zu Ihren individuellen Einstellungen hier hinzufügen können.
- **Blockierte Ausdrücke:** Der Ausdruckfilter prüft den Inhalt von Nachrichten, die den SMTP-Proxy passieren, auf bestimmte Ausdrücke. Verdächtige E-Mails werden blockiert. Weitere Informationen finden Sie unter *Mail Security >> SMTP >> Antispam*. Beachten Sie, dass Sie als dritte Option die globalen Einstellungen zu Ihren individuellen Einstellungen hier hinzufügen können.

6. Klicken Sie *Übernehmen*.

Ihre Einstellungen werden gespeichert. Das neue Profil erscheint auf der Liste *SMTP-Profile*.

Hinweis – Wenn Sie die Option *Globale Einstellungen verwenden* für eine Einstellung verwenden und *Übernehmen* klicken, wechselt das Symbol der Funktion zum Symbol für globale Einstellungen. Dadurch erhalten Sie leicht einen Überblick darüber, für welche Funktionen Sie die globalen Einstellungen verwenden und für welche Funktionen die individuellen Einstellungen.

Um ein Profil umzubenennen, zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen oben unter der Auswahlliste der Profile.

POP3

Im Menü *Mail Security* >> *POP3* können Sie den POP3-Proxy für eingehende E-Mails konfigurieren. Das *Post Office Protocol 3* ist ein Internet-Standardprotokoll auf Anwendungsebene, das es ermöglicht, E-Mails von einem entfernten Server abzuholen. Der POP3-Proxy arbeitet im Transparenzmodus, das heißt alle POP3-Anfragen, die über Port 110 aus dem internen Netzwerk kommen, werden abgefangen und, unsichtbar für den Client, durch den Proxy geleitet. Der Vorteil dieses Modus' ist, dass keine zusätzliche Verwaltung oder client-seitige Konfiguration nötig ist.

Hinweis – Es kann nötig sein, die Einstellungen für die Server-Zeitüberschreitung in der E-Mail-Client-Konfiguration zu erhöhen. Meistens ist die Voreinstellung von einer Minute oder weniger zu gering, insbesondere wenn große E-Mails abgeholt werden.

Das POP3-Protokoll nimmt keine serverseitige Verfolgung davon vor, welche E-Mails bereits abgeholt wurden. Im Allgemeinen holt ein Mail-Client eine E-Mail ab und löscht sie danach auf dem Server. Wenn der Client jedoch so eingestellt ist, dass er keine E-Mails löscht, dann wird auch auf Serverseite nicht gelöscht und der Client nimmt die Verfolgung davon vor, welche E-Mails bereits abgeholt wurden.

Allgemein

Auf der Registerkarte *Mail Security* >> *POP3* >> *Allgemein* können Sie Grundeinstellungen für den POP3-Proxy vornehmen.

Um den POP3-Proxy zu konfigurieren, gehen Sie folgendermaßen vor:

1. Aktivieren Sie den POP3-Proxy.

Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche.

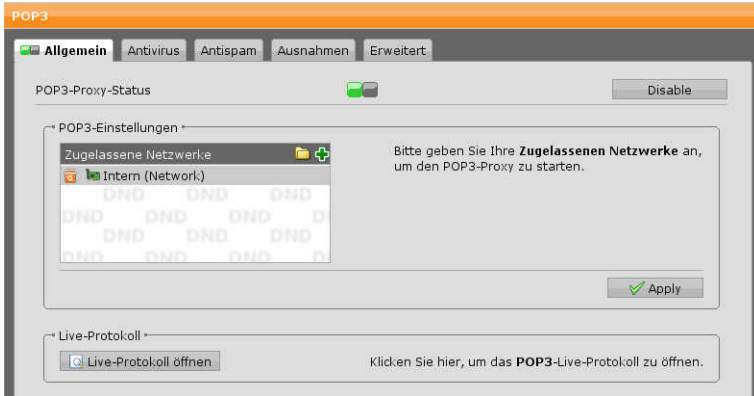


Figure 11.15 POP3-Proxy: Grundkonfiguration

Die Statusampel wird gelb und der Abschnitt *POP3 settings* kann nun bearbeitet werden.

2. Wählen Sie die zugelassenen Netzwerke aus.

Wählen Sie die Netzwerke aus, deren POP3-Verkehr über den Proxy laufen soll. Das interne Netzwerk (*Internal Network*) ist voreingestellt.

3. Klicken Sie *Übernehmen*.

Ihre Einstellungen werden gespeichert.

Um die Konfiguration abzubrechen, klicken Sie auf die Schaltfläche *Abort Enable* oder auf die gelbe Statusampel.

Live-Protokoll

Im *POP3-Live-Protokoll* werden die Aktivitäten des POP3-Proxy protokolliert. Alle eingehenden E-Mails werden darin aufgeführt. Klicken Sie auf die Schaltfläche, um das Live-Protokoll in einem neuen Fenster zu öffnen.

Antivirus

Die Registerkarte *Antivirus* enthält verschiedene Maßnahmen gegen E-Mails, die einen schädlichen oder gefährlichen Inhalt enthalten wie Viren, Würmer oder andere Schadsoftware.

Antiviren-Scan

Wenn Sie diese Option wählen, werden E-Mails nach unerwünschtem Inhalt gescannt wie z. B. Viren, Trojanische Pferde oder verdächtige Dateitypen. Nachrichten mit schädlichem Inhalt werden blockiert oder in der E-Mail-Quarantäne

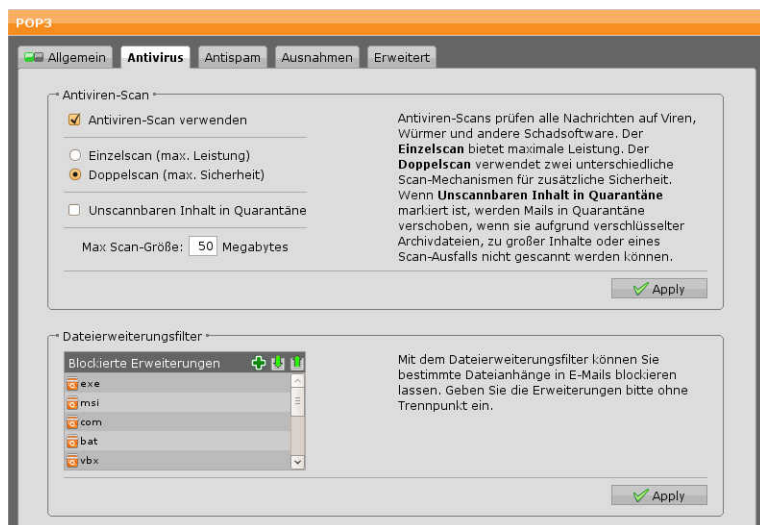


Figure 11.16 POP3-Proxy: Konfiguration der Antivirus-Einstellungen

gespeichert. Benutzer können ihre unter Quarantäne stehenden E-Mails ansehen und freigeben, entweder über das Astaro Benutzerportal oder den täglichen Quarantänebericht. Nachrichten, die schädlichen Inhalt enthalten, können jedoch nur vom Administrator aus der Quarantäne freigegeben werden, über den Mail-Manager. Astaro Security Gateway bietet für höchstmöglichen Schutz mehrere Antivirus-Mechanismen:

- **Einzelscan:** Standardeinstellung, die maximale Leistung bietet.
- **Doppelscan:** Bietet maximale Erkennungsrate, indem aller E-Mails von zwei verschiedenen Virensclannern gescannt wird.

Unscannbaren Inhalt in Quarantäne: Wenn Sie diese Option wählen, werden E-Mails mit Inhalt, der nicht gescannt werden kann, unter Quarantäne gestellt. Unscannbarer Inhalt können verschlüsselte Archive oder sehr große Inhalte sein, oder es kann ein technischer Grund vorliegen wie z. B. der Ausfall eines Scanners.

Max. Scangröße: Geben Sie die maximale Größe der Nachrichten an, die vom Antivirus-Mechanismus gescannt werden soll. Nachrichten, die größer sind als der angegebene Wert, werden nicht gescannt.

Klicken Sie *Übernehmen*, um Ihre Einstellungen zu speichern.

Dateierweiterungsfilter

Diese Funktion filtert E-Mails mit Dateianhängen basierend auf deren Erweiterungen (z. B. ausführbare Binärdateien) aus dem Internetverkehr heraus, wenn diese eine Dateierweiterung besitzen, die in der Liste *Blockierte Erweiterungen* aufgeführt ist. Sie können weitere Dateierweiterungen hinzufügen oder solche Erweiterungen aus der Liste löschen, die nicht blockiert werden sollen. Um eine Dateierweiterung hinzuzufügen, klicken Sie auf das Plus-Symbol im Feld *Blockierte Erweiterungen* und geben Sie die Dateierweiterung ein, die blockiert werden soll, z. B. exe (ohne den Punkt als Trennzeichen). Klicken Sie *Übernehmen*, um Ihre Einstellungen zu speichern.

Hinweis – Verschlüsselte zip-Archive können nicht nach schädlichem Inhalt durchsucht werden und passieren den Virusscanner ungehindert. Um Ihr Netzwerk vor Schadsoftware aus verschlüsselten zip-Dateien zu schützen, sollten Sie in Betracht ziehen, zip-Dateien gänzlich zu blockieren.

Antispam

Astaro Security Gateway kann so konfiguriert werden, dass es unerbetene Spam-E-Mails entdeckt und Spam-Übermittlungen von bekannten oder verdächtigen Spam-Verteilern identifiziert. Die Konfigurationsoptionen auf der Registerkarte *Antispam* ermöglichen die Konfiguration von POP3-Sicherheitsfunktionen, die darauf ausgelegt sind, Ihr Netzwerk vor dem Empfang von unerbetenen kommerziellen E-Mails zu schützen.

Hinweis – Die E-Mails werden bis zu einer Größe von 128 KB auf Spam geprüft. Alle größeren E-Mails werden nicht gescannt.

Spamfilter

Astaro Security Gateway bietet eine heuristische Prüfung eingehender E-Mails auf Spam-Eigenschaften. Es benutzt dafür SMTP-Envelope-Informationen (*envelope* = Umschlag) und eine interne Datenbank mit heuristischen Tests und Eigenschaften. Die Spamfilter-Option bewertet Nachrichten basierend auf ihrem Inhalt und SMTP-Envelope-Informationen. Höhere Werte deuten auf eine höhere Spam-Wahrscheinlichkeit hin.

Mit den folgenden beiden Optionen können Sie festlegen, was mit Nachrichten geschehen soll, denen einen gewissen Spam-Wert zugewiesen bekommen

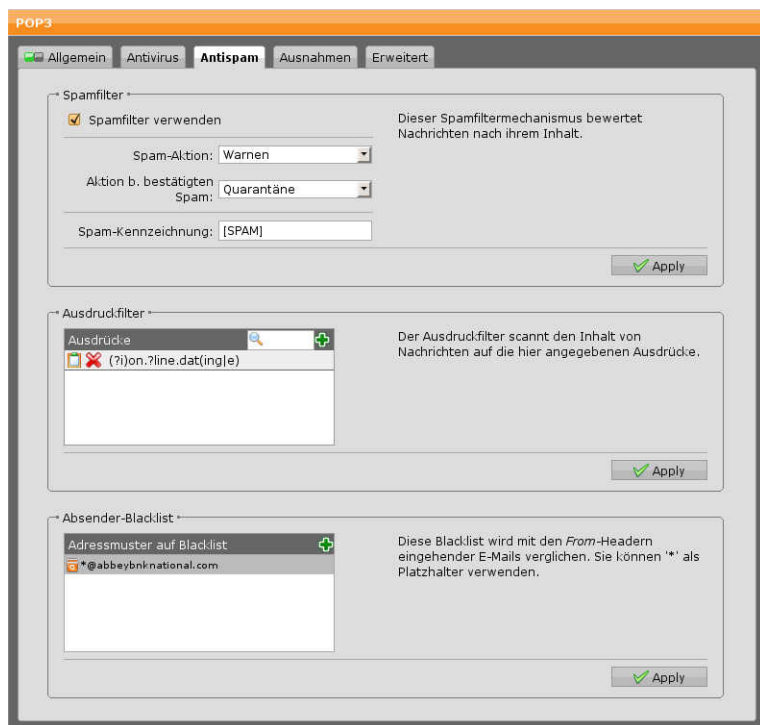


Figure 11.17 POP3-Proxy: Konfiguration der Antispam-Einstellungen

haben. Das stellt sicher, dass potenzielle Spam-E-Mails von der Firewall anders behandelt werden.

- **Spam-Aktion:** Hier können Sie festlegen, was mit Nachrichten geschieht, die als möglicher Spam eingestuft wurden. Beachten Sie, dass es Fehlfunde geben kann, z. B. Newsletter, wodurch durch Verwerfen E-Mails verloren gehen können.
- **Aktion bei bestätigtem Spam:** Hier können Sie festlegen, was mit Nachrichten geschieht, die sicher Spam sind.

Sie können zwischen verschiedenen Aktionen für diese beiden Arten von Spam wählen:

- **Aus:** Es werden keine Nachrichten als Spam markiert oder ausgefiltert.
- **Warnen:** Es werden keine Nachrichten ausgefiltert. Stattdessen wird eine Spam-Markierung („Flag“) zum Header der Nachricht hinzugefügt und der Betreff der Nachricht erhält einen Spam-Kennzeichner.
- **Quarantäne:** Die Nachricht wird blockiert und in die E-Mail-Quarantäne verschoben. Nachrichten in Quarantäne können entweder über das Benutzerportal oder den täglichen Quarantänebericht eingesehen werden.

Spam-Kennzeichner: Mit dieser Option können Sie eine Kennzeichnung für Spam-Nachrichten festlegen, d. h. dass eine Zeichenkette zur Betreffzeile der Nachricht hinzugefügt wird, die es einfach macht, Spam-Nachrichten schnell als solche zu erkennen. Standardmäßig wird die Zeichenkette **SPAM** benutzt, um Nachrichten als Spam zu kennzeichnen.

Ausdruckfilter

Der Ausdruckfilter scannt den Inhalt von Nachrichten, die durch den SMTP-Proxy geleitet werden, auf spezifische Ausdrücke. Verdächtige E-Mails werden blockiert. Wenn auf der Registerkarte *Mail Security >> POP3 >> Erweitert* die Funktion *Vorabholung verwenden* eingeschaltet ist, wird die E-Mail unter Quarantäne gestellt. Ausdrücke können in Form von *Perl Compatible Regular Expressions* (Perl-kompatiblen regulären Ausdrücken) eingegeben werden. Einfache Zeichenfolgen wie „Online Dating“ werden ohne Berücksichtigung der Groß-/Kleinschreibung interpretiert.

Klicken Sie *Übernehmen*, um Änderungen zu speichern.

Absender-Blacklist

Der Envelope-Sender (dt. Absender auf „Umschlag“) von eingehenden POP3-Sitzungen wird mit den Adressen auf dieser Blacklist (dt. schwarze Liste) abgeglichen. Wenn der Envelope-Sender auf der Blacklist gefunden wird, wird die Nachricht unter Quarantäne gestellt und mit *Other* in der Betreffzeile markiert.

Um ein neues Adressmuster zur Blacklist hinzuzufügen, klicken Sie auf das Plus-Symbol im Feld *Adressmuster auf Blacklist*, geben Sie eine (oder einen Teil einer) Adresse ein und klicken Sie *Übernehmen*. Sie können einen Asterisk (*) als Platzhalter verwenden, z. B. **@abbeybnknational.com*.

Ausnahmen

Auf der Registerkarte *POP3 >> Ausnahmen* können Sie Clientrechner/-Netzwerke und Absenderadressen festlegen, die von verschiedenen Sicherheitsmaßnahmen ausgenommen werden sollen.



Figure 11.18 POP3-Proxy: Ausnahmen definieren

Um eine Ausnahmeregel anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Ausnahmen* auf *Neue Ausnahmeliste*.** Das Dialogfenster *Ausnahmeliste erstellen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Name: Geben Sie einen aussagekräftigen Name für diese Ausnahmeregel ein.

Diese Prüfungen ausnehmen: Die Liste kann von den folgenden Sicherheitsfunktionen ausgenommen werden. Weitere Informationen finden Sie unter *Mail Security >> SMTP >> Antivirus* und *Antispam*.

Für diese Clientrechner/-Netzwerke: Wählen Sie die Rechner/Netzwerke (d. h. die Rechner oder Netzwerke, wo Nachrichten herkommen), die von den von dieser Ausnahmeregel definierten Sicherheitsmaßnahmen ausgenommen sein sollen.

Hinweis – Für Localhost muss keine Ausnahmeregel angelegt werden, da lokale Nachrichten standardmäßig nicht gescannt werden.

Wenn Sie diese Option auswählen, wird das Dialogfenster *Clientrechner/-Netzwerke* geöffnet. Sie können einen Rechner oder ein Netzwerk hinzufügen, indem Sie auf das Plus-Symbol oder das Ordner-Symbol klicken.

Diese Absenderadressen: Wählen Sie die Absender-E-Mail-Adressen, die von den Sicherheitsprüfungen ausgenommen werden sollen.

Wenn Sie diese Option auswählen, wird das Dialogfenster *Absender* geöffnet. Sie können entweder eine vollständige gültige E-Mail-Adresse eingeben (z. B. `esoundso@beispiel.de` oder alle E-Mail-Adressen einer bestimmten Domäne, indem Sie einen Asterisk als Platzhalter verwenden (z. B. `*@beispiel.de`).

Hinweis – Verwenden Sie die Option *Absender* mit Bedacht, da Absenderadressen leicht gefälscht werden können.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die Ausnahmeregel hinzu.

3. Klicken Sie *Speichern*.

Die neue Ausnahmeregel wird in der Liste *Ausnahmen* angezeigt.

Um eine Ausnahmeregel zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Erweitert

Auf der Registerkarte *POP3 >> Erweitert* können Sie solche Rechner und Netzwerke bestimmen, die vom Transparenzmodus des POP3-Proxy ausgenommen sein sollen. Des Weiteren beinhaltet die Registerkarte die POP3-Option zur Vorabholung (engl. *prefetch*), welche es ermöglicht, Nachrichten von einem POP3-Server im Vorhinein zu holen und sie in einer Datenbank zu speichern.

Transparenzmodus-Ausnahmen

Diese Option ist nur von Bedeutung, wenn der POP3-Proxy im Transparenzmodus arbeitet. Rechner und Netzwerke, die im Feld *Auszunehmende Rechner/Netze* aufgeführt sind, werden im Gegensatz zum restlichen POP3-Verkehr nicht transparent überwacht. Um jedoch POP3-Verkehr für diese Rechner und Netzwerke zuzulassen, wählen Sie die Option *POP3-Verkehr für aufgelistete Rechner/Netze zulassen*. Wenn Sie diese Option nicht wählen, müssen Sie spezielle Paketfilterregeln für die hier aufgeführten Rechner und Netzwerke anlegen.

POP3-Server und Vorabholung

Sie können hier einen oder mehrere POP3-Server eintragen, die dem Proxy bekannt sein sollen. Zusätzlich können Sie Vorabholung (engl. *prefetching*) aktivieren.

POP3-Server: Geben Sie die POP3-Server an, die in Ihrem Netzwerk bzw. von Ihren Benutzern verwendet werden.

Wenn kein POP3-Server angegeben wird und E-Mails vom Proxy abgefangen werden, ersetzt der Proxy die E-Mails sofort mit einer Benachrichtigung an den Empfänger, die ihn in davon Kenntnis setzt, dass die E-Mails unter Quarantäne gestellt wurden. E-Mails in Quarantäne können im *Mail-Manager* eingesehen

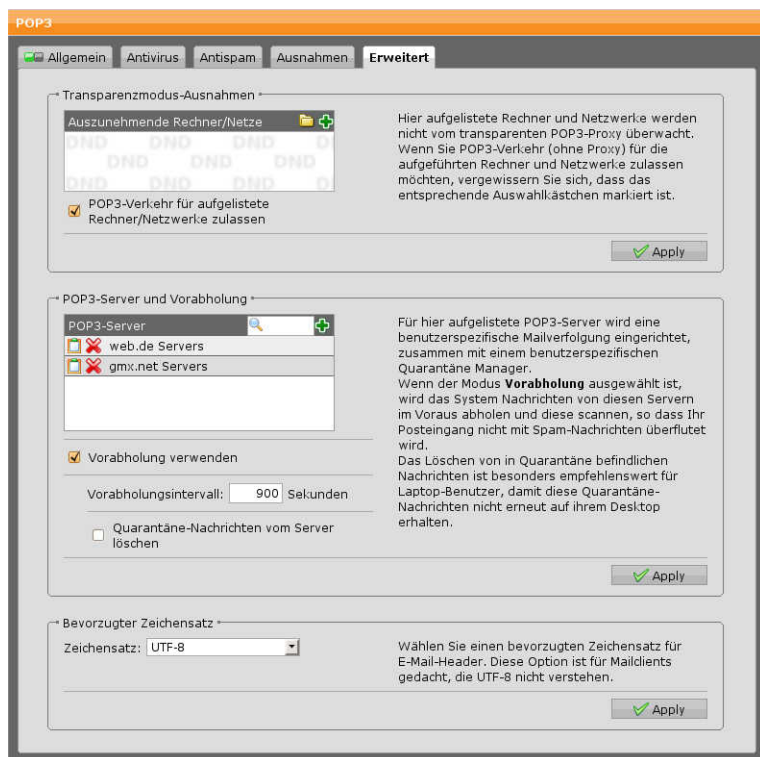


Figure 11.19 POP3-Proxy: Konfiguration der erweiterten Einstellungen

werden, aber da sie nicht mit einem Server oder einem Konto in Verbindung gebracht werden können, können sie bei einer späteren Verbindung nicht freigegeben werden. Die Freigabe von E-Mails ist überhaupt nur möglich für E-Mails die im Voraus abgeholt wurden („Vorabholung“).

Es gibt zwei Szenarien:

- Wenn ein oder mehrere POP3-Server angegeben sind und Vorabholung deaktiviert ist, behält der Proxy die Übersicht darüber, welche E-Mails in Quarantäne zu welchem Server oder Konto gehört. Dadurch können E-Mails in Quarantäne freigegeben werden, wenn der Client die Mailbox das nächste Mal abfragt. Damit das funktioniert, muss der Proxy sicher feststellen,

welche IP-Adresse zu welchem Server gehört (über deren FQDN, die Sie in Ihrem Mail-Client angegeben haben).

- Wenn ein oder mehrere POP3-Server angegeben sind und Vorabholung aktiviert ist, überprüft der POP3-Proxy die POP3-Server periodisch auf neue Nachrichten. Wenn eine neue Nachricht angekommen ist, wird sie zum POP3-Proxy kopiert, gescannt und in einer Datenbank auf dem Sicherheitssystem gespeichert. Die Nachrichten bleiben auf dem POP3-Server. Wenn ein Client versucht, neue Nachrichten abzuholen, kommuniziert er stattdessen mit dem POP3-Proxy und holt nur die Nachrichten aus der Datenbank.

Ein POP3-Proxy, der *Vorabholung* unterstützt, hat unter Anderem folgende Vorteile:

- Keine Zeitablauf-Probleme zwischen Client und Proxy oder umgekehrt.
- Die Zustellung der Nachrichten erfolgt sehr viel schneller, da die E-Mails bereits vorab gescannt wurden.
- Blockierte Nachrichten können vom Benutzerportal aus freigegeben werden – sie werden beim nächsten Abrufen der E-Mails mit abgeholt.

Wenn eine Nachricht blockiert wurde, weil sie bösartigen Inhalt enthält oder als Spam eingestuft wurde, wird sie nicht an den Client ausgeliefert. Stattdessen wird sie unter Quarantäne gestellt. Ein Nachricht, die unter Quarantäne gestellt ist, wird im Bereich *Mail-Manager* im Benutzerportal gespeichert, von wo sie gelöscht oder freigegeben werden kann.

Vorabholung verwenden: Um den Vorabholungsmodus zu aktivieren, markieren Sie das Auswahlkästchen und fügen Sie einen oder mehrere POP3-Server zum Feld *POP3-Server* hinzu.

Vorabholungsintervall: Wählen Sie das Zeitintervall, in dem der POP3-Proxy den POP3-Server kontaktiert, um Nachrichten vorab zu holen.

Hinweis – Das Intervall, in dem Mail-Clients den POP3-Server kontaktieren dürfen, variiert von Server zu Server. Das Vorabholungsintervall sollte deshalb nicht kürzer eingestellt werden als der POP3-Server es zulässt, sonst schlägt das Herunterladen der POP3-Nachrichten fehl, da der Zugang zum POP3-Server nicht gestattet ist.

Beachten Sie auch, dass mehrere Clients das gleiche POP3-Konto abfragen können. Jedes Mal, wenn Nachrichten erfolgreich vom POP3-Server abgerufen wurden, wird von vorne begonnen, die Zeit zu zählen, bis eine erneute Abfrage möglich ist. Wenn aus diesem Grund der POP3-Proxy

den POP3-Server viermal hintereinander nicht erreichen kann (Standardeinstellung ist alle 15 Minuten), wird das Kontokennwort aus der Proxy-Mail-Datenbank gelöscht, und es werden dann solange keine E-Mails mehr abgeholt, bis ein Mail-Client das Kennwort an den POP3-Server schickt und sich wieder erfolgreich anmeldet.

Quarantäne-Nachrichten vom Server löschen: Wenn Sie diese Option wählen, werden Nachrichten in Quarantäne sofort vom POP3-Server gelöscht. Das ist nützlich, um zu verhindern, dass Benutzer Spam- oder virusinfizierte Nachrichten erhalten, wenn Sie sich mit dem POP3-Server nicht über die ASG, sondern beispielsweise über das Webportal des POP3-Servers.

Wenn der E-Mail-Client so konfiguriert ist, dass er Nachrichten vom Server löscht, nachdem er sie abgeholt hat, wird diese Information auch in der Datenbank abgespeichert. Das nächste Mal, wenn der Proxy Nachrichten für dieses POP3-Konto vorab holt, wird er die Nachrichten vom Server löschen. Das bedeutet, so lange kein Client Nachrichten von Astaro Security Gateway abholt *und* kein Löschbefehl konfiguriert ist, werden keine Nachrichten auf dem POP3-Server gelöscht. Dadurch können sie weiterhin gelesen werden, zum Beispiel über das Webportal des E-Mail-Anbieters.

Nachrichten in Quarantäne werden vom POP3-Server in den folgenden Fällen gelöscht:

- Die Nachrichten werden manuell gelöscht über den Mail-Manager.
- Die Nachrichten werden manuell gelöscht über das Benutzerportal.
- Die Nachricht wurde freigegeben (entweder über den Quarantänebericht oder das Benutzerportal) und der E-Mail-Client des Benutzers ist so konfiguriert, dass er Nachrichten nach der Zustellung löscht.
- Die Benachrichtigungs-E-Mail wurde gelöscht.
- Die Aufbewahrungsfrist ist abgelaufen (siehe Abschnitt *Konfiguration* im Kapitel *Mail-Manager*).

Im Vorabholungsmodus können Nachrichten unter Quarantäne nicht direkt durch einen Client-Befehl vom POP3-Server gelöscht werden.

Hinweis – Der E-Mail-Client muss sich mindestens einmal erfolgreich mit dem POP3-Server verbunden haben, bevor Vorabholung funktioniert. Das liegt daran, dass Astaro Security Gateway den Namen des POP3-Servers, den Benutzernamen und das Benutzerkennwort in einer Datenbank speichern muss, um POP3-Nachrichten anstelle des Benutzers abholen zu können. Das kann jedoch *nicht* erreicht werden, wenn das POP3-Konto im Astaro Benutzerportal (weitere Informationen finden Sie unter Benutzerportal) eingerichtet wird. Die POP3-Kontodaten im Benutzerportal werden benötigt, damit die vorab geholten Nachrichten auf der Benutzerportalseite des entsprechenden Benutzers erscheinen und in dessen täglichem Quarantänebericht.

SSL wird im Augenblick nicht unterstützt, deshalb können Mails von Mail-Anbietern wie Googlemail, die ausschließlich SSL-Zugriff gestatten, nicht durch den Proxy gefiltert werden.

Hinweis für Benutzer von Fetchmail: Die TOP-Methode wird aus Sicherheitsgründen nicht unterstützt, um E-Mails vom Mailserver herunterzuladen – Nachrichten, die über TOP empfangen wurden, können nicht gescannt werden. Es funktioniert aber, wenn Sie die Option `fetchall` angeben (–a auf der Kommandozeile). Um weitere Informationen zu erhalten, lesen Sie bitte das Kapitel „RETR or TOP“ im Fetchmail-Handbuch.

Bevorzugter Zeichensatz

In diesem Abschnitt können Sie einen anderen Zeichensatz als UTF-8 auswählen, der dann für Mail-Header verwendet wird. Das ist nützlich, wenn Ihre Benutzer Mail-Clients verwenden, die mit UTF-8 nicht umgehen können.

Verschlüsselung

Seitdem E-Mails im privaten und geschäftlichen Bereich das primäre elektronische Kommunikationsmittel geworden sind, sind verständliche Bedenken über Privatsphäre und Authentifizierung aufgekommen. Allgemein gesagt, das E-Mail-Format wird in Klartext übermittelt, ähnlich einer Postkarte, die jeder lesen kann. Da es darüberhinaus sehr einfach ist, falsche Identitäten anzunehmen, muss der Empfänger feststellen können, ob der Absender auch der ist, für den er sich ausgibt.

Die Lösung zur Beseitigung dieser Bedenken besteht typischerweise aus E-Mail-Verschlüsselung und digitale Zertifizierung – E-Mails werden dabei elektronisch signiert und kryptografisch verschlüsselt. Dies stellt sicher, dass ausschließlich

der Empfänger der Nachricht diese öffnen und den Inhalt der Nachricht anschauen kann (Privatsphäre) und die Identität des Absenders feststellen kann (Authentifizierung). Mit anderen Worten negiert dieser Prozess die Idee, eine „E-Postkarte“ zu erhalten

In der modernen Kryptografie gibt es zwei Verfahren für die Verschlüsselung von E-Mails: Symmetrisch und asymmetrisch. Beide Verfahren haben sich als Standard etabliert und werden in verschiedenen Anwendungen eingesetzt. Bei der symmetrischen Verschlüsselung teilen sich der Absender und der Empfänger den gleichen Schlüssel.

Bei der asymmetrischen Verschlüsselung (auch bekannt als *Public-Key-Kryptografie*) besitzt jeder Benutzer ein Schlüsselpaar – einen öffentlichen Schlüssel (engl. *public key*) für die Verschlüsselung der E-Mail und einen korrespondierenden privaten bzw. geheimen Schlüssel (engl. *private key*) zur Entschlüsselung. Der öffentliche Schlüssel wird frei verteilt, während der private Schlüssel vom Benutzer geheim gehalten wird.

Für die symmetrische Verschlüsselung müssen die beiden Beteiligten sicherstellen, dass für eine sichere Kommunikation die Schlüssel geheim bleiben und nicht für Dritte zugänglich sind. Das größte Problem ist dabei die Übermittlung der Schlüssel, wenn sich die beiden Parteien an unterschiedlichen Standorten befinden: Wie sende ich den Schlüssel an den Empfänger, ohne dass ihn jemand abfängt? Die Public-Key-Kryptografie wurde entwickelt, um genau diese Sicherheitslücke zu schließen. Mit dieser Verschlüsselungs-Methode können zwei Parteien über eine unsichere Verbindung miteinander kommunizieren, ohne dass zuvor ein gemeinsamer Schlüssel ausgetauscht werden muss.

Das Bedürfnis nach E-Mail-Verschlüsselung hat eine Reihe von Standards für die Public-Key-Kryptografie hervorgebracht, vor allem S/MIME und OpenPGP, die beide von Astaro Security Gateway unterstützt werden. S/MIME (*Secure Multipurpose Internet Mail Extensions*) ist ein Standard für asymmetrische Verschlüsselung und das Signieren von MIME-strukturierten E-Mails. Dieses Protokoll wird üblicherweise innerhalb einer Public-Key-Infrastruktur (PKI) eingesetzt und basiert auf einer hierarchischen Struktur aus digitalen Zertifikaten, wobei es eine vertrauenswürdige Instanz als Zertifizierungsstelle (CA, engl. *certificate authority*) benötigt. Die CA stellt ein Zertifikat aus, bei dem sie eine Identität an ein Paar elektronischer Schlüssel bindet. Dieser Vorgang kann als digitales Gegenstück zu herkömmlichen Identitätsdokumenten wie einem Reisepass angesehen werden. Aus technischer Sicht stellt die CA ein Zertifikat aus, bei dem sie einen öffentlichen Schlüssel an einen bestimmten *Distinguished Name* im X.500-Standard bindet, oder an einen *Alternative Name* wie z. B. eine E-Mail-Adresse.

Ein digitales Zertifikat ermöglicht es festzustellen, ob jemand die Berechtigung hat, einen angegebenen Schlüssel zu verwenden. Der Gedanke dahinter ist, dass man sicher sein kann, dass jemandem der fragliche öffentliche Schlüssel gehört, wenn dieser einer CA vertraut und nachweisen kann, dass der öffentliche Schlüssel von dieser CA signiert wurde.

OpenPGP (*Pretty Good Privacy*) nutzt eine asymmetrische Verschlüsselung, die üblicherweise in einem sogenannten *Web of Trust* (WOT, dt. Netz des Vertrauens) eingesetzt wird. Das bedeutet, dass öffentliche Schlüssel digital von anderen Benutzern signiert werden, welche durch diese Handlung die Zusammengehörigkeit von Schlüssel und Benutzer bestätigen.

Hinweis – Beachten Sie, dass, obwohl sie ähnliche Dienste anbieten, die beiden Standards S/MIME und OpenPGP sehr unterschiedliche Formate verwenden. Das bedeutet, dass Benutzer des einen Protokolls nicht mit Benutzern des anderen Protokolls kommunizieren können. Des Weiteren können Authentifizierungszertifikate nicht für beide Protokolle verwendet werden.

Die gesamte E-Mail-Verschlüsselung ist für den Benutzer transparent, so dass keine zusätzliche Verschlüsselungs-Software auf dem Client installiert werden muss. Zur Verschlüsselung der E-Mails wird das Zertifikat der Gegenstelle oder der öffentliche Schlüssel benötigt. Nachfolgend sind die unterschiedlichen Funktionsweisen für ein- und ausgehende Nachrichten beschrieben:

- Standardmäßig werden ausgehende Nachrichten von internen Benutzern auf gescannt, automatisch signiert und verschlüsselt. Für die Signatur und die Verschlüsselung wird entweder das Zertifikat (S/MIME) des Empfängers oder der öffentliche Schlüssel (OpenPGP) verwendet. Das Zertifikat und der öffentliche Schlüssel müssen dafür auf dem Sicherheitssystem vorhanden sein.
- Eingehende verschlüsselte Nachrichten von externen Benutzern, deren S/MIME-Zertifikat oder öffentlicher OpenPGP-Schlüssel dem Sicherheitssystem nicht bekannt sind, werden automatisch entschlüsselt und auf böartigen Inhalt gescannt. Um die Nachricht zu entschlüsseln, muss der S/MIME-Schlüssel oder der private OpenPGP-Schlüssel des internen Benutzers auf dem Sicherheitssystem installiert sein.
- Eingehende verschlüsselte Nachrichten von externen Benutzern oder für interne, dem System unbekannte Benutzer werden zugestellt, obwohl sie nicht entschlüsselt und deshalb nicht auf Viren oder Spam gescannt werden

können. Es liegt dann in der Verantwortung des Empfängers (interner Benutzer), sicherzustellen, dass die E-Mail keine Schadsoftware enthält, beispielsweise durch die Benutzung einer eigenen Firewall.

- Ausgehende Nachrichten, die bereits auf dem Client verschlüsselt wurden, werden direkt an den Empfänger weitergeleitet, wenn das entsprechende Zertifikat (S/MIME) oder der öffentliche Schlüssel (OpenPGP) nicht bekannt ist. Falls jedoch das S/MIME-Zertifikat oder der öffentliche OpenPGP-Schlüssel des Empfängers vorhanden ist, dann werden die Nachrichten ein zweites Mal verschlüsselt. Beachten Sie, dass im Voraus verschlüsselte Nachrichten nicht auf bösartigen Inhalt gescannt werden können.
- Entschlüsselung wird nur bei eingehenden E-Mails durchgeführt, wobei mit „eingehend“ gemeint ist, dass der Domänenname der Absenderadresse nicht Bestandteil eines SMTP-Profiles ist. Beispiel: Damit die Nachricht von der Adresse `esoundso@beispiel.de` entschlüsselt wird, darf die Domäne `beispiel.de` nicht auf der Registerkarte *Mail Security >> SMTP >> Routing* oder irgendeinem SMTP-Profil eingestellt sein.
- In die Betreffzeile jeder E-Mail wird eine Zusammenfassung des Signatur-/Verschlüsselungsergebnisses eingefügt. Beispiel: Einer E-Mail, die mit S/MIME korrekt signiert und verschlüsselt wurde, wird die Information „(S/MIME: Signed and encrypted)“ in der Betreffzeile angefügt.

Hinweis – Das Hinzufügen einer Fußzeile zu Nachrichten, die bereits signiert oder verschlüsselt sind, durch ein E-Mail-Programm (z. B. Microsoft Outlook oder Mozilla Thunderbird), wird ihre Signatur kaputt und damit ungültig machen. Wenn Sie digitale Zertifikate auf Client-Seite erzeugen wollen, deaktivieren Sie die Optionen für Antivirenprüfungsfußzeile und Vertraulichkeitsfußzeile, die sich auf der Registerkarte *Mail Security >> SMTP >> Antivirus* bzw. *Mail Security >> SMTP >> Erweitert* befinden. Wenn Sie jedoch nicht auf Datenschutz und Authentifizierung in Ihrer E-Mail-Kommunikation verzichten möchten und dennoch allgemeine Fußzeilen verwenden wollen, dann sollten Sie in Betracht ziehen, die eingebaute Funktion von Astaro Security Gateway einzusetzen. E-Mail-Verschlüsselung, die auf dem Gateway durchgeführt wird, bedeutet, dass die Fußzeile zur Nachricht hinzugefügt wird, bevor die digitale Signatur erzeugt wird, wodurch die Signatur intakt bleibt.

Allgemein

Auf der Registerkarte *Mail Security >> Verschlüsselung >> Allgemein* können Sie die Grundeinstellungen für die E-Mail-Verschlüsselungsfunktionalität vornehmen.

Querverweis – Für eine umfassende Beschreibung, wie Sie E-Mail-Verschlüsselung verwenden können, lesen Sie bitte den E-Mail Encryption Guide, den Sie in der Astaro Knowledgebase²⁸ finden (navigieren Sie zu *ASG Version 7 >> Astaro Manuals and Guides*).

Bevor Sie E-Mail-Verschlüsselung verwenden können, müssen Sie zunächst eine Zertifizierungsstelle (CA, *Certificate Authority*) erstellen. Diese CA besteht aus einem CA-Zertifikat und einem CA-Schlüssel. Das CA-Zertifikat kann heruntergeladen und lokal gespeichert werden. Es kann außerdem als externe CA (S/MIME Authority) in anderen Geräten installiert werden, um eine transparente E-Mail-Verschlüsselung zwischen zwei Astaro Security Gateways zu realisieren.

Hinweis – Um Problemen beim Herunterladen von Dateien mit dem Internet Explorer 6 vorzubeugen, fügen Sie die URL der Firewall (z.B. <https://192.168.2.100>) und des Benutzerportals (z.B. <https://192.168.2.100>) den *Vertrauenswürdigen Sites* hinzu. Beim Internet Explorer 6 befinden sich diese Einstellungen im Menü *Extras >> Internetoptionen >> Sicherheit*. Beim Internet Explorer 7 aktivieren Sie zusätzlich im Fenster *Sicherheitseinstellungen* die Funktion *Automatische Eingabeaufforderung für Dateidownloads*.

Um E-Mail-Verschlüsselung zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie die E-Mail-Verschlüsselung auf der Registerkarte *Allgemein*.**

²⁸ <http://www.astaro.com/kb>

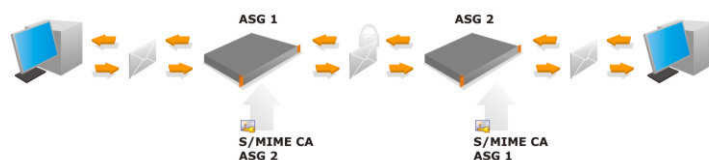


Figure 11.20 E-Mail-Verschlüsselung: E-Mail-Verschlüsselung mit zwei Astaro Security Gateways

Das Screenshot zeigt die Konfigurationsseite 'Verschlüsselung' im Astaro-Webinterface. Die Seite ist in mehrere Tabs unterteilt: 'Allgemein', 'Optionen', 'Interne Benutzer', 'S/MIME-Instanzen', 'S/MIME-Zertifikate' und 'OpenPGP-Schlüssel'. Der 'Allgemein'-Tab ist aktiv. Oben rechts befindet sich ein 'Abort enable' Button. Der Hauptbereich ist mit der Überschrift 'E-Mail-Verschlüsselungsstatus' und einem gelben Status-Symbol versehen. Darunter befindet sich ein Formular für die 'Zertifizierungsstelle (CA) für E-Mail-Verschlüsselung'. Das Formular enthält Felder für: Name d. Organisation (Beispiel AG), Stadt (Berlin), Land (Germany), Postmaster-E-Mail (admin@beispiel.de). Rechts neben dem Formular steht ein Textfeld mit der Anleitung: 'Zur Aktivierung von E-Mail-Verschlüsselung müssen Sie zunächst eine Zertifizierungsstelle (CA) erstellen. Geben Sie dazu die Informationen zu der Organisation in das Formular ein und klicken Sie auf **Speichern**.' Ein 'Speichern' Button befindet sich unten rechts im Formular.

Figure 11.21 E-Mail-Verschlüsselung: Konfiguration

Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche. Die Statusampel wird gelb und der Abschnitt *Zertifizierungsstelle (CA) für E-Mail-Verschlüsselung* kann nun bearbeitet werden.

2. Erstellen Sie eine Zertifizierungsstelle (CA).

Füllen Sie das Formular *Zertifizierungsstelle (CA) für E-Mail-Verschlüsselung* aus. Die Einstellungen aus der Registerkarte *Verwaltung* >> *Systemeinstellungen* >> *Organisatorisches* sind voreingestellt.

3. Klicken Sie **Speichern**.

Die Statusampel wird Grün und die folgenden Zertifikate bzw. Schlüssel werden generiert:

- S/MIME-CA-Zertifikat
- OpenPGP-Postmaster-Schlüssel

Beachten Sie, dass der Generierungsprozess einige Minuten dauern kann. Falls die Fingerabdrücke des *S/MIME-CA-Zertifikats* und des *OpenPGP-Postmaster-Schlüssels* nach einigen Minuten nicht angezeigt werden, klicken

Sie auf die *Aktualisieren*-Schaltfläche in der rechten oberen Ecke des WebAdmin. Das Zertifikat und der Schlüssel können heruntergeladen und lokal gespeichert werden.

Verwenden Sie die Schaltfläche *E-Mail-Verschlüsselungssystem jetzt zurücksetzen*, um alle Einstellungen im Menü *Verschlüsselung* in den Auslieferungszustand zurückzusetzen.

Optionen

Auf der Registerkarte *Verschlüsselung > > Optionen* können Sie die Standardrichtlinie für die Public-Key-Verschlüsselung festlegen.

The screenshot shows the 'Verschlüsselung' (Encryption) settings page. The 'Optionen' (Options) tab is active. The 'Standardrichtlinie' (Standard Policy) section has four checked options: 'Ausgehende E-Mails signieren', 'Ausgehende E-Mails verschlüsseln', 'Eingehende E-Mails verifizieren', and 'Eingehende E-Mails entschlüsseln'. The 'Automatisches Auslesen der S/MIME-Zertifikate' (Automatic reading of S/MIME certificates) section has one checked option: 'Automatisches Auslesen der S/MIME-Zertifikate aktivieren'. The 'OpenPGP-Schlüsselservers' (OpenPGP key servers) section has a text input field containing 'pgpkeys.mit.edu'. Each section has an 'Apply' button.

Figure 11.22 E-Mail-Verschlüsselung: Optionen

Standardrichtlinie: Legen Sie die Standardrichtlinie bezüglich der Verschlüsselung fest. Diese Einstellungen können allerdings durch benutzerspezifische Einstellungen überschrieben werden.

Folgende Aktionen können gewählt werden:

- Ausgehende E-Mails signieren
- Ausgehende E-Mails verschlüsseln

- Eingehende E-Mails verifizieren
- Eingehende E-Mails entschlüsseln

Klicken Sie *Übernehmen*, um die Einstellungen zu speichern.

Hinweis – Damit die Verschlüsselung funktioniert, muss der Absender in der Internen Benutzerliste geführt sein. Ausgehende E-Mails für Empfänger, deren S/MIME-Zertifikat oder öffentlicher OpenPGP-Schlüssel auf der Firewall installiert ist, werden standardmäßig verschlüsselt. Wenn Sie Verschlüsselung für diese Empfänger deaktivieren wollen, löschen Sie deren S/MIME-Zertifikate oder öffentliche OpenPGP-Schlüssel. Wenn dem Sicherheitssystem Zertifikate oder öffentliche Schlüssel unbekannt sind, werden diese E-Mails unverschlüsselt versendet.

Automatische Extraktion von S/MIME-Zertifikaten

Wenn diese Option gewählt ist, werden die an eingehende E-Mails angehängten S/MIME-Zertifikate automatisch extrahiert. Voraussetzung hierfür ist, dass dieses Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle (CA) signiert wurde, das heißt, von einer CA, die auf dem Gerät vorhanden ist und deshalb unter *Mail Security* >> *Verschlüsselung* >> *S/MIME-Instanzen* angezeigt wird. Hinzu kommt, dass die automatische Extraktion nur ausgeführt wird, wenn die Zeit- und Datumsanzeige von Astaro Security Gateway innerhalb der Periode liegen muss, die das Zertifikat gültig ist. Erfolgreich extrahierte S/MIME-Zertifikate werden auf der Registerkarte *Mail Security* >> *Verschlüsselung* >> *S/MIME-Zertifikate* angezeigt. Beachten Sie, dass dieser Prozess ca. fünf bis zehn Minuten benötigt.

Klicken Sie *Übernehmen*, um Änderungen zu speichern.

OpenPGP-Schlüsselserver

OpenPGP-Schlüsselserver (engl. *keyserver*) beherbergen öffentliche PGP-Schlüssel. Sie können hier einen OpenPGP-Schlüsselserver angeben. Bei verschlüsselten eingehenden E-Mails oder bei ausgehenden E-Mails, die verschlüsselt werden sollen, wird die ASG versuchen, den öffentlichen Schlüssel vom angegebenen Server zu holen, wenn der entsprechende Schlüssel der ASG noch unbekannt ist.

Interne Benutzer

Für die Signierung und Verschlüsselung von E-Mails muss entweder der S/MIME-Schlüssel oder der private OpenPGP-Schlüssel auf dem Sicherheits-

system vorhanden sein. Auf der Registerkarte *Verschlüsselung* >> *Interne Benutzer* können Sie für die Benutzer, für die E-Mail-Verschlüsselung aktiviert werden soll, sowohl ein individuelles S/MIME-Schlüssel/Zertifikat-Paar erstellen als auch ein OpenPGP-Schlüsselpaar.

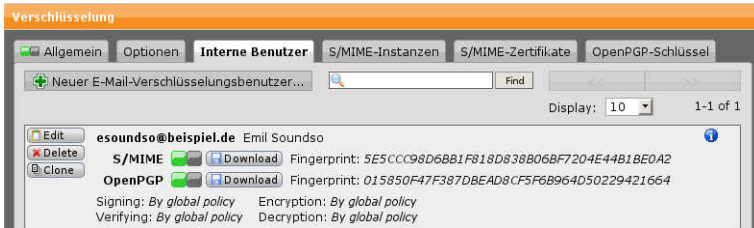


Figure 11.23 E-Mail-Verschlüsselung: Liste der internen Benutzer

Um einen internen E-Mail-Benutzer hinzuzufügen, gehen Sie folgendermaßen vor:

1. Klicken Sie auf der Registerkarte *Interne Benutzer* auf *Neuer E-Mail-Verschlüsselungsbenutzer*.

Das Dialogfenster *Neuen Benutzer erstellen* wird geöffnet.

2. Nehmen Sie die folgenden Einstellungen vor:

E-Mail-Adresse: Geben Sie die E-Mail-Adresse des Benutzers ein.

Vor- und Nachname: Geben Sie den Namen des Benutzers ein.

Signieren: Für die Signierung stehen die folgenden Optionen zur Auswahl:

- Standardrichtlinie verwenden: Die Standardrichtlinie, wie sie auf der Registerkarte *Allgemein* definiert ist, wird verwendet.
- Ein: E-Mails werden mit dem Zertifikat des Benutzers signiert.
- Aus: E-Mails werden nicht signiert.

Verschlüsselung: Für die Verschlüsselung stehen die folgenden Optionen zur Verfügung:

- Standardrichtlinie verwenden: Die Standardrichtlinie, wie sie auf der Registerkarte *Allgemein* definiert ist, wird verwendet.
- Ein: E-Mails werden mit dem öffentlichen Schlüssel des Empfängers verschlüsselt.
- Aus: E-Mails werden nicht verschlüsselt.

Verifizieren: Für die Verifizierung stehen die folgenden Optionen zur Verfügung:

- Standardrichtlinie verwenden: Die Standardrichtlinie, wie sie auf der Registerkarte *Allgemein* definiert ist, wird verwendet.
- Ein: E-Mails mit dem öffentlichen Schlüssel des Absenders verifiziert.
- Aus: E-Mails werden nicht verifiziert.

Entschlüsselung: Für die Entschlüsselung stehen die folgenden Optionen zur Auswahl:

- Standardrichtlinie verwenden: Die Standardrichtlinie, wie sie auf der Registerkarte *Allgemein* definiert ist, wird verwendet.
- Ein: E-Mails werden mit dem Zertifikat des Benutzers entschlüsselt.
- Aus: E-Mails werden nicht entschlüsselt.

S/MIME: Sie können wählen, ob das S/MIME-Zertifikat und der Schlüssel automatisch vom System generiert werden sollen oder ob Sie ein Zertifikat im Format PKCS#12 hochladen wollen. Wenn Sie das Zertifikat hochladen, müssen Sie das Kennwort kennen, mit dem die PKCS#12-Datei geschützt ist. Beachten Sie, dass die PKCS#12-Datei sowohl den S/MIME-Schlüssel als auch das Zertifikat enthalten muss. Ein eventuell zusätzlich enthaltenes CA-Zertifikat wird ignoriert.

OpenPGP: Sie können wählen, ob das OpenPGP-Schlüsselpaar, das aus einem privaten und einem öffentlichen Schlüssel besteht, vom System automatisch generiert werden sollen oder ob Sie das Schlüsselpaar im ASCII-Format hochladen wollen. Beachten Sie, dass der private und der öffentliche Schlüssel in einer einzigen Datei enthalten sein müssen und dass die Datei kein Kennwort enthalten darf.

Hinweis – Falls Sie für einen Benutzer S/MIME und OpenPGP konfigurieren, dann werden die von ihm gesendeten E-Mails mittels S/MIME signiert und verschlüsselt.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über den internen Benutzer hinzu.

3. Klicken Sie *Speichern*.

Das neue Benutzerkonto wird in der Liste *Interne Benutzer* angezeigt.

Verwenden Sie die Statusampel, um die Benutzung von einem oder beiden Schlüsseln abzuschalten ohne die Schlüssel löschen zu müssen.

Hinweis – Aus Sicherheitsgründen kann nur das S/MIME-Zertifikat und der öffentliche Schlüssel aus dem OpenPGP-Schlüsselpaar heruntergeladen werden. Der S/MIME-Schlüssel und der private OpenPGP-Schlüssel können nicht vom System heruntergeladen werden. Um Problemen beim Herunterladen von Dateien mit dem Internet Explorer 6 vorzubeugen, fügen Sie die URL der Firewall (z. B. <https://192.168.2.100>) und des Benutzerportals (z. B. <https://192.168.2.100>) den *Vertrauenswürdigen Sites* hinzu. Beim Internet Explorer 6 befinden sich diese Einstellungen im Menü *Extras >> Internetoptionen >> Sicherheit*. Beim Internet Explorer 7 aktivieren Sie zusätzlich im Fenster *Sicherheitseinstellungen* die Funktion *Automatische Eingabeaufforderung für Dateidownloads*.

S/MIME-Instanzen

Auf der Registerkarte *Verschlüsselung >> S/MIME-Instanzen* können Sie die Zertifikate (z. B. den öffentlichen Schlüssel) einer externen Zertifizierungsstelle (CA) importieren, der Sie vertrauen. Auf diese Weise sind alle eingehenden E-Mails, deren Zertifikate von dieser CA signiert wurden, ebenfalls vertrauenswürdig. Wenn Sie die Funktion *Automatische Extraktion von S/MIME-Zertifikaten* auf der Registerkarte *Verschlüsselung >> Optionen* eingeschaltet ist, werden die Zertifikate dieser CA automatisch extrahiert und auf der Registerkarte *Verschlüsselung >> S/MIME-Zertifikate* angezeigt.

Um eine externe S/MIME-Instanz zu importieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *S/MIME-Instanzen* auf *Neue externe Zert.-Stelle (CA)*.**

Das Dialogfenster *Externe Zert.-Stelle hinzufügen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Format: Wählen Sie das Format der CA. Die folgenden Formate können ausgewählt werden:

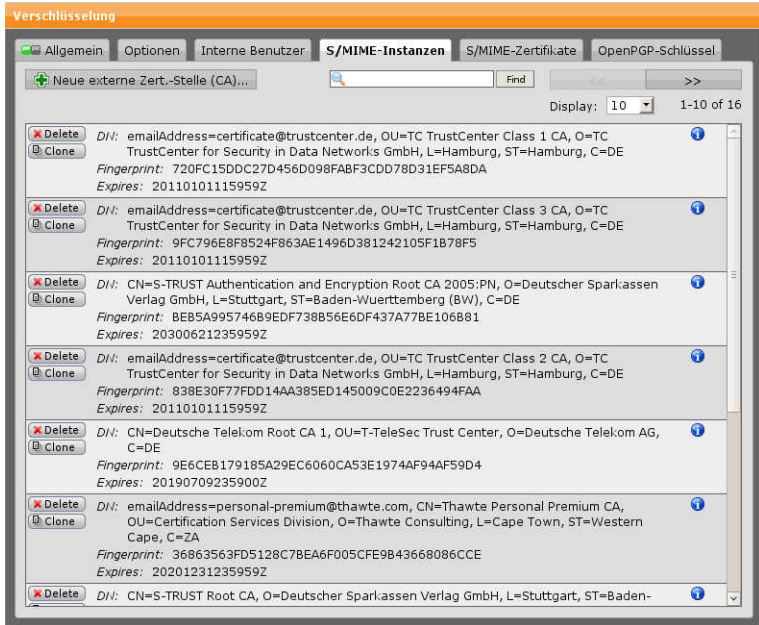


Figure 11.24 E-Mail-Verschlüsselung: Liste der S/MIME-Instanzen

- der (binary)
- pem (ASCII)

Hinweis – Microsoft-Windows-Betriebssysteme nutzen die Dateierweiterung *cer* für beide Formate, *der* und *pem*. Daher müssen Sie im Voraus wissen, ob es sich bei der Datei, die Sie hochladen wollen, um das binär- oder das ASCII-Format handelt. Wählen Sie dann aus der Auswahlliste das entsprechende Format aus.

Zertifikat: Klicken Sie auf das Ordnersymbol, um das Dialogfenster *Upload File* zu öffnen. Wählen Sie die Datei aus und klicken Sie *Save*.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die externe CA hinzu.

3. Klicken Sie *Speichern*.

Die neue CA wird in der Liste *S/MIME-Instanzen* angezeigt.

Astaro Security Gateway wird standardmäßig mit einigen kommerziellen Zertifizierungsstellen (CA) ausgeliefert, um die E-Mail-Verschlüsselung zwischen Ihrem Unternehmen und Ihren Kommunikationspartnern zu erleichtern, die eine Public-Key-Infrastruktur (PKI) unterhalten, welche auf einer oder mehreren dieser CAs basiert. Nachfolgend sind einige Links zu verbreiteten Zertifizierungsanbietern aufgeführt:

- Trustcenter²⁹
- S-TRUST³⁰
- Thawte³¹
- VeriSign³²
- GeoTrust³³

Zusätzlich können Sie die CA auf einem anderen Astaro Security Gateway installieren. Dadurch ermöglichen Sie eine transparente E-Mail-Verschlüsselung zwischen beiden Astaro Security Gateways.

S/MIME-Zertifikate

Auf der Registerkarte *Verschlüsselung* >> *S/MIME-Zertifikate* können Sie externe S/MIME-Zertifikate importieren. E-Mails an Empfänger, deren Zertifikate auf dieser Registerkarte aufgeführt sind, werden automatisch verschlüsselt. Wenn für einen bestimmten Empfänger die E-Mails nicht verschlüsselt werden sollen, löschen Sie einfach das entsprechende Zertifikat aus der Tabelle.

Hinweis – Wenn Sie ein S/MIME-Zertifikat manuell hochladen, wird Nachrichten von E-Mail-Adressen, die mit diesem Zertifikat verknüpft sind, immer vertraut. Selbst wenn kein CA-Zertifikat verfügbar ist, mit dem die Identität der Person auf dem Zertifikat überprüft werden könnte. Das bedeutet also, dass manuell hochgeladene S/MIME-Zertifikate immer als vertrauenswürdig gelten.

²⁹ http://www.trustcenter.de/root_certificates.htm

³⁰ <http://www.s-trust.de/download/ausstellerzertifikate/index.htm>

³¹ <http://www.thawte.com/roots/>

³² <http://www.verisign.com/support/roots.html>

³³ http://www.geotrust.com/resources/root_certificates/index.asp

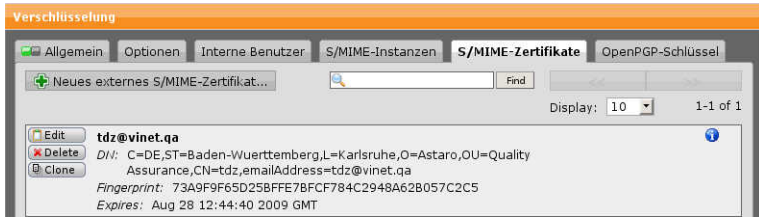


Figure 11.25 E-Mail-Verschlüsselung: Liste der S/MIME-Zertifikate

Ein externes S/MIME-Zertifikat importieren:

1. **Klicken Sie auf der Registerkarte *S/MIME-Zertifikate* auf *Neues externes S/MIME-Zertifikat*.**

Das Dialogfenster *S/MIME-Zertifikat hinzufügen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Format: Wählen Sie das Format des Zertifikats. Die folgenden Formate können ausgewählt werden:

- pem (ASCII)
- der (binary)

Hinweis – Microsoft-Windows-Betriebssysteme nutzen die Dateierweiterung *cer* für beide Formate, *der* und *pem*. Daher müssen Sie im Voraus wissen, ob es sich bei der Datei, die Sie hochladen wollen, um das binär- oder das ASCII-Format handelt. Wählen Sie dann aus der Auswahlliste das entsprechende Format aus.

Zertifikat: Klicken Sie auf das Ordnersymbol, um das Dialogfenster *Upload File* zu öffnen. Wählen Sie die Datei aus und klicken Sie *Save*.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über das Zertifikat hinzu.

3. **Klicken Sie *Speichern*.**

Das neue S/MIME-Zertifikat wird in der Liste *S/MIME-Zertifikate* angezeigt.

OpenPGP-Schlüssel

Auf der Registerkarte *Verschlüsselung >> OpenPGP-Schlüssel* können Sie öffentliche Schlüssel aus OpenPGP-Schlüsselpaaren importieren. Die Dateien

müssen im .asc-Format vorliegen. Sie können auch ganze Schlüsselbunddateien (engl. *keyrings*) hochladen.

Hinweis – Importieren Sie keine Schlüsselbunddateien, die durch ein Kennwort geschützt sind.

Alle öffentlichen Schlüssel aus der Schlüsselbunddatei werden importiert und können dazu verwendet werden, Nachrichten zu verschlüsseln. E-Mails an Empfänger, deren öffentliche Schlüssel auf dieser Registerkarte aufgeführt sind, werden automatisch verschlüsselt. Wenn für einen bestimmten Empfänger die E-Mails nicht verschlüsselt werden sollen, löschen Sie einfach den entsprechenden öffentlichen Schlüssel aus der Liste.

Hinweis – Pro Schlüssel wird nur eine E-Mail-Adresse unterstützt. Falls einem Schlüssel mehrere E-Mail-Adressen zugeordnet sind, wird nur die „erste“ E-Mail-Adresse verwendet (die Reihenfolge hängt von der Sortierung durch OpenPGP ab). Wenn Sie einen Schlüssel importieren möchten, der mehrere E-Mail-Adressen besitzt, so müssen Sie vorher die unerwünschten Adressen mit OpenPGP oder einem anderen Programm entfernen, bevor Sie den Schlüssel in Astaro Security Gateway importieren.



Figure 11.26 E-Mail-Verschlüsselung: Liste der öffentlichen OpenPGP-Schlüssel

Um einen öffentlichen OpenPGP-Schlüssel zu importieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *OpenPGP-Schlüssel* auf *Schlüsselbunddatei importieren*.**
Das Dialogfenster *OpenPGP-Schlüsselbunddatei importieren* wird geöffnet.
2. **Laden Sie die OpenPGP-Schlüssel hoch.**
Klicken Sie auf das Ordnersymbol, um das Dialogfenster *Upload File* zu öffnen. Wählen Sie die Datei aus und klicken Sie *Save*.

Der Schlüssel, oder wenn die Datei mehrere Schlüssel enthält, die Liste von Schlüssel wird angezeigt.

3. Wählen Sie einen oder mehrere Schlüssel aus und klicken Sie **Gewählte Schlüssel importieren**.

Der oder die Schlüssel werden in der Liste *OpenPGP-Schlüssel* angezeigt.

Hinweis – Dem Schlüssel muss eine E-Mail-Adresse zugeordnet sein, ansonsten schlägt die Installation fehl.

Quarantänebericht

Astaro Security Gateway besitzt eine E-Mail-Quarantäne, in der alle Nachrichten enthalten sind (SMTP und POP3), die aus verschiedenen Gründen blockiert und unter Quarantäne gestellt wurden. Das schließt Nachrichten ein, die auf ihre Zustellung warten ebenso wie Nachrichten, die mit bösartiger Software infiziert sind, verdächtige Anhänge enthalten, als Spam identifiziert wurden oder einfach unerwünschte Ausdrücke enthalten.



Figure 11.27 Quarantänebericht: Täglicher Quarantänebericht von Astaro Security Gateway

Um das Risiko zu minimieren, dass Nachrichten irrtümlicherweise zurückgehalten werden (sogenannte *Fehlfindte* oder engl. *false positives*), versendet

Astaro Security Gateway täglich einen Quarantänebericht an jeden Benutzer, der die Benutzer über Nachrichten informiert, die sich in Quarantäne befinden. Benutzer mit mehreren E-Mail-Adressen erhalten einen individuellen Quarantänebericht für jede konfigurierte E-Mail-Adresse. Das gilt auch für zusätzliche POP3-Konten, die für einen Benutzer im Benutzerportal konfiguriert sind, vorausgesetzt der POP3-Proxy von Astaro Security Gateway arbeitet im Vorabholungsmodus. Im Vorabholungsmodus werden die E-Mails vom POP3-Server vorab abgerufen und in einer lokale Datenbank abgelegt. Im Quarantänebericht kann der Benutzer auf eine Spam-E-Mail klicken, um diese Nachricht aus der Quarantäne freigeben, oder er kann den Absender für zukünftige Nachrichten einer Whitelist hinzufügen.

Die folgende Liste enthält weitere Informationen zum Quarantänebericht:

- Die Quarantäneberichte werden nur an Benutzer geschickt, deren E-Mail-Adresse zu einer Domäne gehört, die in einem SMTP-Profil enthalten ist. Dies beinhaltet sowohl die Angaben im Feld *Domänen* in den globalen *SMTP >> Routing*-Einstellungen als auch die Angaben im Feld *Domänen* aller SMTP-Profile.
- Wenn die POP3-Option *Vorabholung* ausgeschaltet ist, werden Nachrichten in Quarantäne, die an dieses Konto geschickt wurden, nicht im Quarantänebericht aufgeführt. Stattdessen wird dem Benutzer die typische Astaro-Benachrichtigung über blockierte POP3-Nachrichten geschickt. Dadurch ist es dann nicht wie über den Quarantänebericht oder das Benutzerportal möglich, die E-Mails freizugeben. Diese E-Mails können dann nur vom Administrator über den Mail-Manager im zip-Format heruntergeladen werden.
- Nur Spam-E-Mails können aus der Quarantäne freigegeben werden. Nachrichten, die sich aus anderen Gründen in Quarantäne befinden, z. B. weil sie Viren oder verdächtige Dateianhänge enthalten, können nur vom Administrator über den Mail-Manager von Astaro Security Gateway freigegeben werden. Außerdem können Benutzer all ihre Nachrichten in Quarantäne über das Astaro Benutzerportal einsehen.
- Wenn eine Spam-E-Mail mehrere Empfänger hat, wie es oft bei Verteilerlisten (auch engl. *mailing list*) der Fall ist, und einer der Empfänger die E-Mail freigibt, wird die E-Mail nur für diesen Empfänger freigegeben, vorausgesetzt die E-Mail-Adresse der Verteilerliste ist auf dem System konfiguriert. Andernfalls wird die E-Mail an alle Empfänger gleichzeitig geschickt. Weitere Informationen finden Sie unter der Option *Interne Verteilerlisten*

definieren auf der Registerkarte *Mail Security >> Quarantänebericht >> Ausnahmen*.

- E-Mails, die an eine SMTP-E-Mail-Adresse geschickt wurden, für die kein Benutzer auf Astaro Security Gateway konfiguriert ist, können vom Administrator über den Quarantänebericht oder den Mail-Manager freigegeben (aber nicht auf die Whitelist gesetzt) werden. Da der Benutzer nicht konfiguriert ist, ist jedoch kein Zugriff über das Benutzerportal möglich.
- An Verteilerlisten geschickte Spam-Mails können grundsätzlich nicht einer Whitelist hinzugefügt werden.
- Einige E-Mail-Programme kodieren den Header einer E-Mail nicht korrekt, was zu einer etwas merkwürdigen Darstellung dieser E-Mails im Quarantänebericht führen kann.

Allgemein

Auf der Registerkarte *Quarantänebericht >> Allgemein* können Sie festlegen, zu welcher Zeit der tägliche Quarantänebericht versendet werden soll. Zusätzlich können Sie eine Nachricht schreiben, die den Quarantäneberichten angefügt wird.

The screenshot shows the 'Quarantänebericht' configuration window with the 'Allgemein' tab selected. The window has three tabs: 'Allgemein', 'Ausnahmen', and 'Erweitert'. The 'Status des Quarantäneberichts' section has a green indicator and a 'Disable' button. Below this, the 'Zeitpunkt für den Berichtversand' section shows a time selection of 09:00. There is a checked option 'Zusatzbericht senden' with a time selection of 16:00. To the right of these settings is explanatory text: 'Zeitpunkt des Versands des Quarantäneberichts. Sie können eine weitere Zeit angeben, um zwei Berichte pro Tag zu erhalten. Bitte beachten Sie, dass Berichte für POP3 bei Bedarf erstellt werden, aber Berichte für SMTP immer erstellt werden, wenn Inhalt für den Bericht vorliegt.' Below this is an 'Apply' button. The 'Anpassbarer Nachrichtentext' section contains a text area with a sample message: 'This report lists all quarantined emails since last report. These are blocked because of spam, virus, bad file extensions, forbidden expressions or delivery errors. For questions please contact your mail administrator.' To the right of the text area is explanatory text: 'Sie können auf Wunsch einen Text eingeben, der mit jedem Bericht gesendet wird. Der Text könnte zum Beispiel die Kontaktangaben des Systemadministrators beinhalten.' Below this is another 'Apply' button.

Figure 11.28 Quarantänebericht: Allgemeine Einstellungen

Um die Einstellungen für den Quarantänebericht zu bearbeiten, aktivieren Sie den Quarantänebericht: Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche.

Die Statusampel wird grün.

Zeitpunkt für den Berichtversand

Hier können Sie festlegen, wann der/die tägliche(n) Quarantäneberichte versendet werden soll. Wählen Sie die Zeit mit Hilfe der Auswahlliste aus und klicken Sie *Übernehmen*.

Sie können auch einen zusätzlichen Bericht versenden. Wählen Sie dazu die Option *Zusatzbericht senden*, stellen Sie die Zeit ein und klicken Sie *Übernehmen*.

Anpassbarer Nachrichtentext

Hier können Sie den Text anpassen, der als Einleitung zum Quarantänebericht dient. Ändern Sie den Nachrichtentext nach Ihren Wünschen und klicken Sie *Übernehmen*.

Hinweis – Es ist nicht möglich, HTML-Tags im Feld für den Nachrichtentext zu verwenden.

Ausnahmen

Auf der Registerkarte *Mail Security >> Quarantänebericht >> Ausnahmen* können Ausnahme-Listen für interne E-Mail-Adressen definiert werden, um sie von den Quarantänebericht auszunehmen.

Quarantäneberichte werden ausgenommen

Hier können Sie die interne E-Mail-Adressen definieren, für die keine Quarantäneberichte versendet werden sollen. Benutzer, deren E-Mail-Adressen hier aufgeführt sind, erhalten keine täglichen Quarantäneberichte. Sie können eine vollständige E-Mail-Adresse eingeben oder einen Asterisk (*) als Platzhalter verwenden, z. B. **@beispiel.de*.

Hinweis – Die Ausnahmeliste gilt nur für den SMTP-Quarantänebericht. Wenn für einen Benutzer ein POP3-Konto angegeben ist, wird der POP3-Quarantänebericht trotzdem versendet.

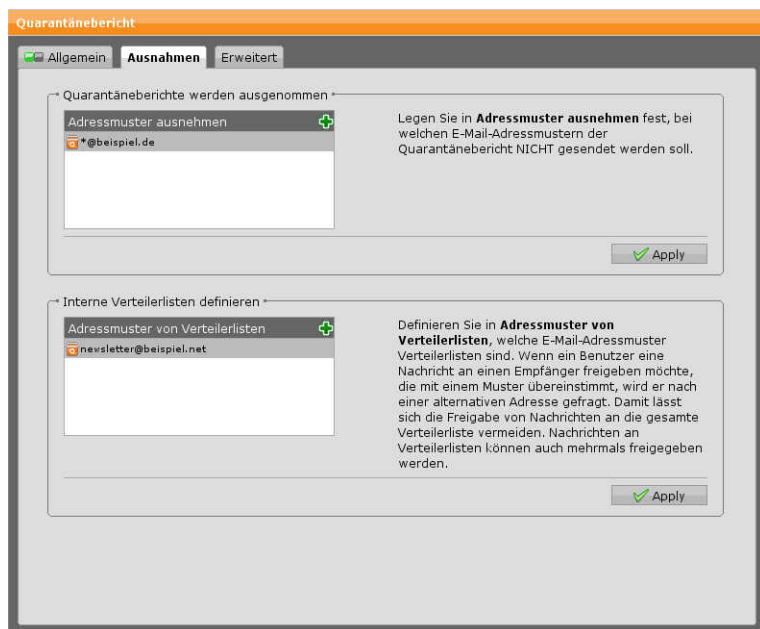


Figure 11.29 Quarantänebericht: Ausnahmen

Interne Verteilerlisten definieren

Wenn die E-Mail-Adresse einer Verteilerliste im Feld *Adressmuster von Verteilerlisten* konfiguriert ist (z. B. *newsletter@beispiel.de*) und eine Spam-E-Mail, die an diese Verteilerliste gesendet wurde, entdeckt und unter Quarantäne gestellt wurde, dann wird der Quarantänebericht aller Empfänger dieser Verteilerliste einen Link zu dieser Spam-E-Mail enthalten. Dadurch kann jeder Empfänger die Spam-E-Mail für sich freigeben, indem er seine E-Mail-Adresse in das Dialogfenster eingibt, das erscheint, wenn er auf den *Freigeben*-Link im Quarantänebericht geklickt hat.

Hinweis – Verteilerlisten können nicht über den Quarantänebericht oder das Benutzerportal auf die Whitelist gesetzt werden.

Alternativ könnten Sie die E-Mail-Adresse dieser Verteilerliste einem lokalen Benutzer als zusätzliche E-Mail-Adresse in dessen Profil eintragen. Dadurch würde dieser Benutzer zu einer Art Mail-Verwalter werden. Nur der Quarantänebericht dieses Benutzers besäße dann einen Link zu der Spam-E-Mail, die

an die Verteilerliste geschickt wurde. Ein Klick auf den *Freigeben*-Link würde dann die Spam-E-Mail an alle Empfänger der Verteilerliste auf einmal versenden.

Hinweis – Wenn die E-Mail-Adresse einer Verteilerliste als zusätzliche E-Mail-Adresse bei einem Benutzerprofil eingetragen ist, wird den übrigen Empfängern dieser Verteilerliste kein *Freigeben*-Link bei Spam-E-Mails angezeigt, die an diese Liste gesendet wurden.

Wenn die E-Mail-Adresse der Mailing-Liste allerdings in einem Benutzerkonto als zusätzliche Adresse und gleichzeitig auch bei im Feld *Adressmuster von Verteilerlisten* eingetragen ist, dann wird im Quarantänebericht mit der Aktion *Freigeben* eine Eingabeaufforderung geöffnet. Der Benutzer kann dann bestimmen, an wen die Spam-Mail zugestellt wird, indem er die entsprechende(n) E-Mail-Adresse(n) manuell in die Eingabeaufforderung einträgt.

Letztlich, wenn die E-Mail-Adresse der Verteilerliste weder in einem Benutzerkonto als zusätzliche Adresse noch im Feld *Adressmuster von Verteilerlisten* eingetragen ist, dann wird eine an diese Verteilerliste gesendete Spam-E-Mail wie eine normale E-Mail behandelt, d. h. wenn einer der Empfänger der Verteilerliste die Spam-E-Mail aus der Quarantäne freigibt, wird diese gleichzeitig auch an alle anderen Empfänger der Verteilerlisten geschickt.

Zusammenfassend gesagt, wann immer die E-Mail-Adresse einer Verteilerliste als Verteilerlisten-Adressmuster konfiguriert ist, erhält jeder Benutzer, der einen Freigabe-Link für die Spam-E-Mail in seinem Quarantänebericht hat, eine Eingabeaufforderung, wo er eine E-Mail-Adresse eintragen muss, an die die Spam-E-Mail gesendet werden soll.

Erweitert

Auf der Registerkarte *Quarantänebericht* >> *Erweitert* können Sie einen alternativen Rechnernamen und Portnummer für die *Freigeben*-Links im Quarantänebericht definieren. Zusätzlich können Sie die Freigabeoptionen für Spam-E-Mails ändern.

Erweiterte Optionen des Quarantäneberichts

Rechnername: Standardmäßig ist das der Rechnername der Firewall, wie er im Bereich *Erweiterte Einstellungen* unter *Mail Security* >> *SMTP* >> *Erweitert* angegeben ist. Es ist jedoch möglich, einen alternativen Rechnername für das Portal anzugeben. Standardmäßig zeigt dieser auf den Rechnernamen der Firewall. Wenn Sie jedoch ermöglichen wollen, dass Benutzer ihre E-Mails über

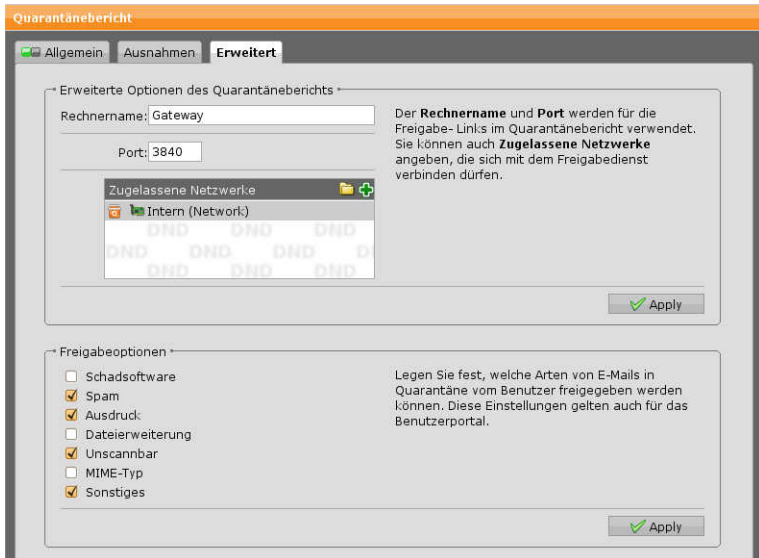


Figure 11.30 Quarantänebericht: Erweiterte Optionen

das Internet freigeben können, kann es nützlich sein, einen alternativen Rechnernamen anzugeben, der öffentlich aufgelöst werden kann.

Port: Standardmäßig ist der Port 3480 eingestellt. Sie können den Port auf einen beliebigen Wert zwischen 1024 und 65535 ändern.

Zugelassene Netzwerke: Sie können auch Netzwerke angeben, denen gestattet ist, sich mit dem Freigabedienst zu verbinden. Standardmäßig ist nur das interne Netzwerk ausgewählt.

Klicken Sie *Übernehmen*, um Ihre Einstellungen zu speichern.

Freigabeoptionen

Hier können Sie auswählen, welche Arten von Nachrichten in Quarantäne durch Benutzer freigegeben werden dürfen. Sie können zwischen den folgenden Optionen wählen:

- Schadsoftware
- Spam
- Ausdruck
- Dateierweiterung
- Unscannbar

- MIME-Typ
- Sonstiges

Mail-Manager

Der Mail-Manager ist ein administratives Werkzeug, mit dem alle E-Mails verwaltet und organisiert werden, die augenblicklich auf dem System gespeichert sind. Das umfasst sowohl Nachrichten, die auf ihre Zustellung warten als auch Nachrichten in Quarantäne, die mit bösartiger Software infiziert sind, verdächtige Anhänge enthalten, als Spam identifiziert wurden oder unerwünschte Ausdrücke enthalten. Sie können den Mail-Manager dazu verwenden, alle Nachrichten einzusehen, bevor Sie sie herunterladen, freigeben oder löschen. Der Mail-Manager unterstützt UTF-8.

Hinweis – Um Problemen beim Herunterladen von Dateien mit dem Internet Explorer 6 vorzubeugen, fügen Sie die URL der Firewall (z.B. <https://192.168.2.100>) und des Benutzerportals (z.B. <https://192.168.2.100>) den *Vertrauenswürdigen Sites* hinzu. Beim Internet Explorer 6 befinden sich diese Einstellungen im Menü *Extras >> Internetoptionen >> Sicherheit*. Beim Internet Explorer 7 aktivieren Sie zusätzlich im Fenster *Sicherheitseinstellungen* die Funktion *Automatische Eingabeaufforderung für Dateidownloads*.

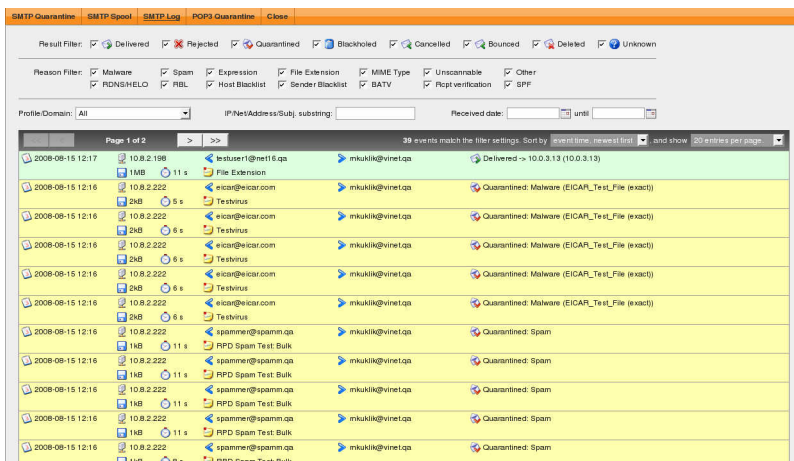


Figure 11.31 Mail-Manager: Mail-Manager von Astaro Security Gateway

Mail-Manager-Fenster

Um das Fenster mit dem Mail-Manager zu öffnen, klicken Sie auf die Schaltfläche *Mail-Manager in neuem Fenster öffnen* auf der Registerkarte *Mail Security* >> *Mail Manager* >> *Allgemein*.

Hinweis – Beachten Sie, dass der Mail Manager im Augenblick nur in englischer Sprache verfügbar ist.

Der Mail-Manager ist in fünf verschiedene Registerkarten unterteilt:

- **SMTP Quarantine:** Die SMTP-Quarantäne zeigt alle Nachrichten an, die momentan unter Quarantäne stehen.
- **SMTP Spool:** SMTP-Spool zeigt alle Nachrichten an, die sich momentan in /var/spool befinden. Die kann der Fall sein, wenn sie auf ihre Zustellung warten oder aufgrund eines Fehlers.
- **SMTP Log:** Das SMTP-Protokoll zeigt das Zustellungsprotokoll für alle Nachrichten, die über SMTP verarbeitet wurden.
- **POP3 Quarantine:** Die POP3-Quarantäne zeigt alle Nachrichten an, die über POP3 geholt wurden und momentan unter Quarantäne stehen.
- **Close:** Klicken Sie hier, um das Mail-Manager-Fenster zu schließen.

SMTP/POP3 Quarantine

Nachrichten in der SMTP- und POP3-Quarantäne können so angezeigt werden, dass der Grund für ihren Quarantäneaufenthalt deutlich wird. Folgende Gründe sind möglich:

- **Malware:** Schadsoftware
- **Spam:** unerbetene Werbemails
- **Expression:** unerwünschte Ausdrücke
- **File Extension:** unerwünschter/verdächtiger Dateianhang
- **MIME Type (SMTP only):** unerwünschter MIME-Typ (nur bei SMTP)

- **Unscannable:** Nachricht konnte nicht gescannt werden
- **Other:** Anderer Grund

Verwenden Sie die Auswahlkästchen, um die Quarantäneursache auszuwählen. Doppelklicken Sie das Auswahlkästchen einer Ursache, um ausschließlich diese Ursache auszuwählen.

Tipp – Doppelklicken Sie eine E-Mail, um sie anzuschauen.

Profile/Domain (SMTP), **Accounts** (POP3): Wählen Sie ein Profil, eine Domäne oder ein Konto, um nur Nachrichten anzuzeigen, die mit diesem/dieser verknüpft sind.

Sender/Rcpt/Subject Substring (Wortteil des Absenders/Empfängers/Betreffs): Hier können Sie einen Absender, Empfänger oder Betreff eingeben (oder einen Wortteil davon), nach dem in den Quarantäne-Nachrichten gesucht werden soll.

Received Date (Eingangsdatum): Um nur Nachrichten anzuzeigen, die während eines bestimmten Zeitraums eingegangen sind, geben Sie ein Datum ein oder wählen Sie ein Datum über das Kalendersymbol.

Sort By (Sortieren nach): Nachrichten können nach Datum, Betreff, Absenderadresse und Nachrichtengröße sortiert werden.

And Show (und anzeigen): Sie können wählen, ob 20, 50 oder 100 Einträge pro Seite angezeigt werden sollen oder alle Nachrichten auf einer Seite. Beachten Sie, dass das Anzeigen aller Nachrichten auf einer Seite viel Zeit in Anspruch nehmen kann.

Verwenden Sie das Auswahlkästchen vor jeder Nachricht oder klicken Sie auf eine Nachricht, um sie auszuwählen und dadurch Aktionen für die gewählten Nachrichten ausführen zu können. Die folgenden Aktionen sind verfügbar:

- **Download** (Herunterladen): Die gewählten Nachrichten werden heruntergeladen.
- **Delete** (Löschen): Die gewählten Nachrichten werden unwiderruflich gelöscht.
- **Release** (Freigeben): Die gewählten Nachrichten werden aus der Quarantäne freigegeben.
- **Release and Report as False Positive** (Freigeben und als Fehlfund melden): Die gewählten Nachrichten werden aus der Quarantäne freigegeben

und als Fehlfund (*false positive*) an das Spam-Scan-Programm gemeldet.

Beachten Sie, dass nur der Administrator *alle* Nachrichten aus der Quarantäne freigeben kann. Benutzer, die ihre Nachrichten im Astaro Benutzerportal einsehen, können nur Nachrichten freigeben, für die ihnen das explizit gestattet ist. Die Autorisierungseinstellungen dafür finden Sie auf der Registerkarte *Mail Security >> Quarantänebericht >> Erweitert*.

Select Global Cleanup Action (Globale Aufräumaktion wählen): Hier finden Sie einige Löschoptionen, die auf alle Nachrichten global angewendet werden, das heißt, unabhängig davon, ob sie ausgewählt sind und/oder angezeigt werden oder nicht.

Warnung – Gelöschte Nachrichten sind nicht wiederherstellbar.

- **Delete Mails Containing Malware:** Alle Mails löschen, die Schadsoftware enthalten.
- **Delete Mails that Are Spam:** Alle Mails löschen, die Spam sind.
- **Delete Mails with Blacklisted File Extensions:** Alle Mails löschen, die Dateierweiterungen enthalten, die auf der Blacklist stehen.
- **Delete Mails with Blacklisted Expressions:** Alle Mails löschen, die Ausdrücke enthalten, die auf der Blacklist stehen.
- **Delete Mails with Blacklisted MIME Types:** Alle Mails löschen, die einen MIME-Typ haben, der auf der Blacklist steht.
- **Delete Mails with Unscannable Content:** Alle Mails löschen, deren Inhalt nicht gescannt werden konnte.
- **Delete Everything Older than 3 Days:** Alle Mails löschen, die älter als drei Tage sind.
- **Delete Everything Older than One Week:** Alle Mails löschen, die älter als eine Woche sind.
- **Delete Everything Older than Two Weeks:** Alle Mails löschen, die älter als zwei Wochen sind.

- **Delete Everything Older than A Month:** Alle Mails löschen, die älter als einen Monat sind.
- **Delete Everything (Use with Caution):** Alle Mails löschen. Verwenden Sie diese Aktion mit Vorsicht.

SMTP Spool

Hier sehen Sie Nachrichten, die entweder darauf warten, zugestellt zu werden oder einen Fehler verursacht haben. Das Zustellungsprotokoll ist auch Teil des Headers einer Nachricht. Verwenden Sie die folgenden Auswahlkästchen, um nur eine Art von Nachrichten zur Ansicht auszuwählen:

- **Waiting** (Ausstehend): Nachrichten, deren Zustellung noch aussteht.
- **Error** (Fehler): Nachrichten, die einen Fehler verursacht haben. Wenn eine Nachricht mehr als einmal einen Fehler verursacht, melden Sie den Fall bitte Ihrem Astaro Partner oder dem Astaro Support-Team.

Tipp – Doppelklicken Sie eine Nachricht, um sie anzuschauen.

Profile/Domain (Profil/Domäne): Wählen Sie ein Profil oder eine Domäne aus, um nur dessen/deren Nachrichten zu sehen.

Sender/Rcpt/Subject Substring (Wortteil des Absenders/Empfängers/Betreffs): Hier können Sie einen Absender, Empfänger oder Betreff eingeben (oder einen Wortteil davon), nach dem in den Quarantäne-Nachrichten gesucht werden soll.

Received Date (Eingangsdatum): Um nur Nachrichten anzuzeigen, die während eines bestimmten Zeitraums eingegangen sind, geben Sie ein Datum ein oder wählen Sie ein Datum über das Kalendersymbol.

Sort By (Sortieren nach): Nachrichten können nach Datum, Betreff, Absenderadresse und Nachrichtengröße sortiert werden.

And Show (und anzeigen): Sie können wählen, ob 20, 50 oder 100 Einträge pro Seite angezeigt werden sollen oder alle Nachrichten auf einer Seite. Beachten Sie, dass das Anzeigen aller Nachrichten auf einer Seite viel Zeit in Anspruch nehmen kann.

Verwenden Sie das Auswahlkästchen vor jeder Nachricht oder klicken Sie auf eine Nachricht, um sie auszuwählen und dadurch Aktionen für die gewählten Nachrichten ausführen zu können. Die folgenden Aktionen sind verfügbar:

- **Download** (Herunterladen): Die gewählten Nachrichten werden heruntergeladen.
- **Retry** (Erneut versuchen): Es wird sofort erneut versucht, die gewählten Nachrichten zuzustellen.
- **Delete** (Löschen): Die gewählten Nachrichten werden unwiderruflich gelöscht.
- **Bounce** (Zurückwerfen): Die gewählten Nachrichten werden „zurückgeworfen“, das heißt, der Absender erhält eine Nachricht, dass die Zustellung seiner Nachricht abgebrochen wurde, weil sie unzustellbar war.

Select Global Cleanup Action (Globale Aufräumaktion wählen): Hier finden Sie einige Löschoptionen, die auf alle Nachrichten global angewendet werden, das heißt, unabhängig davon, ob sie ausgewählt sind und/oder angezeigt werden oder nicht.

Warnung – Gelöschte Nachrichten sind nicht wiederherstellbar.

SMTP Log

Das SMTP-Protokoll (*SMTP log*) zeigt die Protokollmeldungen für alle über SMTP verarbeiteten Nachrichten.

Result Filter (Ergebnisfilter): Wählen Sie aus, welche Arten von Nachrichten angezeigt werden, indem Sie die entsprechenden Auswahlkästchen markieren.

- **Delivered** (Zugestellt): Erfolgreich zugestellte Nachrichten.
- **Rejected** (Abgelehnt): Nachrichten, die von der ASG abgelehnt wurden.
- **Quarantined** (In Quarantäne): Nachrichten, die unter Quarantäne gestellt wurden.
- **Blackholed** (Verworfen): Nachrichten, die ohne Benachrichtigung gelöscht wurden.
- **Cancelled** (Abgebrochen): Nachrichten, deren Zustellung manuell unter *SMTP Spool* abgebrochen wurde.

- **Bounced** (Zurückgeworfen): Nachrichten, die nicht zugestellt werden konnten, aufgrund von z. B. falschen Routing-Einstellungen.
- **Deleted** (Gelöscht): Manuell gelöschte Nachrichten.
- **Unknown** (Unbekannt): Nachrichten, deren Status unbekannt ist. Verwenden Sie die Auswahlkästchen, um *Result-Filter*-Optionen an- oder abzuwählen. Doppelklicken Sie eine Option, um ausschließlich diese Option auszuwählen.

Reason Filter (Ursachenfilter): Verwenden Sie die Auswahlkästchen, um das Nachrichtenprotokoll weiter zu filtern.

Tipp – Doppelklicken Sie eine Protokollmeldung, um sie anzuschauen. Klicken Sie auf das Serversymbol einer Nachricht, um die IP-Adresse aufzulösen. Ein Asterisk (*) kennzeichnet einen erfolgreichen Reverse-DNS-Lookup.

Profile/Domain (Profil/Domäne): Wählen Sie ein Profil oder eine Domäne aus, um nur dessen/deren Nachrichten zu sehen.

IP/Net/Address/Subj. Substring (Wortteil der/des IP/Netzes/Adresse/Betreffs): Hier können Sie eine IP-Adresse, eine Netzwerkadresse oder einen Betreff eingeben, um im SMTP-Protokoll nach dieser/diesem zu suchen.

Received Date (Eingangsdatum): Um nur Nachrichten anzuzeigen, die während eines bestimmten Zeitraums verarbeitet wurden, geben Sie ein Datum ein oder wählen Sie ein Datum über das Kalendersymbol.

Sort By (Sortieren nach): Nachrichten können nach Ereignisdatum, Absenderadresse und Nachrichtengröße sortiert werden.

And Show (und anzeigen): Sie können wählen, ob 20, 50 oder 100 Einträge pro Seite angezeigt werden sollen oder alle Nachrichten auf einer Seite. Beachten Sie, dass das Anzeigen aller Nachrichten auf einer Seite viel Zeit in Anspruch nehmen kann.

Allgemein

Im oberen Bereich der Registerkarte *Mail-Manager* >> *Allgemein* können Sie den Mail-Manager öffnen, indem Sie auf die Schaltfläche *Mail-Manager in neuem Fenster öffnen*.

Im unteren Bereich bietet der Abschnitt *Statistischer Überblick* eine Übersicht über alle Nachrichten, die augenblicklich auf dem System gespeichert sind. Die Daten sind unterteilt in Nachrichten, die über SMTP zugestellt wurden,

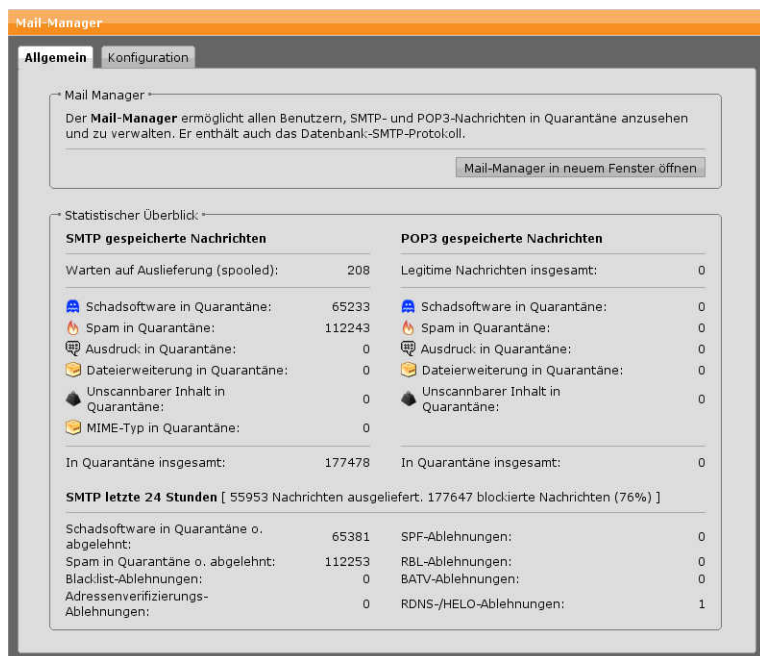


Figure 11.32 Mail-Manager: Übersicht

und solchen, die über POP3 zugestellt wurden. Für beide Arten werden die folgenden Informationen angezeigt:

- **Waiting for Delivery (Spooled)** (SMTP only): Hierbei handelt es sich um Mails, die sich in *Spool* befinden, z. B. weil sie gescannt wurden und bis jetzt noch nicht ausgeliefert werden konnten.
- **Waiting for Client Pickup** (POP3 only): Hierbei handelt es sich um Mails, die vom System vorab geholt wurden und bisher noch nicht von einem Client oder Benutzer abgerufen wurden.
- **Quarantined Malware:** Die Anzahl an Nachrichten, die Schadsoftware enthalten, wie z. B. Viren oder anderen schädlichen Inhalt.
- **Quarantined Spam:** Die Anzahl an Nachrichten, die als Spam identifiziert und deshalb unter Quarantäne gestellt wurden.
- **Quarantined Expression:** Die Anzahl an Nachrichten, die unter Quarantäne gestellt wurden, weil sie unerwünschte Ausdrücke enthalten.

- **Quarantined File Extension:** Die Anzahl an Nachrichten, die unter Quarantäne stehen, weil sie verdächtige Dateianhänge (die über ihre Dateierweiterung identifiziert wurden) enthalten.
- **Quarantined Unscannable:** Die Anzahl an Nachrichten, die unter Quarantäne stehen, weil sie nicht gescannt werden konnten.
- **Quarantined MIME Type (SMTP only):** Die Anzahl an Nachrichten, die unter Quarantäne stehen, weil sie einen MIME-Typ haben, der laut den SMTP-Einstellungen gefiltert werden soll.
- **Quarantined Total:** Die Gesamtzahl an Nachrichten, die unter Quarantäne stehen.

Hinweis – Die Zahlen für *Waiting for Delivery* geben einen Echtzeit-Ausschnitt der SMTP-Nachrichten wieder. Für POP3-Nachrichten hingegen stellen die Zahlen die Anhäufung der Daten seit der letzten Vorabholung dar.

Unten sehen Sie eine kurze Statistik über die SMTP-Quarantäne und die Ablehnungen der letzten 24 Stunden:

- **Malware Quarantined/Rejected:** Nachrichten, die unter Quarantäne gestellt oder abgelehnt wurden, weil sie schädlichen Inhalt besitzen.
- **Spam Quarantined/Rejected:** Nachrichten, die unter Quarantäne gestellt oder abgelehnt wurden, weil sie als Spam identifiziert wurden.
- **Blacklist Rejects:** Nachrichten, die abgelehnt wurden, weil ihr Absender auf der Blacklist geführt wird.
- **Address Verification Rejects:** Nachrichten, die abgelehnt wurden, weil ihre Absenderadresse nicht verifiziert werden konnte.
- **SPF Rejects:** Nachrichten, die abgelehnt wurden, weil der sie sendende Rechner nicht zugelassen wird.
- **RBL Rejects:** Nachrichten, die abgelehnt wurden, weil der Absender auf einer Echtzeit-Blackhole-Liste geführt wird.
- **BATV Rejects:** Nachrichten, die abgelehnt wurden, weil das BATV-Tag ungültig war.
- **RDNS/HELO Rejects:** Nachrichten, die abgelehnt wurden, weil das HELO ungültig war oder RDNS-Einträge fehlten.

Ob es überhaupt Ablehnungen gibt, hängt von Ihren Einstellungen unter *Mail Security >> SMTP* ab.

Konfiguration

Auf der Registerkarte *Mail Security >> Mail-Manager >> Konfiguration* wird definiert, nach wie vielen Tagen das Datenbankprotokoll geleert beziehungsweise die unter Quarantäne gestellten E-Mails gelöscht werden. Alle Protokolle und E-Mails, die älter sind als die hier eingestellte Anzahl an Tagen, werden automatisch geleert/gelöscht.

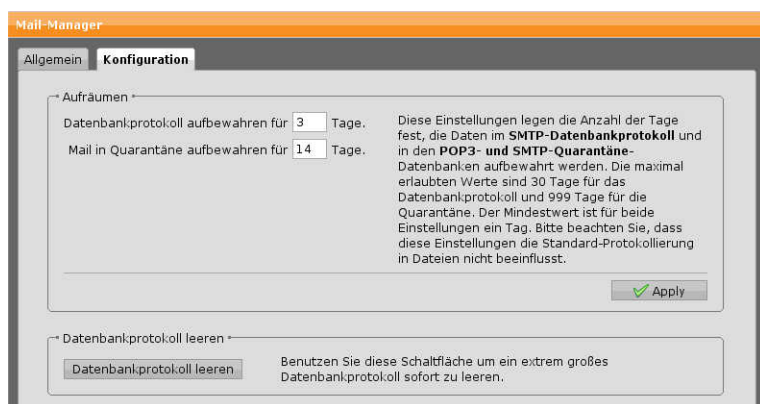


Figure 11.33 Mail-Manager: Konfiguration

Die Voreinstellungen sehen folgendermaßen aus:

- Das Datenbankprotokoll wird nach drei Tagen geleert. Die maximal erlaubte Anzahl an Tagen ist 30.
- Nachrichten in Quarantäne werden nach 14 Tagen gelöscht. Die maximal erlaubte Anzahl an Tagen ist 999.

Die minimal erlaubte Anzahl an Tagen für sowohl das Datenbankprotokoll als auch die Quarantäne ist ein Tag.

Datenbankprotokoll leeren

Diese Option ist nützlich, wenn das Datenbankprotokoll eine enorme Menge an Daten angesammelt hat und Sie das Protokoll sofort leeren möchten. Auf diese Weise müssen Sie nicht warten, bis die normale Aufräumaktion zur Anwendung kommt.

VoIP-Sicherheit

Voice over Internet Protocol (VoIP) ist der Sammelbegriff für das Routing von Sprachkonversationen über das Internet oder jedes andere IP-basierte Netzwerk. Astaro Security Gateway unterstützt die am häufigsten eingesetzten Protokolle, um Stimmsignale über das IP-Netzwerk zu transportieren:

- SIP
- H.323

Die Statistikseite von *VoIP-Sicherheit* im WebAdmin zeigt die Anzahl der SIP- und H.323-Verbindungen für verschiedene Zeitspannen.

SIP

Das *Session Initiation Protocol* (SIP, dt. Sitzungsinitialisierungsprotokoll) ist ein Signalisierungsprotokoll zum Aufbau, zur Modifikation und zum Beenden von Sitzungen zwischen zwei oder mehreren Kommunikationspartnern. Das Protokoll wird hauptsächlich zum Aufbau und zum Beenden von Audio- oder Videotelefonieverbindungen eingesetzt. SIP nutzt standardmäßig TCP auf Port 5060, um während des Telefonverbindungsaufbaus den dynamischen Port-Bereich zwischen den beiden Endpunkten auszuhandeln. Da durch das Öffnen des gesamten Port-Bereichs innerhalb des dynamischen Bereichs eine Sicherheitslücke entstehen würde, ist die Firewall in der Lage, den SIP-Datenverkehr „intelligent“ zu handhaben. Dies wird durch einen speziellen Helfer für die Verbindungsverfolgung (engl. *Connection Tracking Helper*) erreicht, welcher den Steuerkanal überwacht, um festzustellen, welche dynamischen Ports für die Verbindung genutzt werden und daraufhin nur diese Ports für den Datenverkehr zuzulassen, wenn der Steuerkanal beschäftigt ist. Zu diesem Zweck müssen Sie sowohl einen SIP-Server als auch ein SIP-Client-Netzwerk angeben, um die entsprechenden Paketfilterregeln anzulegen, die die Kommunikation über das SIP-Protokoll ermöglichen.

Um die Unterstützung für das SIP-Protokoll zu aktivieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie auf der Registerkarte *SIP* die SIP-Protokoll-Unterstützung.**

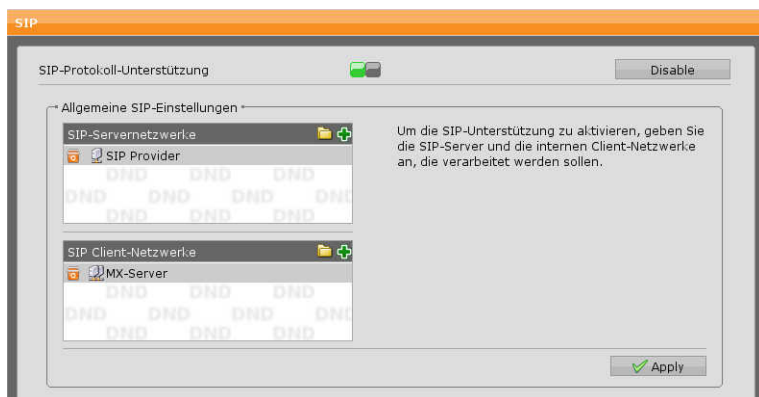


Figure 12.1 VoIP SIP: Konfiguration der Einstellungen

Die Statusampel wird gelb und der Abschnitt *Allgemeine SIP-Einstellungen* kann nun bearbeitet werden.

2. Nehmen Sie die folgenden Einstellungen vor:

SIP-Servernetzwerke: Hier können Sie den SIP-Server (der von Ihrem ISP bereitgestellt wird) auswählen, mit dem sich die SIP-Clients verbinden dürfen sollen. Wählen Sie aus Sicherheitsgründen nicht *Any* aus.

SIP-Client-Netzwerke: Wählen Sie die Rechner oder Netzwerke der SIP-Clients aus, denen gestattet ist, eine SIP-Kommunikation zu beginnen oder anzunehmen. Ein SIP-Client ist ein Endpunkt, der an einer Zweiwege-Kommunikation in Echtzeit mit einem anderen SIP-Client teilnimmt.

3. Klicken Sie *Übernehmen*.

Ihre Einstellungen werden gespeichert.

Um die Konfiguration abzubrechen, klicken Sie auf die Schaltfläche *Abort Enable* oder auf die gelbe Statusampel.

H.323

Das Protokoll *H.323* ist ein internationaler Multimedia-Kommunikationsstandard, der von der Internationalen Fernmeldeunion (engl. *International Telecommunication Union*, ITU-T) veröffentlicht wurde. Es legt die Protokolle fest, mit denen audio-visuelle Kommunikationssitzungen auf jedem paketvermittelten Netzwerk ermöglicht werden. *H.323* wird üblicherweise für *Voice over IP* (VoIP) und IP-basierte Videokonferenzen genutzt.

H.323 nutzt standardmäßig TCP auf Port 1720, um während des Telefonverbindungsbaus den dynamischen Port-Bereich zwischen den beiden Endpunkten auszuhandeln. Da durch das Öffnen des gesamten Port-Bereichs eine Sicherheitslücke entstehen würde, ist die Firewall in der Lage den H.323-Datenverkehr „intelligent“ zu steuern. Dies wird durch einen speziellen Helfer für die Verbindungsverfolgung (engl. *Connection Tracking Helper*) erreicht, welcher den Steuerkanal überwacht, um festzustellen, welche dynamischen Ports für die Verbindung genutzt werden und daraufhin nur diese Ports für den Datenverkehr zuzulassen, wenn der Steuerkanal beschäftigt ist. Zu diesem Zweck müssen Sie sowohl einen H.323-Gatekeeper als auch eine Client-Netzwerkdefinition angeben, um die entsprechenden Paketfilterregeln anzulegen, die die Kommunikation über das H.323-Protokoll ermöglichen.

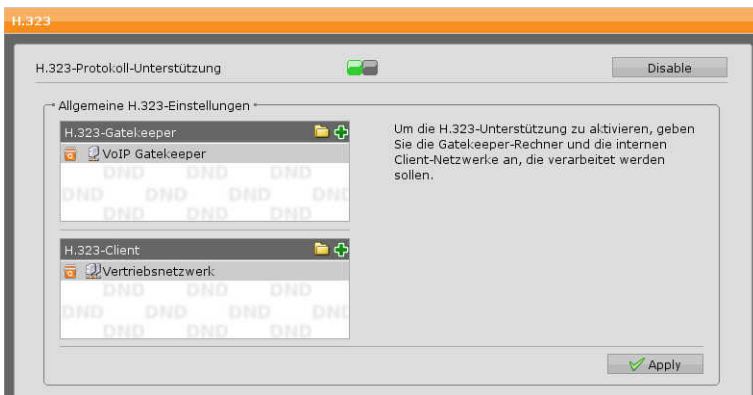


Figure 12.2 VoIP H.323: Konfiguration der Einstellungen

Um die Unterstützung für das H.323-Protokoll zu aktivieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie auf der Registerkarte *H.323* die H.323-Protokoll-Unterstützung.**

Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche. Die Statusampel wird gelb und der Abschnitt *Allgemeine H.323-Einstellungen* kann nun bearbeitet werden.

2. **Nehmen Sie die folgenden Einstellungen vor:**

H.323-Gatekeeper: Wählen Sie einen H.323-Gatekeeper aus. Ein H.323-Gatekeeper kontrolliert alle H.323-Clients (Endpunkte wie z. B. Microsoft's NetMeeting) in seiner Zone. Genauer betrachtet, agiert er als Überwachungsinstanz aller H.323-Anrufe innerhalb seiner Zone im LAN. Sei-

ne wichtigste Aufgabe besteht darin, zwischen den symbolischen Alias-Adressen und IP-Adressen zu übersetzen.

H.323-Client: Hier können Sie den Rechner oder das Netzwerk auswählen, zu dem und von dem aus H.323-Verbindungen aufgebaut werden. Ein H.323-Client ist ein Endpunkt im LAN, der an einer Zweiwege-Kommunikation in Echtzeit mit einem anderen H.323-Client teilnimmt.

3. **Klicken Sie Übernehmen.**

Ihre Einstellungen werden gespeichert.

Um die Konfiguration abubrechen, klicken Sie auf die Schaltfläche *Abort Enable* oder auf die gelbe Statusampel.

Kapitel 13

IM/P2P

Diese Kapitel beschreibt, wie Sie die Sicherheitsfunktionen von Astaro Security Gateway für Sofortnachrichten (engl. *Instant Messaging*) (IM) und Peer-to-Peer (P2P) konfigurieren.

Die Sofortnachrichten- und Peer-to-Peer-Protokolle werden durch den *Astaro Flow Classifier* (AFC), ein dediziertes Teilsystem zur Erkennung von Netzwerkverkehr, erkannt. Wann immer eine Funktion von Astaro Security Gateway erfordert, dass Netzwerkverkehr klassifiziert wird, wird das AFC-Teilsystem aktiv.

Die Seite *Sofortnachrichten-/Peer-to-Peer-Statistik* in WebAdmin gibt einen Überblick über die am häufigsten genutzten IM- und P2P-Protokolle und listet auch die häufigsten Quell-IP-Adressen auf, die auf diese Dienste zugegriffen haben. Jeder der Abschnitte enthält einen *Details*-Link. Ein Klick auf den Link leitet Sie zur entsprechenden Seite des Abschnitts *Berichte* von WebAdmin weiter, wo Sie weitere statistische Informationen finden können.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- Einstellungen
- Sofortnachrichten (IM)
- Peer-to-Peer (P2P)

Einstellungen

Im Menü *IM/P2P* > > *Einstellungen* werden die Einstellungen für den *Astaro Flow Classifier* (AFC) vorgenommen, einem Teilsystem, das zur Klassifizierung des Netzwerkverkehrs dient.

Hinweis – Die Einstellungen wirken sich auf den gesamten Astaro Flow Classifier aus. Dies beinhaltet auch alle definierten AFC Verkehrsbezeichner (engl. *traffic selectors*) auf der Registerkarte *Netzwerk* > > *Dienstqualität (QoS)* > > *Verkehrsbezeichner*.

Allgemein

Auf der Registerkarte *Einstellungen >> Allgemein* können Sie das *Astaro-Flow-Classifizier-(AFC)*-Teilsystem aktivieren.

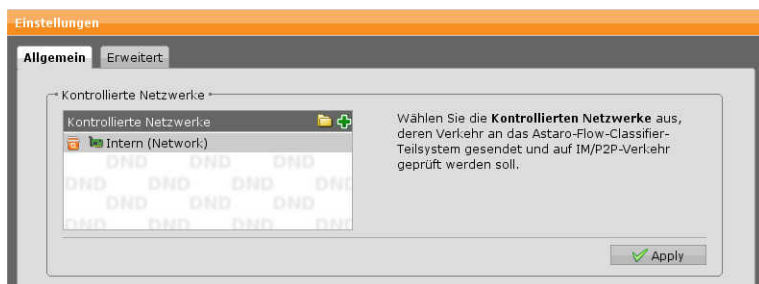


Figure 13.1 IM/P2P: Konfiguration der allgemeinen IM/P2P-Einstellungen

Um IM/P2P zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Wählen Sie die zu kontrollierenden Netzwerke aus:**
Wählen Sie die Netzwerke aus, die auf IM- und P2P-Datenverkehr geprüft werden sollen.
2. **Klicken Sie *Übernehmen*.**
Ihre Einstellungen werden gespeichert.

Erweitert

Auf der Registerkarte *Einstellungen >> Erweitert* können Sie einzelne Rechner oder Netzwerke von der IM- und P2P-Kontrolle ausnehmen. Des Weiteren können Sie festlegen, wie umfangreich der vom Astaro Flow Classifizier klassifizierte Datenverkehr protokolliert wird.

Erweitert

Die Rechner und Netzwerke im Feld *Kontroll-Ausnahmen* werden von der Kontrolle des IM- und P2P-Datenverkehrs durch den Astaro Flow Classifizier ausgenommen, d. h. weder eingehender noch ausgehender Verkehr dieser Rechner oder Netzwerke wird auf IM/P2P-Muster überprüft.



Figure 13.2 IM/P2P: Erweiterte Einstellungen

Protokollierung

Mit dieser Einstellung wird der Protokollumfang eingestellt. Hiermit kann verhindert werden, dass von den IM/P2P-Clients durch viele kurz andauernde Verbindungen zu viele Protokolleinträge generiert werden. Die folgenden Protokollstufen sind verfügbar:

- **Aus:** Wählen Sie diese Protokollierungsstufe, wenn Sie die Protokollierung vollständig abschalten wollen.
- **Begrenze auf 5/Sek.:** Es werden pro Sekunde maximal fünf Pakete protokolliert.
- **Begrenze pro Rechner auf 1/Sek.:** Für jeden Rechner wird maximal ein Paket pro Sekunde protokolliert. Diese Stufe ist voreingestellt.
- **Alles protokollieren:** Wählen Sie diese Protokollierungsstufe, wenn Sie eine ausführliche Protokollierung für den gesamten IM/P2P-Verkehr wollen. Beachten Sie, dass dies zu einer sehr umfangreichen Protokollierung führen kann.

Sofortnachrichten (IM)

Sofortnachrichten (IM, engl. *Instant Messaging*) ist eine Form von Echtzeit-Kommunikation zwischen zwei oder mehreren Kommunikationspartnern, die auf geschriebenem Text basiert. Hierzu muss auf dem Client ein entsprechendes Programm installiert sein, das im Gegensatz zu E-Mail die Kommunikation in Echtzeit ermöglicht.

Astaro Security Gateway besitzt eine Liste mit den gebräuchlichsten Protokollen für Sofortnachrichten. Dadurch können Sie entscheiden, wie das System mit Datenverkehr verfährt, der vom Teilsystem Astaro Flow Classifier als Sofortnachrichten identifiziert wurde.

Sicherheitshinweis – Die Klassifizierung von Datenverkehr ist niemals so exakt wie z. B. die Kontrolle eines speziellen TCP-Ports. Ein bestimmter Grad an Ungewissheit bleibt immer: Client-Protokolle können wechseln oder eine große Ähnlichkeit mit unproblematischem Datenverkehr haben und dadurch die Nutzung einfacher Klassifizierungsalgorithmen erschweren. Strikte Sicherheitsanforderungen lassen sich daher mit der IM/P2P-Kontrolle nur bedingt umsetzen. Vielmehr dient diese IM/P2P-Kontrolle zur Entschärfung von Gefahren, Schutz von Ressourcen und zum Aufdecken von Verstößen gegen Sicherheitsrichtlinien.

Protokolle

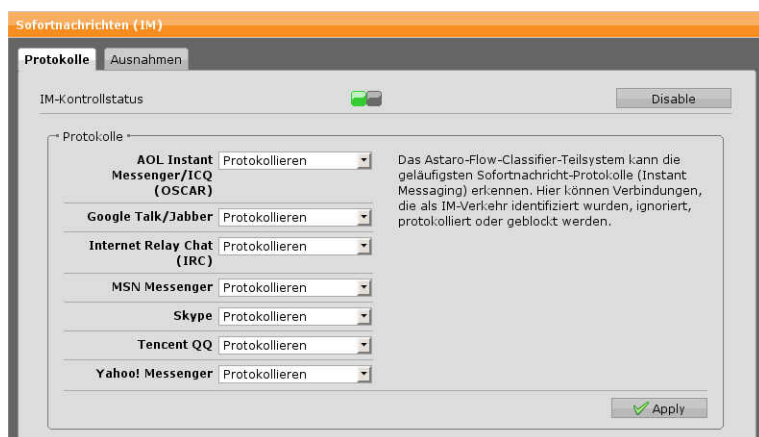


Figure 13.3 Sofortnachrichten: Konfiguration der Dienste

Um die Protokolleinstellungen zu bearbeiten, aktivieren Sie die IM-Kontrolle. Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche.

Die Statusampel wird grün und der Abschnitt *Protokolle* kann nun bearbeitet werden. Sie können die folgenden Aktionen für jeden IM-Dienst durchführen lassen:

- **Nicht kontrollieren:** Das IM-Protokoll wird weder ermittelt noch wird der Datenverkehr beschränkt. Der IM-Datenverkehr kann die Firewall ungehindert passieren.
- **Protokollieren:** Der entsprechende IM-Datenverkehr wird protokolliert, wenn er die Firewall passiert.
- **Dateiübertragungen blockieren:** Es können keine Dateien zwischen den Kommunikationspartnern ausgetauscht werden.

Hinweis – Für einige Protokolle wird diese Option augenblicklich nicht unterstützt und deshalb ausgegraut.

- **Vollständig blockieren:** Kein IM-Verkehr des betreffenden Typs kann die Firewall passieren.

Die folgenden Sofortnachrichten-Protokolle können kontrolliert werden:

- AOL Instant Messenger (AIM) and ICQ (OSCAR)
- Google Talk/Jabber
- Internet Relay Chat (IRC)
- MSN Messenger
- Skype
- Tencent QQ
- Yahoo! Messenger

Hinweis – Skype-Verbindungen können nicht zuverlässig blockiert werden, da Skype einigen Aufwand betreibt, um seinen Datenverkehr zu verschleiern.

Ausnahmen

Auf der Registerkarte *Sofortnachrichten (IM)* >> *Ausnahmen* können Sie feinmaschigere Ausnahmen von Aktionen des Astaro Flow Classifier festlegen. Im Gegensatz zur Funktion *Kontroll-Ausnahmen* auf der Registerkarte *Einstellungen* >> *Erweitert* erfolgt die Auswertung der Ausnahmeregeln nach der Klassifizierung des Netzwerkverkehrs. Dadurch ist es möglich, beispielsweise einzelne Rechner oder Netzwerke von einer spezifischen Protokolleinstellung auszunehmen, während alle anderen Einstellungen weiterhin angewendet werden.

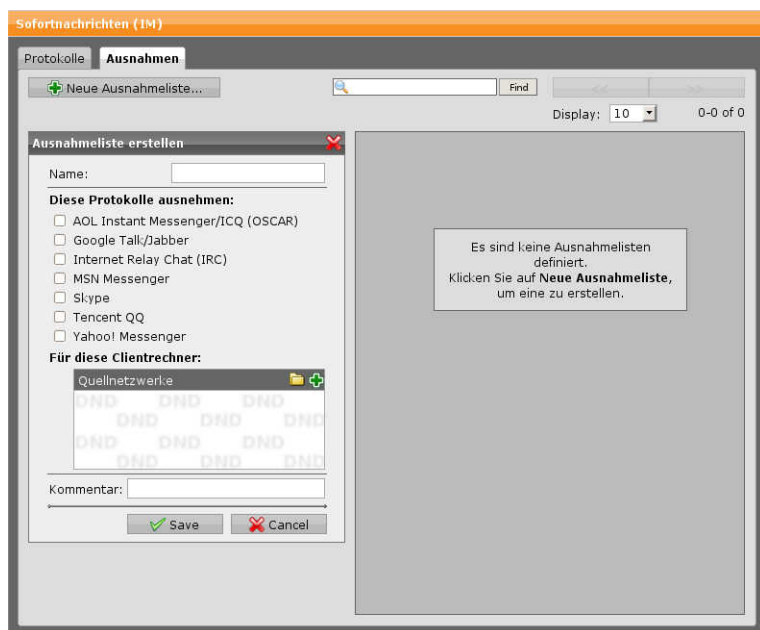


Figure 13.4 Sofortnachrichten: Ausnahmenliste

Um eine Ausnahme zu definieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Ausnahmen* auf *Neue Ausnahmeliste*.**
Das Dialogfenster *Ausnahmeliste erstellen* wird geöffnet.
2. **Nehmen Sie die folgenden Einstellungen vor:**
Name: Geben Sie einen aussagekräftigen Name für ein.

Diese Protokolle ausnehmen: Wählen Sie die Sofortnachrichten-Protokolle aus, die ausgenommen werden sollen.

Für diese Clientrechner: Wählen Sie die Quellrechner/-netzwerke aus, die von den Aktionen des Astaro Flow Classifier ausgenommen werden sollen.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über diese Ausnahme hinzu.

3. Klicken Sie *Speichern*.

Die neue Ausnahmeliste wird in der Liste *Ausnahmen* angezeigt.

Um eine Ausnahmeliste zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Peer-to-Peer (P2P)

Ein Peer-to-Peer-(P2P)-Computernetzwerk ist ein Netzwerk, das sich primär auf die Rechenleistung und Bandbreite der Netzwerkteilnehmer verlässt anstatt sich auf eine Anzahl von Servern zu stützen. Ein reines P2P-Netzwerk kennt keine Einteilung in Clients und Server; alle Rechner-Knoten (*Peers*) sind gleichberechtigt und fungieren sowohl als „Clients“ als auch „Server“ für die anderen Knoten im Netzwerk. Durch diese Besonderheit ist ein P2P-Netzwerk für viele Zwecke einsetzbar, besonders für den Dateiaustausch (engl. *file sharing*), d. h. das Verfahren, Dateien für andere Benutzer zum Herunterladen über das Internet zur Verfügung zu stellen.

Astaro Security Gateway besitzt eine Liste mit den gebräuchlichsten Peer-to-Peer-Diensten. Dadurch können Sie entscheiden, wie das System mit Datenverkehr verfährt, der vom Teilsystem Astaro Flow Classifier als P2P-Dienst identifiziert wurde.

Sicherheitshinweis – Die Klassifizierung von Datenverkehr ist niemals so exakt wie z. B. die Kontrolle eines speziellen TCP-Ports. Ein bestimmter Grad an Ungewissheit bleibt immer: Client-Protokolle können wechseln oder eine große Ähnlichkeit mit unproblematischem Datenverkehr haben und dadurch die Nutzung einfacher Klassifizierungsalgorithmen erschweren. Strikte Sicherheitsanforderungen lassen sich daher mit der IM/P2P-Kontrolle nur bedingt umsetzen. Vielmehr dient diese IM/P2P-Kontrolle zur Entschärfung von Gefahren, Schutz von Ressourcen und zum Aufdecken von Verstößen gegen Sicherheitsrichtlinien.

Protokolle

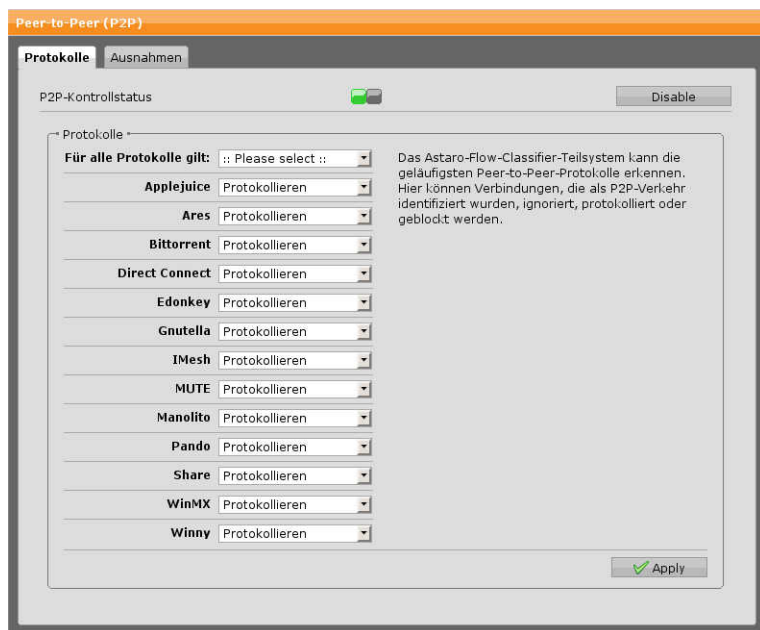


Figure 13.5 P2P: Konfiguration der Dienste

Um die Protokolleinstellungen zu bearbeiten, aktivieren Sie die P2P-Kontrolle. Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche. Die Statusampel wird grün und der Abschnitt *Protokolle* kann nun bearbeitet werden. Sie können die folgenden Aktionen für jeden P2P-Dienst durchführen lassen:

- **Nicht kontrollieren:** Das P2P-Protokoll wird weder ermittelt noch wird der Datenverkehr beschränkt. Der P2P-Datenverkehr kann die Firewall ungehindert passieren.
- **Protokollieren:** Der entsprechende P2P-Datenverkehr wird protokolliert, wenn er die Firewall passiert.

- **Dateiübertragungen blockieren:** Es können keine Dateien zwischen den Kommunikationspartnern ausgetauscht werden.
- **Vollständig blockieren:** Kein P2P-Verkehr des betreffenden Typs kann die Firewall passieren.

Es ist jedoch auch möglich, alle Dienste zentral zu kontrollieren, indem Sie das Feld *Für alle Protokolle gilt* auf den gewünschten Wert setzen.

Die folgenden Peer-to-Peer-Protokolle können kontrolliert werden:

- Applejuice
- Ares
- BitTorrent
- Direct Connect
- Edonkey
- Gnutella
- IMesh
- MUTE
- Manolito
- Pando
- Share
- WinMX
- Winny

Ausnahmen

Auf der Registerkarte *Peer-to-Peer (P2P)* >> *Ausnahmen* können Sie feinmaschigere Ausnahmen von Aktionen des Astaro Flow Classifier festlegen. Im Gegensatz zur Funktion *Kontroll-Ausnahmen* auf der Registerkarte *Einstellungen* >> *Erweitert* erfolgt die Auswertung der Ausnahmeregeln nach der Klassifizierung des Netzwerkverkehrs. Dadurch ist es möglich, beispielsweise einzelne Rechner oder Netzwerke von einer spezifischen Protokolleinstellung auszunehmen, während alle anderen Einstellungen weiterhin angewendet werden.

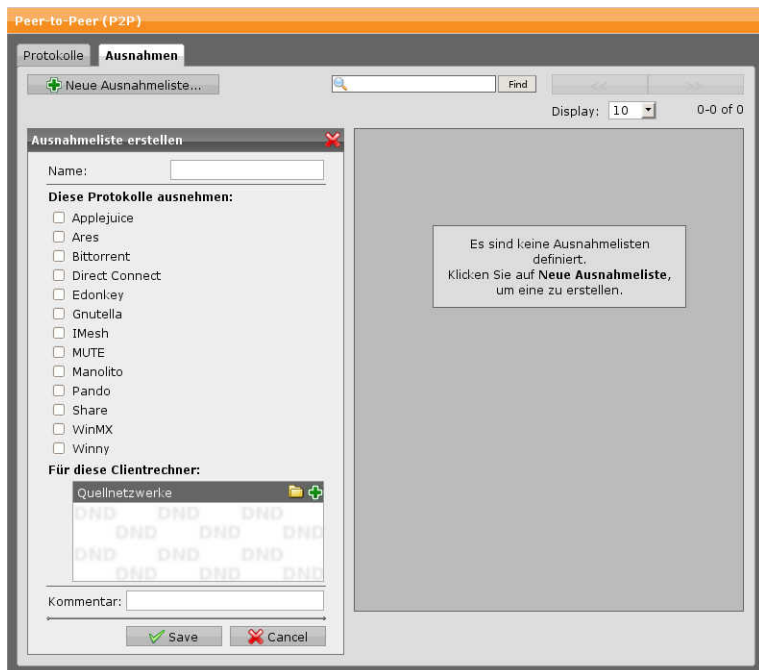


Figure 13.6 P2P: Ausnahmeliste

Um eine Ausnahme zu definieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Ausnahmen* auf *Neue Ausnahmeliste*.**
Das Dialogfenster *Ausnahmeliste erstellen* wird geöffnet.
2. **Nehmen Sie die folgenden Einstellungen vor:**
Name: Geben Sie einen aussagekräftigen Name für diese Ausnahme ein.
Diese Protokolle ausnehmen: Wählen Sie die Peer-to-Peer-Protokolle aus, die ausgenommen werden sollen.
Für diese Clientrechner: Wählen Sie die Quellrechner/-netzwerke aus, die von den Aktionen des Astaro Flow Classifier ausgenommen werden sollen.
Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die Ausnahme hinzu.
3. **Klicken Sie *Speichern*.**
Die neue Ausnahmeliste wird in der Liste *Ausnahmen* angezeigt.

Um eine Ausnahmeliste zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Kapitel 14

Site-to-Site-VPN

In diesem Kapitel wird beschrieben, wie Sie Site-to-Site-VPN-Einstellungen von Astaro Security Gateway konfigurieren. Site-to-Site-VPNs werden in Astaro Security Gateway über sogenannte *Virtual Private Networks* (VPNs, dt. virtuelle private Netzwerke) realisiert. Diese sind ein kostengünstiges und sicheres Mittel für räumlich getrennte Netzwerke, um miteinander über ein öffentliches Netzwerk wie das Internet vertraulich zu kommunizieren. Dazu verwenden sie das kryptografische Tunnelprotokoll IPSec, das Vertraulichkeit und Datenschutz für die mit IPSec übermittelten Daten bietet.

Querverweis – Detaillierte Informationen zur Konfiguration von VPN-Verbindungen (auch Tunnel genannt) finden Sie in der Astaro Knowledgebase³⁴ im Verzeichnis *ASG Version 7 >> Astaro Manuals and Guides*.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- IPSec
- SSL
- Zertifikatverwaltung

Die Übersichtsseite *Site-to-Site-VPN* in WebAdmin zeigt alle konfigurierten IPSec- und SSL-Verbindungen sowie ihren augenblicklichen Zustand. Der Zustand einer Verbindung wird durch die Farbe seines Statusampel wiedergegeben. Es gibt zwei Arten von Statusampeln: die größeren neben dem Verbindungsnamen informieren Sie über den Gesamtzustand einer Verbindung. Die verschiedenen Farben bedeuten Folgendes:

- Grün – Alle SAs (*Security Association*, dt. Sicherheitsverbindung) wurden hergestellt. Die Verbindung ist voll funktionsfähig.
- Gelb – Nicht alle SAs wurden hergestellt. Die Verbindung ist nur eingeschränkt funktionsfähig.
- Rot – Keine SAs wurden hergestellt. Die Verbindung ist nicht funktionsfähig.

³⁴ <http://www.astaro.com/kb/>

Die kleineren Statusampeln neben der Information zum Tunnel geben den Zustand für den Tunnel wieder. Hier bedeuten die Farben Folgendes:

- Grün – Alle SAs wurden hergestellt. Der Tunnel ist voll funktionsfähig.
- Gelb – Die IPSec-SA wurde hergestellt, die ISAKMP-SA (*Internet Security Association and Key Management Protocol*) hingegen wurde nicht hergestellt. Der Tunnel ist voll funktionsfähig.
- Rot – Keine SAs wurden hergestellt. Die Verbindung ist nicht funktionsfähig.

IPSec

IP Security (IPSec) ist ein Standard für die Sicherung von *Internet-Protocol* (IP)-Kommunikationen durch Verschlüsselung- und/oder Authentifizierung aller IP-Pakete.

Der IPSec-Standard kennt zwei Betriebsarten (Modi) und zwei Protokolle:

- Transportmodus (engl. *Transport Mode*)
- Tunnelmodus (engl. *Tunnel Mode*)
- *Authentication Header* (AH): Protokoll für Authentifizierung
- *Encapsulated Security Payload* (ESP): Protokoll für Verschlüsselung (und Authentifizierung)

Des Weiteren bietet IPSec Methoden für die manuelle und die automatische Verwaltung von Sicherheitsverbindungen (SAs, engl. *Security Associations*) sowie zur Schlüsselverteilung. Alle diese Merkmale wurden in einer *Domain of Interpretation* (DOI) zusammengefasst.

IPSec-Modi

IPSec kann entweder im Transportmodus oder im Tunnelmodus arbeiten. Eine Rechner-zu-Rechner-Verbindung kann grundsätzlich jeden Modus verwenden. Wenn es sich bei einem der beiden Tunnelendpunkte jedoch um ein Astaro Security Gateway handelt, muss der Tunnelmodus verwendet werden. Die IPSec-VPN-Verbindungen dieses Sicherheitssystems arbeiten immer im Tunnelmodus.

Im Transportmodus wird das zu bearbeitende IP-Paket nicht in ein anderes IP-Paket eingepackt. Der ursprüngliche IP-Header wird beibehalten und das übrige Paket wird entweder im Klartext (AH) oder verschlüsselt (ESP) gesendet.

Nun kann entweder das komplette Paket mit AH authentifiziert oder die Payload mit Hilfe von ESP verschlüsselt und authentifiziert werden. Bei beiden Varianten wird der Original-Header in Klartext über das WAN geschickt.

Im Tunnelmodus wird das komplette Paket – Header und Payload – in ein neues IP-Paket eingepackt. Ein neuer IP-Header wird vorne an das IP-Paket angehängt, wobei die Zieladresse auf den empfangenden Tunnelendpunkt gesetzt wird. Die IP-Adressen des eingepackten Paketes bleiben unverändert. Das Originalpaket kann dann mit AH authentifiziert oder mit ESP authentifiziert und verschlüsselt werden.

IPSec-Protokolle

IPSec verwendet für die sichere Kommunikation auf IP-Ebene zwei Protokolle:

- **Authentication Header (AH):** Ein Protokoll für die Authentifizierung von Absendern eines Pakets sowie zur Überprüfung der Integrität des Paketinhalts.
- **Encapsulating Security Payload (ESP):** Ein Protokoll für die Verschlüsselung des gesamten Pakets sowie für die Authentifizierung seines Inhalts.

Das *Authentication-Header*-Protokoll (AH) überprüft die Authentizität und die Integrität des Paketinhalts. Des Weiteren überprüft es, ob die Sender- und Empfänger-IP-Adressen während der Übertragung geändert wurden. Die Authentifizierung des Pakets erfolgt anhand einer Prüfsumme, die mittels eines *Hash-based Message Authentication Codes* (HMAC) in Verbindung mit einem Schlüssel und einem der folgenden Hash-Algorithmen berechnet wurde:

- **Message Digest Version 5 (MD5):** Dieser Algorithmus erzeugt aus einer Nachricht mit beliebiger Länge einen 128-Bit-langen Hash-Wert. Dieser resultierende Hash-Wert stellt eine Art Fingerabdruck des Paketinhalts dar und ändert sich, wenn die Nachricht verändert wird. Dieser Hash-Wert wird manchmal auch als digitale Signatur oder als *Message Digest* (dt. Prüfsumme) bezeichnet.
- **The Secure Hash (SHA-1):** Dieser Algorithmus erzeugt analog zum MD5 einen 160Bit-langen Hash-Wert. SHA-1 ist aufgrund des längeren Schlüssels sicherer als MD5.

Der Aufwand, einen Hash-Wert mittels SHA-1 zu berechnen, ist im Vergleich zum MD5-Algorithmus etwas höher. Die Berechnungsgeschwindigkeit hängt natürlich von der Prozessorgeschwindigkeit und der Anzahl der IPSec-VPN-Verbindungen ab, die auf Astaro Security Gateway verwendet werden.

Das *Encapsulated-Security-Payload*-Protokoll (ESP) bietet zusätzlich zur Verschlüsselung auch die Möglichkeit der Absender-Authentifizierung und der Verifizierung von Paketinhalten. Wenn ESP im Tunnelmodus verwendet wird, wird das komplette IP-Paket (Header und Payload) verschlüsselt. Zu diesem verschlüsselten Paket wird ein neuer unverschlüsselter IP- und ESP-Header hinzugefügt: Der neue IP-Header beinhaltet die Adresse des Empfänger-Gateway und die Adresse des Absender-Gateway. Diese IP-Adressen entsprechen denen des VPN-Tunnels.

Für ESP mit Verschlüsselung werden üblicherweise die folgenden Algorithmen verwendet:

- Triple Data Encryption Standard (3DES)
- Advanced Encryption Standard (AES)

Von diesen bietet AES den höchsten Sicherheitsstandard. Die effektiven Schlüssellängen, die mit AES verwendet werden können, sind 128, 192 oder 256 Bits. Astaro Security Gateway unterstützt mehrere Verschlüsselungs-Algorithmen. Für die Authentifizierung kann der MD5- oder der SHA-1-Algorithmus verwendet werden.

NAT Traversal (NAT-T)

NAT-Traversal ist ein Verfahren um zwischen Rechnern in TCP/IP-Netzwerken Verbindungen über NAT-Geräte aufzubauen. Dies wird erreicht, indem UDP-Verkapselung der ESP-Pakete benutzt wird, um IPSec-Tunnel über NAT-Geräte aufzubauen. Die UDP-Verkapselung wird nur verwendet, wenn zwischen den IPSec-Gegenstellen NAT gefunden wird; andernfalls werden normale ESP-Pakete verwendet.

Mit NAT-Traversal kann ein IPSec-Tunnel auch aufgebaut werden, wenn sich firewall oder ein Road Warrior hinter einem NAT-Router befindet. Wenn Sie diese Funktion nutzen wollen, müssen allerdings beide IPSec-Endpunkte NAT-Traversal unterstützen – das wird automatisch ausgehandelt. Zusätzlich muss auf dem NAT-Gerät der *IPSec-Passthrough* (IPSec-Durchreichung) ausgeschaltet sein, da dies NAT-Traversal beeinträchtigen kann.

Wenn Road Warrior NAT-Traversal verwenden wollen, muss ihr entsprechendes Benutzerobjekt in WebAdmin eine Statische Fernzugriffs-IP-Adresse (RAS, engl. *remote access IP address*) besitzen. Die Einstellung hierfür heißt *Statische Fernzugriffs-IP verwenden* und Sie finden sie auf der Seite Benutzer in WebAdmin.

Um zu verhindern, dass der Tunnel abgebaut wird, wenn keine Daten übermittelt werden, sendet NAT-Traversal in einem Intervall von 60 Sekunden ein

Signal zur Aufrechterhaltung (engl. *keep alive*). Durch dieses Aufrechterhaltungssignal wird sichergestellt, dass der NAT-Router sich die Statusinformation der Sitzung behält, damit der Tunnel offen bleibt.

Verbindungen

Auf der Registerkarte *Site-to-Site VPN >> IPSec >> Verbindungen* können Sie IPSec-Verbindungen erstellen und bearbeiten.

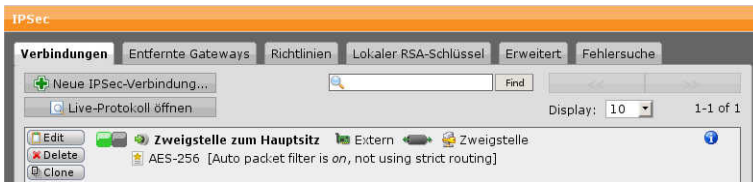


Figure 14.1 Site-to-Site IPSec: Verbindungen

Um eine IPSec-Verbindung zu erstellen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Verbindungen* auf *Neue IPSec-Verbindung*.**

Das Dialogfenster *Neue IPSec-Verbindung* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Name: Geben Sie einen aussagekräftigen Name für diese Verbindung ein.

Entferntes Gateway: Wählen Sie eine Definition für das entfernte Gateway. Entfernte Gateways werden auf der Registerkarte *Site-to-Site-VPN >> IPSec >> Entfernte Gateways* definiert.

Lokale Schnittstelle: Wählen Sie die Schnittstelle für den lokalen Verbindungsendpunkt des IPSec-Tunnels aus.

Richtlinie: Wählen Sie die IPSec-Sicherheitsrichtlinie für diese IPSec-Verbindung aus. Die IPSec-Sicherheitsrichtlinien werden auf der Registerkarte *Site-to-Site-VPN >> IPSec >> Richtlinien* definiert.

Lokale Netzwerke: Wählen Sie die lokalen Netzwerke aus, die über den VPN-Tunnel erreichbar sein sollen.

Autom. Paketfilter: Wählen Sie diese Option, um automatisch Paketfilterregeln hinzuzufügen, die den Datenverkehr für diese VPN-Verbindung zulassen. Die Regeln werden hinzugefügt, sobald die VPN-Verbindung erfolgreich aufgebaut wurde; und sie werden entfernt, wenn die Verbindung beendet wurde. Wenn Sie eine striktere VPN-Verbindung möchten, deaktivieren Sie die Option *Autom. Paketfilter* und verwenden Sie stattdessen IPSec-Objekte im Paketfilter-Regelwerk.

Striktes Routing: Wenn diese Funktion eingeschaltet ist, erfolgt das VPN-Routing nicht nur anhand der Zieladresse, sondern anhand von Quell- und Zieladresse. Auf diese Weise werden nur Datenpakete durch den VPN-Tunnel geleitet, die mit der Tunneldefinition exakt übereinstimmen. Als Folge davon können Sie kein SNAT verwenden, um Netzwerke oder Rechner zum VPN-Tunnel hinzuzufügen, die nicht von vorneherein Teil der Tunneldefinition sind. Andererseits, wenn striktes Routing ausgeschaltet ist, können Sie kein gemischtes unverschlüsseltes/verschlüsseltes Setup für dasselbe Netzwerk je nach Quelladresse haben.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die IPSec-Verbindung hinzu.

3. Klicken Sie **Speichern**.

Die neue Verbindung wird in der IPSec-Liste *Verbindungen* angezeigt.

Um eine Verbindung zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Live-Protokoll öffnen: Der *IPSec-VPN-Live-Protokoll* dient zur Überwachung der aufgebauten IPSec-Verbindungen. Durch einen Klick auf die Schaltfläche wird das Fenster geöffnet.

Entfernte Gateways

Auf der Registerkarte *IPSec >> Entfernte Gateways* können Sie die entfernten Gateways (engl. *Remote Gateway*) für Ihre Site-to-Site-VPN-Tunnel definieren. Diese entfernten Netzwerkdefinitionen stehen dann für die Konfiguration der IPSec-Verbindungen auf der Registerkarte *IPSec >> Verbindungen* zur Verfügung.

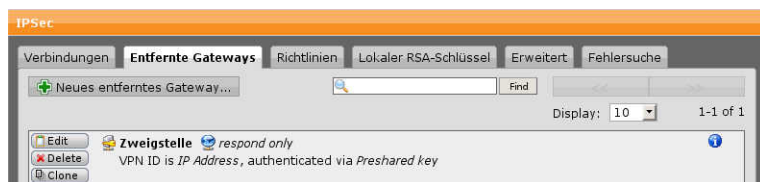


Figure 14.2 Site-to-Site IPSec: Liste entfernter Gateways

Um ein entferntes Gateway hinzuzufügen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte auf *Neues entferntes Gateway*.**

Das Dialogfenster *Entferntes Gateway hinzufügen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Name: Geben Sie einen aussagekräftigen Name für dieses entfernte Gateway ein.

Gateway-Typ: Wählen Sie den Gateway-Typ aus. Die folgenden Typen stehen zur Verfügung:

- **Verbindung initiieren:** Wählen Sie diesen Typ aus, wenn der entfernte Endpunkt eine statische IP-Adresse besitzt, so dass eine Verbindung zum entfernten Gateway von der Firewall initiiert werden kann. Geben Sie im Feld *Gateway* das entfernte Gateway an. Sie können diesen Typ auch wählen, wenn das entfernte Gateway über DynDNS aufgelöst werden kann.
- **Nur antworten:** Wählen Sie diesen Typ aus, wenn die IP-Adresse des entfernten Endpunkts unbekannt ist oder nicht über DynDNS aufgelöst werden kann. Die Firewall ist nicht in der Lage, eine Verbindung zu dem entfernten Gateway aufzubauen und wartet deshalb auf eingehende Verbindungen, auf die sie lediglich antworten muss.

Authentifizierungsmethode: Wählen Sie die Authentifizierungsmethode für diese entfernte Gateway-Definition aus. Die folgenden Arten sind verfügbar:

- **Vorvereinbarter Schlüssel:** Authentifizierung mit *vorvereinbarten Schlüsseln* (PSK, engl. *Preshared Keys*) verwendet geheime Kennwörter als Schlüssel. Diese Kennwörter müssen an die Endpunkte verteilt werden, bevor eine Verbindung aufgebaut wird. Wenn ein neuer VPN-Tunnel aufgebaut ist, überprüft jede Seite, ob die andere Seite das geheime Kennwort kennt. Die Sicherheit der PSKs hängt von der Qualität der verwendeten Kennwörter ab: normale Wörter und Ausdrücke fallen schnell Wörterbuchangriffen zum Opfer. Permanente oder langdauernde IPSec-Verbindungen sollten stattdessen Zertifikate oder RSA-Schlüssel verwenden.
- **RSA-Schlüssel:** Authentifizierung mit RSA-Schlüsseln ist technologisch ausgefeilter. Bei dieser Methode erzeugt jede Seite der Verbindung ein Schlüsselpaar, das aus einem öffentlichen (engl. *public key*) und einem privaten Schlüssel (engl. *private key*) besteht. Der private Schlüssel wird

zur Verschlüsselung und Authentifizierung während des Schlüsselaustauschs benötigt. Beide Endpunkte einer IPSec-VPN-Verbindung benötigen bei dieser Authentifizierungsmethode ihr eigenes Schlüsselpaar. Kopieren Sie den öffentlichen RSA-Schlüssel der Gegenstelle (*Site-to-Site-VPN >> IPSec >> Lokaler RSA-Schlüssel*) in das Feld *Öffentlicher Schlüssel* auf dem lokalen System und andersherum. Geben Sie darüber hinaus die VPN-ID-Typen und die VPN-Identifizierungen (VPN-ID) an, die zu den entsprechenden RSA-Schlüsseln gehören.

- **Lokales X.509-Zertifikat:** Das X.509-Zertifikat basiert ähnlich wie die Authentifizierung mit RSA-Schlüsseln auf öffentlichen Schlüsseln und privaten Schlüsseln. Ein X.509-Zertifikat enthält den öffentlichen Schlüssel zusammen mit zusätzlichen Informationen über den Besitzer des Schlüssels. Solche Zertifikate sind von einer CA (Zertifizierungsstelle, engl. *Certificate Authority*) signiert und ausgestellt, der der Besitzer vertraut. Während des Schlüsselaustauschs werden die Zertifikate ausgetauscht und mit Hilfe des lokal gespeicherten CA-Zertifikats überprüft. Wählen Sie diese Authentifizierungsmethode aus, wenn das X.509-Zertifikat des entfernten VPN-Gateway auf dem lokalen System gespeichert ist.
- **Remote-X.509-Zertifikat:** Wählen Sie diese Authentifizierungsmethode aus, wenn das X.509-Zertifikat des entfernten VPN-Gateway nicht auf dem lokalen System gespeichert ist. In diesem Fall müssen Sie dann den *VPN-ID-Typ* und die *VPN-ID* des Zertifikats angeben, das auf dem entfernten VPN-Gateway genutzt wird, d. h. das Zertifikat, das im Bereich *Lokales X.509-Zertifikat* auf der Registerkarte *Site-to-Site-VPN >> IPSec >> Erweitert* ausgewählt ist.

VPN-ID-Typ: Abhängig von der ausgewählten Authentifizierungsmethode müssen Sie einen *VPN-ID-Typ* und eine *VPN-ID* angeben. Die hier angegebene VPN-ID muss mit dem Wert auf der Gegenstelle übereinstimmen. Angenommen, Sie verwenden zwei ASG-Systeme, um einen Site-to-Site-VPN-Tunnel aufzubauen. Wenn Sie dann als Authentifizierungsmethode RSA-Schlüssel auf dem lokalen System auswählen, müssen der VPN-ID-Typ und die VPN-ID mit dem übereinstimmen, was auf der Registerkarte *Site-to-Site-VPN >> IPSec >> Lokale RSA-Schlüssel*) im WebAdmin der Gegenstelle konfiguriert ist.

Die folgenden VPN-ID-Typen können ausgewählt werden:

- IP-Adresse
- Rechnername

- E-Mail-Adresse
- Distinguished Name (nur bei Authentifizierungsmethode *Remote-X.509-Zertifikat*)

Entfernte Netzwerke: Wählen Sie die entfernten Netzwerke aus, die über das entfernte Gateway erreichbar sein sollen.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über das entfernte Gateway hinzu.

3. Klicken Sie *Speichern*.

Die Gateway-Definition wird in der Liste *Entfernte Gateways* angezeigt.

Um eine Definition eines entfernten Gateways zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Richtlinien

Auf der Registerkarte *IPSec >> Richtlinien* können Sie die Parameter für IPSec-Verbindungen definieren und in einer IPSec-Richtlinie zusammenfassen. Eine IPSec-Richtlinie legt die Schlüsselaustausch-Methode (IKE) und die IPSec-Antragsparameter für eine IPSec-Verbindung fest. Beachten Sie, dass jede IPSec-Verbindung eine IPSec-Richtlinie benötigt.

Um eine IPSec-Richtlinie zu definieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Richtlinien* auf *Neue IPSec-Richtlinie*.**
Das Dialogfenster *IPSec-Richtlinie hinzufügen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Name: Geben Sie einen aussagekräftigen Name für diese Richtlinie ein.

IKE-Verschlüsselungsalgorithmus: Der Verschlüsselungsalgorithmus legt den Algorithmus fest, der für die Verschlüsselung der IKE-Nachrichten verwendet wird. Die folgenden Algorithmen werden unterstützt:

- *DES* (56 Bit)
- *3DES* (168 Bit)
- *AES 128* (128 Bit)
- *AES 192* (192 Bit)
- *AES 256* (256 Bit)

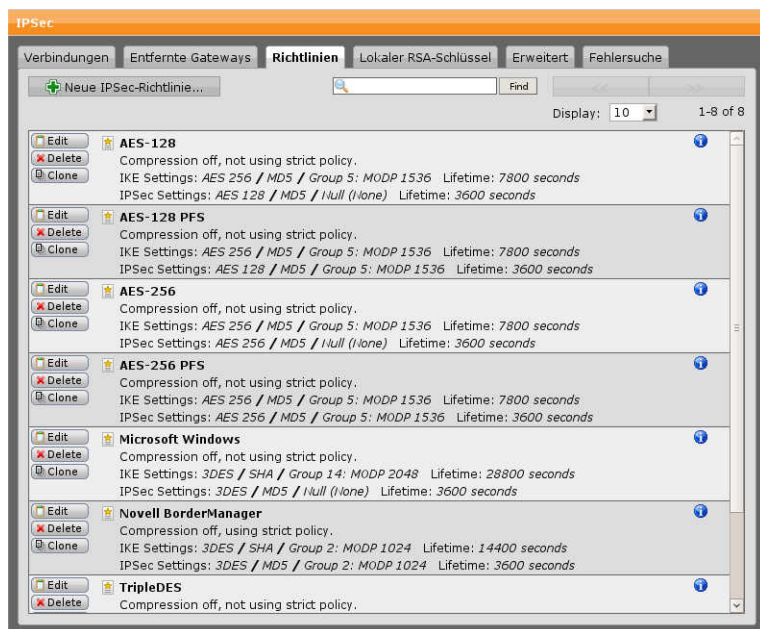


Figure 14.3 Site-to-Site IPsec: Liste der Richtlinien

- *Blowfish* (128 Bit)
- *Twofish* (128 Bit)
- *Serpent* (128 Bit)

IKE-Authentifizierungsalgorithmus: Der Authentifizierungsalgorithmus legt fest, welcher Algorithmus verwendet wird, um die Intaktheit der IKE-Nachricht zu prüfen. Die folgenden Algorithmen werden unterstützt:

- *MD5* (128 Bit)
- *SHA* (160 Bit)
- *SHA-256* (256 Bit)
- *SHA-512* (512 Bit)

IKE-SA-Lebensdauer: Dieser Wert bestimmt die Zeitspanne in Sekunden, für die die IKE-SA (*Security Association*, dt. Sicherheitsverbindung) gültig ist und wann die nächste Schlüsselerneuerung stattfindet. Gültige Werte liegen zwischen 60 und 28800 Sekunden (8 Std.) möglich. Standardmäßig sind 7800 Sekunden (2 Std. 10 Min.) eingestellt.

IKE-DH-Gruppe: Während der Aushandlung einer Verbindung, gleichen die beiden Gegenstellen auch die aktuellen Schlüssel für die Datenverschlüsselung ab. Für die Generierung des Session Key nutzt IKE den *Diffie-Hellman*-(DH)-Algorithmus. Dieser Algorithmus generiert den Schlüssel per Zufallsprinzip basierend auf sogenannten *Pool Bits*. Die IKE-Gruppe gibt hauptsächlich Aufschluss über die Anzahl der Pool Bits. Je mehr Pool Bits, umso länger ist die zufällige Zahlenkette – je größer die Zahlenkette, umso schwerer kann der Diffie-Hellman-Algorithmus geknackt werden. Folglich bedeuten mehr Pool Bits höhere Sicherheit, was allerdings auch bedeutet, dass mehr CPU-Leistung für die Generierung benötigt wird. Die folgenden DH-Algorithmen werden unterstützt:

- Gruppe 1: MODP 768
- Gruppe 2: MODP 1024
- Gruppe 5: MODP 1536
- Gruppe 14: MODP 2048
- Gruppe 15: MODP 3072
- Gruppe 16: MODP 4096

Hinweis – Gruppe 1 (MODP 768) wird allgemein als sehr schwach eingestuft und wird hier nur aus Kompatibilitätsgründen unterstützt.

IPSec-Verschlüsselungsalgorithmus: Die gleichen Verschlüsselungsalgorithmen wie für IKE.

IPSec-Authentifizierungsalgorithmus: Die gleichen Verschlüsselungsalgorithmen wie für IKE.

IPSec-SA-Lebensdauer: Dieser Wert bestimmt die Zeitspanne in Sekunden, für die die IPSec-SA (*Security Association*, dt. Sicherheitsverbindung) gültig ist und wann die nächste Schlüsselerneuerung stattfindet. Gültige Werte liegen zwischen 60 und 86400 Sekunden (1 Tag) möglich. Standardmäßig sind 7800 Sekunden (2 Std. 10 Min.) eingestellt.

IPSec-PFS-Gruppe: *Perfect Forward Secrecy* (PFS) ist eine Eigenschaft von Verschlüsselungsverfahren, die sicherstellt, dass aus einem geknackten Schlüssel nicht auf vorhergehende oder nachfolgende Sitzungsschlüssel einer Kommunikationsverbindung geschlossen werden kann. Damit PFS besteht, darf der zum Schutz der IPSec-SA-Verbindung genutzte Schlüssel nicht von dem selben zufällig erzeugten Schlüsselungsmaterial hergeleitet

worden sein wie die Schlüssel für die IKE-SA-Verbindung. Daher initiiert PFS einen zweiten Diffie-Hellman-Schlüsselaustausch mit der Absicht, dass die ausgewählte DH-Gruppe für die IPSec-Verbindung einen neuen zufällig erzeugten Schlüssel erhält. Es werden die gleichen DH-Gruppen wie bei IKE unterstützt.

Hinweis – PFS ist nicht immer gänzlich kompatibel unter den verschiedenen Herstellern. Wenn Sie Probleme während der Aushandlung feststellen, schalten Sie diese Funktion aus.

Strikte Richtlinie: Wenn ein IPSec Gateway eine Anfrage hinsichtlich eines Verschlüsselungsalgorithmus' und der Verschlüsselungsstärke unternimmt, kann es vorkommen, dass das Gateway des Empfängers diese Anfrage akzeptiert, obwohl das nicht mit der entsprechenden IPSec-Richtlinie übereinstimmt. Wenn Sie diese Option wählen und der entfernte Endpunkt nicht exakt die von Ihnen festgelegten Parameter verwenden will, kommt keine IPSec-Verbindung zustande. Angenommen die IPSec-Richtlinie Ihres Sicherheitssystems verlangt AES-256-Verschlüsselung, wohingegen ein Road Warrior mit SSH-Sentinel sich mit AES-128 verbinden will – wenn die Option *Strikte Richtlinie* aktiviert ist, wird die Verbindung abgewiesen.

Hinweis – Die Komprimierungseinstellung wird durch die Aktivierung von der Option *Strikte Richtlinie* nicht erzwungen.

Komprimierung: Diese Option legt fest, ob IP-Pakete vor der Verschlüsselung mit dem *IP Payload Compression Protocol* (IPComp) komprimiert werden sollen. IPComp reduziert die Größe von IP-Paketen, indem es sie komprimiert, um die allgemeine Kommunikationsleistung zwischen einem Paar von kommunizierenden Rechnern oder Gateways zu erhöhen. Komprimierung ist standardmäßig ausgeschaltet.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die Richtlinie hinzu.

3. Klicken Sie *Speichern*.

Die neue IPSec-Richtlinie wird in der Liste *Richtlinien* angezeigt.

Um eine Richtlinie zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Lokaler RSA-Schlüssel

Bei der RSA-Authentifizierung werden zur Authentifizierung der VPN-Endpunkte RSA-Schlüssel verwendet. Die öffentlichen Schlüssel der Endpunkte werden manuell ausgetauscht, bevor die Verbindung aufgebaut wird. Wenn Sie diese Authentifizierungsmethode verwenden wollen, müssen Sie eine *VPN-ID* definieren und einen lokalen öffentlichen RSA-Schlüssel generieren. Dieser öffentliche RSA-Schlüssel der Firewall muss anschließend den IPSec-Geräten der Gegenstelle zugänglich gemacht werden, die IPSec-RSA-Authentifizierung für Astaro Security Gateway verwenden.

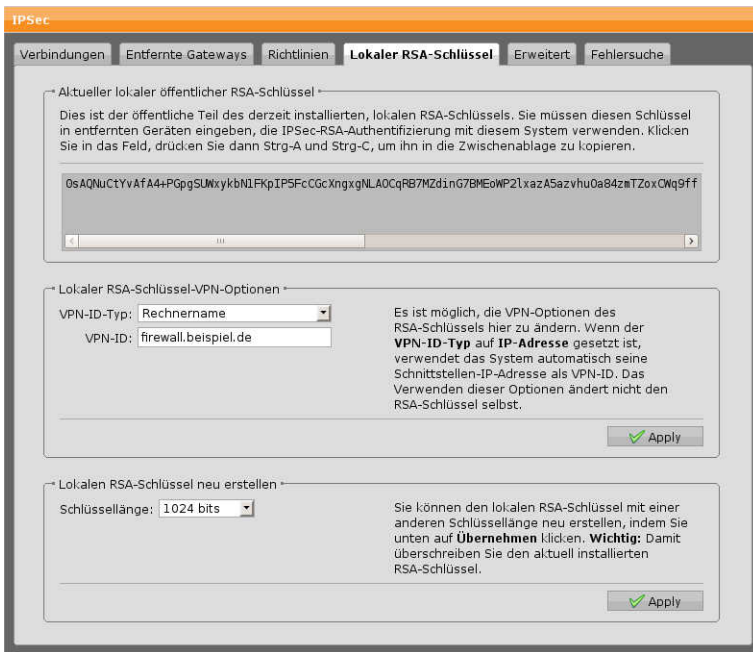


Figure 14.4 Site-to-Site IPSec: Konfiguration des lokalen RSA-Schlüssels

Aktueller lokaler öffentlicher RSA-Schlüssel: In diesem Fenster wird der öffentliche Teil des aktuell installierten RSA-Schlüsselpaares angezeigt. Um den Schlüssel in die Zwischenablage zu kopieren, klicken Sie in das Feld, drücken Sie CTRL-a und anschließend CTRL-c.

Lokaler RSA-Schlüssel-VPN-Optionen: Wählen Sie den VPN-ID-Typ entsprechend Ihren Anforderungen aus. Der Rechnername der Firewall ist als VPN-ID voreingestellt. Wenn Sie eine statische IP-Adresse als VPN-Endpunkt haben,

wählen Sie *IP-Adresse*. Verwenden Sie alternativ eine E-Mail-Adresse als VPN-ID für mobile IPSec-Road-Warriors.

- **Rechnername:** Standardeinstellung. Der Rechnername der Firewall. Sie können jedoch auch einen anderen Rechnernamen eingeben.
- **E-Mail-Adresse:** Die E-Mail-Adresse des Admin-Kontos der Firewall ist vor-eingestellt. Sie können aber eine beliebige andere E-Mail-Adresse eintragen.
- **IP-Adresse:** Die IP-Adresse der externen Schnittstelle der Firewall.

Klicken Sie *Übernehmen*, um Ihre Einstellungen zu speichern. Änderungen haben keine Auswirkungen auf den RSA-Schlüssel.

Lokalen RSA-Schlüssel neu erstellen: Um einen neuen RSA-Schlüssel zu generieren, wählen Sie die gewünschte Schlüssellänge aus und klicken auf die Schaltfläche *Übernehmen*. Anschließend wird der Generierungsprozess gestartet, der – abhängig von der Schlüssellänge und der verwendeten Hardware – zwischen ein paar Minuten und zwei Stunden benötigen kann. Die Schlüssellänge ist ein Maß für die Anzahl der Schlüssel, die bei einer Chiffre möglich sind. Die Länge wird üblicherweise in Bits angegeben. Die folgenden Schlüssellängen werden unterstützt:

- 1024 Bits
- 2048 Bits
- 4096 Bits

Sobald der neue RSA-Schlüssel generiert wurde, wird der zugehörige öffentliche Schlüssel im Feld *Aktueller lokaler öffentlicher RSA-Schlüssel* angezeigt. Das Generieren eines neuen RSA-Schlüssel überschreibt den alten Schlüssel.

Erweitert

Auf der Registerkarte *Site-to-Site-VPN >> IPSec >> Erweitert* können Sie die erweiterten Einstellungen für IPSec-VPN durchführen. Abhängig von Ihrer bevorzugter Authentifizierungsmethode können Sie unter Anderem das lokale Zertifikat (für X.509-Authentifizierung) und den lokalen RSA-Schlüssel (für RSA-Authentifizierung) festlegen. Diese Einstellungen sollten nur von erfahrenen Benutzern durchgeführt werden.

IPsec

Verbindungen | Entfernte Gateways | Richtlinien | Lokaler RSA-Schlüssel | **Erweitert** | Fehlersuche

Lokales X.509-Zertifikat

Local X509 Cert

Bitte wählen Sie das lokale X.509-Zertifikat aus, das standardmäßig für IPsec-Verbindungen verwendet wird.

✓ Apply

Dead Peer Detection (DPD)

☒ Dead Peer Detection verwenden

Wenn diese Option aktiviert ist, versucht das System, nicht antwortende (offline) entfernte Systeme zu erkennen.

✓ Apply

NAT-Traversal (NAT-T)

☒ NAT-Traversal verwenden

NAT-Traversal Keep-Alive: 60 Sekunden

Durch NAT-Traversal kann IPsec-Verkehr Upstream-Systeme passieren, die NAT (Network Address Translation) verwenden.

✓ Apply

CRL-Handhabung

☐ Automatische Abholung

☐ Strikte Richtlinie

Diese Einstellungen definieren, wie Zertifikat-Sperlisten (Certificate Renovation Lists) gehandhabt werden. Bei aktivierter **Automatischer Abholung** versucht das System automatisch, CRLs von entfernten Sites einzuholen.

✓ Apply

Sonstige Einstellungen

☐ ToS-Wert (Type of Service) kopieren

☒ Pfad-MTU-Erkennung zulassen

MTU: 1420 Bytes

Sie können auswählen, ob ToS-Werte in die eingebetteten Pakete kopiert werden sollen und Pfad-MTU-Erkennung zugelassen wird.

✓ Apply

Figure 14.5 Site-to-Site IPsec: Konfiguration der erweiterten Einstellungen

Lokales X.509-Zertifikat

Bei der X.509-Authentifizierung werden Zertifikate verwendet, um die öffentlichen Schlüssel der VPN-Endpunkte zu überprüfen. Wenn Sie diese Authentifizierungsmethode verwenden wollen, müssen Sie im Abschnitt *Lokales X.509-Zertifikat* ein lokales Zertifikat aus der Auswahlliste wählen. Das ausgewählte Zertifikat bzw. Schlüssel wird anschließend dafür genutzt, um die Firewall gegenüber Gegenstellen zu authentifizieren, falls X.509-Authentifizierung ausgewählt ist.

Sie können nur Zertifikate auswählen, für die auch der zugehörige private Schlüssel vorhanden ist, andere Zertifikate sind in der Auswahlliste nicht verfügbar.

Wenn keine Zertifikate zur Auswahl angezeigt werden, müssen Sie zunächst eines im Menü *Zertifikatverwaltung* hinzufügen, entweder indem Sie ein neues erzeugen oder indem Sie eines über die Upload-Funktion importieren.

Nachdem Sie das Zertifikat ausgewählt haben, geben Sie das Kennwort ein, mit dem der private Schlüssel geschützt ist. Während des Speichervorgangs wird das Kennwort verifiziert und eine Fehlermeldung angezeigt, falls das Kennwort nicht zum verschlüsselten Schlüssel passt.

Sobald ein aktiver Schlüssel oder Zertifikat ausgewählt ist, wird er im Abschnitt *Lokales X.509-Zertifikat* angezeigt.

Dead Peer Detection (DPD)

Dead Peer Detection verwenden: Die IPSec-Verbindung wird automatisch beendet, wenn das VPN-Gateway oder der Client auf der Gegenseite nicht erreichbar ist. Bei Verbindungen mit statischen Endpunkten wird der Tunnel nach einem Ausfall automatisch neu ausgehandelt. Für Verbindungen mit dynamischen Endpunkten wird für eine neue Aushandlung des Tunnels die Anfrage seitens der Gegenstelle benötigt. In der Regel ist diese Funktion betriebssicher und kann immer eingeschaltet bleiben. Die IPSec-Partner bestimmen automatisch, ob die Gegenstelle Dead Peer Detection unterstützt oder nicht, und verwenden den normalen Modus falls nötig.

NAT-Traversal (NAT-T)

NAT-Traversal verwenden: Wählen Sie diese Option, um zu ermöglichen, dass IPSec-Verkehr Upstream-Systeme passieren kann, die *Network Address Translation* (NAT, dt. Netzwerkadressumsetzung) verwenden. Zusätzlich können Sie das Intervall für die Aufrechterhaltung (engl. *keep-alive*) für NAT-Traversal festlegen. Klicken Sie Übernehmen, um Ihre Einstellungen zu speichern.

CRL-Handhabung

Es sind Situationen denkbar, in denen ein Zertifikatsaussteller noch während der Gültigkeitsdauer eines Zertifikats die darin gegebene Bestätigung für ungültig erklären möchte, z. B. weil zwischenzeitlich bekannt wurde, dass das Zertifikat vom Zertifikatnehmer unter Angabe falscher Daten (Name usw.) erschlichen wurde oder weil der zum zertifizierten öffentlichen Schlüssel gehörende private Schlüssel einem Angreifer in die Hände gefallen ist. Zu diesem Zweck werden sogenannte Zertifikatsperrlisten (CRLs, engl. *Certificate Revocation Lists*) verwendet. Diese enthalten üblicherweise die Seriennummern derjenigen Zertifikate einer Zertifizierungsinstanz, die für ungültig erklärt werden und deren regulärer Gültigkeitszeitraum noch nicht abgelaufen ist.

Nach Ablauf dieses Zeitraums besitzt das Zertifikat in jedem Fall keine Gültigkeit mehr und muss daher auch nicht weiter auf der Zertifikatsperrliste geführt werden.

Automatische Abholung: Mit der Funktion *Automatische Abholung* wird die

CRL automatisch über die URL abgeholt, die im Partnerzertifikat angegeben ist, via HTTP, Anonymous FTP oder LDAP Version 3. Die CRL kann auf Anfrage heruntergeladen, abgespeichert und aktualisiert werden, sobald der Gültigkeitszeitraum abgelaufen ist. Wenn Sie diese Funktion nutzen, achten Sie darauf, dass die Paketfilterregeln so gesetzt sind, dass auf den CRL-Distributionsserver zugegriffen werden kann.

Strikte Richtlinie: Wenn Sie diese Option auswählen, werden alle Partnerzertifikate ohne eine zugehörige CRL zurückgewiesen.

Sonstige Einstellungen

ToS-Wert (Type of Service) kopieren: Type-of-Service-Bits (TOS) sind einige Vier-Bit-Flags im IP-Header. Die Bits werden *Type-of-Service-Bits* genannt, da sie es der übertragenden Anwendung ermöglichen, dem Netzwerk mitzuteilen, welche Art von Dienstqualität benötigt wird. Die folgenden Dienstqualitätsarten sind: * Minimale Verzögerung (Binärzahl: 1000)

- maximaler Durchsatz (Binärzahl: 0100)
- maximale Zuverlässigkeit (Binärzahl: 0010)
- minimale Kosten (Binärzahl: 0001)
- normaler Dienst (Binärzahl: 0000)

Mit dieser Funktion wird der Inhalt des *Type-of-Service*-Feldes in das verschlüsselte Datenpaket kopiert, so dass der IPSec-Datenverkehr entsprechend seiner Priorität geroutet werden kann.

Pfad-MTU-Erkennung zulassen: Die gesendeten IP-Datenpakete sollten so groß sein, dass sie gerade noch ohne Fragmentierung entlang der Strecke zum Ziel transportiert werden können. Diese maximale Datengröße wird als *Path Maximum Transmission Unit* (PMTU) bezeichnet. Zu große Datenpakete werden von den Routern auf der Strecke verworfen, wenn diese Pakete ohne Fragmentierung nicht weitergeleitet werden können. An die Absender werden dann ICMP-Pakete mit der Nachricht *ICMP Destination Unreachable* (dt. ICMP-Ziel nicht erreichbar) mit einem Code der bedeutet „Fragmentierung benötigt und DF gesetzt“ gesendet. Aufgrund dieser Nachricht setzt der Quellrechner seinen angenommenen PMTU-Wert für die Strecke herab.

MTU: Tragen Sie in das Eingabefeld den Wert für die *Maximum Transmission Unit* (MTU) ein. Der voreingestellte MTU-Wert ist 1420 Byte.

Fehlersuche

Auf der Registerkarte *IPSec >> Fehlersuche* können Sie die Optionen für die IKE-Fehlersuche konfigurieren. Mit Hilfe der Auswahlkästchen legen Sie fest,

für welche Arten von IKE-Nachrichten zusätzliche Informationen in das Fehlerprotokoll geschrieben werden. Die folgenden Flags können protokolliert werden:

- **Control:** Kontrollnachrichten zum IKE-Status
- **Emitting:** Inhalte von ausgehenden IKE-Nachrichten
- **Parsing:** Inhalte von eingehenden IKE-Nachrichten
- **Raw:** Nachrichten werden im Rohformat angezeigt
- **Crypt:** Verschlüsselungs- und Entschlüsselungsoperationen

SSL

Site-to-Site-VPN-Tunnel können über eine SSL-Verbindung aufgebaut werden. SSL-VPN-Verbindungen benutzen dabei eindeutige Rollen: Die Tunnelendpunkte agieren entweder als Client oder als Server. Es ist immer der Client, der die Verbindung initiiert, während der Server auf Client-Anfragen antwortet. Denken Sie daran, dass hierbei der Unterschied zu IPSec liegt, wo beide Endpunkte normalerweise eine Verbindung initiieren können.

Hinweis – Wenn Sie Probleme haben, eine Verbindung aufzubauen und der HTTP-Proxy im Transparenzmodus arbeitet, überprüfen Sie, ob SSL-Scanning aktiviert ist. Wenn das der Fall ist, stellen Sie sicher, dass der Zielrechner der VPN-Verbindung zu den *Transparenzmodus-Ausnahmen* unter *Web Security* >> *HTTP/S* >> *Erweitert* hinzugefügt wurde.

Verbindungen

Um einen SSL-VPN-Site-to-Site-Tunnel anzulegen, ist es entscheidend, zuerst die Serverkonfiguration anzulegen. Die Konfiguration des Clients muss immer erst der zweite Schritt sein.

Um eine Serverkonfiguration anzulegen, gehen Sie folgendermaßen vor:

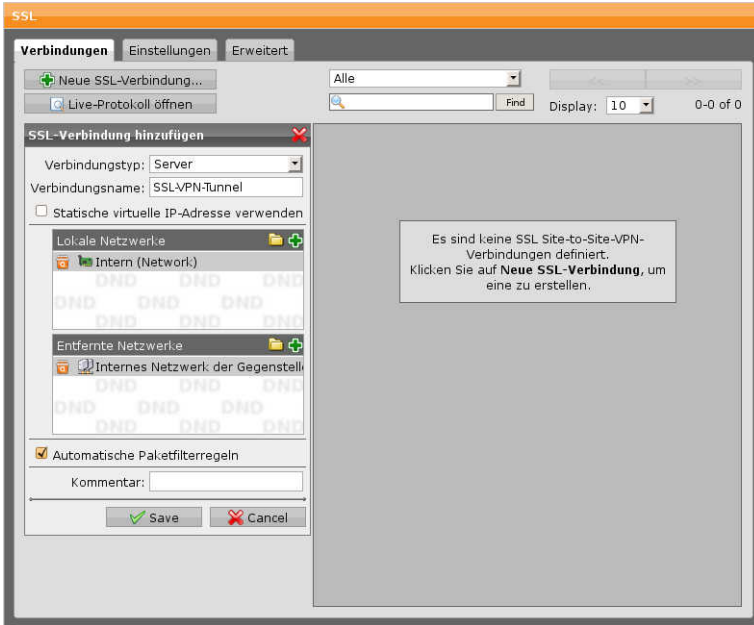


Figure 14.6 Site-to-Site SSL: Konfiguration der Serververbindung

1. Klicken Sie auf der Registerkarte **Verbindungen** auf **Neue SSL-Verbindung**.

Das Dialogfenster *SSL-Verbindung hinzufügen* wird geöffnet.

2. Nehmen Sie die folgenden Einstellungen vor:

Verbindungstyp: Wählen Sie *Server* aus der Auswahlliste.

Verbindungsname: Geben Sie einen aussagekräftigen Name für die Verbindung ein.

Statische virtuelle IP-Adresse verwenden (optional): Wählen Sie diese Option nur, wenn der IP-Adressenpool nicht mit der Netzwerkumgebung des Clients kompatibel ist: Standardmäßig erhalten Clients eine IP-Adresse aus dem *Virtuellen IP-Pool* (konfigurierbar auf der Registerkarte *Einstellungen*). Dennoch kann es in Ausnahmefällen passieren, dass solch eine IP-Adresse auf dem Rechner des Clients bereits in Benutzung ist. Geben Sie in diesem Fall eine passende IP-Adresse in das Feld *Statische Peer-IP* ein, welche daraufhin dem Client während des Tunnelaufbaus zugewiesen wird.

Lokale Netzwerke: Fügen Sie ein oder mehrere Netzwerke hinzu, die für den Fernzugriff zugelassen sein sollen.

Entfernte Netzwerke: Fügen Sie ein oder mehrere Netzwerke der Gegenstelle hinzu, die sich mit dem/den lokalen Netzwerk(en) verbinden dürfen.

Hinweis – Sie können die *lokalen Netzwerke* und die *entfernten Netzwerke* auch später noch konfigurieren, ohne dass Sie den Client neu konfigurieren müssten.

Automatische Paketfilterregeln (optional): Wenn Sie diese Option wählen, wird das Sicherheitssystem automatisch den Zugriff auf die gewählten lokalen Netzwerke für alle SSL-VPN-Clients erlauben.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die SSL-Verbindung hinzu.

3. **Klicken Sie *Speichern*.**

Die neue SSL-Serververbindung wird auf der Liste *Verbindungen* angezeigt.

4. **Laden Sie die Konfigurationsdatei herunter.**

Klicken Sie auf die Schaltfläche *Download*, die sich im Feld der neuen SSL-Serververbindung befindet, um die Client-Konfigurationsdatei für diese Verbindung herunterzuladen.

Konfigurationsdatei verschlüsseln: Es wird empfohlen, die Konfigurationsdatei aus Sicherheitsgründen zu verschlüsseln. Geben Sie ein Kennwort ein und bestätigen Sie es.

Diese Datei wird vom Administrator der Client-Seite benötigt, um in der Lage zu sein, den Client-Endpunkt des Tunnels zu konfigurieren.

Der nächste Schritt ist die Client-Konfiguration, die auf Client-Seite stattfinden muss und *nicht* auf Serverseite. Stellen Sie sicher, dass die Client-Konfigurationsdatei bereitliegt.

Um eine Client-Konfiguration anzulegen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Verbindungen* auf *Neue SSL-Verbindung*.**

Das Dialogfenster *SSL-Verbindung hinzufügen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Verbindungstyp: Wählen Sie *Client* aus der Auswahlliste.

Verbindungsname: Geben Sie einen aussagekräftigen Name für die Verbindung ein.

Konfigurationsdatei: Klicken Sie auf das Ordnersymbol, wechseln Sie zur Client-Konfigurationsdatei und klicken Sie *Save*.

Kennwort (optional): Wenn die Datei verschlüsselt ist, geben Sie das Kennwort ein.

HTTP-Proxy-Server verwenden (optional): Wählen Sie diese Option,

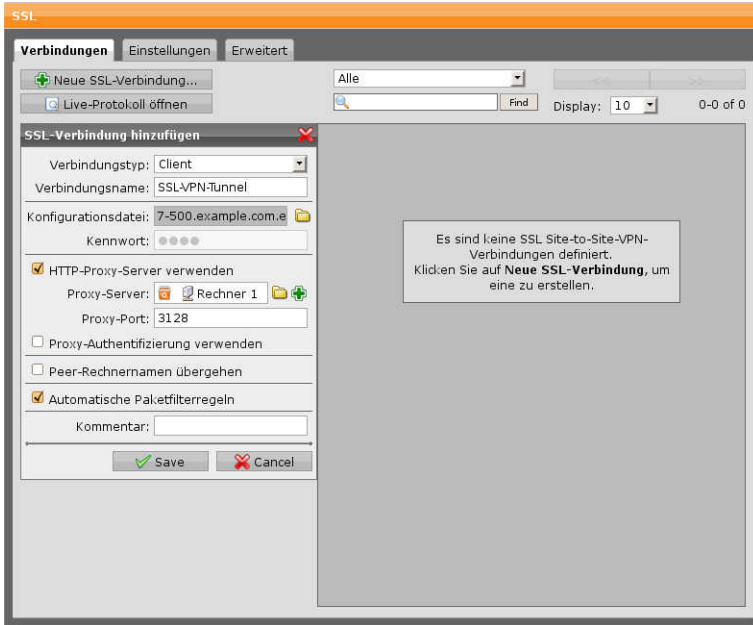


Figure 14.7 Site-to-Site SSL: Konfiguration der Clientverbindung

wenn sich der Client hinter einem Proxy befindet, und geben Sie die Einstellungen für den Proxy ein.

- **Proxy-Authentifizierung verwenden (optional):** Wählen Sie diese Option, wenn sich der Client am Proxy authentifizieren muss, und geben Sie Benutzernamen und Kennwort ein.

Peer-Rechnernamen übergehen: Wählen Sie diese Option und geben Sie einen Rechnernamen ein, wenn der reguläre Rechnername des Serversystems (oder sein DynDNS-Rechnername) nicht vom Clientrechner aufgelöst werden kann.

Automatische Paketfilterregeln (optional): Wenn Sie diese Option aktivieren, wird das Sicherheitssystem automatisch Verkehr zwischen Rechnern der zum Tunnel gehörenden lokalen und entfernten Netzwerke zulassen.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die SSL-Verbindung hinzu.

3. Klicken Sie *Speichern*.

Die neue SSL-VPN-Client-Verbindung wird in der Liste *Verbindungen* angezeigt.

Um eine SSL-Server oder -Clientverbindung zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Klicken Sie auf den Menüpunkt *Site-to-Site-VPN*, um den Status der SSL-VPN-Verbindung auf der Übersichtsseite zu sehen. Die Statusampel dort wird grün, wenn die Verbindung aufgebaut ist. Dann werden auch Informationen zu den miteinander verbundenen Subnetzen beider Seiten des Tunnel angezeigt.

Einstellungen

Auf der Registerkarte *SSL >> Einstellungen* können Sie die Grundeinstellungen für SSL-VPN-Serververbindungen konfigurieren.

Hinweis – Diese Registerkarte ist identisch für *Site-to-Site-VPN >> SSL* und *Fernzugriff >> SSL*. Hier vorgenommene Änderungen wirken sich auf beide SSL-Konfigurationen aus.

The screenshot shows the 'Einstellungen' (Settings) tab for SSL in the Site-to-Site-VPN configuration. The window is titled 'SSL' and has three tabs: 'Verbindungen', 'Einstellungen' (selected), and 'Erweitert'.

Servereinstellungen

- Protokoll: TCP (dropdown menu)
- Port: 443 (text field)
- Rechnernamen übergehen: (text field)

Wählen Sie das Netzwerk-**Protokoll** und den **Port**, den alle SSL-VPN-Clients verwenden müssen. In der Standardeinstellung ist dies TCP-Port 443. Beachten Sie, dass Port 10443 und der vom WebAdmin verwendete Port nicht verwendet werden können. Bei allen SSL-VPN-Verbindungen ignoriert die Einstellung **Rechnernamen übergehen** die integrierte Voreinstellung, den konfigurierten *DynDNS-Namen* dem System-**Rechnernamen** vorzuziehen.

Virtueller IP-Pool

- Pool-Netzwerk: (icon) VPN Pool (SSL) (dropdown menu)

Virtuelle IP-Adressen für Peers werden aus diesem **IP-Pool** ausgewählt. Bei Konflikten kann dieser geändert oder ersetzt werden. Bei SSL-Site-to-Site-Verbindungen ist es möglich, einem Peer eine statische virtuelle IP-Adresse zuzuweisen, die diesen Pool dann umgeht.

Doppelte CN

- ☒ Mehrere gleichzeitige Verbindungen pro Benutzer zulassen

Markieren Sie dieses Auswahlkästchen, um doppelte allgemeine Namen (CN) in verschiedenen SSL-VPN-Sitzungen zu erlauben. So können Benutzer mehrere SSL-VPN-Sitzungen gleichzeitig auf unterschiedlichen Rechnern öffnen. Andernfalls wird nur eine SSL-VPN-Sitzung pro Benutzer zugelassen.

Figure 14.8 Site-to-Site-VPN SSL: Konfiguration der Einstellungen

Servereinstellungen

Sie können die folgenden Einstellung für die SSL-VPN-Verbindung vornehmen:

- **Protokoll:** Wählen Sie das Protokoll aus, das verwendet werden soll. Sie können entweder *TCP* oder *UDP* auswählen.
- **Port:** Sie können den Port ändern. Der Standardport ist 443. Sie können jedoch nicht den Port 10443, den ACC-Gateway-Manager-Port 4422 oder den Port der WebAdmin-Schnittstelle verwenden.
- **Rechnernamen übergehen:** Der Wert im Feld *Rechnernamen übergehen* wird als Zielrechnername für Client-VPN-Verbindungen verwendet und ist standardmäßig der Rechnername von der Firewall. Ändern Sie den vor-eingestellten Wert nur, wenn der reguläre Rechnername (oder DynDNS-Rechnername) nicht unter diesem Name vom Internet aus erreichbar ist.

Virtueller IP-Pool

Pool-Netzwerk: Das ist der virtuelle IP-Adressenpool, der verwendet wird, um IP-Adressen aus einem bestimmten IP-Adressbereich SSL-Clients zuzuweisen. Standardmäßig ist *VPN Pool (SSL)* ausgewählt. Falls Sie einen anderen Adressenpool auswählen, darf die Netzmaske nicht größer als 29 Bits sein, da OpenVPN nicht mit Adressenpools umgehen kann, deren Netzmaske /30, /31 oder /32 ist.

Doppelte CN

Wählen Sie *Mehrere gleichzeitige Verbindungen pro Benutzer zulassen*, wenn Sie zulassen wollen, dass Ihre Benutzer sich von verschiedenen IP-Adressen aus zur gleichen Zeit verbinden können. Wenn diese Option deaktiviert ist, ist nur eine gleichzeitige SSL-VPN-Verbindung pro Benutzer erlaubt.

Erweitert

Auf der Registerkarte *SSL >> Erweitert* können Sie diverse erweiterte Serveroptionen konfigurieren, wie z. B. Einstellungen zur Kryptografie, zur Komprimierung und zur Fehlersuche.

Hinweis – Diese Registerkarte ist identisch für *Site-to-Site-VPN >> SSL* und *Fernzugriff >> SSL*. Hier vorgenommene Änderungen wirken sich auf beide SSL-Konfigurationen aus.

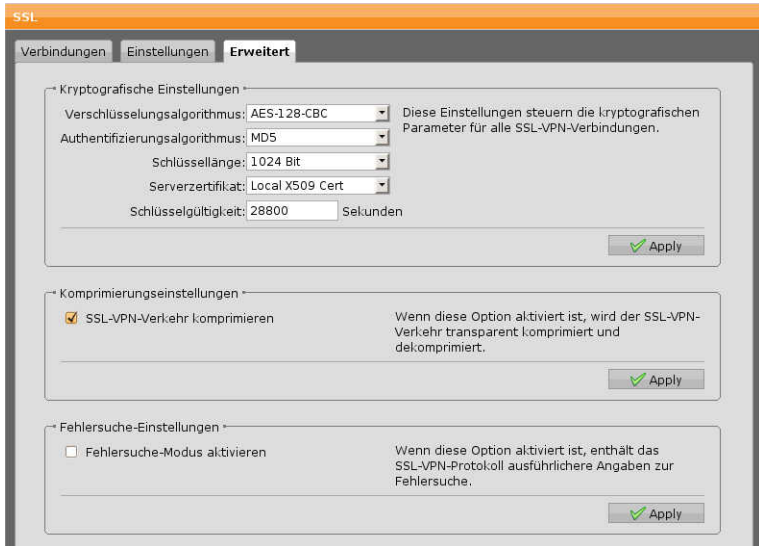


Figure 14.9 Site-to-Site-VPN SSL: Konfiguration der erweiterten Einstellungen

Kryptografische Einstellungen

Diese Einstellungen kontrollieren die Verschlüsselungsparameter für alle SSL-VPN-Fernzugriff-Clients:

- **Verschlüsselungsalgorithmus:** Der Verschlüsselungsalgorithmus legt den Algorithmus fest, der für die Verschlüsselung der für die Daten verwendet wird, die durch den Tunnel gesendet werden. Die folgenden Algorithmen werden unterstützt und sie sind alle im CBC-Modus (*Cipher Block Chaining*):
 - *DES-EDE3-CBC*
 - *AES-128-CBC* (128 bit)
 - *AES-192-CBC* (192 bit)
 - *AES-256-CBC* (256 bit)
 - *BF-CBC* (Blowfish (128 bit))
- **Authentifizierungsalgorithmus:** Der Authentifizierungsalgorithmus legt den Algorithmus fest, der für die Integritätsprüfung der Daten verwendet

wird, die durch den VPN-Tunnel gesendet werden. Unterstützte Algorithmen sind:

- MD5 (128 bit)
- SHA-1 (160 bit)
- **Schlüssellänge:** Die Schlüssellänge ist die Länge des Diffie-Hellman-Schlüsselaustauschs. Je länger der Schlüssel ist, desto sicherer sind die symmetrischen Schlüssel. Die Länge wird in Bits angegeben. Sie können zwischen einer Schlüssellänge von 1024 und 2048 Bits wählen.
- **Serverzertifikat:** Wählen Sie ein lokales SSL-Zertifikat, das der SSL-VPN-Server verwenden soll, um sich gegenüber Clients zu identifizieren.
- **Schlüsselgültigkeit:** Geben Sie einen Zeitpunkt an, nach dem der Schlüssel abläuft. Der Standard ist 28.800 Sekunden.

Komprimierungseinstellungen

SSL-VPN-Verkehr komprimieren: Wenn diese Option aktiviert ist, werden alle Daten, die durch SSL-VPN-Tunnel geschickt werden, vor der Verschlüsselung komprimiert.

Fehlersuche-Einstellungen

Fehlersuche-Modus aktivieren: Wenn Sie den Fehlersuche-Modus aktivieren, wird die SSL-VPN-Protokolldatei zusätzliche Informationen enthalten, die nützlich für die Fehlersuche sind.

Zertifikatverwaltung

Das Menü *Site-to-Site-VPN >> Zertifikatverwaltung* ist der zentrale Ort, wo alles, was mit Zertifikaten auf Astaro Security Gateway zu tun hat, verwaltet wird. Das schließt unter Anderem das Anlegen oder Importieren von X.509-Zertifikaten ebenso ein wie das Hochladen sogenannter Zertifikatsperrlisten (CRLs, engl. *Certificate Revocation Lists*).

Zertifikate

Auf der Registerkarte *Site-to-Site-VPN >> Zertifikatverwaltung >> Zertifikate* können Sie öffentliche Schlüssel-Zertifikate im X.509-Standard erstellen oder importieren. Solche Zertifikate sind digital signierte Bescheinigungen, die üblicherweise von einer Zertifizierungsstelle (CA, *Certificate Authority*) ausgestellt

werden und einen öffentlichen Schlüssel mit einem bestimmten *Distinguished Name* (DN) in X.500-Schreibweise verknüpfen.

Alle Zertifikate, die Sie auf dieser Registerkarte erzeugen, werden von der Zertifizierungsstelle (CA) selbst signiert. Diese CA wurde während der allerersten Anmeldung automatisch angelegt mit den Informationen, die Sie für die Anmeldung angegeben haben.

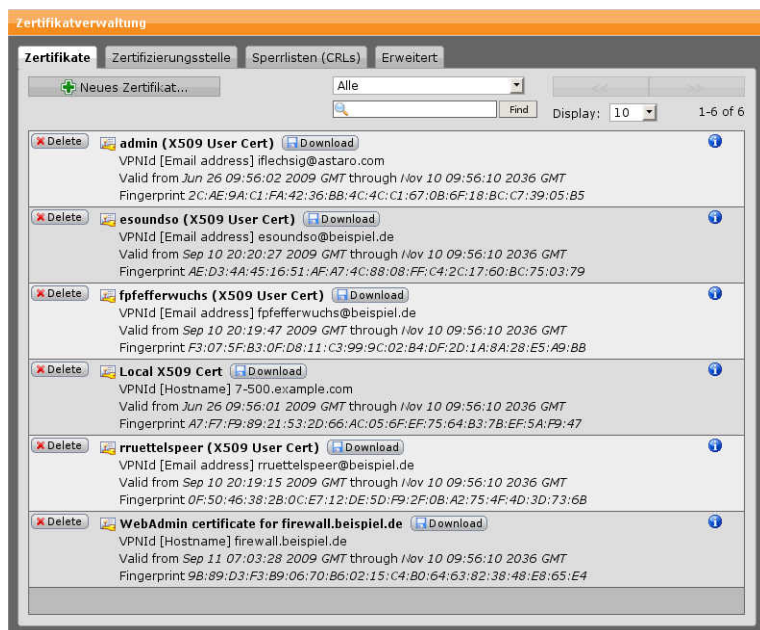


Figure 14.10 Site-to-Site-VPN: Zertifikatliste

Um ein Zertifikat neu zu generieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Zertifikate* auf *Neues Zertifikat*.**
Das Dialogfenster *Zertifikat hinzufügen* wird geöffnet.
2. **Nehmen Sie die folgenden Einstellungen vor:**
Name: Geben Sie einen aussagekräftigen Name für dieses Zertifikat ein.
Methode: Um ein Zertifikat zu erstellen, wählen Sie *Generieren* aus (weitere Informationen zum Hochladen von Zertifikaten finden Sie weiter unten). Geben Sie die folgenden Informationen an:
 - **VPN-ID-Typ:** Legen Sie eine einzigartige Identifikation (engl. *identifier*) für das Zertifikat fest. Die folgenden Identifikationsarten sind verfügbar:

- E-Mail-Adresse
 - Rechnername
 - IP-Adresse
 - Distinguished Name
- **VPN-ID:** Tragen Sie abhängig von der gewählten Identifikationsart den passenden Wert in das Feld ein. Beispiel: Wenn Sie *IP-Adresse* aus der Liste *VPN-ID-Typ* gewählt haben, geben Sie eine IP-Adresse in dieses Textfeld ein. Beachten Sie, dass dieses Textfeld nicht angezeigt wird, wenn Sie *Distinguished Name* aus der Liste *VPN-ID-Typ* gewählt haben. Tragen Sie die Informationen zum Zertifikatsinhaber in die Textfelder *Land* bis *E-Mail* ein. Diese Informationen werden dazu verwendet, um den *Distinguished Name* zu erstellen, das heißt den Namen der Instanz, deren öffentlichen Schlüssel das Zertifikat identifiziert. Dieser Name enthält eine Menge an persönlichen Informationen im X.500-Standard, weswegen davon ausgegangen wird, dass dieser Name im gesamten Internet einzigartig ist. Wenn das Zertifikat für eine Road-Warrior-Verbindung benötigt wird, geben Sie den Namen des Benutzers im Feld *Allgemeiner Name* ein. Wenn das Zertifikat für einen Rechner ist, geben Sie einen Rechnernamen ein.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über das Zertifikat hinzu.

3. Klicken Sie *Speichern*.

Das Zertifikat wird in der Liste *Zertifikate* angezeigt.

Um ein Zertifikat zu löschen, klicken Sie auf die Schaltfläche *Delete* des entsprechenden Zertifikats.

Alternativ, um ein Zertifikat hochzuladen (zu importieren), gehen Sie folgendermaßen vor:

1. Klicken Sie auf der Registerkarte *Zertifikate* auf *Neues Zertifikat*.

Das Dialogfenster *Zertifikat hinzufügen* wird geöffnet.

2. Nehmen Sie die folgenden Einstellungen vor:

Name: Geben Sie einen aussagekräftigen Name für dieses Zertifikat ein.

Methode: Um ein Zertifikat zu importieren wählen Sie *Hochladen* aus.

Dateityp: Wählen Sie den Dateityp des Zertifikats aus. Sie können Zertifikate der folgenden Dateitypen hochladen:

- **PKCS#12-Container:** PKCS bezieht sich auf eine Gruppe von *Public Key Cryptography Standards* (dt. etwa *Standards für Kryptografie öffentlicher Schlüssel*), die von den *RSA Laboratories* entwickelt und veröffentlicht wurden. Das Dateiformat PKCS#12 wird geheimhin dafür benutzt, private Schlüssel mit dem zugehörigen öffentlichen Schlüsselzertifikat zu speichern und mit einem Kennwort zu schützen. Sie müssen diese Container-Kennwort kennen, um Dateien in diesem Format hochladen zu können (geben Sie das Kennwort ein zweites Mal zur Bestätigung ein).
- **PEM:** Ein Basis64-kodiertes Format (*Privacy Enhanced Mail*), das kein Kennwort erfordert.

Datei: Klicken Sie auf das Ordnersymbol und wählen Sie die Datei aus, die hochgeladen werden soll.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über das Zertifikat hinzu.

3. Klicken Sie **Speichern**.

Das Zertifikat wird in der Liste *Zertifikate* angezeigt.

Um ein Zertifikat zu löschen, klicken Sie auf die Schaltfläche *Delete* des entsprechenden Zertifikats.

Sie können das Zertifikat entweder im PKCS#12- oder PEM-Format herunterladen. Die PEM-Datei enthält nur das Zertifikat selbst, wohingegen die PKCS#12-Datei auch noch den privaten Schlüssel sowie das CA-Zertifikat enthält, mit dem das Zertifikat signiert wurde.

Hinweis – Um Problemen beim Herunterladen von Dateien mit dem Internet Explorer 6 vorzubeugen, fügen Sie die URL der Firewall (z.B. <https://192.168.2.100>) und des Benutzerportals (z.B. <https://192.168.2.100>) den *Vertrauenswürdigen Sites* hinzu. Beim Internet Explorer 6 befinden sich diese Einstellungen im Menü *Extras >> Internetoptionen >> Sicherheit*. Beim Internet Explorer 7 aktivieren Sie zusätzlich im Fenster *Sicherheitseinstellungen* die Funktion *Automatische Eingabeaufforderung für Dateidownloads*.

Zertifizierungsstelle

Auf der Registerkarte *Site-to-Site-VPN >> Zertifikatverwaltung >> Zertifizierungsstelle* können Sie neue Zertifizierungsstellen importieren. Eine Zertifizie-

ungsstelle (CA, engl. *Certificate Authority*) ist eine Instanz, die digitale Zertifikate für die Benutzung durch andere Parteien ausstellt. Eine CA attestiert, dass der im Zertifikat enthaltene öffentliche Schlüssel zur der Person, Organisation, Rechner oder anderen Instanz gehört, die im Zertifikat aufgeführt ist. Dies wird erreicht, indem bei der Signierungsanfrage das Zertifikat mit dem privaten Schlüssel des Zertifikats der CA signiert wird. Solch eine CA wird deshalb auch als Signierungs-CA bezeichnet.

Auf diesem Sicherheitssystem wurde die Signierungs-CA automatisch während der ersten Anmeldung am System generiert, wobei die angegebenen Informationen verwendet wurden. Dadurch sind alle Zertifikate, die Sie auf der Registerkarte *Zertifikate* erzeugen, selbst-signierte Zertifikate, das bedeutet, dass der Aussteller und der Inhaber identisch sind. Alternativ können Sie jedoch eine Signierungs-CA eines Drittanbieters importieren. Darüber hinaus können Sie auch andere CA-Zertifikate verwenden, deren private Schlüssel unbekannt sind, um die Authentizität eines Rechners oder Benutzers zu überprüfen, der versucht, sich über IPSec zu verbinden. Diese Zertifikate wiederum werden als Verifizierungs-CAs bezeichnet und könne auch auf dieser Registerkarte importiert werden.

Wichtiger Hinweis – Auf dem Sicherheitssystem können mehrere Verifizierungs-CAs vorhanden sein, allerdings nur eine Signierungs-CA. Wenn Sie also eine neue Signierungs-CA hochladen, wird die zuvor installierte Signierungs-CA automatisch in eine Verifizierungs-CA umgewandelt.



Figure 14.11 Site-to-Site-VPN: Liste der Zertifizierungsstellen

Um eine Verifizierungs-CA zu importieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Zertifizierungsstelle* auf *CA importieren*.**
Das Dialogfenster *CA importieren* wird geöffnet.
2. **Nehmen Sie die folgenden Einstellungen vor:**
Name: Geben Sie einen aussagekräftigen Name für diese CA ein.

Typ: Wählen Sie den CA-Typ, den Sie importieren werden. Sie können zwischen Verifizierungs-CA und Signierungs-CA wählen. Eine Verifizierungs-CA muss im PEM-Format vorliegen, wohingegen eine Signierungs-CA im PKCS#12-Format vorliegen muss.

CA-Zertifikat: Klicken Sie auf das Ordner-Symbol und wählen Sie die zu importierende Datei aus. Wenn Sie eine neue Signierungs-CA hochladen, beachten Sie, dass Sie das Kennwort eingeben müssen mit dem der PKCS#12-Container gesichert wurde.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die CA hinzu.

3. Klicken Sie *Speichern*.

Das neue CA-Zertifikat wird in der Liste *Zertifizierungsstelle* angezeigt.

Um eine CA zu löschen, klicken Sie auf die Schaltfläche *Delete* der entsprechenden CA.

Die Signierungs-CA kann im PKCS#12-Format heruntergeladen werden. Sie werden dann aufgefordert, ein Kennwort einzugeben, das benutzt wird, um den PKCS#12-Container zu sichern. Außerdem können Sie Verifizierungs-CAs im PEM-Format herunterladen.

Hinweis – Um Problemen beim Herunterladen von Dateien mit dem Internet Explorer 6 vorzubeugen, fügen Sie die URL der Firewall (z.B. <https://192.168.2.100>) und des Benutzerportals (z.B. <https://192.168.2.100>) den *Vertrauenswürdigen Sites* hinzu. Beim Internet Explorer 6 befinden sich diese Einstellungen im Menü *Extras >> Internetoptionen >> Sicherheit*. Beim Internet Explorer 7 aktivieren Sie zusätzlich im Fenster *Sicherheitseinstellungen* die Funktion *Automatische Eingabeaufforderung für Dateidownloads*.

Sperrlisten (CRLs)

Eine Zertifikatssperrliste (CRL, engl. *Certificate Revocation List*) (auch *Widerrufsliste*) ist eine Liste von Zertifikaten (genauer: ihren Seriennummern), die widerrufen wurden, das heißt, die nicht länger gültig sind, und aus diesem Grund nicht vertrauenswürdig sind. Auf der Registerkarte *Site-to-Site-VPN >> Zertifikatverwaltung >> Sperrlisten (CRLs)* können Sie eine Zertifikatssperrliste importieren, die sich auf Ihre Public-Key-Infrastruktur (PKI, dt. *Infrastruktur für öffentliche Schlüssel*) bezieht.



Figure 14.12 Site-to-Site-VPN: Liste der Sperrlisten (CRLs)

Um eine Zertifikatssperrliste (CRL) hochzuladen, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Sperrlisten (CRLs)* auf *CRL hochladen*.**

Das Dialogfenster *CRL hochladen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Name: Geben Sie einen aussagekräftigen Name für diese CRL ein.

CRL-Datei: Klicken Sie auf das Ordner-Symbol und wählen Sie die zu importierende Datei aus.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die CRL hinzu.

3. **Klicken Sie *Speichern*.**

Die neue CRL wird in der Liste der Sperrlisten angezeigt.

Um eine Sperrliste zu löschen, klicken Sie auf die Schaltfläche *Delete* der entsprechenden Sperrliste.

Erweitert

Auf der Registerkarte *Site-to-Site-VPN >> Zertifikatverwaltung >> Erweitert* können Sie die VPN-Signierungs-CA neu generieren, die während der ersten Anmeldung am Sicherheitssystem automatisch generiert wurde. Mit der VPN-Signierungs-CA werden die Zertifikate für die Fernzugriffs- und Site-to-Site-VPN-Verbindungen digital signiert.

Signierungs-CA neu erstellen

Sie können alle Benutzerzertifikate mit der aktuellen Signierungs-CA erneuern. Das wird dann notwendig, wenn Sie eine alternative VPN-Signierungs-CA auf der Registerkarte *Zertifizierungsstelle* installiert haben.

Zertifikatsverwaltung

Zertifikate Zertifizierungsstelle Sperrlisten (CRLs) **Erweitert**

→ Signierungs-CA neu erstellen ←

Organisation Name:	Beispiel AG	Hier können Sie die VPN-Signierungs-CA neu erstellen, die bei dem erstmaligen Setup der Einheit eingerichtet wurde. Die VPN-Signierungs-CA ist die Zertifizierungsstelle, die Digitalzertifikate signiert, die für den Fernzugriff- und für Site-to-Site-VPN-Verbindungen verwendet werden. Um zu gewährleisten, dass VPN-Verbindungen mit der alten VPN-Signierungs-CA nach Austausch der Signierungs-CA noch funktionieren, wird die alte VPN-Signierungs-CA als Verifizierungs-CA beibehalten. Achtung! Die Geräte- und alle Benutzerzertifikate werden mit der neuen Signierungs-CA neu erstellt. Dies kann zu einer Unterbrechung aktuell bestehender Site-to-Site-VPN- und Roadwarrior-Verbindungen führen.
Stadt:	Berlin	
Land:	Germany	
E-Mail:	admin@beispiel.de	

 **Apply**

Figure 14.13 Site-to-Site-VPN: Erweiterte Einstellungen

Fernzugriff

In diesem Kapitel wird beschrieben, wie Sie den Fernzugriff (engl. *Remote Access*) für Astaro Security Gateway konfigurieren. Der Fernzugriff wird in Astaro Security Gateway mittels virtuellen privaten Netzwerken (VPN, engl. *virtual private network*) realisiert. Diese sind ein kosteneffektiver und sicherer Weg, entfernten Benutzern wie Angestellten, die von unterwegs und von zu Hause aus arbeiten, den Zugang zum Firmennetzwerk zu ermöglichen. VPNs verwenden kryptografische Tunnelprotokolle wie IPSec und PPTP, um Vertraulichkeit und Datenschutz für die übertragenen Daten zu gewährleisten.

Querverweis – Weitere Informationen zur Konfiguration von Fernzugriff-VPN-Verbindungen in der Astaro Knowledgebase³⁵ im Verzeichnis *ASG Version 7 >> Astaro Manuals and Guides*.

Die ASG generiert automatisch die notwendigen Installations- und Konfigurationsdateien für die jeweiligen Verbindungsart des Fernzugriffs. Diese Dateien können direkt über das Benutzerportal heruntergeladen werden. Es sind jedoch nur jene Dateien für einen Benutzer verfügbar, die mit den Verbindungsarten übereinstimmen, die für ihn aktiviert sind. Beispiel: Ein Benutzer, für den der SSL-Fernzugriff aktiviert ist, findet nur eine SSL-Installationsdatei vor.

Die Seite *Fernzugriffsstatus* enthält eine Übersicht mit allen Online-Benutzern. Dieses Kapitel enthält Informationen zu den folgenden Themen:

- SSL
- PPTP
- L2TP über IPSec
- IPSec
- Cisco VPN Client

³⁵ <http://www.astaro.com/kb/>

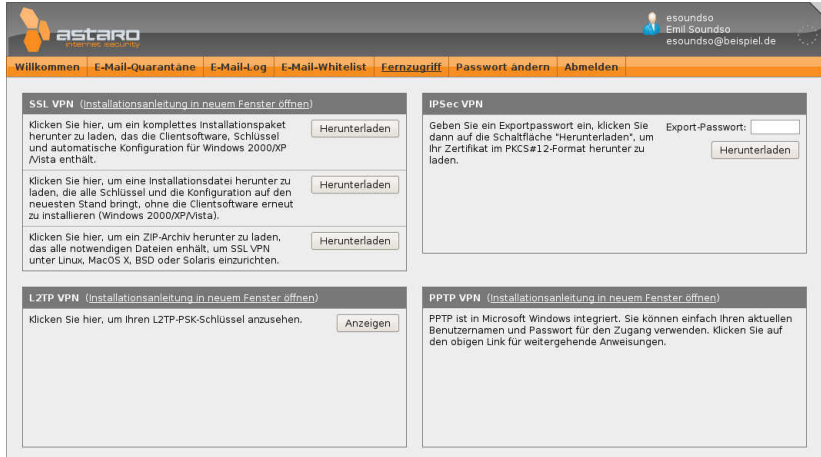


Figure 15.1 Installationsdateien für den Fernzugriff im Benutzerportal

- Erweitert
- Zertifikatverwaltung

SSL

Der Fernzugriff-SSL-Funktion von Astaro Security Gateway wird durch OpenVPN realisiert, einer umfassenden SSL-VPN-Lösung. Es bietet die Möglichkeit, zwischen entfernten Mitarbeitern und dem Unternehmensnetzwerk punkt-zu-punkt-verschlüsselte Tunnel aufzubauen, wobei SSL-Zertifikate und eine Benutzer-Kennwort-Kombination benötigt werden, um sich für den Zugriff auf interne Ressourcen zu authentifizieren. Zusätzlich bietet es ein sicheres Benutzerportal, das von jedem autorisierten Benutzer erreicht werden kann, um ein maßgeschneidertes SSL-VPN-Client-Software-Paket herunterzuladen. Dieses Paket beinhaltet einen freien SSL-VPN-Client, SSL-Zertifikate und eine Konfiguration, die mit einer einfachen Ein-Klick-Installationsprozedur verarbeitet werden. Der SSL-VPN-Client unterstützt die gängigsten Business-Anwendungen wie natives Outlook, native Windows-Dateifreigabe und viele weitere.

Querverweis – Weitere Informationen zur Benutzung des SSL-VPN-Clients finden Sie in der Astaro Knowledgebase³⁶ im Verzeichnis *ASG Version 7 > > Astaro Manuals and Guides*.

³⁶ <http://www.astaro.com/kb/>

Allgemein

Auf der Registerkarte *Fernzugriff* >> *SSL* >> *Allgemein* werden die Grundeinstellung für den VPN-Zugang durchgeführt. Die SSL-VPN-Lösung von Astaro Security Gateway setzt sogenanntes *Split Tunneling* (dt. etwa *geteiltes Tunneln*) ein. Das bedeutet, dass ein entfernter Benutzer Zugang zu einem öffentlichen Netzwerk (z. B. dem Internet) hat und gleichzeitig auf Ressourcen im VPN zugreifen kann. Split-Tunneling kann jedoch auch umgangen werden, indem Sie *Any* als lokales Netzwerk definieren (siehe unten). Dadurch wird aller Verkehr durch den VPN-SSL-Tunnel geroutet. Ob Benutzer dann noch auf ein öffentliches Netzwerk zugreifen dürfen oder nicht, hängt von Ihren Paketfiltereinstellungen ab.

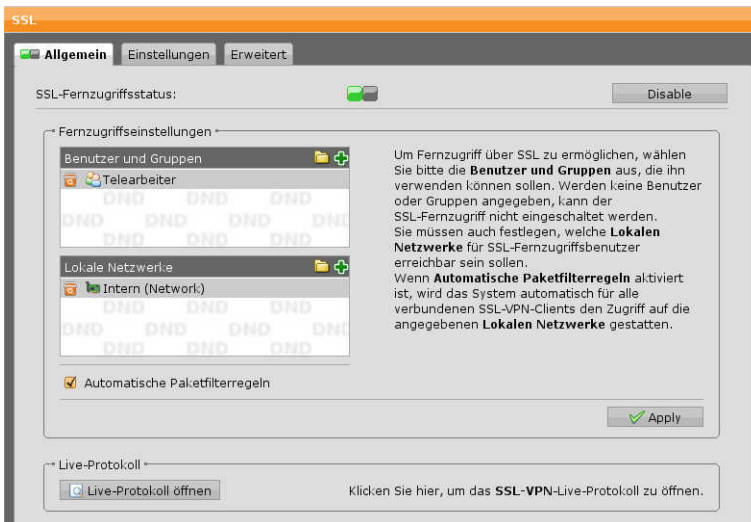


Figure 15.2 Fernzugriff SSL: Konfiguration

Um die globalen SSL-VPN-Optionen zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie auf der Registerkarte *Allgemein* den Fernzugriff.**
Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche.

Die Statusampel wird gelb und der Abschnitt *Fernzugriffseinstellungen* kann nun bearbeitet werden.

2. Nehmen Sie die folgenden Einstellungen vor:

Benutzer und Gruppen: Wählen Sie die für den Fernzugriff zugelassenen Benutzer und Benutzergruppen aus. Solange keine entsprechenden Benutzerkonten ausgewählt sind, kann der SSL-Fernzugriff nicht eingeschaltet werden.

Hinweis – Das SSL-VPN-Client-Software-Paket im Benutzerportal kann nur von Benutzern heruntergeladen werden, für die auf der Registerkarte Benutzer ein Benutzerkonto hinzugefügt wurde *und* wenn dieses Konto hier im Dialogfenster *Benutzer und Gruppen* ausgewählt wurde. Bei Benutzern, für die *nur* eine Benutzerdefinition existiert, steht kein SSL-VPN-Client-Software-Paket bereit. Dennoch haben Sie Zugang zum Benutzerportal. Im Benutzerportal wird auf der Registerkarte *Fernzugriff >> SSL-VPN* die folgende Meldung angezeigt: „Unfortunately this remote access method is not configured for you“ (dt. Diese Fernzugriffsmethode ist leider nicht für Sie konfiguriert).

Lokale Netzwerke: Wählen Sie das/die lokale(n) Netzwerk(e) aus, die für SSL-Clients erreichbar sein soll(en).

Automatische Paketfilterregeln: Wählen Sie diese Option, damit die notwendigen Paketfilterregeln automatisch angelegt werden.

3. Klicken Sie *Übernehmen*.

Ihre Einstellungen werden gespeichert.

Live-Protokoll öffnen

Im *OpenVPN Live Log* werden die Aktivitäten betreffend den Fernzugriff protokolliert. Klicken Sie auf die Schaltfläche, um das Live-Protokoll in einem neuen Fenster zu öffnen.

Einstellungen

Auf der Registerkarte *SSL >> Einstellungen* können Sie die Grundeinstellungen für SSL-VPN-Serververbindungen konfigurieren.

Hinweis – Diese Registerkarte ist identisch für *Site-to-Site-VPN >> SSL* und *Fernzugriff >> SSL*. Hier vorgenommene Änderungen wirken sich auf beide SSL-Konfigurationen aus.

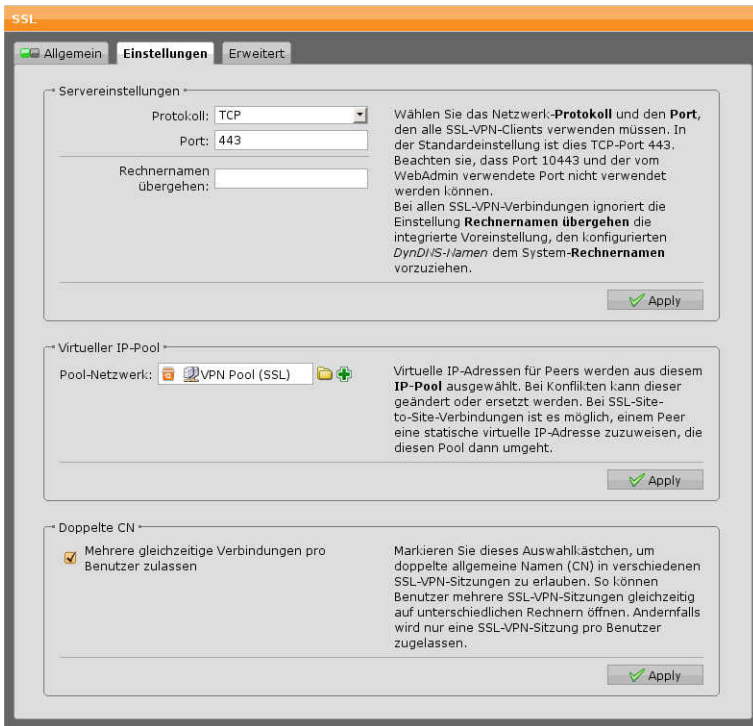


Figure 15.3 Fernzugriff SSL: Konfiguration der Einstellungen

Servereinstellungen

Sie können die folgenden Einstellung für die SSL-VPN-Verbindung vornehmen:

- **Protokoll:** Wählen Sie das Protokoll aus, das verwendet werden soll. Sie können entweder *TCP* oder *UDP* auswählen.
- **Port:** Sie können den Port ändern. Der Standardport ist 443. Sie können jedoch nicht den Port 10443, den ACC-Gateway-Manager-Port 4422 oder den Port der WebAdmin-Schnittstelle verwenden.
- **Rechnernamen übergehen:** Der Wert im Feld *Rechnernamen übergehen* wird als Zielrechnernamen für Client-VPN-Verbindungen verwendet und ist standardmäßig der Rechnername von der Firewall. Ändern Sie den vor-eingestellten Wert nur, wenn der reguläre Rechnername (oder DynDNS-Rechnername) nicht unter diesem Name vom Internet aus erreichbar ist.

Virtueller IP-Pool

Pool-Netzwerk: Das ist der virtuelle IP-Adressenpool, der verwendet wird, um IP-Adressen aus einem bestimmten IP-Adressbereich SSL-Clients zuzuweisen. Standardmäßig ist *VPN Pool (SSL)* ausgewählt. Falls Sie einen anderen Adressenpool auswählen, darf die Netzmaske nicht größer als 29 Bits sein, da OpenVPN nicht mit Adressenpools umgehen kann, deren Netzmaske /30, /31 oder /32 ist.

Doppelte CN

Wählen Sie *Mehrere gleichzeitige Verbindungen pro Benutzer zulassen*, wenn Sie zulassen wollen, dass Ihre Benutzer sich von verschiedenen IP-Adressen aus zur gleichen Zeit verbinden können. Wenn diese Option deaktiviert ist, ist nur eine gleichzeitige SSL-VPN-Verbindung pro Benutzer erlaubt.

Erweitert

Auf der Registerkarte *SSL >> Erweitert* können Sie diverse erweiterte Serveroptionen konfigurieren, wie z. B. Einstellungen zur Kryptografie, zur Komprimierung und zur Fehlersuche.

Hinweis – Diese Registerkarte ist identisch für *Site-to-Site-VPN >> SSL* und *Fernzugriff >> SSL*. Hier vorgenommene Änderungen wirken sich auf beide SSL-Konfigurationen aus.

Kryptografische Einstellungen

Diese Einstellungen kontrollieren die Verschlüsselungsparameter für alle SSL-VPN-Fernzugriff-Clients:

- **Verschlüsselungsalgorithmus:** Der Verschlüsselungsalgorithmus legt den Algorithmus fest, der für die Verschlüsselung der für die Daten verwendet wird, die durch den Tunnel gesendet werden. Die folgenden Algorithmen werden unterstützt und sie sind alle im CBC-Modus (*Cipher Block Chaining*):
 - *DES-EDE3-CBC*
 - *AES-128-CBC* (128 bit)
 - *AES-192-CBC* (192 bit)

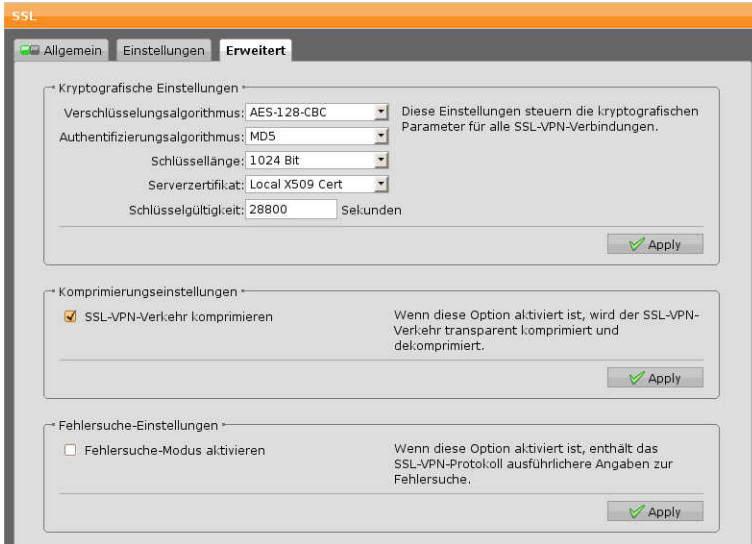


Figure 15.4 Fernzugriff SSL: Konfiguration der erweiterten Einstellungen

- *AES-256-CBC* (256 bit)
- *BF-CBC* (Blowfish (128 bit))
- **Authentifizierungsalgorithmus:** Der Authentifizierungsalgorithmus legt den Algorithmus fest, der für die Integritätsprüfung der Daten verwendet wird, die durch den VPN-Tunnel gesendet werden. Unterstützte Algorithmen sind:
 - *MD5* (128 bit)
 - *SHA-1* (160 bit)
- **Schlüssellänge:** Die Schlüssellänge ist die Länge des Diffie-Hellman-Schlüsselaustauschs. Je länger der Schlüssel ist, desto sicherer sind die symmetrischen Schlüssel. Die Länge wird in Bits angegeben. Sie können zwischen einer Schlüssellänge von 1024 und 2048 Bits wählen.
- **Serverzertifikat:** Wählen Sie ein lokales SSL-Zertifikat, das der SSL-VPN-Server verwenden soll, um sich gegenüber Clients zu identifizieren.
- **Schlüsselgültigkeit:** Geben Sie einen Zeitpunkt an, nach dem der Schlüssel abläuft. Der Standard ist 28.800 Sekunden.

Komprimierungseinstellungen

SSL-VPN-Verkehr komprimieren: Wenn diese Option aktiviert ist, werden alle Daten, die durch SSL-VPN-Tunnel geschickt werden, vor der Verschlüsselung komprimiert.

Fehlersuche-Einstellungen

Fehlersuche-Modus aktivieren: Wenn Sie den Fehlersuche-Modus aktivieren, wird die SSL-VPN-Protokolldatei zusätzliche Informationen enthalten, die nützlich für die Fehlersuche sind.

PPTP

PPTP (*Point-to-Point Tunneling Protocol*) ermöglicht einzelnen Rechnern mithilfe eines verschlüsselten Tunnels den Zugriff über das Internet auf interne Netzwerkdienste. PPTP ist einfach einzurichten und benötigt auf Microsoft Windows-Systemen keine spezielle Software.

PPTP ist in Microsoft Windows ab Version 95 enthalten. Um PPTP mit Astaro Security Gateway verwenden zu können, muss der Client das MSCHAPv2-Authentifizierungsprotokoll unterstützen. Benutzer von Windows 95 und 98 müssen ein Update aufspielen, damit dieses Protokoll unterstützt wird.

Allgemein

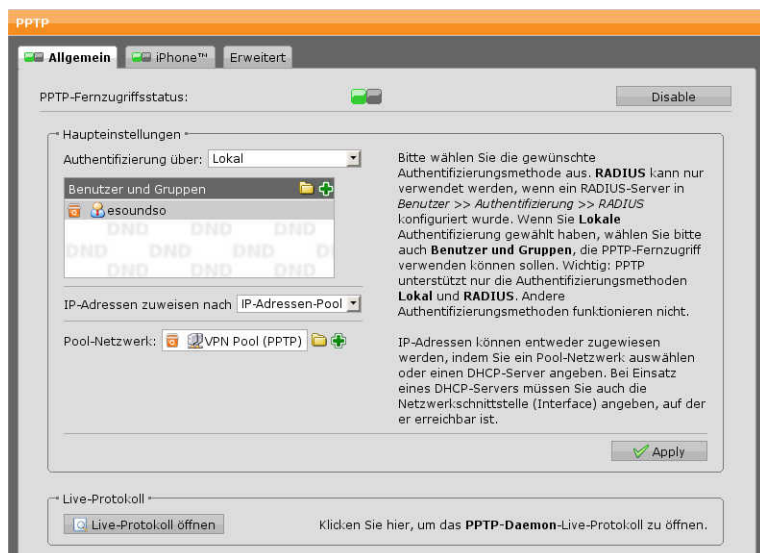


Figure 15.5 Fernzugriff PPTP: Grundeinstellungen

Um die allgemeinen Optionen für PPTP zu konfigurieren, gehen Sie folgendermaßen vor:

1. Aktivieren Sie auf der Registerkarte *Allgemein* den PPTP-Fernzugriff.

Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche.

Die Statusampel wird gelb und der Abschnitt *Haupteinstellungen* kann nun bearbeitet werden.

2. Nehmen Sie die folgenden Einstellungen vor:

Authentifizierung über: Wählen Sie die Authentifizierungsmethode. PPTP-Fernzugriff unterstützt nur die lokale und RADIUS-Authentifizierung.

- **Lokal:** Wenn Sie *Lokal* wählen, geben Sie die Benutzer und Benutzergruppen an, die PPTP-Fernzugriff verwenden dürfen. Es ist nicht möglich, Backend-Benutzergruppen in das Feld zu ziehen. Solange keine entsprechenden Benutzerkonten ausgewählt sind, kann der PPTP-Fernzugriff nicht eingeschaltet werden.

Hinweis – Ähnlich wie bei SSL-VPN kann auf den Menüpunkt *Fernzugriff* im Benutzerportal nur von Benutzern zugegriffen werden, die im Feld *Benutzer und Gruppen* eingetragen sind und für die eine Benutzerdefinition auf dem Sicherheitssystem besteht. Andernfalls wird im Benutzerportal auf der Registerkarte *Fernzugriff >> PPTP-VPN* die folgende Meldung angezeigt: „Unfortunately this remote access method is not configured for you“ (dt. Diese Fernzugriffsmethode ist leider nicht für Sie konfiguriert). Autorisierte Benutzer, die sich erfolgreich am Benutzerportal angemeldet haben, finden einen Link zu einer Installationsanleitung, die in der Astaro Knowledgebase³⁷ verfügbar ist (unter *ASG Version 7 >> Remote Access >> PPTP*).

- **RADIUS:** *RADIUS* kann nur ausgewählt werden, wenn zuvor ein RADIUS-Server konfiguriert wurde. Bei dieser Authentifizierungsmethode werden Benutzer an einem externen RADIUS-Server authentifiziert, welcher auf der Registerkarte *Benutzer >> Authentifizierung >> Server* konfiguriert werden kann. Das Feld *Benutzer und Gruppen* wird dann ausgegraut; seine Einstellungen können zwar

³⁷ <http://www.astaro.com/kb>

noch geändert werden, haben aber keinen Effekt mehr. Der RADIUS-Server muss MSCHAPv2-Challenge-Response-Authentifizierung unterstützen. Der Server kann Parameter wie die Client-IP-Adresse und die DNS/WINS-Serveradresse zurückgeben. Das PPTP-Modul sendet die folgende NAS-ID an den RADIUS-Server: pptp. Wenn RADIUS-Authentifizierung gewählt ist, beachten Sie, dass lokale Benutzer nicht länger mit PPTP authentifiziert werden können. Des Weiteren müssen auch Clients die MSCHAPv2-Authentifizierung unterstützen.

IP-Adressen zuweisen nach: Bei PPTP können Sie IP-Adressen entweder aus einem festgelegten IP-Adressen-Pool zuweisen oder von einem DHCP-Server verteilen lassen. Die folgenden Optionen sind möglich:

- **IP-Adressen-Pool:** Wählen Sie diese Option aus, wenn Sie IP-Adressen aus einem bestimmten IP-Adressbereich an Clients zuweisen wollen, die sich per Fernzugriff über PPTP verbinden. Standardmäßig werden Adressen aus dem privaten IP-Raum 10.242.1.0/24 zugewiesen. Diese Netzwerkdefinition heißt *VPN Pool (PPTP)* und kann in alle netzwerk-spezifischen Konfigurationsoptionen verwendet werden. Wenn Sie ein anderes Netzwerk verwenden wollen, ändern Sie einfach die Definition von *VPN Pool (PPTP)* auf der Registerkarte *Definitionen >> Netzwerk*. Alternativ können Sie auch einen anderen IP-Adressen-Pool anlegen, indem Sie auf das Plus-Symbol neben dem Textfeld *Pool-Netzwerk* klicken.
- **DHCP-Server:** Wenn Sie diese Option wählen, geben Sie die folgenden Einstellungen für den DHCP-Server an:
 - **DHCP-Server:** Geben Sie die IP-Adresse des DHCP-Servers an. Beachten Sie, dass der lokale DHCP-Server nicht unterstützt wird. Der hier angegebene DHCP-Server muss auf einem anderen System laufen.
 - **auf Schnittstelle:** Wählen Sie die lokale Schnittstelle aus, über die der DHCP-Server erreicht werden kann. Beachten Sie, dass der DHCP-Server nicht direkt mit der Schnittstelle verbunden sein muss – der Zugang kann auch über einen Router erfolgen.

3. Klicken Sie **Übernehmen**.

Ihre Einstellungen werden gespeichert.

Live-Protokoll

Im *PPTP Daemon Live Log* werden die Aktivitäten des PPTP-Fernzugriffs protokolliert. Klicken Sie auf die Schaltfläche, um das Live-Protokoll in einem neuen Fenster zu öffnen.

iPhone

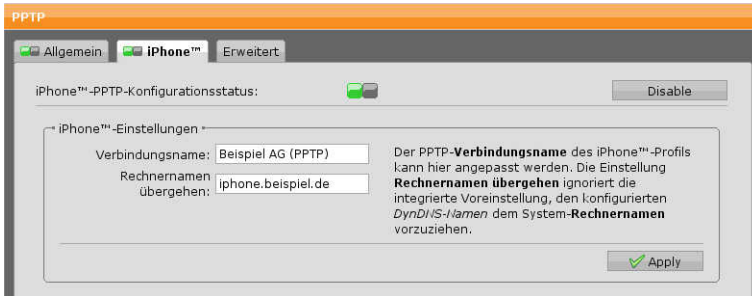


Figure 15.6 Fernzugriff PPTP: Konfiguration von iPhone-Fernzugriff

Sie können ermöglichen, dass iPhone-Benutzer eine automatische PPTP-Konfiguration im Benutzerportal angeboten wird.

Allerdings werden nur Benutzer, die im Feld *Benutzer und Gruppen* auf der Registerkarte *Allgemein* aufgeführt sind, die Konfigurationsdateien auf ihrer Benutzerportal-Site finden. Der iPhone-Status ist standardmäßig aktiviert.

Verbindungsname: Geben Sie einen aussagekräftigen Namen für die PPTP-Verbindung ein, sodass iPhone-Benutzer die Verbindung identifizieren können, die sie im Begriff sind aufzubauen. Der Name Ihrer Firma gefolgt vom Protokoll PPTP ist voreingestellt.

Hinweis – Der *Verbindungsname* muss zwischen allen iPhone-Verbindungseinstellungen (PPTP, L2TP über IPSec, Cisco VPN Client) einzigartig sein.

Rechnernamen übergehen: Im Falle, dass der Systemrechnernamen vom Client nicht öffentlich aufgelöst werden kann, können Sie hier einen Server-Rechnernamen eingeben, der die interne Präferenz übergeht, bei der der *DynDNS-Rechnernamen* dem *Systemrechnernamen* vorgezogen wird.

Um die automatische iPhone-Konfiguration auszuschalten, klicken Sie auf die Statusampel oder *Disable* oben auf der Registerkarte.

Die Statusampel wird rot.

Erweitert

Auf der Registerkarte *Fernzugriff >> PPTP >> Erweitert* können Sie die Verschlüsselungsstärke und die Menge an Fehlersuchemeldungen für PPTP-Fernzugriff konfigurieren. Die erweiterten PPTP-Einstellungen können nur konfiguriert werden, wenn PPTP auf der Registerkarte *Allgemein* aktiviert ist.

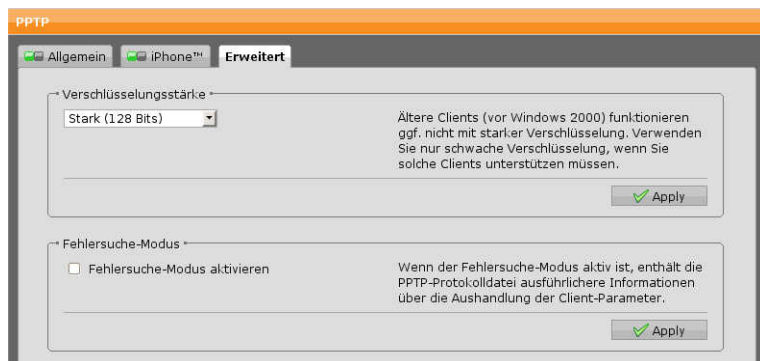


Figure 15.7 Fernzugriff PPTP: Erweiterte Einstellungen

Verschlüsselungsstärke

Sie können zwischen einer starken (128 Bit) Tunnel-Verschlüsselung (MPPE) und einer schwachen (40 Bit) wählen. Verwenden Sie nach Möglichkeit nicht die schwache Verschlüsselung, außer Sie haben Gegenstellen, die die 128-Bit-Verschlüsselung nicht unterstützen.

Fehlersuche-Modus

Fehlersuche-Modus aktivieren: Diese Option kontrolliert die Menge an Fehlersuchemeldungen, die im PPTP-Protokoll erzeugt wird. Aktivieren Sie diese Option, wenn Sie Verbindungsprobleme haben und detaillierte Informationen über beispielsweise die Aushandlung der Client-Parameter benötigen.

L2TP über IPSec

L2TP ist die Kurzform für *Layer 2 Tunneling Protocol* ist ein Datenlink-Ebene-Protokoll (Ebene 2 des OSI-Modells) für das Tunneln von Netzwerkverkehr zwischen zwei Peers über ein existierendes Netzwerk (meistens das Internet), auch bekannt als Virtuelles Privates Netzwerk (VPN, engl. *Virtual Private Network*). Da das L2TP-Protokoll keine Vertraulichkeit bietet wird es oft mit IPSec kombiniert: *L2TP über IPSec* (engl. *L2TP over IPSec*). Diese Kombination bietet Vertraulichkeit, Authentifizierung und Integrität. Mit L2TP über IPSec können Sie mit der gleichen Funktionalität wie PPTP einzelnen Rechner über

einen verschlüsselten IPSec-Tunnel der Zugang zum Unternehmensnetzwerk ermöglichen.

Allgemein

Auf der Registerkarte *L2TP über IPSec* >> *Allgemein* können Sie die grundlegenden Optionen für den Einsatz von Fernzugriff über L2TP über IPSec vornehmen.

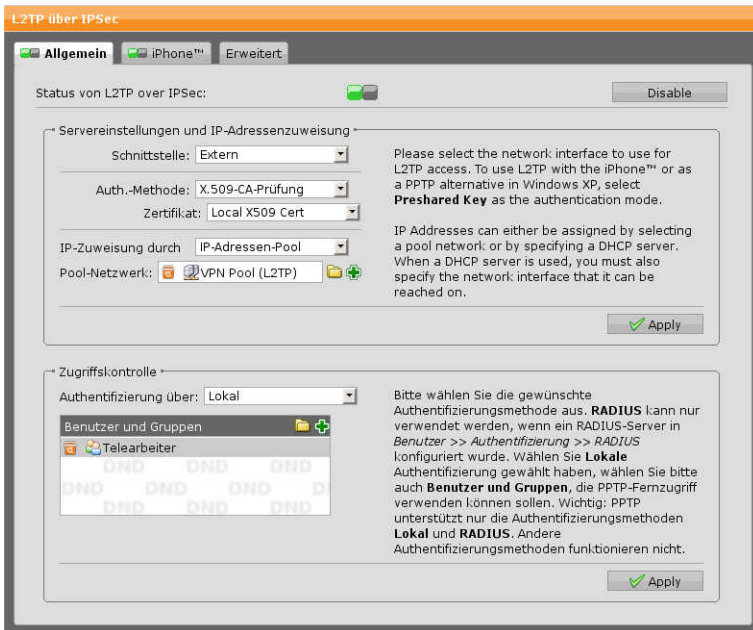


Figure 15.8 Fernzugriff L2TP: Grundeinstellungen

Um L2TP über IPSec zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie auf der Registerkarte *Allgemein* die Funktion *L2TP über IPSec*.**

Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche.

Die Statusampel wird gelb und der Abschnitt *Servereinstellungen und IP-Adressenzuweisung* kann nun bearbeitet werden.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Schnittstelle: Wählen Sie die Netzwerkschnittstelle, die für den L2TP-über-IPSec-Zugang verwendet werden soll.

Auth.-Methode: Sie können zwischen den folgenden Authentifizierungsmethoden wählen:

- **Vorvereinbarter Schlüssel:** Geben Sie ein Kennwort ein, das als vorvereinbarter Schlüssel dient. Die Authentifizierung mit vorvereinbarten Schlüsseln (PSK, engl. *preshared keys*) erfolgt durch Schlüssel mit einem geheimen Kennwort, die vor der eigentlichen Verbindung unter den Beteiligten ausgetauscht werden. Um zu kommunizieren, beweisen beide Gegenstellen, dass sie das Kennwort kennen. Der vorvereinbarte Schlüssel ist ein Kennwort, das dazu benutzt wird, den Datenverkehr mit dem Verschlüsselungsalgorithmus von L2TP zu verschlüsseln. Um die höchstmögliche Sicherheit zu gewährleisten, sollten Sie sich an den gängigen Maßgaben für die Stärke des Kennwortes orientieren. Wie sicher solche PSKs sind, hängt davon ab, wie sicher das Kennwort gewählt wurde und wie sicher es übertragen wird. Kennwörter, die aus allgemeinen Wörter bestehen sind sehr anfällig für Wörterbuchangriffe. Daher sollte ein Kennwort ziemlich lang sein und eine Reihe von Buchstaben, Großbuchstaben und Nummern enthalten. Folglich sollte ein vorvereinbarter Schlüssel auch nicht als Authentifizierungsmethode verwendet, sondern durch Zertifikate ersetzt werden, wo immer das möglich ist.
- **X.509-CA-Prüfung:** Die Authentifizierung durch X.509-Zertifikate erleichtert den Austausch des öffentlichen Schlüssels in großen VPN-Installationen mit vielen Teilnehmern. Eine sogenannte Zertifizierungsstelle (CA, engl. *Certificate Authority*) erfasst und überprüft die öffentlichen Schlüssel der VPN-Endpunkte und stellt für jeden Teilnehmer ein Zertifikat aus. Dieses Zertifikat enthält Informationen zur Identität des Teilnehmers und den zugehörigen öffentlichen Schlüssel. Da das Zertifikat digital signiert ist, kann niemand anderes ein gefälschtes Zertifikat verteilen, ohne entdeckt zu werden.
Während des Schlüsselaustauschs werden die X.509-Zertifikate durch die lokal installierten CAs beglaubigt. Die eigentliche Authentifizierung der VPN-Endpunkte wird dann durch die öffentlichen und privaten Schlüssel durchgeführt. Wenn Sie diese Authentifizierungsmethode verwenden wollen, wählen Sie ein X.509-Zertifikat.
Beachten Sie, dass Sie für die X.509-Authentifizierungsmethode auf der Registerkarte *Fernzugriff >> Zertifikatverwaltung >> Zertifizierungsstelle* eine gültige CA konfiguriert haben müssen.

IP-Zuweisung durch: Die IP-Adressen können den L2TP-VPN-Clients während des Verbindungsaufbaus aus einem vordefinierten *IP-Adressen-Pool* oder automatisch von einem *DHCP-Server* zugewiesen werden.

- **Pool-Netzwerk:** Standardmäßig ist *IP-Adressen-Pool* für die IP-Adressenzuweisung ausgewählt, wobei die Netzwerkdefinition *VPN Pool (L2TP)* als Pool-Netzwerk voreingestellt ist. Der *VPN Pool (L2TP)* ist ein zufällig generiertes Netzwerk aus dem IP-Adressbereich 10.x.x.x für private Netzwerke, für das ein Klasse-C-Subnetz verwendet wird. Normalerweise ist es nicht notwendig, das zu ändern, da es sicherstellt, dass die Benutzer einen bestimmten Adressen-Pool haben, von dem aus sie Verbindungen aufbauen können. Wenn Sie ein anderes Netzwerk verwenden wollen, können Sie einfach die Definition des *VPN Pool (L2TP)* ändern, oder hier ein anderes Netzwerk als IP-Adressen-Pool angeben.

Hinweis – Wenn Sie private IP-Adressen für Ihren L2TP-VPN-Pool verwenden und wollen, dass IPSec-Rechner auf das Internet zugreifen dürfen, legen Sie entsprechende Maskierungs- oder NAT-Regeln für den IP-Adressen-Pool an.

- **DHCP-Server:** Wenn Sie *DHCP-Server* auswählen, geben Sie auch die Netzwerkschnittstelle an, über die der DHCP-Server erreichbar ist. Der DHCP-Server muss nicht direkt mit der Schnittstelle verbunden sein – er kann auch über einen Router erreichbar sein. Beachten Sie, dass der lokale DHCP-Router nicht unterstützt wird; der hier gewählte DHCP-Server muss auf einem physikalisch anderen System laufen.

3. Klicken Sie **Übernehmen**.

Ihre Einstellungen werden gespeichert.

Um die Konfiguration abzubrechen, klicken Sie auf die Schaltfläche *Abort* *Enable* oder auf die gelbe Statusampel.

Zugriffskontrolle

Authentifizierung über: L2TP-Fernzugriff unterstützt nur die lokale und RADIUS-Authentifizierung.

- **Lokal:** Wenn Sie *Lokal* wählen, geben Sie die Benutzer und Benutzergruppen an, die sich per L2TP-Fernzugriff verbinden dürfen. Es ist nicht möglich, Backend-Benutzergruppen in das Feld zu ziehen. Lokale Benutzer müssen auf dem herkömmlichen Weg hinzufügen und L2TP für sie aktivieren. Wenn keine Benutzer oder Gruppen ausgewählt sind, wird L2TP-Fernzugriff ausgeschaltet.

Hinweis – Ähnlich wie bei SSL-VPN kann auf den Menüpunkt *Fernzugriff* im Benutzerportal nur von Benutzern zugegriffen werden, die im Feld *Benutzer und Gruppen* eingetragen sind und für die eine Benutzerdefinition auf dem Sicherheitssystem besteht. Andernfalls wird im Benutzerportal auf der Registerkarte *Fernzugriff >> L2TP-VPN* die folgende Meldung angezeigt: „Unfortunately this remote access method is not configured for you“ (dt. Diese Fernzugriffsmethode ist leider nicht für Sie konfiguriert). Autorisierte Benutzer, die sich erfolgreich am Benutzerportal angemeldet haben, finden einen Link zu einer Installationsanleitung, die in der Astaro Knowledgebase³⁸ verfügbar ist (unter *ASG Version 7 >> Remote Access >> L2TP over IPsec*).

- **RADIUS:** Wenn Sie *RADIUS* auswählen, werden die Authentifizierungsanfragen an den RADIUS-Server weitergeleitet. Das L2TP-Modul sendet die NAS-ID „l2tp“ an den RADIUS-Server.

Der Authentifizierungsalgorithmus wird automatisch zwischen dem Client und dem Server ausgehandelt. Für lokale Benutzer unterstützt Astaro Security Gateway die folgenden Authentifizierungsprotokolle:

- MSCHAPv2
- PAP

Ein Windows-Client handelt standardmäßig MSCHAPv2 aus.

Für RADIUS-Benutzer unterstützt Astaro Security Gateway die folgenden Authentifizierungsprotokolle:

- MSCHAPv2
- MSCHAP
- CHAP
- PAP

iPhone

³⁸ <http://www.astaro.com/kb>

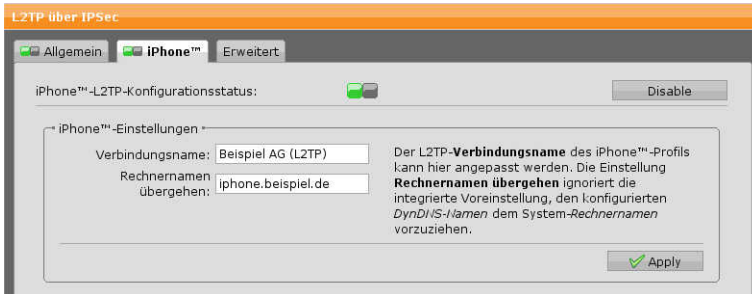


Figure 15.9 Fernzugriff L2TP: Konfiguration von iPhone-Fernzugriff

Sie können ermöglichen, dass iPhone-Benutzer eine automatische L2TP über IPSec-Konfiguration im Benutzerportal angeboten wird.

Allerdings werden nur Benutzer, die im Feld *Benutzer und Gruppen* auf der Registerkarte *Allgemein* aufgeführt sind, die Konfigurationsdateien auf ihrer Benutzerportal-Site finden. Der iPhone-Status ist standardmäßig aktiviert.

Verbindungsname: Geben Sie einen aussagekräftigen Namen für die L2TP über IPSec-Verbindung ein, sodass iPhone-Benutzer die Verbindung identifizieren können, die sie im Begriff sind aufzubauen. Der Name Ihrer Firma gefolgt vom Protokoll L2TP über IPSec ist voreingestellt.

Hinweis – Der *Verbindungsname* muss zwischen allen iPhone-Verbindungseinstellungen (PPTP, L2TP über IPSec, Cisco VPN Client) einzigartig sein.

Rechnernamen übergehen: Im Falle, dass der Systemrechnernamen vom Client nicht öffentlich aufgelöst werden kann, können Sie hier einen Server-Rechnernamen eingeben, der die interne Präferenz übergeht, bei der der *DynDNS-Rechnernamen* dem *Systemrechnernamen* vorgezogen wird.

Um die automatische iPhone-Konfiguration auszuschalten, klicken Sie auf die Statusampel oder *Disable* oben auf der Registerkarte.

Die Statusampel wird rot.

Erweitert

Fehlersuche-Modus

Fehlersuche-Modus aktivieren: Diese Option kontrolliert die Menge an Fehlermeldungen, die im L2TP über IPSec-Protokoll erzeugt wird. Aktivieren



Figure 15.10 Fernzugriff L2TP: Erweiterte Einstellungen

Sie diese Option, wenn Sie Verbindungsprobleme haben und detaillierte Informationen über beispielsweise die Aushandlung der Client-Parameter benötigen.

IPSec

IP Security (IPSec) ist ein Standard für die Sicherung von *Internet-Protocol* (IP)-Kommunikationen durch Verschlüsselung- und/oder Authentifizierung aller IP-Pakete.

Der IPSec-Standard kennt zwei Betriebsarten (Modi) und zwei Protokolle:

- Transportmodus (engl. *Transport Mode*)
- Tunnelmodus (engl. *Tunnel Mode*)
- *Authentication Header* (AH): Protokoll für Authentifizierung
- *Encapsulated Security Payload* (ESP): Protokoll für Verschlüsselung (und Authentifizierung)

Des Weiteren bietet IPSec Methoden für die manuelle und die automatische Verwaltung von Sicherheitsverbindungen (SAs, engl. *Security Associations*) sowie zur Schlüsselverteilung. Alle diese Merkmale wurden in einer *Domain of Interpretation* (DOI) zusammengefasst.

IPSec-Modi

IPSec kann entweder im Transportmodus oder im Tunnelmodus arbeiten. Eine Rechner-zu-Rechner-Verbindung kann grundsätzlich jeden Modus verwenden. Wenn es sich bei einem der beiden Tunnelendpunkte jedoch um ein Astaro Security Gateway handelt, muss der Tunnelmodus verwendet werden. Die IPSec-VPN-Verbindungen dieses Sicherheitssystems arbeiten immer im Tunnelmodus.

Im Transportmodus wird das zu bearbeitende IP-Paket nicht in ein anderes IP-Paket eingepackt. Der ursprüngliche IP-Header wird beibehalten und das übrige Paket wird entweder im Klartext (AH) oder verschlüsselt (ESP) gesendet.

Nun kann entweder das komplette Paket mit AH authentifiziert oder die Payload mit Hilfe von ESP verschlüsselt und authentifiziert werden. Bei beiden Varianten wird der Original-Header in Klartext über das WAN geschickt.

Im Tunnelmodus wird das komplette Paket – Header und Payload – in ein neues IP-Paket eingepackt. Ein neuer IP-Header wird vorne an das IP-Paket angehängt, wobei die Zieladresse auf den empfangenden Tunnelendpunkt gesetzt wird. Die IP-Adressen des eingepackten Paketes bleiben unverändert. Das Originalpaket kann dann mit AH authentifiziert oder mit ESP authentifiziert und verschlüsselt werden.

IPSec-Protokolle

IPSec verwendet für die sichere Kommunikation auf IP-Ebene zwei Protokolle:

- **Authentication Header (AH):** Ein Protokoll für die Authentifizierung von Absendern eines Pakets sowie zur Überprüfung der Integrität des Paketinhalts.
- **Encapsulating Security Payload (ESP):** Ein Protokoll für die Verschlüsselung des gesamten Pakets sowie für die Authentifizierung seines Inhalts.

Das *Authentication-Header*-Protokoll (AH) überprüft die Authentizität und die Integrität des Paketinhalts. Des Weiteren überprüft es, ob die Sender- und Empfänger-IP-Adressen während der Übertragung geändert wurden. Die Authentifizierung des Pakets erfolgt anhand einer Prüfsumme, die mittels eines *Hash-based Message Authentication Codes* (HMAC) in Verbindung mit einem Schlüssel und einem der folgenden Hash-Algorithmen berechnet wurde:

- **Message Digest Version 5 (MD5):** Dieser Algorithmus erzeugt aus einer Nachricht mit beliebiger Länge einen 128-Bit-langen Hash-Wert. Dieser resultierende Hash-Wert stellt eine Art Fingerabdruck des Paketinhalts dar und ändert sich, wenn die Nachricht verändert wird. Dieser Hash-Wert wird manchmal auch als digitale Signatur oder als *Message Digest* (dt. Prüfsumme) bezeichnet.
- **The Secure Hash (SHA-1):** Dieser Algorithmus erzeugt analog zum MD5 einen 160Bit-langen Hash-Wert. SHA-1 ist aufgrund des längeren Schlüssels sicherer als MD5.

Der Aufwand, einen Hash-Wert mittels SHA-1 zu berechnen, ist im Vergleich zum MD5-Algorithmus etwas höher. Die Berechnungsgeschwindigkeit hängt natürlich von der Prozessorgeschwindigkeit und der Anzahl der IPSec-VPN-Verbindungen ab, die auf Astaro Security Gateway verwendet werden.

Das *Encapsulated-Security-Payload*-Protokoll (ESP) bietet zusätzlich zur Verschlüsselung auch die Möglichkeit der Absender-Authentifizierung und der Verifizierung von Paketinhalten. Wenn ESP im Tunnelmodus verwendet wird, wird das komplette IP-Paket (Header und Payload) verschlüsselt. Zu diesem verschlüsselten Paket wird ein neuer unverschlüsselter IP- und ESP-Header hinzugefügt: Der neue IP-Header beinhaltet die Adresse des Empfänger-Gateway und die Adresse des Absender-Gateway. Diese IP-Adressen entsprechen denen des VPN-Tunnels.

Für ESP mit Verschlüsselung werden üblicherweise die folgenden Algorithmen verwendet:

- Triple Data Encryption Standard (3DES)
- Advanced Encryption Standard (AES)

Von diesen bietet AES den höchsten Sicherheitsstandard. Die effektiven Schlüssellängen, die mit AES verwendet werden können, sind 128, 192 oder 256 Bits. Astaro Security Gateway unterstützt mehrere Verschlüsselungs-Algorithmen. Für die Authentifizierung kann der MD5- oder der SHA-1-Algorithmus verwendet werden.

NAT Traversal (NAT-T)

NAT-Traversal ist ein Verfahren um zwischen Rechnern in TCP/IP-Netzwerken Verbindungen über NAT-Geräte aufzubauen. Dies wird erreicht, indem UDP-Verkapselung der ESP-Pakete benutzt wird, um IPSec-Tunnel über NAT-Geräte aufzubauen. Die UDP-Verkapselung wird nur verwendet, wenn zwischen den IPSec-Gegenstellen NAT gefunden wird; andernfalls werden normale ESP-Pakete verwendet.

Mit NAT-Traversal kann ein IPSec-Tunnel auch aufgebaut werden, wenn sich die Firewall oder ein Road Warrior hinter einem NAT-Router befindet. Wenn Sie diese Funktion nutzen wollen, müssen allerdings beide IPSec-Endpunkte NAT-Traversal unterstützen – das wird automatisch ausgehandelt. Zusätzlich muss auf dem NAT-Gerät der *IPSec-Passthrough* (IPSec-Durchreichung) ausgeschaltet sein, da dies NAT-Traversal beeinträchtigen kann.

Wenn Road Warrior NAT-Traversal verwenden wollen, muss ihr entsprechendes Benutzerobjekt in WebAdmin eine Statische Fernzugriffs-IP-Adresse (RAS, engl. *remote access IP address*) besitzen. Die Einstellung hierfür heißt *Statische Fernzugriffs-IP verwenden* und Sie finden sie auf der Seite Benutzer in WebAdmin.

Um zu verhindern, dass der Tunnel abgebaut wird, wenn keine Daten übermittelt werden, sendet NAT-Traversal in einem Intervall von 60 Sekunden ein

Signal zur Aufrechterhaltung (engl. *keep alive*). Durch dieses Aufrechterhaltungssignal wird sichergestellt, dass der NAT-Router sich die Statusinformation der Sitzung behält, damit der Tunnel offen bleibt.

Verbindungen

Auf der Registerkarte *IPSec* > > *Verbindungen* können Sie IPSec-Verbindungen anlegen und bearbeiten.



Figure 15.11 Fernzugriff IPSec: Verbindungen

Um eine IPSec-Verbindung zu konfigurieren, gehen Sie folgendermaßen vor:

1. Klicken Sie auf der Registerkarte *Verbindungen* auf *Neue IPSec-Fernzugriffsregel*.

Das Dialogfenster *IPSec-Fernzugriffsregel hinzufügen* wird geöffnet.

2. Nehmen Sie die folgenden Einstellungen vor:

Name: Geben Sie einen aussagekräftigen Name für ein.

Schnittstelle: Wählen Sie den Namen der Schnittstelle aus, die als lokaler Endpunkt für den IPSec-Tunnel dienen soll.

Lokale Netzwerke: Wählen Sie die lokalen Netzwerke aus, die über den VPN-Tunnel erreichbar sein sollen.

Richtlinie: Wählen Sie die IPSec-Richtlinie für diese IPSec-Verbindung aus. IPSec-Richtlinien könne auf der Registerkarte *Fernzugriff* > > *IPSec* > > *Richtlinien* definiert werden.

Authentifizierungsmethode: Wählen Sie die Authentifizierungsmethode für diese Fernzugriffsdefinition aus. Die folgenden Arten sind verfügbar:

- **Vorvereinbarter Schlüssel:** Authentifizierung mit *vorvereinbarten Schlüsseln* (PSK, engl. *Preshared Keys*) verwendet geheime Kennwörter als Schlüssel. Diese Kennwörter müssen an die Endpunkte verteilt werden, bevor eine Verbindung aufgebaut wird. Wenn ein neuer VPN-Tunnel aufgebaut ist, überprüft jede Seite, ob die andere Seite das geheime Kennwort kennt. Die Sicherheit der PSKs hängt von der Qualität der verwendeten Kennwörter ab: normale Wörter und Ausdrücke

fallen schnell Wörterbuchangriffen zum Opfer. Permanente oder langdauernde IPSec-Verbindungen sollten stattdessen Zertifikate verwenden.

- **X.509-Zertifikat:** Das X.509-Zertifikat basiert auf öffentlichen Schlüsseln und privaten Schlüsseln. Ein X.509-Zertifikat enthält den öffentlichen Schlüssel zusammen mit zusätzlichen Informationen über den Besitzer des Schlüssels. Solche Zertifikate sind von einer CA (Zertifizierungsstelle, engl. Certificate Authority) signiert und ausgestellt, der der Besitzer vertraut. Wenn Sie diese Authentifizierungsmethode wählen, geben Sie die Benutzer an, die diese IPSec-Verbindung benutzen dürfen. Es ist nicht möglich, Backend-Benutzergruppen in das Feld *Zugelassene Benutzer* zu ziehen. Wenn Sie die Option *Automatische Paketfilterregeln* abwählen, müssen Sie entsprechende Paketfilterregeln manuell im Menü *Network Security* anlegen.

Hinweis – Auf das Benutzerportal kann nur von Benutzern zugegriffen werden, die im Feld *Zugelassene Benutzer* ausgewählt sind und für die eine Benutzerdefinition auf dem Sicherheitssystem existiert. Autorisierte Benutzer, die sich erfolgreich am Benutzerportal angemeldet haben, finden den *Astaro Secure Client* (ASC) vor, dessen Konfigurationsdatei, die PKCS#12-Datei sowie einen Link zur Installationsanleitung, die auf der Astaro Knowledgebase³⁹ verfügbar ist (unter *ASG Version 7 >> Remote Access >> IPSec*).

- **CA-DN-Übereinstimmung:** Bei der Authentifizierungsmethode *CA-DN-Übereinstimmung* (engl. *CA DN Match*) wird eine Übereinstimmung der Distinguished Names (DN) von den CA-Zertifikaten benutzt, um die Schlüssel der VPN-Endpunkte zu verifizieren. Wenn Sie diese Authentifizierungsmethode wählen, wählen Sie eine *Zertifizierungsstelle* und eine *DN-Maske*, die zu den DNs der Fernzugriff-Clients passt. Wählen Sie danach einen *Peer-Subnetzbereich* aus oder fügen Sie einen hinzu. Clients ist es nur gestattet sich zu verbinden, wenn die DN-Maske zu derjenigen in ihrem Zertifikat passt.

XAUTH aktivieren (optional): XAUTH, erweiterte Authentifizierung (engl. *extended authentication*), sollte aktiviert werden, um von Benutzern eine Authentifizierung gegen konfigurierte Backends zu verlangen.

Automatische Paketfilterregeln (optional): Diese Funktion steht bei der

³⁹ <http://www.astaro.com/kb>

Authentifizierungsmethode *X.509 Certificate* zur Verfügung.

Sobald die IPSec-Verbindung erfolgreich aufgebaut wurde, werden die Paketfilterregeln für den Datenverkehr automatisch hinzugefügt. Beim Beenden der Verbindung, werden die Paketfilterregeln wieder entfernt.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über die IPSec-Verbindung hinzu.

3. Klicken Sie *Speichern*.

Die neue Fernzugriffsregel wird in der Liste *Verbindungen* angezeigt.

Um eine Fernzugriffsregel zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Richtlinien

Auf der Registerkarte *Remote Access >> IPSec >> Richtlinien* können Sie die Parameter für die IPSec-Verbindung definieren und in einer IPSec-Richtlinie vereinen. Eine IPSec-Richtlinie legt die Schlüsselaustausch-Methode (IKE, *Internet Key Exchange*) und die IPSec-Antragsparameter für eine IPSec-Verbindung fest. Jede IPSec-Verbindung benötigt eine IPSec-Richtlinie.

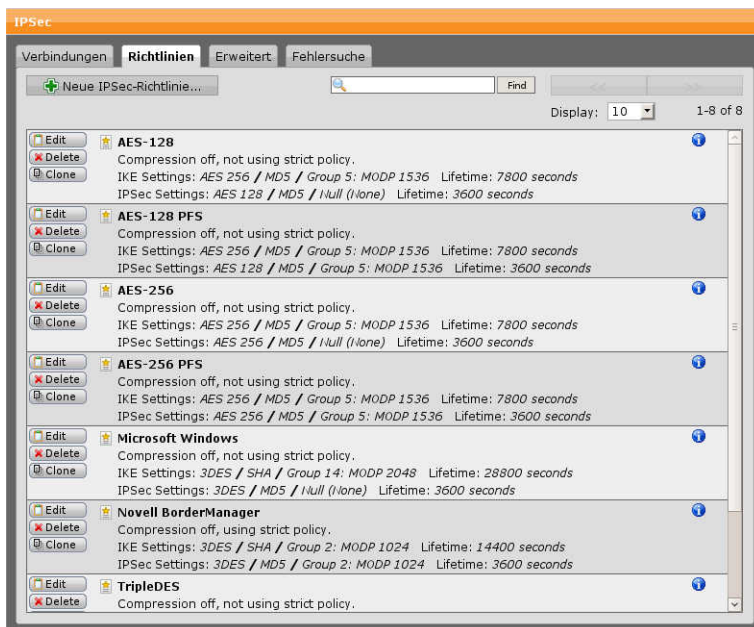


Figure 15.12 Fernzugriff IPSec: Liste der Richtlinien

Um eine IPSec-Richtlinie zu definieren, gehen Sie folgendermaßen vor:

1. **Klicken Sie auf der Registerkarte *Richtlinien* auf *Neue IPSec-Richtlinie*.**
Das Dialogfenster *IPSec-Richtlinie hinzufügen* wird geöffnet.

2. **Nehmen Sie die folgenden Einstellungen vor:**

Name: Geben Sie einen aussagekräftigen Name für ein.

IKE-Verschlüsselungsalgorithmus: Der Verschlüsselungsalgorithmus legt den Algorithmus fest, der für die Verschlüsselung der IKE-Nachrichten verwendet wird. Die folgenden Algorithmen werden unterstützt:

- *DES* (56 Bit)
- *3DES* (168 Bit)
- *AES 128* (128 Bit)
- *AES 192* (192 Bit)
- *AES 256* (256 Bit)
- *Blowfish* (128 Bit)
- *Twofish* (128 Bit)
- *Serpent* (128 Bit)

IKE-Authentifizierungsalgorithmus: Der Authentifizierungsalgorithmus legt fest, welcher Algorithmus verwendet wird, um die Intaktheit der IKE-Nachricht zu prüfen. Die folgenden Algorithmen werden unterstützt:

- *MD5* (128 Bit)
- *SHA* (160 Bit)
- *SHA-256* (256 Bit)
- *SHA-512* (512 Bit)

IKE-SA-Lebensdauer: Dieser Wert bestimmt die Zeitspanne in Sekunden, für die die IKE-SA (*Security Association*, dt. Sicherheitsverbindung) gültig ist und wann die nächste Schlüsselerneuerung stattfindet. Gültige Werte liegen zwischen 60 und 28800 Sekunden (8 Std.) möglich. Standardmäßig sind 7800 Sekunden (2 Std. 10 Min.) eingestellt.

IKE-DH-Gruppe: Während der Aushandlung einer Verbindung, gleichen

die beiden Gegenstellen auch die aktuellen Schlüssel für die Datenverschlüsselung ab. Für die Generierung des Session Key nutzt IKE den *Diffie-Hellman*-(DH)-Algorithmus. Dieser Algorithmus generiert den Schlüssel per Zufallsprinzip basierend auf sogenannten *Pool Bits*. Die IKE-Gruppe gibt hauptsächlich Aufschluss über die Anzahl der Pool Bits. Je mehr Pool Bits, umso länger ist die zufällige Zahlenkette – je größer die Zahlenkette, umso schwerer kann der Diffie-Hellman-Algorithmus geknackt werden. Folglich bedeuten mehr Pool Bits höhere Sicherheit, was allerdings auch bedeutet, dass mehr CPU-Leistung für die Generierung benötigt wird. Die folgenden DH-Algorithmen werden unterstützt:

- Gruppe 1: MODP 768
- Gruppe 2: MODP 1024
- Gruppe 5: MODP 1536
- Gruppe 14: MODP 2048
- Gruppe 15: MODP 3072
- Gruppe 16: MODP 4096

Hinweis – Gruppe 1 (MODP 768) wird allgemein als sehr schwach eingestuft und wird hier nur aus Kompatibilitätsgründen unterstützt.

IPSec-Verschlüsselungsalgorithmus: Die gleichen Verschlüsselungsalgorithmen wie für IKE.

IPSec-Authentifizierungsalgorithmus: Die gleichen Verschlüsselungsalgorithmen wie für IKE.

IPSec-SA-Lebensdauer: Dieser Wert bestimmt die Zeitspanne in Sekunden, für die die IPSec-SA (*Security Association*, dt. Sicherheitsverbindung) gültig ist und wann die nächste Schlüsselerneuerung stattfindet. Gültige Werte liegen zwischen 60 und 86400 Sekunden (1 Tag) möglich. Standardmäßig sind 7800 Sekunden (2 Std. 10 Min.) eingestellt.

IPSec-PFS-Gruppe: *Perfect Forward Secrecy* (PFS) ist eine Eigenschaft von Verschlüsselungsverfahren, die sicherstellt, dass aus einem geknackten Schlüssel nicht auf vorhergehende oder nachfolgende Sitzungsschlüssel einer Kommunikationsverbindung geschlossen werden kann. Damit PFS besteht, darf der zum Schutz der IPSec-SA-Verbindung genutzte Schlüssel nicht von dem selben zufällig erzeugten Schlüsselungsmaterial hergeleitet worden sein wie die Schlüssel für die IKE-SA-Verbindung. Daher initiiert

PFS einen zweiten Diffie-Hellman-Schlüsselaustausch mit der Absicht, dass die ausgewählte DH-Gruppe für die IPSec-Verbindung einen neuen zufällig erzeugten Schlüssel erhält. Es werden die gleichen DH-Gruppen wie bei IKE unterstützt.

Hinweis – PFS ist nicht immer gänzlich kompatibel unter den verschiedenen Herstellern. Wenn Sie Probleme während der Aushandlung feststellen, schalten Sie diese Funktion aus.

Strikte Richtlinie: Wenn ein IPSec Gateway eine Anfrage hinsichtlich eines Verschlüsselungsalgorithmus' und der Verschlüsselungsstärke unternimmt, kann es vorkommen, dass das Gateway des Empfängers diese Anfrage akzeptiert, obwohl das nicht mit der entsprechenden IPSec-Richtlinie übereinstimmt. Wenn Sie diese Option wählen und der entfernte Endpunkt nicht exakt die von Ihnen festgelegten Parameter verwenden will, kommt keine IPSec-Verbindung zustande. Angenommen die IPSec-Richtlinie Ihres Sicherheitssystems verlangt AES-256-Verschlüsselung, wohingegen ein Road Warrior mit SSH-Sentinel sich mit AES-128 verbinden will – wenn die Option *Strikte Richtlinie* aktiviert ist, wird die Verbindung abgewiesen.

Hinweis – Die Komprimierungseinstellung wird durch die Aktivierung von der Option *Strikte Richtlinie* nicht erzwungen.

Komprimierung: Diese Option legt fest, ob IP-Pakete vor der Verschlüsselung mit dem *IP Payload Compression Protocol* (IPComp) komprimiert werden sollen. IPComp reduziert die Größe von IP-Paketeten, indem es sie komprimiert, um die allgemeine Kommunikationsleistung zwischen einem Paar von kommunizierenden Rechnern oder Gateways zu erhöhen. Komprimierung ist standardmäßig ausgeschaltet.

Kommentar (optional): Fügen Sie eine Beschreibung oder sonstige Informationen über hinzu.

3. Klicken Sie *Speichern*.

Die neue IPSec-Richtlinie wird in der Liste *Richtlinien* angezeigt.

Um eine Richtlinie zu bearbeiten oder zu löschen, klicken Sie auf die entsprechenden Schaltflächen.

Erweitert

Auf der Registerkarte *Site-to-Site-VPN >> IPSec >> Erweitert* können Sie die erweiterten Einstellungen für IPSec-VPN durchführen. Abhängig von Ihrer bevorzugter Authentifizierungsmethode können Sie unter Anderem das lokale Zertifikat (für X.509-Authentifizierung) und den lokalen RSA-Schlüssel (für RSA-Authentifizierung) festlegen. Diese Einstellungen sollten nur von erfahrenen Benutzern durchgeführt werden.

The screenshot shows the 'IPSec' configuration window with the 'Erweitert' (Advanced) tab selected. The window is divided into several sections, each with a title bar, a description, and an 'Apply' button.

- Lokales X.509-Zertifikat:** A dropdown menu shows 'Local X509 Cert'. The text says: 'Bitte wählen Sie das lokale X.509-Zertifikat aus, das standardmäßig für IPSec-Verbindungen verwendet wird.'
- Dead Peer Detection (DPD):** A checkbox 'Dead Peer Detection verwenden' is checked. The text says: 'Wenn diese Option aktiviert ist, versucht das System, nicht antwortende (offline) entfernte Systeme zu erkennen.'
- NAT-Traversal (NAT-T):** A checkbox 'NAT-Traversal verwenden' is checked. Below it, 'NAT-Traversal Keep-Alive: 60 Sekunden'. The text says: 'Durch NAT-Traversal kann IPSec-Verkehr Upstream-Systeme passieren, die NAT (Network Address Translation) verwenden.'
- CRL-Handhabung:** Two checkboxes are present: 'Automatische Abholung' (unchecked) and 'Strikte Richtlinie' (unchecked). The text says: 'Diese Einstellungen definieren, wie Zertifikat-Sperrlisten (Certificate Renovation Lists) gehandhabt werden. Bei aktivierter **Automatischer Abholung** versucht das System automatisch, CRLs von entfernten Sites einzuholen.'
- Sonstige Einstellungen:** Two checkboxes are present: 'ToS-Wert (Type of Service) kopieren' (unchecked) and 'Pfad-MTU-Erkennung zulassen' (checked). Below it, 'MTU: 1420 Bytes'. The text says: 'Sie können auswählen, ob ToS-Werte in die eingebetteten Pakete kopiert werden sollen und Pfad-MTU-Erkennung zugelassen wird.'

Figure 15.13 Fernzugriff IPSec: Konfiguration der erweiterten Einstellungen

Lokales X.509-Zertifikat

Bei der X.509-Authentifizierung werden Zertifikate verwendet, um die öffentlichen Schlüssel der VPN-Endpunkte zu überprüfen. Wenn Sie diese Authenti-

fizierungsmethode verwenden wollen, müssen Sie im Abschnitt *Lokales X.509-Zertifikat* ein lokales Zertifikat aus der Auswahlliste wählen. Das ausgewählte Zertifikat bzw. Schlüssel wird anschließend dafür genutzt, um die Firewall gegenüber Gegenstellen zu authentifizieren, falls X.509-Authentifizierung ausgewählt ist.

Sie können nur Zertifikate auswählen, für die auch der zugehörige private Schlüssel vorhanden ist, andere Zertifikate sind in der Auswahlliste nicht verfügbar.

Wenn keine Zertifikate zur Auswahl angezeigt werden, müssen Sie zunächst eines im Menü *Zertifikatverwaltung* hinzufügen, entweder indem Sie ein neues erzeugen oder indem Sie eines über die Upload-Funktion importieren.

Nachdem Sie das Zertifikat ausgewählt haben, geben Sie das Kennwort ein, mit dem der private Schlüssel geschützt ist. Während des Speichervorgangs wird das Kennwort verifiziert und eine Fehlermeldung angezeigt, falls das Kennwort nicht zum verschlüsselten Schlüssel passt.

Sobald ein aktiver Schlüssel oder Zertifikat ausgewählt ist, wird er im Abschnitt *Lokales X.509-Zertifikat* angezeigt.

Dead Peer Detection (DPD)

Dead Peer Detection verwenden: Die IPSec-Verbindung wird automatisch beendet, wenn das VPN-Gateway oder der Client auf der Gegenseite nicht erreichbar ist. Bei Verbindungen mit statischen Endpunkten wird der Tunnel nach einem Ausfall automatisch neu ausgehandelt. Für Verbindungen mit dynamischen Endpunkten wird für eine neue Aushandlung des Tunnels die Anfrage seitens der Gegenstelle benötigt. In der Regel ist diese Funktion betriebssicher und kann immer eingeschaltet bleiben. Die IPSec-Partner bestimmen automatisch, ob die Gegenstelle Dead Peer Detection unterstützt oder nicht, und verwenden den normalen Modus falls nötig.

NAT-Traversal (NAT-T)

NAT-Traversal verwenden: Wählen Sie diese Option, um zu ermöglichen, dass IPSec-Verkehr Upstream-Systeme passieren kann, die *Network Address Translation* (NAT, dt. Netzwerkadressumsetzung) verwenden. Zusätzlich können Sie das Intervall für die Aufrechterhaltung (engl. *keep-alive*) für NAT-Traversal festlegen. Klicken Sie Übernehmen, um Ihre Einstellungen zu speichern.

CRL-Handhabung

Es sind Situationen denkbar, in denen ein Zertifikataussteller noch während der Gültigkeitsdauer eines Zertifikats die darin gegebene Bestätigung für ungültig erklären möchte, z. B. weil zwischenzeitlich bekannt wurde, dass das Zertifikat vom Zertifikatnehmer unter Angabe falscher Daten (Name usw.) erschlichen

wurde oder weil der zum zertifizierten öffentlichen Schlüssel gehörende private Schlüssel einem Angreifer in die Hände gefallen ist. Zu diesem Zweck werden sogenannte Zertifikatsperrlisten (CRLs, engl. *Certificate Revocation Lists*) verwendet. Diese enthalten üblicherweise die Seriennummern derjenigen Zertifikate einer Zertifizierungsinstanz, die für ungültig erklärt werden und deren regulärer Gültigkeitszeitraum noch nicht abgelaufen ist.

Nach Ablauf dieses Zeitraums besitzt das Zertifikat in jedem Fall keine Gültigkeit mehr und muss daher auch nicht weiter auf der Zertifikatsperrliste geführt werden.

Automatische Abholung: Mit der Funktion *Automatische Abholung* wird die CRL automatisch über die URL abgeholt, die im Partnerzertifikat angegeben ist, via HTTP, Anonymous FTP oder LDAP Version 3. Die CRL kann auf Anfrage heruntergeladen, abgespeichert und aktualisiert werden, sobald der Gültigkeitszeitraum abgelaufen ist. Wenn Sie diese Funktion nutzen, achten Sie darauf, dass die Paketfilterregeln so gesetzt sind, dass auf den CRL-Distributionsserver zugegriffen werden kann.

Strikte Richtlinie: Wenn Sie diese Option auswählen, werden alle Partnerzertifikate ohne eine zugehörige CRL zurückgewiesen.

Sonstige Einstellungen

ToS-Wert (Type of Service) kopieren: Type-of-Service-Bits (TOS) sind einige Vier-Bit-Flags im IP-Header. Die Bits werden *Type-of-Service-Bits* genannt, da sie es der übertragenden Anwendung ermöglichen, dem Netzwerk mitzuteilen, welche Art von Dienstqualität benötigt wird. Die folgenden Dienstqualitätsarten sind: * Minimale Verzögerung (Binärzahl: 1000)

- maximaler Durchsatz (Binärzahl: 0100)
- maximale Zuverlässigkeit (Binärzahl: 0010)
- minimale Kosten (Binärzahl: 0001)
- normaler Dienst (Binärzahl: 0000)

Mit dieser Funktion wird der Inhalt des *Type-of-Service*-Feldes in das verschlüsselte Datenpaket kopiert, so dass der IPSec-Datenverkehr entsprechend seiner Priorität geroutet werden kann.

Pfad-MTU-Erkennung zulassen: Die gesendeten IP-Datenpakete sollten so groß sein, dass sie gerade noch ohne Fragmentierung entlang der Strecke zum Ziel transportiert werden können. Diese maximale Datengröße wird als *Path Maximum Transmission Unit* (PMTU) bezeichnet. Zu große Datenpakete werden von den Routern auf der Strecke verworfen, wenn diese Pakete ohne Fragmentierung nicht weitergeleitet werden können. An die Absender werden dann

ICMP-Pakete mit der Nachricht *ICMP Destination Unreachable* (dt. ICMP-Ziel nicht erreichbar) mit einem Code der bedeutet „Fragmentierung benötigt und DF gesetzt“ gesendet. Aufgrund dieser Nachricht setzt der Quellrechner seinen angenommenen PMTU-Wert für die Strecke herab.

MTU: Tragen Sie in das Eingabefeld den Wert für die *Maximum Transmission Unit* (MTU) ein. Der voreingestellte MTU-Wert ist 1420 Byte.

Fehlersuche

Auf der Registerkarte *Fehlersuche* können Sie die Optionen für die IKE-Fehlersuche konfigurieren. Mit Hilfe der Auswahlkästchen legen Sie fest, für welche Arten von IKE-Nachrichten zusätzliche Informationen in das Fehlerprotokoll geschrieben werden. Die folgenden Flags können protokolliert werden:

- **Control:** Kontrollnachrichten zum IKE-Status
- **Emitting:** Inhalte von ausgehenden IKE-Nachrichten
- **Parsing:** Inhalte von eingehenden IKE-Nachrichten
- **Raw:** Nachrichten werden im Rohformat angezeigt
- **Crypt:** Verschlüsselungs- und Entschlüsselungsoperationen

Cisco VPN Client

Astaro Security Gateway unterstützt IPSec-Fernzugriff über Cisco VPN Client. Der Cisco VPN Client ist ein ausführbares Programm von Cisco Systems, das es ermöglicht, entfernte Computer auf sichere Weise mit einem virtuellen privaten Netzwerk (VPN, *Virtual Private Network*) zu verbinden.

Allgemein

Auf der Registerkarte *Fernzugriff* >> *Cisco VPN Client* >> *Allgemein* können Sie die grundlegenden Optionen für den Fernzugriff über Cisco VPN Client konfigurieren.

Um Astaro Security Gateway so zu konfigurieren, dass es Cisco-VPN-Client-Verbindungen zulässt, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie auf der Registerkarte *Allgemein* den Cisco VPN Client.** Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche.

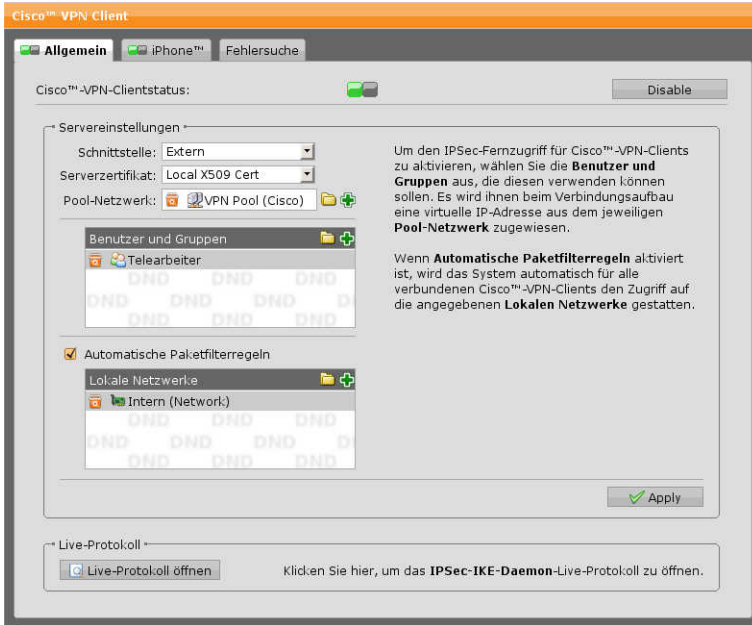


Figure 15.14 Cisco VPN Client: Konfiguration

Die Statusampel wird gelb und der Abschnitt *Servereinstellungen* kann nun bearbeitet werden.

2. Nehmen Sie die folgenden Einstellungen vor:

Schnittstelle: Wählen Sie eine Schnittstelle, die für Cisco-VPN-Client-Verbindungen verwendet werden soll.

Serverzertifikat: Wählen Sie das Zertifikat, mit dem sich der Server gegenüber dem Client identifizieren soll.

Pool-Netzwerk: Wählen Sie einen Netzwerk-Pool, dessen virtuelle Netzwerkadressen den Clients zugewiesen werden sollen, wenn sie sich verbinden. *VPN Pool (Cisco)* ist vorausgewählt.

Benutzer und Gruppen: Wählen Sie Benutzer oder Gruppen, die sich über Cisco VPN Client mit dem Sicherheitssystem verbinden dürfen.

Automatische Paketfilterregeln (optional): Wählen Sie diese Option, um automatisch Paketfilterregeln anlegen zu lassen, den den (unten) definierten Netzwerken Zugang zu den lokalen Netzwerken ermöglichen. Wenn Sie diese Option nicht wählen und keine Paketfilterregeln manuell anlegen, werden Clients von der Firewall blockiert.

Lokale Netzwerke: Wählen Sie die lokalen Netzwerke aus, für die automatischen Paketfilterregeln angelegt werden sollen. Auf diese Netzwerke

dürfen Benutzer zugreifen, die sich per Cisco VPN Client mit dem Sicherheitssystem verbinden.

3. Klicken Sie **Übernehmen**.

Ihre Einstellungen werden gespeichert.

Live-Protokoll: Verwenden Sie das Live-Protokoll, um die Verbindung-Protokolleinträge des IPSec-IKE-Daemon-Protokolls zu verfolgen. Es zeigt Informationen zum Aufbau, dem Erhalt und der Beendigung von Verbindungen an.

iPhone

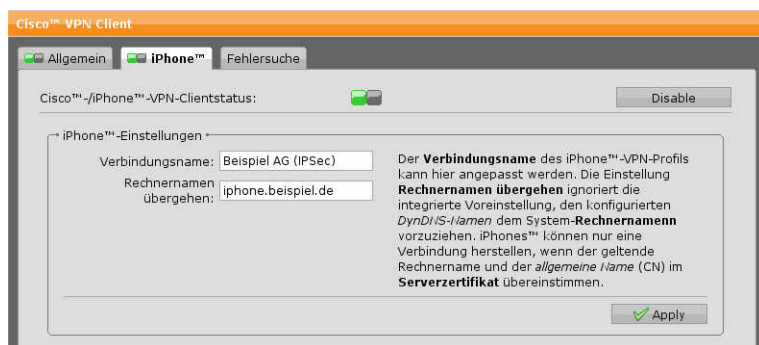


Figure 15.15 Cisco VPN Client: Konfiguration des iPhone-Fernzugriffs

Sie können ermöglichen, dass iPhone-Benutzer eine automatische Cisco IPSec-Konfiguration im Benutzerportal angeboten wird.

Allerdings werden nur Benutzer, die im Feld *Benutzer und Gruppen* auf der Registerkarte *Allgemein* aufgeführt sind, die Konfigurationsdateien auf ihrer Benutzerportal-Site finden. Der iPhone-Status ist standardmäßig aktiviert.

Verbindungsname: Geben Sie einen aussagekräftigen Namen für die Cisco IPSec-Verbindung ein, sodass iPhone-Benutzer die Verbindung identifizieren können, die sie im Begriff sind aufzubauen. Der Name Ihrer Firma gefolgt vom Protokoll Cisco IPSec ist voreingestellt.

Hinweis – Der *Verbindungsname* muss zwischen allen iPhone-Verbindungseinstellungen (PPTP, L2TP über IPSec, Cisco VPN Client) einzigartig sein.

Rechnernamen übergehen: Im Falle, dass der Systemrechnernamen vom Client nicht öffentlich aufgelöst werden kann, können Sie hier einen Server-Rechnernamen eingeben, der die interne Präferenz übergeht, bei der der *DynDNS-Rechnernamen* dem *Systemrechnernamen* vorgezogen wird.

Um die automatische iPhone-Konfiguration auszuschalten, klicken Sie auf die Statusampel oder *Disable* oben auf der Registerkarte.

Die Statusampel wird rot.

Beachten Sie, dass iPhones, die sich verbinden, das Serverzertifikat gezeigt wird, das auf der Registerkarte *Allgemein* definiert ist. Das iPhone überprüft, ob die VPN-ID dieses Zertifikats mit dem Server-Rechnernamen übereinstimmt, und lehnt eine Verbindung ab, wenn es keine Übereinstimmung gibt. Wenn das Serverzertifikat einen *Distinguished Name* als VPN-ID verwendet, vergleicht das iPhone den Server-Rechnernamen stattdessen mit dem Feld *Allgemeiner Name* (*Common Name*). Sie sollten sicherstellen, dass das Server-Zertifikat diese Bedingungen erfüllt.

Fehlersuche

Auf der Registerkarte *Fehlersuche* können Sie die Optionen für die IKE-Fehlersuche konfigurieren. Mit Hilfe der Auswahlkästchen legen Sie fest, für welche Arten von IKE-Nachrichten zusätzliche Informationen in das Fehlerprotokoll geschrieben werden. Die folgenden Flags können protokolliert werden:

- **Control:** Kontrollnachrichten zum IKE-Status
- **Emitting:** Inhalte von ausgehenden IKE-Nachrichten
- **Parsing:** Inhalte von eingehenden IKE-Nachrichten
- **Raw:** Nachrichten werden im Rohformat angezeigt
- **Crypt:** Verschlüsselungs- und Entschlüsselungsoperationen

Erweitert

Auf der Seite *Fernzugriff >> Erweitert* können Sie die erweiterten Einstellungen für die Fernzugriff-Clients durchführen. Die IP-Adressen der DNS- und WINS-Server, die Sie hier angeben, werden für die Benutzung durch Fernzugriff-Clients während des Verbindungsaufbaus mit der Firewall zur Verfügung gestellt, wodurch eine vollständige Namensauflösung für Ihr System gewährleistet wird.

Figure 15.16 Fernzugriff: Erweiterte Einstellungen

DNS-Server: Sie können bis zu zwei DNS-Server für Ihr Unternehmen definieren.

WINS-Server: Sie können bis zu zwei WINS-Server für Ihr Unternehmen definieren.

Der *Windows Internet Naming Service* (WINS, dt. Windows Internet Namensdienst) ist Microsofts Implementierung des *NetBIOS Name Server* (NBNS) für Windows Betriebssysteme. Unter dem Strich macht WINS für NetBIOS-Namen das, was DNS für Domännennamen macht: einen zentralen Abgleich zwischen Rechnernamen und IP-Adressen.

Domänenname: Tragen Sie den *Fully Qualified Domain Name* (FQDN) Ihres Unternehmens ein. Dies ist ein eindeutiger Domänenname, der in einer DNS-Baumstruktur die absolute Position des Knotens spezifiziert (z. B. `intranet.example.com`).

Hinweis – Der Domänenname kann nur automatisch an den Fernzugriff-Client während des Verbindungsaufbaus mit SSL verteilt werden. Bei IPsec hingegen wird der Domänenname in die Konfigurationsdatei des Astaro Secure Clients geschrieben. Diese Konfigurationsdatei muss manuell in den Client importiert werden. Bei PPTP und L2TP über IPsec kann der Domänenname *nicht* automatisch verteilt werden – er muss auf dem Client manuell konfiguriert werden.

Zertifikatverwaltung

Über das Menü *Fernzugriff >> Zertifikatverwaltung*, das dieselben Konfigurationsoptionen enthält wie das Menü *Site-to-Site-VPN >> Zertifikatverwaltung*, können Sie alle zertifikatsbezogenen Vorgänge verwalten. Das beinhaltet unter Anderem das Anlegen und Importieren von X.509-Zertifikaten ebenso wie das Hochladen sogenannter Zertifikatssperrlisten (CRLs).

Zertifikate

Wechseln Sie zu *Site-to-Site-VPN >> Zertifikatverwaltung >> Zertifikate*.

Zertifizierungsstelle

Wechseln Sie zu *Site-to-Site-VPN >> Zertifikatverwaltung >> Zertifizierungsstelle*.

Sperrlisten

Wechseln Sie zu *Site-to-Site-VPN >> Zertifikatverwaltung >> Sperrlisten (CRLs)*.

Erweitert

Wechseln Sie zu *Site-to-Site-VPN >> Zertifikatverwaltung >> Erweitert*.

Protokollierung

In diesem Kapitel wird beschrieben, wie Sie die Protokollfunktionen (engl. *Logging*) von Astaro Security Gateway konfigurieren.

Astaro Security Gateway bietet umfangreiche Protokollfunktionen, indem es die verschiedenen Ereignisse betreffend den Schutz des Systems und des Netzwerks dauernd überwacht. Aufgrund der detaillierten historischen Informationen und den aktuellen Analysen der verschiedenen Netzwerkaktivitäten können potenzielle Sicherheitsbedrohungen identifiziert oder aufkommende Probleme verhindert werden.

Die Seite *Protokollpartitionsstatus* in WebAdmin zeigt den aktuellen Status der Protokoll-Partition auf Astaro Security Gateway an. Die Übersicht liefert folgende Informationen: Den verbleibenden Speicherplatz auf der Protokoll-Partition, die durchschnittliche Speicherrate (in MB/Tag), die verbleibende Zeit (in Tagen) bis die Partition voll ist und eine Analyse der Protokoll-Partitionsauslastung für einen Zeitraum über vier Wochen. Für die Berechnung der durchschnittlichen Füllrate wird das aktuelle Datenvolumen durch die verstrichene Zeit dividiert – die Angaben sind daher zu Beginn etwas ungenau. Sie werden genauer, je länger das System aktiv ist.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- Einstellungen
- Protokolldatei-Ansicht

Einstellungen

Im Menü *Protokollierung* >> *Einstellungen* können Sie die Grundeinstellungen für die lokale und die entfernte Protokollierung (engl. *remote logging*) durchführen.

Lokale Protokollierung

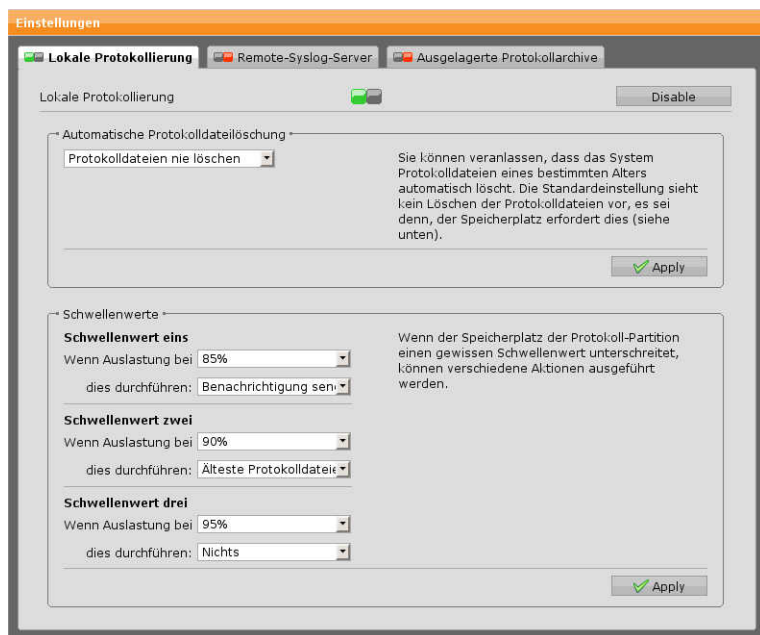


Figure 16.1 Protokollierung: Lokale Protokollierung einschalten

Auf der Registerkarte *Protokollierung* >> *Einstellungen* >> *Lokale Protokollierung* werden die Einstellung für die lokale Protokollierung (engl. *local logging*) durchgeführt. Diese Funktion ist standardmäßig eingeschaltet. Falls es deaktiviert wurde, können Sie es folgendermaßen wieder einschalten:

1. **Aktivieren Sie auf der Registerkarte *Lokale Protokollierung* die Funktion *Lokale Protokollierung*.**
Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche. Die Statusampel wird grün und der Abschnitt *Automatische Protokolldateilöschung* kann nun bearbeitet werden.
2. **Wählen Sie eine Zeitspanne, nach der die Protokolldateien automatisch gelöscht werden sollen.**
Wählen Sie aus der Auswahlliste, welche Aktion automatisch auf die Protokolldateien angewendet werden soll. *Protokolldateien nie löschen* ist voreingestellt.
3. **Klicken Sie *Übernehmen*.**
Ihre Einstellungen werden gespeichert.

Schwellenwerte

Hier können Sie Schwellenwerte für die lokale Protokollierung festlegen. Diese Schwellenwerte sind an bestimmte Aktionen gekoppelt, welche ausgeführt werden, wenn ein Schwellenwert erreicht ist. Sie können zwischen den folgenden Aktionen wählen:

- **Nichts:** Es werden keine Aktionen gestartet.
- **Benachrichtigung senden:** Es wird eine Benachrichtigung an den Administrator gesendet, die ihm mitteilt, dass der Schwellenwert erreicht wurde.
- **Älteste Protokolldateien löschen:** Die ältesten Protokolldateien werden automatisch gelöscht bis die Datenmenge entweder unterhalb des eingestellten Schwellenwerts liegt oder bis die Protokoll-Partition leer ist. Zusätzlich erhält der Administrator eine Benachrichtigung über das Ereignis.
- **System herunterfahren:** Das System fährt automatisch herunter. Der Administrator erhält eine Benachrichtigung über das Ereignis.

Falls das System heruntergefahren wird, muss der Administrator die Konfiguration für die lokale Protokollierung ändern, die Löschung von Protokolldateien konfigurieren oder Protokolldateien manuell wegbewegen beziehungsweise löschen. Wenn die Ursache für das Herunterfahren des Systems weiterhin besteht, wird sich das System wieder herunterfahren, sobald der Prozess der Protokollüberprüfung das nächste Mal läuft. Dieser Prozess findet täglich um 0:00 Uhr statt. Klicken Sie *Übernehmen*, um Änderungen zu speichern.

Remote-Syslog-Server

Auf der Registerkarte *Protokollierung >> Einstellungen >> Remote Syslog Server* können Sie die Einstellungen für eine ausgelagerte Protokollierung durchführen. Diese Funktion ermöglicht es, Protokollmeldungen von der Firewall zu anderen Rechnern weiterzuleiten. Das ist insbesondere nützlich in Netzwerken, die einen dedizierten Rechner besitzen, der die Protokollinformationen von mehreren Firewalls sammelt. Auf dem ausgewählten Server muss in diesem Fall ein Protokollierungs-Daemon in Betrieb sein, der mit dem Syslog-Protokoll kompatibel ist.

Um einen Remote-Syslog-Server zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie auf der Registerkarte *Remote Syslog Server* die Funktion *Remote Syslog*.**



Figure 16.2 Protokollierung: Konfiguration eines Remote-Syslog-Servers

Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche. Die Statusampel wird gelb und der Abschnitt *Remote-Syslog-Einstellungen* kann nun bearbeitet werden.

2. Nehmen Sie die folgenden Einstellungen vor:

Rechner: Wählen Sie den Server aus, auf dem die Protokolldaten der Firewall gesammelt werden sollen.

Warnung – Wählen Sie keine Netzwerkkarte des Systems aus, um sie als Remote-Syslog-Rechner zu verwenden – das würde zu einer Protokollschleife führen.

Dienst: Das Syslog-Protokoll ist voreingestellt.

3. Klicken Sie **Übernehmen**.

Ihre Einstellungen werden gespeichert.

Remote-Syslog-Protokollauswahl

Dieser Abschnitt kann nur bearbeitet werden, wenn die Funktion *Remote Syslog* aktiviert ist. Wählen Sie über die Auswahlkästchen die Protokolle aus, die an den Syslog-Server geschickt werden sollen. Klicken Sie **Übernehmen**, um Ihre Einstellungen zu speichern.

Ausgelagerte Protokollarchive

Auf der Registerkarte *Protokollierung >> Einstellungen >> Ausgelagerte Protokollarchive* können Sie die Einstellungen für eine ausgelagerte Archivierung der Protokolldaten durchführen. Wenn die ausgelagerte Protokolldatei-Archivierung aktiviert ist, werden die Protokolldateien des Vortages in einer Datei zusammengepackt und komprimiert, welche dann an den entfernten Protokollarchiv-Rechner gesendet werden.

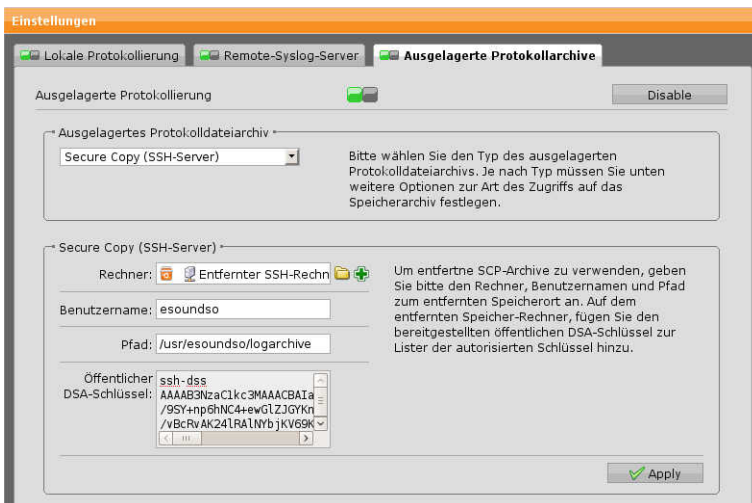


Figure 16.3 Protokollierung: Konfiguration eines ausgelagerten Protokollarchivs

Um ein ausgelagertes Protokollarchiv zu konfigurieren, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie die Funktion *Ausgelagerte Protokollierung*.**

Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche. Die Statusampel wird gelb und der Abschnitt *Ausgelagertes Protokolldateiarchiv* kann nun bearbeitet werden.

2. **Stellen Sie die Archivierungsmethode ein.**

Wählen Sie aus der Auswahlliste Ihre bevorzugte Archivierungsmethode aus. Abhängig von Ihrer Wahl, werden unten die zugehörigen Konfigurationsoptionen angezeigt. Sie können zwischen den folgenden Archivierungsmethoden wählen:

- **FTP-Server:** Für das *File Transfer Protocol* (FTP, *Dateiübertragungsprotokoll*) müssen die folgenden Parameter gesetzt werden:
 - *Rechner*: Wählen Sie die Rechnerdefinition für den FTP-Server aus.
 - *Dienst*: Wählen Sie den TCP-Port aus, auf dem der Server lauscht.
 - *Benutzername*: Tragen Sie den Benutzernamen für das FTP-Serverkonto ein.
 - *Kennwort*: Tragen Sie das Kennwort für das FTP-Serverkonto ein.
 - *Pfad*: Tragen Sie den relativen Pfad zum FTP-Server sein.
- **SMB-(CIFS)-Freigabe:** Für die SMB-Methode müssen die folgenden Parameter gesetzt werden:
 - *Rechner*: Wählen Sie die Rechnerdefinition für den SMB-Server aus.
 - *Benutzername*: Tragen Sie den Benutzernamen für das SMB-Konto ein.
 - *Kennwort*: Tragen Sie das Kennwort für das SMB-Konto ein.
 - *Freigabe*: Tragen Sie den SMB-Freigabenamen ein.
 - *Arbeitsgruppe/Domäne*: Geben Sie die Arbeitsgruppe oder Domäne an, zu der das Protokollarchiv gehört.
- **Secure Copy (SSH-Server):** Für die SCP-Methode muss der öffentliche SSH-DSA-Schlüssel zu den autorisierten Schlüsseln des SCP-Servers hinzugefügt werden. Auf einem Linux-System können Sie den SSH-DSA-Schlüssel einfach über die Zwischenablage in die Datei `~/.ssh/authorized_keys` des dafür konfigurierten Benutzerkontos

kopieren. Astaro Security Gateway erzeugt während der Installation einen neuen SSH-DSA-Schlüssel an. Aus Sicherheitsgründen wird dieser Schlüssel nicht in den Backups enthalten. Nach einer Neuinstallation oder wenn ein Backup installiert wird, müssen Sie daher den neuen SSH-DSA-Schlüssel auf den SCP-Server kopieren werden, damit die Protokolldateiarchive auf den SCP-Server kopiert werden können.

Für die SCP-Methode müssen die folgenden Parameter gesetzt werden:

- *Rechner*: Wählen Sie die Rechnerdefinition für den SCP-Server aus.
 - *Benutzername*: Tragen Sie den Benutzernamen für das SCP-Serverkonto ein.
 - *Pfad*: Tragen Sie den vollständigen Pfad ein, wo die Protokolldateien gespeichert werden sollen.
 - *Öffentlicher DSA-Schlüssel*: Fügen sie den öffentlichen DSA-Schlüssel zur Liste der autorisierten Schlüssel auf dem entfernten Speicher-Rechner hinzu.
- **Per E-Mail senden**: Damit die Protokollarchive per E-Mail versendet werden, geben Sie eine gültige Empfänger-E-Mailadresse ein.

3. Klicken Sie **Übernehmen**.

Ihre Einstellungen werden gespeichert.

Wenn die Datenübertragung fehlschlägt, verbleibt die Archivdatei auf der Firewall. Die Firewall versucht bei jeder Protokollüberprüfung alle verbliebenen Archivdateien zu übertragen.

Protokolldatei-Ansicht

Im Menü *Protokollierung* >> *Protokolldatei-Ansicht* können alle verschiedenen Protokolldateien angesehen werden. Es ist auch möglich, über die Protokolldateien eine Suche auszuführen.

Heutige Protokolldateien

Auf der Registerkarte *Protokollierung* >> *Protokolldatei-Ansicht* >> *Heutige Protokolldateien* können alle aktuellen Protokolldateien (engl. *log files*) einfach eingesehen werden.

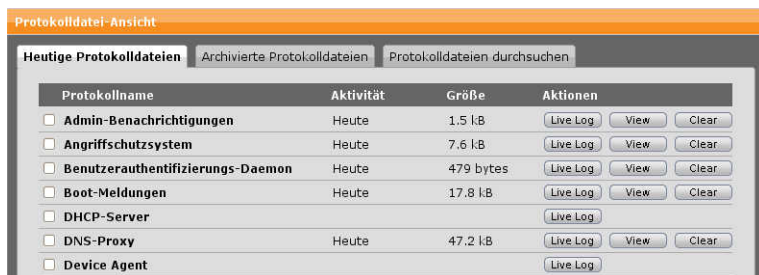


Figure 16.4 Protokollierung: Protokollübersicht

Diese Registerkarte bietet außerdem einige Aktionen, die auf alle Protokolldateien angewendet werden können. Die folgenden Aktionen sind verfügbar:

- **Live Log:** Ein Klick auf diese Schaltfläche öffnet ein neues Fenster, in dem Sie das Protokoll in Echtzeit mitverfolgen können. Neue Zeilen kommen automatisch hinzu. Wenn die Funktion *Autoscroll* eingeschaltet ist, werden immer die aktuellsten Einträge so angezeigt, dass die letzte Zeile sichtbar ist. Mit der Funktion *Filter* können Sie neue Protokolleinträge begrenzen, so dass nur jene Einträge angezeigt werden, die mit dem Ausdruck im Filter übereinstimmen.
- **View:** Im Dialogfenster wird der aktuelle Stand des Protokolls angezeigt.
- **Clear:** Der Inhalt der Protokolldatei wird gelöscht.

Mit der Auswahlliste unterhalb der Tabelle können Sie vorher ausgewählte Protokolldateien entweder als zip-Datei herunterladen oder ihre Inhalte gleichzeitig löschen.

Hinweis – Um Problemen beim Herunterladen von Dateien mit dem Internet Explorer 6 vorzubeugen, fügen Sie die URL der Firewall (z.B. <https://192.168.2.100>) und des Benutzerportals (z.B. <https://192.168.2.100>) den *Vertrauenswürdigen Sites* hinzu. Beim Internet Explorer 6 befinden sich diese Einstellungen im Menü *Extras >> Internetoptionen >> Sicherheit*. Beim Internet Explorer 7 aktivieren Sie zusätzlich im Fenster *Sicherheitseinstellungen* die Funktion *Automatische Eingabeaufforderung für Dateidownloads*.

Archivierte Protokolldateien

Auf der Registerkarte *Protokollierung* >> *Protokolldatei-Ansicht* >> *Archivierte Protokolldateien* wird das Protokolldateiarchiv verwaltet. Alle Protokoll-dateien werden tageweise archiviert. Um eine bestimmte Protokolldatei zu öff-nen, wählen Sie in der Auswahlliste ein Teilsystem von Astaro Security Gate-way aus, für das ein Protokoll geführt wurde, sowie ein Jahr und einen Monat.

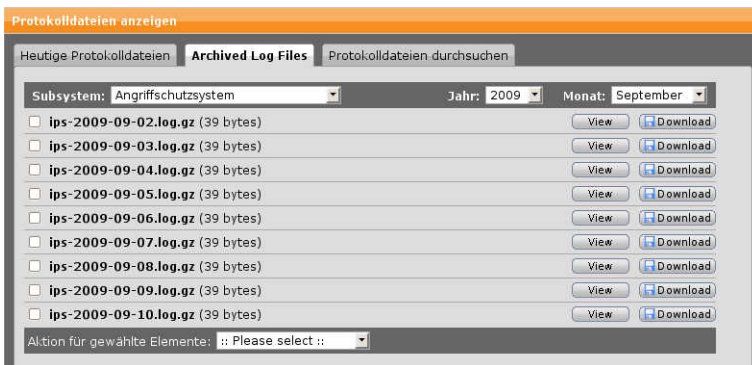


Figure 16.5 Protokollierung: Auswahl von archivierten Protokolldateien

Alle verfügbaren Protokolldateien, die Ihrer Auswahl entsprechen, werden in chronologischer Reihenfolge angezeigt. Die Protokolle können angeschaut werden oder als Datei im zip-Format heruntergeladen werden.

Mit der Auswahlliste unterhalb der Tabelle können Sie vorher ausgewählte Protokolldateien entweder als zip-Datei herunterladen oder ihre Inhalte gleichzeitig löschen.

Hinweis – Um Problemen beim Herunterladen von Dateien mit dem Internet Explorer 6 vorzubeugen, fügen Sie die URL der Firewall (z.B. <https://192.168.2.100>) und des Benutzerportals (z.B. <https://192.168.2.100>) den *Vertrauenswürdigen Sites* hinzu. Beim Internet Explorer 6 befinden sich diese Einstellungen im Menü *Extras* >> *Internetoptionen* >> *Sicherheit*. Beim Internet Explorer 7 aktivieren Sie zusätzlich im Fenster *Sicherheitseinstellungen* die Funktion *Automatische Eingabeaufforderung für Dateidownloads*.

Protokolldateien durchsuchen

Auf der Registerkarte *Protokollierung* >> *Protokolldatei-Ansicht* >> *Protokolldateien durchsuchen* kann das lokale Protokolldateiarchiv für verschiedene Zeiträume durchsucht werden. Wählen Sie zunächst eine Protokolldatei, die Sie durchsuchen wollen. Geben Sie dann einen Suchbegriff ein und wählen Sie einen Zeitraum. Wenn Sie *Benutzerdefinierter Zeitraum* unter *Zeitraum* auswählen, können Sie ein Start- und Enddatum angeben. Nachdem Sie auf die Schaltfläche *Suche starten* geklickt haben, wird ein neues Fenster geöffnet, in dem die Ergebnisse Ihrer Suche angezeigt werden. Abhängig von Ihrem Browser, kann es nötig sein, Pop-Up-Fenster für WebAdmin zu erlauben.

The screenshot shows a web application window titled 'Protokolldatei-Ansicht'. It has three tabs: 'Heutige Protokolldateien', 'Archivierte Protokolldateien', and 'Protokolldateien durchsuchen'. The third tab is active. Below the tabs is a section titled 'Protokolldateien abfragen'. It contains a paragraph of instructions: 'Sie können Protokolldateien mit diesem Formular durchsuchen. Wählen Sie das Teilsystem und einen Zeitraum aus und geben Sie die Zeichenfolge ein, nach der Sie suchen. Es wird ein Popup-Fenster mit den Ergebnissen angezeigt. Sie können mehrere Fenster gleichzeitig öffnen.' Below this are several input fields: 'Zu suchende Protokolldatei auswählen:' with a dropdown menu showing 'Paketfilter'; 'Suchbegriff:' with a text input field; 'Zeitraum auswählen:' with a dropdown menu showing 'Benutzerdefinierter Zeitraum'; 'Benutzerdefiniertes Startdatum:' with three dropdown menus showing '1', 'September', and '2008'; and 'Benutzerdefiniertes Enddatum:' with three dropdown menus showing '11', 'September', and '2009'. At the bottom right of the form is a button labeled 'Suche starten'.

Figure 16.6 Protokollierung: Protokolldateien durchsuchen

Berichte

Die Berichtsfunktion von Astaro Security Gateway bietet System- und Netzwerkinformationen in Echtzeit. Dabei werden die Informationen aus den Protokolldateien gesammelt und in Diagrammen und Tabellen dargestellt.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- Einstellungen
- Hardware
- Netzwerknutzung
- Network Security
- Web Security
- Mail Security
- Gesamtbericht

Einstellungen

Im Menü *Berichte* > > *Einstellungen* können Sie die Einstellungen für Berichtsfunktionen vornehmen, wie das Ein- und Ausschalten bestimmter Berichtsfunktionen, das Bestimmen von Zeiträumen und Menge für zu speichernde Daten. Des Weiteren können Sie Daten anonymisieren, um den Datenschutz zu verbessern.

Einstellungen

Die Registerkarte *Einstellungen* ermöglicht Ihnen, den Umgang mit Berichtsdaten zu regeln und festzulegen, wie lange Berichtsdaten auf dem System gespeichert werden, bevor sie automatisch gelöscht werden. Einstellungen für die folgenden Themenbereiche können vorgenommen werden:

- Netzwerkstatistik (auch *Accounting*)
- Authentifizierung

- Mail Security
- IM/P2P
- IPS
- Paketfilter
- Web Security

Verwenden Sie die Auswahlkästchen auf der linken Seite, um die Berichtsfunktion für einen bestimmten Themenbereich ein- oder auszuschalten. Standardmäßig ist die Berichtsfunktion für alle Themenbereiche eingeschaltet.

Verwenden Sie die Auswahlliste auf der rechten Seite, um festzulegen, wie lange die Berichtsdaten aufbewahrt werden sollen.

Hinweis – Das Ausschalten unnötiger Berichtsfunktionen senkt die Grundbelastung des Systems und reduziert Leistungseingpässe. Versuchen Sie, die Zeiträume so kurz wie möglich zu halten, da große Mengen gespeicherter Daten eine höhere Grundbelastung des Systems bedeuten und verschlechterte Antwortzeiten auf den dynamischen Berichtsseiten.

Die Einstellungen auf dieser Registerkarte wirken sich nicht auf die Protokoll-dateiarchive aus.

Einstellungen für Gesamtbericht

In diesem Abschnitt können Sie jeweils die Anzahl an Gesamtberichten festlegen, die aufbewahrt werden soll:

- Tägliche Berichte: Maximal 60
- Wöchentliche Berichte: Maximal 52
- Monatliche Berichte: Maximal 12

Klicken Sie *Übernehmen*, um Ihre Änderungen zu speichern.

Weitere Information zum Gesamtbericht (engl. *Executive Report*) und seine Optionen finden Sie unter *Berichte >> Gesamtbericht*.

PDF-Papiereinstellungen

Das voreingestellte Papierformat für den PDF-Gesamtbericht ist A4. Sie können die Auswahlliste verwenden, um alternativ *Letter* oder *Legal* zu wählen. Klicken Sie *Übernehmen*, um Ihre Änderungen zu speichern.

Ausnahmen

Über die Registerkarte *Einstellungen* >> *Ausnahmen* können Sie bestimmte Domänen und Adressen von der Berichterstellung ausnehmen. Das betrifft sowohl den Gesamtbericht als auch die jeweiligen Abschnitte *Berichte*. Sie können Ausnahmen für die folgenden Berichte festlegen:

- Web Security: Domänen
- Mail Security: Domänen und Adressen
- Network Security: IP-Adressen

Definieren Sie die Ausnahmen im jeweiligen Feld und klicken Sie *Übernehmen*. Beachten Sie die Import-Funktion, mit der Sie mehrere Einträge auf einmal definieren können.

Anonymisierung

Die Registerkarte *Einstellungen* >> *Anonymisierung* ermöglicht Ihnen, Daten – basierend auf dem Vier-Augen-Prinzip – zu anonymisieren. Das bedeutet, dass eine Entanonymisierung nur möglich ist, wenn zwei verschiedene Leute dieses Vorgehen beschließen.

Anonymisierung stellt sicher, dass Benutzerdaten nicht offen gelegt werden, wenn Protokoll- und Berichtsdaten eingesehen werden. Dadurch können Aktionen (wie z. B. Surfverhalten) nicht auf eine bestimmte Person zurückverfolgt werden.

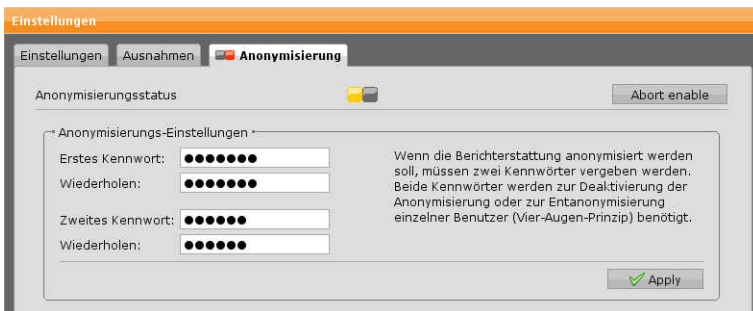


Figure 17.1 Berichte: Aktivierung der Anonymisierung von Benutzerdaten

Um Anonymisierung zu verwenden, gehen Sie folgendermaßen vor:

1. **Aktivieren Sie auf der Registerkarte *Anonymisierung* die Anonymisierungsfunktion.**

Sie können entweder auf die Statusampel klicken oder auf die *Enable*-Schaltfläche.

Die Statusampel wird gelb und der Abschnitt *Anonymisierungseinstellungen* kann nun bearbeitet werden.

2. **Geben Sie zwei Sicherheitskennwörter.**

Das Vier-Augen-Prinzip ist nur gewährleistet, wenn zwei verschiedene Personen ein Kennwort eingeben, das der jeweils anderen Person unbekannt ist.

3. **Klicken Sie *Übernehmen*.**

Ihre Einstellungen werden gespeichert.

Um Anonymisierung (global) wieder zu deaktivieren, sind beide Kennwörter erforderlich.

1. **Klicken Sie auf der Registerkarte *Anonymisierung* entweder *Disable* oder auf die Statusampel.**

Die Statusampel wird gelb und der Abschnitt *Anonymisierungseinstellungen* kann nun bearbeitet werden.

2. **Geben Sie beide Kennwörter ein.**

Geben Sie das erste und zweite Kennwort ein, die verwendet wurden, um Anonymisierung zu aktivieren.

3. **Klicken Sie *Übernehmen*.**

Ihre Einstellungen werden gespeichert.

Falls nötig kann die Anonymisierung für einzelne Benutzer aufgehoben werden. Weitere Informationen hierzu finden Sie unter *Berichte >> Web Security* und *Berichte >> Mail Security*.

Hardware

Im Menü *Berichte* >> *Hardware* werden die Auslastung der verschiedenen Hardware-Komponenten über einen bestimmten Zeitraum angezeigt.

Täglich

Auf der Registerkarte *Täglich* wird eine Statistik über die letzten 24 Stunden für die folgenden Hardware-Komponenten angezeigt:

- CPU Usage: CPU-Auslastung
- Memory/Swap Usage: Speicher- bzw. Swap-Auslastung
- Partition Usage: Speicherplatzbelegung der verschiedenen Partitionen

CPU Usage: Das Diagramm zeigt die aktuelle Auslastung des Prozessors in Prozent an.

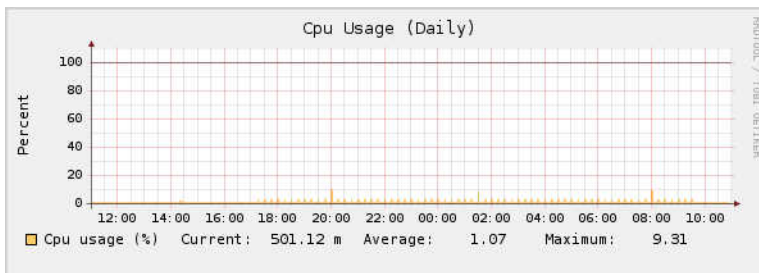


Figure 17.2 Berichte: Diagramm über die CPU-Auslastung

Memory/Swap Usage: Das Diagramm zeigt die aktuelle Auslastung von Speicher und Swap in Prozent. Die Swap-Auslastung hängt stark von Ihrer Systemkonfiguration ab. Die Aktivierung von Systemdiensten wie Intrusion Prevention oder den Proxy-Servern führen zu einer höheren Speicherauslastung. Wenn kein freier Hauptspeicher mehr zur Verfügung steht, erfolgt der Zugriff auf den virtuellen Speicher (Swap), wodurch sich die gesamte Leistungsfähigkeit des Systems verschlechtert. Die Nutzung von Swap sollte so gering wie möglich sein. Um das zu erreichen, sollten Sie wenn nötig den verfügbaren Hauptspeicher erhöhen.

Partition Usage: Die Diagramme zeigen die Belegung der verschiedenen Festplattenpartitionen in Prozent, wobei jede Partition durch einen eigenen Graph dargestellt wird:

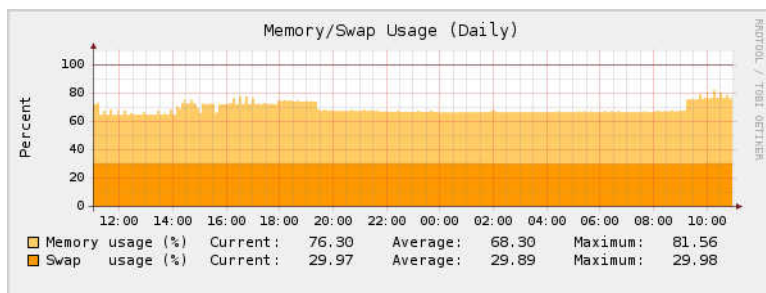


Figure 17.3 Berichte: Diagramm über die Speicher-/Swap-Auslastung

- **Root:** Die Auslastung der Root-Partition, wo sich das Root-Verzeichnis von Astaro Security Gateway befindet. Hier werden auch die Update-Pakete und Backups gespeichert.
- **Log:** Die Auslastung der Protokoll-Partition, wo die Protokolldateien und Berichtsdaten gespeichert werden. Falls die Auslastung kritisch wird, passen Sie bitte auf der Registerkarte *Protokollierung* >> *Einstellungen* >> *Lokale Protokollierung* die Einstellungen an.
- **Storage:** Die Auslastung der Speicherpartition, wo die Proxy-Dienste ihre Daten abspeichern, z. B. Bilder für den HTTP-Proxy, Meldungen für den SMTP-Proxy, E-Mails in Quarantäne usw.

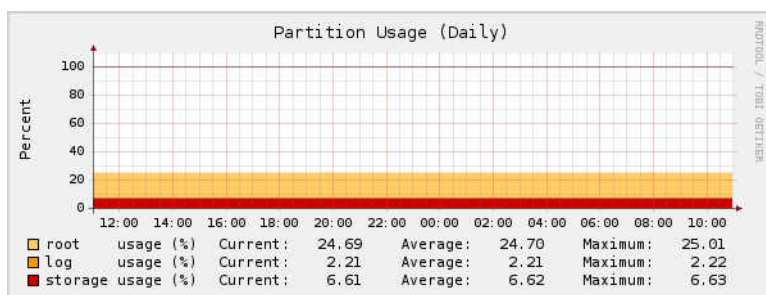


Figure 17.4 Berichte: Diagramm über die Auslastung der Speicherpartition

Wöchentlich

Auf der Registerkarte *Wöchentlich* werden die statistischen Übersichten für die letzten sieben Tage dargestellt. Die Diagramme werden auf der Seite „Täglich“ beschrieben.

Monatlich

Auf der Registerkarte *Monatlich* wird eine Statistik über die letzten vier Wochen für die Hardware-Komponenten angezeigt. Die Diagramme werden auf der Seite „Täglich“ beschrieben.

Jährlich

Auf der Registerkarte *Jährlich* wird eine Statistik über die letzten zwölf Monate für die Hardware-Komponenten angezeigt. Die Diagramme werden auf der Seite „Täglich“ beschrieben.

Netzwerknutzung

Die Registerkarten unter *Berichte* >> *Netzwerknutzung* bieten einen statistischen Überblick für verschiedene Zeiträume über den Datenverkehr, der jede Schnittstelle von Astaro Security Gateway passiert. In den Diagrammen wird der eingehende und ausgehende Datenverkehr in separaten Kurven angezeigt. Zur Darstellung werden die folgenden Maßeinheiten verwendet:

- u (Micro, $10e^{-6}$)
- m (Milli, $10e^{-3}$)
- k (Kilo, $10e^3$)
- M (Mega, $10e^6$)
- G (Giga, $10e^9$)

Beachten Sie, dass die Skalierung zwischen $10e^{-18}$ und $10e^8$ variiert.

Täglich

Auf der Registerkarte *Netzwerknutzung* >> *Täglich* wird für jede konfigurierte Schnittstelle der Datendurchsatz der letzten 24 Stunden angezeigt.

Jedes Diagramm enthält zwei grafische Darstellungen:

- **Inbound:** Eingehender Datenverkehr auf dieser Schnittstelle in Bits pro Sekunde.
- **Outbound:** Ausgehender Datenverkehr auf dieser Schnittstelle in Bits pro Sekunde.

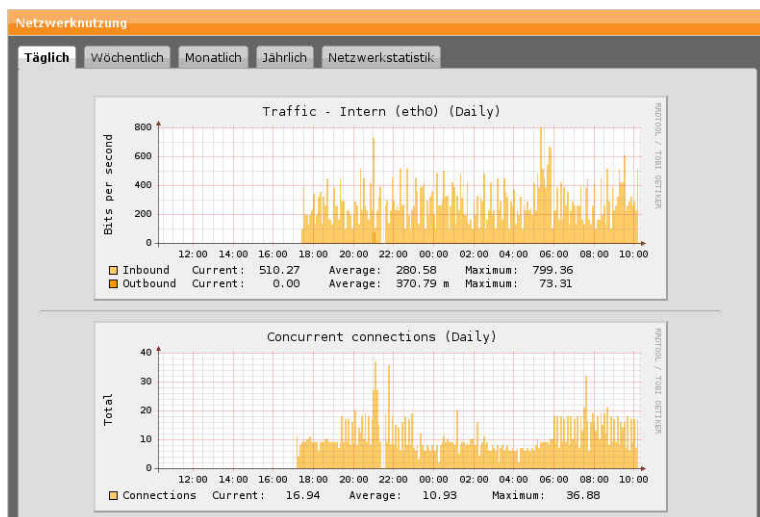


Figure 17.5 Berichte: Diagramm über den Datendurchsatz einer Ethernet-Schnittstelle

Das Diagramm *Concurrent Connections* (dt. gleichzeitige Verbindungen) zeigt die Summe der gleichzeitigen Verbindungen.

Wöchentlich

Auf der Registerkarte *Netzwerknutzung* >> *Wöchentlich* werden zu den einzelnen konfigurierten Schnittstellen die Datendurchsatzraten der letzten sieben Tage dargestellt. Die Diagramme werden auf der Seite „Täglich“ beschrieben.

Monatlich

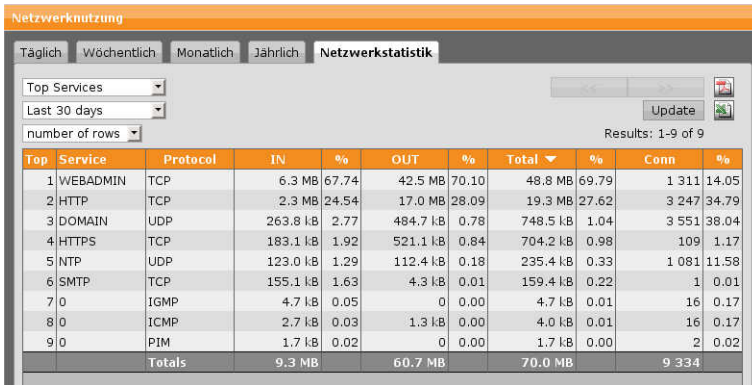
Auf der Registerkarte *Netzwerknutzung* >> *Monatlich* werden zu den einzelnen konfigurierten Schnittstellen die Datendurchsatzraten der letzten vier Wochen dargestellt. Die Diagramme werden auf der Seite „Täglich“ beschrieben.

Jährlich

Auf der Registerkarte *Netzwerknutzung* >> *Jährlich* werden zu den einzelnen konfigurierten Schnittstellen die Datendurchsatzraten der letzten 12 Monate dargestellt. Die Diagramme werden auf der Seite „Täglich“ beschrieben.

Netzwerkstatistik

Die Registerkarte *Netzwerknutzung* >> *Netzwerkstatistik* enthält umfangreiche statistische Angaben zu jeglichem Datenverkehr, der an, von und durch das System gesendet wurde.



Top	Service	Protocol	IN	%	OUT	%	Total	%	Conn	%
1	WEBADMIN	TCP	6.3 MB	67.74	42.5 MB	70.10	48.8 MB	69.79	1 311	14.05
2	HTTP	TCP	2.3 MB	24.54	17.0 MB	28.09	19.3 MB	27.62	3 247	34.79
3	DOMAIN	UDP	263.8 kB	2.77	484.7 kB	0.78	748.5 kB	1.04	3 551	38.04
4	HTTPS	TCP	183.1 kB	1.92	521.1 kB	0.84	704.2 kB	0.98	109	1.17
5	NTP	UDP	123.0 kB	1.29	112.4 kB	0.18	235.4 kB	0.33	1 081	11.58
6	SMTP	TCP	155.1 kB	1.63	4.3 kB	0.01	159.4 kB	0.22	1	0.01
7	0	IGMP	4.7 kB	0.05	0	0.00	4.7 kB	0.01	16	0.17
8	0	ICMP	2.7 kB	0.03	1.3 kB	0.00	4.0 kB	0.01	16	0.17
9	0	PIM	1.7 kB	0.02	0	0.00	1.7 kB	0.00	2	0.02
	Totals		9.3 MB		60.7 MB		70.0 MB		9 334	

Figure 17.6 Berichte: Netzwerkstatistik-Daten sortiert nach den häufigsten Diensten

Wenn Sie auf eine IP-Adresse oder einen Rechnernamen in der Ergebnistabelle der Ansicht *By Client/By Server* (nach Client/ nach Server) klicken, wird diese Auswahl automatisch als Filter für die Ansicht *Top Services By Client* (Häufigste Dienste nach Client) verwendet. Sie können diese Ansicht wiederum danach in die Ansicht *Top Services by Server* (Häufigste Dienste nach Server) ändern, oder manuell ein(e) IP/Netzwerk angeben sowie Netzwerkbereiche (z. B. 192.168.1.0/24 oder 10/8), und diese Einstellungen anwenden, indem Sie auf die Schaltfläche *Update* klicken.

Bei den Ansichten *By Service* (Nach Dienst) können Sie ein Protokoll und einen Dienst angeben, mit Komma getrennt (z. B. *TCP,SMTP, UDP,6000*). Wenn Sie kein Protokoll angeben, wird TCP angenommen (z. B. *HTTP* ist auch gültig). Wenn es pro Seite mehr als 20 Ergebnisse gibt, können Sie vorwärts und rückwärts blättern, indem Sie die Schaltflächen für nächste (>>) bzw. vorherige (<<) Seite verwenden.

Der Einfachheit halber können die Netzwerkstatistik-Daten im PDF- oder Excel-Format heruntergeladen werden, indem Sie auf die entsprechende Schaltfläche in der rechten oberen Ecke der Registerkarte *Netzwerkstatistik* klicken. Der Bericht wird aus der aktuell gewählten Ansicht generiert.

Bitte beachten Sie, dass die Bezeichnungen *IN* und *OUT* für Datenverkehr je nach Betrachtungsweise variieren können. Wenn der Proxy eingeschaltet ist,

verbinden sich die Clients auf Port 8080 mit der ASG (auch im Transparenzmodus), so dass Daten, die von den Clients gesendet werden (die Anfrage), auf der internen Netzwerkschnittstelle als *eingehender* Verkehr, und Daten, die an den Client gesendet werden (die Antwort), als *ausgehender Verkehr* angesehen werden.

Tipp – Sie können die Daten sortieren, indem Sie auf die Überschriften in den Tabellenspalten klicken. Um z. B. alle Rechner nach dem eingehenden Datenverkehr zu sortieren, klicken Sie auf die Überschrift *IN*. Der Rechner mit dem meisten Datenverkehr wird dann ganz oben angezeigt. Das Datenvolumen wird beim Datenverkehr in Kibibytes (*KiB*) und Mebibytes (*MiB*) angegeben; beides sind Basis-2-Einheiten des Computerspeichers (z. B. Kibibyte = 2^{10} Bytes = 1 024 Bytes).

Network Security

Im Menü *Berichte >> Network Security* werden relevante Ereignisse betreffend der Netzwerksicherheit von Astaro Security Gateway grafisch dargestellt.

Täglich

Auf der Registerkarte *Täglich* werden statistische Übersichten der letzten 24 Stunden zu den folgenden Ereignissen angezeigt.

- Packet Filter Violations (Paketfilterregelverletzungen)
- Intrusion Prevention Events (Angriffsschutz-Ereignisse)

Packet Filter Violations: Jedes Datenpaket, das verworfen oder abgelehnt wird zählt als Paketfilterregelverletzung. Die Anzahl der Regelverletzungen wird aus einer Zeitspanne von fünf Minuten ermittelt.

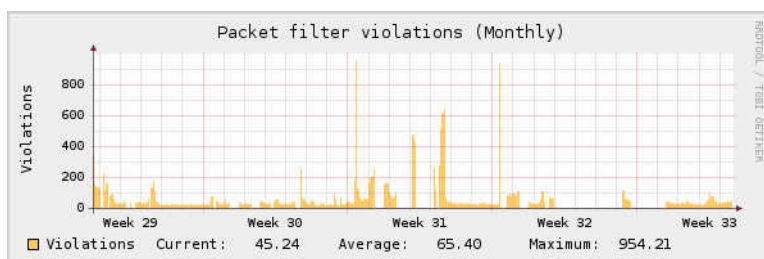


Figure 17.7 Berichte: Diagramm über Paketfilterregelverletzungen

Intrusion Prevention Events: Jedes Diagramm enthält zwei grafische Darstellungen:

- **Alert Events:** Die Anzahl der Datenpakete, die einen Angriff-Alarm ausgelöst haben.
- **Drop Events:** Die Anzahl der Datenpakete, die durch das Angriffsschutz-System verworfen wurden.

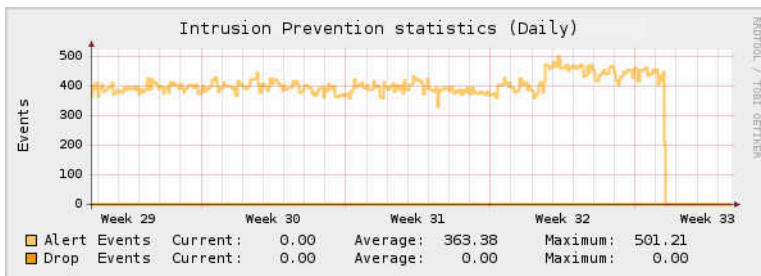


Figure 17.8 Berichte: Diagramm über Angriffsschutz-Ereignisse

Wöchentlich

Auf der Registerkarte *Wöchentlich* werden Paketfilterregelverletzungen und Angriffsschutz-Ereignisse der letzten sieben Tage dargestellt. Die Diagramme werden auf der Seite „Täglich“ beschrieben.

Monatlich

Auf der Registerkarte *Monatlich* werden Paketfilterregelverletzungen und Angriffsschutz-Ereignisse der letzten vier Wochen dargestellt. Die Diagramme werden auf der Seite „Täglich“ beschrieben.

Jährlich

Auf der Registerkarte *Jährlich* werden Paketfilterregelverletzungen und Angriffsschutz-Ereignisse der letzten 12 Monate dargestellt. Die Diagramme werden auf der Seite „Täglich“ beschrieben.

Paketfilter

Die Registerkarte *Network Security >> Paketfilter* bietet umfassende Daten über die Paketfilter-Aktivitäten, dargestellt nach Quell-IP, Quellrechner, Anzahl empfangener Pakete und Anzahl von Diensten.

Wenn Sie auf eine IP-Adresse oder einen Rechnernamen in der Ergebnistabelle klicken, wird diese Auswahl automatisch als Filter für die Ansicht *Top Services* (Häufigste Dienste) verwendet. Sie können manuell eine IP/ ein Netzwerk angeben sowie Netzwerkbereiche (z. B. 192.168.1.0/24 or 10/8) und diese Einstellungen anwenden, indem Sie auf die Schaltfläche *Update* klicken.

Bei den Ansichten *By Service* (Nach Dienst) können Sie ein Protokoll und einen Dienst angeben, mit Komma getrennt (z. B. *TCP,SMTP, UDP,6000*).

Wenn es pro Seite mehr als 20 Ergebnisse gibt, können Sie vorwärts und rückwärts blättern, indem Sie die Schaltflächen für nächste (>) bzw. vorherige (<) Seite verwenden.

Der Einfachheit halber können die Netzwerkstatistik-Daten im PDF- oder Excel-Format heruntergeladen werden, indem Sie auf die entsprechende Schaltfläche in der rechten oberen Ecke der Registerkarte *Paketfilter* klicken. Der Bericht wird aus der aktuell gewählten Ansicht generiert.

Tipp – Sie können die Daten sortieren, indem Sie auf die Überschriften in den Tabellenspalten klicken. Um z. B. die Tabelle nach der Anzahl der Dienste zu sortieren, klicken Sie auf die Überschrift *Services*. Die Quell-IP, die die meisten Dienstanfragen geschickt hat, wird dann ganz oben angezeigt.

IPS

Die Registerkarte *Network Security >> IPS* bietet umfassende Daten zu Angriffsschutz-Aktivitäten (Intrusion Prevention) in Ihrem Netzwerk.

Der Einfachheit halber können die IPS-Daten im PDF- oder Excel-Format heruntergeladen werden, indem Sie auf die entsprechende Schaltfläche in der rechten oberen Ecke der Registerkarte *Paketfilter* klicken. Der Bericht wird aus der aktuell gewählten Ansicht generiert.

Tipp – Sie können die Daten sortieren, indem Sie auf die Überschriften in den Tabellenspalten klicken. Um z. B. die Tabelle nach der Anzahl der Pakete zu sortieren, klicken Sie auf die Überschrift *Packets*. Die Quell-IP, die die meisten Pakete angefragt hat, wird dann ganz oben angezeigt.

Web Security

Im Menü *Berichte* >> *Web Security* werden Statistiken zu den aktivsten Internetnutzern und den meistaufgerufenen Internetadressen (URLs) dargestellt.

Internetnutzung

Die Registerkarte *Web Security* >> *Web Usage* enthält umfangreiche statistische Angaben zu den aktivsten Internetnutzern und den meistaufgerufenen Domänen innerhalb verschiedener Zeiträume. Bestätigen Sie Einstellungen immer durch einen Klick auf die Schaltfläche *Update*. Wenn es pro Seite mehr als 20 Ergebnisse gibt, können Sie vorwärts und rückwärts blättern, indem Sie die Schaltflächen für nächste (>>) bzw. vorherige (<<) Seite verwenden.

Der Einfachheit halber können die Netzwerkstatistik-Daten im PDF- oder Excel-Format heruntergeladen werden, indem Sie auf die entsprechende Schaltfläche in der rechten oberen Ecke der Registerkarte *Internetnutzung* klicken. Der Bericht wird aus der aktuell gewählten Ansicht generiert.

Tipp – Sie können die Daten sortieren, indem Sie auf die Überschriften in den Tabellenspalten klicken. Um z. B. alle Benutzer nach Datenverkehr zu sortieren, klicken Sie auf die Überschrift *Traffic*. Dadurch werden Benutzer mit dem meisten Datenverkehr zuerst aufgeführt. Das Datenvolumen wird beim Datenverkehr in Kibibytes (*KiB*) und Mebibytes (*MiB*) angegeben; beides sind Basis-2-Einheiten des Computerspeichers (z. B. Kibibyte = 2^{10} Bytes = 1 024 Bytes).

Die aktivsten Internetnutzer erscheinen nicht sofort in der Übersicht, sondern erst nachdem eine Sitzungs-Zeitüberschreitung stattgefunden hat. Dies ist der Fall, wenn ein bestimmter Client (Benutzername oder IP-Adresse) für fünf Minuten das Surfen im Internet unterbricht. Das Sicherheitssystem erklärt diese Verbindung für „tot“ und sendet die Information an eine Datenbank, bevor sie in die Liste der aktivsten Internetbenutzer aufgenommen wird.

Zusätzlich können auch die Kriterien *Top Users By Domain* (Aktivste Benutzer nach Domäne) oder *Top Domains By User* (Häufigste Domänen nach Benutzer) ausgewählt werden. Wenn Sie *Top Users By Domain* wählen, geben Sie eine Domäne in das Textfeld *Domain* ein, nach der Sie suchen wollen, und bestätigen Sie Ihre Einstellungen dann mit der Schaltfläche *Update*.

Top	Domain	Users	%	Requests	%	Duration	%	Traffic	%	Domains	%
1		1	0.01	32	0.30	00:30:37	0.32	85.9 KB	0.17	1	0.01
2		1	0.01	144	1.34	00:27:14	0.29	337.1 KB	0.68	1	0.01
3		1	0.01	48	0.45	00:26:55	0.28	172.3 KB	0.35	1	0.01
4		1	0.01	86	0.80	00:25:35	0.27	435.5 KB	0.88	1	0.01
5		1	0.01	17	0.16	00:18:50	0.20	1.7 KB	0.00	1	0.01
6		1	0.01	11	0.10	00:18:02	0.19	3.4 KB	0.01	1	0.01
7		1	0.01	113	1.05	00:17:58	0.19	478.8 KB	0.97	1	0.01
8		1	0.01	88	0.82	00:17:53	0.19	237.7 KB	0.48	1	0.01
9		1	0.01	13	0.12	00:17:07	0.18	0	0.00	1	0.01
10		1	0.01	20	0.19	00:13:52	0.15	2.3 KB	0.00	1	0.01
11		1	0.01	18	0.17	00:13:33	0.14	154.4 KB	0.31	1	0.01
12		1	0.01	10	0.09	00:13:06	0.14	24.6 KB	0.05	1	0.01
13		1	0.01	10	0.09	00:12:43	0.13	22.6 KB	0.05	1	0.01
14		1	0.01	11	0.10	00:11:19	0.12	16.9 KB	0.03	1	0.01
15		1	0.01	5	0.05	00:10:56	0.11	72.4 KB	0.15	1	0.01
16		1	0.01	6	0.06	00:10:24	0.11	33.4 KB	0.07	1	0.01
17		1	0.01	6	0.06	00:10:23	0.11	26.9 KB	0.05	1	0.01
18		1	0.01	8	0.07	00:10:14	0.11	34.5 KB	0.07	1	0.01
19		1	0.01	7	0.07	00:10:08	0.11	113.1 KB	0.23	1	0.01
20		1	0.01	9	0.08	00:10:01	0.10	45.1 KB	0.09	1	0.01
Totals				10 713		159:02:52		48.4 MB			

Figure 17.9 Berichte: Rangliste der häufigsten Domänen

Beachten Sie, dass Sie das Prozentzeichen („%“) kann als Platzhalter verwenden können. Durch das Prozentzeichen wird bekräftigt, dass nach exakten Übereinstimmungen oder Untergruppen gesucht wird. Beispiel: Für die Suchanfrage „beispiel%“ werden die folgenden Domänen angezeigt: beispiel.com, beispiel.net, beispiel.org.

Wenn Sie *Top Domains By User* wählen, geben Sie in das Textfeld *User* die IP-Adresse ein, nach der Sie suchen wollen, und bestätigen Sie Ihre Einstellungen dann mit der Schaltfläche *Update*. Auch hier können Sie das Prozentzeichen als Platzhalter verwenden.

Hinweis zu Error-Domänen – Wenn Client versuchen, sich mit ungültigen URLs zu verbinden, wird der Proxy diese Anfrage protokollieren, aber die Anfrage nicht beantworten können. Diese Links werden mit „error“ als Domäne ausgegeben. Das ist kein Fehler der Berichtsfunktion oder des HTTP/S-Proxy; in den meisten Fällen, tauchen solche Fehler aufgrund von ungültigen oder fehlerhaften Links auf, die auf Webseiten vom Webseitenersteller platziert wurden.

Blockierungen

Die Registerkarte *Web Security* >> *Blockierungen* enthält umfangreiche statistische Information über alle blockierten Webanfragen, basierend auf *Surf Protection* und Antivirus. Bestätigen Sie Einstellungen immer durch einen Klick auf die Schaltfläche *Update*. Wenn es pro Seite mehr als 20 Ergebnisse gibt, können Sie vorwärts und rückwärts blättern, indem Sie die Schaltflächen für nächste (>>) bzw. vorherige (<<) Seite verwenden.

Der Einfachheit halber können die Netzwerkstatistik-Daten im PDF- oder Excel-Format heruntergeladen werden, indem Sie auf die entsprechende Schaltfläche in der rechten oberen Ecke der Registerkarte *Blockierungen* klicken. Der Bericht wird aus der aktuell gewählten Ansicht generiert.

IM

Die Registerkarte *Web Security* >> *IM* bietet umfassende Daten zu Sofortnachrichten-Aktivitäten (Instant Messaging) in Ihrem Netzwerk.

Der Einfachheit halber können die IM-Daten im PDF- oder Excel-Format heruntergeladen werden, indem Sie auf die entsprechende Schaltfläche in der rechten oberen Ecke der Registerkarte *Paketfilter* klicken. Der Bericht wird aus der aktuell gewählten Ansicht generiert.

Tipp – Sie können die Daten sortieren, indem Sie auf die Überschriften in den Tabellenspalten klicken. Um z. B. die Tabelle nach der Anzahl der Pakete zu sortieren, klicken Sie auf die Überschrift *Packets*. Die Quell-IP, die die meisten Pakete angefragt hat, wird dann ganz oben angezeigt.

P2P

Die Registerkarte *Web Security* >> *P2P* bietet umfassende Daten zu Peer-to-Peer-Aktivitäten in Ihrem Netzwerk.

Der Einfachheit halber können die P2P-Daten im PDF- oder Excel-Format heruntergeladen werden, indem Sie auf die entsprechende Schaltfläche in der

rechten oberen Ecke der Registerkarte *Paketfilter* klicken. Der Bericht wird aus der aktuell gewählten Ansicht generiert.

Tipp – Sie können die Daten sortieren, indem Sie auf die Überschriften in den Tabellenspalten klicken. Um z. B. die Tabelle nach der Anzahl der Pakete zu sortieren, klicken Sie auf die Überschrift *Packets*. Die Quell-IP, die die meisten Pakete angefragt hat, wird dann ganz oben angezeigt.

Entanonymisierung

Auf die Registerkarte *Web Security >> Entanonymisierung* kann nur zugegriffen werden, wenn Anonymisierung aktiviert ist (siehe *Berichte >> Einstellungen >> Anonymisierung*).

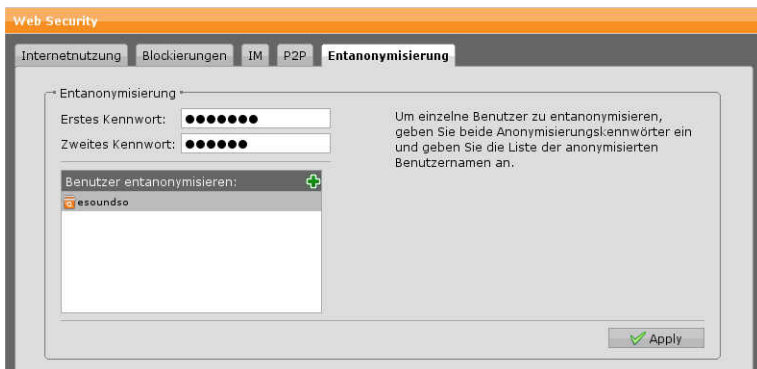


Figure 17.10 Berichte: Entanonymisierung einzelner Benutzer

Es ist hier möglich, die Anonymisierung für bestimmte Benutzer im Hinblick auf Web-Security-Berichte auszusetzen. Gehen Sie folgendermaßen vor:

1. **Geben Sie beide Kennwörter ein.**
Geben Sie das erste und das zweite Kennwort ein, die verwendet wurden, um die Anonymisierung zu aktivieren.
2. **Fügen Sie Benutzer hinzu, die entanonymisiert werden sollen.**
Fügen Sie zum Feld *Benutzer entanonymisieren* die Benutzernamen derjenigen Benutzer hinzu, die Sie entanonymisieren wollen.
3. **Klicken Sie Übernehmen.**
Ihre Einstellungen werden gespeichert.

Mail Security

Die Registerkarten des Menüs *Berichte >> Mail Security* bieten statistische Übersichten über den E-Mail-Verkehr, E-Mail-Nutzung und E-Mail-Sicherheit.

Nutzungsdiagramme

Die Registerkarte *Mail Security >> Nutzungsdiagramme* bietet einen statistischen Überblick über den E-Mail-Verkehr auf der ASG über verschiedene Zeiträume:

- Täglich
- Wöchentlich
- Monatlich
- Jährlich

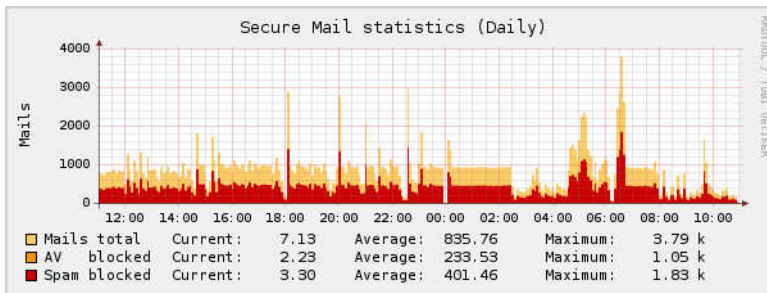


Figure 17.11 Berichte: Diagramm über den E-Mail-Verkehr

Mail-Nutzung

Die Registerkarte *Mail Security >> Mail-Nutzung* enthält umfassende Statistiken über die am häufigsten genutzten E-Mail-Adressen und Adress-Domänen über verschiedene Zeiträume gesehen. Bestätigen Sie Einstellungen immer durch einen Klick auf die Schaltfläche *Update*. Wenn es pro Seite mehr als 20 Ergebnisse gibt, können Sie vorwärts und rückwärts blättern, indem Sie die Schaltflächen für nächste (>>) bzw. vorherige (<<) Seite verwenden.



Figure 17.12 Berichte: Aufstellung der am häufigsten genutzten E-Mail-Adressen

Blockierte Mails

Die Registerkarte *Mail Security* >> *Blockierte Mails* enthält umfassende Statistiken über alle blockierten E-Mail-Anfragen, basierend auf Antivirus und Antispam. Bestätigen Sie Einstellungen immer durch einen Klick auf die Schaltfläche *Update*. Wenn es pro Seite mehr als 20 Ergebnisse gibt, können Sie vorwärts und rückwärts blättern, indem Sie die Schaltflächen für nächste (>>) bzw. vorherige (<<) Seite verwenden.

Entanonymisierung

Auf die Registerkarte *Mail Security* >> *Entanonymisierung* kann nur zugegriffen werden, wenn Anonymisierung aktiviert ist (siehe *Berichte* >> *Einstellungen* >> *Anonymisierung*).

Es ist hier möglich, die Anonymisierung für bestimmte E-Mail-Adressen und/oder Domänen im Hinblick auf Web-Security-Berichte auszusetzen. Gehen Sie folgendermaßen vor:

- 1. Geben Sie beide Kennwörter ein.**

Geben Sie das erste und das zweite Kennwort ein, die verwendet wurden, um die Anonymisierung zu aktivieren.

- 2. Nehmen Sie die folgenden Einstellungen vor:**

Adressen entanonymisieren: Sie können E-Mail-Adressen hinzufügen, die entanonymisiert werden sollen.

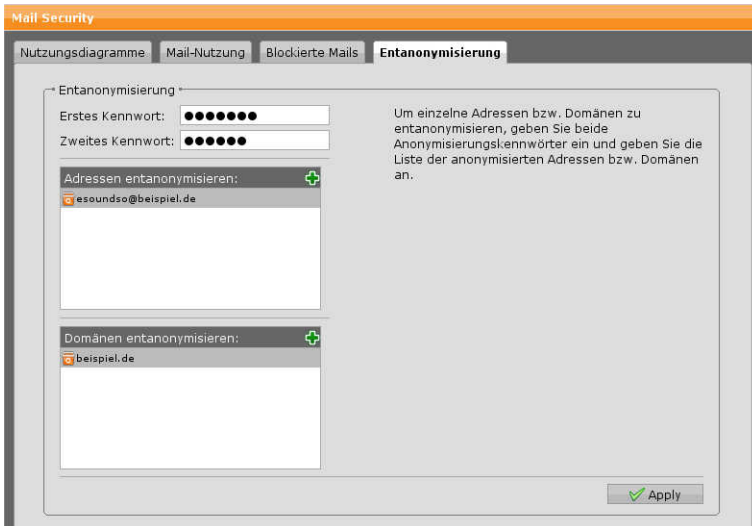


Figure 17.13 Berichte: Entanonymisierung von E-Mail-Adressen und Domänen

Domänen entanonymisieren: Sie können Domänen hinzufügen, die entanonymisiert werden sollen.

3. Klicken Sie *Übernehmen*.

Ihre Einstellungen werden gespeichert. Die angegebenen E-Mail-Adressen und Domänen werden in Berichten nun lesbar angezeigt.

Gesamtbericht

Im Menü *Berichte >> Gesamtbericht* können Sie einen Gesamtbericht erstellen, der eine Zusammenstellung aus den wichtigsten Berichtsdaten ist und in grafischer Form die Netzwerknutzung für eine Reihe von Diensten anzeigt.

Bericht anzeigen

Auf der Registerkarte *Gesamtbericht >> Bericht anzeigen* können Sie einen kompletten Gesamtbericht erstellen, der aus den einzelnen Berichten auf den Registerkarten und Seiten des Menüs *Berichte* zusammengestellt wird. Klicken Sie dazu auf die Schaltfläche *Bericht jetzt erstellen*, um den Gesamtbericht in einem neuen Fenster zu öffnen.

Archivierte Gesamtberichte

Die Registerkarte *Gesamtbericht* >> *Archivierte Gesamtberichte* bietet einen Überblick über alle archivierten Gesamtberichte. Es werden nur diejenigen Gesamtberichte archiviert, für die Archivierung auf der Registerkarte *Konfiguration* aktiviert wurde.

Konfiguration

Auf der Registerkarte *Gesamtbericht* >> *Konfiguration* können Sie die Einstellungen für die Gesamtberichte vornehmen.

Wählen Sie einen Zeitraum für den Gesamtbericht. Der Bericht kann täglich, wöchentlich oder monatlich erstellt werden. Wenn Sie *Wöchentlich* wählen, können Sie zusätzlich noch einen Wochentag auswählen, an dem der Gesamtbericht beginnen soll, seine Daten zu sammeln.

Geben Sie darüber hinaus die E-Mail-Adressen der Empfänger an, die den Gesamtbericht erhalten sollen. Beachten Sie, dass für verschiedene Zeiträume unterschiedliche E-Mail-Adressen konfiguriert werden können.

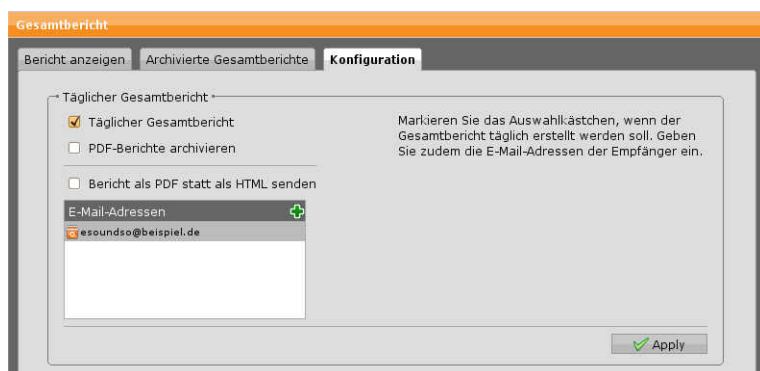


Figure 17.14 Berichte: Konfiguration des täglichen Gesamtberichts

Kapitel 18

Support

Dieses Kapitel beschreibt die Support-Tools (dt. Werkzeuge), die Astaro Security Gateway zur Verfügung stellt.

Die Seiten des Menüs *Support* enthalten viele Funktionen, die den Benutzer unterstützen, von Weblinks über Kontaktinformationen bis hin zu nützlichen Netzwerk-Tools, ohne dass auf die Kommandozeilen-Schnittstelle der Firewall zugegriffen werden muss.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

- Handbuch
- Support kontaktieren
- Tools
- Erweitert

Darüber hinaus enthält die Hauptseite des Menüs *Support* Weblinks zu den folgenden Ressourcen:

- **Knowledgebase:** Astaros offizielle Knowledgebase mit Konfigurationsanleitungen und Informationen rund um Astaro Security Gateway.
- **Known Issue List:** Die beschriebenen Probleme können entweder nicht behoben werden oder es sind Workarounds verfügbar, die zur Lösung führen.
- **Hardware Compatibility List:** Eine Liste mit kompatibler Hardware für die Astaro Security Gateway Software.
- **Up2Date Information:** Astaros Up2Date-Blog informiert über Produktentwicklungen und Firmware-Updates.

Handbuch

Auf der Seite *Support >> Handbuch* kann das aktuelle Administrationshandbuch im PDF-Format heruntergeladen werden. Wählen Sie die Sprache aus und klicken Sie auf die Schaltfläche *Herunterladen*. Um die Datei zu öffnen, benötigen Sie ein spezielles Programm wie Adobe Reader oder Xpdf.

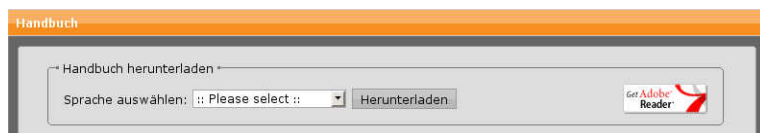


Figure 18.1 Support: Administrationshandbuch von Astaro Security Gateway herunterladen

Hinweis – Um Problemen beim Herunterladen von Dateien mit dem Internet Explorer 6 vorzubeugen, fügen Sie die URL der Firewall (z.B. <https://192.168.2.100>) und des Benutzerportals (z.B. <https://192.168.2.100>) den *Vertrauenswürdigen Sites* hinzu. Beim Internet Explorer 6 befinden sich diese Einstellungen im Menü *Extras >> Internetoptionen >> Sicherheit*. Beim Internet Explorer 7 aktivieren Sie zusätzlich im Fenster *Sicherheitseinstellungen* die Funktion *Automatische Eingabeaufforderung für Dateidownloads*.

Support kontaktieren

Astaro bietet für seine Sicherheitslösungen umfangreiche Unterstützung an. Je nach Support-/Wartungsvertrag gibt es verschiedene Stufen. Diese unterscheiden sich hinsichtlich der Art des Kontakts zum Support und der zugesicherten Reaktionszeit durch die Astaro Service-Abteilung und/oder Astaro-zertifizierte Partner unterscheiden.

Alle Supportfälle, die Astaro Security Gateway betreffen, werden über das Astaro Partner Portal⁴⁰ abgewickelt. Sie können über das Webformular einen Supportfall öffnen, indem Sie auf die Schaltfläche *Open Support Case* klicken.

⁴⁰ https://www.astaro.de/license/support_cases

Tools

Die Registerkarten des Menüs *Support >> Tools* beinhalten nützliche Netzwerk-Tools, mit denen wichtige Netzwerkeigenschaften herausgefunden werden können, ohne auf die Kommandozeilen-Schnittstelle der Firewall zugreifen zu müssen. Die folgenden Tools stehen zur Verfügung:

- Ping
- Traceroute
- DNS-Lookup

Ping-Prüfung

Das Programm *Ping* ist ein Computer-Netzwerkwerkzeug mit dem man testen kann, ob ein bestimmter Rechner über ein IP-Netzwerk erreichbar ist. Ping arbeitet indem es ICMP-Echo-Anfragen an den Zielrechner schickt und auf Antworten in Form von ICMP-Echo-Antworten lauscht. Aus Zeitintervallen und Antworthäufigkeiten schätzt Ping die Dauer des Paketumlaufs und die Paketverlustrate zwischen den Rechnern.

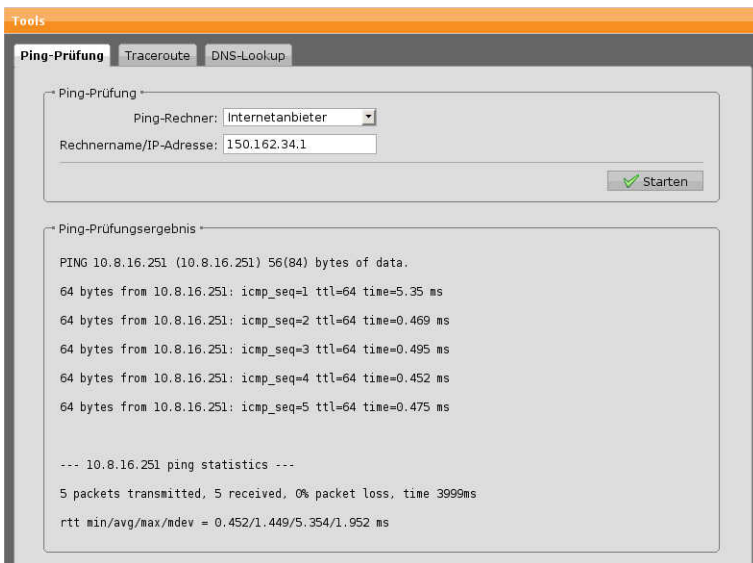


Figure 18.2 Support: Erreichbarkeit eines Rechners mittels Ping testen

Um eine Ping-Prüfung durchzuführen, gehen Sie folgendermaßen vor:

1. Wählen Sie den Ping-Rechner.

Wählen Sie den Rechner, den Sie „anpingen“ möchten. Im Feld *Ping-Rechner* können Sie einen Rechner auswählen, für den eine Rechnerdefinition existiert. Alternativ können Sie auch *Benutzerdefinierter Rechnername/IP-Adresse* wählen und im Feld darunter einen benutzerdefinierten Rechnernamen oder eine IP-Adresse angeben.

2. Klicken Sie Starten.

Die Ausgabe der Ping-Prüfung wird im Abschnitt *Ping-Prüfungsergebnis* angezeigt.

Traceroute

Das Programm *Traceroute* ist ein Computer-Netzwerkwerkzeug zur Bestimmung der Route, die von Paketen in einem IP-Netzwerk genommen werden. Es listet die IP-Adressen der Router auf, über die das versendete Paket transportiert wurde. Sollte der Pfad der Datenpakete kurzfristig nicht nachweisbar sein, wird ein Stern (*) an Stelle der IP-Adresse angezeigt. Nach einer bestimmten Menge an Fehlversuchen wird die Überprüfung abgebrochen. Der Abbruch einer Überprüfung kann viele Gründe haben, der wahrscheinlichste ist jedoch, dass ein Paketfilter im Netzwerkpfad Traceroute-Pakete blockiert.

1. Geben Sie eine(n) Rechnernamen/IP-Adresse ein.

Geben Sie den Rechnernamen oder die IP-Adresse eines Rechners ein, dessen Route Sie bestimmen wollen.

2. Hop-Adressen (Abschnitte) numerisch statt symbolisch und numerisch ausgeben.

Wenn Sie diese Option wählen, wird für jedes Gateway im Pfad eine Adresse-zu-Name-Auflösung durch einen Namensserver durchgeführt und gespeichert.

3. Klicken Sie Starten.

Die Ausgabe von Traceroute wird im Abschnitt *Traceroute-Ergebnis* angezeigt.

DNS-Lookup

Das Programm *dig* (Abkürzung für *Domain Information Groper*) ist ein Netzwerk-Tool zur Abfrage von DNS-Namensservern. Es führt DNS-Lookups

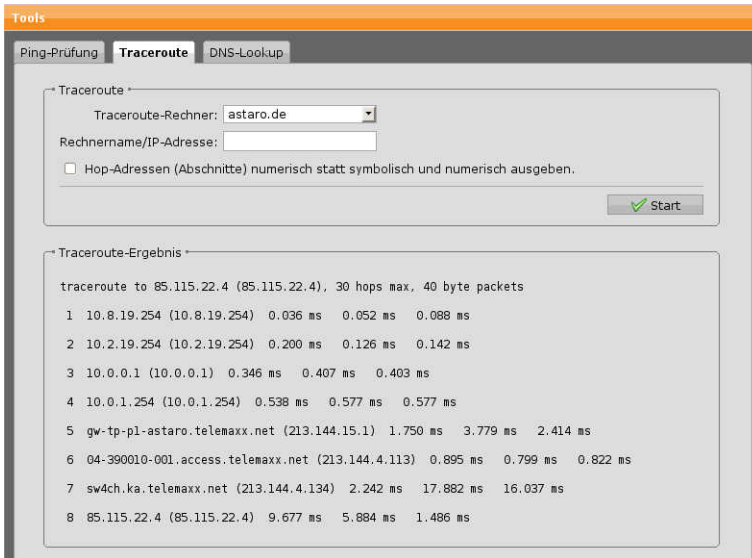


Figure 18.3 Support: Nachvollziehen einer Route mit Hilfe von Traceroute

durch und zeigt die Antworten an, die von den befragten Namensservern zurückkommen. Ein DNS-Lookup bezeichnet das Nachschauen, welcher Domänenname zu welcher IP-Adresse gehört. Diese Information halten Namensserver bereit.

Um ein DNS-Lookup durchzuführen, gehen Sie folgendermaßen vor:

- Geben Sie den Rechnernamen/ die IP-Adresse ein.**
Geben Sie den Rechnernamen oder die IP-Adresse eines Rechners ein, für den Sie DNS-Informationen erhalten wollen.
- Wählen Sie *Ausführliche Ausgabe aktivieren* (optional).** Wählen Sie diese Option, damit in der Ausgabe ausführlichere Informationen auftauchen.
- Klicken Sie *Starten*.**
Die Ausgabe von *dig* wird im Abschnitt *DNS-Suchergebnis* angezeigt.

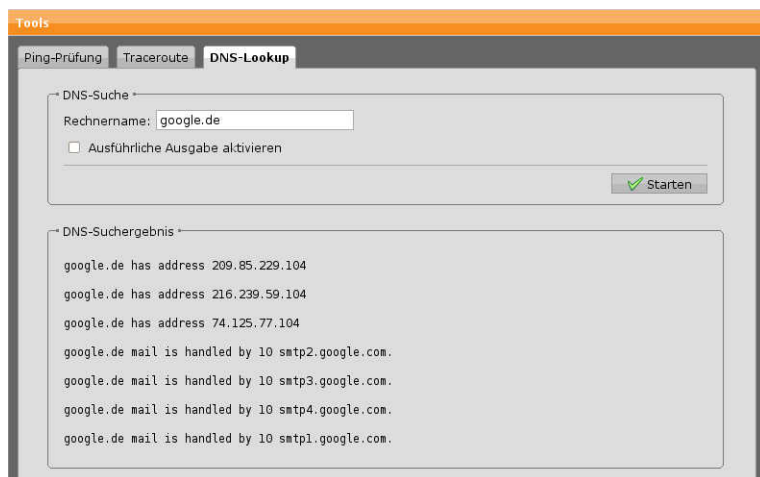


Figure 18.4 Support: Nachschlagen eines DNS-Eintrags mit Hilfe von dig

Erweitert

Im Menü *Support* >> *Erweitert* werden weitere Systeminformationen zu der Firewall angezeigt, wie z. B. der Prozessestatus.

Prozessliste

Das Programm *ps* stellt eine Kopfzeile dar gefolgt von Zeilen, die Informationen über die laufenden Prozesse auf dem System enthalten. Diese Informationen sind nach ihrem „Controlling Terminal“ (dt. kontrollierende Konsole) und dann nach ihrer Prozess-ID sortiert.

Lokale Netzwerkverbindungen

Das Programm *netstat* (Abkürzung für *Network Statistics*, dt. Netzwerkstatistiken) ist ein Netzwerk-Tool, das alle aktiven, sowohl eingehenden als auch ausgehenden, Internetverbindungen anzeigt, die ein Computer augenblicklich besitzt.

Routen-Tabelle

Das Programm *ip* ist ein Netzwerk-Tool, das zur Kontrolle des TCP/IP-Netzwerk- und des Datenverkehrs. Mit dem Parameter `route show table all` werden die Inhalte aller Routing-Tabellen der Firewall angezeigt.

Schnittstellen-Tabelle

In dieser Tabelle werden alle auf Astaro Security Gateway konfigurierten Schnittstellen aufgeführt, sowohl Netzwerkkarten als auch virtuelle Schnittstellen. Die Daten werden vom Programm *ip* durch den Parameter *addr* erzeugt.

Konfig-Abbild

Für die Fehlersuche und für Wiederherstellungszwecke ist es nützlich, so viele Informationen wie möglich über Ihre Installation von Astaro Security Gateway zusammenzutragen. Auf der Registerkarte *Support >> Erweitert >> Konfig-Abbild* kann das Support-Paket heruntergeladen werden. Die zip-Datei enthält die folgenden Elemente:

- Der komplette Auszug der Firewall-Konfiguration (*storage.abf*). Bitte beachten Sie, dass es sich dabei nicht um eine echte Backup-Datei handelt – einige Informationen, z. B. die Kennwörter sind nicht in dieser Datei enthalten – und kann daher nur zur Fehlerbeseitigung genutzt werden.
- Informationen über die gegenwärtig genutzte Hardware (*hwinfo*).
- Informationen über die installierten Software-Pakete (*swinfo*).

Hinweis – Um Problemen beim Herunterladen von Dateien mit dem Internet Explorer 6 vorzubeugen, fügen Sie die URL der Firewall (z. B. <https://192.168.2.100>) und des Benutzerportals (z. B. <https://192.168.2.100>) den *Vertrauenswürdigen Sites* hinzu. Beim Internet Explorer 6 befinden sich diese Einstellungen im Menü *Extras >> Internetoptionen >> Sicherheit*. Beim Internet Explorer 7 aktivieren Sie zusätzlich im Fenster *Sicherheitseinstellungen* die Funktion *Automatische Eingabeaufforderung für Dateidownloads*.

REF_ auflösen

Für die Fehlerbehebung können vom System genutzte *Configuration References* (Konfigurationsreferenzen) aufgelöst werden. Wenn Sie irgendwo in den Protokollen (Logs) auf solche *References* stoßen, können Sie die Zeichenfolge (z. B. *REF_DefaultSuperAdmin*) in das Eingabefeld kopieren. Auf der Registerkarte wird anschließend ein Auszug aus der Datenstruktur des Konfigurations-Daemons angezeigt.

Erweitert

Glossar

ACPI

(Advanced Configuration and Power Interface) ACPI ist ein offener Industriestandard und stellt Schnittstellen zur Hardwareerkennung, Gerätekonfiguration und zum Energiemanagement von Computern zur Verfügung.

AH

(Authentication Header) AH ist ein IPSec-Protokoll und stellt die Authentizität der übertragenen Pakete sicher. Darüber hinaus schützt es gegen Replay-Angriffe.

APIC

(Advanced Programmable Interrupt Controller) ist eine Architektur für die Verteilung von Interrupts in Multiprozessor-Computersystemen.

ARP

(Address Resolution Protocol) ARP ist ein Netzwerkprotokoll, das die Zuordnung von Netzwerkadressen (IP-Adressen) zu Hardwareadressen (MAC-Adressen) möglich macht.

AS

(Autonomes System) Ein AS ist ein IP-Netz, welches als Einheit verwaltet wird und ein gemeinsames (oder auch mehrere) interne Routing-Protokolle verwendet.

BATV

(Bounce Address Tag Validation) BATV ist der Name einer Methode zur Bestimmung ob die Antwort-Adresse einer E-Mail gültig ist. Es wurde entwickelt, um Bounce-Messages für gefälschte Antwort-Adressen zu verwerfen.

Broadcast

Ein Broadcast in einem Computernetzwerk ist eine Nachricht, bei der Datenpakete von einem Punkt aus an alle Teilnehmer eines Netzes übertragen werden. Zum Beispiel: Ein Netzwerk mit der IP-Adresse 192.168.2.0 und einer Netzmaske 255.255.255.0 hat die Broadcast-Adresse 192.168.2.255.

CA

(Certificate Authority) Eine CA (dt. *Zertifizierungsstelle*) ist eine Entität oder Organisation, die digitale Zertifikate herausgibt.

CBC

(Cipher Block Chaining) In der Kryptographie bezeichnet CBC eine Betriebsart, in der Blockchiffrierungsalgorithmen arbeiten. Vor dem Verschlüsseln eines Klartextblocks wird dieser erst mit dem im letzten Schritt erzeugten Geheimtextblock per XOR (exklusives Oder) verknüpft.

DER

(Distinguished Encoding Rules) DER ist eine Methode zur Verschlüsselung von Datenobjekten (z.B. X.509-Zertifikate), um sie digital zu signieren oder um ihre Signatur zu überprüfen.

DNAT

(Destination Network Address Translation) DNAT ist ein spezieller Fall von NAT (Network Address Translation), bei dem die Zieladressinformationen in Datenpaketen durch andere ersetzt werden.

DNS

(Domain Name System) DNS ist ein hierarchisches System von Namen im Internet und dient zur Auflösung dieser Namen in IP-Adressen.

DSA

(Digital Signature Algorithm) DSA ist ein Standard der US-Regierung für digitale Signaturen.

DSL

(Digital Subscriber Line) DSL ist eine Technologie zur digitalen Datenübertragung über herkömmliche Telefonleitungen.

ESP

(Encapsulating Security Payload) ESP ist ein IPSec-Protokoll und sorgt für die Authentifizierung, Integrität und Vertraulichkeit von IP-Paketen.

FTP

(File Transfer Protocol) FTP ist ein Netzwerkprotokoll zur Dateiübertragung über TCP/IP-Netzwerke.

GRE

(Generic Routing Encapsulation) GRE ist ein Netzwerkprotokoll und dient der Einkapselung von Datenpaketen in andere Protokolle, um sie in Form von IP-Tunneln zu transportieren.

H.323

H.323 ist ein Protokoll für die audiovisuelle Kommunikation über paketvermittelte Netzwerke.

ICMP

(Internet Control Message Protocol) ICMP ist ein Teil der Internetprotokollfamilie und dient in Netzwerken zum Austausch von Fehler- und Informationsmeldungen.

IDENT

Das IDENT-Protokoll ist ein Netzwerkprotokoll, mit dem ein Server feststellen kann, welcher Benutzer eines Mehrbenutzersystems eine bestimmte TCP-Verbindung geöffnet hat.

IP

(Internet Protocol) IP ist ein in Computernetzen weit verbreitetes Netzwerkprotokoll und bildet die erste vom Übertragungsmedium unabhängige Schicht der Internetprotokollfamilie.

IP-Adresse

Eine IP-Adresse (Internet-Protocol-Adresse) ist eine Nummer, die die Adressierung von Rechnern und anderen Geräten in einem IP-Netzwerk erlaubt.

IRC

(Internet Relay Chat) IRC ist ein offenes Protokoll und ermöglicht eine direkte Kommunikation über das Internet.

ISP

(Internet Service Provider) Ein ISP ist ein Anbieter von Diensten, Inhalten oder technischen Leistungen, die für die Nutzung oder den Betrieb im Internet erforderlich sind.

LSA

(Link-state Advertisement) LSA ist ein elementares Kommunikationsprinzip innerhalb des OSPF Routing-Protokolls.

MAC-Adresse

Eine MAC-Adresse (Media Access Control) ist die Hardware-Adresse jedes einzelnen Netzwerkadapters, die zur eindeutigen Identifikation des Geräts im Netzwerk dient.

Masquerading

Masquerading ist eine Form von *Network Address Translation*, die es mehreren Computern (mit privaten IP-Adressen) in einem LAN ermöglicht, bei Verwendung einer einzigen öffentlichen IP-Adresse mit dem Internet zu kommunizieren.

MIB

(Management Information Base) Eine MIB ist eine Informationsstruktur zum Verwalten von Netzwerkgeräten (z.B. Router und Switches). Diese stellen Status-, Parameter-, Fähigkeits- und Steuerinformationen über sich selbst in einer MIB zusammen, die an anfragende Geräte gesendet wird.

MD5

(Message-Digest algorithm 5) MD5 ist eine kryptographische Hash-Funktion, die einen 128-Bit-Hashwert erzeugt.

MIME

(Multipurpose Internet Mail Extensions) MIME ist ein Kodierstandard, der die Struktur und den Aufbau von E-Mails und anderer Internetnachrichten festlegt.

MX record

Ein MX-Eintrag ist eine Art Ressourcen-Eintrag im *Domain Name System* (DNS), der festlegt, wie E-Mails über das Internet geroutet werden sollen.

Netzmaske

Eine Netzmaske, oft auch als Subnetzmaske bezeichnet, ist eine Bitmaske, die eine IP-Adresse in einen Netzwerk- und einen Geräte- bzw. Hostteil trennt.

NSSA

(Not-So-Stubby-Area) Eine NSSA ist ein Area-Type im Routingprotokoll OSPF.

NTP

(Network Time Protocol) NTP ist ein Protokoll für die Zeitsynchronisation von Computern in einem Netzwerk.

OpenPGP

OpenPGP ist ein Kryptographie-Protokoll basierend auf PGP (Pretty Good Privacy) zur Verschlüsselung von Informationen und Erzeugung digitaler Signaturen.

OSPF

(Open Shortest Path First) OSPF ist ein dynamisches Routing-Protokoll, das auf einem Link-State-Algorithmus basiert.

PEM

(Privacy Enhanced Mail) PEM ist ein frühes Protokoll zur Verschlüsselung von E-Mails mittels eines asymmetrischen Verschlüsselungsverfahrens.

POP3

(Post Office Protocol version 3) POP3 ist ein Protokoll für die Übertragung von E-Mails in einem paketvermittelten Netzwerk.

Port

Ports sind Adresskomponenten, die in Netzwerkprotokollen eingesetzt werden, um Datenpakete den richtigen Diensten (Protokollen) zuzuordnen.

Protokoll

Protokolle sind Regeln, welche das Format, den Inhalt, die Bedeutung und die Reihenfolge gesendeter Nachrichten zwischen verschiedenen Instanzen (der gleichen Schicht) festlegen.

Proxy

Ein Proxy ist ein zwischengeschalteter Computer, der zur Pufferung, Überwachung und Zugriffskontrolle dient.

RADIUS

(Remote Authentication Dial In User Service) RADIUS ist ein Client-Server-Protokoll, das zur Authentifizierung, Autorisierung und zum Accounting von Benutzern bei Einwahlverbindungen in ein Computernetzwerk dient.

RAID

(Redundant Array of Independent Disks) Ein RAID-System dient zur Organisation mehrerer physikalischer Festplatten eines Computers zu einem logischen Laufwerk.

RBL

(Real-time Blackhole List) Eine RBL ist eine in Echtzeit abfragbare *Schwarze Liste*, die verwendet wird, um E-Mails zweifelhafter Herkunft als Spam zu klassifizieren.

Router

Ein Router ist ein Vermittlungsrechner, der in einem Netz dafür sorgt, dass bei ihm eintreffende Daten eines Protokolls zum vorgesehenen Zielnetz bzw. Subnetz weitergeleitet werden.

SIP

(Session Initiation Protocol) SIP ist ein Netzprotokoll zum Aufbau einer Kommunikationssitzung zwischen zwei oder mehr Teilnehmern und wird hauptsächlich im Zusammenhang mit *Voice over IP* Anwendungen verwendet.

S/MIME

(Secure / Multipurpose Internet Mail Extensions) S/MIME ist ein Standard für die Verschlüsselung und Signatur von MIME-gekapselter E-Mail durch ein asymmetrisches Verschlüsselungsverfahren.

SMTP

(Simple Mail Transfer Protocol) SMTP ist ein Protokoll der Internetprotokollfamilie, das zum Austausch von E-Mails in Computernetzen dient.

SNAT

(Source Network Address Translation) SNAT ist ein Spezialfall von *Network Address Translation* (NAT) bei dem die Quell-IP-Adresse ersetzt wird.

SOCKS

"SOCKS" ist eine Abkürzung für "SOCKetS", ein Protokoll, das es Client-Server-Anwendungen erlaubt, transparent die Dienste einer Firewall zu nutzen.

SPF

(Sender Policy Framework) SPF ist eine Erweiterung des SMTP Protokolls zum Schutz gegen das Versenden von Spam-E-Mails mit falschen Absender-Adressen.

SPI

(Security Parameter Index) SPI identifiziert in Verbindung mit der IP-Adresse und dem Sicherheitsprotokoll die Sicherheitsassoziation beim Tunneln von Daten mit IPSec.

SSH

(Secure Shell) SSH ist ein Protokoll bzw. Implementierung dieses Protokolls, mit dem sich eine verschlüsselte Netzwerkverbindung zu einem

entfernten Computer aufbauen lässt.

SSO

(Single Sign-On) SSO bedeutet, dass ein Benutzer nach einer einmaligen Authentifizierung auf alle Rechner und Dienste, für die er berechtigt ist, zugreifen kann, ohne sich jedes Mal neu anmelden zu müssen.

TCP

(Transmission Control Protocol) TCP ist ein Protokoll der Internet-Protokollfamilie, das zusammen mit dem Internetprotokoll (IP) eingesetzt wird, um Daten in Form von Paketen zwischen Computern über das Internet zu transportieren.

TLS

(Transport Layer Security) TLS und sein Vorgänger *Secure Sockets Layer* (SSL) sind Verschlüsselungsprotokolle für die sichere Datenübertragung im Internet.

TTL

(Time-to-live) TTL ist der Name eines Header-Felds des Internetprotokolls (IP) und gibt an, wie lange ein Paket auf dem Weg vom Ziel zum Sender unterwegs sein darf, bevor es verworfen wird, und soll verhindern, dass unzustellbare Pakete unendlich lange weitergeroutet werden.

UDP

(User Datagram Protocol) UDP ist ein Protokoll für den verbindungslosen Datenaustausch, das hauptsächlich für die Verteilung von Nachrichten über ein Netzwerk verwendet wird.

USV

Ein Gerät zur unterbrechungsfreien Stromversorgung (USV) wird eingesetzt, um bei Störungen der Stromversorgung einen durchgehenden Betrieb zu ermöglichen.

URL

(Uniform Resource Locator) URLs identifizieren eine Ressource in Computernetzwerken und sind der Standard von Adressen im Internet.

VoIP

(Voice over IP) Unter VoIP versteht man ganz allgemein das Telefonieren über Computernetzwerke.

VPN

(Virtual Private Network) Ein VPN ist eine verschlüsselte Verbindung zwischen zwei Standorten, die zum Transport privater Daten ein öffentliches Netz wie das Internet nutzt.

WINS

(Windows Internet Naming Service) WINS ist ein von Microsoft entwickeltes System zur dynamischen Auflösung von NetBIOS-Namen.

X.509

X.509 ist ein Standard für digitale Zertifikate, der von der ITU-T (International Telecommunications Union – Telecommunication) herausgegeben wird. Dort sind Informationen und Attribute spezifiziert, die zur Identifikation einer Person oder eines Computers erforderlich sind.

Abbildungsverzeichnis

1.1	IE7 Sicherheitseinstellungen	3
1.2	Initiale Anmeldemaske des WebAdmin	10
1.3	Reguläre Anmeldemaske des WebAdmin	11
1.4	WebAdmin-Dashboard	13
2.1	WebAdmin: Übersicht	15
2.2	WebAdmin: Beispiel einer Liste	18
2.3	WebAdmin: Beispiel eines Dialogfensters	18
2.4	WebAdmin: Ziehen eines Objekts aus der Objektleiste <i>Networks</i>	22
3.1	WebAdmin: Beispielhafte Dashboard-Anzeige der ASG Software V7 WebAdmin	23
4.1	Systemeinstellungen: Einstellung von Datum und Uhrzeit	30
4.2	WebAdmin-Einstellungen: Konfiguration der WebAdmin-Zugriffskontrolle	34
4.3	WebAdmin-Einstellungen: Konfiguration der Benutzereinstellungen	37
4.4	MyAstaro-Portal	38
4.5	Lizenzen: Warnhinweis zur Lizenz	43
4.6	Lizenzen: Lizenzübersicht (Klassisches Lizenzmodell)	44
4.7	Lizenzen: Installation einer Lizenz	44
4.8	Up2Date: Übersicht	46
4.9	Up2Date: Fortschrittsbalken	47
4.10	Up2Date: Installation von Up2Date-Paketen, die inbegriffen sind	47
4.11	Benutzerportal: Benutzerportal von Astaro Security Gateway	55
4.12	Benutzerportal: Zugriffskontrolle für das Benutzerportal	57

4.13	Anpassung: Beispiel einer blockierten Webseite mit Angabe der anpassbaren Elemente	62
4.14	HTTP-Proxy: HTTP-Statusmeldung Schritt 1 von 3	64
4.15	HTTP-Proxy: HTTP-Statusmeldung Schritt 2 von 3	65
4.16	HTTP-Proxy: HTTP-Statusmeldung Schritt 3 von 3	65
4.17	POP3-Proxy: Blockierte POP3-Nachricht	66
4.18	SNMP: Konfiguration von SNMP-Anfragen	67
4.19	Zentralverwaltung: Dashboard von Astaro Command Center	71
4.20	Zentralverwaltung: Konfiguration der zentralen Verwaltung durch einen ACC V1.9-Server	73
4.21	Zentralverwaltung: Konfiguration der zentralen Verwaltung durch einen ACC V1.4-Server	75
4.22	Hochverfügbarkeit: Statusseite	79
4.23	Hochverfügbarkeit: Ressourcennutzung der einzelnen HA- oder Cluster-Geräte	80
4.24	Hochverfügbarkeit: Konfiguration eines Clusters	83
5.1	Benutzer: Benutzerkonten	90
5.2	Gruppen: Gruppenliste	92
5.3	Gruppen: eDirectory Browser of Astaro Security Gateway	95
5.4	Authentifizierung: Benutzerauthentifizierung mit eDirectory	98
5.5	Authentifizierung: Benutzerauthentifizierung mit Active Directory	100
5.6	Authentifizierung: Microsoft Management-Konsole	103
5.7	Authentifizierung: Benutzerauthentifizierung mit LDAP	104
5.8	Authentifizierung: Benutzerauthentifizierung mit RADIUS	107
5.9	Authentifizierung: Benutzerauthentifizierung mit TACACS+	109
5.10	Authentifizierung: Konfiguration von Single Sign-On	111

6.1	Definitionen: Liste der Netzwerkdefinitionen	116
6.2	Dienste: Dienstdefinitionen	119
6.3	Zeitereignisse: Liste der Zeitereignisdefinitionen	122
7.1	Schnittstellen: Konfiguration von Schnittstellen	127
7.2	Schnittstellen: Konfiguration der Uplink-Ausgleich-Funktion	144
7.3	Schnittstellen: Multipfad-Regeln	146
7.4	Bridging: Konfiguration einer Bridge	149
7.5	Bridging: Aktiviertes Bridging	151
7.6	Bridging: Entfernen einer Bridge	151
7.7	Statisches Routing: Tabelle der statischen Routen	152
7.8	Statisches Routing: Tabelle der Richtlinienrouten	154
7.9	OSPF: Konfiguration von OSPF	156
7.10	OSPF: Übersicht mit konfigurierten Bereichen	160
7.11	QoS: Status	164
7.12	QoS: Verkehrskennzeichner	166
7.13	QoS: Bandbreiten-Pools	168
7.14	Beispielkonfiguration PIM-SM	170
7.15	PIM-SM: Schnittstellenliste	171
7.16	PIM-SM: Liste der Rendezvous-Point-Router	173
7.17	PIM-SM: Routen-Liste	174
8.1	DNS: Konfiguration von DynDNS	180
8.2	DHCP: Konfiguration eines DHCP-Relay	185
8.3	DHCP: Lease-Tabelle	187
9.1	Paketfilter: Regelsatz	190

9.2	Paketfilter: Live-Protokoll	192
9.3	NAT: Maskierungsregeln	199
9.4	NAT: Regeln	200
9.5	Angriffsschutz: Aktivierung des Angriffsschutzsystems	203
9.6	Angriffsschutz: IPS-Regelwerk	206
9.7	Angriffsschutz: Konfiguration des Flood-Schutzes	207
9.8	Angriffsschutz: Konfiguration des Portscan-Schutzes	210
9.9	Angriffsschutz: Ausnahmenliste	212
9.10	Server-Lastverteilung: Lastverteilungsregeln	215
9.11	Generischer Proxy: Regelliste	217
10.1	HTTP-Proxy: Allgemeine Einstellungen	222
10.2	HTTP-Proxy: Konfiguration der Antiviren- und Schadsoftware-Einstellungen	226
10.3	HTTP-Proxy: Konfiguration für das Entfernen von aktivem Inhalt	227
10.4	HTTP-Proxy: Konfiguration der URL-Filterung	229
10.5	HTTP-Proxy: Ausnahmenliste	233
10.6	HTTP-Proxy: Erweiterte Einstellungen, Teil 1	235
10.7	HTTP-Proxy: Erweiterte Einstellungen, Teil 2	237
10.8	Proxy-Profile: Liste der Proxy-Profile	245
10.9	Proxy-Profile: Liste der Filterzuweisungen	249
10.10	Proxy-Profile: Liste der Filteraktionen	251
10.11	FTP-Proxy: Grundeinstellungen	254
10.12	FTP-Proxy: Konfiguration von Antivirus für den FTP-Proxy	255
10.13	FTP-Proxy: Definition von Ausnahmen	256
10.14	FTP-Proxy: Konfiguration der erweiterten Einstellungen	258

11.1	SMTP-Proxy: Grundeinstellungen	260
11.2	SMTP-Proxy: Konfiguration von Domänen und Routingzielen	261
11.3	SMTP-Proxy: Konfiguration der Antivirus-Einstellungen	264
11.4	SMTP-Proxy: Dateierweiterungsfilter	265
11.5	SMTP-Proxy: Fußzeile zur Antivirenprüfung	267
11.6	SMTP-Proxy: Konfiguration der Antispam-Einstellungen	268
11.7	SMTP-Proxy: Erweiterung der Absender-Blacklist	271
11.8	SMTP-Proxy: Hinzufügen von Ausdrücken zum Ausdruckfilter	272
11.9	SMTP-Proxy: Erweiterte Antispam-Funktionen	274
11.10	SMTP-Proxy: Ausnahmenliste	275
11.11	SMTP-Proxy: Konfiguration von Relaying	277
11.12	SMTP-Proxy: Aktivierung der Blacklist für Rechner/Netzwerke	279
11.13	SMTP-Proxy: Aktivierung des Inhaltsscans für Relay-Nachrichten	279
11.14	SMTP-Profile: Konfiguration eines SMTP-Profiles	283
11.15	POP3-Proxy: Grundkonfiguration	289
11.16	POP3-Proxy: Konfiguration der Antivirus-Einstellungen	290
11.17	POP3-Proxy: Konfiguration der Antispam-Einstellungen	292
11.18	POP3-Proxy: Ausnahmen definieren	294
11.19	POP3-Proxy: Konfiguration der erweiterten Einstellungen	296
11.20	E-Mail-Verschlüsselung: E-Mail-Verschlüsselung mit zwei Astaro Security Gateways	304
11.21	E-Mail-Verschlüsselung: Konfiguration	304
11.22	E-Mail-Verschlüsselung: Optionen	305
11.23	E-Mail-Verschlüsselung: Liste der internen Benutzer	307
11.24	E-Mail-Verschlüsselung: Liste der S/MIME-Instanzen	310

11.25 E-Mail-Verschlüsselung: Liste der S/MIME-Zertifikate	312
11.26 E-Mail-Verschlüsselung: Liste der öffentlichen OpenPGP-Schlüssel	313
11.27 Quarantänebericht: Täglicher Quarantänebericht von Astaro Security Gateway	314
11.28 Quarantänebericht: Allgemeine Einstellungen	316
11.29 Quarantänebericht: Ausnahmen	318
11.30 Quarantänebericht: Erweiterte Optionen	320
11.31 Mail-Manager: Mail-Manager von Astaro Security Gateway	321
11.32 Mail-Manager: Übersicht	328
11.33 Mail-Manager: Konfiguration	330
12.1 VoIP SIP: Konfiguration der Einstellungen	332
12.2 VoIP H.323: Konfiguration der Einstellungen	333
13.1 IM/P2P: Konfiguration der allgemeinen IM/P2P-Einstellungen	336
13.2 IM/P2P: Erweiterte Einstellungen	337
13.3 Sofortnachrichten: Konfiguration der Dienste	338
13.4 Sofortnachrichten: Ausnahmenliste	340
13.5 P2P: Konfiguration der Dienste	342
13.6 P2P: Ausnahmenliste	344
14.1 Site-to-Site IPSec: Verbindungen	349
14.2 Site-to-Site IPSec: Liste entfernter Gateways	350
14.3 Site-to-Site IPSec: Liste der Richtlinien	354
14.4 Site-to-Site IPSec: Konfiguration des lokalen RSA-Schlüssels	357
14.5 Site-to-Site IPSec: Konfiguration der erweiterten Einstellungen	359
14.6 Site-to-Site SSL: Konfiguration der Serververbindung	363
14.7 Site-to-Site SSL: Konfiguration der Clientverbindung	365

14.8	Site-to-Site-VPN SSL: Konfiguration der Einstellungen	366
14.9	Site-to-Site-VPN SSL: Konfiguration der erweiterten Einstellungen	368
14.10	Site-to-Site-VPN: Zertifikatliste	370
14.11	Site-to-Site-VPN: Liste der Zertifizierungsstellen	373
14.12	Site-to-Site-VPN: Liste der Sperrlisten (CRLs)	375
14.13	Site-to-Site-VPN: Erweiterte Einstellungen	376
15.1	Installationsdateien für den Fernzugriff im Benutzerportal	378
15.2	Fernzugriff SSL: Konfiguration	379
15.3	Fernzugriff SSL: Konfiguration der Einstellungen	381
15.4	Fernzugriff SSL: Konfiguration der erweiterten Einstellungen	383
15.5	Fernzugriff PPTP: Grundeinstellungen	384
15.6	Fernzugriff PPTP: Konfiguration von iPhone-Fernzugriff	387
15.7	Fernzugriff PPTP: Erweiterte Einstellungen	388
15.8	Fernzugriff L2TP: Grundeinstellungen	389
15.9	Fernzugriff L2TP: Konfiguration von iPhone-Fernzugriff	393
15.10	Fernzugriff L2TP: Erweiterte Einstellungen	394
15.11	Fernzugriff IPSec: Verbindungen	397
15.12	Fernzugriff IPSec: Liste der Richtlinien	399
15.13	Fernzugriff IPSec: Konfiguration der erweiterten Einstellugnen	403
15.14	Cisco VPN Client: Konfiguration	407
15.15	Cisco VPN Client: Konfiguration des iPhone-Fernzugriffs	408
15.16	Fernzugriff: Erweiterte Einstellungen	410
16.1	Protokollierung: Lokale Protokollierung einschalten	414
16.2	Protokollierung: Konfiguration eines Remote-Syslog-Servers	416

16.3	Protokollierung: Konfiguration eines ausgelagerten Protokollarchivs	417
16.4	Protokollierung: Protokollübersicht	420
16.5	Protokollierung: Auswahl von archivierten Protokolldateien	421
16.6	Protokollierung: Protokolldateien durchsuchen	422
17.1	Berichte: Aktivierung der Anonymisierung von Benutzerdaten	425
17.2	Berichte: Diagramm über die CPU-Auslastung	427
17.3	Berichte: Diagramm über die Speicher-/Swap-Auslastung	428
17.4	Berichte: Diagramm über die Auslastung der Speicherpartition	428
17.5	Berichte: Diagramm über den Datendurchsatz einer Ethernet-Schnittstelle	430
17.6	Berichte: Netzwerkstatistik-Daten sortiert nach den häufigsten Diensten	431
17.7	Berichte: Diagramm über Packetfilterregelverletzungen	432
17.8	Berichte: Diagramm über Angriffsschutz-Ereignisse	433
17.9	Berichte: Rangliste der häufigsten Domänen	436
17.10	Berichte: Entanonymisierung einzelner Benutzer	438
17.11	Berichte: Diagramm über den E-Mail-Verkehr	439
17.12	Berichte: Aufstellung der am häufigsten genutzten E-Mail-Adressen	440
17.13	Berichte: Entanonymisierung von E-Mail-Adressen und Domänen	441
17.14	Berichte: Konfiguration des täglichen Gesamtberichts	442
18.1	Support: Administrationshandbuch von Astaro Security Gateway herunterladen	444
18.2	Support: Erreichbarkeit eines Rechners mittels Ping testen	445
18.3	Support: Nachvollziehen einer Route mit Hilfe von Traceroute	447
18.4	Support: Nachschlagen eines DNS-Eintrags mit Hilfe von dig	448